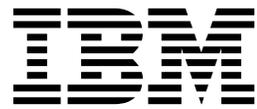


IBM Tivoli Composite Application Manager for Applications  
Version 7.3

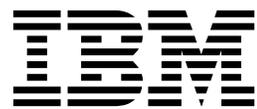
*WebSphere MQ Monitoring Agent  
User's Guide*





IBM Tivoli Composite Application Manager for Applications  
Version 7.3

*WebSphere MQ Monitoring Agent  
User's Guide*



**Note:**

Before using this information and the product it supports, read the information in "Notices" on page 205.

This edition applies to version 7.3 of WebSphere MQ Monitoring agent (product number 5724-V09) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 1996, 2014.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>Figures</b> . . . . .	<b>vii</b>
--------------------------	------------

<b>Tables</b> . . . . .	<b>ix</b>
-------------------------	-----------

## Chapter 1. Introducing WebSphere MQ

### Monitoring agent . . . . . 1

New in this release . . . . .	1
Supported versions of WebSphere MQ. . . . .	1
WebSphere MQ Monitoring agent overview . . . . .	2
User interface . . . . .	2
Attributes . . . . .	3
Event indicator and event workspace . . . . .	4
IBM Tivoli Monitoring . . . . .	6
Client. . . . .	6
Server . . . . .	6
Agent. . . . .	7
Agent Management Services . . . . .	7
IBM Tivoli OMEGAMON DE. . . . .	7
Policy management . . . . .	9
Where to find more information . . . . .	9

### Chapter 2. Customizing monitoring options . . . . . 11

Creating multiple instances of the WebSphere MQ Monitoring agent . . . . .	11
Creating multiple instances on Windows systems . . . . .	11
Creating multiple instances on UNIX and Linux systems. . . . .	12
Creating multiple instances on i5/OS systems . . . . .	12
Changing monitoring options . . . . .	14
Changing monitoring options on UNIX and Linux systems . . . . .	14
Changing monitoring options on Windows systems. . . . .	15
Changing monitoring options on i5/OS systems . . . . .	17
Monitoring a multi-instance queue manager . . . . .	18
Configuring remote agents . . . . .	20
Configuring remote agents through Tivoli Enterprise Portal. . . . .	20
Configuring remote agents from the command line . . . . .	20
Parameters for remote configuration through Tivoli Enterprise Portal . . . . .	21
Monitoring options . . . . .	26
SET GROUP . . . . .	26
SET MANAGER. . . . .	29
SET QACCESS . . . . .	36
SET QUEUE . . . . .	39
SET CHANNEL . . . . .	41
SET EVENTLOG . . . . .	42
SET EVENTQIN. . . . .	43
SET EVENTQOUT . . . . .	46
PERFORM INCLUDE . . . . .	48
PERFORM STARTMON . . . . .	48

SET AGENT . . . . .	50
SET APPL (z/OS systems only). . . . .	51
SET MQIMONITOR (z/OS systems only) . . . . .	53
SET QSG (z/OS systems only) . . . . .	55
SET SUBSYSTEM (z/OS systems only) . . . . .	56

### Chapter 3. Using situations and Take Action commands . . . . . 59

Predefined situations . . . . .	59
Creating a situation using a predefined situation as a template . . . . .	59
Take Action commands . . . . .	60
Creating a custom Take Action command . . . . .	60
Sending a Take Action command . . . . .	61
Using Take Action commands in situations . . . . .	61

### Chapter 4. Data collection for workspaces . . . . . 63

Collecting data for the Application Accounting workspace. . . . .	63
Collecting data for the Application Debugging workspace. . . . .	64
Collecting data for the Application Statistics workspaces . . . . .	65
Collecting data for the Buffer Pool Statistics workspaces . . . . .	65
Collecting data for the Channel Performance and Channel Status workspace . . . . .	66
Collecting data for channel related workspaces . . . . .	66
Collecting data for the Event Log workspace . . . . .	67
Collecting data for the Queue Accounting workspace. . . . .	68
Collecting data for the Queue Statistics workspace . . . . .	69
Collecting data for the Queue Statistics workspace on z/OS systems . . . . .	70
Collecting data for the Queue Status workspace . . . . .	71
Collecting data for the Log Manager workspaces . . . . .	71
Collecting data for the Message Manager workspaces . . . . .	72
Collecting data for the MQSeries Events workspace . . . . .	73
Collecting data for the MQI Statistics workspace . . . . .	73
Collecting data for the MQ Channel Statistics workspace. . . . .	74
Collecting data for the MQ Queue Statistics workspace. . . . .	75
Collecting data for queue related workspaces . . . . .	76
Collecting data for the Topic Manager workspaces . . . . .	77

### Chapter 5. Collecting historical data . . . . . 79

Enabling historical data collection . . . . .	79
Enabling historical data collection on Windows systems. . . . .	80
Enabling historical data collection on UNIX and Linux systems . . . . .	80

Enabling historical data collection on i5/OS systems . . . . .	81
Enabling historical data collection on z/OS systems . . . . .	82
Starting historical data collection . . . . .	82
Stopping historical data collection . . . . .	83
Viewing historical data for a selected time frame . . . . .	83
Tables available for historical data collection . . . . .	85
A mapping table for attribute groups and historical workspaces . . . . .	85

**Chapter 6. Manipulating WebSphere MQ messages. . . . . 89**

Settings for controlling access to WebSphere MQ messages . . . . .	89
Setting the message access authorization level . . . . .	90
Interrelationship of Message Manipulation Access and Message Manipulation Account settings . . . . .	91

**Chapter 7. Collecting queue statistics data . . . . . 95**

Enabling queue statistics monitoring . . . . .	95
Queue Statistics feature consideration . . . . .	96
Queue service interval events monitoring . . . . .	96
Queue events information monitoring . . . . .	96
Another application using the Reset Queue Statistics command . . . . .	96
Coexistence with Application Statistics (z/OS systems only) . . . . .	96

**Chapter 8. Monitoring the publish and subscribe environment. . . . . 97**

Subscription topology . . . . .	97
Situations for queue depth monitoring . . . . .	98
Searching for publish and subscribe information (WebSphere MQ 7.0 or later) . . . . .	98
Viewing the subscription topology . . . . .	101
Preventing destination queues from overflowing (WebSphere MQ 7.0 or later) . . . . .	101
Resolving publishing failures . . . . .	103

**Chapter 9. Running Reports with Tivoli Common Reporting . . . . . 105**

Prerequisite . . . . .	105
Installing Cognos reports for WebSphere MQ Monitoring agent . . . . .	106
Working with reports . . . . .	107
Creating or editing web-based reports . . . . .	108
Creating ad hoc reports . . . . .	108
Data model of WebSphere MQ Monitoring agent . . . . .	109
Sample reports . . . . .	110
Known problems and workarounds . . . . .	113

**Chapter 10. Monitoring with workspaces . . . . . 115**

Creating custom workspaces . . . . .	115
Predefined workspaces . . . . .	115
Creating a workspace using a predefined workspace as a template . . . . .	116

Application Accounting workspaces (distributed systems only) . . . . .	116
Guide for action . . . . .	117
Application Debugging workspaces (z/OS systems only) . . . . .	118
Guide for action . . . . .	118
Application Statistics workspaces (z/OS systems only) . . . . .	118
Application Statistics feature (z/OS systems only) . . . . .	118
Guide for action . . . . .	119
Buffer Pool Statistics workspaces (z/OS systems only) . . . . .	119
Guide for action . . . . .	119
Channel Definitions workspaces . . . . .	120
Guide for action . . . . .	121
Channel Initiator Status workspaces (z/OS systems only) . . . . .	121
Guide for action . . . . .	121
Channel Performance workspaces . . . . .	122
Guide for action . . . . .	122
Cluster Queue Manager workspaces . . . . .	123
Guide for action . . . . .	123
Dead-Letter Queue Messages Workspaces . . . . .	123
Guide for action . . . . .	123
Deleting a message from the dead-letter queue . . . . .	124
Forwarding a message on the dead-letter queue to another queue . . . . .	124
Error Log workspaces (distributed systems only) . . . . .	125
Error Log monitoring (distributed systems only) . . . . .	125
Guide for action . . . . .	126
Log Data Set Status workspace (z/OS systems only) . . . . .	126
Guide for action . . . . .	126
Log Manager Performance workspaces (z/OS systems only) . . . . .	126
Guide for action . . . . .	127
Message Manager Performance workspaces (z/OS systems only) . . . . .	127
Guide for action . . . . .	127
Message Statistics workspaces . . . . .	128
Message Statistics feature . . . . .	128
Guide for action . . . . .	130
MQ Action Log workspace . . . . .	130
Guide for action . . . . .	131
MQI Statistics workspaces (distributed systems only) . . . . .	131
Guide for action . . . . .	132
MQSeries Events workspaces . . . . .	132
Guide for action . . . . .	133
Searching for WebSphere MQ events . . . . .	133
Page Set Statistics workspaces (z/OS systems only) . . . . .	134
Guide for action . . . . .	134
Publish Subscribe workspaces . . . . .	135
Guide for action . . . . .	135
Queue Definitions workspaces . . . . .	135
Guide for action . . . . .	136
Queue Manager Status workspaces . . . . .	136
Guide for action . . . . .	136
Application topology view . . . . .	137
Queue Statistics workspaces . . . . .	144

Purging a local queue . . . . .	145
Clearing a local queue . . . . .	145
Guide for action . . . . .	146
Queue-Sharing Group workspaces (z/OS systems only) . . . . .	147
Guide for action . . . . .	147
Queue-Sharing Group Monitoring (z/OS systems only) . . . . .	148
Queue Messages workspace . . . . .	148
Guide for action . . . . .	149
Deleting a message from a queue. . . . .	149
Forwarding a message to another queue . . . . .	149
Topic Manager Performance workspaces(z/OS systems only) . . . . .	150
Guide for action . . . . .	150
Additional workspace information . . . . .	150

**Chapter 11. Configuring in a cluster environment on Windows systems . . . 151**

Introducing MSCS clusters . . . . .	151
Active/active clustering . . . . .	152
Prerequisites. . . . .	153
Configuring the WebSphere MQ Monitoring agent . . . . .	154
Active/passive clustering . . . . .	157
Prerequisites. . . . .	157
Configuring the WebSphere MQ Monitoring agent . . . . .	158

**Chapter 12. Configuring in a cluster environment on AIX systems. . . . . 163**

Active/active clustering . . . . .	163
Active/passive clustering . . . . .	165
Configuring the WebSphere MQ Monitoring agent . . . . .	166

**Appendix A. Accessibility . . . . . 171**

Magnifying what is displayed on the screen . . . . .	171
Navigating the interface using the keyboard . . . . .	171

**Appendix B. Data collection mode . . . . . 173**

Sampled and on-demand tables . . . . .	173
--	-----

**Appendix C. Monitoring events on non-supported systems . . . . . 177**

**Appendix D. Monitoring remote queue managers . . . . . 179**

Remote monitoring . . . . .	179
Setting up the environment for remote queue manager monitoring . . . . .	180
Monitoring multiple queue managers . . . . .	182
Limitations of remote queue manager monitoring . . . . .	183

**Appendix E. Disk space requirements for historical data tables . . . . . 185**

Historical data tables . . . . .	185
Historical table record sizes . . . . .	187
Historical space requirement worksheets . . . . .	188
Historical disk space summary worksheet . . . . .	195

**Appendix F. Check the existence of WebSphere MQ Client. . . . . 197**

Checking the existence of WebSphere MQ Client on Windows systems . . . . .	197
Checking the existence of WebSphere MQ Client on AIX systems. . . . .	197
Checking the existence of WebSphere MQ Client on Linux systems . . . . .	197

**Appendix G. Object configuration . . . 199**

**Appendix H. Granting WebSphere MQ OAM authorities to a user ID. . . . . 201**

**Appendix I. Library for the WebSphere MQ Monitoring agent . . . . . 203**

**Notices . . . . . 205**

Privacy policy considerations . . . . .	206
Trademarks . . . . .	207

**Glossary . . . . . 209**

A . . . . .	209
B . . . . .	209
C . . . . .	210
D . . . . .	210
E . . . . .	210
F . . . . .	211
H . . . . .	211
I . . . . .	211
L . . . . .	211
M . . . . .	211
O . . . . .	212
P . . . . .	212
Q . . . . .	212
R . . . . .	212
S . . . . .	212
T . . . . .	213
U . . . . .	214
V . . . . .	214
W . . . . .	214

**Index . . . . . 215**



---

## Figures

1. An alert flagged in a Navigator view . . . . .	3	19. Browse mode for connections to a queue	140
2. An example of an alert in the WebSphere MQ Monitoring agent workspace . . . . .	3	20. Workspace Link Wizard - Welcome . . . . .	141
3. Navigator item for an event workspace . . . . .	5	21. Workspace Link Wizard - Link to Modify	141
4. Event workspace . . . . .	5	22. Workspace Link Wizard - Parameters	142
5. Agent-Server-Client architecture. . . . .	6	23. Workspace Link Wizard - Parameters	142
6. Configuring a channel with IBM Tivoli OMEGAMON DE. . . . .	8	24. Workspace Link Wizard - Summary . . . . .	143
7. WebSphere MQ Monitoring Agent selection	15	25. Access QSG workspaces from the Queue-Sharing Group item . . . . .	147
8. WebSphere MQ Monitoring Agent reconfiguration . . . . .	16	26. A two-computer MSCS cluster . . . . .	152
9. An opened notepad session after the mq_instance.cfg file update . . . . .	16	27. An example cluster environment architecture with one cluster group active on each cluster node . . . . .	153
10. A Take Action command used in a situation	62	28. Setting local variables. . . . .	156
11. The subscription topology view. . . . .	97	29. An example cluster environment architecture with a cluster group active on one cluster node and inactive on the other node. . . . .	158
12. The search window with advanced options displayed . . . . .	100	30. Setting local variables. . . . .	160
13. Specifying conditions in the advanced options of the search window.. . . . .	100	31. An example active-active cluster environment architecture with one cluster group active on each cluster node . . . . .	164
14. Preventing destination queues from overflowing . . . . .	102	32. An example active-passive cluster environment architecture. . . . .	165
15. Resolving publishing failure . . . . .	103	33. Remote monitoring communications architecture . . . . .	179
16. Compact mode for application connections	138		
17. Drill-down mode for an application connection . . . . .	139		
18. Drill-down mode for all application connections . . . . .	140		



## Tables

1. IBM Tivoli OMEGAMON DE workspaces and actions . . . . .	8	31. Channel Status (QMCHAN_ST) worksheet	190
2. Parameters for The configure TEMA(CFGOMAMQ) Dialog . . . . .	13	32. Channel Summary (QMCHAN_SUM) worksheet. . . . .	190
3. A mapping table for attribute groups and historical workspaces . . . . .	85	33. Connection Objects (QMCONNOBJ) worksheet. . . . .	190
4. Message manipulation on a specified queue name. . . . .	90	34. Current Queue Manager Status (QMCURSTAT) worksheet . . . . .	190
5. Combination of MSGACCESS settings and WebSphere MQ settings . . . . .	92	35. Event Archive (QMEVENTL) worksheet	191
6. Comparison of different situations for monitoring queue depth . . . . .	98	36. Event Log (QMEVENTH) worksheet	191
7. Historical attribute groups for sample reports	110	37. Listener Status (QMLSTATUS) worksheet	191
8. Parameters of Channel Daily Availability report . . . . .	110	38. Log Data Set Status (QMDSPUSAGE) worksheet. . . . .	191
9. Parameters of Channel Weekly Availability report . . . . .	111	39. Log Manager Long-Term History (QMLHLM) worksheet. . . . .	191
10. Parameters of Queue Full Detail report	111	40. Message Manager Long-Term History (QMLHMM) worksheet . . . . .	191
11. Parameters of Queue Manager Daily Availability report . . . . .	112	41. Message Statistics (QMMMSG_STAT) worksheet	192
12. Parameters of Queue Manager Weekly Availability report . . . . .	112	42. MQ Action Log (QMACTLOG) worksheet	192
13. Parameters of Top N Queue Full report	113	43. MQ Channel Statistics (QMCH_STAT) worksheet. . . . .	192
14. Icons used in the Application Topology view	137	44. MQ Queue Statistics (QMQ_STAT) worksheet	192
15. Overriding local variables . . . . .	155	45. MQI Call Statistics Details (QMMQICDET) worksheet. . . . .	192
16. Overriding local variables . . . . .	159	46. MQI Message Statistics Details (QMMQIMDET) worksheet . . . . .	193
17. Sampled and on-demand tables . . . . .	173	47. MQI Statistics (QMMQISTAT) worksheet	193
18. Comparison between monitoring a queue manager locally and remotely . . . . .	179	48. Page Set Long-Term History (QMPS_LH) worksheet. . . . .	193
19. Historical data tables . . . . .	185	49. QSG Channels (QSG_CHANS) worksheet	193
20. Historical table record sizes . . . . .	187	50. QSG Coupling Facility Structure Backups (QSG_CFBKUP) worksheet . . . . .	193
21. Application Accounting (QMMQIACCT) worksheet. . . . .	188	51. QSG Coupling Facility Structure Connections (QSG_CFCONN) worksheet. . . . .	193
22. Application Connections (QMCONNAPP) worksheet. . . . .	188	52. QSG Coupling Facility Structures (QSG_CFSTR) worksheet. . . . .	194
23. Application Long-Term History (QM_APAL) worksheet. . . . .	189	53. QSG QMgrs (QSG_QMGR) worksheet	194
24. Application Queue Long-Term History (QM_APQL) worksheet . . . . .	189	54. QSG Queues (QSG_QUEUEES) worksheet	194
25. Application Transaction/Program Long-Term History (QM_APTL) worksheet . . . . .	189	55. Queue Accounting (QMQ_ACCT) worksheet	194
26. Buffer Manager Long-Term History (QMLHBM) worksheet . . . . .	189	56. Queue Data (QMQ_DATA) worksheet	194
27. Channel Data (QMCH_DATA) worksheet	189	57. Queue Definitions (QMQUEUE) worksheet	194
28. Channel Definitions (QMCHANNEL) worksheet. . . . .	189	58. Queue Handle Status (QMQ_HDL_ST) worksheet. . . . .	194
29. Channel Initiator Detail (QMCHANIN) worksheet. . . . .	190	59. Queue Long-Term History (QMQ_LH) worksheet. . . . .	195
30. Channel Long-Term History (QMCH_LH) worksheet. . . . .	190	60. Queue Status (QMQ_QU_ST) worksheet	195
		61. Topic Manager Long-Term History (QMLHTM) worksheet . . . . .	195
		62. Historical disk space summary worksheet	195
		63. Objects configuration from different workspaces in WebSphere MQ. . . . .	199



---

## Chapter 1. Introducing WebSphere MQ Monitoring agent

With WebSphere® MQ Monitoring agent, you can easily collect and analyze data that is specific to WebSphere MQ for all your remote and local queue managers from a single vantage point. You can then track trends in the data that is collected and troubleshoot system problems using the product provided workspaces.

The information provided by WebSphere MQ Monitoring agent can be used to do the following tasks:

- Monitor the performance of each system that is managed by WebSphere MQ, solve problems by identifying bottlenecks, and fine-tune the system for better performance.
- Select the most effective threshold values for monitored attributes and trigger a warning situation when the attributes exceed the value.
- View status information related to a particular resource when a change in its state is detected.

---

### New in this release

Version 7.3 of WebSphere MQ Monitoring agent has the following enhancements:

- Miscellaneous improvements:
  - Support of IBM® MQ V8.0 is provided (also known as WebSphere MQ).
  - Support of IBM Integration Bus V9 is provided (also known as WebSphere Message Broker).
  - The User ID attribute is added to WebSphere MQ event data to improve the usability of situations.
  - More attributes are added for WebSphere MQ objects, such as queue managers, queues, and channels.
- Enhancements that apply to the distributed systems only:
  - 64-bit native support and support for queue manager start date and time is provided on Windows systems.
  - Error Log format is updated with the WebSphere MQ installation information.
  - Basic channel summary data is provided for telemetry channels.

---

### Supported versions of WebSphere MQ

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

- On distributed systems:
  - WebSphere MQ 7.0
  - WebSphere MQ 7.0.1
  - WebSphere MQ 7.1
  - WebSphere MQ 7.5
  - IBM MQ 8.0
- On z/OS® systems:
  - WebSphere MQ 7.0
  - WebSphere MQ 7.0.1

- WebSphere MQ 7.1
- IBM MQ 8.0

**Remember:** WebSphere MQ server and client components must exist on the same system where the WebSphere MQ Monitoring agent is installed and running.

---

## WebSphere MQ Monitoring agent overview

With WebSphere MQ Monitoring agent, you can expect the following benefits:

- *Increase knowledge* with extensive reporting capabilities that provide real-time access to reliable, up-to-the-minute data. Thus, you can make faster, better-informed operating decisions.
- *Enhance system performance* by integrating, monitoring, and managing your system, environment, console, and critical applications. For example, WebSphere MQ Monitoring agent can alert you when conditions in your environment meet or exceed the thresholds that you set. These alerts notify your system administrator to limit and control system traffic.
- *Simplify application and system management* by managing applications, systems, and resources across your system.

### User interface

WebSphere MQ Monitoring agent uses the Tivoli® Enterprise Portal interface. By providing a consolidated view of your environment, you can monitor and resolve performance problems throughout your enterprise by using Tivoli Enterprise Portal. The characteristics of this user interface include the following items:

- *A Navigator view* of your enterprise. When a condition that you are monitoring exceeds the thresholds that you define, an alert, which is a round red mark with white cross in the center, is displayed in the physical Navigator view to notify you.

In this example, Queue Manager Status for the QM\_AUTO\_3 queue manager is flagged with an alert.

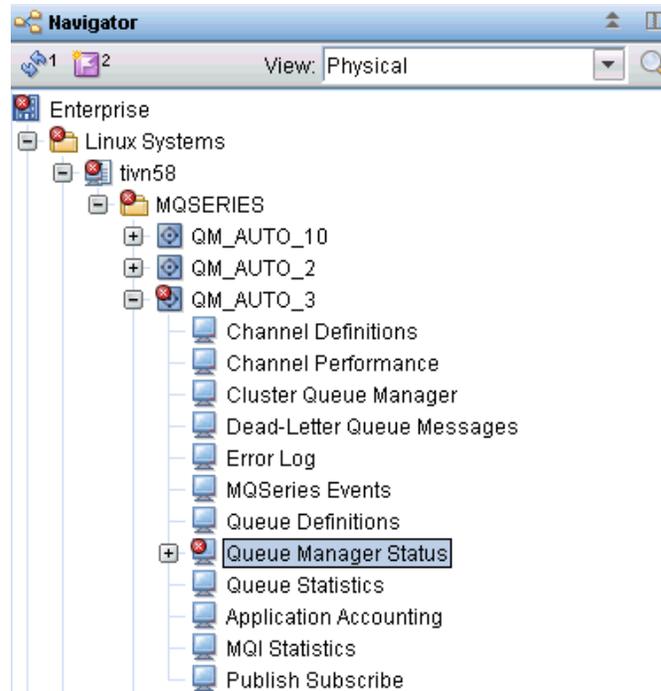


Figure 1. An alert flagged in a Navigator view

- *Workspaces* that contain various types of information. When a condition that you are monitoring exceeds the thresholds that you define, an alert is displayed in the WebSphere MQ Monitoring agent workspace to notify you. The following figure is an example of such an alert displayed in the table view of a workspace.

Queue Manager Status							
	QMgr Name	Host Name	QMgr Subsys	Host Jobname	Start Date & Time	QMgr Status	QMgr Type
	QM_AUTO_3	tivn58			n/a	QueueManager Not Available	Linux

Figure 2. An example of an alert in the WebSphere MQ Monitoring agent workspace

For more information about predefined workspaces included with WebSphere MQ Monitoring agent, see Chapter 10, “Monitoring with workspaces,” on page 115, and the online help of WebSphere MQ Monitoring agent.

- *Attributes* that you can use to create situations that monitor areas of particular interest and issue alerts when specified conditions are met.
- *Predefined situations* that you can use immediately to begin monitoring or that you can use as templates to create specific situations.

For more information about predefined situations included with WebSphere MQ Monitoring agent and how to create custom situations, see Chapter 3, “Using situations and Take Action commands,” on page 59

## Attributes

WebSphere MQ Monitoring agent gathers data about the managed systems of your network and stores the data as system elements called attributes. You can use these attributes to do the following things:

- Build situations to monitor the performance of the managed systems that you are concerned with

- Create queries and use the resulting data to build custom views

Related attributes are grouped into attribute groups or attribute tables.

You can use attributes to create situations that monitor the state of your system, database, or application. A situation describes a condition that you want to test. When you start a situation, Tivoli Enterprise Portal compares the values that you assign for the attributes of the situation with the values that are collected by WebSphere MQ Monitoring agent and registers an *event* if the condition is met. You are alerted to events by indicator icons that are displayed in the Navigator physical view.

Chart and table views use queries to specify which attribute values to request from the monitoring agents. You can use the Query editor to create a new query, modify an existing one, or apply filters and set styles to define the content and appearance of a view based on an existing query.

For complete descriptions of the attributes that are provided with WebSphere MQ Monitoring agent, see Tivoli Enterprise Portal online help.

## Event indicator and event workspace

When the conditions of a situation are met, the situation evaluates true, which causes an event indicator to be displayed in the Navigator view. You can investigate the cause of an event in its event workspace by clicking the workspace link icon next to the situation name.

Two table views are displayed in the event workspace, one with the values of the attributes when the situation evaluates true, and the other with the current values of the attributes.

A view with any expert advice that is written by the author of the situation is also available in the event workspace. The advice is displayed as web text and any links that you define are active. The Take Action view is also displayed in the event workspace, so you can send a command to the application that is started on that system.

Figure 3 on page 5 is an example Navigator with raised event indicators: red indicators for critical conditions and yellow indicators for warnings. If both a warning and a critical condition occur for the same workspace, the indicator always displays the highest level alert.

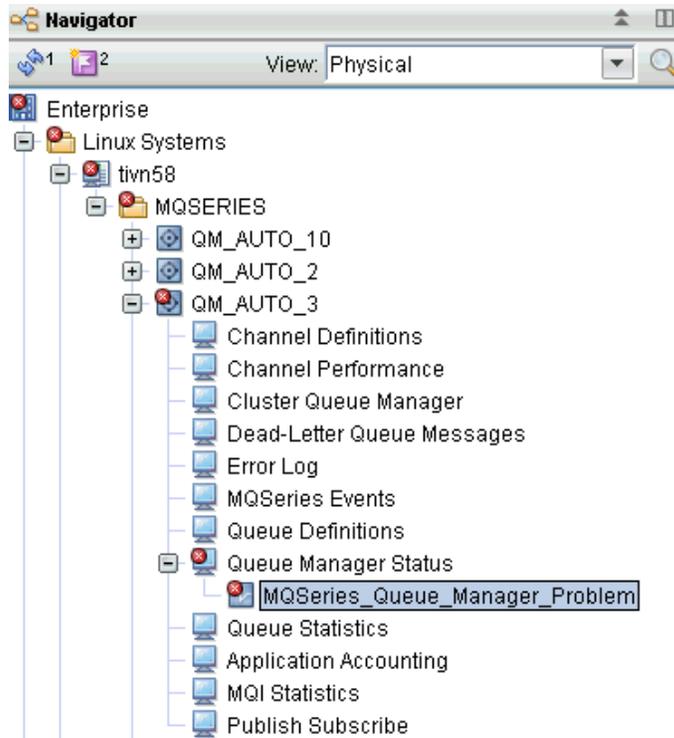


Figure 3. Navigator item for an event workspace

When you see an alert icon overlaying a Navigator icon, open the event workspace and drill down to investigate the cause of the alert. Figure 4 is an example event workspace for WebSphere MQ Monitoring agent.

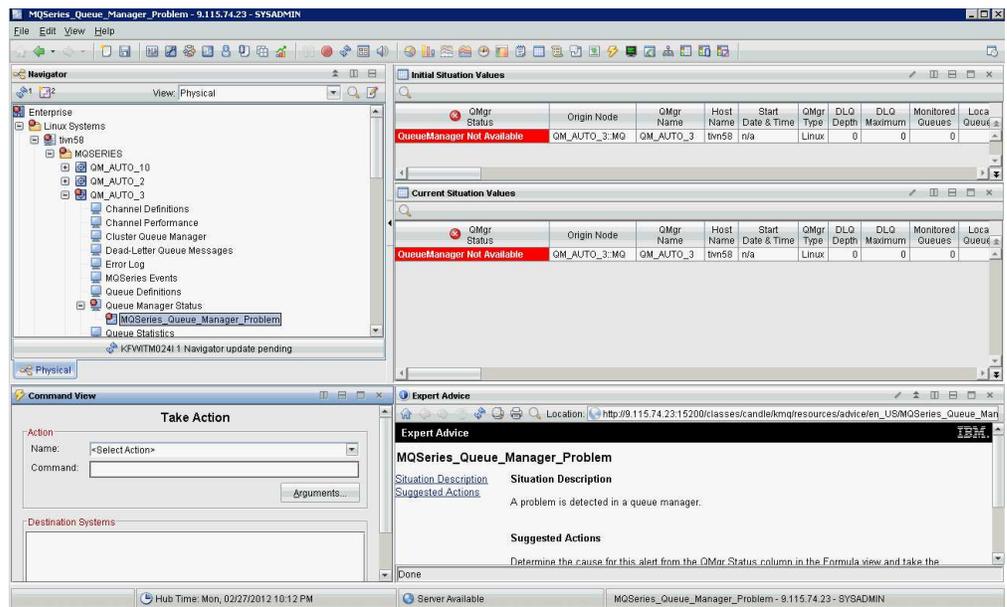


Figure 4. Event workspace

By looking at this workspace, you can determine the situation that raised the event and the attributes whose values are contributing to the alert. You can also review available advice and take appropriate actions.

## Acknowledgments

When you see an event indicator in the Navigator, you can create an acknowledgment by right-clicking the navigator item with the event indicator and clicking **Acknowledge Event**. An acknowledgment notifies other users that you have taken ownership of the problem that is related to the event and are working on it. When you acknowledge an event, a blue check mark is displayed next to the situation in the event flyover list. If you opened the event workspace, a blue check mark is also displayed over the situation item in the Navigator. If the situation is still true when the acknowledgment expires, the indicator changes accordingly. You can also cancel the acknowledgment before it expires. This changes the indicator, so that users can see that the acknowledgment is removed, although the situation remains true.

---

## IBM Tivoli Monitoring

IBM Tivoli Monitoring manages system and network applications on a variety of operating systems and keeps track of the availability and performance of all parts of your enterprise. It provides IBM Tivoli OMEGAMON<sup>®</sup> XE products and IBM Tivoli Composite Application Manager products with a common agent-server-client architecture:

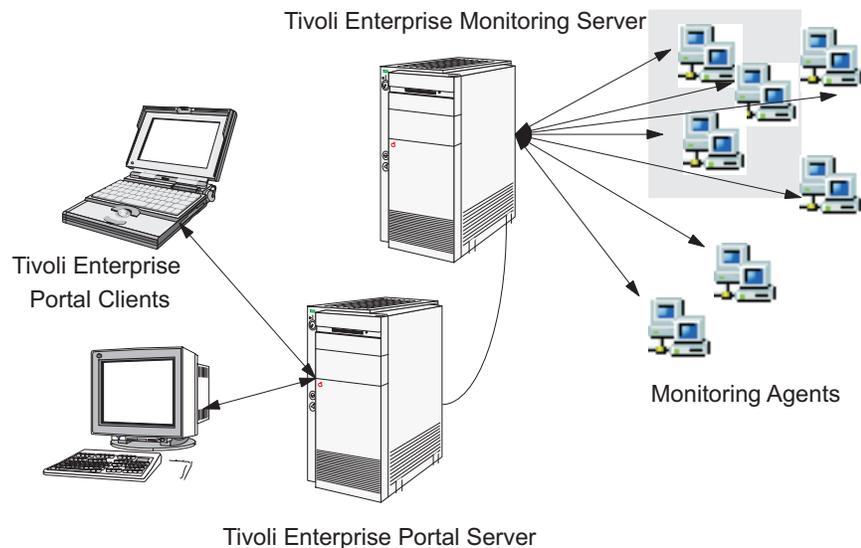


Figure 5. Agent-Server-Client architecture

### Client

The IBM Tivoli Monitoring client, Tivoli Enterprise Portal, is a Java<sup>™</sup> based user interface for viewing and monitoring your enterprise network. Depending on how it is installed, you can start Tivoli Enterprise Portal as a desktop application (desktop mode) or through your browser (browser mode).

### Server

The Tivoli Enterprise Portal client connects to the Tivoli Enterprise Portal Server. The Tivoli Enterprise Portal Server provides a range of software services for the client that enables retrieval, manipulation and analysis of data obtained by monitoring agents in the enterprise.

The Tivoli Enterprise Portal Server connects to the main, or *hub* Tivoli Enterprise Monitoring Server. The Tivoli Enterprise Monitoring Server acts as a collection and control point for alerts that are received from monitoring agents, and collects performance and availability data from them. The hub monitoring server correlates data that is collected by monitoring agents and remote monitoring server and passes it to the Tivoli Enterprise Portal Server for presentation in the Tivoli Enterprise Portal user interface and your evaluation.

## Agent

Monitoring agents are installed on systems whose resources or applications you want to monitor. The agent collects monitoring data from managed systems and passes the data to the Tivoli Enterprise Monitoring Server that it connects to. The Tivoli Enterprise Portal gathers the current values of the attributes and produces reports, which are displayed in tables and charts. It can also test values against thresholds and display an alert icon when the thresholds are exceeded or a value is matched. These tests are called *situations*.

## Agent Management Services

WebSphere MQ Monitoring agent that runs on a Windows, Linux, or UNIX computer can be managed by IBM Tivoli Monitoring 6.2.2's Agent Management Services. These services are available in the IBM Tivoli Monitoring OS Monitoring Agent for Windows, Linux, and UNIX, and are designed to keep WebSphere MQ Monitoring agent available and to provide information about its status to the Tivoli Enterprise Portal. More information about Agent Management Services can be found at this URL: [http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc\\_6.2.2/itm\\_agentmgmtsvcs\\_intro.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.2/itm_agentmgmtsvcs_intro.htm).

## IBM Tivoli OMEGAMON DE

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

Tivoli OMEGAMON DE extends the capabilities of Tivoli OMEGAMON XE to include the following items:

- Enterprise-specific Navigator views  
The Navigator physical view displays the hierarchy of your managed enterprise that is organized by systems and types of monitoring agents. The Navigator business view offered by Tivoli OMEGAMON DE displays the hierarchy of any managed objects. You can also define Navigator views for any logical grouping, such as a business process or a 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 display views from as many different agent types as are included on that branch of the Navigator.
- Linking application workspaces  
You can define a link from a workspace that is associated with one type of monitoring agent to a workspace that is associated with another type of agent.

## Details of operation

With Tivoli OMEGAMON DE, you can easily change the parameters of specific WebSphere MQ objects (queue managers, queues, channels, and other objects) by providing cross-product access to the Tivoli OMEGAMON DE version of WebSphere MQ Configuration agent.

Upgrading to the optional DE feature gives you a more integrated view of your WebSphere MQ environment. You can select the attributes of a WebSphere MQ resource that are displayed in the workspaces of WebSphere MQ Monitoring agent and you can easily modify these attributes to meet your needs. Your changes take effect immediately.

For example, you are using the Channel Performance workspace, and you notice a problem with a SYSTEM.DEF.SENDER channel. You can select the channel, right-click it, and then click **Configure Channel**.

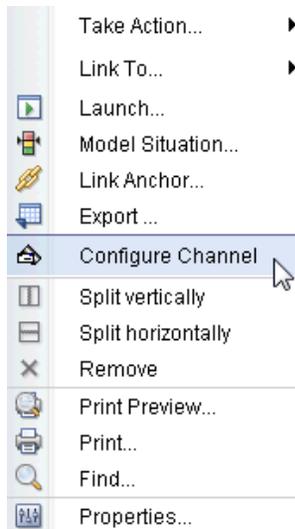


Figure 6. Configuring a channel with IBM Tivoli OMEGAMON DE

The setting list of WebSphere MQ Configuration agent for the channel opens. On the list you can change the parameters of the channel, save your changes, and update your actual WebSphere MQ configuration.

Any WebSphere MQ resource that you want to configure by using WebSphere MQ Configuration agent must already be completely defined in the configuration database of WebSphere MQ Configuration agent. If the resource is not defined, the following message is displayed:

KCF0045E The requested object does not exist in the configuration database.

Table 1 lists the workspaces in which these additional actions are available.

Table 1. IBM Tivoli OMEGAMON DE workspaces and actions

Workspace in IBM Tivoli OMEGAMON DE for WebSphere MQ Monitoring agent	Action that can be performed
Channel Definitions	Configure Channel
Channel Performance	Configure Channel

Table 1. IBM Tivoli OMEGAMON DE workspaces and actions (continued)

Workspace in IBM Tivoli OMEGAMON DE for WebSphere MQ Monitoring agent	Action that can be performed
Cluster Queue Manager	Configure Channel
Namelist Detail	Configure Namelist
Queue Definitions	Configure Queue
Queue Manager Status	Configure Queue Manager
Queue Statistics	Configure Queue

Your user ID must have the permission of modifying WebSphere MQ Configuration agent to use this feature.

## Policy management

The Tivoli Enterprise Portal Policy Management solution incorporates all the features of Tivoli OMEGAMON DE and adds automation capabilities by means of the Workflow editor. In the Workflow editor you can design sets of automated system processes, called policies, to resolve system problems. A policy performs actions, schedules work to be performed by users, or automates manual tasks.

## Where to find more information

For more information about IBM Tivoli Monitoring, see Tivoli Enterprise Portal online help and the books of IBM Tivoli Monitoring library.



---

## Chapter 2. Customizing monitoring options

You can create multiple instances of the WebSphere MQ Monitoring agent to monitor multiple queue managers on the same computer. You can also change the monitoring options of local and remote agents on supported operating systems to suit the needs of your environment.

---

### Creating multiple instances of the WebSphere MQ Monitoring agent

By default, the WebSphere MQ Monitoring agent monitors a single queue manager. You can create multiple instances of the agent to monitor multiple queue managers on the same computer.

#### Creating multiple instances on Windows systems

The first instance of the agent, which is created during installation, is called the primary agent. Any other agent instances that you create on the same computer are secondary agents.

**Remember:**

- You cannot use the following process to create multiple instances of WebSphere MQ Monitoring agent if the agent is deployed remotely instead of being installed locally.
- Names of WebSphere MQ Monitoring agent instances are not case-sensitive, but names of WebSphere MQ queue managers are case-sensitive. Therefore, avoid using WebSphere MQ queue manager names that are different only by case. For example, if you have a queue manager named `qm_apple`, do not name another queue manager `QM_APPLE`.

To create multiple instances of the WebSphere MQ Monitoring agent:

1. Click **Start > Programs > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services** to open the Manage Tivoli Enterprise Monitoring Services window.
2. Right-click **WebSphere MQ Monitoring Agent** and click **Create Multi-Instance**.

A window displays the queue managers that are not monitored by WebSphere MQ Monitoring agent. They are displayed in the **Available Instances** list. You can use **Instance Filter** to specify criteria for filtering queue managers in the **Available Instances** list. The filter can only be used to filter queue managers that begin with a specific string. The asterisk (\*) and question mark (?) wildcard characters are not supported by the filter.

3. Select the queue managers that you want to monitor from **Available Instances**, and click the add symbol (>>) to add them to **Selected Instances**. Click **OK**.

New agent instances are created and listed on the Manage Tivoli Enterprise Monitoring Services window. The agents are configured and ready to start.

Configuration files are created for each new agent instance. The configuration files are located in one of the following directories and their names are in the format of `mq_qmgr.cfg`, where `install_dir` is the installation directory of IBM Tivoli Monitoring and `qmgr` is the name of the monitored queue manager.

- 32-bit agent: `install_dir/TMAITM6`
- 64-bit agent: `install_dir/TMAITM6_x64`

## Creating multiple instances on UNIX and Linux systems

By default, the WebSphere MQ Monitoring agent that is created during installation monitors the default queue manager on your system. It is called the primary agent instance. You can create agent instances to monitor other queue managers on your system.

A WebSphere MQ Monitoring agent instance monitors a single queue manager.

**Restriction:** You cannot use the following process to create instances of the WebSphere MQ Monitoring agent if the agent is deployed remotely instead of installed locally.

Do the following steps to create instances of the WebSphere MQ Monitoring agent:

1. Run the following commands to open the Manage Tivoli Enterprise Monitoring Services window:

```
cd install_dir/bin
./itmcmd manage
```

where *install\_dir* is the installation directory of IBM Tivoli Monitoring. The default directory is /opt/IBM/ITM.

2. In the Manage Tivoli Enterprise Monitoring Services window, right-click **WebSphere MQ Monitoring Agent** and click **Create MultiInstance**. The Specify Queue Manager window is displayed.

The queue managers on this computer are displayed in the **Available Instances** list. You can use **Instance Filter** to specify criteria for filtering queue managers in the **Available Instances** list. The filter can only be used to filter queue managers that begin with a specific string. The asterisk (\*) and question mark (?) wildcard characters are not supported by the filter.

3. Select the queue manager that you want the new agent instance to monitor, click **Add**, and click **OK**.

Configuration files are created for each new agent instance. The configuration files are in the *install\_dir*/config directory and their file names have the following format:

```
hostname_mq_qmgrname.cfg
```

where *hostname* is the name of the host system and *qmgrname* is the name of the queue manager that is monitored by the agent instance.

## Creating multiple instances on i5/OS systems

If you want to create multiple instances of WebSphere MQ Monitoring agent, do the following steps. The first instance is automatically assigned suffix 00001, the second instance is automatically assigned suffix 00002, and so on.

1. From an i5/OS™ system command line, enter this command:

```
WRKOMAMQ
```

The Add OMEGAMON Agent for WebSphere MQ window is displayed.

(If this is not the first access, a different window is displayed; press F6 to display the Add OMEGAMON Agent for WebSphere MQ window.)

2. Enter the name and a text description of the Queue Manager that this agent monitors and press Enter.

The configure TEMA (CFGOMAMQ) dialog box is displayed.

3. Enter your preferred values for the displayed parameters using the guidelines in Table 2.

Table 2. Parameters for The configure TEMA(CFGOMAMQ) Dialog

Parameter	Description
TEMS SNA location	The SNA location of the Tivoli Enterprise Monitoring Server that this agent reports to. If you do not use SNA, enter *NONE. If the correct SNA location is already defined, enter *SAME to retrieve it. If you need to define a new SNA location (which can be the Control Point Name or the remote location name) enter the new location name (for example: S10B6322).
TEMS TCP/IP address	The TCP/IP address. If you do not use TCP/IP, enter *NONE. If the correct TCP/IP address is already defined, enter *SAME to retrieve it. If you need to define a different TCP/IP address, enter the new address (for example: 129.0.132.45).
TEMS IP.PIPE Address	If the WebSphere MQ Monitoring agent must connect to the Tivoli Enterprise Monitoring Server through a firewall, you must use IP.PIPE. Specify the IP.PIPE address. If you do not use IP.PIPE, enter *NONE.
Secondary TEMS SNA location	The SNA location of a secondary Tivoli Enterprise Monitoring Server that this agent reports to if it cannot communicate with the primary Tivoli Enterprise Monitoring Server at startup.
Secondary TEMS IP address	The TCP/IP address of the system where a secondary Tivoli Enterprise Monitoring Server is. The agent reports to this Tivoli Enterprise Monitoring Server if it cannot communicate with the primary Tivoli Enterprise Monitoring Server at startup.
Secondary TEMS IP.PIPE Address	The IP.PIPE address of the system where a secondary Tivoli Enterprise Monitoring Server is. The agent reports to this Tivoli Enterprise Monitoring Server if it cannot communicate with the primary Tivoli Enterprise Monitoring Server at startup.
Partition Name	This is required only by sites with firewalls that use address translation. The name of the partition that this instance of the WebSphere MQ Monitoring agent is in (up to 32 alphanumeric characters).
Firewall in use	If the WebSphere MQ Monitoring agent must connect to the Tivoli Enterprise Monitoring Server through a firewall, enter *YES. If not, retain the default of *NO.
TEMS TCP/IP port address	The listening port of the Tivoli Enterprise Monitoring Server that this agent reports to (usually 1918). If your site uses SNA or IP.PIPE, ignore this field. If the correct port address is already defined, enter *SAME to retrieve it. If you need to specify a different Tivoli Enterprise Monitoring Server port address, enter the new address (up to 6 numeric characters).
TEMS SNA port address	The listening port of the Tivoli Enterprise Monitoring Server that this agent reports to (usually 1918). If your site uses TCP/IP or IP.PIPE, ignore this field. If the correct port address is already defined, enter *SAME to retrieve it. If you need to specify a different Tivoli Enterprise Monitoring Server port address, enter the new address (up to 6 numeric characters).
TEMS IP.PIPE port address	The listening port of the Tivoli Enterprise Monitoring Server that this agent reports to (usually 1918). If your site uses TCP/IP or SNA, ignore this field. If you need to specify a different Tivoli Enterprise Monitoring Server port address, enter the new address (up to 6 numeric characters).

Table 2. Parameters for The configure TEMA(CFGOMAMQ) Dialog (continued)

Parameter	Description
Action user profile	The user authority under which user action must be administered. Retain the default value of QAUTOMON to grant user system operator authority.
SNA transaction program	This prompt is displayed only if you enter a value (or *SAME) for Tivoli Enterprise Monitoring Server SNA location. The name of the SNA transaction program. Retain the default value of KDTMSNAP.
Library	This prompt is displayed only if you enter a value (or *SAME) for SNA location. The name of the SNA transaction program library. Retain the default value of KMSCMS.
Transaction program (backup)	This prompt is displayed only if you enter a value (or *SAME) for Secondary Tivoli Enterprise Monitoring Server SNA location. The name of the SNA transaction program. Retain the default value of KDTMSNAP.
Library	This prompt is displayed only if you enter a value (or *SAME) for Secondary Tivoli Enterprise Monitoring Server SNA location. The name of the SNA transaction program library. Retain the default value of KMSCMS.

4. Read the Options choices and Function Key choices that are available for each window to determine which keys to press to save and exit the window.  
If you are reconfiguring the agent, the changes take effect the next time the agent is started.

---

## Changing monitoring options

Instructions about changing monitoring options for each supported system.

### Changing monitoring options on UNIX and Linux systems

On UNIX and Linux systems, you can change monitoring options by editing the `mq.cfg` monitoring file. The `mq.cfg` file is located in the `install_dir/config` directory, where `install_dir` is the IBM Tivoli Monitoring installation directory. The default directory is `/opt/IBM/ITM`. If your site has multiple queue managers, you might have created multiple instances of the monitoring agent, each with its own uniquely named monitoring file pointing to a single queue manager. The monitoring file for an instance of the WebSphere MQ Monitoring agent has the following naming convention: `Hostname_mq_queue_manager_name.cfg`. You can customize monitoring options in any or all of these monitoring files.

If you are unfamiliar with the various monitoring options, see the descriptions of the options in “Monitoring options” on page 26.

To change the monitoring options, do the following steps:

1. Edit the monitoring file as your site requires. The following guidelines apply:
  - Lines in the monitoring file cannot exceed 80 characters. If a command is longer than 80 characters, you must write it on two lines.
  - Before continuing a command on an additional line, append a hyphen (-) to the end of the current line.
  - A single parameter must be written on the same line.
  - A single parameter value must be written on the same line.

- Parameters that you set when you are grouping objects are effective for all the objects in the group.
  - You can override parameters for an object in a group by defining parameters for that object.
2. Verify that the queue manager and its command server are running.
  3. Restart each monitoring agent for your changes to take effect.

**Remember:** If you want to collect historical data for attribute groups whose data is sampled by the agent, you must set the **HISTORY** option to YES in the PERFORM STARTMON statement of the monitoring file. For information about using the historical data collection function, see Chapter 5, “Collecting historical data,” on page 79. For information about sampled and on-demand attribute groups, see “Sampled and on-demand tables” on page 173.

## Changing monitoring options on Windows systems

On Windows system, you can change monitoring options by editing the mq.cfg monitoring file. If your site has multiple queue managers, you might have created multiple instances of the monitoring agent, each with its own uniquely named monitoring file pointing to a single queue manager. You can customize monitoring options in any or all of these monitoring files.

If you are unfamiliar with the various monitoring options, review the descriptions of the options in “Monitoring options” on page 26.

Do the following steps to edit the monitoring file for an agent instance:

1. Click **Start > Programs > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.
2. In the Manage Tivoli Enterprise Monitoring window, select **WebSphere MQ Monitoring Agent -- instance**, where *instance* is the name of the agent instance for which you want to change monitoring options.

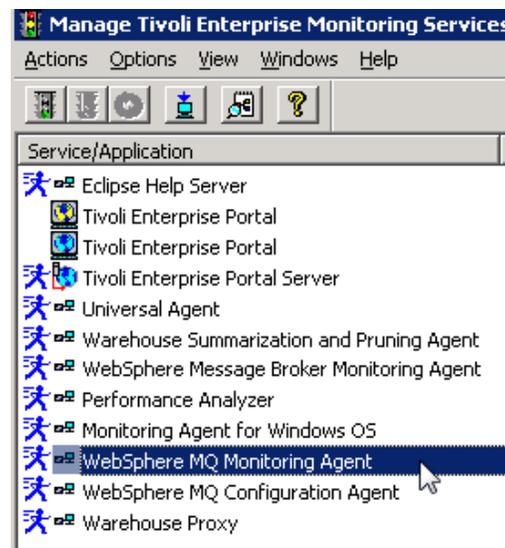


Figure 7. WebSphere MQ Monitoring Agent selection

3. Click **Actions > Reconfigure**.

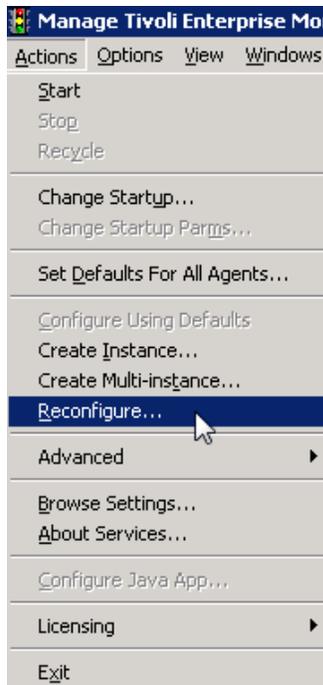


Figure 8. Websphere MQ Monitoring Agent reconfiguration

4. Verify settings or changes as needed, and click **OK**.
5. Click **Yes** when you are asked whether you want to update the `mq_instance.cfg` file.
6. Click **OK**.  
A Notepad session opens.

```

*****
*
* Licensed Materials - Property of IBM
*
* (C) Copyright IBM Corp. 1996, 2008 All Rights Reserved.
*
* US Government Users Restricted Rights - Use, duplication or
* disclosure restricted by GSA ADP Schedule Contract with
* IBM Corp.
*
*****

SET GROUP NAME (GROUP1) -
  DEFAULT(YES) -
  RETAINHIST(120) -
  COMMAND (YES) -
  MSGACCESS(DESC) -
  EVENTS(REMOVE) -
  ACCOUNTINGINFO(REMOVE) -
  STATISTICSINFO(REMOVE)
SET MANAGER NAME(QM1)
SET QUEUE NAME(*) MGRNAME(QM1) QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(QM1)
PERFORM STARTMON SAMPINT(300) HISTORY(YES)
  
```

Figure 9. An opened notepad session after the `mq_instance.cfg` file update

7. Add, delete, or modify monitoring options as required for your site. The following guidelines apply:
  - Lines in the monitoring file cannot exceed 80 characters. If a command is longer than 80 characters, you must write it on two lines.
  - Before continuing a command on an additional line, append a hyphen (-) to the end of the current line.
  - A single parameter must be written on the same line
  - A single parameter value must be written on the same line.
  - Parameters that you set when you are grouping objects are effective for all the objects in the group.
  - You can override parameters for an object in a group by defining parameters for that object.
8. Close the Notepad.
9. At the next prompt, click **Yes** to continue.
10. Verify that your queue manager and its command server are running.
11. Restart the agent for the changes to take effect.

**Remember:** If you want to collect historical data for attribute groups whose data is sampled by the agent, you must set the **HISTORY** option to YES on the “PERFORM STARTMON” on page 48 statement in the monitoring file. For information about using the historical data collection function, see Chapter 5, “Collecting historical data,” on page 79. For information about sampled and on-demand attribute groups, see “Sampled and on-demand tables” on page 173.

## Changing monitoring options on i5/OS systems

On i5/OS systems, you can use the agent management program to change monitoring options. (You can also use the agent management program to start, stop, delete, replicate, view status, display the log for, or change Tivoli Enterprise Monitoring Server configuration for one or more WebSphere MQ Monitoring agents on the same i5/OS system.)

If you are unfamiliar with the various monitoring options and the statements to enable them, review the descriptions of the options in “Monitoring options” on page 26.

To edit the monitoring file, do the following steps:

1. When you are ready to customize the monitoring file, enter the following command on an i5/OS command line:

```
WRKOMAMQ
```

The main panel for working with the WebSphere MQ Monitoring agent is displayed.

```
Work with monitoring agent for WebSphere MQ System MYSYSTEM
```

```
Type Option, press Enter
```

```
2=Change, 4=Delete, 5=Display agent Log, 14=Start, 15=End
```

Option	Agent for MQ Manager...	Suffix	Status
	MYSYSTEM	00001	Not Started
	MQITMISDE1	00002	Started

**Tip:** If you click the **Display agent Log** option and a message is not issued, enter the following command on the command line:

```
wrkmsg msgq(kmqlib/KMSOMLOG)
```

On the panel, one or more monitoring agents are listed. These agents on an i5/OS system (and the unique monitoring file associated with each agent) are differentiated by a unique 5-character numeric suffix. The first agent added is automatically assigned suffix 00001, the second agent added is automatically assigned suffix 00002, and so on.

2. Enter 2 in the Option column next to the agent whose monitoring file you want to change.

The panel for changing the WebSphere MQ Monitoring agent is displayed.

3. Press F8 to change the monitoring file associated with the agent.

An editing panel is displayed.

4. Insert, delete, or modify monitoring option commands, as your site requires. The following guidelines apply:

- Lines in the monitoring file cannot exceed 80 characters. If a command is longer than 80 characters, you must write it on two lines.
- Before continuing a command on an additional line, append a hyphen (-) to the end of the current line.
- A single parameter must be written on the same line.
- A single parameter value must be written on the same line.
- Parameters that you set when you are grouping objects are effective for all the objects in the group.
- You can override parameters for an object in a group by defining parameters for that object.

5. When you finish customizing the monitoring file, press F3 to save your changes and exit. Press F3 another two times to exit the interface.

6. Verify that the queue manager and its command server are running.

7. Restart the agent for your changes to take effect.

**Remember:** If you want to collect historical data for attribute groups whose data is sampled by the agent, you must set the **HISTORY** option to YES on the "PERFORM STARTMON" on page 48 statement in the monitoring file. (For information about using the historical data collection function, see Chapter 5, "Collecting historical data," on page 79. For information about sampled and on-demand attribute groups, see "Sampled and on-demand tables" on page 173).

---

## Monitoring a multi-instance queue manager

If you are using WebSphere MQ version 7.0.1 or later versions, you can create multi-instance queue managers to improve availability and use the WebSphere MQ Monitoring agent to monitor these multi-instance queue managers.

Multi-instance queue managers improve availability by automatically switching to a standby server if the active server fails. The active and standby servers are multiple instances of the same queue manager; they share the same queue manager data. When the active instance fails you need to transfer its journal to the standby that takes over so that the queue manager can rebuild its queues. You can create multi-instance queue managers on Windows, UNIX, or Linux systems. For more detailed information about multi-instance queue managers, see WebSphere MQ documentation.

To avoid confusion when multiple monitoring agents and queue managers exist in your environment, add the **SET AGENT** statement to the mq.cfg file. The **SET AGENT** statement specifies the middle qualifier of the managed system name, which can

distinguish the managed system names for queue managers. For detailed information about this statement, see “SET AGENT” on page 50.

## Windows system requirements

To use the WebSphere MQ Monitoring agent to monitor multi-instance queue managers on Windows systems, make sure that the following requirements are met in your environment:

- The **DataPath** parameter of the multi-instance queue manager is set to a UNC name, for example, \\host1\MQHA\data\QM1.

The **DataPath** parameter is in the following path in the registry, where *<qm\_name>* is the name of the multi-instance queue manager:

```
HKEY_LOCAL_MACHINE\SOFTWARE\IBM\MQSeries\CurrentVersion\Configuration\
QueueManager\<qm_name>
```

- The WebSphere MQ Monitoring agent is started by a user account that has access to the shared queue manager data.

You can specify the user account that is used to start the agent by doing the following steps:

1. Open the Manage Tivoli Enterprise Monitoring Services window.
2. Right-click the WebSphere MQ Monitoring agent instance, and click **Change Startup**.
3. In the Service Startup for WebSphere MQ Monitoring Agent window, select **This Account** in the **Log on As** section.
4. Type the user ID and password of the account that you want to use to start the agent.
5. Click **OK** to close the window.

## UNIX or Linux system requirements

To use the WebSphere MQ Monitoring agent to monitor multi-instance queue managers on UNIX or Linux systems, check the location of the `mqs.ini` file. If the `mqs.ini` file is not located in the default location, set the **AMQ\_MQS\_INI\_LOCATION** parameter in the `mq.ini` file 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 `mq.ini` file is located in the `ITM_HOME/config` directory, where `ITM_HOME` is the directory where IBM Tivoli Monitoring is installed.

## WebSphere MQ installation path requirements

If any of the following cases applies to your environment, you must specify the WebSphere MQ installation path by adding the **KMQ\_LATEST\_WMQ\_INSTALLPATH** parameter to the `kmqenv` file on a Windows system or to the `mq.ini` file on a UNIX or Linux system:

- More than one copy of WebSphere MQ is installed on the system and the latest version of WebSphere MQ on the system is not a primary installation.
- Only one copy of WebSphere MQ is installed and it is not installed in the default directory.

For more information about how to set this parameter, see the configuration section about specifying multiple installation paths of WebSphere MQ in the *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide*.

---

## Configuring remote agents

On distributed systems, the configuration file is encoded using UTF-8 and can contain non-English characters. On these operating systems you can use the remote agent configuration function instead of editing this file directly. You can configure a remote agent through the Tivoli Enterprise Portal or from the command line.

**Restriction:** This function is not available on i5/OS and z/OS systems.

Before you can remotely configure the WebSphere MQ Monitoring agent, identify the operating system where you want to remotely configure the agents and ensure that the following requirements are fulfilled in your monitoring environment:

- An OS agent is installed or deployed on the computer where the WebSphere MQ Monitoring agent that you want to remotely configure is installed. For example, if you want to configure the WebSphere MQ Monitoring agent on the computer where the Windows operating system is running, you must have the monitoring agent for Windows OS installed on that computer. For information about how to install the OS agent, see *IBM Tivoli Monitoring: Installation and Setup Guide*.
- The agent depot is populated on the Tivoli Enterprise Monitoring Server from which you configure agents across your environment. For example, if you want to remotely configure the WebSphere MQ Monitoring agent, you must have the agent depot for the WebSphere MQ Monitoring agent populated on the Tivoli Enterprise Monitoring Server. For detailed information about how to populate the agent depot, see "Population your agent depot" in Chapter 12, *Deploying monitoring across your environment from a central location in the IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide*.

## Configuring remote agents through Tivoli Enterprise Portal

Before you configure a remote WebSphere MQ Monitoring agent, ensure that an OS agent is installed or deployed on the computer where the remote WebSphere MQ Monitoring agent you want to configure is installed, and the agent depot is populated on the Tivoli Enterprise Monitoring Server from which you configure agents across your environment. See "Configuring remote agents" for detailed information about these prerequisites.

Do the following steps to configure the WebSphere MQ Monitoring agent remotely through the Tivoli Enterprise Portal:

1. Log on to the Tivoli Enterprise Portal.
2. Navigate to the system where the agent that you want to configure is installed.
3. Select the agent.
4. Right-click the agent, and then click **Configuration**.
5. Modify the parameters as needed.
6. Click **OK** to save the changes.
7. In the displayed window, click **View Status Workspace** to view the configuration status, or click **OK** to close the window.

All the parameters available for remote configuration are described in "Parameters for remote configuration through Tivoli Enterprise Portal" on page 21.

## Configuring remote agents from the command line

Before you configure a remote WebSphere MQ Monitoring agent, ensure that an OS agent is installed or deployed on the computer where the remote WebSphere

MQ Monitoring agent you want to configure is installed, and the agent depot is populated on the Tivoli Enterprise Monitoring Server from which you configure agents across your environment. See “Configuring remote agents” on page 20 for detailed information about these prerequisites.

Do the following steps to configure the WebSphere MQ Monitoring agent remotely from the command line:

1. Run the following command to log on to the Tivoli Enterprise Monitoring Server:

```
tacmd login -s TEMS_name -u user_ID -p password
```

where *TEMS\_name* is the host name of the monitoring server that you want to log in, *user\_ID* is the user ID, and *password* is the corresponding password.

2. Run the following command to configure the remote agent:

```
tacmd configureSystem -m system  
                    -p SECTION.NAME=VALUE
```

where *system* is the name of the managed system, *SECTION.NAME* is the monitoring option that you want to modify, and *VALUE* is the new value for the monitoring option.

For detailed descriptions about the configuration parameters, see “Monitoring options” on page 26.

For further information about the **tacmd CLI** commands, including parameter descriptions, see *IBM Tivoli Monitoring: Installation and Setup Guide* and *IBM Tivoli Monitoring: Command Reference*.

The following example changes the level of user access to messages in queues for the specified queue manager to DATA:

```
tacmd configureSystem -m QM_App::MQ -p MANAGER.MSGACCESS=DATA
```

**Tip:** Use the **tacmd listSystems** command to list the existing managed systems. The following command lists all the systems in your enterprise with the product code *MQ* (WebSphere MQ Monitoring agent).

```
tacmd listSystems -t MQ
```

## Parameters for remote configuration through Tivoli Enterprise Portal

All the parameters for remote agent configuration are attributes of one of these tags: General Agent Settings, Queue Manager Groups, Queue Access, Queues, Channels, Event Log, Event Queue In, Event Queue Out, Include File, Start Monitoring, Agent name, and Agent.

### General Agent Settings

- **Queue Manager Name:** The name of the queue manager.
- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Is Active:** Indicates whether to actively monitor this queue manager. Valid values are Yes and No. The default value is YES.
- **Is Remote:** Indicates whether the queue manager is running on a separate system from the agent. Valid values are Yes and No. The default value is NO.
- **Number of Samples in History:** Number of samples to maintain in recent history for this queue manager.

- **Command:** Controls the MQ Command feature. Valid values are Yes and No. The default value is YES.
- **Sampling Interval:** The interval of the error log collection cycle in seconds. The default value is 10.
- **Maximum Number of Message:** Specifies the maximum number of error messages that are held in memory and displayed in the Error Log workspace. The default value is 100.
- **Access to event queues:** Specifies how to access system event queues. Valid values are Remove, Browse, and No. The default value is NO.
- **High Level Qualifier:** Specifies the high-level qualifier for product-created queue names. The default value is KMQ.
- **Interval Cycle:** Specifies the number of sample interval cycles to wait before the queue manager performance data is gathered. The default value is 1.
- **Like Manager Name:** The name or the nickname of a previously defined manager.
- **Accounting Queue Access:** Specifies how to access the accounting messages from the system accounting queues. Read and remove messages, or browse without removing messages. Valid values are Remove and Browse. The default value is REMOVE.
- **Retain Recent Accounting Samples:** The number of recent records to keep for application or queue accounting data.
- **Statistics Queue Access:** Specifies how to access the statistics messages from the system statistics queues. Read and remove messages, or browse without removing messages. Valid values are Remove and Browse. The default value is REMOVE.
- **Retain Recent Statistics Samples:** The number of recent records to keep for MQI, queue, or channel statistics data.
- **Take Action Authorized Users:** The authorized Tivoli Enterprise Portal users to launch take action commands. There can be multiple entries that are associated with this parameter, each entry is separated by a comma, and each entry can be a mask, which can include the asterisk (\*) and the question mark (?).
- **Take Action Specified User:** The specified user that is used to launch take action commands: UIUSER (The user that is used to login Tivoli Enterprise Portal), MQAGENT (The user that is used to launch MQ Agent), or USER=user-id.
- **Message Access Level:** Controls the level of user access to messages in queues for the specified queue managers. Valid values are None, Desc, Retry, Data, Delete, and Use Queue Access. The default value is DESC.
- **Nickname:** The nickname (alternate name) for this queue manager. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **History Data Display Time:** The number of minutes that historical data is displayed for queue manager objects. The default value is 1440.
- **Model Queue of Reply-to Queue:** The name of a model queue to use as a model for the reply-to queue of this product.
- **Status:** Specifies what to do if this **SET MANAGER** command was previously specified with the same name. Valid values are Add, Delete, and Reset.
- **SMF System ID:** The SMF system ID where this queue manager runs.

## Queue Manager Group

- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Is Default Group:** Specifies whether this is the default group. Valid values are Yes and No.

- **Number of Sample in History:** The number of samples to maintain in recent history for all queue managers in this group. The default value is 15.
- **Command:** Controls the MQ Command feature. Valid values are Yes and No. The default value is YES.
- **Sampling Interval:** The interval of the error log collection cycle in seconds. The default value is 10.
- **Maximum Number of Message:** Specifies the maximum number of error messages that are held in memory and displayed in the Error Log workspace. The default value is 100.
- **Access to event queues:** Specifies how to access system event queues. Valid values are Remove, Browse, and No. The default value is NO.
- **High Level Qualifier:** Specifies the high-level qualifier for product-created queue names. The default value is KMQ.
- **Interval Cycle:** Specifies the number of sample interval cycles to wait before queue manager performance data is gathered. The default value is 1.
- **Like Group Name:** The name of a previously defined manager group.
- **Accounting Queues Access:** Specifies how to access the accounting messages from the system accounting queues. Read and remove messages, or browse without removing messages. Valid values are Remove and Browse. The default value is REMOVE.
- **Retain Recent Accounting Samples:** The number of recent records to keep for application or queue accounting data.
- **Statistics Queue Access:** Specifies how to access the statistics messages from the system statistics queues. Read and remove messages, or browse without removing messages. Valid values are Remove and Browse. The default value is REMOVE.
- **Retain Recent Statistics Samples:** The number of recent records to keep for MQI, queue, or channel statistics data.
- **Take Action Authorized Users:** The authorized Tivoli Enterprise Portal users to launch take action commands. There can be multiple entries that are associated with this parameter, each entry is separated by a comma, and each entry can be a mask, which can include the asterisk (\*) and the question mark (?).
- **Take Action Specified User:** The specified user that is used to launch take action commands: UIUSER (The user that is used to login Tivoli Enterprise Portal), MQAGENT (The user that is used to launch MQ Agent) or USER=user-id.
- **Message Access Level:** The level of user access to messages in queues. Valid values are None, Desc, Retry, Data, Delete, and Use Queue Access. The default value is DESC.
- **History Data Display Time:** The number of minutes that historical data is displayed for queue manager objects. The default value is 1440.
- **Model Queue of Reply-to Queue:** The name of a model queue to use as a model for the reply-to queue of this product.

## Queue Access

- **Name:** Name for this Queue Access option group. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Queue Name:** Defines the specific or generic queue name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Message Manipulation Authorized Users:** The authorized Tivoli Enterprise Portal users to manipulate messages. There can be multiple entries that are associated

with this parameter, each entry is separated by a comma, and each entry can be a mask which can include the asterisk (\*) and the question mark (?).

- **Message Manipulation Specified User:** The specified user that is used to manipulate messages: UIUSER (The user that is used to login Tivoli Enterprise Portal), MQAGENT (The user that is used to launch MQ Agent) or USER=user-id.
- **Message Access Level:** The level of user access to messages in queues. Valid values are None, Desc, Retry, Data, and Delete. The default value is DESC.
- **Queue Manager Name:** The queue manager name.
- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Status:** Specifies what to do if this **SET QUEUE** command was previously specified with the same name. Valid values are Add and Delete.

## Queues

- **Queue Name:** Defines the specific or generic queue name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Queue Manager Name:** The queue manager name.
- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Types Of Queues:** Indicates which kinds of queues to monitor. Valid values are Predefined, Permanent Dynamic, Temporary Dynamic, and All. The default value is All.
- **Collect QueueStatistics:** Specifies whether to collect queue statistics using WebSphere MQ Reset Queue Statistics command processing. Valid values are Yes and No. The default value is NO.
- **Status:** Specifies what to do if this **SET QUEUE** command was previously specified with the same name. Valid values are Add and Delete.

## Channels

- **Channel Name:** Defines the specific or generic channel name to monitor. The valid format is an alphanumeric string of up to 20 case-sensitive characters.
- **Queue Manager Name:** The queue manager name.
- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Status:** Specifies what to do if this **SET CHANNEL** command was previously specified with the same name. Valid values are Add and Delete.

## Event Log

- **File Size:** The maximum event log file size. The default value is 10.
- **Directory:** The directory to write the event log file to. The default value is @logpath@.
- **Archive File Name:** The archive directory and file name. The default value is @logpath@\Qmeventh.arc.
- **Kra Rolloff Options:** The krarloff (kra rolloff) command.

## Event Queues In

- **Queue Manager Name:** The queue manager name.
- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Queue Manager Event Queue:** Specifies the name of the queue manager event queue to monitor. The default value is SYSTEM.ADMIN.QMGR.EVENTS.

- **Channel Event Queue:** Specifies the name of the channel event queue to monitor. The default value is `SYSTEM.ADMIN.CHANNEL.EVENTS`.
- **Performance Event Queue:** Specifies the name of the performance event queue to monitor. The default value is `SYSTEM.ADMIN.PERFM.EVENTS`.
- **Logger Event Queue:** Specifies the name of the logger event queue to monitor. The default value is `SYSTEM.ADMIN.LOGGER.EVENT`.

## Event Queues Out

- **Queue Manager Name:** The queue manager name.
- **Group Name:** The group name. The valid format is an alphanumeric string of up to 48 case-sensitive characters.
- **Queue Manager Event Queue:** Specifies the name of the local queue where queue manager events are copied after being processed.
- **Channel Event Queue:** Specifies the name of the local queue where channel events are copied after being processed.
- **Performance Event Queue:** Specifies the name of the local queue where performance events are copied after being processed.
- **Logger Event Queue:** Specifies the name of the local queue where logger events are copied after being processed.

## Include File

- **File Name:** The name of the file containing the list of customization commands of the WebSphere MQ Monitoring agent.

## Start Monitoring

- **Sample Interval:** Specifies how often, in seconds, WebSphere MQ Monitoring agent samples your queue manager(s) for performance data. The default value is 60.
- **Collect Historical Data:** Defines whether historical data is collected. Valid values are Yes and No. The default value is NO.
- **Only Active Queue Managers:** This optional parameter indicates whether to monitor only active queue managers. Valid values are Yes and No. The default value is NO.
- **Row Limit:** This optional parameter specifies the maximum number of messages that are processed and returned by the agent when reading messages from a queue for report requests. The default value is 0.
- **Server Connection:** This optional parameter indicates whether to collect server connection channel statistics that are displayed in the Channel Performance workspaces. Valid values are Yes and No. The default value is YES.
- **Queue Sharing Group Check Interval:** This optional parameter specifies how often, in seconds, the WebSphere MQ Monitoring agent performs queue-sharing group monitoring activities. The default value is 300.
- **XCF Group Name:** You can use this optional parameter to specify an alternative SysPlex XCF group name. The default value is `KMQQSG`.

## Agent Name

- **Agent Name:** The name to be used for the middle qualifier of the managed system name. It can only be provided when you create a new agent instance, you must modify the remote agent configuration file manually if you want to change it.

## Agent

- **Run as:** The user account that is used to run the WebSphere MQ Monitoring agent. You can use the system account or set a new account for the agent.
- **Version:** The version number of the WebSphere MQ Monitoring agent that the managed system is using.

---

## Monitoring options

WebSphere MQ Monitoring agent provides monitoring options that you can modify to suit the needs of your environment. The monitoring options are defined in a command file, which is referred to as the monitoring file. When the WebSphere MQ Monitoring agent is started, the parameter values in the monitoring file are read and the commands in it are issued. The actual file name and location varies by operating system. After reading the following descriptions of monitoring options, see “Monitoring options” for information about how to change monitoring options on different operating systems and the rules for correctly specifying and changing monitoring options.

For example, you can configure the following settings by editing the monitoring file:

- Define the queue managers, queues, and channels that you want to monitor
- Specify the interval for collecting WebSphere MQ data
- Manage the disposal of event messages from an event queue
- Specify whether you want to collect historical monitoring data and how long you want the data to be available

By default, the WebSphere MQ Monitoring agent monitors the following objects:

- On a z/OS system:
  - all predefined queues
  - all channels for all queue managers
- On a UNIX, Linux, Windows, or i5/OS system:
  - all predefined queues
  - all channels on a single default queue manager

## SET GROUP

The **SET GROUP** statement defines a group of queue managers that have common monitoring characteristics. It defines the default monitoring options for all queue managers that are in the group. You can use the **SET MANAGER** statement to override some of those parameters for a given queue manager in the group.

At least one **SET GROUP** statement is required.

### Syntax

```
SET GROUP NAME(group-name)
                [DEFAULT(YES|NO)]
                [AGGRHIST(aggregation-samples)]
                [COMMAND(YES|NO)]
                [ERRLOGCYCLE(sampling-interval)] (distributed systems only)
                [ERRLOGMAX(max-messages-in-memory)] (distributed systems only)
                [EVENTS(REMOVE|BROWSE|NO)]
                [HLQ(high-level-qualifier)]
                [ICYCLE(interval-cycle)] (z/OS systems only)
                [LIKE(like-group-name)]
                [ACCOUNTINGINFO(REMOVE|BROWSE)] (distributed systems only)
```

```
[RECENTACCOUNTINGSAMPLES(recent-sample-count)]
  (distributed systems only)
[STATISTICSINFO(REMOVE|BROWSE)] (distributed systems only)
[RECENTSTATISTICSSAMPLES(recent-sample-count)]
  (distributed systems only)
[ACTIONAUTHUSERS (user-name-mask-list)]
[ACTIONACCOUNT (UIUSER|MQAGENT|USER=user-id)]
[MSGACCESS(NONE|DESC|RETRY|DATA|DELETE|USEQACCESS)]
[RETAINHIST(historical-retention-value)]
[RQMODEL(reply-to-queue's-model-queue)]
```

## Parameters

### NAME(*group-name*)

A 1- through 48-character group name. Subsequent commands refer to the group and its parameter settings by this name. This parameter is required.

### DEFAULT(YES|NO)

Specifies whether this is the default group. If this parameter is set to yes, the settings in this statement apply to any **SET MANAGER** statement that omits the **GROUP** parameter. The default group is named DEFAULT.

### AGGRHIST(*aggregation-samples*)

Specifies the number of samples to maintain in recent history for all queue managers in this group. The default value is 15.

### COMMAND(YES|NO)

Controls the MQ Command feature. For more details, see the description of the **COMMAND** parameter in “SET MANAGER” on page 29.

### ERRLOGCYCLE(*sampling-interval*)

Specifies, in seconds, the interval of the error log collection cycle. For more details, see the description of the **ERRLOGCYCLE** parameter in “SET MANAGER” on page 29.

### ERRLOGMAX(*max-messages-in-memory*)

Specifies the maximum number of error messages that are held in memory and displayed in the Error Log workspace. For more details, see the description of the **ERRLOGMAX** parameter in “SET MANAGER” on page 29.

### EVENTS(REMOVE|BROWSE|NO)

Specifies how to access system event queues. For more details, see the description of the **EVENTS** parameter in “SET MANAGER” on page 29.

### HLQ(*high-level-qualifier*)

Specifies the high-level qualifier for queue names. The default value is KMQ. For more details, see the description of the **HLQ** parameter in “SET MANAGER” on page 29.

### ICYCLE(*interval-cycle*)

This parameter applies only to z/OS systems.

Specifies the number of sample interval cycles to wait before queue manager performance data is gathered. For more details, see the description of the **ICYCLE** parameter in “SET MANAGER” on page 29.

### LIKE(*like-group-name*)

The name of a previously defined queue manager group. Parameter values that have similar names are copied from the values in the named group definition.

### ACCOUNTINGINFO(REMOVE|BROWSE|NO)

This parameter is not valid for z/OS systems.

Specifies how WebSphere MQ Monitoring agent accesses the accounting application and queue data that is produced by the queue manager. For more details, see the description of the **ACCOUNTINGINFO** parameter in "SET MANAGER" on page 29.

**RECENTACCOUNTINGSAMPLES**(*recent-sample-count*)

This parameter is not valid for z/OS systems.

Specifies the number of recent records that WebSphere MQ Monitoring agent keeps in memory for the application or queue accounting data. For more details, see the description of the **RECENTACCOUNTINGSAMPLES** parameter in "SET MANAGER" on page 29.

**STATISTICSINFO**(REMOVE | BROWSE | NO)

This parameter is not valid for z/OS systems.

Specifies how WebSphere MQ Monitoring agent accesses the statistics data that is produced by the queue manager. For more details, see the description of the **STATISTICSINFO** parameter in "SET MANAGER" on page 29.

**RECENTSTATISTICSSAMPLES**(*recent-sample-count*)

This parameter is not valid for z/OS systems.

Specifies the number of recent records that the WebSphere MQ Monitoring agent keeps in memory for queue managers, queues or channel statistics data. For more details, see the description of the **RECENTSTATISTICSSAMPLES** parameter in "SET MANAGER" on page 29.

**ACTIONAUTHUSERS**(*user-name-mask-list*)

This parameter is only applicable to the manual Take Action command.

Specifies that the Tivoli Enterprise Portal user ID must match one of the user name mask lists, before the Take Action command can be issued. For more details, see the description of the **ACTIONAUTHUSERS** parameter in "SET MANAGER" on page 29.

**ACTIONACCOUNT**(UIUSER | MQAGENT | USER=*user-id*)

This parameter is only applicable to the Take Action commands that are provided with WebSphere MQ Monitoring agent.

Specifies that WebSphere MQ Monitoring agent uses the **ACTIONACCOUNT** value as an alternate user ID to interact with WebSphere MQ for message manipulation. For more details, see the description of the **ACTIONACCOUNT** parameter in "SET MANAGER" on page 29.

**UIUSER:** The agent uses the Tivoli Enterprise Portal user ID to interact with WebSphere MQ.

**MQAGENT:** The agent uses the monitoring agent account to interact with WebSphere MQ.

**USER=*user-id*:** The agent uses the predefined account ("*user-id*") to interact with WebSphere MQ.

**MSGACCESS**(NONE | DESC | RETRY | DATA | DELETE | USEQACCESS)

Specifies the level of user access to messages in queues. For more details, see the description of the **MSGACCESS** parameter in "SET MANAGER" on page 29.

**RETAINHIST**(*historical-retention-value*)

Number of minutes that queue manager objects (such as channels and queues) that are no longer defined in the queue manager are retained in

agent memory and returned for display in workspaces, so that it is easier to link to historical data about the object. You can decrease the **RETAINHIST** value if you want less data to be maintained in memory for these objects that are no longer defined. The default value is 120 (2 hours). This parameter is only valid for channels and local queues.

#### **RQMODEL**(*reply-to-queue's-model-queue*)

Specifies the 1- through 48-character name of a model queue to use as a model for the reply-to queue for this product. If this parameter is not specified, the standard system default model is used. For more details, see the description of the **RQMODEL** parameter in "SET MANAGER."

### **Example**

To define a manager group named MYGROUP with new values for aggregation and historical retention, specify the following statement:

```
SET GROUP NAME(MYGROUP) LIKE(DEFAULT) -
AGGRHIST(20) RETAINHIST(2400)
```

## **SET MANAGER**

The **SET MANAGER** statement specifies the queue managers that you want to monitor.

### **Syntax**

```
SET MANAGER NAME(manager-name-mask)
    [GROUP(group-name)]
    [ACTIVE(YES|NO)]
    [AGGRHIST(aggregation-samples)]
    [COMMAND(YES|NO)]
    [ERRLOGCYCLE(sampling-interval)] (distributed systems only)
    [ERRLOGMAX(max-messages-in-memory)] (distributed systems only)
    [EVENTS(REMOVE|BROWSE|NO)]
    [HLQ(high-level-qualifier)]
    [ICYCLE(interval-cycle)] (z/OS systems only)
    [LIKE(like-manager-name)]
    [ACCOUNTINGINFO(NO|REMOVE|BROWSE)] (distributed systems only)
    [RECENTACCOUNTINGSAMPLES(recent-sample-count)] (distributed systems only)
    [STATISTICSINFO(NO|REMOVE|BROWSE)] (distributed systems only)
    [RECENTSTATISTICSSAMPLES(recent-sample-count)] (distributed systems only)
    [ACTIONAUTHUSERS (user-name-mask-list)]
    [ACTIONACCOUNT (UIUSER|MQAGENT|USER=user-id)]
    [MSGACCESS(NONE|DESC|RETRY|DATA|DELETE|USEQACCESS)]
    [NICKNAME(nickname)]
    [RETAINHIST(historical-retention-value)]
    [RQMODEL(reply-to-queue's-model-queue)]
    [STATUS(ADD|DELETE|RESET)] (z/OS systems only)
    [SYSNAME(z/OS-system-id)]
    [REMOTE(YES|NO)]
```

### **Parameters**

#### **NAME**(*manager-name-mask*)

On z/OS systems, this parameter value is the 1- through 4-character specific or generic name of the queue managers that you want to monitor. To specify a generic name, enter a character string followed by an asterisk (\*). For example, to monitor all z/OS system queue managers, specify NAME(\*). This parameter is required on z/OS systems.

On distributed systems, specify the full name of the queue manager that you want to monitor without any asterisks. If you do not specify this parameter, the default queue manager is monitored.

**GROUP**(*group-name*)

A previously defined group that has parameter defaults that apply to this queue manager. The name must exactly match the name that is specified on a prior **SET GROUP** statement. The default group that is provided is named DEFAULT.

**ACTIVE**(YES | NO)

Indicates whether to actively monitor this queue manager. YES is the default.

**AGGRHIST**(*aggregation-samples*)

Specifies the number of samples to maintain in storage for monitored objects that are associated with the queue manager. This number of samples is displayed for the object in recent workspaces.

**COMMAND**(YES | NO)

Specifies if passing WebSphere MQ commands to the queue manager from Tivoli Enterprise Portal is available. Valid values are:

YES: Enables the MQ Command feature. You can then pass WebSphere MQ commands to the queue manager from Tivoli Enterprise Portal. YES is the default value.

NO: Disables the MQ Command feature.

**ERRLOGCYCLE**(*sampling-interval*)

Specifies, in seconds, the interval of the error log collection cycle. The default value is 10.

Specifying the value 0 turns off error log collection for the queue manager and disables the Error Log monitoring feature.

See “Error Log monitoring (distributed systems only)” on page 125 for more information about the Error Log monitoring feature.

**ERRLOGMAX**(*max-messages-in-memory*)

Specifies the maximum number of error messages that are held in memory and displayed in the Error Log workspace. The default value is 100.

**EVENTS**(REMOVE | BROWSE | NO)

Specifies how to access system event queues. Valid values are:

REMOVE: Read and remove messages from the system event queues. This setting provides the most accurate event reporting. The value that is configured automatically during the installation and configuration process is REMOVE. When REMOVE is specified, the agent opens the event queues for exclusive access.

To provide support for multiple applications to read event queues, use the **SET EVENTQIN** and **SET EVENTQOUT** commands as described in “SET EVENTQIN” on page 43 and “SET EVENTQOUT” on page 46.

BROWSE: Browse (read without removing) messages in the system event queues. Specify this value if more than one application (WebSphere MQ Monitoring agent or another application) reads the event queues. In this case, you must run a separate application to clean the queues, such as CSQUTIL with the EMPTY function.

**Remember:** If you specify EVENTS(BROWSE) and other applications perform destructive reads against the event queues, WebSphere MQ Monitoring agent might miss some or all event messages.

NO: Do not monitor system event queues.

### **HLQ**(*high-level-qualifier*)

Specifies the high-level qualifier for queue names that are created by WebSphere MQ Monitoring agent. The default value is KMQ.

If you predefine queues with the following names, WebSphere MQ Monitoring agent uses these names:

On z/OS systems:

*hlq*.COMMAND.REPLY  
*hlq*.REPLY

On other operating systems:

*hlq*.IRA.AGENT.QUEUE

where *hlq* is the value that is specified by the **HLQ** parameter of the **SET MANAGER** or the **SET GROUP** command.

If you do not predefine queues with these names, WebSphere MQ Monitoring agent creates dynamic queues using the model queue that is specified by the **RQMODEL** parameter on the **SET MANAGER** or the **SET GROUP** command. In this case, the names of the dynamic queues are as follows.

On z/OS systems:

*hlq*.COMMAND.REPLY.*dynamicsuffix*  
*hlq*.REPLY.*dynamicsuffix*

On other operating systems:

*hlq*.IRA.AGENT.QUEUE.*dynamicsuffix*

where *hlq* is the value that is specified using the **HLQ** parameter of the **SET MANAGER** or the **SET GROUP** command, and *dynamicsuffix* is the standard dynamic suffix that is provided by WebSphere MQ.

### **ICYCLE**(*interval-cycle*)

This parameter applies only to z/OS systems.

This optional parameter specifies the number of sample interval cycles to wait before gathering performance data for the specified queue managers. The default value is 1 minute. You can use this parameter to lengthen the sampling interval for a specific queue manager or a group of queue managers whose data collection is less critical and can be performed less frequently. For example, if the sample interval (**SAMPINT**) for a queue manager is set to 60 and its interval cycle (**ICYCLE**) is set to 5, interrogative processing for that queue manager is performed on only every fifth cycle; every five minutes instead of every minute.

If you do not specify the **ICYCLE** parameter, or if it is not specified on a prior **SET GROUP** statement, the default value is 1; queue manager data is gathered once every sample interval (**SAMPINT**).

### **LIKE**(*queue-manager-name*)

The name or the nickname of a previously defined queue manager. Parameter values that are not specified in this **SET MANAGER** statement are copied from the corresponding values for the named queue manager.

### **ACCOUNTINGINFO**(**NO** | **REMOVE** | **BROWSE**)

This parameter is not valid on z/OS systems.

Specifies how WebSphere MQ Monitoring agent accesses the accounting application and queue data that is produced by the queue manager. Valid values are as follows:

NO: The agent does not monitor accounting application and queue data.

REMOVE : The agent reads and removes messages from the system accounting queues. This setting provides the most accurate event reporting. The value that is configured automatically during the installation and configuration process is REMOVE. When REMOVE is specified, the agent opens the system accounting queues for exclusive access.

BROWSE: The agent browses (reads without removing) messages in the system accounting queues. Specify this value if more than one application (WebSphere MQ Monitoring agent or another application) reads the accounting queues. If this is the case, you must run a separate application to clean the queues.

#### **RECENTACCOUNTINGSAMPLES**(*recent-sample-count*)

This parameter is not valid for z/OS systems.

Specifies the number of recent records that WebSphere MQ Monitoring agent keeps in memory for the application or queue accounting data. If this parameter is not specified, 5 is the default value.

#### **STATISTICSINFO**(NO | REMOVE | BROWSE)

This parameter is not valid on z/OS systems.

Specifies how WebSphere MQ Monitoring agent accesses the statistics data that is produced by the queue manager (queue manager, queue and channel). Valid values are as follows:

NO: The agent does not monitor statistics data (queue manager, queue and channel).

REMOVE: The agent reads and removes messages from the system statistics queues. This setting provides the most accurate event reporting. The value that is configured during the installation and configuration process is REMOVE. When REMOVE is specified, the agent opens the system statistics queues for exclusive access.

BROWSE: The agent browses (reads without removing) messages in the system statistics queues. Specify this value if more than one application (WebSphere MQ Monitoring agent or another application) read the statistics queues. If this is the case, you must run a separate application to clean the queues.

#### **RECENTSTATISTICSSAMPLES**(*recent-sample-count*)

This parameter is not valid on z/OS systems.

Specifies the number of recent records that WebSphere MQ Monitoring agent keeps in memory for queue managers, queues, or channel statistics data. If this parameter is not specified, 5 is the default value. The following workspaces are affected by this parameter:

- Recent MQI Statistics
- Recent MQ Queue Statistics
- Recent MQ Channel Statistics

#### **ACTIONAUTHUSERS**(*user-name-mask-list*)

This parameter is only applicable to the manual Take Action command.

Specifies that the Tivoli Enterprise Portal user ID must match one of the user name mask lists before the Take Action command can be issued.

If the **ACTIONAUTHUSERS** parameter value is specified as empty [()], it indicates that **ACTIONAUTHUSERS** is not defined in the parameters list. This **ACTIONAUTHUSERS** parameter is ignored.

If the **ACTIONAUTHUSERS** parameter value is set to a user name mask list, it specifies which Tivoli Enterprise Portal users are authorized to issue the Take Action commands that are associated with this WebSphere MQ Monitoring agent. There can be multiple entries that are associated with this parameter. Separate each entry with a comma (.). An entry can be a mask that includes the asterisk (\*) and question mark (?) wildcard characters. A Tivoli Enterprise Portal user that has an ID that matches any masks in this list is authorized to issue the Take Action commands. Tivoli Enterprise Portal user IDs are defined within the Tivoli Enterprise Monitoring Server and do not necessarily exist on the node on which the WebSphere MQ Monitoring agent is running.

#### **ACTIONACCOUNT(UIUSER|MQAGENT|USER=user-id)**

This parameter is only applicable to the Take Action commands that are provided with WebSphere MQ Monitoring agent.

Specifies that WebSphere MQ Monitoring agent uses the **ACTIONACCOUNT** value as an alternate user ID when interacting with WebSphere MQ. The **ACTIONACCOUNT** parameter specifies whether the authorization should use the Tivoli Enterprise Portal user ID, the monitoring agent account, or the predefined account. Valid values are as follows:

( ): Overrides the value defined on the **SET GROUP** or **SET MANAGER** command.

UIUSER: The agent uses the Tivoli Enterprise Portal user ID to interact with WebSphere MQ.

MQAGENT: The agent uses the monitoring agent account to interact with WebSphere MQ.

USER=user-id: The agent uses the predefined account ('user-id') to interact with WebSphere MQ.

If a value other than these values is specified, the value is not valid; the **ACTIONACCOUNT** parameter is regarded as not being defined on the command.

For the reflex automation, only the ID that is specified in **ACTIONACCOUNT(USER=user\_id)** is used to issue the WebSphere MQ command; otherwise, the MQ agent user ID is used to issue the WebSphere MQ command.

#### **MSGACCESS(NONE|DESC|RETRY|DATA|DELETE|USEQACCESS)**

Controls the level of user access to messages in queues for the specified queue managers.

NONE: No access to message functions is permitted for the specified queue managers, including the ability to list messages on a queue or collect message statistics.

DESC: Message descriptor browse is permitted for message summary workspaces, message detail workspaces, or message statistics workspaces and situations. This is the default level.

RETRY: DLQ retry and message descriptor browse are permitted.

DATA: Message data (contents) browse, message descriptor browse, and DLQ retry are permitted.

DELETE: Deletion of messages and all other message functions are permitted.

USEQACCESS: Specifies that all the queues that belongs to the current group or queue manager *must* be defined by a new **SET QACCESS** command to grant message access rights. The queues that belong to the current group and that are not defined by a **SET QACCESS** command have the message access level NONE.

**NICKNAME**(*nickname*)

A 1- through 48-character nickname (alternate name) for this queue manager. Subsequent commands can refer to the manager by its manager name or by this nickname. This parameter is optional.

**RETAINHIST**(*historical-retention-value*)

Number of minutes that queue manager objects (such as channels and queues) that are no longer defined in the queue manager are retained in agent memory and returned for display in workspaces, so that it is easier to link to historical data about the objects. You can decrease the **RETAINHIST** value if you want less data to be maintained in memory for these objects that are no longer defined. This parameter is only valid for channels and local queues.

**RQMODEL**(*reply-to-queue's-model-queue*)

Specifies the 1- through 48-character name of a model queue to use as a model for the reply-to queue of WebSphere MQ Monitoring agent, if you did not predefine queues. If you require dynamic queues, see the description of the **HLQ** parameter.

If you do not specify a value for the **RQMODEL** parameter, the following standard system default models are used as a model for the reply-to-queue of WebSphere MQ Monitoring agent.

On z/OS systems:

SYSTEM.COMMAND.REPLY.MODEL

On other operating systems:

SYSTEM.DEFAULT.MODEL.QUEUE

If the queue that you specify as a model has a definition type of permanent dynamic [DEFTYPE(PERMDYN)], some unused reply-to-queues might accumulate. These have the names in the following forms:

On z/OS systems:

*hlq*.COMMAND.REPLY.*dynamicsuffix*  
*hlq*.REPLY.*dynamicsuffix*

On other operating systems:

*hlq*.IRA.AGENT.QUEUE.*dynamicsuffix*

where the *hlq* value is the value that is specified on the **HLQ** parameter on the **SET MANAGER** or the **SET GROUP** command, and the *dynamicsuffix* value is the standard dynamic suffix that is provided by WebSphere MQ.

**STATUS**(ADD | DELETE | RESET)

Specifies what to do if this **SET MANAGER** command was previously specified with the same name.

This parameter applies only to z/OS systems.

If this parameter is omitted, the manager definition is added if it is a new name; it is modified if the same name was specified previously.

ADD: Creates a new manager definition.

DELETE: Deletes the manager definition and all associated historical data.

RESET: Resets the monitoring parameters that are associated with this queue manager to their original values (as defined on the original **SET MANAGER** command for this manager name).

#### **SYSNAME(z/OS-system-id)**

This parameter applies only to z/OS systems.

The SMF system ID where this queue manager runs. If this parameter is omitted, this **SET MANAGER** command applies to any z/OS systems.

#### **REMOTE(YES|NO)**

Specifies whether the queue manager is a remote queue manager or a local one.

If this parameter is omitted, the queue manager is a local queue manager.

YES: The queue manager is a remote queue manager.

NO: The queue manager is a local queue manager.

### **Example**

- To monitor all z/OS system queue managers that have names that begin with MQM, specify the following statement  
SET MANAGER NAME(MQM\*)
- To monitor the queue manager named PAYROLL, specify the following statement  
SET MANAGER NAME(PAYROLL)
- To set the number of recent samples to 30 and the retention interval for historical displays to 10 hours for the MGRA queue manager, specify the following statement:  
SET MANAGER NAME(MGRA) AGGRHIST(30) RETAINHIST(600)
- To sample the error log every 20 seconds and display up to 200 error log events for the queue manager named QMGRA, specify the following statement:  
SET MANAGER NAME(QMGRA) ERRLOGCYCLE(20) ERRLOGMAX(200)
- To specify three queue managers with nicknames, specify the following statements:  
SET MANAGER NAME(MGRD) NICKNAME(DALLAS) EVENTS(REMOVE)  
SET MANAGER NAME(MGRA) NICKNAME(ATLANTA) EVENTS(NO)  
SET MANAGER NAME(MGRS) NICKNAME(SANFRAN) EVENTS(BROWSE)

Because the **GROUP**, **AGGRHIST**, and **RETAINHIST** parameters are omitted, the values that are specified on the **SET GROUP** command for the default group are in effect for those parameters. Each manager defines a different access to the system event queues.

- To specify an effective sample interval of 1 minute for the z/OS system queue manager named QM01 and 5 minutes for the z/OS system queue manager named QM02, specify the following statements:

```
SET MANAGER NAME(QM01)  
SET MANAGER NAME(QM02) ICYCLE(5)  
PERFORM STARTMON SAMPINT(60)
```

## SET QACCESS

Use the **SET QACCESS** statement to specify a set of queues that have group level or manager level message access rights specified. Follow the guidelines that are described in “Changing monitoring options” on page 14 when changing this monitoring option.

### Syntax

```
SET QACCESS NAME(queue-name-mask)
                MSGAUTHUSERS(user-name-mask-list)
                MSGACCOUNT(UIUSER|MQAGENT|USER=user-id)
                MSGACCESS(NONE|DESC|RETRY|DATA|DELETE)
                MGRNAME(mgr-name)|GROUP(group-name)
                [STATUS(ADD|DELETE)]
                [DEFAULT(YES|NO)]
```

### Parameters

#### NAME(*queue-name-mask*)

Specifies a 1- through 48-character specific or generic queue name that is used to specify access authorization. To specify a generic name, enter a characters string followed by an asterisk (\*). This parameter is required.

If the queue-name-mask is empty (set to ()), this **SET QACCESS** statement is ignored, and the next statement is processed. A warning message is displayed on the console (this error message is not recorded in the IBM Tivoli Monitoring log files).

#### MSGAUTHUSERS(*user-name-mask-list*)

Defines the Tivoli Enterprise Portal clients that are authorized to manipulate messages according to the associated **MSGACCESS** parameter. There can be multiple entries associated with this parameter. Separate each entry with a comma (.). An entry can be a mask, which includes the asterisk (\*) and question mark (?) wildcard characters. A Tivoli Enterprise Portal user that has an ID that matches any masks in this list is authorized to issue the **MSGACCESS** command (Description, Retry, Data, and Delete) that is handled by the WebSphere MQ Monitoring agent. Tivoli Enterprise Portal user IDs are defined within the Tivoli Enterprise Monitoring Server, and do not necessarily exist on the node on which the agent is running.

There is no default value for this parameter.

If the user name mask list is empty (set to ()), this **SET QACCESS** statement is ignored and the next statement is processed. A warning message is logged.

#### MSGACCOUNT(UIUSER|MQAGENT|USER=*user-id*)

Defines the user ID that WebSphere MQ Monitoring agent uses to interact with WebSphere MQ. When there is a requirement for message manipulation, and a predefined account or the monitoring agent account is authorized to interact with WebSphere MQ, the user ID defined by the **MSGACCOUNT** parameter is used.

If the value of the **MSGACCOUNT** parameter is not valid, this **SET QACCESS** statement is ignored and the next statement is processed. A warning message is logged.

#### MSGACCESS(NONE|DESC|RETRY|DATA|DELETE)

Controls the level of user access to messages for specified queues.

If the **MSGACCESS** value is not NONE, DESC, RETRY, DATA, or DELETE, this **SET QACCESS** statement is ignored and the next statement is processed. A warning message is issued.

- NONE: No access to message functions is permitted for these specified queues, including the ability to list messages on a queue or collect message statistics.
- DESC: Message descriptor browse is permitted for message summary workspaces, message detail workspaces, or message statistics workspaces and situations. This is the default level.
- RETRY: DLQ retry and message descriptor browse are permitted.
- DATA: Message data (contents) browse, message descriptor browse, and DLQ retry are permitted.
- DELETE: Deletion of messages and all other message functions are permitted.

#### **MGRNAME**(*manager-name*)

Associates this **SET QACCESS** statement with a queue manager that was defined on a previous **SET MANAGER** statement. You can use the name or the nickname of the manager. The name must exactly match the name that is specified on the corresponding **SET MANAGER** statement. This parameter is required if the **GROUP** parameter is not specified.

If the **MGRNAME** parameter is empty, the queue manager is the default queue manager.

#### **GROUP**(*group-name*)

Associates this **SET QACCESS** statement with a group of queues that were defined on a previous **SET GROUP** statement. The name must exactly match the name specified on the corresponding **SET GROUP** statement. This parameter is required if the **MGRNAME** name is not specified.

If both the **MGRNAME** and **GROUP** parameters are not defined, this **SET QACCESS** statement is ignored and the next statement is processed. A warning message is issued.

#### **STATUS**(**ADD** | **DELETE**)

Specifies what to do if this **SET QACCESS** statement was previously specified with the same queue name mask and user name mask list.

If this parameter is omitted, the queue access definition is added if a **SET QACCESS** statement was not previously specified with the same name for both the queue name mask and user name mask list, or it is modified if the same name was previously specified for both the queue name mask and user name mask list.

- ADD: Creates a new queue access definition. If this **SET QACCESS** statement was previously specified with the same name for both queue name mask and user name mask list, it is not modified and an error message is issued.
- DELETE: Deletes a queue access definition.

#### **DEFAULT**(**YES** | **NO**)

Allows the specification of default queue access behavior. This allows a more restrictive default access to be applied only if there are no other matching queue access statements. If the **DEFAULT** value is not specified, **DEFAULT(NO)** is used.

The queue access applied will be the non-default statement (**DEFAULT(NO)**) with the most restrictive access that matches queue and user name. If there are no non-default statements that match, the queue access applied will be the default statement (**DEFAULT(YES)**) with the most restrictive access that matches queue and user name.

## Example

- To set message manipulation for all queues to DATA, specify the following statements:

```
SET GROUP NAME (GROUP1) -  
    DEFAULT (YES) -  
    COMMAND (YES) -  
    MSGACCESS (USEQACCESS)  
SET QACCESS NAME(*) -  
    MSGAUTHUSERS (*) -  
    MSGACCOUNT (MQAGENT) -  
    MSGACCESS (DATA)  
    GROUP (GROUP1)
```

- To give the DELETE MSGACCESS privilege to all queues that have the **queue1** prefix and belong to the QM1 manager, to give the NONE MSGACCESS privilege to all other queues that belong to the QM1 manager, and to give the DATA MSGACCESS privilege to all queues that belong to the QM2 manager, specify the following statements:

```
SET GROUP NAME (GROUP1) DEFAULT (YES) COMMAND (YES) MSGACCESS (DATA)  
SET MANAGER NAME (QM1) MSGACCESS (USEQACCESS)  
SET MANAGER NAME (QM2)  
SET QACCESS NAME (queue1*) -  
    MSGAUTHUSERS (*) -  
    MSGACCOUNT (MQAGENT) -  
    MSGACCESS (DELETE) -  
    MGRNAME (QM1)  
SET QACCESS NAME (q1*) -  
    MSGAUTHUSERS (*) -  
    MSGACCOUNT (MQAGENT) -  
    MSGACCESS (DELETE) -  
    MGRNAME (QM2)
```

- To give the DESC privilege to all queues that have the **q1** prefix, and give the DATA privilege to all queues that have the **q2** prefix, specify the following statements:

```
SET GROUP NAME (GROUP1) DEFAULT (YES)  
SET MANAGER NAME (QM1) MSGACCESS (USEQACCESS)  
SET QACCESS NAME (q1*) -  
    MSGAUTHUSERS (A*, B?C) -  
    MSGACCOUNT (UIUSER) -  
    MSGACCESS (DESC) -  
    MGRNAME (QM1)  
SET QACCESS NAME (q2*) -  
    MSGAUTHUSERS (John) -  
    MSGACCOUNT (USER=mqoperator) -  
    MSGACCESS (DATA) -  
    MGRNAME (QM1)
```

- To give the DELETE MSGACCESS privilege to all queues that have the **queue1** prefix and belong to the QM1 manager, to give the DATA MSGACCESS privilege to all other queues that belong to the QM1 manager, specify the following statements:

```
SET GROUP NAME (GROUP1) DEFAULT (YES) COMMAND (YES) MSGACCESS (DATA)  
SET MANAGER NAME (QM1) MSGACCESS (USEQACCESS)  
SET QACCESS NAME (queue1*) -  
    MSGAUTHUSERS (*) -  
    MSGACCOUNT (MQAGENT) -  
    MSGACCESS (DELETE) -  
    DEFAULT (NO) -  
    MGRNAME (QM1)  
SET QACCESS NAME (*) -  
    MSGAUTHUSERS (*) -
```

MSGACCOUNT(MQAGENT) -  
MSGACCESS(DATA) -  
DEFAULT(YES) -  
MGRNAME(QM1)

## SET QUEUE

Use the **SET QUEUE** statement to specify the queues to be monitored.

**Agent behavior change:** Beginning with V7.0.1 Fix Pack 1, the WebSphere MQ Monitoring agent monitors only the dead-letter queue by default. To monitor other system or application queues, specify them with the **SET QUEUE** statement. For previous releases, the WebSphere MQ Monitoring agent monitors all the queues on the specified queue manager by default.

### Syntax

```
SET QUEUE NAME(queue-name-mask)  
MGRNAME(manager-name) | GROUP(group-name)  
[QDEFTYPE(PREDEFINED|PERMDYN|TEMPDYN|ALL)]  
[STATISTICS(YES|NO)]  
[STATUS(ADD|DELETE)]  
[QTYPE (ALL|QLOCAL|QALIAS|QCLUSTER|QREMOTE|QMODEL)]  
[DEFSAMPCYCLE(n-sample-interval)] (z/OS systems only)
```

### Parameters

#### NAME(*queue-name-mask*)

Specifies a 1- through 48-character specific or generic name of the queues that you want to monitor. To specify a generic name, enter a character string followed by an asterisk (\*). This parameter is required.

If you leave this parameter empty (set to ()), the WebSphere MQ Monitoring agent monitors only the dead-letter queue or all the queues on the queue manager, depending on the agent version. If the agent version is V7.0.1 Fix Pack 1 or later, the agent monitors only the dead-letter queue. When you are working with V7.0.1 Fix Pack 1 or later and you want to monitor all queues on the queue manager, set this parameter to \*.

#### MGRNAME(*manager-name*)

Associates this **SET QUEUE** statement with a queue manager that was defined on a previous **SET MANAGER** statement. You can use the name or nickname of the manager. The name must exactly match the name that is specified on the corresponding **SET MANAGER** command. This parameter is required if the **GROUP** parameter is not specified.

#### GROUP(*group-name*)

Associates this **SET QUEUE** statement with a group of queue managers that were defined on a previous **SET GROUP** statement. The name must exactly match the name that is specified on the corresponding **SET GROUP** statement. This parameter is required if the **MGRNAME** parameter is not specified.

#### QDEFTYPE(PREDEFINED|PERMDYN|TEMPDYN|ALL)

Indicates which types of queues to monitor. Specify any or all of the following definition types:

**PREDEFINED:** Monitor only predefined queues that match the specific or generic queue name. This is the default value.

**PERMDYN:** Monitor only permanent dynamic queues that match the specific or generic queue name.

TEMPDYN: Monitor only temporary dynamic queues that match the specific or generic queue name.

ALL: Monitor all queues that match the specific or generic queue name.

**Remember:** This option does not affect workspaces that contain on-demand data. For example, the Real-time Queue Definitions and Real-time Queue Data workspaces display information that is related to all queues regardless of this attribute.

#### STATISTICS(YES | NO)

Specifies whether to collect queue statistics using WebSphere MQ Reset Queue Statistics command processing.

YES: Collect statistics using Reset Queue Statistics command processing for queues that match the specific or generic queue name.

NO: Do not collect statistics using Reset Queue Statistics command processing for queues that match the specific or generic queue name. This is the default value. See Chapter 7, "Collecting queue statistics data," on page 95 for a description of the Queue Statistics feature.

#### STATUS(ADD | DELETE)

Specifies what to do if this **SET QUEUE** command was previously specified with the same name.

If this parameter is omitted, the queue definition is added if it is a new name; it is modified if the same name was previously specified.

ADD: Creates a new queue definition. If this **SET QUEUE** command was previously specified with the same name, it is not modified and an error message is issued.

DELETE: Deletes a queue definition and all associated historical data.

#### QTYPE (ALL | QLOCAL | QALIAS | QCLUSTER | QREMOTE | QMODEL)

Specifies what types of queues to monitor. Specify any or all of the following queue types:

ALL: Monitor all types of queues. This is the default value.

QLOCAL: Monitor only the local queues.

QALIAS: Monitor only the alias queues.

QCLUSTER: Monitor only the cluster queues.

QREMOTE: Monitor only the remote queues.

QMODEL: Monitor only the model queues.

**Remember:** This parameter does not affect the workspaces that contain on-demand data. For example, the Real-time Queue Definitions and Real-time Queue Data workspaces display information about all queues regardless of this parameter value. You can specify multiple types, such as QTYPE(QLOCAL,QREMOTE).

#### DEFSAMPCYCLE(*n-sample-interval*)

This parameter applies to z/OS systems only.

Specifies how often the queue definition data is to be sampled. The specified number, *n*, indicates that agent collects queue definition data every *n*-th sample. The default value is 1, which indicates that agent collects data at every sample interval. The value 0 indicates that the agent

collects the definitional data only at the first sample interval. After that, the definition data is refreshed only when the agent finds a new local queue.

### Example

- To monitor all queues managed by the MGRA queue manager , specify the following statement:  
SET QUEUE NAME(\*) MGRNAME(MGRA) QDEFTYPE(ALL)
- To monitor a predefined queue named ACCOUNTS, specify the following statement:  
SET QUEUE NAME(ACCOUNTS) MGRNAME(MGRA)
- To monitor and collect statistics using Reset Queue Statistics command processing for all predefined queues managed by the QMGRA queue manager, specify the following statement:  
SET QUEUE NAME(\*) MGRNAME(QMGRA) STATISTICS(YES)
- To monitor permanent dynamic queues on the MGRA queue manager and whose names start with PAYR, specify the following statement:  
SET QUEUE NAME(PAYR\*) MGRNAME(MGRA) QDEFTYPE(PERMDYN)
- To monitor predefined and temporary dynamic queues on the MGRC queue manager and whose names start with MARCH, specify the following statement:  
SET QUEUE NAME(MARCH\*) MGRNAME(MGRC) -  
QDEFTYPE(PREDEFINED,TEMPDYN)

## SET CHANNEL

Use the **SET CHANNEL** statement to specify the channels to be monitored.

### Syntax

```
SET CHANNEL NAME(channel-name-mask)  
MGRNAME(manager-name) | GROUP(group-name)  
[STATUS(ADD|DELETE)]
```

### Parameters

#### NAME(*channel-name-mask*)

Specifies a 1- through 20-character specific or generic name of the channels that you want to monitor. To specify a generic name, enter a string of characters followed by an asterisk (\*). This field is required.

#### MGRNAME(*manager-name*)

Associates this **SET CHANNEL** statement with a queue manager that is defined on a previous **SET MANAGER** statement. You can use the name or nickname of the manager. The name must exactly match the name specified on the corresponding **SET MANAGER** statement. This parameter is required if the **GROUP** parameter is not specified.

#### GROUP(*group-name*)

Associates this **SET CHANNEL** statement with a group of queue managers defined on a previous **SET GROUP** statement. The name must exactly match the name specified on the corresponding **SET GROUP** statement. This parameter is required if the **MGRNAME** parameter is not specified.

#### STATUS(ADD|DELETE)

Specifies what to do if this **SET CHANNEL** statement was previously specified with the same name.

If this parameter is omitted, the result is the same as specifying ADD.

**ADD:** Creates a new channel definition. If this **SET CHANNEL** statement was previously specified with the same name, it is not modified and an error message is issued.

**DELETE:** Deletes a channel definition and all associated historical data.

## Example

To monitor a channel named MONTANA on the SMONICA queue manager, specify the following statement:

```
SET CHANNEL NAME(MONTANA) MGRNAME(SMONICA)
```

## SET EVENTLOG

Use the **SET EVENTLOG** statement to specify the size, location, and other attributes of the event log.

All parameters are optional; but, if the **SET EVENTLOG** statement is set, you must specify at least one parameter.

This statement applies to all systems except z/OS systems.

### Syntax

```
SET EVENTLOG
    [SIZE(n)]
    [DIR(dir_name)]
    [ARCHIVEFILE(arch_filename)]
    [ARCHIVEOPTS(krarloff_options)]
```

### Parameters

#### SIZE(*n*)

The *n* value is the maximum event log file size, in MBs. The default value is 10. Specify SIZE(0) to disable the event log.

#### DIR(*dir\_name*)

The directory to write the event log file to. The default value is the value that is assigned to the ctira\_hist\_dir variable @logpath@:

- Windows systems (32-bit agent): *install\_dir*\TMAITM6\logs\History\KMQ\*instance\_name*
- Windows systems (64-bit agent): *install\_dir*\TMAITM6\_x64\logs\History\KMQ\*instance\_name*
- UNIX and Linux systems: *install\_dir/arch/mq/hist/instance\_name*

Where *instance\_name* is the name of the queue manager that you want to monitor, *install\_dir* is the IBM Tivoli Monitoring installation directory, and *arch* is the architecture code of the operating system. See *Installation and Setup Guide* for a complete list of architecture codes.

#### ARCHIVEFILE(*arch\_filename*)

The archive directory and file name. The default value is @logpath@\Qmeventh.arc. If this file already exists, new data is appended to it.

#### ARCHIVEOPTS(*krarloff\_options*)

If **ARCHIVEOPTS** is not specified, all *krarloff* defaults are taken. See the *IBM Tivoli Monitoring Administrator's Guide* for details of the **krarloff** (krapolloff) command.

## SET EVENTQIN

Use the **SET EVENTQIN** statement to specify the event queues that are monitored by the WebSphere MQ Monitoring agent for a queue manager or group of queue managers, which includes the queue manager event queue, channel event queue, performance event queue, configuration event queue, command event queue, and logger event queue.

If there is not a **SET EVENTQIN** statement that applies to a queue manager, the following default WebSphere MQ event queues are monitored:

- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT

### Syntax

```
SET EVENTQIN
    MGRNAME(manager-name) | GROUP(group-name)
    [QMGRQ(queue-name)]
    [CHANNELQ(queue-name)]
    [PERFMQ(queue-name)]
    [CONFIGQ(queue-name)]
    [COMMANDQ(queue-name)]
    [LOGGERQ(queue-name)] (distributed systems only)
    [REPEATLIMIT(event-repeat-time-limit)]
    [QMGRQREPEATLIMIT(qmgrevent-repeat-time-limit)]
    [CHANNELQREPEATLIMIT(chnlevent-repeat-time-limit)]
    [PERFQREPEATLIMIT(perfqevent-repeat-time-limit)]
    [CONFIGQREPEATLIMIT(configqevent-repeat-time-limit)]
    [COMMANDQREPEATLIMIT(cmdqevent-repeat-time-limit)]
    [LOGGERQREPEATLIMIT(loggerqevent-repeat-time-limit)]
    (distributed systems only)
```

### Parameters

#### MGRNAME(*manager-name*)

The queue manager that owns the specified event queues. You can use the name or nickname of the queue manager. The name must exactly match the name that is specified on the corresponding **SET MANAGER** statement. This parameter is required if the **GROUP** parameter is not specified.

#### GROUP(*group-name*)

A group of queue managers (as specified on a previous **SET GROUP** statement), each of which owns the specified event queues. The name must exactly match the name that is specified on the corresponding **SET GROUP** statement. This parameter is required if the **MGRNAME** parameter is not specified.

#### QMGRQ(*queue-name*)

Specifies the name of the queue manager event queue to monitor.

#### CHANNELQ(*queue-name*)

Specifies the name of the channel event queue to monitor.

#### PERFMQ(*queue-name*)

Specifies the name of the performance event queue to monitor.

**CONFIGQ(*queue-name*)**

Specifies the name of the configuration event queue to monitor. Configuration events occur on WebSphere MQ for distributed systems V7.0.1 and higher versions, or WebSphere MQ for z/OS systems V5.3 and higher versions only.

**COMMANDQ(*queue-name*)**

Specifies the name of the command event queue to monitor. Command events occur on WebSphere MQ for distributed systems V7.0.1 and higher versions, or WebSphere MQ for z/OS systems V6.0 and higher versions only.

**LOGGERQ(*queue-name*)**

This parameter is not valid on z/OS systems.

Specifies the name of the logger event queue to monitor.

**REPEATLIMIT(*event-repeat-time-limit*)**

Specifies the maximum number of times that an event is repeated before the agent stops logging the event of the same type and resource within the same 5 minute interval. If an event repeats more than the specified value within 5 minute interval, the agent will stop writing the repeated events to event logs or event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0, which means every event will be processed.

This parameter applies to all event queues unless a specific value is specified for a queue by using the following parameters:

- QMGRQREPEATLIMIT
- CHANNELQREPEATLIMIT
- PERFMQREPEATLIMIT
- CONFIGQREPEATLIMIT
- COMMANDQREPEATLIMIT
- LOGGERQREPEATLIMIT

**QMGRQREPEATLIMIT(*qmgrevent-repeat-time-limit*)**

Specifies the maximum number of times that a queue manager event is repeated before the agent stops logging the event within the same 5 minute interval. If a queue manager event repeats more than the specified value within 5 minute interval, when the repeated events of the same type and resource come into the queue manager event queue, the agent will stop writing the repeated events to event logs or event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0.

**CHANNELQREPEATLIMIT(*chnnevent-repeat-time-limit*)**

Specifies the maximum number of times that an event from a channel event queue is repeated before the agent stops logging the event within the same 5 minute interval. If an event repeats more than the specified value within 5 minute interval, when the repeated events of the same type and resource come into the channel event queue, the agent will stop writing the repeated events to event log ors event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0.

**PERFQREPEATLIMIT(*perfqevent-repeat-time-limit*)**

Specifies the maximum number of times that an event from a performance event queue is repeated before the agent stops logging the event within the

same 5 minute interval. If an event repeats more than the specified value within 5 minute interval, when the repeated events of the same type and resource come into the performance event queue, the agent will stop writing the repeated events to event logs or event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0.

**CONFIGQREPEATLIMIT***(configevent-repeat-time-limit)*

Specifies the maximum number of times that an event from a configuration event queue is repeated before the agent stops logging the event within the same 5 minute interval. If an event repeats more than the specified value within 5 minute interval, when the repeated events of the same type and resource come into the configuration event queue, the agent will stop writing the repeated events to event logs or event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0.

**COMMANDQREPEATLIMIT***(cmdqevent-repeat-time-limit)*

Specifies the maximum number of times that an event from a command event queue is repeated before the agent stops logging the event within the same 5 minute interval. If an event repeats more than the specified value within 5 minute interval, when the repeated events of the same type and resource come into the default or specified command event queue, the agent will stop writing the repeated events to event logs or event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0.

**LOGGERQREPEATLIMIT***(loggerqevent-repeat-time-limit)*

This parameter is for distributed systems only.

Specifies the maximum number of times that an event from a logger event queue is repeated before the agent stops logging the event within the same 5 minute interval. If an event repeats more than the specified value within 5 minute interval, when the repeated events of the same type and resource come into the logger event queue, the agent will stop writing the repeated events to event logs or event tables. Processing of events of the specific event type and resource will be resumed after the 5 minute interval. The default value is 0.

For all the event repeat limit parameter, the event processing occurs as follows:

- If a repeat limit of 0 is specified (or no REPEATLIMIT specified), every event processed will be processed.
- If a nonzero repeat limit value is specified, when an event of a specific event type with the same resource repeats more than the specified value and are processed within the last 5 minutes, the event will not be passed to MQSeries Events (pure event table), Event Archive (pure event table with details), and Event Log tables. An internal limit of 5 unique resources for a given event type and queue manager is retained for checking repeat limit. In cases where more than 5 events of the same type are repeating at the same time within a 5 minute interval, one or more repeating events might still be written out if more than the specified repeat limit value, because only the last 5 resources will be retained.
- All events are processed for the purpose of current events.
- All events are passed to the EVENTQOUT queues.

**Example**

- To read events from a performance event queue named PERFORMANCE.EVENTS.IN on the MQM3 queue manager instead of from the

default WebSphere MQ performance event queue  
SYSTEM.ADMIN.PERFM.EVENT, specify the following statement:

```
SET EVENTQIN MGRNAME(MQM3) PERFMQ(PERFORMANCE.EVENTS.IN)
```

This example can apply to two possible scenarios:

- An application is reading from the default WebSphere MQ performance event queue and copying events to the PERFORMANCE.EVENTS.IN queue.
- Your site has changed the default WebSphere MQ performance queue name from SYSTEM.ADMIN.PERFM.EVENT to PERFORMANCE.EVENTS.IN
- To read events from a channel event queue called CHANNEL.EVENTS.IN on the MQM2 queue manager and copy these events to a queue called CHANNEL.EVENTS.OUT, specify the following statements:

```
SET EVENTQIN MGRNAME(MQM2) CHANNELQ(CHANNEL.EVENTS.IN)
```

```
SET EVENTQOUT MGRNAME(MQM2) CHANNELQ(CHANNEL.EVENTS.OUT)
```

This example also uses the SET EVENTQOUT statement (see “SET EVENTQOUT”).

**Remember:** If the queues that you specify in the SET EVENTQIN statement do not exist in your WebSphere MQ environment, you must restart the agent after you create these queues in your environment.

## SET EVENTQOUT

If you use the EVENTS(Remove) option on the **SET GROUP** or **SET MANAGER** statement, when WebSphere MQ Monitoring agent reads an event message from an event queue, it deletes the message from the event queue to ensure that it is processed only once. If another application that is running at your site requires access to event messages, you can use the **SET EVENTQOUT** to define output queues where these messages are copied and point the other application to these queues.

The **SET EVENTQOUT** statement identifies one or more output queues where queue manager event messages, channel event messages, performance event messages, configuration event messages, command event messages, and logger event messages are copied to.

If there is no **SET EVENTQOUT** statement that applies to a queue manager, the event messages are discarded after being processed.

### Syntax

```
SET EVENTQOUT
  MGRNAME(manager-name) | GROUP(group-name)
  [QMGRQ(queue-name)]
  [CHANNELQ(queue-name)]
  [PERFMQ(queue-name)]
  [CONFIGQ(queue-name)]
  [COMMANDQ(queue-name)]
  [LOGGERQ(queue-name)] (distributed systems only)
```

### Parameters

#### MGRNAME(*manager-name*)

The queue manager that owns the specified output queues. You can use the name or nickname of the queue manager. The name must exactly match the name that is specified on the corresponding **SET MANAGER** statement. This parameter is required if the **GROUP** parameter is not specified.

**GROUP**(*group-name*)

The group of queue managers (as specified on a previous **SET GROUP** statement), each of which owns the specified event queues. The name must exactly match the name that is specified on the corresponding **SET GROUP** statement. This parameter is required if the **MGRNAME** parameter is not specified.

**QMGRQ**(*queue-name*)

Specifies the name of the local queue where queue manager events are copied after being processed. This queue must exist when the **SET EVENTQOUT** statement is processed.

**CHANNELQ**(*queue-name*)

Specifies the name of the local queue where channel events are copied after being processed. This queue must exist when the **SET EVENTQOUT** statement is processed.

**PERFMQ**(*queue-name*)

Specifies the name of the local queue where performance events are copied after being processed. This queue must exist when the **SET EVENTQOUT** statement is processed.

**CONFIGQ**(*queue-name*)

Specifies the name of the local queue where configuration events are copied after being processed. This queue must exist when the **SET EVENTQOUT** statement is processed. Configuration events occur on WebSphere MQ for distributed systems V7.0.1 and higher versions, or WebSphere MQ for z/OS systems V5.3 and higher versions only.

**COMMANDQ**(*queue-name*)

Specifies the name of the local queue where command events are copied after being processed. This queue must exist when the **SET EVENTQOUT** statement is processed. Command events occur on WebSphere MQ for distributed systems V7.0.1 and higher versions, or WebSphere MQ for z/OS systems V6.0 and higher versions only.

**LOGGERQ**(*queue-name*)

Specifies the name of the local queue where logger events are copied after being processed. This queue must exist when the **SET EVENTQOUT** statement is processed. Logger events occur on WebSphere MQ for distributed systems V6.0 and higher versions only.

**Example**

- To read events from the default queue manager SYSTEM.ADMIN.QMGR.EVENT event queue on the MQM1 queue manager, and copy them to a queue named QMGR.EVENTS.OUT, specify the following statement:  

```
SET EVENTQOUT MGRNAME(MQM1) QMGRQ(QMGR.EVENTS.OUT)
```
- To read events from a channel event queue named CHANNEL.EVENTS.IN on the MQM2 queue manager, and copy these events to a queue called CHANNEL.EVENTS.OUT, specify the following statements:  

```
SET EVENTQIN MGRNAME(MQM2) CHANNELQ(CHANNEL.EVENTS.IN)
```

```
SET EVENTQOUT MGRNAME(MQM2) CHANNELQ(CHANNEL.EVENTS.OUT)
```

This example also uses the SET EVENTQIN statement (see “SET EVENTQIN” on page 43).

**Remember:** If the queues that you specify in the SET EVENTQOUT statement do not exist in your WebSphere MQ environment, you must restart the agent after you create these queues in your environment.

## PERFORM INCLUDE

The **PERFORM INCLUDE** statement points to an external file that contains customization commands. To issue the commands in this file while the agent is starting up, specify the **PERFORM INCLUDE** statement in the monitoring file of the agent.

### Syntax

```
PERFORM INCLUDE LIST(file-ID)
```

### Parameters

#### LIST(*file-ID*)

The name of the file that contains a list of WebSphere MQ Monitoring agent customization commands. On z/OS systems, *file-ID* must be a member of the RKANCMD data set. This parameter is required.

### Example

- To issue a set of external commands in the `remote.txt` file, specify the following statement:

```
PERFORM INCLUDE LIST(remote.txt)
```

- To issue a set of external commands in the MYSET member of the RKANCMD data set on a z/OS system, specify the following statement:

```
PERFORM INCLUDE LIST(MYSET)
```

## PERFORM STARTMON

Use the **PERFORM STARTMON** statement to initiate monitoring of WebSphere MQ objects, to specify the sampling interval for collecting WebSphere MQ data, and to specify whether historical data is collected.

The **PERFORM STARTMON** statement is required.

### Syntax

```
PERFORM STARTMON
  SAMPINT(sample-interval)
  HISTORY (YES|NO)
  [ACTIVEONLY(YES|NO)]
  [ROWLIM(limit)]
  [SVRCONN(YES|NO)]
  [QSGCHKINTERVAL(sss)] (z/OS systems only)
  [GRPNAME(KMQQSG|ggggggg)] (z/OS systems only)
  [STAGGERSAMPLE(YES|NO)]
```

### Parameters

#### SAMPINT(*sample-interval*)

How often, in seconds, WebSphere MQ Monitoring agent samples your queue managers for performance data. The default value is 300. The minimum is 10 seconds. The **SAMPINT** setting does not affect the amount of historical data that is produced.

If your site is monitoring a large number of queues or channels, you might experience a degradation in performance. If this occurs, increase the SAMPINT value to improve performance.

If your site is monitoring queue-sharing groups on z/OS systems, the sample interval must be the same for all the agents that monitor queue managers in queue-sharing groups.

You can modify the effective sampling interval for a specific queue manager or a group of queue managers with the **ICYCLE** parameter of the **SET MANAGER** or the **SET GROUP** statement. See **ICYCLE** in “SET MANAGER” on page 29 and **ICYCLE** in “SET GROUP” on page 26.

#### **HISTORY(YES | NO)**

Defines whether historical data is collected for attribute groups whose data is sampled by the agent. Set it to YES to collect historical data. On distributed systems and z/OS systems, the value that is configured automatically during the installation and configuration process is NO. (For information about using the historical data collection function, see Chapter 5, “Collecting historical data,” on page 79. For information about sampled and on-demand attribute groups, see “Sampled and on-demand tables” on page 173.)

#### **ACTIVEONLY(YES | NO)**

This parameter applies only to z/OS systems

This optional parameter indicates whether to monitor *only* active queue managers.

YES: Only queue managers that are running when the agent is started, or that become active while the agent is running, are referenced in situations and displayed in the Navigator physical view. You can set it to YES if your environment has a large number of queue managers defined but only some of them are in use.

NO: All defined queue managers, active or not, are referenced in situations and displayed in the Navigator physical view.

The default value is NO.

#### **ROWLIM(limit)**

This optional parameter specifies the maximum number of messages that are processed and returned by the agent when reading messages from a queue for report requests. The default value is 0 (zero), which means that the maximum number of messages is not limited.

#### **SVRCONN(YES | NO)**

This optional parameter indicates whether to collect server connection channel statistics that are displayed in the Channel Performance workspaces (and the short and long-term Channel Performance History workspaces). The default value is YES.

#### **QSGCHKINTERVAL(sss)**

This parameter applies only to z/OS systems

This optional parameter specifies how often, in seconds, WebSphere MQ Monitoring agent performs queue-sharing group monitoring activities. The default value is 300, which is a 5-minute interval. The minimum is 60 seconds. This value can be set to 0 to turn off queue-sharing group monitoring activities. If you turn this processing off, you must recycle the agent to turn this processing back on.

### GRPNAME(KMQQSG | gggggggg)

This parameter applies only to z/OS systems

Use this optional parameter to specify an alternative sysplex XCF group name, *gggggggg* (1 - 8 characters), for the coexistence of multiple collection agents. The default value is KMQQSG. Typically, this parameter is not specified. By using this parameter that is intended for testing purposes, multiple agents can coexist while being tested.

**Exception:** Do not specify an XCF group name that is in use by other system components because unexpected consequences might occur.

### STAGGERSAMPLE(YES | NO)

Specifies whether queue manager sample collection is done all at once or at staggered intervals.

**YES:** The sample collection for different queue managers is started at different times during the interval. When the agent is monitoring several queue managers, the value YES can help avoid a spike in CPU utilization at each sample interval.

**NO:** The sample collection for all queue managers is started at the same time.

The default value is NO.

## Example

To start monitoring with a sampling interval of 120 seconds, and to explicitly specify that historical data and server connection channel statistics are to be collected, you can specify the following statement:

```
PERFORM STARTMON SAMPINT(120) HISTORY(YES) SVRCONN(YES)
```

## SET AGENT

Use the **SET AGENT** statement to specify the middle qualifier that is used in the managed system name.

When the WebSphere MQ Monitoring agent is started, it registers the following managed system:

- On distributed system: *monitoredqueuemanagername:agentid:MQ*
- On z/OS systems: *monitoredqueuemanagername:agentid:MQESA*

where *monitoredqueuemanagername* is the name of the queue manager that is monitored by the agent, *agentid* is the middle qualifier of the managed system name.

On distributed systems, if the *agentid* value is not specified, no value is used.

On z/OS systems, if the *agentid* value is not specified, the host name is used. If you specify this value, it is used only in the managed system names of subnodes.

For example, to avoid confusion and to enable multiple WebSphere MQ Monitoring agents, instead of issuing the default agent startup command `IRAMAN KMQAGENT START`, which starts a node named *hostname:MQIRA*, issue the modified agent startup command to start a node named *agentid:MQIRA*:

```
IRAMAN KMQAGENT START agentid
```

You can use the **SET AGENT** statement to do the following operations:

- Two active WebSphere MQ Monitoring agents that connect to the same hub monitoring server cannot have the same managed system name.
  - On distributed systems, if your site has multiple queue managers with the same name that are running on different nodes, you must specify the agent name for each queue manager. So that the WebSphere MQ Monitoring agent can create unique managed system name.
  - On distributed systems, If the length of the managed system name exceeds 32 characters, two different queue manager names might resolve to the same one because of truncation. To distinguish the managed system names for queue managers, specify the agent name for each queue manager.
- Group and identify queue manager names by something other than the host name and queue manager name, such as a high availability cluster name.
- Enable multiple agents that are connected to the same Tivoli Enterprise Monitoring Server to monitor the same queue manager.

## Syntax

```
SET AGENT NAME(agentid)
```

## Parameters

**NAME(*agentid*)**

The name to be used for the middle qualifier of the managed system name.

On distributed systems, the complete managed system name is *monitoredqueuemanagername:agentid:MQ*.

On z/OS systems, the complete managed system name is *monitoredqueuemanagername:agentid:MQESA*.

The maximum length for the complete managed system name is 32 characters, so the maximum length for *agentid* depends on the length of the queue manager name. If there are not enough characters to fit the full *agentid* that is specified, it is truncated to no less than 8 characters.

## Example

To monitor a queue manager named PERSONNEL on the AIX1 node when there is also a queue manager named PERSONNEL on a node named HPUX2, specify the following statements in the monitoring file for the AIX1 node:

```
SET MANAGER NAME(PERSONNEL)
SET AGENT NAME(AIX1)
```

To simultaneously monitor the PERSONNEL queue manager on the HPUX2 node, specify the following statements in the monitoring file for the HPUX2 node:

```
SET MANAGER NAME(PERSONNEL)
SET AGENT NAME(HPUX2)
```

## SET APPL (z/OS systems only)

Use the **SET APPL** statement to identify the z/OS system applications that are based on WebSphere MQ, CICS<sup>®</sup> transactions, and IMS<sup>™</sup> programs that must be monitored for application debugging information and application statistics.

Use the **SET APPL** statement must be used in combination with the SET MQIMONITOR statement to activate the application debugging and application statistics features. See “SET MQIMONITOR (z/OS systems only)” on page 53 for a description of SET MQIMONITOR.

## Syntax

```
SET APPL NAME(application-name)  
    [TRANPGM(program-name)]  
    [MGRNAME(manager-name)]  
    [TRACE(NO|YES)]  
    [TRACELIMIT(1000|number-of-trace-records)]  
    [STATISTICS(NONE|NOQDATA|NODYNAMQ|ALL)]  
    [STATUS(ADD|DELETE)]
```

## Parameters

### NAME(*application-name*)

A 1- through 8-character name of the z/OS system application to be monitored. To specify a generic name, enter a character string followed by an asterisk (\*).

The application name format differs, depending on the monitored applications:

- For batch applications, it is the 1- through 8-character job name.
- For TSO applications it is the 1- through 7-character user ID of the TSO session.
- For CICS applications it is the 1- through 8-character VTAM® applid.
- For IMS applications it is the 1- through 4-character IMS subsystem ID that is prefixed with the characters IMS and padded with a blank.

This parameter is required.

### TRANPGM(*program-name*)

Further identifies one or more programs to monitor, as follows:

- The 1- through 4-character name of the CICS transaction to monitor in the VTAM applid that is identified by the **NAME** parameter.
- The 1- through 8-character name of the IMS program in the IMS subsystem that is identified by the **NAME** parameter.
- The 1- through 8-character name of the batch or TSO program in the address space that is identified by the **NAME** parameter.

To specify a generic name, enter a character string followed by an asterisk (\*). This parameter is optional. The default value is an asterisk (\*).

### MGRNAME(*manager-name*)

The name of one or more z/OS system queue managers with applications that are to be monitored. To specify a generic name, enter a character string followed by an asterisk (\*). The name must exactly match the name specified on the corresponding **SET MANAGER** statement. This parameter is optional. The default value is an asterisk (\*).

### TRACE(NO|YES)

Specifies whether to record WebSphere MQ tracing information for this application. This parameter is optional. The default value is NO.

### TRACELIMIT(1000|*number-of-trace-records*)

Specifies the number of trace records to save for later viewing. After this value is reached, trace recording for this application is stopped. The maximum value is 12000; the default value is 1000. You can issue the **SET APPL** statement again with this parameter to resume trace recording after saving the maximum number of records. This parameter is optional.

## STATISTICS(NONE | NOQDATA | NODYNAMQ | ALL)

Specify the level of statistical information to collect for the applications that is identified by the **NAME** parameter, as follows:

- NONE  
No statistical information is collected for this application.
- NOQDATA  
Application statistical information is not collected at the queue level; however, statistical information is still collected at the application and transaction levels.
- NODYNAMQ  
Application statistical information is not collected for dynamic queues (temporary and permanent); however, statistical information is still collected for predefined queues. Specifying NODYNAMQ activates Application Queue Statistics monitoring. Specifying NODYNAMQ does not affect the collection of application statistics at the application and transaction level.
- ALL  
Statistical information is collected at the application, transaction, and queue levels.

This parameter is optional. The default value is NODYNAMQ.

## STATUS(ADD | DELETE)

Specifies what to do if this **SET APPL** statement was previously specified with the same name.

If this parameter is omitted, the application definition is added if it is a new name, it is modified if the same name was specified previously.

- ADD  
Creates a new application definition. If this **SET APPL** statement was previously specified with the same name, it is modified and an error message is issued.
- DELETE  
Deletes the application definition and all its associated historical data.

## Example

To collect only application-level and transaction-level statistics and WebSphere MQ tracing information, specify the following statement for all the transactions that are running in the PAYR CICS region :

```
SET APPL NAME(PAYR) TRACE(YES) STATISTICS(NOQDATA)
```

## SET MQIMONITOR (z/OS systems only)

The **SET MQIMONITOR** statement activates monitoring for the applications that you specify using the **SET APPL** statement. You must specify the **SET MQIMONITOR** statement to turn on monitoring after using **SET APPL** to specify the applications to monitor.

Use the **SET MQIMONITOR** statement with the **SET APPL** statement to activate the application debugging and application statistics features.

## Syntax

```
SET MQIMONITOR STATUS(INSTALL|REMOVE|FREMOVE)
    MGRNAME(manager-name) | GROUP(group-name)
    BUFFERSIZE(initial-buffer-space)
    BUFFERSIZEMAX(max-buffer-space)
    BUFFERINCREMENTSIZ(increment-buffer-size)
```

## Parameters

### STATUS(INSTALL|REMOVE|FREMOVE)

This parameter is required. It specifies whether monitoring for the z/OS system applications, CICS transactions, and IMS programs that are identified on the SET APPL statement is turned on.

- **INSTALL**  
Application monitoring is turned on for the z/OS system applications, CICS transactions, and IMS programs that are identified on the **SET APPL** statement. (If no **SET APPL** statement is specified, no data is collected.)
- **REMOVE**  
Application monitoring is turned off for the applications that are identified on the **SET APPL** statement. If monitoring is not activated by a previous SET MQIMONITOR STATUS(INSTALL) statement, this request is ignored.
- **FREMOVE**  
Use the FREMOVE option only when you are instructed to do so by IBM Software Support. This parameter removes and stops application monitoring.

### MGRNAME(*manager-name*)

Application monitoring is turned on or off for the queue manager that is identified by a previous **SET MANAGER** statement. The name must exactly match the name that is specified on a previous **SET MANAGER** statement. This parameter is required if the **GROUP** parameter is not specified.

### GROUP(*group-name*)

Application monitoring is turned on or off for the group of queue managers that are identified by a previous **SET GROUP** statement. The name must exactly match the name that is specified on a previous **SET GROUP** statement. This parameter is required if the **MGRNAME** parameter is not specified.

### BUFFERSIZE(*initial-buffer-space*)

Applies only when the **STATUS(INSTALL)** statement is also specified. This parameter specifies the initial buffer size (in MBs) of buffer data space for monitoring WebSphere MQ applications.

This parameter is optional. The default value, if **BUFFERSIZE** is not specified on the **SET MQIMONITOR** command, is 32.

The maximum value is 2048 (2 GB of buffer storage).

### BUFFERSIZEMAX(*max-buffer-space*)

This parameter specifies the maximum buffer size (in MBs) of buffer data space for monitoring WebSphere MQ applications. This parameter is optional.

The default value, if **BUFFERSIZEMAX** is not specified on the **SET MQIMONITOR** command, is 128 or the value of **BUFFERSIZE**, whichever is greater.

The maximum value is 2048 (2 GB of buffer storage). When the maximum data space size that is available is reached, the applications monitoring is temporarily disabled, and enabled again when the data space is available.

#### **BUFFERINCREMENTSIZ**(*increment-buffer-size*)

This parameter specifies the increment buffer size (in MBs) of buffer data space to be expanded when the data space usage reaches the threshold (75%). This parameter is optional.

The default value, if **BUFFERINCREMENTSIZ** is not specified on the **SET MQIMONITOR** command, is 32.

The maximum value is 2048 (2 GB of buffer storage).

### **Example**

To begin collecting application debugging information and application statistics for the applications running for the PRD1 queue manager, with a buffersize of 32 MBs, specify the following statement:

```
SET MQIMONITOR STATUS(INSTALL) MGRNAME(PRD1) BUFFERSIZE(32) -  
BUFFERSIZEMAX(512) BUFFERINCREMENTSIZ(32)
```

## **SET QSG (z/OS systems only)**

Use the **SET QSG** statement to specify the queue-sharing groups that the WebSphere MQ Monitoring agent on z/OS system monitors and the queue managers that the agent uses to collect queue-sharing group data. At any given time, for a particular queue-sharing group, WebSphere MQ Monitoring agent uses only one queue manager to gather data. If that queue manager becomes unavailable, another queue manager collects the data instead.

The **SET QSG** statement is optional. If this statement is not specified, the default behavior of the agent is to monitor *all* queue-sharing groups that are associated with monitored queue managers.

You can use the **SET QSG** statement to specify the following behaviors:

- No queue-sharing groups are monitored.
- A particular queue-sharing group is monitored.
- A particular queue manager is used to collect queue-sharing group data.

### **Syntax**

```
SET QSG [NAME(nnnn)]  
        [MGRNAME(mmmm)]  
        [MONITOR(NO|YES|TAKEOVER)]
```

### **Parameters**

#### **NAME**(*nnnn*)

Specifies the name of a queue-sharing group. This parameter is optional. The default value is an asterisk (\*).

#### **MGRNAME**(*mmmm*)

Specifies a queue manager name in a particular queue-sharing group. This parameter is optional. The default value is an asterisk (\*).

## MONITOR(NO|YES|TAKEOVER)

Specifies whether the agent monitors the specified combination of queue-sharing group and queue manager. It also specifies whether takeover processing is performed.

This parameter is optional. The default value is YES.

NO: The WebSphere MQ Monitoring agent does not monitor the indicated combination of queue-sharing group and queue manager.

YES: The WebSphere MQ Monitoring agent monitors the indicated combination of queue-sharing group and queue manager. This is the default behavior.

TAKEOVER: The WebSphere MQ Monitoring agent takes over monitoring the indicated queue-sharing group even if another WebSphere MQ Monitoring agent is already monitoring it. (Takeover processing does not occur if the other agent also specified TAKEOVER.)

### Example

- To monitor no queue-sharing groups, specify the following statement:  
SET QSG MONITOR(NO)
- To eliminate queue manager PMQ5 from queue-sharing group monitoring, specify the following statement:  
SET QSG MONITOR(NO) MGRNAME(PMQ5)
- To direct queue-sharing group monitoring to the PMQ6 queue manager, specify the following statement:  
SET QSG MONITOR(TAKEOVER) MGRNAME(PMQ6)
- To specify that a particular queue-sharing group is, or is not, monitored might require multiple **SET QSG** statements.

For example, suppose that you have three queue-sharing groups in your environment named QSGA, QSGB, and QSGC. To monitor only the QSGC queue-sharing group, specify the following statements:

```
SET QSG NAME(*) MONITOR(NO)
SET QSG NAME(QSGC) MONITOR(YES)
```

The following statements produce the same result:

```
SET QSG NAME(QSGA) MONITOR(NO)
SET QSG NAME(QSGB) MONITOR(NO)
SET QSG NAME(QSGC) MONITOR(YES)
```

However, if you specify only the following statement, all three queue-sharing groups, including QSGA and QSGB, are monitored. This is because the default behavior of the agent is to monitor all queue-sharing groups.

```
SET QSG NAME(QSGC) MONITOR(YES)
```

## SET SUBSYSTEM (z/OS systems only)

Use the **SET SUBSYSTEM** statement to specify the subsystem that is used by the WebSphere MQ Monitoring agent on a z/OS system to collect application statistics data. A single subsystem used by the WebSphere MQ Monitoring agent can be shared among all WebSphere MQ Monitoring agents that are running on the same logical partition (LPAR).

The **SET SUBSYSTEM** command is optional. This statement must not be specified under typical circumstances. If this statement is not specified, the WebSphere MQ Monitoring agent uses the default subsystem named KMQ1 on a z/OS system.

You can use the **SET SUBSYSTEM** command under the following circumstances:

- The initialization of default subsystem KMQ1 failed and you do not want to wait for an initial program load (IPL).
- You want to use a separate subsystem for some WebSphere MQ Monitoring agents.

For more information about subsystem, see *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide*.

## Syntax

```
SET SUBSYSTEM NAME(nnnn)
```

## Parameters

**NAME(*nnnn*)**

The name of the subsystem that is used by the WebSphere MQ Monitoring agent. *nnnn* must be a valid subsystem identifier. It can be up to four characters long.

## Example

- To use the KMQ2 subsystem as the subsystem for the WebSphere MQ Monitoring agent, specify the following statement:

```
SET SUBSYSTEM NAME(KMQ2)
```



---

## Chapter 3. Using situations and Take Action commands

A set of predefined situations and Take Action commands are included with WebSphere MQ Monitoring agent.

---

### Predefined situations

A situation is a logical expression involving one or more system conditions. Situations are used to monitor the condition of systems in your network. You can manage situations from Tivoli Enterprise Portal by using the Situation editor.

A set of predefined situations is included with WebSphere MQ Monitoring agent to check system conditions that are common to many enterprises. These predefined situations can also be used as templates for creating your own custom situations. Using predefined situations can improve the speed with which you can begin using WebSphere MQ Monitoring agent.

For a list of the predefined situations that are provided with WebSphere MQ Monitoring agent and the descriptions and formulas of these situations, see Tivoli Enterprise Portal online help.

**Restriction:** Do not customize the predefined situations because they are overwritten when you install fix packs or upgrade to a later version of WebSphere MQ Monitoring agent, and the changes are lost.

---

### Creating a situation using a predefined situation as a template

You can create your own custom situations to alert you of certain conditions in your environment.

Before you create your own situations, make sure that you understand the event conditions and formulas of the predefined situations.

To create a situation using a predefined one as a template, do the following steps:

1. In the Tivoli Enterprise Portal, click **Edit > Situation Editor** to open the Situation Editor window.
2. Right-click the predefined situation that you want to use as a template, and click **Create Another**.
3. Type a name that is different from the original one for the situation, change the default description, and click **OK**.
4. In the Situation Editor, select the tabbed pages to make appropriate changes.
5. When you finish composing or editing the situation, save your changes, and start the situation by clicking **Apply** to keep the editor open, or click **OK** to close the Situation editor.

**Remember:** When you use the Topic Status attribute group to define a condition that you want to monitor, if the **Topic String** attribute is not added to the situation, the situation filters only the topics that are displayed by default in the **Topic Status** view. If you want to filter all the topics, add the Query String == '#' expression to the formula.

---

## Take Action commands

By using the Take Action feature of Tivoli Enterprise Portal, you can issue a command to any system in your network where one or more monitoring agents are installed. You can implement commands from the Take Action view, from a situation (when it becomes true), from the Navigator, or from a row in a table view.

For a complete description of the predefined Take Action commands provided with this product, see Tivoli Enterprise Portal online help.

---

## Creating a custom Take Action command

You can create take action definitions and save them, and then invoke them at will from the menu for Navigator item or query-based view, or automatically when a situation event is opened.

Your user ID must have Modify permission for the Action feature.

Take the following steps to create a custom Take Action command:

1. Right-click the Navigator item that is associated with the application on which you want to run the command.
2. Click **Take Action > Create or Edit**.
3. In the Selection Action window, select **<Create new action>** and click **OK**.
4. In the Create New Action window, type a name and description for the command.
5. Select **MQSeries** from the Monitored Application list.
6. Select the type of command.
  - System Command is for issuing a control command.
  - MQSeries is for issuing an MQSC command.
7. In the **Command** field, type the command just as you would from the command line.

**Remember:** The character limit is 512 bytes, including the attribute substitution that you select in the next step.

8. If you want to insert an attribute variable, which will be replaced by its value at run time, click **Insert Attribute**, select one from the Select Attribute window and click **OK**.
9. Click **OK** to save the Take Action command.

Your user-defined Take Action command is now selectable from the list of Take Actions available for this agent.

For example, to create a Take Action command to modify a queue manager to enable the collection of statistics monitoring information and set the collection interval, select **MQSERIES** in step 6 and enter `ALTER QMGR STATMQI(ON) STATINT(n)` in step 7, where *n* is a number that ranges from 1 through 604800, which specifies how often (in seconds) statistics monitoring data is written to the monitoring queue.

To create a Take Action command to start a queue manager, select **System Command** in step 6 and enter `STRMQM (QMgr)` in step 7, where *QMGr* is the name of the queue manager that you want to start.

For information about how to issue a Take Action command, see “Sending a Take Action command.”

---

## Sending a Take Action command

You can use the take action feature to issue a command on a managed system in your monitored enterprise.

Make sure that the user ID to issue a Take Action command and the user ID to issue the WebSphere MQ command match the agent configuration, otherwise the command cannot be executed successfully.

The **ACTIONAUTHUSERS** parameter in the **SET GROUP** (or **SET MANAGER**) statement determines the user IDs that have the authority to issue Take Action commands. The **ACTIONACCOUNT** parameter determines the user ID that is used by the agent to interact with WebSphere MQ. For details of these two parameters, see “SET GROUP” on page 26 or “SET MANAGER” on page 29.

Do the following steps to send a Take Action command from the Tivoli Enterprise Portal to systems in your managed enterprise:

1. Select the Navigator item that is associated with the component or application on which you want to run the command.
2. Right-click the Navigator, or right-click a row in a table view or a bar in a bar chart.
3. Click **Take Action > Select**. The Take Action window is displayed.
4. In the **Name** field, click the arrow to display the list.
5. Select the command that you want to run from the **Name** list. The command is displayed in the field below.
6. For the commands that require argument values, enter or edit the values as needed:
  - If the Edit Argument Values window opens, enter a value to identify the item on which you want to run the selected commands, and click **OK**.
  - If the values are filled automatically and you want to change those values, click the **Arguments** button, edit the argument values, and click **OK**.
7. Click the host system in the **Destination Systems** field where the component is located and click **OK**.

---

## Using Take Action commands in situations

You can use Take Action commands in situations that you create. The *reflex automation* term refers to a situation that issues a command.

To issue a command from a situation, enter the MQ: syntax form of the command on the Action tab of the Situation Editor. Figure 10 on page 62 shows an example of the **MQ Start Channel** command used in a situation.

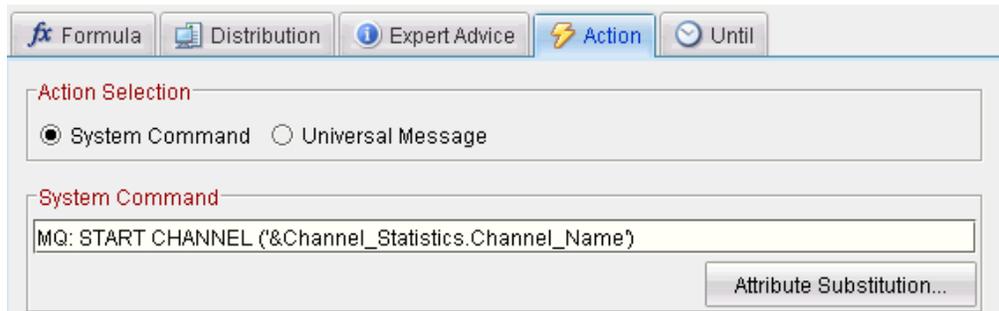


Figure 10. A Take Action command used in a situation

This example is from the MQ\_Automation\_ChStart predefined situation, which substitutes an attribute from the Channel Performance workspace. The **Attribute Substitution** button, visible in Figure 10, is used to select the attribute (this prevents misspellings and inserts the ampersand character (&), which is needed for attribute substitution). The single quotation marks enclosing the command parameter are required. When you are using a Take Action command in a situation, create a working, manual version of the Take Action command before you attempt to automate its use by adding it to a situation. For instructions, see “Creating a custom Take Action command” on page 60.

**Remember:**

The **ACTIONAUTHUSERS** parameter in the **SET GROUP** (or **SET MANAGER**) statement determines the user IDs that have the authority to issue Take Action commands. The **ACTIONACCOUNT** parameter determines the user ID that is used by the agent to interact with WebSphere MQ. Make sure that the user ID to issue a Take Action command and the user ID to issue the WebSphere MQ command match the agent configuration, otherwise the command cannot be executed successfully. For details of these two parameters, see “SET GROUP” on page 26 or “SET MANAGER” on page 29.

---

## Chapter 4. Data collection for workspaces

Workspaces of the WebSphere MQ Monitoring agent present information about various aspects of your WebSphere MQ environment. The table views and graphs in each workspace report attribute information that you are monitoring. By default, most workspaces display correct data with the default configuration; however, some columns in the following workspaces might contain no data or incorrect data if you use the default configuration.

For information about how to collect data for these workspaces, read the following sections:

- Application Accounting workspace
- Application Debugging workspace
- Application Statistics workspaces
- Buffer Pool Statistics workspaces
- Channel Performance and Channel Status workspace
- Channel related workspaces
- Event Log workspace
- Queue Accounting workspace
- Queue Statistics workspace and Queue Statistics workspace on z/OS systems
- Queue Status workspace
- Log Manager workspaces
- Message Manager workspaces
- MQSeries Events workspace
- MQI Statistics workspace
- MQ Queue Statistics workspace
- MQ Channel Statistics workspace
- Queue related workspaces
- Topic Manager workspaces
- Historical workspaces

---

### Collecting data for the Application Accounting workspace

Data in the Application Accounting workspace is retrieved from the accounting messages in a system queue of the queue manager. For this workspace to display correct data, you must configure the queue manager and the WebSphere MQ Monitoring agent.

You must have the required authorities for the **ALTER QMGR** command.

Do the following steps to collect data for the Application Accounting workspace:

1. Configure the queue manager to collect application accounting information by doing one of the following steps:
  - Run the following MQSC command:  
`ALTER QMGR ACCTMQI(ON)`
  - Send the command for collecting application accounting information to the queue manager by using the Take Action command. See “Sending a Take

- Action command” on page 61 for information about how to send a Take Action command to a managed system.
2. Set the interval over which the accounting data is collected in the queue manager by doing one of the following steps:
    - Run the following MQSC command:  

```
ALTER QMGR ACCTINT(n)
```

where *n* is the number of seconds over which the accounting data is collected in the queue manager.
    - Send the command for setting the interval over which the accounting data is collected to the queue manager by using the Take Action command. For information about how to send a Take Action command to a managed system, see “Sending a Take Action command” on page 61.
  3. Optional: Edit the monitoring file of the WebSphere MQ Monitoring agent to allow it to read messages from the system statistics queues. The **ACCOUNTINGINFO** attribute specifies how the WebSphere MQ Monitoring agent accesses the data that is produced by the queue manager. It is set to REMOVE by default. You can set it to BROWSE to suit the requirements of your environment. See “Changing monitoring options” on page 14 for information about how to change monitoring options.
  4. If you changed the monitoring file of the WebSphere MQ Monitoring agent, restart the agent for the changes to take effect.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the Application Debugging workspace

The Application Debugging workspace can help you debug your WebSphere MQ applications by providing debugging trace data. Data for the workspace is available only if application debug trace is collected on z/OS systems.

Do the following steps to configure the WebSphere MQ Monitoring agent to collect data for this workspace:

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on your operating system.
2. Set the TRACE monitoring option of the SET APPL statement in the monitoring file to YES to collect application trace information for applications that are specified by the SET APPL statement. See “SET APPL (z/OS systems only)” on page 51 for information about how to use the SET APPL statement.
3. Use the SET MQIMONITOR statement to activate monitoring for the applications that you specified in the SET APPL statement. See “SET MQIMONITOR (z/OS systems only)” on page 53 for information about how to use the SET MQIMONITOR statement.
4. Restart the agent for the changes to take effect.

**Remember:** You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the Application Statistics workspaces

The Application Statistics workspaces provide statistics about WebSphere MQ applications that are running on z/OS systems. Data for these workspaces is available only if application statistics are being collected on z/OS systems.

Do the following steps to configure the WebSphere MQ Monitoring agent to collect data for these workspaces:

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on your operating system.
2. Use the SET APPL statement to collect the application statistics information and specify for which applications and which queues the application statistics information is collected. See “SET APPL (z/OS systems only)” on page 51 for information about how to use the SET APPL statement.

**Tip:** By default, all application statistics are collected for predefined queues. To change the default or add more specific SET APPL statements, you can manually tailor the KMQUSER Member.

3. Use the SET MQIMONITOR statement to activate monitoring for the applications that you specify in the SET APPL statement. See “SET MQIMONITOR (z/OS systems only)” on page 53 for information about how to use the SET MQIMONITOR statement.
4. Restart the agent for the changes to take effect.

**Remember:** You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the Buffer Pool Statistics workspaces

The Buffer Pool Statistics workspaces display current buffer manager performance information for all monitored queue managers on a z/OS system. Data in these workspaces are collected from WebSphere MQ performance statistics that are written as SMF (System Management Facility) type 115 records. You can use SMF to collect data for these workspaces.

SMF must be running before you can send data to it. For more information about SMF, see the *MVS System Management Facilities (SMF)* manual.

Do the following steps to collect data for the Buffer Pool Statistics workspaces:

1. Use SMF to collect data for monitored queue managers. To record performance statistics (record type 115) to SMF, specify the following in the SMFPRMxx member of SYS1.PARMLIB:  
SYS(TYPE(115))

You can also use the **SETSMF** z/OS operator command for this.

2. Ensure that SMF is running.
3. Specify YES on the SMFSTAT (SMF STATISTICS) parameter of the CSQ6SYSP macro to customize the monitored queue managers.
4. Optional: Specify the interval at which statistics records are produced by setting the STATIME parameter of the CSQ6SYSP macro. If you set the STATIME parameter to zero, statistics records are produced at the SMF global accounting interval.

5. Restart the queue managers for the changes to take effect.

---

## Collecting data for the Channel Performance and Channel Status workspace

By default, the values of some columns in the Channel Performance and Channel Status workspace are n/a or blank. If you want the values that are produced by the queue manager for real-time channel monitoring to be displayed in these workspaces, you must enable real-time monitoring for the channel at the queue manager.

You must have the required authorities for the MQSC commands.

Depending on the value of the MONCHL attribute of the channel, do one of the following things:

- If the value is OFF, change its value to LOW, MEDIUM, or HIGH by running the following MQSC command:

```
ALTER CHANNEL(channel_name) MONCHL(collection_level)
```

Where *channel\_name* is the name of the channel and *collection\_level* specifies the collection level of monitoring data for the channel. Here you can set it to LOW, MEDIUM, or HIGH to suit the requirement of your environment.

- If the value is QMGR, change the MONCHL attribute of its queue manager to LOW, MEDIUM, or HIGH by running the following MQSC command:

```
ALTER QMGR MONCHL(collection_level)
```

Where *collection\_level* specifies the collection level of monitoring data for the channels on the queue manager whose MONCHL attribute is set to QMGR. Here you can set it to LOW, MEDIUM, or HIGH to suit the requirement of your environment.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for channel related workspaces

By default, some channel related workspaces are configured to monitor all channels on the monitored queue manager. If you want these workspaces to display data for channels with specific channel names, you must configure the WebSphere MQ Monitoring agent.

Make sure that you understand how to edit the agent monitoring file to suit the needs of your environment.

By default, the following channel related workspaces are configured to monitor all channels on the monitored queue manager:

- Channel Definitions
- Channel Definitions for Sender Type
- Channel Definitions for Server Type
- Channel Definitions for Receiver Type
- Channel Definitions for Requester Type
- Channel Definitions for Client Connection Type
- Channel Definitions for Server Connection Type
- Channel Definitions for Cluster Receiver Type

- Channel Definitions for Cluster Sender Type
- Channel Performance
- Channel Performance by Type/Status
- Channel Performance for Current Channels
- Channel Performance for Transmitting Channels
- Channel Performance for Channels with XmitQ Depth
- Channel Performance for In-Doubt Channels
- Channel Summary

For these workspaces to display data for channels with specific channel names, configure the WebSphere MQ Monitoring agent as follows:

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on your operating system.
2. Set the NAME monitoring option of the SET CHANNEL command in the monitoring file to a 1- through 20-character specific or generic name of the channels that you want to monitor. To specify a generic name, enter a character string followed by an asterisk (\*).

**Remember:** This option does not affect workspaces that contain on-demand data. For example, the Real-time Channel Definitions workspace displays information that is related to all queues regardless of this attribute.

For example, the following command sets the NAME monitoring option to monitor all the channels on the queue manager QMGR that match the generic name "MARCH\*":

```
SET CHANNEL NAME(MARCH*) MGRNAME(QMGR)
```

---

## Collecting data for the Event Log workspace

With the default queue manager configuration, several types of events are not monitored and displayed in the Event Log workspace. You must first enable the queue manager to emit the related events, so that these events can be displayed in the Event Log workspace.

You must have the required authorities for the **ALTER QMGR** commands.

The following types of events are not monitored and displayed in the Event Log workspace with the default queue manager configuration:

- Authority events
- Channel events
- Command events
- Configuration events
- IMS Bridge events
- Inhibit events
- Local events
- Logger events
- Performance events
- Remote events
- SSL events

- Start and Stop events

Depending on the events that you want to be displayed in the Event Log workspace, run one or more of the following commands:

- To enable the queue manager to emit authority events, run the following command:  
ALTER QMGR AUTHOREV(ENABLED)
- To enable the queue manager to emit channel events, run the following command:  
ALTER QMGR CHLEV(ENABLED)
- To enable the queue manager to emit command events, run the following command:  
ALTER QMGR CMDEV(ENABLED)
- To enable the queue manager to emit configuration events, run the following command:  
ALTER QMGR CONFIGEV(ENABLED)
- To enable the queue manager to emit IMS Bridge events, run the following command:  
ALTER QMGR BRIDGEV(ENABLED)
- To enable the queue manager to emit local events, run the following command:  
ALTER QMGR LOCALEV(ENABLED)
- To enable the queue manager to emit logger events, run the following command:  
ALTER QMGR LOGGERSV(ENABLED)
- To enable the queue manager to emit performance events, run the following command:  
ALTER QMGR PERFMV(ENABLED)
- To enable the queue manager to emit remote events, run the following command:  
ALTER QMGR REMOTESV(ENABLED)
- To enable the queue manager to emit SSL events, run the following command:  
ALTER QMGR SSLEV(ENABLED)
- To enable the queue manager to emit start and stop events, run the following command:  
ALTER QMGR STRSTPEV(ENABLED)

You do not need to restart the queue manager for the changes to take effect.

---

## Collecting data for the Queue Accounting workspace

Data in the Queue Accounting workspace is retrieved from the accounting messages in a system queue of the queue manager. For the workspace to display correct data, you must configure the queue manager and the WebSphere MQ Monitoring agent.

You must have the required authorities for the MQSC commands.

Do the following steps to collect data for the Queue Accounting workspace:

1. Configure the queue manager to collect queue accounting information by doing one of the following steps:
  - Run the following MQSC command:  
ALTER QMGR ACCTQ(ON)

- Send the command for configuring the queue manager to collect queue accounting information by using the Take Action command. See “Sending a Take Action command” on page 61 for information about how to send a Take Action command to a managed system.
2. Set the interval over which the accounting data is collected in the queue manager by doing one of the following steps:
    - Run the following MQSC command:
 

```
ALTER QMGR ACCTINT(n)
```

where *n* is the number of seconds over which the accounting data is collected in the queue manager.
    - Send the command for setting the interval over which the accounting data is collected to the queue manager by using the Take Action command. For information about how to send a Take Action command to a managed system, see “Sending a Take Action command” on page 61.
  3. If necessary, enable accounting information collection for the queues for which you want accounting data by doing one of the following steps:
    - Run the following MQSC command:
 

```
ALTER QLOCAL(queue_name) ACCTQ(QMGR)
```

where *queue\_name* is the name of the queue for which you want to enable accounting information collection. You can also specify a generic name by entering a character string that is followed by an asterisk (\*).
    - Send the command to enable accounting information collection for the queues by using the Take Action command. For information about how to send a Take Action command to a managed system, see “Sending a Take Action command” on page 61.
  4. Optional: Edit the monitoring file of the WebSphere MQ Monitoring agent to allow it to read messages from the system statistics queues. The **ACCOUNTINGINFO** attribute specifies how the WebSphere MQ Monitoring agent accesses the data that is produced by the queue manager. It is set to REMOVE by default. You can set it to BROWSE to suit the requirements of your environment. For information about how to change monitoring options, see “Changing monitoring options” on page 14.
  5. If you changed the monitoring file of the WebSphere MQ Monitoring agent, restart the agent for the changes to take effect.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the Queue Statistics workspace

By default, if the WebSphere MQ Monitoring agent is running on a distributed system, several columns of the Queue Statistics workspace display zero. You must configure the WebSphere MQ Monitoring agent to collect the data that is displayed in these columns.

Before you make any changes to the monitoring file, read Chapter 7, “Collecting queue statistics data,” on page 95.

Perform this procedure to configure WebSphere MQ Monitoring agent to collect data for the following columns in the Queue Statistics workspace:

- Highest Depth
- Messages Put

- Messages Put per Sec
  - Messages Read
  - Messages Read per Sec
  - Time to Full Queue (Secs)
  - Time to Zero Msgs (Secs)
1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on your operating system.
  2. Set the STATISTICS monitoring option of the SET QUEUE command in the monitoring file to YES. For example, the following command sets the STATISTICS monitoring option for all queues on the queue manager QMGR to YES:
 

```
SET QUEUE NAME(*) MGRNAME(QMGR) QDEFTYPE(PREDEFINED) STATISTICS(YES)
```
  3. Restart the agent for the changes to take effect.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the Queue Statistics workspace on z/OS systems

By default, if the WebSphere MQ Monitoring agent is running on a z/OS system, several columns of the Queue Statistics workspace display zero. You must configure the WebSphere MQ Monitoring agent to collect the data that is displayed in these columns.

Before you make any changes to the monitoring file, read Chapter 7, “Collecting queue statistics data,” on page 95.

Perform this procedure to configure WebSphere MQ Monitoring agent to collect data for the following columns in the Queue Statistics workspace for a z/OS system:

- Average MQ Response Time
- Average Application Time Between Calls
- Input Message Size Average
- Messages Put
- Messages Read
- Messages Browsed
- Number of Transaction/Programs
- Output Message Size Average

Some of these columns are the same as the columns that are described in “Collecting data for the Queue Statistics workspace” on page 69. If you enable both ways on a z/OS system, the Queue Statistics data that are enabled in the “Collecting data for the Queue Statistics workspace” on page 69 section are used for these columns.

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on your operating system.
2. Use the SET MQIMONITOR statement with the SET APPL statement to activate the application debugging and application statistics functions. See “SET APPL

(z/OS systems only)” on page 51 and “SET MQIMONITOR (z/OS systems only)” on page 53 for information about how to use the SET APPL and SET MQIMONITOR statement.

3. Restart the agent for the changes to take effect.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the Queue Status workspace

By default, the values of some columns in the Queue Status workspace are n/a or blank. To ensure that the data that is displayed in the Queue Status workspace is complete and accurate, you must enable real-time monitoring for the queue.

You must have the required authorities for the MQSC commands.

Do the following steps to enable real-time monitoring for one or multiple queues so that the Queue Status workspace displays complete and accurate data:

1. Display the value of the MQNQ attribute of the queue or queues by doing one of the following steps:

- Run the following MQSC command:

```
DISPLAY QLOCAL(queue_name) MONQ
```

where *queue\_name* is the name of the queue. You can also specify a generic name by entering a character string that is followed by an asterisk (\*).

- Send the command for displaying the value of the MQNQ attribute of a queue by using the Take Action command. For information about how to send a Take Action command to a managed system, see “Sending a Take Action command” on page 61.
2. Depending on the value of the MONQ attribute of the queue, do one of the following things:
    - If the value is OFF, change its value to LOW, MEDIUM, or HIGH by running the following MQSC command:

```
ALTER QLOCAL(queue_name) MONQ(collection_level)
```
- where *queue\_name* is the name of the queue and *collection\_level* specifies the collection level of monitoring data for the queue. You can set it to LOW, MEDIUM, or HIGH to suit the requirements of your environment.
- If the value is QMGR, change the MONQ attribute of the queue manager to LOW, MEDIUM, or HIGH by running the following MQSC command:

```
ALTER QMGR MONQ(collection_level)
```

where *collection\_level* specifies the collection level of monitoring data for the queues whose MONQ attribute is set to QMGR. You can set it to LOW, MEDIUM, or HIGH to suit the requirements of your environment.

You do not have to restart the queue manager for these changes to take effect.

---

## Collecting data for the Log Manager workspaces

The Log Manager workspaces provide information about the logging activity (such as I/O levels and the number of times that a WebSphere MQ application is delayed because no logging buffers are available) for each monitored queue manager on a z/OS system. Data in these workspaces are collected from

WebSphere MQ performance statistics that are written as SMF (System Management Facility) type 115 records. You can use SMF to collect data for these workspaces.

SMF must be running before you can send data to it. For more information about SMF, see the *MVS System Management Facilities (SMF)* manual.

Do the following steps to collect data for the Log Manager workspaces:

1. Use SMF to collect data for monitored queue managers. To record performance statistics (record type 115) to SMF, specify the following in the SMFPRMxx member of SYS1.PARMLIB:  
SYS(TYPE(115))

You can also use the **SETSMF** z/OS operator command.

2. Ensure that SMF is running.
3. Specify YES for the SMFSTAT (SMF STATISTICS) parameter of the CSQ6SYSP macro to customize the monitored queue managers.
4. Optional: Specify the interval at which statistics records are produced by setting the STATIME parameter of the CSQ6SYSP macro. If you set the STATIME parameter to zero, statistics records are produced at the SMF global accounting interval.
5. Restart the queue managers for the changes to take effect.

---

## Collecting data for the Message Manager workspaces

The Message Manager workspaces provide information about how frequently calls to the WebSphere MQ application programming interface (API) are made on a z/OS system. Data in these workspaces are collected from WebSphere MQ performance statistics that are written as SMF type 115 records. You can use SMF to collect data for these workspaces.

SMF must be running before you can send data to it. For more information about SMF, see the *MVS System Management Facilities (SMF)* manual.

Do the following steps to collect data for the Message Manager workspaces:

1. Use SMF to collect data for monitored queue managers. To record performance statistics (record type 115) to SMF, specify the following in the SMFPRMxx member of SYS1.PARMLIB:  
SYS(TYPE(115))

You can also use the **SETSMF** z/OS operator command for this.

2. Ensure that SMF is running.
3. Specify YES for the SMFSTAT (SMF STATISTICS) parameter of the CSQ6SYSP macro to customize the monitored queue managers.
4. Optional: Specify the interval at which statistics records are produced by setting the STATIME parameter of the CSQ6SYSP macro. If you set the STATIME parameter to zero, statistics records are produced at the SMF global accounting interval.
5. Restart the queue managers for the changes to take effect.

---

## Collecting data for the MQSeries Events workspace

By default, the MQSeries® Events workspace does not display events such as the Queue Full, Queue Depth High, Queue Service Interval High, Bridge Stopped, Channel Stopped, and Channel Not Activated event with the default configuration of a queue manager. If you want to use event monitoring, you must configure the queue manager to emit the events.

You must have the required authorities for the **ALTER QMGR** and **ALTER QLOCAL** commands.

Different commands are required depending on what type of event data you want.

- To enable channel and bridge events so that they are displayed in the MQSeries Events workspace, run the following MQSC commands:

```
ALTER QMGR CHLEV(ENABLED)
ALTER QMGR BRIDGEEV(ENABLED)
```

- To enable Queue Service Interval High events with a service interval time of 10 seconds (10 000 milliseconds), run the following MQSC commands:

```
ALTER QMGR PERFMEV(ENABLED)
ALTER QLOCAL('queue_name') QSVCI(10000) QSVCI(HIGH)
```

where *queue\_name* is the name of the queue.

- To enable Queue Depth High events on a specific queue, run the following MQSC commands:

```
ALTER QMGR PERFMEV(ENABLED)
ALTER QLOCAL('queue_name') QDPHIEV(ENABLED)
```

- To enable Queue Depth Low events on a specific queue, run the following MQSC commands:

```
ALTER QMGR PERFMEV(ENABLED)
ALTER QLOCAL('queue_name') QDPLOEV(ENABLED)
```

- To enable Queue Depth Full events on a specific queue, run the following MQSC commands:

```
ALTER QMGR PERFMEV(ENABLED)
ALTER QLOCAL('queue_name') QDPMAEV(ENABLED)
```

---

## Collecting data for the MQI Statistics workspace

Data in the MQI Statistics workspace is retrieved from the statistics messages in a system queue of the queue manager. To display correct data, you must configure the queue manager and the WebSphere MQ Monitoring agent for the workspace.

You must have the required authorities for the **ALTER QMGR** command.

Do the following steps to collect data for the MQI Statistics workspace:

1. Configure the queue manager to collect MQI statistics information by doing one of the following steps:

- Run the following MQSC command to configure the queue manager:

```
ALTER QMGR STATMQI(ON)
```

- Send the command for collecting MQI statistics information by using the Take Action command. See “Sending a Take Action command” on page 61 for information about how to send a Take Action command to a managed system.

2. Set the interval over which the statistics information is collected by doing one of the following steps:
  - Run the following MQSC command:
 

```
ALTER QMGR STATINT(n)
```

where *n* is the number of seconds over which the statistics information is collected.
  - Send the command for setting the interval to the queue manager by using the Take Action command.
3. Optional: Edit the monitoring file of the WebSphere MQ Monitoring agent to allow it to read messages from the system statistics queues. The STATISTICSINFO attribute specifies how the WebSphere MQ Monitoring agent accesses the data that is produced by the queue manager. It is set to REMOVE by default. You can set it to BROWSE to suit the requirements of your environment. For information about how to change monitoring options, see “Changing monitoring options” on page 14.
4. If you changed the monitoring file of the WebSphere MQ Monitoring agent, restart the agent for the changes to take effect.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the MQ Channel Statistics workspace

Data in the MQ Channel Statistics workspace is retrieved from the statistics messages in a system queue of the queue manager. To display correct data, you must configure the queue manager and the WebSphere MQ Monitoring agent for the workspace.

You must have the required authorities for the MQSC commands.

Do the following steps to collect data for the MQ Channel Statistics workspace.

**Important:** The commands in the following instructions set the level of statistics that is produced at the queue manager level. You can also set that level at the individual channel level. For detailed commands about how to set the level of statistics that is produced at the channel level, see the WebSphere MQ documentation.

1. Configure the queue manager to collect channel statistics information by doing one of the following steps:
  - Run the following MQSC command:
 

```
ALTER QMGR STATCHL(collection_level)
```

where *collection\_level* is the collection level of channel statistics information. You can set it to LOW, MEDIUM, or HIGH to suit the requirements of your environment.
  - Send the command for configuring the queue manager to collect channel statistics information by using the Take Action command. For information about how to send a Take Action command to a managed system, see “Sending a Take Action command” on page 61.
2. Set the interval over which the accounting data is collected by doing one of the following steps:
  - Run the following MQSC command:
 

```
ALTER QMGR STATINT(n)
```

where  $n$  is the number of seconds over which the accounting data is collected.

- Send the command for setting the interval by using the Take Action command.
3. Enable the statistics information collection for the channels for which you want to collect statistics information by doing one of the following steps:
    - Run the following MQSC command:  
`ALTER CHANNEL(channel_name) STATCHL(QMGR)`
- where *channel\_name* is the name of the channel for which you want to collect statistics information. You can also specify a generic name by entering a character string that is followed by an asterisk (\*).
- Send the command for enabling statistics information collection for the channels by using the Take Action command.
4. Optional: Edit the monitoring file of the WebSphere MQ Monitoring agent to allow it to read messages from the system statistics queues. The STATISTICSINFO attribute specifies how the WebSphere MQ Monitoring agent accesses the data that is produced by the queue manager. It is set to REMOVE by default. You can set it to BROWSE to suit the requirements of your environment. See “Changing monitoring options” on page 14 for information about how to change monitoring options.
  5. If you changed the monitoring file of the WebSphere MQ Monitoring agent, restart the agent for the changes to take effect.

You do not need to restart the queue manager for these changes to take effect.

---

## Collecting data for the MQ Queue Statistics workspace

Data in the MQ Queue Statistics workspace is retrieved from the statistics messages in a system queue of the queue manager. To display correct data, you must configure the queue manager and the WebSphere MQ Monitoring agent for the workspace.

You must have the required authorities for the MQSC commands.

Do the following steps to collect data for the MQ Queue Statistics workspace.

**Important:** The commands in the following instructions set the level of statistics that is produced at the queue manager level. You can also set that level at the individual queue level. For detailed commands about how to set the level of statistics that is produced at the queue level, see the WebSphere MQ documentation.

1. Configure the queue manager to collect queue statistics information by doing one of the following steps:
  - Run the following MQSC command:  
`ALTER QMGR STATQ(ON)`
  - Send the command for configuring the queue manager to collect queue statistics information by using the Take Action command. For information about how to send a Take Action command to a managed system, see “Sending a Take Action command” on page 61.
2. Set the interval over which the accounting data is collected by doing one of the following steps:
  - Run the following MQSC command:

```
ALTER QMGR STATINT(n)
```

where *n* is the number of seconds over which the accounting data is collected.

- Send the command for setting the interval by using the Take Action command.
3. Enable statistics information collection for the queues for which you want to collect statistics information by running the following MQSC command:  

```
ALTER QLOCAL(queue_name) STATQ(QMGR)
```

where (*queue\_name*) is the name of the queue for which you want to collect statistics information. You can also specify a generic name by entering a character string that is followed by an asterisk (\*).

4. Edit the monitoring file of the WebSphere MQ Monitoring agent to allow it to read messages from the system statistics queues. The STATISTICSINFO attribute specifies how the WebSphere MQ Monitoring agent accesses the data that is produced by the queue manager. Here you can set it to REMOVE or BROWSE to suit the requirements of your environment. For information about how to change monitoring options, see “Changing monitoring options” on page 14.
5. If you changed the monitoring file of the WebSphere MQ Monitoring agent, restart the agent for the changes to take effect.

You do not have to restart the queue manager for these changes to take effect.

---

## Collecting data for queue related workspaces

By default, some queue related workspaces are configured to display data about all predefined queues on the monitored queue manager. You can configure the WebSphere MQ Monitoring agent, so that these workspaces can display data for queues of other types and with specific queue name.

Make sure that you understand how to edit the agent monitoring file to suit the needs of your environment.

Configure the agent for the following queue related workspaces to display data for queues of other types and with specific queue names:

- Queue Definitions
- Queue Statistics
- Queue Statistics for Monitored Queues with Messages
- Queue Statistics for Monitored Open Queues
- Queue Statistics for Monitored Transmission Queues

**Remember:** The QDEFTYPE and NAME monitoring options in the following procedure do not affect workspaces that contain on-demand data. For example, the Real-time Queue Definitions and Real-time Queue Data workspaces display information that is related to all queues regardless of the values that you set to the two options.

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on your operating system.
2. Set the QDEFTYPE monitoring option of the SET QUEUE command in the monitoring file to one of following values:

- **PREDEFINED:** Monitor only predefined queues that match the specific or generic queue name. This is the default value.
  - **PERMDYN:** Monitor only permanent dynamic queues that match the specific or generic queue name.
  - **TEMPDYN:** Monitor only temporary dynamic queues that match the specific or generic queue name.
  - **ALL:** Monitor all queues that match the specific or generic queue name.
3. Set the NAME monitoring option of the SET QUEUE command in the monitoring file to a 1- through 48-character specific or generic name of the queues that you want to monitor. To specify a generic name, enter a character string followed by an asterisk (\*).

For example, the following command sets the QDEFTYPE monitoring option to monitor all the queues on the queue manager QMGR that match the generic name "MARCH\*" in NAME option:

```
SET QUEUE NAME(MARCH*) MGRNAME(QMGR) QDEFTYPE(ALL)
```

---

## Collecting data for the Topic Manager workspaces

The Topic Manager workspaces provide information about the publication and subscription activities (such as how frequently subscriptions are made and how many subscriptions have expired ) for each monitored z/OS system queue manager. Data in these workspaces are collected from WebSphere MQ performance statistics written as SMF(System Management Facility) type 115 records. You can use SMF to collect data for these workspaces.

SMF must be running before you can send data to it. For more information about SMF, see the *MVS System Management Facilities (SMF)* manual.

Do the following steps to collect data for the Topic Manager workspaces:

1. Use SMF to collect data for monitored queue managers. To record performance statistics (record type 115) to SMF, specify the following in the SMFPRMxx member of SYS1.PARMLIB:  
SYS(TYPE(115))

You can also use the **SETSMF** z/OS operator command for this.

2. Ensure that SMF is running.
3. Specify YES on the SMFSTAT (SMF STATISTICS) parameter of the CSQ6SYSP macro to customize the monitored queue managers.
4. Optional: Specify the interval at which statistics records are produced by setting the STATIME parameter of the CSQ6SYSP macro. If you set the STATIME parameter to zero, statistics records are produced at the SMF global accounting interval.
5. Restart the queue managers for the changes to take effect.



---

## Chapter 5. Collecting historical data

In addition to the real-time reports that are provided by Tivoli Enterprise Portal workspaces, you can set up historical data collection to store and save WebSphere MQ Monitoring agent data. You can specify the following items:

- Attribute groups for historical data collection
- Data collection intervals
- Data warehousing interval (if you choose to write your data to a data warehouse)
- Storage time of the collected data
- Type of the reports that are generated from the data
- Storage location for the collected data (Historical data can be stored either at the location of the monitoring agent or on the Tivoli Enterprise Monitoring Server.)

To ensure that data samplings are saved to populate your predefined historical workspaces, you must first configure and start historical data collection. This requirement does not apply to workspaces that use attribute groups that are historical in nature and display all their entries without your starting data collection separately.

**Important:** Historical data collection requires additional disk space. You should ensure that there is enough space on the computer when configuring historical data collection, otherwise there is no data displayed in the related workspaces. The attribute history tables, default file names, default tables collected, and the estimated disk space required per 24-hour period for the historical data collected for WebSphere MQ Monitoring agent are listed in Appendix E, “Disk space requirements for historical data tables,” on page 185.

**Remember:** If you choose to collect historical data for the Error Log attribute group, check the Error Log workspace periodically and take immediate actions to fix the errors that are displayed in this workspace, otherwise, the short-term historical file for Error Log grows rapidly and occupies a large amount of your disk space, which might eventually cause the agent to become offline.

There are several tables containing historical data, some contain sampled data and some contain real-time on-demand data. Some sampled and on-demand tables contain similar attributes. If you enable historical data collection for both sampled and on-demand tables, this increases the historical data collection overhead unnecessarily. Instead, select one table depending on whether you want sampled or on-demand data to be displayed in historical workspaces.

For more information about which tables contain sampled data and which are on-demand, see “Sampled and on-demand tables” on page 173

---

### Enabling historical data collection

To view historical data for attribute groups whose data is sampled by the agent, you must first enable historical data collection by editing the configuration file of the WebSphere MQ Monitoring agent.

## Enabling historical data collection on Windows systems

On Windows systems, do the following steps to enable historical data collection for attribute groups whose data are sampled by the agent:

1. Open the Manage Tivoli Enterprise Monitoring Services window.
2. Right-click the agent for which you want to enable historical data collection.
3. Click **Reconfigure**.
4. Click **OK** on both of the two configuration windows that are displayed.
5. Click **Yes** when asked whether you want to edit the configuration file. The file opens in the default text editor. A window containing a message that indicates that configuration waits until you close the text editor is also displayed.
6. Click **OK**.
7. Look for the **HISTORY** parameter in the configuration file; the parameter is followed by either a YES or NO value enclosed in brackets. If the value is NO, change it to YES. The resulting line in the configuration file is displayed similarly to the following statement:  

```
PERFORM STARTMON SAMPINT(300) HISTORY(YES)
```
8. Optional: You can change the value of the **SAMPINT** parameter to specify the frequency with which historical data is sampled (in seconds). However, the more frequently data is sampled, the greater the performance overhead of collecting historical data.
9. Save and close the file.
10. Click **Yes** when asked whether you want to perform configuration. Historical data collection is now enabled.

For information about configuring historical data collection on z/OS systems, see *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide*.

**Important:** You must ensure that the date and time of the operating systems on all systems running monitoring agent, Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are synchronized, otherwise no historical data is displayed in historical workspaces.

## Enabling historical data collection on UNIX and Linux systems

On UNIX and Linux systems, do the following steps to enable historical data collection for attribute groups whose data are sampled by the agent:

1. Navigate to the following directory:  

```
install_dir/config
```

where *install\_dir* is the IBM Tivoli Monitoring installation directory. The default directory is /opt/IBM/ITM.
2. Open the configuration file of the agent for which you want to enable historical data collection.
3. Look for the **HISTORY** parameter in the configuration file; the parameter is followed by either a YES or NO value enclosed in brackets. If the value is NO, change it to YES. The resulting line in the configuration file is displayed similarly to the following statement:  

```
PERFORM STARTMON SAMPINT(300) HISTORY(YES)
```
4. Optional: You can change the value of the **SAMPINT** parameter to specify the frequency with which historical data is sampled (in seconds). However, the more frequently data is sampled, the greater the performance overhead of collecting historical data.

5. Save and close the file.

For information about configuring historical data collection on z/OS systems, see *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide*.

**Important:** You must ensure that the date and time of the operating systems on all systems running monitoring agent, Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are synchronized, otherwise no historical data is displayed in historical workspaces.

## Enabling historical data collection on i5/OS systems

On i5/OS systems, do the following steps to enable historical data collection for attribute groups whose data are sampled by the agent:

1. At the i5/OS command line, enter the following command:

```
WRKOMAMQ
```

The main dialog box for working with the WebSphere MQ Monitoring agent is displayed as follows:

```
Work with Tivoli Monitoring Agent for WebSphere MQ System MYSYSTEM
Type Option, press Enter
  2=Change, 4=Delete, 5=Display monitoring agent Log, 14=Start, 15=End
```

Option	Agent for MQ Manager...	Suffix	Status
	MYSYSTEM	00001	Not Started
	MQITMISDE1	00002	Started

Multiple instances of the WebSphere MQ Monitoring agent might be listed in this window. These can be distinguished by their unique 5-character numeric suffix. The first instance of the agent that is installed is automatically assigned the suffix 00001, the second is assigned suffix 00002, and so on. The files that are associated with each instance have corresponding suffixes. The monitoring file for each instance is named in the form: MQnmmmm, where nmmmm is the 5-character numeric suffix.

2. In the Option column next to the monitoring file that you want to change, enter 2 (change). The panel for changing the WebSphere MQ Monitoring agent is displayed.
3. Press F8 to change the monitoring file associated with the agent. A file editing panel is displayed.
4. In the configuration file, look for the **HISTORY** parameter; the parameter is followed by either a YES or NO value enclosed in brackets. If the value is NO, change it to YES.
5. When you finish customizing the monitoring file, press F3 to save your changes and exit. Press F3 twice more to exit the interface.
6. Ensure that the queue manager and its command server are running.
7. Restart the agent for the changes to take effect.

**Important:** You must ensure that the date and time of the operating systems on all systems running monitoring agent, Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are synchronized, otherwise no historical data is displayed in historical workspaces.

## Enabling historical data collection on z/OS systems

On z/OS systems, use the `KMQ_HISTCOLL_DATA_FLAG` parameter to control historical data collection with PARMGEN.

For information about configuring historical data collection on z/OS systems, see *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide* and *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Parameter Reference*.

---

### Starting historical data collection

For historical data to be available for an attribute group on one or more managed systems, you must start historical data collection for the attribute group.

Your user ID must have Configure History permission to open the History Collection Configuration window. If you do not have the permission, you will not see the menu item or tool for historical configuration.

To start collecting historical data for one or more attribute groups, do the following steps.

**Remember:** You must do this task regardless of whether the data collection type of the attribute group is sampled, on-demand, or background-collected.

1. Click **Edit > History Configuration** in the Tivoli Enterprise Portal to open the History Collection Configuration window.
2. Click **WebSphere MQ** on the left side of the window.
3. Click **Create new collection setting** at the upper left corner of the window. The Create New Collection Settings window is opened.
4. In the **Name** field, enter a name of up to 256 characters.
5. Optional: In the **Description** field, enter a description of up to 64 characters for the collection.
6. Select an attribute group from the Attribute Group list. Only attribute groups that are appropriate for historical collection and reporting are displayed in the list. See A mapping table for attribute groups and historical workspaces for a list of attribute groups that are available for historical collection.
7. Click **OK**. The configuration tabs for historical collection are displayed.
8. Complete the following fields in the **Basic** tab page:
  - **Collection Interval** is the frequency of data transmission to the short-term history file on the computer where the data is saved (Tivoli Enterprise Monitoring Agent or Tivoli Enterprise Monitoring Server). The options are every one, five, 15, or 30 minutes, every hour, or once per day. The default interval is 15 minutes. The shorter the interval is, the faster and larger the history file grows. A short interval should be used only for an attribute group that is critical in your work.
  - **Collection Location** is where the short-term history data file resides: at the TEMA (Tivoli Enterprise Monitoring Agent) or the TEMS (Tivoli Enterprise Monitoring Server). The default location is TEMA, which minimizes the performance impact on the Tivoli Enterprise Monitoring Server from historical data management.
  - **Warehouse Interval** determines whether the collected data is warehoused and how often. The options are 15 minutes, 30 minutes, 1 hour, 12 hours, 1 day or Off.

9. In the **Distribution** tab page, select the managed systems for which you want to start historical data collection from the Available Systems list and click the left arrow to move them to the **Start collection on** list.
10. Click **OK** to start historical data collection on the selected managed systems.

---

## Stopping historical data collection

Stop data collection on one or more managed systems for a historical collection definition when you are no longer interested in gathering data on the managed system or would like to temporarily disable data collection.

Your user ID must have Configure History permission to open the History Collection Configuration window. If you do not have this permission, you will not see the tool for historical configuration.

You can edit historical collection for an attribute group to stop data collection on some or all of the managed systems in the distribution list. The managed systems that remain in the distribution list continue to collect historical data. To stop historical data collection on one or more managed systems, do the following steps.

**Remember:** You must do this task regardless of whether the data collection type of the attribute group is sampled, on-demand, or background-collected.

1. Click **Edit > History Configuration** in the Tivoli Enterprise Portal to open the History Collection Configuration window.
2. Click the plus sign (+) to expand the **WebSphere MQ** branch on the left side of the window.
3. Click the collection that the managed system for which you want to stop historical data collection is assigned to.
4. Click the **Distribution** tab.
5. In the **Start collection on** list, select the managed system for which you want to stop historical data collection and click the right arrow to move it to the **Available** list.
6. To save your changes, click **Apply** to keep the window open or **OK** to close it.

Historical data collection is stopped on the managed systems that you move out of the **Start collection on** list for the historical collection definition.

---

## Viewing historical data for a selected time frame

In historical workspaces, you can choose to display only historical data that is collected over a period of time in which you are interested.

Historical data collection must be configured and distributed to the managed systems that you are querying data from.

To do view historical data for a selected time frame, do the following steps:

1. Navigate to the historical workspace for which you want to view data from a particular period of time.
2. Click the **Specify Time Span for Query** button, which is located in the top left of each view in the historical workspace. The Select the Time Span window is displayed.
3. Select the data that you want to be displayed in the table. Available options are as follows:

- **Real time**  
If you select this option, only the data that is collected during the most recent sampling period is displayed in the table.
  - **Last X hours**  
If you select this option, you can choose to display all historical data that goes back to a certain date and time. For example, all data collected over the past 24 hours.
  - **Custom**  
If you select this option, you can specify the exact period for which you want historical data to be displayed.
4. Do one of the following steps, depending on which option you have selected in the previous step.
    - If you selected the **Last X hours** option, enter the time period for which you want data to be displayed in the field provided, and select the units in which it is specified (for example, hours or days). You can also specify the following parameters:
      - **Use Detailed data**  
If you select this option, the data from the detailed data tables is displayed in the table without summarization. You can also select the column that you want to be used in determining whether data falls within the selected period from the Time column list of columns containing timestamps.
      - **Use summarized data**  
If you select this option, the data from the summarized data tables is displayed in the table. This data is aggregated by the time frame configured in the Historical Collection Configuration window. If you configured shift times when you installed IBM Tivoli Monitoring, you can also select for which shifts and days data is displayed. See your IBM Tivoli Monitoring documentation for further information.
    - If you selected the **Custom** option, you can specify the following parameters:
      - **Use Detailed data**  
If you select this option, the data from the detailed data tables is displayed in the table without summarization. You can also select the column that you want to be used in determining whether data falls within the selected period from the Time column list of columns containing timestamps.
      - **Use summarized data**  
If you select this option, the data from the summarized data tables is displayed in the table. From the Interval list, select the time period over which you want the data to be aggregated. If you configured shift times when you installed IBM Tivoli Monitoring, you can also select for which shifts and days data is displayed. See your IBM Tivoli Monitoring documentation for further information.
      - In the **Start time and End time** fields, select the time period for which you want data to be displayed.
  5. Optional: To apply the time span to all other views in this workspace that use the same query, select the **Apply to all views associated with this view's query** check box.
  6. Click **OK** to exit the Select the Time Span window.

The workspace is refreshed to reflect the time span that you selected.

---

## Tables available for historical data collection

For a complete list of tables that support historical data collection, see “Historical table record sizes” on page 187.

---

## A mapping table for attribute groups and historical workspaces

You can use the mapping table to decide which attribute group to choose when configuring historical data collection for a workspace.

You can use the following mapping table to decide which attribute group to choose when configuring historical data collection for a workspace:

*Table 3. A mapping table for attribute groups and historical workspaces*

<b>Attribute group name</b>	<b>Workspace name</b>	<b>Note</b>
Application Accounting	Historical Application Accounting workspace	distributed systems only
Application Connections	Historical Application Connections workspace	distributed and z/OS systems
Application Long-Term History	Application Statistics by ApplID workspace	z/OS systems only
Application Queue Long-Term History	Historical Tran/Pgm Statistics by Queue workspace	z/OS systems only
Application Transaction/Program Long-Term History	Historical Application Statistics by Tran/Pgm workspace	z/OS systems only
Buffer Manager Long-Term History	Historical Buffer Pool Performance workspace	z/OS systems only
Channel Data	Real-time Channel Definitions workspace	distributed and z/OS systems
Channel Definitions	Channel Definitions workspace	distributed and z/OS systems
Channel Initiator Detail	Channel Initiator Status workspace	z/OS systems only
Channel Long-Term History	Historical Channel Performance workspace	distributed and z/OS systems
Channel Status	Channel Status workspace	distributed and z/OS systems
Channel Summary	Channel Summary workspace	distributed and z/OS systems
Connection Objects	Connection Objects workspace	distributed and z/OS systems
Current Queue Manager Status	Current Queue Manager Status workspace	distributed and z/OS systems
Error Log	Error Log workspace	distributed systems only
Event Archive	Event Archive workspace	distributed and z/OS systems
Listener Status	Listener Status workspace	distributed systems only
Log Data Set Status	Log Data Set Status workspace	distributed and z/OS systems

Table 3. A mapping table for attribute groups and historical workspaces (continued)

Attribute group name	Workspace name	Note
Log Manager Long-Term History	Historical Log Manager Performance workspace	z/OS systems only
MQ Action Log	MQ Action Log workspace	distributed and z/OS systems
MQ Channel Statistics	Historical MQ Channel Statistics workspace	distributed systems only
MQ Queue Statistics	Historical MQ Queue Statistics workspace	distributed systems only
MQI Call Statistics Details	Historical MQI Call Statistics workspace	distributed systems only
MQI Message Statistics Details	Historical MQI Message Statistics workspace	distributed systems only
MQI Statistics	Historical MQI Statistics workspace	distributed systems only
Message Manager Long-Term History	Historical Message Manager Performance workspace	z/OS systems only
Message Statistics	Historical Message Statistics workspace	distributed and z/OS systems
Page Set Long-Term History	Historical Page Set Statistics workspace	z/OS systems only
QSG Channels	Queue Sharing Group Channel Statistics workspace	z/OS systems only
QSG Coupling Facility Structure Backups	Queue Sharing Group CF Structure Backup Statistics workspace	z/OS systems only
QSG Coupling Facility Structure Connections	Queue Sharing Group CF Structure Connection Statistics workspace	z/OS systems only
QSG Coupling Facility Structures	Queue Sharing Group CF Structure Statistics workspace	z/OS systems only
QSG Qmgrs	Queue Sharing Group Queue Manager Status workspace	z/OS systems only
QSG Queues	Queue Sharing Group Queue Statistics workspace	z/OS systems only
Queue Accounting	Historical Queue Accounting workspace	distributed systems only
Queue Data	Real-time Queue Data workspace	distributed and z/OS systems
Queue Definitions	Queue Definitions workspace	distributed and z/OS systems
Queue Handle Status	Open Queue Handles workspace	distributed and z/OS systems
Queue Long Term History	Historical Queue Statistics workspace	distributed and z/OS systems
Queue Status	Queue Status workspace	distributed and z/OS systems

*Table 3. A mapping table for attribute groups and historical workspaces (continued)*

<b>Attribute group name</b>	<b>Workspace name</b>	<b>Note</b>
Topic Manager Long-Term History	Historical Topic Manager Performance workspace	z/OS systems only



---

## Chapter 6. Manipulating WebSphere MQ messages

By using the message manipulation features of WebSphere MQ Monitoring agent, you can manipulate queued WebSphere MQ messages in the following ways:

- Browse the head and contents of a message
- Delete a message from a queue
- Forward a message from one queue to another
- The browse and delete messages functions that apply to messages on DLQs are accessed from the Dead-Letter Queue Messages workspace (see “Dead-Letter Queue Messages Workspaces” on page 123)
- The forward message function that applies to messages on DLQs is accessed from the Dead-Letter Queue Messages workspace (see “Dead-Letter Queue Messages Workspaces” on page 123)
- The browse and delete messages functions that apply to messages on other queues are accessed from the Queue Messages workspace (see “Queue Messages workspace” on page 148)
- The forward message function that applies to messages on other queues are accessed from the Queue Messages workspace (see “Queue Messages workspace” on page 148)

---

### Settings for controlling access to WebSphere MQ messages

Because of their potential for serious damage, there are special security considerations for message manipulation. You can specify authorization level of access to Websphere MQ messages for all user IDs or for a specific ID.

Control the level of user access to queue manager messages with the following settings:

- The **MSGACCESS** parameter (at the QMGR and GROUP levels) and **SET QACCESS** monitoring settings in the configuration file of the WebSphere MQ Monitoring agent.

These elements set restrictions on the monitoring agent. The **MSGACCESS** parameter of the **SET GROUP**, **SET MANAGER**, and **SET QACCESS** monitoring options specify the level of message access that a Tivoli Enterprise Portal user ID has to messages on queues in the specified queue managers. Use the **SET QACCESS** options to specify which user account is used for message manipulation. When the WebSphere MQ Monitoring agent performs the message manipulate operation, it uses the message manipulation account as the user account to communicate with WebSphere MQ.

- The WebSphere MQ security setting on message manipulation account.

You can set restrictions on the message manipulation account that is passed to WebSphere MQ when the monitoring agent manipulates messages. For this level of security, you must do the following operations:

- Set up WebSphere MQ security on each system where WebSphere MQ is running.
- Enable and customize the WebSphere MQ API resource security feature.

## Setting the message access authorization level

For security considerations, you can use WebSphere MQ Monitoring agent to control the level of user access to WebSphere MQ messages with the **MSGACCESS** parameter.

If you are unfamiliar with how to change monitoring options for an agent instance, review the steps in “Changing monitoring options” on page 14. If you are unfamiliar with the monitoring options used, review the descriptions of the options in “Monitoring options” on page 26.

WebSphere MQ Monitoring agent can be configured to set message access authorization level when one of the following accounts is used:

- The Tivoli Enterprise Portal user ID as the account (default setting).
- The account of the WebSphere MQ Monitoring agent.
- The predefined account.

Do the following steps to set message access authorization level:

1. Open the monitoring file of the agent instance that you want to configure.
2. Modify the **MSGACCESS** parameter in the **SET MANAGER** statement for a queue manager as needed, to specify the message manipulation authorization level. If not specified, this setting for the applicable **SET GROUP** statement is used.
  - If you specify the **MSGACCESS** parameter as NONE, DESC, RETRY, DATA, or DELETE, the **SET QACCESS** statement is ignored, and the message manipulation account is the same as the Tivoli Enterprise Portal user ID.
  - If you specify the value of USEQACCESS on the **MSGACCESS** parameter, the message manipulation account is defined on the **SET QACCESS** statement. If you do not specify the **SET QACCESS** statement, or if the **SET QACCESS** statement does not accommodate the specified Tivoli Enterprise Portal user ID for the specified queue name, the Tivoli Enterprise Portal user ID has the default message manipulation right of NONE; the specified Tivoli Enterprise Portal user ID cannot perform any message manipulation on the specified queue.
- a. Use the **SET QACCESS** statement to define multiple rules so that different Tivoli Enterprise Portal user IDs can have different message manipulation authorization levels. In this case, the message manipulation account can be specified. Table 4 shows the outcomes when a Tivoli Enterprise Portal user attempts to manipulate a message on a specified queue name. (These outcomes assume that the specified queue name passes the **NAME** parameter value check that is defined in **SET QACCESS** statement).

Table 4. Message manipulation on a specified queue name

<b>MSGACCOUNT value</b>	<b>Tivoli Enterprise Portal user ID matches the MSGAUTHUSERS parameter value?</b>	<b>Rule result</b>	<b>Message Manipulation Account</b>
UIUSER	YES	SUCCESS	Tivoli Enterprise Portal user ID
	NO	FAIL	N/A
MQAGENT	YES	SUCCESS	monitoring agent Account
	NO	FAIL	N/A

Table 4. Message manipulation on a specified queue name (continued)

MSGACCOUNT value	Tivoli Enterprise Portal user ID matches the MSGAUTHUSERS parameter value?	Rule result	Message Manipulation Account
USER=user-id	YES	SUCCESS	user ID
	NO	FAIL	N/A

If the rule result in the above table is FAIL, the given **SET QACCESS** settings are ignored for the current request, and other SET QACCESS settings are checked. If none apply (all result in FAIL), the resultant access is NONE.

- b. Optional: Use multiple **SET QACCESS** statements to impose the strictest rules on a particular Tivoli Enterprise Portal user for a particular queue. If you issue multiple **SET QACCESS** commands that specify different manipulation access settings, and more than one of the access settings applies to a given Tivoli Enterprise Portal user, WebSphere MQ Monitoring agent assigns the lowest manipulation access to that user. The order of manipulation access settings from lowest to highest is: NONE, DESC, RETRY, DATA, DELETE.

3. Save your settings.

If you set the monitoring options as follows, the user SYSADMIN potentially has the manipulation access of DESC:

```
SET GROUP NAME(GROUP1) DEFAULT(YES) COMMAND(YES) MSGACCESS(DATA)
SET MANAGER NAME(QM1) MSGACCESS(USEQACCESS)
SET QACCESS NAME(DEMO*) MSGAUTHUSERS(*) MSGACCOUNT(MQAGENT) MSGACCESS(DELETE)
MGRNAME(QM1)
SET QACCESS NAME(D*) MSGAUTHUSERS(SYS*) MSGACCOUNT(USER=DEMOUSER) MSGACCESS(DESC)
MGRNAME(QM1)
```

Assume that the Tivoli Enterprise Portal user SYSADMIN wants to manipulate messages on the DEMO.QUEUE1 queue. The first manipulation access that applies to this user is DELETE, and the message manipulation account is the agent account (MQAGENT). However, the manipulation access of DESC also applies to this user, and the message manipulation account is DEMOUSER. WebSphere MQ Monitoring agent assigns the message manipulation access of DESC to this user, because that is the lowest manipulation access that applies. If this Tivoli Enterprise Portal user attempts to delete a message, the following message is displayed: (KMQW008E) Not allowed By MSGACCESS, and the WebSphere MQ Monitoring agent prevents the user from deleting the message. See Chapter 2, "Customizing monitoring options," on page 11 for more detailed description.

---

## Interrelationship of Message Manipulation Access and Message Manipulation Account settings

You do not need to use the WebSphere MQ security feature; you can use only the **MSGACCESS** parameter settings on the **SET GROUP** and **SET MANAGER** monitoring options to control access to queue manager messages. For example, you can accept the default setting of DESC; then users can browse message descriptors in summary or detail reports. Or, you can change the default to DATA so that users can browse message contents. However, these settings apply to all user IDs at your site. If someone at your site needs to delete messages, you must set **MSGACCESS** to DELETE, which gives all user IDs permission to delete messages.

Use the **SET QACCESS** statement in conjunction with WebSphere MQ security. The WebSphere MQ security settings on the **Message Manipulation Account** are passed to the monitoring agent. Using the two options together ensures that user IDs have only the message access that they need. If a user attempts to view a message report and the user does not have the permission to view that report, the following message is displayed:

```
(KMQW000W)2035-Not_Authorized
```

Table 5 shows the combinations of MSGACCESS settings and WebSphere MQ settings that a user ID needs for the different levels of access to queue manager messages.

*Table 5. Combination of MSGACCESS settings and WebSphere MQ settings*

Level of message access	The required MSGACCESS for the queue manager	The required MQ security access to the queue for the user ID
List the messages on a queue (display the Queue Messages workspace)	DESC, RETRY, DATA, or DELETE	MQGET (with the browse option)
Browse the descriptor of a message	DESC, RETRY, DATA, or DELETE	MQGET (with the browse option)
Retry a message on the dead-letter queue or forward a message on the dead-letter queue to another queue	RETRY, DATA, or DELETE	MQGET (without the browse option)
Browse the contents of a message	DATA or DELETE	MQGET (with the browse option)
Delete a message	DELETE	MQGET (without the browse option)

The following two sample are procedures for implementing security for your queue manager messages:

- Procedure 1: The simplest implementation for manipulating messages is the following statements:

```
SET GROUP NAME(GROUP1) DEFAULT(YES) COMMAND(YES) MSGACCESS(USEQACCESS)
SET MANAGER NAME(QM1)
SET QACCESS NAME(*) MSGAUTHUSERS(*) MSGACCOUNT(MQAGENT) MSGACCESS
-(DELETE) MGRNAME(QM1)
```

Any Tivoli Enterprise Portal user can browse, retry, view message content, and delete the messages on any queues on the QM1 queue manager through this configuration. There is no security check and your queue manager message protection is minimal.

- Procedure 2: The moderate implementation for manipulating messages is as follows:

```
SET GROUP NAME(GROUP1) DEFAULT(YES) COMMAND(YES) MSGACCESS(USEQACCESS)
SET MANAGER NAME(QM1)
SET QACCESS NAME(*) MSGAUTHUSERS(*) MSGACCOUNT(MQAGENT)
-MSGACCESS(DESC) MGRNAME(QM1)
SET QACCESS NAME(DEADQ*) MSGAUTHUSERS(A*) MSGACCOUNT(MQAGENT)
-MSGACCESS(RETRY) MGRNAME(QM1)
SET QACCESS NAME(DATAQ*) MSGAUTHUSERS(B*) MSGACCOUNT(USER=DATAOPR)
```

```
-MSGACCESS(DATA) MGRNAME(QM1)
SET QACCESS NAME(TEMP*) MSGAUTHUSERS(SYS*) MSGACCOUNT(MQAGENT)
-MSGACCESS(DELETE) MGRNAME(QM1)
```

This configuration has the following implications:

- Any Tivoli Enterprise Portal user can browse the description of any queue messages.
- A Tivoli Enterprise Portal user named A\* (for example, Admin, Albert) can retry the messages that belong to queues named DEADQ\* (for example, DEADQ1, DEADQ.BACKUP), and browse the message descriptions.
- The Tivoli Enterprise Portal user named B\* (for example, Bob) can view the message contents that belongs to queues named DATAQ\* (for example, DATAQ1, DATAQ.CUSTOMER1), browse the message descriptions, and retry the messages. When the WebSphere MQ Monitoring agent issues the message manipulation to WebSphere MQ, it uses the DATAOPR as the account to interact with the WebSphere MQ. DATAOPR can have the right to view the message at queues named DATAQ\* when the WebSphere MQ security environment of each node is customized.
- A Tivoli Enterprise Portal user named SYS\* (for example, SYSAdmin) has all the rights for the messages that belong to queues named TEMP\* (for example, TEMP1).



---

## Chapter 7. Collecting queue statistics data

The Queue Statistics feature provides additional current and historical information about message arrival and departure rates, high queue depth, and the time when most recent activity occurred.

You can better monitor queue activity with this information, such as determining whether activity is at expected levels, whether messages are being read from the queues within a reasonable time frame, or whether messages are being put on a queue and not retrieved.

This optional feature provides additional data in the Queue Statistics and Queue Manager Status workspaces, additional Queue Statistics attributes for use in situations, and data for the MQSeries\_No\_Queue\_Messages\_Read predefined situation. You must enable this optional feature first, otherwise the value of some attributes in the related workspaces is 0.

For details about attributes, predefined situations, and the workspaces that are provided with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

---

### Enabling queue statistics monitoring

WebSphere MQ Monitoring agent uses the **Reset Queue Statistics** command to obtain queue statistics information. Monitoring for queue statistics data is disabled by default to ensure downward compatibility. Queue statistics data is available only when it is collected for the queue or queues.

If you are unfamiliar with how to change monitoring options for an agent instance, review the steps in “Changing monitoring options” on page 14. If you are unfamiliar with the monitoring options used, review the descriptions of the options in “Monitoring options” on page 26.

#### Remember:

- Make sure that the WebSphere MQ Monitoring agent is the only application that issues the **Reset Queue Statistics** command.
- The **Reset Queue Statistics** command has an impact on the event data of generated performance events. If WebSphere MQ events are monitored by other applications that rely on the event data of performance events, do not specify STATISTICS(YES) to enable queue statistics monitoring.

To enable the queue statistics monitoring, do the following steps:

1. Open the agent monitoring file.
2. Specify STATISTICS(YES) in the **SET QUEUE** statement for the queue or queues that you want to monitor.
3. Optional: To generate performance-related events, specify the **PERFMEV** attribute of the monitored queue manager as Enabled. For instructions about how to change attribute values of queue managers, see the *System Administration Guide* of WebSphere MQ.
4. Save your settings.

---

## Queue Statistics feature consideration

Using the Queue Statistics feature affects other information processing. Review the information about the information processing that might be affected.

### Queue service interval events monitoring

If you are monitoring queue service interval events for some queues, specify `STATISTICS(NO)` in the **SET QUEUE** statement for those queues. This configuration ensures that the queue service interval events continue to function correctly. However, some queue statistics are not available on these queues unless application queue statistics monitoring is active on z/OS systems (`SET APPL STATISTICS(ALL|NODYNAMQ)`).

### Queue events information monitoring

When you are monitoring for queue events information and the following events occur, the same queue statistics are collected and reset:

- `Queue_Depth_High`
- `Queue_Depth_Low`
- `Queue_Full`

After the reset, the queue statistics information that the agent collects is incomplete. The agent attempts to get queue statistics from events, but the agent succeeds only if event monitoring is turned on. If event monitoring is not turned on, the collected information is incomplete. If you are monitoring for queue events, specify `EVENTS(BROWSE)` or `EVENTS(REMOVE)` on the **SET MANAGER** command to ensure the most accurate event reporting.

### Another application using the Reset Queue Statistics command

When the **Reset Queue Statistics** command is issued, the queue statistics information is reset. As a result, if another application in addition to the WebSphere MQ Monitoring agent issues this command, the agent cannot provide complete and accurate statistics.

### Coexistence with Application Statistics (z/OS systems only)

If Queue Statistics data that is collected by the Reset Queue Statistics command and the Application Statistics data are both being collected for a queue, the data used by the WebSphere MQ Monitoring agent is the same data that is collected by the Reset Queue Statistics command. The Reset Queue Statistics command provides data about all activities in a queue, but Application Statistics data provides information about the applications that are being monitored.

---

## Chapter 8. Monitoring the publish and subscribe environment

The WebSphere MQ Monitoring agent provides a wide range of options for monitoring your WebSphere MQ publish and subscribe environment.

**Important:** Publish/subscribe related workspaces and features are only available when WebSphere MQ 7.0 or later is installed.

---

### Subscription topology

You can use the WebSphere MQ Monitoring agent to get a clear overview of a particular topic and the subscriptions that are associated with it by viewing a graphical version of the topology. This view is a part of the Topic Status - Subscribers workspace.

The topology view contains information about subscriptions to a single topic. The topmost node in this view represents a topic, which is labeled with the topic string. The second tier of the view contains subscriptions to the topic, labeled with the subscription names. The third tier contains the applications and destination queues that are associated with each subscription. A single destination queue might be used by more than one application, and for more than one subscription. Only applications that are currently running are displayed.

The topic is labeled with the first 48 characters of the topic string. If the topic string is longer than 48 characters, it is truncated. Subscriptions are labeled with the subscription name by default. If a subscription has no name defined, the subscription ID is used instead.

An example of the topology view is shown in Figure 11.

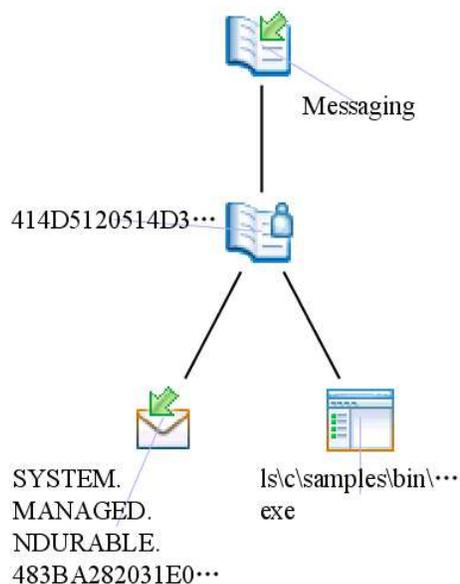


Figure 11. The subscription topology view

This topology shows subscriptions to the topic messaging, which is displayed in tier 1 of the diagram. Tier two contains the subscriptions to the topic. There is only one subscription to the Messaging topic. The subscription has no name value, and is labeled with its subscription ID. The third tier contains the destination queue and the application that subscribes to the topic. This subscription has a destination queue in which published messages are stored before being read by the application, and an application that subscribes to the topic. If the application with which the subscription is associated is not currently running, it is not displayed in the diagram.

For instructions about how to view the subscription topology, see “Viewing the subscription topology” on page 101

---

## Situations for queue depth monitoring

The following two situations are available for monitoring the depth of destination queues that are used by subscriptions:

- MQSeries\_Queue\_Depth\_High
- MQSeries\_Local\_DestQ\_Depth\_High

The first of these situations can be used to monitor the depth of any queue. The second can only be used to monitor the depth of queues that are used as destination queues by subscriptions. A comparison of the MQSeries\_Queue\_Depth\_High situation and the MQSeries\_Local\_DestQ\_Depth\_High situation is shown in Table 6.

*Table 6. Comparison of different situations for monitoring queue depth*

Feature	MQSeries_Queue_Depth_High	MQSeries_Local_DestQ_Depth_High
Types of monitored queues	Any queue	Any destination queue that are used by a subscriber
Queue location	Local and remote queues	Local queues only
Identifies which subscriptions are affected	No	Yes

In most circumstances, use the MQSeries\_Local\_DestQ\_Depth\_High situation to monitor destination queues that are used by subscribers if the queue manager that manages the queue is running on the same system as the subscriber. This is advantageous because this situation provides additional functionality for identifying subscriptions that are affected by a queue that reaches its high depth threshold. The MQSeries\_Queue\_Depth\_High situation does not.

If the queue does not run on the same system as its subscribers, the MQSeries\_Local\_DestQ\_Depth\_High situation cannot detect queue depth. In this case use the MQSeries\_Queue\_Depth\_High situation. If the queue is not used as a destination queue by subscribers, use the MQSeries\_Queue\_Depth\_High situation.

---

## Searching for publish and subscribe information (WebSphere MQ 7.0 or later)

You can use the search function to search for specific topic string, topic name, and subscription name information. Search facilities are accessed from different workspaces, depending on the information that you want to search for.

Before you perform a search operation, determine an appropriate search criteria in form of a topic string. The topic string can contain plus sign (+) and number sign (#) wildcard characters.

When you perform a search operation from a workspace, the workspace is not closed. Instead, a search window in which you can enter search criteria is displayed. When the search is completed, the results are displayed in the original workspace in place of its original data.

**Remember:** Do not try modifying the properties of the workspace where the search results are displayed after you perform a search from a workspace; if you do, the original workspace is displayed even if you cancel the modification. If you want to modify the workspace properties, do it before you perform the search operation.

To search for topic string, topic definition, and subscription name information, do the following steps:

1. Navigate to the workspace containing the type of data that you want to search for. The following workspaces support searching:
  - Topic Status
  - Topic Status – Subscribers
  - Topic Definitions
  - Subscription Definitions
  - Enterprise Wide Subscription Definitions
2. Right-click the workspace and click **MQ Search** to open the search window.
3. Enter the search criteria in the form of a topic string. The topic string can contain plus sign (+) and number sign (#) wildcard characters. These wildcard characters perform as follows:

**plus sign (+)**

Includes all nodes at the specified level of the hierarchy, but not their descendents. For example, the /STOCK/+ search string returns objects that are referenced by the /STOCK/NYSE topic string , but not /STOCK/NYSE/IBM.

**number sign (#)**

Includes all nodes at the specified level of the hierarchy, and their descendents. For example, the /STOCK/# search string returns both objects that are referenced by the /STOCK, /STOCK/NYSE, and /STOCK/NYSE/IBM topic strings.

4. Optional: If you want to enter advanced search criteria, click **Advanced**.

In the **Conditions** section of the window, enter any search conditions that you want to specify. You can use advanced search criteria to specify extra conditions that limit the returned search results. The search window with advanced options displayed is shown in Figure 12 on page 100.



Figure 12. The search window with advanced options displayed

Available options are as follows:

- **Conditions** Use the Conditions options to limit the number of results that the search returns by specifying additional criteria. Do the following steps:
  - a. Select the check box on the left.
  - b. In the leftmost field, select the attribute for which you want to add a condition. Not all columns are available for use as search conditions.
  - c. In the middle field, select the comparison operator that you want to use. For example, **equals** or **less than**.
  - d. In the rightmost field, enter the value that you want to use against the data that you are searching. This field supports the asterisk wildcard (\*) character representing any combination of alphanumeric characters at the end of the input string.

**Remember:** If the asterisk is not the last character in the input string, it is treated as a regular character and not as a wildcard character.

For example, you might enter the criteria shown in Figure 13.

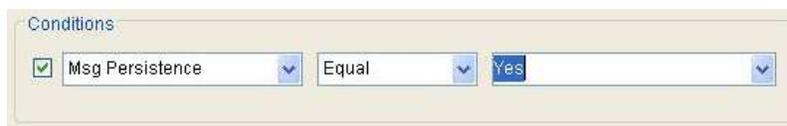


Figure 13. Specifying conditions in the advanced options of the search window.

- **Number of rows to return** The value of this option determines the maximum number of rows that are returned by the search. If the number of items matching the search criteria exceeds this value, some items are omitted from the results. If this value is set too high, searching might be very slow.
5. Click **Search**.
  6. If you change the value of the **Number of rows to return** option and the value is greater than the default value (2000), a warning message is displayed reminding you that setting this value too high might cause the search to be very slow. Click **OK**.

After the search completes, the results are displayed in the workspace in place of the original data.

---

## Viewing the subscription topology

You can view the subscription topology by navigating to the Topic Status - Subscribers workspace.

Before you open the workspace, make sure that the WebSphere MQ Monitoring agent is running.

Use Tivoli Enterprise Portal to view the subscribe topology of a particular topic.

1. In the navigator view, right-click **Publish Subscribe**; then click **Topic Status** workspace.
2. In the table at the bottom of the workspace for which you want to view the topology, right-click the topic, and click **Link To > Topic Status - Subscribers**. The Topic Status - Subscribers workspace containing the topology view is displayed.

**Requirement:** The topic that you select in the Topic Status workspace must have at least one subscriber, otherwise no topology view is available. The number of subscribers to a topic is indicated in the **Subscriber count** field in the Topic Status workspace.

---

## Preventing destination queues from overflowing (WebSphere MQ 7.0 or later)

You can use the WebSphere MQ Monitoring agent to alert you to destination queues used by subscriptions that are likely to overflow, and to take steps to resolve the problem before messages are lost.

Use the following flowchart to understand the procedure of how to prevent destination queues from overflowing.

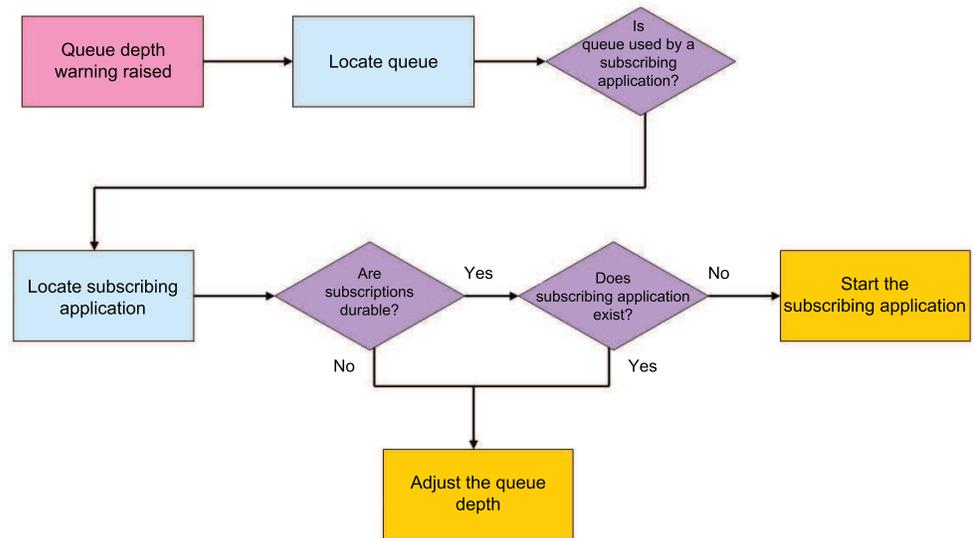


Figure 14. Preventing destination queues from overflowing

Do the following steps as illustrated in Figure 14:

1. Use the MQSeries\_Queue\_Depth\_High predefined situation to monitor the depth of subscription queues and to alert you that a queue becomes too full.
2. When the MQSeries\_Queue\_Depth\_High situation is triggered because that a queue is too full, move the mouse over the situation icon in the navigator view. A window containing information about the situation and a link to further details is displayed. Click the link.
3. The detailed situation information that is displayed indicates which queue triggered the situation. In the table that represents the queue, right-click the row, and link to the Subscription Definitions or Enterprise Wide Subscription Definitions workspace to see which subscriptions are using the queue that triggered the situation.

The Subscription Definitions workspace contains information about all subscriptions. The Enterprise Wide Subscription Definitions workspace contains information about all system defined remote subscriptions. A remote subscription is a subscription that stores published messages in a queue that belongs to a queue manager other than the queue manager that hosts the subscription.

4. Right-click the subscription that uses the queue that triggered the situation, and link to the Subscription Status workspace. In the Subscription Status workspace, check whether the subscription is durable.
5. If the subscription is durable, in the Subscription Status workspace that contains information about the subscription that triggered the situation, right-click the row and link to the Application Connections workspace.
  - If the Application Connections workspace contains no data, the application is stopped and messages that are sent to the queue by the publisher are not removed from the queue. Start the application to resolve the problem.
  - If the Application Connections workspace contains data, messages are probably not being processed fast enough by the subscribing application. To resolve this problem, increase the depth of the subscription queue.

6. If the subscription is nondurable, the subscription application is not processing messages fast enough. To resolve this problem increase the depth of the subscription queue.

**Remember:** If this situation persists for a long time, the message queue eventually becomes full even after you increase its depth.

---

## Resolving publishing failures

You can use the WebSphere MQ Monitoring agent to alert you to publishing failures and to troubleshoot the problem in the environment.

Publishing failure can occur when a message cannot be delivered to its destination queue or a dead letter queue. However, whether a publishing failure occurs in this situation depends on the values of two WebSphere MQ variables, NPMGDLV and PMSGDLV. If these variables are configured incorrectly, you can ignore the publishing failure. For more information about these two variables, see your WebSphere MQ documentation.

Publishing fails if a published message cannot be delivered to the destination queue that is used by a subscriber or to a dead letter queue. In this case, when the publishing application tries to publish the message, the application is notified that publishing failure occurs by WebSphere MQ. The most likely cause of a publishing failure is that the destination queue is full. The procedure for resolving publishing failures is illustrated in Figure 15.

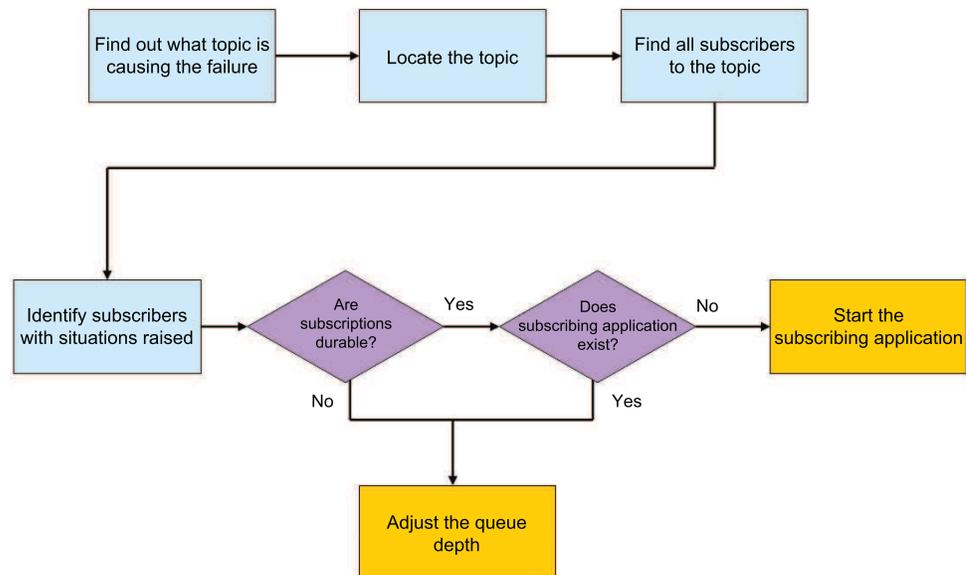


Figure 15. Resolving publishing failure

To find the cause of publishing failure and resolve the problem, do the following steps:

1. Locate the subscription for which publishing failure occurred by searching for the topic string using the Topic Status by Search option. The topic string is probably written to a log by the publishing application (although this depends

on how the application is written). For more information about searching, see “Searching for publish and subscribe information (WebSphere MQ 7.0 or later)” on page 98.

2. In the Topic Status workspace that contains information about the subscription for which publishing failed, right-click the row, and link to the Subscription Definitions workspace.
3. Right-click the subscription that is associated with the queue that triggered the situation, and link to the Subscription Status workspace. In the Subscription Status workspace, check whether the subscription is durable.
4. If the subscription is durable, in the Subscription Status workspace that contains information about the subscription that caused the publishing failure, right-click the row, and link to the Application Connections workspace.
  - If the Application Connections workspace contains no data, the application is stopped and messages that are sent to the queue by the publisher are not removed from the queue. Start the application to resolve the problem.
  - If the Application Connections workspace contains data, messages are probably not being processed fast enough by the subscribing application. To resolve this problem, increase the depth of the subscription queue.
5. If the subscription is non-durable, messages are probably not being processed fast enough by the subscribing application. To resolve this problem, increase the depth of the subscription queue.

**Remember:** If this situation persists for a long time, the message queue eventually becomes full even after you increase its depth.

---

## Chapter 9. Running Reports with Tivoli Common Reporting

Tivoli Common Reporting is a reporting feature available to users of Tivoli products, and provides a consistent approach to viewing and administering reports. Cognos® data model and sample reports for WebSphere MQ Monitoring agent are provided in a report package for use with Tivoli Common Reporting 2.1.1. The report package is a set of historical reports for both raw and summarized data that is collected in Tivoli Data Warehouse. You can use the sample reports to create your own reports on the data model.

---

### Prerequisite

Before you can run reports with Tivoli Common Reports, make sure that the following requirements are met in your environment.

- The WebSphere MQ Monitoring agent is installed and running.
- The Warehouse Proxy Agent is started.
- The Summarization and Pruning Agent is started.
- Historical data collection is enabled for the related attribute group.
- Summarized tables and views are created and populated in the Tivoli Data Warehouse.

#### Tips:

- To check whether the required summarized tables and views have been created, run the following queries against Tivoli Data Warehouse. If the tables and views have been correctly created, you can see the result sets that contain HV, DV, WV, QV, and YV in each base table, for example, Channel\_Status, Channel\_Status\_HV, Channel\_Status\_DV, Channel\_Status\_WV, Channel\_Status\_MV, Channel\_Status\_QV, and Channel\_Status\_YV.
  - DB2

```
select distinct "TABNAME" from SYSCAT.TABLES where
  "TABSHEMA" = 'ITMUSER'
```
  - Oracle

```
select distinct "TABLE_NAME" from USER_TABLES
```
  - SQL Server

```
select TABLE_NAME "VIEWNAME" from INFORMATION_SCHEMA.TABLES
```
- Cognos reports can be run against yearly, quarterly, monthly, weekly, daily, and hourly summarization intervals. You can decide which summarization interval is important to you to run reports against, and enable summarization for the related attribute group.
  - Application Accounting
  - Application Connections
  - Application Long-Term History
  - Application Queue Long-Term History
  - Application Transaction/Program Long-Term History
  - Buffer Manager Long-Term History
  - Channel Data
  - Channel Definitions
  - Channel Initiator Detail

- Channel Long-Term History
- Channel Status
- Channel Summary
- Connection Objects
- Current Queue Manager Status
- Error Log
- Listener Status
- Log Data Set Status
- Log Manager Long-Term History
- MQ Action Log
- MQ Channel Statistics
- MQ Event Statistics
- MQ Queue Statistics
- MQI Call Statistics Details
- MQI Message Statistics Details
- MQI Statistics
- Message Manager Long-Term History
- Message Statistics
- Page Set Long-Term History
- QSG Channels
- QSG Coupling Facility Structure Backups
- QSG Coupling Facility Structure Connections
- QSG Coupling Facility Structures
- QSG QMgrs
- QSG Queues
- Queue Accounting
- Queue Data
- Queue Definitions
- Queue Handle Status
- Queue Long Term History
- Queue Status
- Topic Manager Long-Term History

---

## Installing Cognos reports for WebSphere MQ Monitoring agent

Installing Cognos reports for the WebSphere MQ Monitoring agent includes installing agent-specific reports, configuring Cognos data source, and creating Tivoli Reporting and Analytics Model (TRAM) dimensions. The Cognos reports for the WebSphere MQ Monitoring agent must be installed on Tivoli Common Reporting server.

A report package for the WebSphere MQ Monitoring agent is provided in a folder named REPORTS on the installation disk. Use one of the following folders within the REPORTS folder to install Cognos reports depending on the database type of Tivoli Data Warehouse:

- DB2® and SQL Server: ITCAM\_Agents\_for\_WebSphere\_Messaging\_v71
- Oracle: ITCAM\_Agents\_for\_WebSphere\_Messaging\_v71\_for\_Oracle

1. If the report package folder is on a remote system, do one of the steps depending on the operating system where the Tivoli Common Reporting server is installed:
  - Windows: Map the remote folder to a local drive.
  - Systems other than Windows: Mount the remote system.
2. In the report folder, start the installation program by doing one of the following steps:
  - Windows: Double-click the `setup_windows.exe` file.
  - Systems other than Windows: Run the `setup_<platform>.bin` file.
3. Select the language of the installation program and click **OK**.
4. In the Welcome window, click **Next**.
5. In the Choose the Installation Folder window, specify the path to the Tivoli Common Reporting component directory and click **Next**.

**Important:** After this step, you cannot step back to this window to change the installation folder again. If you want to change the installation folder afterwards, cancel the installation program and start it again from Step 2.

6. In the Choose the reports for the installation window, select **WebSphere MQ Monitoring Agent Reports** and click **Next**.
7. In the Cognos Engine Configuration window, type the Tivoli Common Reporting user name and password, and then click **Next**.
8. In the Cognos Data Source TDW Configuration window, provide all required database information to define the Cognos data source, and click **Next**.

**Remember:** If you choose to skip this step, you must configure the connection to a database to access your data after the installation is complete. For instructions about how to configure a data connection, see Tivoli Common Reporting documentation.

9. In the Data Script runDbScript Configuration window, provide all required database information to create TRAM dimensions and click **Next**.

**Important:** The user ID that is used to run the database script must have administrator access to the IBM\_TRAM schema. The script requires the administrator access to delete the IBM\_TRAM schema related objects and re-create them.

**Remember:** Do not skip this step, otherwise, you must manually add TRAM dimensions, which are required for running Cognos reports and using the data model.

10. Review the installation information and click **Install**.
11. After the installation is complete, click **Done** to exit.

---

## Working with reports

Topics in this section provide instructions about how to run Cognos reports. If you did not use the installation wizard to install Cognos reports (see “Installing Cognos reports for WebSphere MQ Monitoring agent” on page 106), you must do the following steps before you can run Cognos reports:

1. Save the report package for WebSphere MQ Monitoring agent to the `TCR_component_dir\cognos\deployment` directory.

2. Import the WebSphere MQ Monitoring agent report package to Tivoli Common Reporting.
3. Create the Cognos data source for your report.

**Tips:**

- The report package for the WebSphere MQ Monitoring agent is provided as a compressed file named WebSphereMQReports.zip on the installation disk in the following folders:
  - For DB2 and SQL Server: REPORTS\  
ITCAM\_Agents\_for\_WebSphere\_Messaging\_v71\reports\cognos\_reports\  
Messaging\packages\WebSphereMQReports.zip
  - For Oracle: REPORTS\ITCAM\_Agents\_for\_WebSphere\_Messaging\_v71\_for\_Oracle\  
reports\cognos\_reports\Messaging\packages\  
WebSphereMQReports\_Oracle.zip
- For more information about how to work with reports using IBM Cognos 8 Business Intelligence Reporting, see the IBM Tivoli Common Reporting Information Center.

## Creating or editing web-based reports

You can create and customize your own reports using the Cognos Report Studio, which is a web-based report editor.

1. Log on to the Tivoli Common Reporting interface, and go to **Common Reporting**.
2. In the Work with reports window on the right, select **Report Studio** from the **Launch** list.
3. Use the menu controls to create a report or edit existing reports by formatting the layout and manipulating the data that appears in the report.
4. Save your report, and run it anytime you want to present on its underlying data.

## Creating ad hoc reports

After you import the report package provided for the WebSphere MQ Monitoring agent, you can create ad hoc reports by using simple queries and formatting.

To create ad hoc reports, perform the following steps:

1. Log on to the Tivoli Common Reporting interface, and go to **Common Reporting**.
2. In the Work with reports window on the right, select **Query Studio** from the **Launch** list.
3. Select the WebSphere MQ Monitoring Agent package. A new window is open and you can create a report.
4. From the navigation on the left, drag the data items that you want to include in your report.

**Remember:** Always drag the attributes that belong to the same query to your report. If you drag two attributes from different queries, the resulting data might be wrong. However, you can drag any time-related attributes from the Time identifier to your report.

5. Once you finish editing the report data and appearance, save the report by specifying a name, and optionally a description, and a screen tip.

**Tip:** When you do an ad hoc query, you can either see the live data as you drag the items, or switch the mode to show placeholders for the data and then run the report.

### Some other things that you can do in a report

- Combining metrics in one table

You can combine different metrics into one table. For example, you can drag Connection Name from the Channel Long-Term History table, and In-Doubt Status from the Channel Status table to the same table.

- Grouping data

You can group the data by clicking the Type column and then the Group icon



- Creating a chart

To create a chart, click the Chart icon . A chart is created for each section with appropriate groups.

For more information about using Query Studio, see Query Studio User Guide at the IBM Cognos 8 v4 Business Intelligence Information Center.

---

## Data model of WebSphere MQ Monitoring agent

The data model for the WebSphere MQ Monitoring agent is a star schema with dimensions or identifiers that are separated from facts or metrics. Metrics are measurable (numeric) attributes, which can be aggregated by identifiers. The relationship among the metric tables is defined using two common identifiers, resources and time.

The WebSphere MQ Monitoring agent collects various metrics. All the metrics are modeled for the agent. The metrics are classified into two categories, key metrics and extended metrics.

### Key metrics

The key metrics are the most important or the most frequently used metrics. The key metrics are divided into three groups, Resource Usage, Performance, and Availability. You can either see the raw metrics or summarized (daily and hourly) metrics.

### Extended metrics

In addition to the key metrics, the extended metrics include all the other metrics of the WebSphere MQ Monitoring agent.

### Identifiers

Identifiers are used to link metrics data across different agents. The two primary identifiers that are used by the WebSphere MQ Monitoring agent are resource and time.

Resource identifiers include execution group and host name. Time identifiers include various attributes of time, by which the metrics can be grouped, such as standard timestamp, date, minute, hour, day, week of year, month, quarter, or year.

## Attributes

Attributes describe the identifiers. For example, the detailed information about a channel can be described by the attributes, such as channel type, query type, or command level.

---

## Sample reports

Six sample reports are provided in the report package for the WebSphere MQ Monitoring agent. For the agent to get data to display in the sample reports, historical data collection must be enabled for the related attribute groups.

*Table 7. Historical attribute groups for sample reports*

Sample report	Attribute group
"Queue Manager Daily Availability report" on page 112	Current Queue Manager Status (detailed data)
"Queue Manager Weekly Availability report" on page 112	
"Channel Daily Availability report"	Channel Status (detailed data)
"Channel Weekly Availability report" on page 111	
"Top N Queue Full report" on page 112	Queue Long Term History (summarized data)
"Queue Full Detail Report" on page 111	

## Channel Daily Availability report

This report shows the daily availability of the channel that you specified, including the availability of the whole day and the availability of each hour during the day. Use this report to check the channel status in one day.

*Table 8. Parameters of Channel Daily Availability report*

Parameter group	Parameter name	Usage
<b>Date Range</b>	Report Period	Select the day that you want to check the channel status for.
<b>Sampling Interval</b>	Sampling Interval	Select the collection interval on the History Collection Configuration panel of Tivoli Enterprise Portal.
<b>Resource Selection</b>	Host Name	Specify the host name of the channel that you want to check.
	Queue Manager Name	Specify the name of the queue manager.
	Channel Name	Specify the name of the channel.
<b>Status</b>	Warning	Specify an integer as the warning threshold. If the channel availability percentage is less than the specified value, it is marked as warning status.
	Critical	Specify an integer as the critical threshold. If the channel availability percentage is less than the specified value, it is marked as critical status.

## Channel Weekly Availability report

This report shows the weekly availability of the channel that you specified, including the availability of a whole week and the availability of each day in the week. Use this report to check the channel status in one week.

Table 9. Parameters of Channel Weekly Availability report

Parameter group	Parameter name	Usage
Date Range	Report Period	Select one day in a week that you want to check the channel status for.
Sampling Interval	Sampling Interval	Select the collection interval on the History Collection Configuration panel of Tivoli Enterprise Portal.
Resource Selection	Host Name	Specify the host name of the channel that you want to check.
	Queue Manager Name	Specify the name of the queue manager.
	Channel Name	Specify the name of the channel.
Status	Warning	Specify an integer as the warning threshold. If the channel availability percentage is less than the specified value, it is marked as warning status.
	Critical	Specify an integer as the critical threshold. If the channel availability percentage is less than the specified value, it is marked as critical status.

## Queue Full Detail Report

This report displays the utilization of a specified queue over a time period.

Table 10. Parameters of Queue Full Detail report

Parameter group	Parameter name	Usage
Date Range	Report Period	Specify a time range for the report, such as Last Week, Current Month, Last 30 Days.
	Start Date	Select a start date from the calendar and start time from the time widget. Both date and time have to be specified.
	End Date	Select an end date from the calendar and end time from the time widget. Both date and time have to be specified.
Sampling Interval	Summarization Type	Specify the collection interval on the History Collection Configuration panel of Tivoli Enterprise Portal.
	Include shift period	Select to see data during peak hours, off-peak hours, or both.
	Include vacation period	Select to see data during the working days, vacations, or both.
Resource Selection	Host Name	Specify the name of the host that you want to check.
	MQ Manager Name	Specify the name of the queue manager that runs on the specified host.
	Queue Name	Specify the name of the queue within the specified queue manager.

## Queue Manager Daily Availability report

This report shows the daily availability of the queue manager that you specified, including the availability of the whole day and the availability of each hour during the day. Use this report to check the queue manager status in one day.

Table 11. Parameters of Queue Manager Daily Availability report

Parameter group	Parameter name	Usage
Date Range	Report Period	Select the day that you want to check the queue manager status for.
Sampling Interval	Sampling Interval	Select the collection interval on the History Collection Configuration panel of Tivoli Enterprise Portal.
Resource Selection	Host Name	Specify the host name of the queue manager that you want to check.
	Queue Manager Name	Specify the name of the queue manager.
Status	Warning	Specify an integer as the warning threshold. If the queue manager availability percentage is less than the specified value, it is marked as warning status.
	Critical	Specify an integer as the critical threshold. If the queue manager availability percentage is less than the specified value, it is marked as critical status.

## Queue Manager Weekly Availability report

This report shows the weekly availability of the queue manager that you specified, including the availability of a whole week and the availability of each day in the week. Use this report to check the queue manager status in one week.

Table 12. Parameters of Queue Manager Weekly Availability report

Parameter group	Parameter name	Usage
Date Range	Report Period	Select one day in a week that you want to check the queue manager status for.
Sampling Interval	Sampling Interval	Select the collection interval on the History Collection Configuration panel of Tivoli Enterprise Portal.
Resource Selection	Host Name	Specify the host name of the queue manager that you want to check.
	Queue Manager Name	Specify the name of the queue manager.
Status	Warning	Specify an integer as the warning threshold. If the queue manager availability percentage is less than the specified value, it is marked as warning status.
	Critical	Specify an integer as the critical threshold. If the queue manager availability percentage is less than the specified value, it is marked as critical status.

## Top N Queue Full report

This report shows the top  $n$  queues with the biggest queue full percentage. The queue full percentage is calculated by dividing the current queue depth by the

maximum queue depth, and then multiplying the result by 100. The number, *n*, can be customized as an input parameter. By default the report displayed top 10 queues.

Table 13. Parameters of Top N Queue Full report

Parameter group	Parameter name	Usage
Date Range	Report Period	Specify a time range for the report, such as Last Week, Current Month, Last 30 Days.
	Start Date	Select a start date from the calendar and start time from the time widget. Both date and time have to be specified.
	End Date	Select an end date from the calendar and end time from the time widget. Both date and time have to be specified.
Sampling Interval	Summarization Type	Specify the collection interval on the History Collection Configuration panel of Tivoli Enterprise Portal.
	Include shift period	Select to see data during peak hours, off-peak hours, or both.
	Include vacation period	Select to see data during the working days, vacations, or both.
Resource Selection	Number of Systems to Display	Specify an integer to filter the number of top resources that you want to see.
Status	Warning	Specify an integer as the warning threshold. If the queue full percentage exceeds the specified value, it is marked as warning status.
	Critical	Specify an integer as the critical threshold. If the queue full percentage exceeds the specified value, it is marked as critical status.

---

## Known problems and workarounds

This section contains problems that might occur when you work with Cognos reports.

### Arithmetic overflow errors in ad hoc querying

If you drag certain columns in an ad hoc query and it returns an arithmetic overflow error, switch to Limited Data or No Data preview and add Standard Timestamp to the query.

Certain columns might average or sum up to a number that is larger than the size supported by the database. So the SQL error of arithmetic overflow is returned. If you see the data by hourly timestamp or daily timestamp, or set a query to limit the data, the aggregated value is forced to be within the supported size.

### No data available message in ad hoc querying on two tables

The No data available message is displayed in an ad hoc querying on two tables, but the resulting data indicates that the two tables are queried.

This error occurs because there is no relationship defined between the two tables. Make sure all your ad hoc queries have at least one identifier.

## Errors of missing table or attribute

Make sure that all the prerequisites are met and the warehouse is collecting historical data. If you enable historical data collection appropriately, you are able to use the data model for WebSphere MQ Monitoring agent.

If you have all the required tables but still get this error, it might be because the WebSphere MQ Monitoring agent is not compatible with the version that is used in the generic model.

To check the query that runs, open the report in the Report Studio. Click **Tools > Show Generated SQL/MDX**. The queries in the report are displayed. You can view the native SQL.

## The table schema is not ITMUser

If the table schema that you use is not ITMUser, use the framework manager to update the schema to what you used.

1. Extract the report package to your local system that the framework manager is installed on.
2. In the model\WebSphere MQ Monitoring Agent v7.1 Data Model folder, open the WebSphere MQ Monitoring Agent v7.1 Data Model.cpf file with the framework manager.
3. In the Project Viewer view, expand **Data Sources** and click **TDW**.
4. In the Property view, change the schema property from ITMUser to the schema that you used and save the changes.
5. In the Project Viewer view, expand **Packages**, right-click the WebSphere MQ Monitoring Agent package and click **Publish Packages** to publish the package to the Cognos server.

---

## Chapter 10. Monitoring with workspaces

WebSphere MQ Monitoring agent is installed with default views that are displayed in workspaces. Where applicable, links are provided within the workspace to link from a parent view to a more detailed view about a selected row, or to a related workspace (for example, a workspace containing historical information).

You can customize the following settings for views in a workspace in the Time Span window:

- Time span for data presented in the views: real time, a specific time frame, or a custom time period
- Granularity of the data: summarized data or detailed data

**Important:** When you change these settings for one view in a workspace, make sure that you select the **Apply to all views associated with this view's query** check box at the bottom of the Select the Time Span window; otherwise, the data that is displayed in the workspace might be inaccurate.

---

### Creating custom workspaces

WebSphere MQ Monitoring agent displays information in workspaces. A workspace is the working area of the Tivoli Enterprise Portal application window and is made up of one or more views. A view is a pane in the workspace, typically a chart or table, which displays data that is collected by monitoring agents.

A workspace can be linked to other workspaces. A link is usually context-sensitive; right-click a row in a table or a data series in a chart to link to another workspace that provides more detailed information about one of the attributes in the row or data series.

As you select items in the Navigator view, the workspace presents views that are relevant to your selection. Every workspace has at least one view, and every workspace has a set of properties that are associated with it. You can customize a workspace by working in the Properties editor to change the style and content of each view. Another way to customize a workspace is to change the type of view or to add views to the workspace.

### Predefined workspaces

A set of predefined workspaces is included with WebSphere MQ Monitoring agent. Predefined workspaces make it easy for you to quickly start using WebSphere MQ Monitoring agent effectively to monitor your environment. They can also be used as templates to create your own custom workspaces.

A high-level overview of the types of workspaces that are included with WebSphere MQ Monitoring agent is provided.

For a complete list of the predefined workspaces that are included with WebSphere MQ Monitoring agent, see Tivoli Enterprise Portal online help.

For information about creating and customizing views and workspaces, see “Creating a workspace using a predefined workspace as a template” on page 116.

**Remember:** Do not customize the predefined workspaces because they are overwritten when you install fix packs or upgrade to a later version of WebSphere MQ Monitoring agent and the customized changes are lost.

## Creating a workspace using a predefined workspace as a template

You can create your own workspaces from a predefined workspace to display information about a specific set of attributes. The new workspace is associated with the same Navigator item as the original workspace.

Your user ID must have Workspace Author Mode permission to save the new workspace.

**Exceptions:** You cannot create your own workspaces based on the following predefined workspaces:

- Enterprise Wide Subscription Definitions
- Topic Definitions
- Topic Status
- Topic Status - Publishers
- Topic Status - Subscribers
- Subscription Definitions
- Subscription Status

Use Tivoli Enterprise Portal to complete this task.

1. Open the predefined workspace that you want to use as a template.
2. Click **File > Save Workspace As** to create a copy of the predefined workspace.
3. Enter a workspace name and, optionally, a description. The workspace name is displayed on the title bar.
4. Optional: Select one or more of the following workspace options:
  - Assign as default for this Navigator Item: Select this option if you want this workspace to be displayed when this navigator item is clicked.
  - Do not allow modifications: Select this option to prevent this workspace from being modified in the future.
  - Only selectable as the target of a workspace link: Select this option if you do not want this workspace to be displayed unless it is linked to from another workspace.
  - Assign as Home Workspace: Select this option if you want this workspace to be displayed as the home workspace by default.
5. Click **OK**. A copy of the predefined workspace is created with the name that you entered.
6. Open the new workspace and customize it to meet your requirements.

---

## Application Accounting workspaces (distributed systems only)

The Application Accounting workspaces can help you monitor accounting messages that are generated by queue managers to record information about the MQI operations that are performed by the WebSphere MQ applications, or to record information about the activities that occur in a WebSphere MQ system.

The Application Accounting workspaces apply to WebSphere MQ V6.0 and later versions only.

You can access these workspaces from the **Application Accounting** item for the selected queue manager in the Navigator physical view.

You need to enable WebSphere MQ before the application accounting data is shown in the Application Accounting workspaces. The following examples of commands are used to enable the Application Accounting messages.

**ALTER QMGR ACCTMQI(ON)**

Enable MQI accounting information collection.

**ALTER QLOCAL(Q1) ACCTQ(ON)**

Enable accounting information collection for the Q1 queue.

**ALTER QMGR ACCTQ(ON)**

Enable accounting information collection for all queues that specify the ACCTQ queue attribute as QMGR.

**ALTER QMGR ACCTCONO(ENABLED)**

Enable accounting overrides per connection.

**ALTER QMGR ACCTINT(900)**

Change the accounting interval to 900 seconds (15 minutes) from the default of 1800 seconds (30 minutes).

**ALTER QMGR STATMQI(ON)**

Enable MQI statistics

**ALTER QLOCAL(Q1) STATQ(ON)**

Enable statistics information collection for the Q1 queue.

**ALTER QMGR STATQ(ON)**

Enable statistics information collection for all queues that specify the STATQ queue attribute as QMGR.

**ALTER CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) STATCHL(MEDIUM)**

Enable statistics information collection, with a medium level of detail, for the QM1.TO.QM2 sender channel .

**ALTER QMGR STATCHL(MEDIUM)**

Enable statistics information collection, at a medium level of detail, for all channels that specify the STATCHL channel attribute as QMGR.

**ALTER QMGR STATACLS(MEDIUM)**

Enable statistics information collection, at a medium level of detail, for all automatically defined cluster-sender channels.

**ALTER QMGR STATINT(900)**

Change the statistics interval to 900 seconds (15 minutes) from the default of 1800 seconds (30 minutes).

## Guide for action

Use the Application Accounting workspaces to assist you with the following activities:

- Monitor application resource usage
- Record application activities
- Detect problems in your queue manager network
- Determine the causes of problems in your queue manager network
- Improve the efficiency of your queue manager network
- Familiarize yourself with the running of your queue manager network
- Confirm that your queue manager network is running correctly

These workspaces might include application connections which were active, but are not currently active. It might not include the currently active application connections, in cases where the application connections are new and for which accounting data is not published by the queue manager.

---

## Application Debugging workspaces (z/OS systems only)

Use these workspaces to debug your WebSphere MQ applications by viewing and sorting debugging trace data.

Data for these workspaces is available only if Application Debug Trace is collected on a z/OS system. You can collect application statistics by using the **TRACE** parameter of the **SET APPL** monitoring option. See Chapter 2, “Customizing monitoring options,” on page 11 for details.

Access these workspaces from the **Application Debugging** item for the selected queue manager in the Navigator physical view.

### Guide for action

Use the Application Debugging workspaces to trace a WebSphere MQ application that is running on a z/OS system. The Application Statistics workspaces show you the applications, CICS transactions, or programs that are experiencing or causing bottlenecks in your WebSphere MQ system; the Application Debugging workspaces can help you trace what went wrong in an application and correct it.

---

## Application Statistics workspaces (z/OS systems only)

The Application Statistics workspaces provide statistics about WebSphere MQ applications that are running on z/OS systems only.

Data for these workspaces is available only if Application Statistics are collected on a z/OS system. This can be activated using the **STATISTICS** parameter of the **SET APPL** monitoring option. See “Monitoring options” on page 26 for details.

You can access these workspaces from the **Application Statistics** item for the selected queue manager in the Navigator physical view.

### Application Statistics feature (z/OS systems only)

The application statistics feature provides detailed statistical information on an application's use of WebSphere MQ resources. Application statistics feature collects data as MQI events occur, compiling the data into statistics at each sample cycle. This data is extremely useful when analyzing performance problems. By isolating the WebSphere MQ portion of a transaction's total response time, the performance analyst can identify which subsystem experienced a slowdown and focus their diagnostic effort accordingly.

This feature provides data for the Application Debugging workspaces and Application Statistics workspaces.

Application Statistics data is available only if it is being collected for the queue manager and the applications. Monitoring for application statistics is turned off by default to prevent excessive system resource consumption. You can activate monitoring by specifying **SET MQIMONITOR** and **SET APPL** statements for the queue manager and application. You also need to set up an WebSphere MQ

Monitoring subsystem. For descriptions of monitoring options, see “SET MQIMONITOR (z/OS systems only)” on page 53 and “SET APPL (z/OS systems only)” on page 51.

For the instructions about how to set up the WebSphere MQ Monitoring subsystem, see *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Configuration Guide*.

## Guide for action

Use the information in the Application Statistics workspaces for trend analysis, performance history, and security checking. For billing purposes, for example, you might want to check how often a particular application runs. To streamline the workload, compare current and historical queue and queue manager usage across different page sets.

You can check the following things when viewing the data in these workspaces:

- Examine the number of puts versus the number of gets.  
If they are not equal, where is the data flow breaking down? If one queue has a large number of puts, you might want to alter the queue definition to use a different page set.
- Whether the average MQPUT and MQGET response times meet your objectives:  
If one application is running significantly faster than another, you might want to use a different page set to provide better processing time.
- The number of queues that are being browsed, the reason that they are being browsed, and the applications that are browsing them:  
Verify that restricted queues (such as a payroll queue) are not being browsed without proper authority.
- Review the average message size for your queues; whether messages are typically the maximum size (see the MaxMsgLength queue attribute.):  
If messages are usually at maximum size, there might be a problem in an application or a queue definition.

You can use these workspaces in conjunction with the Application Debugging workspaces to help you locate and correct problems in your WebSphere MQ applications.

---

## Buffer Pool Statistics workspaces (z/OS systems only)

You can use the Buffer Pool Statistics workspaces to ensure that buffer managers are performing efficiently.

These workspaces display current buffer manager performance for all monitored queue managers on a z/OS system. You can also drill down to display information about a specific buffer pool to isolate recent or historical performance trends.

Access these workspaces from the **Buffer Pool Statistics** item for the selected queue manager in the Navigator physical view.

## Guide for action

Each queue manager on a z/OS system includes a buffer manager. The buffer manager uses the buffers in a buffer pool to hold WebSphere MQ objects, including

messages. When your buffer pools are allocated correctly, you can access messages more efficiently because they are retrieved from buffers in storage, rather than from disk.

To enhance buffer pool performance, monitor the following conditions:

- Examine the ratio of pages that are read from DASD to retrieved pages. The ratio indicates the efficiency of page retrieval within buffer pool storage. The objective is to keep this ratio low.

The ratio of pages that are not found in the buffer pool to retrieved pages is another measure of how efficiently pages are retrieved.

The number of asynchronous write-processor starts indicates how many times more than 85% of the buffer pool is waiting for write I/Os or how many times less than 15% of the buffer pool is available for read. The objective is to keep the number of these starts low.

For any of these problems, first increase the buffer pool size. If the ratio remains high, pages are not reaccessed frequently enough. This might result in long delays between putting messages and subsequently getting them for a WebSphere MQ application.

The ratio of pages that are updated to pages that are written to DASD indicates the efficiency of the asynchronous write processor. The objective is to keep this ratio high. To increase this ratio, increase buffer pool size.

- Monitor the number of updates that are done synchronously. A synchronous update occurs when more than 95% of the pages in the buffer pool are waiting for write I/Os or when less than 5% of the buffer pool is available for read. The objective is to maintain zero synchronous updates. Monitor the number of times there are no buffers available for page gets. If this number is ever nonzero, WebSphere MQ is under severe stress.

In these cases, increase buffer pool size, and then look at I/O contention on the DASD page sets.

You can also consult the Page Set Statistics workspace to review the performance of the page sets associated with a specific buffer pool ID (see “Page Set Statistics workspaces (z/OS systems only)” on page 134).

---

## Channel Definitions workspaces

The Channel Definitions workspaces provide you with information about the channels for each monitored queue manager. Included in this information is the channel type (sender, receiver, server, or requestor) and other definition data. The Real-time Channel Definitions workspace contains on-demand data that is collected in real-time, when you open or refresh the workspace. If you have many channels defined, the real-time workspace can have a slow response time and consume more resources to retrieve the data. All other workspaces contain sampled data.

You can access these workspaces from the **Channel Definitions** item for the selected queue manager in the Navigator physical view.

The Channel Definitions Summary chart that is contained in the Real-time Channel Definitions workspace does not necessarily match the data that is displayed in the table at the bottom of this workspace. It is intended only to give an overview of the sampled data at the queue manager level according to the current parameters of the agent. The data that is displayed in the table is on-demand data, which is collected when the workspace is opened or refreshed, whereas the data on which the chart is based is sampled during standard sampling intervals.

**Tip:** The key for the Channel Definitions Summary chart is read from top to bottom and corresponds to the columns of the chart when read from left to right.

## Guide for action

Use the Channel Definitions workspaces to check channel definitions and channel parameters. You can often solve channel problems by correcting channel definitions.

You might need to define multiple channels to accommodate high message traffic, different message priorities, or different queue types.

---

## Channel Initiator Status workspaces (z/OS systems only)

The Channel Initiator Status workspaces apply only to the queue managers on z/OS systems. These workspaces provide information about the following items:

- Channel connection status (the number of current, maximum, active, starting, stopping, and retrying channels)
- Whether the channel initiator, TCP/IP listener, and LU62 listener are active
- The status of adapter subtask and dispatcher activity

Channel Initiator Status information can also be stored historically. See Chapter 5, “Collecting historical data,” on page 79 for information about how to enable historical data collection.

Access the top-level workspace from the **Channel Initiator Status** item for the selected queue manager in the Navigator physical view.

## Guide for action

Use the Channel Initiator Status workspaces to improve your processing capacity and to detect errors in your communication system.

- Compare the number of adapter subtasks that are currently active to the number of adapter subtasks that are requested in the channel initiator parameters.  
If the numbers are different, some adapter subtasks fail and do not restart, which reduces processing capacity.
- Compare the number of dispatchers that are currently active to the number of dispatchers that are requested in the channel initiator parameters.  
If the numbers are different, some dispatchers fail and do not restart. The number of current TCP/IP and LU 6.2 channels that are available are reduced proportionately, and other processing capacity might be reduced.
- Compare the numbers of channel connections that are current, active, maximum, starting, stopping, and retrying.
- Check whether the channel initiator, TCP/IP listener, TCP/IP group listener, LU 6.2 listener, and LU 6.2 group listener are active.  
If a listener was started, and was not deliberately stopped, this might indicate an error in the communications system.

On z/OS systems, TCP/IP listeners can be started many times with different combinations of port number and address. If this occurs, the TCP/IP Listener Active and Port Number columns in this workspace display the most recent TCP/IP listener information that is provided by WebSphere MQ. To access the TCP/IP Started Listeners workspace and display all started TCP/IP listeners, right-click a row that contains an active TCP/IP listener.

---

## Channel Performance workspaces

The Channel Performance workspaces provide performance information about the monitored channels on each monitored queue manager. Included in this information is whether each channel is in doubt, current, or inactive, and the channel type.

The Channel Status workspace provides on-demand, the most current, real time information about channels in the queue manager.

Client connection channel definitions do not produce statistics, therefore they are not listed in any of the Channel Performance workspaces.

You can access these workspaces from the **Channel Performance** item for the selected queue manager within the Navigator physical view.

The Channel Performance Summary chart that is contained in these workspaces does not necessarily match the data that is displayed in the table at the bottom of this workspace. It is intended only to give an overview of the sampled data at the queue manager level according to the current parameters of the agent. The data that is displayed in the table represents only a subsection of collected data, whereas the data that is displayed in the chart provides a summary of all sampled data.

### Guide for action

A channel provides a communication path between two queue managers (on the same system or on different systems). It shields the application programs from the complexities of the underlying network protocols. A channel consists of a transmission queue, a message channel agent (communications program), and a communications link.

When using these workspaces, you can check for the following things:

- The depth of the transmission queue  
If this number remains high, consider assigning more channels. You might need to define multiple channels to accommodate high message traffic, different message priorities, or different queue types. Sequence number and logical unit-of-work data can help you with channel recovery and restart.
- Use the information in the Channel Performance workspace to examine and compare channel performance among the selected channels. Look for patterns in resource activity, traffic, or time of day.
- Use the information in the Recent Channel Performance workspace to investigate recent trends in the performance of the selected channels. Look for patterns in time of day, channel type, or transmission rate.
- Use the information in the Channel Parameters workspace to check the defined parameters for the selected channel.
- Use the information in the Channel Summary workspace to get the summary data about all the channel instances per channel.

---

## Cluster Queue Manager workspaces

The Cluster Queue Manager workspaces provide information about explicitly and automatically defined cluster channels and the cluster queue manager that is associated with them. The Cluster Queue Manager workspace contains sampled data and the Real-time Cluster Queue Manager workspace contains on-demand data that is collected in real-time when the workspace is opened or refreshed.

You can access these workspaces from the **Cluster Queue Manager** item for the selected queue manager in the Navigator physical view.

The Cluster Queue Manager Summary chart that is contained in the Real-time Cluster Queue Manager workspace does not necessarily match the data that is displayed in the table at the bottom of this workspace. It is intended only to give an overview of the sampled data at the queue manager level according to the current parameters of the agent. The data that is displayed in the table is on-demand data, which is collected when the workspace is opened or refreshed, whereas the data on which the chart is based is sampled during standard sampling intervals.

### Guide for action

Use the Cluster Queue Manager workspaces to determine clustering activity and definitions for monitored queue managers. For example, the workspaces provides you with the following information:

- The number of automatically defined cluster-defined channels that exist
- Cluster queues and cluster queue managers that are associated with cluster channels
- The queue managers that are repositories for the cluster

---

## Dead-Letter Queue Messages Workspaces

Use the Dead-Letter Queue Messages workspaces to list and to examine the messages that a queue manager queues to its dead-letter queue (DLQ) because the messages cannot be delivered. Use these workspaces to manage the dead-letter queues and to ensure that you maintain the efficiency and integrity of your business application data. With these workspaces, you can recover important messages or resend them to their original destinations, delete obsolete messages, and identify problem applications.

You can access these workspaces from the **Dead-Letter Queue Messages** item for the selected queue manager in the Navigator physical view.

### Guide for action

Whether you can access and use Dead-Letter Queue Messages workspaces depends on certain parameter settings. See “Settings for controlling access to WebSphere MQ messages” on page 89.

WebSphere MQ puts a message on the dead-letter queue when it cannot deliver the message to the requested queue. Messages cannot be delivered when the message is too long, the queue name is not valid, or the queue is full.

You can use these workspaces as follows:

- Select a message to view its header or application data, delete it, or retry its delivery.

- If a queue is full, you can use the Queue Messages workspace to delete unnecessary messages (as described in “Queue Messages workspace” on page 148). Then, you can use the Dead-Letter Queue Messages workspace to retry delivering those messages that fails because the queue is full.

When you confirm a delete or retry, a return code and message are returned. For an explanation of numeric return codes, see *IBM WebSphere MQ Application Programming Reference* manual.

## Deleting a message from the dead-letter queue

You can delete a message from a dead-letter queue directly from the Dead-Letter Queue Messages workspace.

Before you open the workspace, make sure that the WebSphere MQ Monitoring agent is running.

Use Tivoli Enterprise Portal to complete this task.

1. In the Dead-Letter Queue Messages workspace, right-click the message that you want to delete; then click **MQ Commands > Delete**
2. A message is displayed asking whether you want to delete the message. To delete the message, click **Yes**.

**Remember:** If you delete a segmented or grouped message, WebSphere MQ Monitoring agent deletes the entire logical message.

3. The status of your delete request is displayed showing whether it is successful. To remove the status message, click **OK**.

## Forwarding a message on the dead-letter queue to another queue

From the Dead-Letter Queue Messages workspace, you can forward a message on the dead-letter queue to a destination queue that you specify and delete it from the dead-letter queue.

Before you open the workspace, make sure that the WebSphere MQ Monitoring agent is running.

The message can be forwarded to a queue on any queue manager that is known to the WebSphere MQ system. Deleting the message after you forward it prevents the message from being displayed more than once on the dead-letter queue if it becomes undeliverable again.

1. In the Dead-Letter Queue Messages workspace, right-click the message that you want to forward; then click **MQ Commands > Forward**
2. In the dialog box that displays the original destination queue of the message and the current queue manager, complete the following fields:
  - In the **Queue name** field, enter the name of the queue to send the message to.
  - In the **Queue Manager** field, enter the name of the queue manager for the queue that you specified in the **Queue name** field.
3. Click **Yes**. The message is forwarded and then deleted from the dead-letter queue.

**Remember:** If you forward a segmented or grouped message, WebSphere MQ Monitoring agent forwards the entire logical message.

4. The status of your forward request is displayed; click **OK** to clear the status message.

---

## Error Log workspaces (distributed systems only)

Use this workspace to view and monitor WebSphere MQ error log data that is retrieved from a monitored queue manager (distributed systems only). It does not provide error log data that is associated with unknown queue managers or with client applications.

Error Log data is available for display only if the data is collected for the queue manager. See “Error Log monitoring (distributed systems only).” Error Log data can also be stored historically. See Chapter 5, “Collecting historical data,” on page 79 for information about how to enable historical data collection.

You can access this workspace from the **Error Log** item for the selected queue manager in the Navigator physical view.

## Error Log monitoring (distributed systems only)

By using the Error Log monitoring, you can view and monitor WebSphere MQ error log data that is retrieved from a monitored queue manager. Error Log monitoring does not provide error log data that is associated with unknown queue managers or with client applications.

This feature provides data for the Error Log workspace, provides you with Error Log attributes that you can use in situations, and provides the MQSeries\_Channel\_Out\_Of\_Sync predefined situation .

For details about attributes, predefined situations, and the workspace provided with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

Error Log data is available only if it is collected for the queue manager. Monitoring of the queue manager error log is active by default. However, you can deactivate the error log monitoring feature using the **ERRLOGCYCLE** parameter of the **SET MANAGER** or **SET GROUP** monitoring option. You can also adjust the maximum number of messages that are displayed in the Error Log workspace using the **ERRLOGMAX** parameter of the **SET MANAGER** or **SET GROUP** monitoring option. For details of these monitoring options, see “Monitoring options” on page 26.

WebSphere MQ Monitoring agent monitors error logs that are in the following default locations.

- On i5/OS systems:  
`/QIBM/UserData/mqm/qmgrs/qmname/errors`  
where *qmname* is the name of the queue manager.
- On UNIX and Linux systems:  
`/var/mqm/qmgrs/qmname/errors`  
where *qmname* is the name of the queue manager.
- On Windows systems:  
`MQ WorkPath\qmgrs\qmname/errors`  
where *MQ WorkPath* is obtained from the `\Software\IBM\MQSeries\CurrentVersion\WorkPath` NT Registry Key and *qmname* is the name of the queue manager.

After you create a queue manager, error log files that are read by WebSphere MQ Monitoring agent are automatically created when the queue manager needs them. The files are named as follows:

- AMQERR01.LOG
- AMQERR02.LOG
- AMQERR03.LOG

Each of these error log files has a capacity of 256 KB. As error messages are generated, they are placed in the AMQERR01 file. When the AMQERR01 file gets bigger than 256 KB, it is copied to the AMQERR02 file. Before the AMQERR01 file is copied, the AMQERR02 file is copied to the AMQERR03 file. The previous contents of the AMQERR03 file (if any) are discarded.

The latest error messages are always placed in the AMQERR01 file. The monitoring agent monitors the AMQERR01 file.

## Guide for action

The Error Log table view provides you with the most recent WebSphere MQ error log data that is retrieved from a monitored (distributed systems only) queue manager. Use the information in this workspace to resolve queue manager problems in a timely manner. Only error log entries that are recorded after the start of the monitoring agent are displayed.

---

## Log Data Set Status workspace (z/OS systems only)

The Log Data Set Status workspace provides you with information about the log data sets. The log is made up of log records, each of which is a set of log data that is treated as a single unit. A log record is identified either by the relative byte address (RBA) of the first byte of its header, or by its log record sequence number (LRSN).

This is a secondary workspace; in the Navigator physical view, you can access it by right-clicking the **Queue Manager Status** item for the selected queue manager and clicking **Workspace > Log Data Set Status**.

For the complete list of predefined workspaces that are included with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

## Guide for action

Use the information in the Log Data Set Status workspace to identify whether there is an outstanding unit of work (UOW) for the following items:

- Currently active UOWs
- Page set updates that are not flushed from the buffer pools to disk
- CF structure backups and whether the log of this queue manager contains required information in any recovery operation that is using them

---

## Log Manager Performance workspaces (z/OS systems only)

These workspaces provide information about the logging activity (such as I/O levels and the number of times a WebSphere MQ application is delayed because no logging buffers are available) for each monitored queue manager on a z/OS system.

Access these workspaces from the **Log Manager Performance** item for the selected queue manager in the Navigator physical view.

## Guide for action

Use the information in the Log Manager Performance workspaces to monitor recent and long-running activities for a particular queue manager on a z/OS system, or to compare log manager performance of queue managers on z/OS systems.

The log entries are used to roll back an incomplete logical unit of work or to recover messages after a queue manager or system failure. For best performance, eliminate contention for DASD log files, provide sufficient buffer and log file capacity, and maintain correct log buffer thresholds.

Use the Log Manager Performance workspaces to monitor the following conditions:

- Check the number of times that a task is suspended because all buffers are waiting to be written to the active log data set.

Ensure that the active log is available for writing. If it is available, you can increase the value of the **OUTBUFF** parameter within the CSQ6LOGP log.

- Whether the ratio of reads that are satisfied from the archive data set to all of the read requests is excessive. Most log reads should come from the output buffer or the active log.

To satisfy requests for a rollback, unit-of-recovery records are read from the in-storage buffer, the active log, and the archived logs. Also, the ratio of log reads to log writes can indicate how much work must be backed out.

A long-running unit of recovery might require that log records be spread across many different logs. This degrades performance because extra work is required to recover the log records.

Request that the WebSphere MQ application reduce the unit-of-recovery length. Also, consider increasing the size of the active log. Statistics that are produced immediately after system startup might show significant log activity because the log is used to roll back inflight logical units of work. Check that log activity subsides after startup.

---

## Message Manager Performance workspaces (z/OS systems only)

The Message Manager Performance workspaces provide information on how frequently calls to the WebSphere MQ application programming interface (API) are made on a z/OS system. These rates can help you determine how frequently messages are passed to and pulled from a particular queue manager.

Access these workspaces from the **Message Manager Performance** item for the selected queue manager within the Navigator physical view.

## Guide for action

Use the information in these workspaces to determine how frequently the following operations are performed on the monitored queue manager on a z/OS system:

- Queues are opened (MQOPEN calls).
- Queues are closed (MQCLOSE calls).
- Messages are put to queues (MQPUT calls).

- Messages are pulled from queues (MQGET calls).
- A single API call is used to open a queue, queue a message, and then close the queue (MQPUT1 calls).
- Object characteristics are queried (MQINQ calls).
- Object characteristics are modified (MQSET calls).
- subscriptions are registered to certain topics (MQSUB routines).
- requests on subscriptions are made (MQSUBRQ routines).
- callbacks are called by WebSphere MQ when certain events occur (MQCB routines).
- controlling actions are performed on the object handles opened for a connection (MQCTL routines).
- status information are retrieved (MQSTAT routines) .
- WebSphere MQ handles are closed independently of WebSphere MQ API calls.

---

## Message Statistics workspaces

Use the Message Statistics workspaces to closely monitor the messages on a particular queue.

Access these workspaces from the **Queue Definitions** item (or from the **Queue Statistics** item) for the selected queue manager in the Navigator physical view.

For example, from the Queue Definitions workspace, if you right-click a table row and select **Link To**, you can select one of the following workspaces:

- Current Message Statistics
- Current Message Statistics by Application Name
- Current Message Statistics by Correlation ID
- Current Message Statistics by Group ID
- Recent Message Statistics

For the complete list of predefined workspaces that are included with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

## Message Statistics feature

The Message Statistics feature provides summarized statistics about all messages on a particular queue.

This feature provides data for the Message Statistics workspaces (for an overview, see “Message Statistics workspaces”), and provides you with Message Statistics attributes that you can use in situations, and provides MQSeries\_Delayed\_Message\_Group and MQSeries\_High\_Delayed\_Messages predefined situation.

You can also store message statistics historically. The data that is kept historically for message statistics is determined by the active situations for the Message Statistics attribute group.

For details about attributes, predefined situations, and the workspaces that are provided with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

## Details of operation

Message statistics are collected only when requested and a sampling interval is not used. When these statistics are requested, each message in the specified queue is read and processed to provide the summarized message statistics.

WebSphere MQ Monitoring agent requests message statistics data collection whenever you open or refresh one of the Current Message Statistics workspaces (that is, whenever you query the Message Statistics attribute group).

To view the Current Message Statistics workspaces, the WebSphere MQ Security Access level to the selected queue for your Message Manipulation Account for specified Tivoli Enterprise Portal Logon user ID must be MQGET (with the browse option). Additionally, users must have access to the messages that are in the queue. You can modify user access during customization using the **MSGACCESS** parameter of the **SET GROUP**, **SET MANAGER**, and **SET QACCESS** monitoring options. Any value other than MSGACCESS (NONE) results in the collection of message statistics. If you attempt to view one of the Current Message Statistics workspaces without the correct access, no data is returned. For information about how to configure the Message Manipulation Account for a specific Tivoli Enterprise Portal Logon user ID, see “Setting the message access authorization level” on page 90.

The Recent Message Statistics workspace displays all rows that are associated with the requested queue that are waiting to be written to the historical data warehouse. This workspace only contains data if the following two conditions are met:

- Historical data collection of the attributes that belong to the Message Statistics attribute group must be enabled. See Chapter 5, “Collecting historical data,” on page 79 for information about enabling historical data collection.
- One of the following situations must be triggered:
  - MQSeries\_Delayed\_Message\_Group
  - MQSeries\_High\_Delayed\_Messages

After the data is stored in the data warehouse, it is no longer displayed in the Recent Message Statistics workspace.

WebSphere MQ Monitoring agent also requests message statistics data collection whenever a situation uses the Message Statistics attributes. A situation drives the collection of message statistics data for a particular queue name. The queue name is a required input attribute for message statistics situations, and if it is not specified, no data is collected. The Queue Name attribute must specify an individual queue name; no wildcard characters can be used. You must create a separate situation for every queue that is to be monitored. Because of the overhead of collecting message statistics data, it should be collected only for those queues that need to be closely monitored. For situations, the user ID of the monitoring agent is used to access the queue.

Many of the message statistics are calculated using the put-date-and-time attribute of the message in the queue. If the queue has messages with a put-date-and-time attribute that does not reflect accurately the date and time that the message is put into the input queue, the statistics is correspondingly inaccurate. Put-date-and-time attributes are not accurate indicators when origin context is preserved or set for a message during the putting operation by an application to the queue. Inaccurate dates and times are common when an application is a message mover that moves messages from one queue to another, or when any application passes or sets origin context for a message.

If no data is returned for Message Statistics situations or workspaces, see the agent log to determine the reason. The KMQMI209E and KMQMI210E messages are associated with this feature.

## Guide for action

Whether you can access and use the Message Statistics workspaces depends on the certain parameter settings. See “Message Statistics feature” on page 128.

Use the information in the Message Statistics workspaces to determine how many messages of different priorities reside on a particular queue and to determine whether messages for a particular queue are processed in an acceptable amount of time.

The following examples show the type of message statistics that you can access.

- Average message time (the average number of seconds that messages is on the queue)
- Delayed messages (the number of messages that are not processed within a time threshold)
- Oldest message time (the number of seconds that the oldest message is on the queue)
- Priority 0 – Priority 9 messages (the number of messages in each priority group on the queue)
- Total messages

---

## MQ Action Log workspace

The MQ Action Log workspace provides information about actions performed by end users. The described actions refer to message manipulation actions and actions that are performed by issuing Take Action commands.

**Important:** Make sure that you select the MQ\_Action\_Log group in the History Collection Configuration window to start collecting historical data for this attribute group before viewing data in this workspace. The MQ\_Action\_Log group is started by default in the History Collection Configuration.

This workspace contains information only if Take Action commands or message manipulation actions are issued since WebSphere MQ Monitoring agent is installed or since historical data for this log is cleared or warehoused. If no actions occur since installation, the MQ Action Log view is empty, and the KFWITM217E error message is displayed at the bottom of the workspace. However, after the first Take Action command is issued, this message is no longer displayed and the contents of the Take Action log are displayed correctly.

This workspace contains information only if the date, time and time zone settings of the systems on which the Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server run are the same.

This is a secondary workspace. In the Navigator physical view, you can access it by right-clicking the Queue Manager Status item for the selected queue manager and clicking **Workspace > MQ Action Log**.

For the complete list of predefined workspaces that are included with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

## Guide for action

Use the information in the MQ Action Log workspace to view message manipulation actions and actions that are performed by issuing Take Action commands.

This workspace provides the following information about the actions performed by issuing Take Action commands:

- Name of the action that is performed
- Name of the object on which the action is performed
- ID of the user who performs the action
- Time that the action is performed
- Result of the action

The following information about message manipulation actions is provided:

- Type of the action, whether delete, retry, or forward
- The queue manager, queue, and message, on which the message manipulation action is performed
- ID of the user who performs the action
- Time that the action is performed
- Result of the action

---

## MQI Statistics workspaces (distributed systems only)

These workspaces monitor the statistics messages that are used to record information about the activities that occur in a WebSphere MQ system.

These workspaces apply to WebSphere MQ V6.0 and later versions.

Access these workspaces from the **MQI Statistics** item for the selected queue manager in the Navigator physical view.

You need to enable WebSphere MQ before the MQI statistics is displayed in the MQI Statistics workspaces. The following examples of commands are used to enable the MQI statistics messages.

### **ALTER QMGR ACCTMQI(ON)**

Enable MQI accounting information collection.

### **ALTER QLOCAL(Q1) ACCTQ(ON)**

Enable accounting information collection for the queue, Q1.

### **ALTER QMGR ACCTQ(ON)**

Enable accounting information collection for all queues that specify the ACCTQ queue attribute as QMGR.

### **ALTER QMGR ACCTCONO(ENABLED)**

Enable accounting overrides per connection.

### **ALTER QMGR ACCTINT(900)**

Change the accounting interval to 900 seconds (15 minutes) from the default of 1800 seconds (30 minutes).

### **ALTER QMGR STATMQI(ON)**

Enable MQI statistics

**ALTER QLOCAL(Q1) STATQ(ON)**

Enable statistics information collection for the Q1 queue.

**ALTER QMGR STATQ(ON)**

Enable statistics information collection for all queues that specify the STATQ queue attribute as QMGR.

**ALTER CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) STATCHL(MEDIUM)**

Enable statistics information collection, with a medium level of detail, for the QM1.TO.QM2 sender channel.

**ALTER QMGR STATCHL(MEDIUM)**

Enable statistics information collection, at a medium level of detail, for all channels that specify the STATCHL channel attribute as QMGR.

**ALTER QMGR STATACLS(MEDIUM)**

Enable statistics information collection, at a medium level of detail, for all automatically defined cluster-sender channels.

**ALTER QMGR STATINT(900)**

Change the statistics interval to 900 seconds (15 minutes) from the default of 1800 seconds (30 minutes).

## Guide for action

Use the information in the MQI Statistics workspaces to review the messages that are used to record information about the activities occurring in a WebSphere MQ system.

The information that is contained in statistics messages can be used for the following purposes:

- Account for application resource use
- Record application activity
- Plan capacity
- Detect problems in your queue manager network
- Assist in determining the causes of problems in your queue manager network
- Improve the efficiency of your queue manager network
- Familiarize yourself with the running of your queue manager network
- Confirm that your queue manager network is running correctly

Use the MQI Statistics workspaces to review the following items:

- MQI statistics data for a queue manager, which includes all queues
- New statistics data for individual queues within a queue manager
- Data of channels within a queue manager

---

## MQSeries Events workspaces

The MQSeries Events workspaces provide information about the following six events for each monitored queue manager:

- Channel Stopped
- Queue Full
- Queue Depth High
- Queue Service Interval High
- Bridge Stopped
- Channel Not Activated

These events require prompt resolution. The statistics are reported for local queue managers (managers that belong to the system that WebSphere MQ Monitoring agent is monitoring) and for remote queue managers. To have events reported for remote queue managers, you must define the event queues of these remote queue managers to be local to the system that WebSphere MQ Monitoring agent is monitoring.

The Event Log workspace provides a log of all recent events that are produced by the queue manager in monitored event queues. For both workspaces to have data, WebSphere MQ must be enabled for the various types of events, and the monitoring agent parameters must be properly set to capture the events. See “SET GROUP” on page 26 and “SET MANAGER” on page 29 for information about how to set these parameters to capture the events.

The Event Archive workspace provides an audit log of events that are recorded historically with detailed data. All the data that is associated with an event is included in a readable XML format attribute. You can see this XML format attribute without linking to anywhere else.

**Remember:** The APPL ID of CICS events that are displayed in the Event Log workspace is always CICS applid and transactions.

Access these workspaces from the **MQSeries Events** item for the selected queue manager in the Navigator physical view.

## Guide for action

Use the information in the MQSeries Events workspace to review the exception conditions that are currently on the event queue. Exception conditions, such as Queue Full, Channel Stopped, and other conditions, continue to be reported in this workspace until another condition occurs and resets them. For example, a Queue Service Interval High condition continues to be reported in this workspace until a Service Interval OK event occurs for that queue.

Events can occur on the local queue manager or on any remote queue manager, only if the following things are true:

- The remote queue manager supports events.
- Events are activated and enabled on the remote queue manager or local queue manager.
- The system event queues in the remote queue manager are defined as remote.
- The system event queues for the remote queue manager are local to a monitored queue manager.

To maintain good performance, investigate the problems that are displayed on these workspaces. Look for patterns in time of day, day of week, and resource that are used. You can use the information in the Event Parameters workspace to review more detailed information about a specific event. The data displayed in this workspace varies depending on the event.

## Searching for WebSphere MQ events

In the Event Archive workspace, you can use the search function to search for specific archived WebSphere MQ events that are reported to the selected queue manager.

Before you can use the search function in the Event Archive workspace, enable historical data collection for the Event Archive attribute group.

To search for specific WebSphere MQ events, do the following steps:

1. Navigate to the Event Archive workspace.
2. Right-click any row in the Event Archive table and click **MQ Event Search**. The Event Archive by Search window opens.
3. Specify the search criteria in the **Conditions** section. You can set a search condition for the following attributes:
  - Event (The name of the WebSphere MQ event)
  - Event MQ Host Name (The name of the host where the event occurred)
  - Event MQ Manager Name (The name of the queue manager on which the event occurred)
  - Resource Name (The name of the WebSphere MQ resource that the event occurred on, such as a queue or channel name)
    - a. In the leftmost field, select the check box that is next to the attribute name.
    - b. In the middle field, select the comparison operator to use for the attribute.
    - c. In the rightmost field, enter the value to use against the data that you are searching for.
4. Optional: To search for the WebSphere MQ events that occur in a certain period of time, enter the search criteria in the **Search Option** section.
  - a. In the leftmost field, select the check box.
  - b. In the middle field, enter an integer in the range of 1 - 31.
  - c. In the rightmost field, select the time unit, hour, day, or month.
5. Click **Search**.

After the search is completed, the search results replace the original data in the workspace.

---

## Page Set Statistics workspaces (z/OS systems only)

These workspaces provide information about the uses and allocation of page sets for each monitored queue manager on a z/OS system.

Access these workspaces from the **Page Set Statistics** item for the selected queue manager in the Navigator physical view.

### Guide for action

A queue manager that is running on WebSphere MQ for z/OS systems uses page sets to store object definitions and queue messages. Use the Page Set Statistics workspaces to monitor the following conditions:

- Examine the percentage of pages in use and the total number of pages to ensure that no page sets are reaching capacity.

When a page set is full, applications cannot put messages on a queue that is mapped to that page set. This situation is especially critical when the full page set is the number 0, because all object definitions that are required by the queue manager are stored there.

If a page set is full, expand that page set, or balance the load between page sets by moving queues from one page set to another.

- Examine the number of buffers in the buffer pool that is being used.

If the buffer pool efficiency is poor and a page set is responsible for most of the activity, try increasing the buffer pool size or assigning that page set to another buffer pool.

---

## Publish Subscribe workspaces

The Publish Subscribe workspaces provide the information for monitoring the WebSphere MQ publish and subscribe environment. The Topic Status workspace provides information about the root level of topic nodes. The Topic Definitions workspace provides information about all system-defined topics. The Subscriptions Definitions workspace contains the information about all system-defined subscriptions. The Enterprise Wide Subscription Definitions workspace contains information about all system-defined remote and local subscriptions.

Access these workspaces from the **Publish Subscribe** item in the Navigator physical view.

**Tip:** If you want to include Publish Subscribe in the Navigator logical view for a MQSERIES agent, the agent node of higher level should also be included in the Navigator tree; otherwise, some dynamic workspace link cannot work.

### Guide for action

Use the information in the Publish Subscribe workspaces to monitor your WebSphere MQ publish and subscribe environment by performing the following tasks:

- Use the search function to search for specific topic string, topic name, and subscription name information.
- Use the subscription topology view in the Publish Subscribe workspaces to get a clear overview of a particular topic and the subscriptions associated with it.
- Prevent the destination queues that are used by subscriptions from overflowing.

For detailed instructions about how to perform these tasks, see Chapter 8, “Monitoring the publish and subscribe environment,” on page 97.

---

## Queue Definitions workspaces

The Queue Definitions workspaces provide information about the queues that are defined in the queue manager. The Real-time Queue Definitions and Real-time Queue Definitions for Queues with Messages workspaces contain on-demand data that is collected in real time when the workspaces are opened or refreshed, note that if you have many queues defined, the real-time workspace can have a slow response time, and consume more resources to retrieve the data. Other Queue Definitions workspaces contain sampled data.

Access these workspaces from the **Queue Definitions** item for the selected queue manager in the Navigator physical view.

The Queue Definitions Summary chart that is contained in the Real-time Queue Definitions and Real-time Queue Definitions for Queues with Messages workspaces does not necessarily match the data displayed in the table at the bottom of this workspace. It is intended only to give an overview of data that is sampled at the queue manager level according to the current parameters of the agent. The data displayed in the table is on-demand data, collected when the workspace is opened or refreshed, whereas the data on which the chart is based is sampled during standard sampling intervals.

## Guide for action

Use the information in the Queue Definitions workspaces to compare queue definitions among your monitored queue managers.

The following application and system queue characteristics must be defined to WebSphere MQ:

- Whether applications can retrieve messages from the queue
- Whether applications can put messages on the queue
- Whether access to the queue is exclusive or shared
- The maximum number of messages that can be stored on the queue
- The maximum length of messages that can be put on the queue

Application queues can be local, alias, or model. System queues can be initiation, transmission, channel, dead-letter, system-command input, event, or system default.

**Remember:** On z/OS systems, the alias queue and the remote queue are considered as predefined queues by default and therefore are displayed in this workspace. To display the model queue in this workspace, the **QDEFTYPE** parameter must be specified with the value of PREDEFINED.

---

## Queue Manager Status workspaces

These workspaces display the status of the monitored queue managers in your network and give basic descriptive information about each monitored queue manager. Workspaces in this area also report on application connections to the queue manager and listener status.

Access these workspaces from the **Queue Manager Status** item for the selected queue manager in the Navigator physical view.

**Tip:** To include Queue Manager Status in the Navigator logical view for a MQSERIES agent, include the agent node of higher level in the Navigator tree; otherwise, some dynamic workspace link cannot work.

## Guide for action

Use the information in the Queue Manager Status workspaces to compare the status and activity of your queue managers and to look for patterns in resource usage, status, or time of day.

Check the following factors:

- Dead-letter queue depth
- The status of each queue manager (Active, Queue Manager Not Available, Command Server Not Responding, Dynamic Queue Allocation Error, Cluster Repository Not Available, Standby, Running Elsewhere)

**Note:** Standby and Running Elsewhere apply to multi-instance queue managers only.

**Remember:** The time and date that the queue manager is started are available on UNIX, Linux, and z/OS systems only.

## Application topology view

The Application Topology view in the Application Connections workspace provides a graphical representation of connections between the monitored queue manager, the applications that are connected to it, and the queues that are opened by the applications.

In the navigator view, you can access the Application Connections workspace by right-clicking the **Queue Manager Status** node and clicking **Workspace > Application Connections**.

See Table 14 for information about the icons that are used to represent queue managers, applications, and queues:

Table 14. Icons used in the Application Topology view

Resource type	Icon
Application	
Queue	
Queue manager	

The Application Topology view can be displayed in the following modes:

- “Mode 1: Compact mode for application connections”
- “Mode 2: Drill-down mode for an application connection” on page 138
- “Mode 3: drill-down mode for all application connections” on page 139
- “Mode 4: browse mode for connections to a queue” on page 140

### Mode 1: Compact mode for application connections

By default, when you open the Application Connections workspace, the Application Topology view only displays connections between the monitored queue manager and applications that are connected to it, as shown in Figure 16 on page 138. This is called the compact mode for application connections. You can see how many application connections are active by examining the Application Topology view in this mode.

The top node in this view represents the monitored queue manager, labeled with the name of the queue manager. The second tier contains applications that are connected to it, labeled with the name of each application.

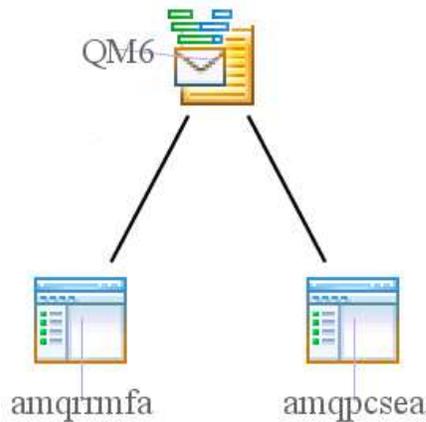


Figure 16. Compact mode for application connections

**Tip:** When the Application Topology view is running in compact mode for application connections, the name of the monitored queue manager is displayed in the workspace footer.

## Mode 2: Drill-down mode for an application connection

To view connections between a specific application and the queues that it opens, in addition to its connection to the monitored queue manager, in the Application Topology view, right-click the application node, and click **Link To > Application Topology for Selected Application**. The connection between the monitored queue manager and the selected application, and connections between the selected application and all the queues that it opens are displayed in the Application Topology view. This is called the drill-down mode for an application connection.

If any of the queues that are opened by the selected application are also opened by other applications, connections between these applications and the queues are also displayed, regardless of the type of application. Connections between these applications and other queues that are opened by them are not displayed.

In this mode, the Application Topology view looks similar to Figure 17 on page 139, which displays the connection between the selected application and the queue manager that it connects to, and the connections between the application and the queues that it opens.

The topmost node represents the queue manager that the selected application connects to, labeled with its name. The second tier contains the selected application and other applications if they are using the queues that are opened by the selected application, labeled with the name of each application. The third tier contains queues that are opened by the selected application, labeled with the name of each queue.

If the application that you want to select is not displayed as a node in the Application Topology view, you can right-click it in the Application Connections table of the Application Connections workspace, and click **Link To > Application Topology for Selected Application**.

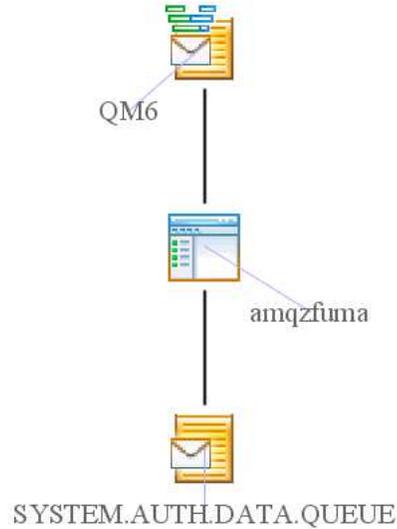


Figure 17. Drill-down mode for an application connection

**Tip:** When the Application Topology view is in drill-down mode for an application connection, the name of the selected application is displayed in the workspace footer.

**Remember:** The **Application Topology for Selected Applications** link is designed to support the application node only. If you right-click a node other than the application node to access the Application Topology view in this mode, the last accessed application node is used to present the Application Topology view.

### Mode 3: drill-down mode for all application connections

In the drill-down mode for all application connections, connections between the monitored queue manager and the applications that are connected to it, and connections between these applications and the queues that are opened by them are displayed in the Application Topology view.

To access the Application Topology view in this mode, in the Application Topology view, right-click any application node or the monitored queue manager node, and click **Link To > Application Topology for All Applications**.

With all application connections displayed in the Application Topology view, you can get a clear overview of the whole application topology. However; if there is a large number of application connections, especially when the **MaxRow\_AppTop** parameter is set to a value larger than the default, updating the Application Topology view is time-consuming. For information about the **MaxRow\_AppTop** parameter, see “Controlling the number of displayed connections” on page 140.

In this mode the Application Topology view looks similar to Figure 18 on page 140:

The topmost node represents the monitored queue manager, labeled with its name. The second tier contains the applications that are connected to it, labeled with the name of each application. The third tier contains the queues that are opened by these applications, labeled with the name of each queue.

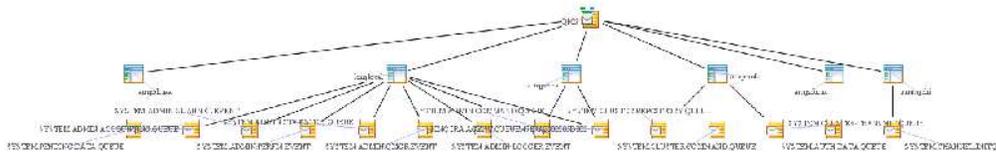


Figure 18. Drill-down mode for all application connections

#### Mode 4: browse mode for connections to a queue

In the browse mode for connections to a queue, connections between a specific queue and all the applications that open it are displayed in the Application Topology view.

To access the Application Topology view in this mode, do one of the following steps:

- In the Application Topology view, right-click a queue node, and click **Link To > Application Topology for Selected Queue**.
- In the table view of the Real-time Queue Definitions or Queue Status workspace, right-click a row, and click **Link To > Application Topology**.

In this mode the Application Topology view looks similar to Figure 19:

The first tier contains the applications that open the selected queue, labeled with the name of each application. The bottom node represents the selected queue, labeled with its name.

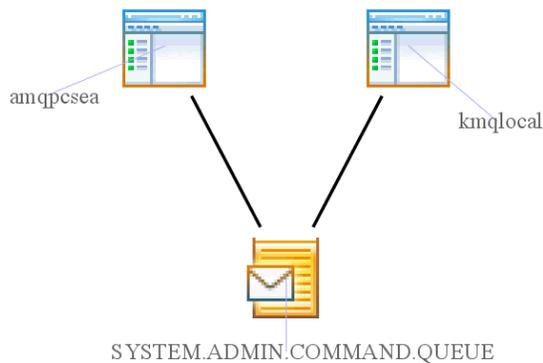


Figure 19. Browse mode for connections to a queue

**Tip:** When the Application Topology view is in the browse mode for connections to a queue, the name of the selected queue is displayed in the workspace footer.

#### Controlling the number of displayed connections

The `MaxRow_AppTop` parameter is used to control the maximum number of rows that are returned by the WebSphere MQ Monitoring agent to draw the nodes and connections in the Application Topology view. Change the value if you want more or fewer connections and nodes to be displayed.

Remember that the default value of **MaxRow\_AppTop** parameter is 200. If this parameter is set to a value greater than the default value, the Application Topology view might take a long time to refresh.

**Tip:**

- If the application topology that is displayed in the Application Topology view is incomplete, in other words, if there are nodes with no connection to other nodes or connections with a node at only one end, increase the value of the **MaxRow\_AppTop** parameter.
- It is not recommended to change the default value. If the **MaxRow\_AppTop** parameter must be changed, change the value with a user ID other than SYSADMIN.

Do the following steps to change the value of the **MaxRow\_AppTop** parameter.

1. In the Application Topology view, right-click a node; then click **Link to > Link Wizard**.
2. Select **Modify an existing link** in the Workspace Link Wizard - Welcome window, and click **Next**, as shown in Figure 20.

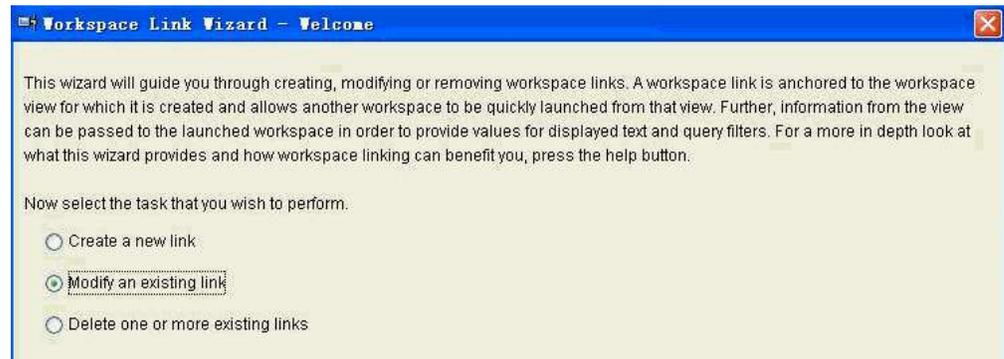


Figure 20. Workspace Link Wizard - Welcome

3. Select the link that you want to modify in the Workspace Link Wizard - Link to Modify window and click **Next**. For example, if you want to change the maximum number of rows that are returned for Application Topology for All Applications, select Application Topology for All Applications, as shown in Figure 21.

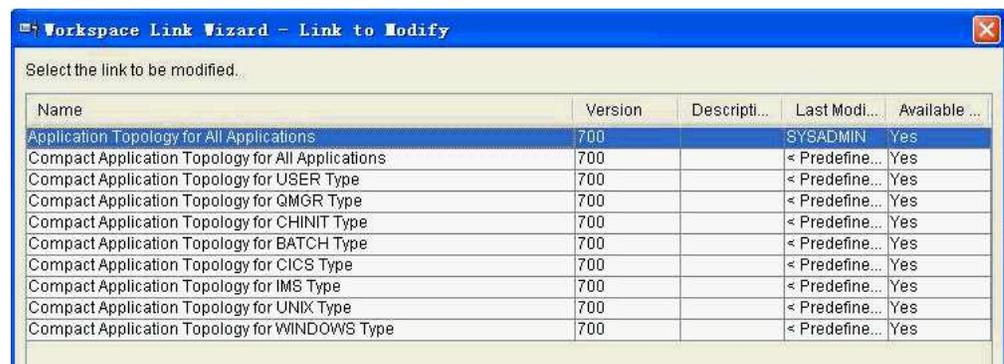


Figure 21. Workspace Link Wizard - Link to Modify

4. In the Workspace Link Wizard - Link Name window, click **Next** without changing the name of the link.
5. In the Workspace Link Wizard - Parameters window, click the plus sign (+) next to **TargetWorkspace**, as shown in Figure 22.

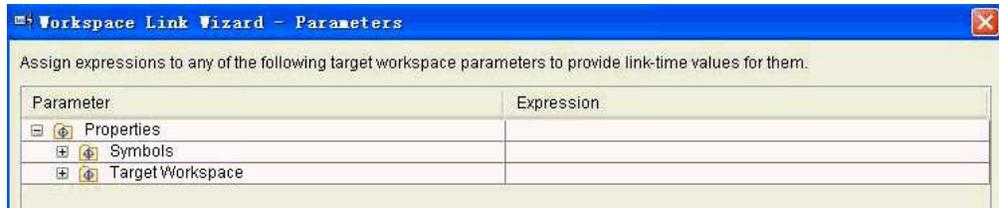


Figure 22. Workspace Link Wizard - Parameters

6. In the Workspace Link Wizard - Parameters window, click the plus sign (+) next to **Query - Application Topology** under **TargetWorkspace**.
7. In the Workspace Link Wizard - Parameters window, click the plus sign (+) next to **Symbols** under **Query - Application Topology**.
8. In the Workspace Link Wizard - Parameters window, double-click **MaxRow\_AppTop**, as shown in Figure 23:

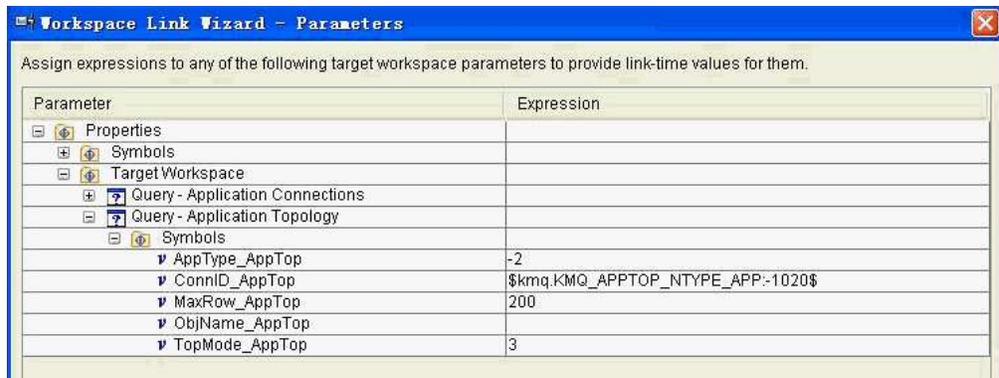


Figure 23. Workspace Link Wizard - Parameters

9. In the Expression Editor window, change the value of **MaxRow\_AppTop**, and click **OK**.
10. In the Workspace Link Wizard - Parameters window, click **Next**.
11. Review the changes in the Workspace Link Wizard - Summary window, as shown in Figure 24 on page 143, and click **Finish**.



Figure 24. Workspace Link Wizard - Summary

You do not need to restart the agent for the change to take effect. The value of the **MaxRow\_AppTop** parameter applies to all instances of the WebSphere MQ Monitoring agent.

### Predefined links in the Application Topology view

Predefined links are available at the queue manager, application, and queue nodes in the Application Topology view. Use them to view the Application Topology view that contains the information you want.

**Predefined links at the queue manager node:** The following links are predefined for the queue manager node:

- Compact Application Topology for All Applications
- Compact Application Topology for USER Type
- Compact Application Topology for UNIX Type
- Compact Application Topology for WINDOWS Type
- Compact Application Topology for BATCH Type
- Compact Application Topology for CICS Type
- Compact Application Topology for IMS Type
- Compact Application Topology for QMGR Type
- Compact Application Topology for CHINIT Type
- Application Topology for All Applications

For example, if the currently displayed Application Topology view displays connections between the monitored queue manager and all applications but you want to view only connections between the queue manager and Windows system applications, you can right-click the queue manager node, and click **Link To > Compact Application Topology for WINDOWS Type**. After the Application Topology view refreshes, it contains only connections between the queue manager and Windows system applications.

To view connections between the queue manager and all types of applications as well as connections between applications and the queues that are opened by them, right-click the queue manager node, and click **Link To > Application Topology for All Applications**.

To view connections between the monitored queue manager and a certain type of application that is not listed in the predefined links, create your own link using the predefined links as a template.

**Predefined links at the application node:** The following links are predefined for the application node:

- Application Topology for All Applications
- Application Topology for Selected Application
- Compact Application Topology for All Applications
- Compact Application Topology for USER Type
- Compact Application Topology for UNIX Type
- Compact Application Topology for WINDOWS Type
- Compact Application Topology for BATCH Type
- Compact Application Topology for CICS Type
- Compact Application Topology for IMS Type
- Compact Application Topology for QMGR Type
- Compact Application Topology for CHINIT Type
- Connection Objects

To view connections between a specific application and the queues that it opens, in addition to its connection to the monitored queue manager, in the Application Topology view, right-click the application node, and click **Link To > Application Topology for Selected Application**.

To view detailed information about connections of the selected application, right-click the application node, and click **Link To > Connection Objects**.

**Predefined links at the queue node:** The following links are predefined for the queue node:

- Application Topology for Selected Queue
- Queue Messages
- Queue Parameters
- Queue Status

To view the status of a specific queue, right-click the queue node, and click **Link To > Queue Status**. The Queue Status workspace displays the status of the selected queue.

To view connections between a specific queue and all the applications that are connected to it, right-click the queue node, and click **Link To > Application Topology for Selected Queue**.

To view the messages on a specific queue, right-click the queue node, and click **Link To > Queue Messages**.

---

## Queue Statistics workspaces

The Queue Statistics workspaces provide usage information about all monitored queues and queue managers (such as the number of open queues, how full they are, whether messages are prohibited from being put into or got out of the queues, and the number of messages currently on the dead-letter queue of each queue manager). Alternative Queue Statistics workspaces include the Queue Status, Open

Queue Handles, Real-Time Queue Data for Queues with Messages, and Real-Time Queue Data for Open Queues workspaces. They provide the most current, on-demand real time information about queues in the queue manager. Note that if you have many queues, the real-time workspace can have a slow response time, and consume more resources to retrieve the data.

The Queue Statistics workspace is the default top-level workspace. You can access it from the **Queue Statistics** item for the selected queue manager in the Navigator physical view.

Both the Queue Statistics and Queue Statistics for Monitored Temporary Dynamic Queues workspaces do not contain information that is related to model queues. This is because model queues are templates from which queues can be created, not physical queues about which statistics can be collected.

The Queue Statistics Summary chart that is contained in these workspaces does not necessarily match the data that is displayed in the table at the bottom of this workspace. It is intended only to give an overview of sampled data at the queue manager level according to the current parameters of the agent. The data that is displayed in the table represents only a subsection of collected data, whereas the data that is displayed in the chart provides a summary of all sampled data.

## Purging a local queue

You can delete all messages from a local queue in the Queue Statistics workspace.

**Remember:** If there is uncommitted messages in the queue, these messages will not be deleted.

Perform the following steps to delete all messages from a local queue in the Queue Statistics workspace:

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on a specific operating system.
2. Add the following command to the monitoring file to allow deletion of messages from the queue:  

```
SET QACCESS NAME(queue_name) MSGACCESS(DELETE) MGRNAME(qmgr_name)
```

where *queue\_name* is the name of the queue whose messages you want to delete and *qmgr\_name* is the name of the queue manager that the queue belongs to.
3. Restart the WebSphere MQ Monitoring agent for the changes to take effect.
4. Click **Queue Statistics** in the Navigator physical view to open the Queue Statistics workspace.
5. In the **Queue Statistics for Monitored Queues with Messages** table, right-click the row that corresponds to the queue whose messages you want to delete, and click **Purge Queue (MQGET)**. A message is displayed, asking if you want to purge all messages from the selected queue.
6. Click **Yes**.

All the messages on the queue are deleted.

## Clearing a local queue

You can clear a local queue in the Queue Statistics workspace.

**Remember:** You cannot clear a queue and get an error message in the following circumstances:

- There are uncommitted messages that have been put on the queue under syncpoint.
- An application currently has the queue open.

To avoid this error, use the Purge Queue option to delete messages from a local queue (see “Purging a local queue” on page 145). When you purge a queue, the message is gotten and deleted one by one. The message, which cannot be deleted, will be discarded.

Do the following steps to delete all messages from a local queue in the Queue Statistics workspace:

1. Open the monitoring file of the WebSphere MQ Monitoring agent. See “Changing monitoring options” on page 14 for information about how to open the monitoring file on a specific operating system.
2. Check the value of the ACTIONACCOUNT monitoring option in the monitoring file:
  - If the value is UIUSER, which indicates that the WebSphere MQ Monitoring agent uses the Tivoli Enterprise Portal user ID to interact with WebSphere MQ, ensure that this user ID matches one of the user name mask lists in the ACTIONAUTHUSERS monitoring option.
  - If the value is MQAGENT or USER = *user\_id*, where *user\_id* is a predefined user ID, go to step 4.
3. Restart the WebSphere MQ Monitoring agent for the changes to take effect.
4. Click **Queue Statistics** in the Navigator physical view to open the Queue Statistics workspace.
5. In the **Queue Statistics for Monitored Queues with Messages** table, right-click the row that corresponds to the queue that you want to clear, and click **Clear Queue**. A message is displayed, asking if you want to clear all messages from the selected queue.
6. Click **Yes**.

## Guide for action

Use the Queue Statistics workspaces to compare activity and parameter definitions among your queues. Look for activity and usage trends.

To maximize message integrity, you must minimize dead-letter queue depth. Determine how many open queues you have and review their patterns of activity. Also, check to determine how many undeliverable messages fell into the dead-letter queue.

The following issues can adversely affect performance:

- Lengthy logical units of work
- A CICS transaction or a program that is consuming resources

You can use the SCAN and STR functions with the Queue Name column of the Queue Status attribute group. You can create workspaces based on queries that include only queues with names containing certain strings, such as those that include the word SYSTEM. In addition, you can use these functions to create a situation that can be triggered by the same subset of queues, instead of creating a new situation for each queue that you want to trigger the situation.

For example, to create a situation that can be triggered by any queue with a name field beginning with SYSTEM and a depth exceeding 100 messages, use the following formula.

```
IF STR(Queue_Name) == 1, SYSTEM AND Current_Depth > 100 THEN [situation event occurs]
```

Because the performance overhead of these functions is relatively high, when creating a query, include additional filtering thresholds to reduce the number of times these functions are used. In particular, if you are creating your own query, you can include a condition that includes only queues with a current depth attribute of greater than zero, eliminating all queues that do not currently contain messages. The default query already includes this condition.

To create a new version of the queue status workspace containing only a filtered subset of the queues that are listed in the original workspace, do not modify the original workspace and the queries on which it is based. Instead, create copies of both the workspace and query, and modify the copies. The query must be copied because the original query is read-only and cannot be modified. Predefined workspaces that are included with the WebSphere MQ Monitoring agent must not be modified, because this causes problems when upgrading to future versions.

For more information about using the SCAN and STR functions, see the Formula functions appendix in the *IBM Tivoli Monitoring User's Guide*.

---

## Queue-Sharing Group workspaces (z/OS systems only)

Access these workspaces from the **Queue-Sharing Group** item (at the same level as the MQSERIES item) in the Navigator physical view tree.

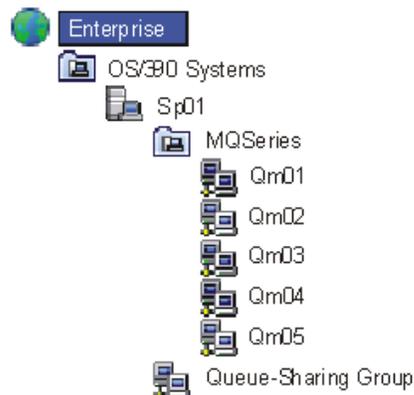


Figure 25. Access QSG workspaces from the Queue-Sharing Group item

See “Queue-Sharing Group Monitoring (z/OS systems only)” on page 148.

### Guide for action

Use the information in the Queue-Sharing Group workspaces to examine the following items:

- The status of each queue manager in the queue-sharing group
- The status of the Coupling Facility (CF) application structures that store the essential data of the queue-sharing group. You can also see the date and time that these CF application structures were last backed up

- The status of shared queues and channels that are used by the queue-sharing group

## Queue-Sharing Group Monitoring (z/OS systems only)

Use the Queue-Sharing Group monitoring feature to monitor and display data that is unique to WebSphere MQ queue managers in a sysplex. The queue managers must be configured to form queue-sharing groups.

This feature provides workspaces on z/OS systems only, provides additional Queue Statistics attributes for use in situations, and provides data for predefined situations (named in the form **MQSeries\_QSG\_\***).

For details about attributes, predefined situations, and workspaces that are provided with WebSphere MQ Monitoring agent, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help. For a navigational introduction to the Queue-Sharing Group workspaces, see “Queue-Sharing Group workspaces (z/OS systems only)” on page 147.

If no queue-sharing groups that are associated with your queue managers, you cannot use the Queue-Sharing Group Monitoring feature.

To successfully monitor queue-sharing groups, install a WebSphere MQ Monitoring agent on the host system of each queue manager that participates in the queue-sharing group, and ensure that the agent is configured to monitor those queue managers.

The default behavior of the agent is to monitor *all* queue-sharing groups that are associated with monitored queue managers. You can modify the default, if necessary (see the **SET QSG** monitoring option and the **QSGCHKINTERVAL** and **GRPNAME** parameters of the “PERFORM STARTMON” on page 48 monitoring option). Also, use the same sample interval length for all WebSphere MQ Monitoring agents that monitor queue managers in queue-sharing groups (see the **SAMPINT** parameter of the “PERFORM STARTMON” on page 48 monitoring option).

For information about queue-sharing groups see *IBM WebSphere MQ for z/OS System Concepts and Planning Guide*.

---

## Queue Messages workspace

Use Queue Messages workspaces to do the following things:

- Display queue contents.
- List queued messages.
- Display message descriptor information.
- Display message application data (that is, message contents).
- Delete messages.
- Forward messages to other queues.

With these tools, you can balance queue usage, test and debug applications, and delete obsolete messages.

Access these workspaces from the **Queue Definitions** item (or from the Queue Statistics item) for the selected queue manager in the Navigator physical view.

To access the Queue Messages workspace, from the top-level Queue Definitions workspace, right-click a table row and select **Link To**.

For the complete list of predefined workspaces that are included with this product, see the WebSphere MQ Monitoring agent section of the Tivoli Enterprise Portal online help.

## Guide for action

Whether you can access messages in the Queue Messages workspaces to perform the described actions that follow depends on certain parameter settings. See “Settings for controlling access to WebSphere MQ messages” on page 89.

Use the Queue Messages workspace to get detailed information about the messages, to delete a message from a queue, or to forward a message to another queue.

After you confirm a message deletion or forwarding operation, a return code and a message are displayed. The value 0 indicates a successful completion. A nonzero value indicates a problem. The workspace is automatically refreshed after you delete or forward a message. For an explanation of nonzero return codes, see *IBM WebSphere MQ Application Programming Reference*.

For detailed instructions about how to delete messages, see “Deleting a message from a queue.”

For detailed instructions about how to forward messages, see “Forwarding a message to another queue.”

## Deleting a message from a queue

Use the Queue Messages workspace to delete a message from the selected queue.

Before you open the workspace, make sure that the WebSphere MQ Monitoring agent is running.

Do the following steps to delete a message from the selected queue:

1. Open the Queue Messages workspace.
2. Right-click the message that you want to delete, and click **Delete**.  
A confirmation message showing the current queue and current queue manager is displayed.
3. To delete the message that has parameters matching those in the confirmation message, click **Yes**.

The matching message is deleted. The status of your delete request is displayed; click **OK** to clear the status message.

**Important:** If you delete a segmented or grouped message, WebSphere MQ Monitoring agent deletes the entire logical message.

## Forwarding a message to another queue

From the Queue Messages workspace, you can forward a message on the selected queue to a destination queue that you specify.

Before you open the workspace, make sure that the WebSphere MQ Monitoring agent is running.

The message can be forwarded to a queue on any queue manager that is known to the WebSphere MQ system.

1. In the Queue Messages workspace, right-click the message that you want to forward, and click **Forward**.
2. You are prompted for the destination queue and queue manager. Complete the following fields:
  - In the **Queue** field, enter the name of the queue to send the message to.
  - In the **Queue manager** field, enter the name of the queue manager for the queue that you specified in the **Queue** field.
3. Click **Yes**. The message is forwarded to its destination queue. The status of your forward request is displayed; click **OK** to clear the status message.

**Important:** If you forward a segmented or grouped message, WebSphere MQ Monitoring agent forwards the entire logical message.

---

## Topic Manager Performance workspaces(z/OS systems only)

The Topic Manager Performance workspaces provide information about the publication and subscription activities (such as how frequently subscriptions are made and how many subscriptions are expired ) for each monitored z/OS system queue manager.

Access the top-level workspace from the **Topic Manager Performance** item for the selected queue manager in the Navigator physical view.

### Guide for action

Use the information in the Topic Manager Performance workspaces to monitor recent and long-running publications and subscription activities for a particular z/OS system queue manager from the following items:

- Subscription and publication rate per second
- Number range of subscriptions and publications
- The number of expired subscriptions
- The maximum number of subscriptions for a specific publication and the number of publications that have no subscribers
- Time performing the publication request

---

## Additional workspace information

With Queue Statistics, Queue Definitions, Channel Performance, and Channel Definitions workspaces, if there are too many queues or channels, they are listed in an unsorted order. You can use the sort function only on the current page for the Tivoli Enterprise Portal table. To easily find the queue that you want to work with, you can set those queues in the mq.cfg file.

**Exception:** Some attributes are not available for WebSphere MQ 5.3. Unavailable numerical attributes are displayed as "n/a" in the table view and "-1" in the chart view of the workspaces.

---

## Chapter 11. Configuring in a cluster environment on Windows systems

You can configure the WebSphere MQ Monitoring agent to run in a Microsoft Cluster Service (MSCS) cluster environment on Windows systems. The WebSphere MQ Monitoring agent supports both active/active and active/passive clustering. If you are configuring the agent in an active/active cluster environment, see “Active/active clustering” on page 152 for instructions. If you are configuring the agent in an active/passive cluster environment, see “Active/passive clustering” on page 157 for instructions.

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**

MSCS clusters are groups of two or more 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 starting their operation 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.

---

## Introducing MSCS clusters

By using the Microsoft Cluster Service (MSCS), you can 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.

MSCS supports failover of virtual servers, which correspond to applications, Web sites, print queues, or file shares (including their disk spindles, files, IP addresses, and other items).

Looking at a two-computer cluster. A two-computer cluster comprises two computers (for example, A and B) that are jointly connected to a network for client access using a virtual IP address. They might also be connected to each other by one or more private networks. A and B share at least one disk for each of the two computers to use for server applications. There is also another shared disk, which must be a redundant array of independent disks (RAID) Level 1, for the exclusive use of MSCS; this is known as the quorum disk. MSCS monitors both computers to check that the hardware and software are running correctly.

In a setup such as this, both computers have all the applications installed on each of them, but only computer A runs with live applications; computer B is just running and waiting. If computer A encounters any one of a range of problems, MSCS shuts down the disrupted application in an orderly manner, transfers its

state data to the other computer, and starts the application there. This is known as a failover. Applications can be made cluster-aware so that they interact fully with MSCS and failover smoothly.

A typical setup for a two-computer cluster is as shown in Figure 26.

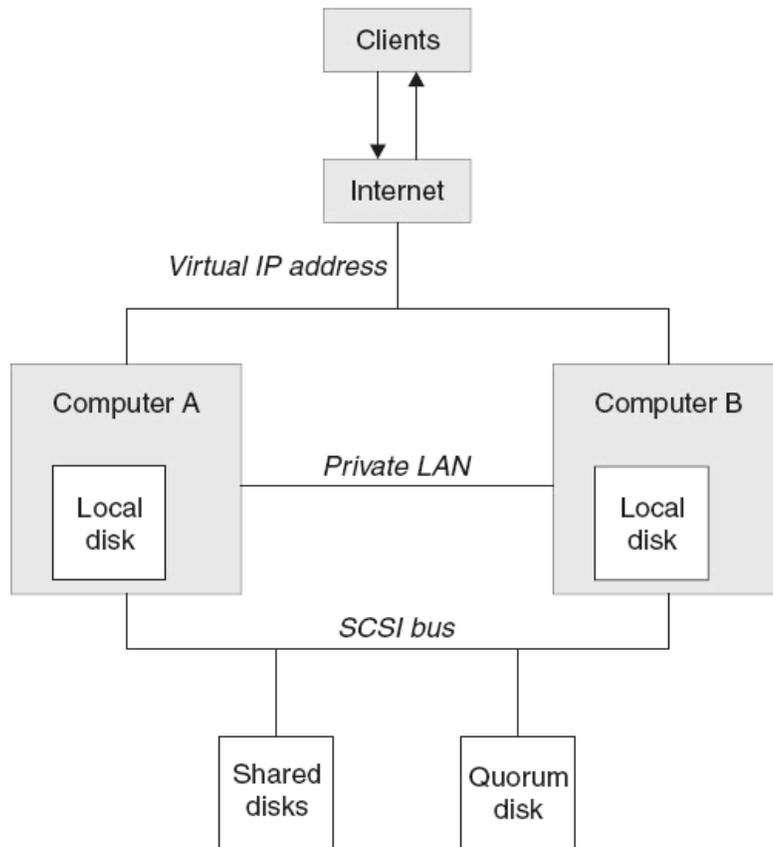


Figure 26. A two-computer MSCS cluster

Each computer can access the shared disks, but only one at a time, under the control of MSCS. In the event of a failover, MSCS switches the access to the other computer. The shared disk itself is usually a RAID, but need not be.

Each computer is connected to the external network for client access, and each has an IP address. However an external client, communicating with this cluster, sees only one virtual IP address, and MSCS routes the IP traffic within the cluster appropriately.

MSCS also performs its own communications between the two computers, either over one or more private connections or over the public network, in order to monitor their states using the heartbeat, synchronize their databases, and to do other things.

---

## Active/active clustering

Configure the WebSphere MQ Monitoring agent to run in an active/active environment.

## Prerequisites

Before you begin configuring the WebSphere MQ Monitoring agent to run in a cluster environment, ensure that the two systems that host the WebSphere MQ Monitoring agents are correctly configured. Ensure that both systems meet 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 used MSCS to configure both systems as cluster nodes.
- WebSphere MQ is installed and configured to run in a domain environment. See your WebSphere MQ documentation for information about how to install WebSphere MQ in a cluster environment.
- Queue managers to be monitored are created.
- The IBM Tivoli Monitoring framework is installed. This must be installed separately on both cluster nodes. For instructions about how to install IBM Tivoli Monitoring in a cluster environment, see your IBM Tivoli Monitoring documentation.
- The WebSphere MQ Monitoring agent version 7.0 or later is installed. This must be installed separately on both cluster nodes. See *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for installation instructions.

Also ensure that you have two separate logical drives in the cluster environment that are available for storing log and historical data that is collected from the agents. These drives are referenced as drives R and S in the following procedure.

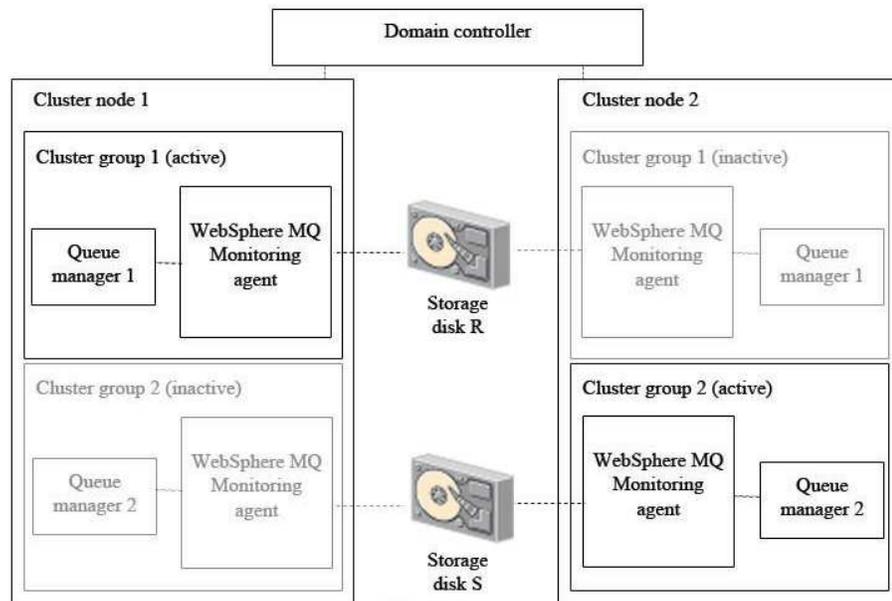


Figure 27. An example cluster environment architecture with one cluster group active on each cluster node

An example of a cluster environment is shown in Figure 27. 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 between them there are two identical copies of cluster group 1 and two

identical copies of cluster group 2. Each cluster group contains one queue manager and a single instance of the WebSphere MQ Monitoring agent to monitor the queue manager.

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 27 on page 153), the copy of cluster group 1 on 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 is started 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, such as logs, 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 is started, 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.

## Configuring the WebSphere MQ Monitoring agent

To configure the WebSphere MQ Monitoring agent to run in a cluster environment, complete the following procedure:

**Important:** The following procedure assumes that you have two cluster groups on each cluster node, as this is the most common scenario. If you have more than two cluster groups, create additional instances of the WebSphere MQ Monitoring agent to monitor the queue managers in each additional cluster group.

1. Run the following commands on both cluster nodes to move the configuration information and log files of each queue manager to the R and S drives :

```
hamvmqm /m QM1 /dd "R:\WMQ" /ld "R:\WMQ\log"
hamvmqm /m QM2 /dd "S:\WMQ" /ld "S:\WMQ\log"
```

**Remember:** Make sure that the paths in the commands do not contain any spaces.

2. Run the following command in the *WMQInstall/bin* directory on both cluster nodes to register the **IBM MQSeries MSCS** resource type, where *WMQInstall* is the installation directory of WebSphere MQ:

```
haregtyp.exe /r
```

3. Use the **Cluster Administrator** to add the **IBM MQSeries MSCS** type resource that named QM1 to cluster group 1.
4. Use the **Cluster Administrator** to add the **IBM MQSeries MSCS** type resource that named QM2 to cluster group 2.
5. Create new instances of the WebSphere MQ Monitoring agent by doing the following steps on both cluster nodes:
  - a. Start Manage Tivoli Enterprise Monitoring Services.
  - b. Right-click the WebSphere MQ Monitoring agent, and then click **Create Instance** to create a new instance of the WebSphere MQ Monitoring agent to monitor the QM1 queue manager.
  - c. Enter a name for the instance when prompted. In this procedure, assume that you entered KMQ1. Click **OK**.
  - d. Right-click the KMQ1 instance, and then click **Change Startup**.

- e. In the Service Startup for WebSphere MQ Monitoring Agent window, select **Manual**, and click **OK**.
- f. Right-click the WebSphere MQ Monitoring agent, and click **Create Instance** again to create a second new instance of the WebSphere MQ Monitoring agent to monitor the QM2 queue manager .
- g. Enter a name for the instance when prompted. In this procedure, assume that you entered KMQ2. Click **OK**.
- h. Right-click the KMQ2 instance, and then click **Change Startup**.
- i. In the Startup Type window, select **Manual**, and click **OK**.
- j. Edit the configuration file for the KMQ1 instance to configure it to monitor the queue manager QM1.
- k. Edit the configuration file for the KMQ2 instance to configure it to monitor the queue manager QM2.
- l. Stop the primary instance of the WebSphere MQ Monitoring agent.

**Remember:** Do not use the primary WebSphere MQ Monitoring agent to monitor queue managers in a cluster environment.

- 6. Set local variables by doing the following steps on each cluster node:
  - a. Right-click the KMQ1 instance, and click **Advanced > Edit Variables**.
  - b. In the Override Local Variable Settings window, add the variables in Table 15, which specify where the data that is saved by the KMQ1 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 15. Overriding local variables

Variable	Details
CTIRA_SIT_PATH	The location where situation data is stored.
CTIRA_LOG_PATH	The location where log data is stored.
CTIRA_HIST_DIR	The location where historical data is stored.

For example, you might set the variables as follows:

```
CTIRA_SIT_PATH=R:\WMQ\kmc\QM1\sitpath
CTIRA_LOG_PATH=R:\WMQ\kmc\QM1\logs
CTIRA_HIST_DIR=R:\WMQ\kmc\QM1\logs\History\@CanProd@\@CanTask@
```

This is illustrated in Figure 28 on page 156.

**Remember:**

- 1) Variable paths cannot contain spaces. For example, CTIRA\_LOG\_PATH = R:\Websphere MQ\kmc\log is not valid.
- 2) Each agent must have its own logical drive on which to store data. More than one agent cannot share a single drive.

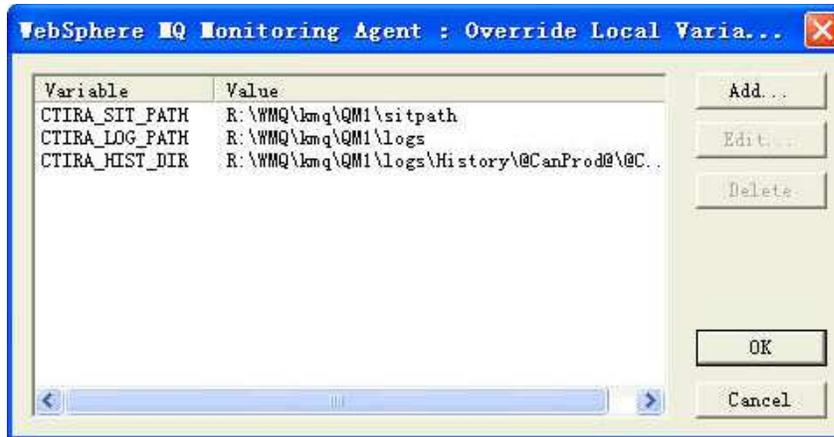


Figure 28. Setting local variables

- c. Click **OK** to close the window.
  - d. Right-click the KMQ2 instance, and click **Advanced > Edit Variables**.
  - e. In the Override Local Variable Settings window, add same variables as specified in step b to specify the location on drive S where you want data saved by the agent KMQ2 to be stored. For example, you might set the variables as follows:
 

```
CTIRA_SIT_PATH=S:\WMQ\kmq\QM2\sitpath
CTIRA_LOG_PATH=S:\WMQ\kmq\QM2\logs
CTIRA_HIST_DIR=S:\WMQ\kmq\QM2\logs\History\@CanProd@\@CanTask@
```
  - f. Click **OK** to close the window.
  - g. Change the start mode of both the KMQ1 and KMQ2 instances to manual startup.
7. Configure the Tivoli Enterprise Portal Server to list agents that are running in cluster groups by cluster name instead of by host system name in Tivoli Enterprise Portal:
    - a. Open Manage Tivoli Enterprise Monitoring Services, and right-click the name of the agent instance.
    - b. Click **Reconfigure**. The `mq.instance_name.cfg` file is opened, where `instance_name` is the name of the agent instance.
    - c. Add the following line at the bottom of the file:
 

```
SET AGENT NAME($cluster_name)
```

 where `cluster_name` is the name of the MSCS cluster.
    - d. If the portal server is running on a Windows system, do the following steps:
      - 1) Stop the portal server if it is running.
      - 2) In the Manage Tivoli Enterprise Monitoring Services window, right-click the Tivoli Enterprise Portal Server icon, and then click **Advanced > Edit Variables**.
      - 3) In the Tivoli Enterprise Portal Server Override Local Variable Setting window, click **Add**.
      - 4) In the **Variable** menu of the Add Environment Setting Override window, look for the **KFW\_TOPOLOGY\_CLUSTER\_LIST** variable. If it exists, append `AFF_MVS_MQM` to any existing values, separated by a space. If it does not already exist, create the variable and set its value to `AFF_MVS_MQM`.

- 5) Reconfigure and recycle the portal server.
- e. If the Tivoli Enterprise Portal Server is running on a UNIX or Linux system, do the following steps:
  - 1) Stop the portal server if it is running.
  - 2) Navigate to the following directory: *ITM\_HOME/config/*, where *ITM\_HOME* is the IBM Tivoli Monitoring installation directory.
  - 3) Open the *cq.ini* file in a text editor.
  - 4) Look for the **KFW\_TOPOLOGY\_CLUSTER\_LIST** parameter. If it already exists, add **AFF\_MVS\_MQM** to any existing values, separated by a space. If the parameter does not already exist, add the following line to the file:  
`KFW_TOPOLOGY_CLUSTER_LIST=AFF_MVS_MQM`
  - 5) Save and close the file.
  - 6) Reconfigure and recycle the portal server.
8. Use **Cluster Administrator** to add a type **Generic Service** resource with the name **KMQ1** to cluster group 1, a **Physical Disk** type resource with the name **R** to cluster group 1, a **Generic Service** type resource with the name **KMQ2** to cluster group 2, and a **Physical Disk** type resource with the name **S** to cluster group 2.
9. 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.
10. Use **Cluster Administrator** to start the queue manager and the WebSphere MQ Monitoring agent in each cluster group .

The configuration of the WebSphere MQ Monitoring agent to monitor queue managers in a cluster environment is completed.

---

## Active/passive clustering

Configure the WebSphere MQ Monitoring agent to run in an active/passive environment.

### Prerequisites

Before you begin configuring the WebSphere MQ Monitoring agent to run in a cluster environment, ensure that the two systems that host the WebSphere MQ Monitoring agents are correctly configured. Ensure that both systems meet 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 used MSCS to configure both systems as cluster nodes.
- WebSphere MQ is installed and configured to run in a domain environment. See your WebSphere MQ documentation for information about how to install WebSphere MQ in a cluster environment.
- Queue managers to be monitored are created.
- The IBM Tivoli Monitoring framework is installed. This must be installed separately on both cluster nodes. For instructions about how to install IBM Tivoli Monitoring in a cluster environment, see your IBM Tivoli Monitoring documentation.
- The WebSphere MQ Monitoring agent version 7.0 or later is installed. This must be installed separately on both cluster nodes. See *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for installation instructions.

Also ensure that you have a separate logical drive in the cluster environment available for storing log and historical data collected from the agents. The drive is referenced as drive R in the following procedure.

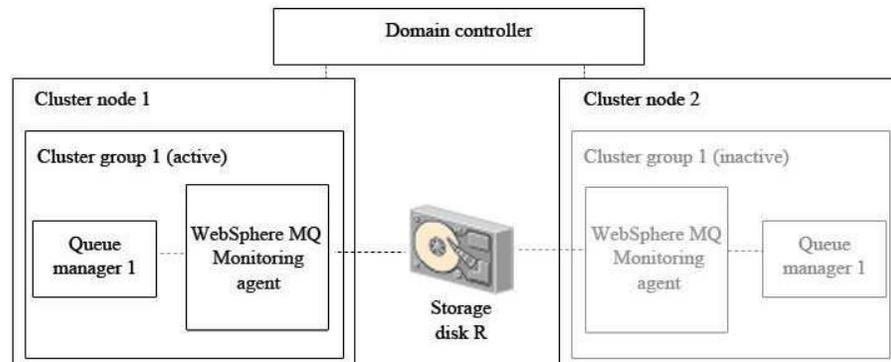


Figure 29. An example cluster environment architecture with a cluster group active on one cluster node and inactive on the other node

An example of a cluster environment is shown in Figure 29. The environment consists of two cluster nodes on separate physical systems. Each cluster node hosts one cluster group (There is no limit to the number of cluster groups that can be hosted by a cluster node). The cluster groups that are hosted by each system are the same, so between them there are two identical copies of cluster group 1. Each cluster group contains one queue manager and a single instance of the WebSphere MQ Monitoring agent to monitor the queue manager.

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 29), 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 is started 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, such as logs, 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 is started, 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 logs and historical information that must be accessed by different copies of the same agent.

## Configuring the WebSphere MQ Monitoring agent

To configure the WebSphere MQ Monitoring agent to run in a cluster environment, do the following steps:

**Important:** The following procedure assumes that you have one cluster group on each cluster node. If you have more than one cluster group, create additional instances of the WebSphere MQ Monitoring agent to monitor the queue manager in each additional cluster group.

1. Run the following command on both cluster nodes to move the configuration information and log files of the queue manager to the drive R:

```
hamvmqm /m QM1 /dd "R:\WMQ" /ld "R:\WMQ\log"
```

**Remember:** Make sure that the paths in the command do not contain any spaces.

2. Run the following command in the *WMQInstall/bin* directory on both cluster nodes to register the **IBM MQSeries MSCS** resource type, where *WMQInstall* is the installation directory of WebSphere MQ:  
haregtyp.exe /r
3. Use the **Cluster Administrator** to add a **IBM MQSeries MSCS** type resource with the name QM1 to cluster group 1.
4. Create a new instance of the WebSphere MQ Monitoring agent by completing the following procedure on both cluster nodes:
  - a. Start Manage Tivoli Enterprise Monitoring Services.
  - b. Right-click the WebSphere MQ Monitoring agent, and click **Create Instance** to create a new instance of the WebSphere MQ Monitoring agent to monitor the QM1 queue manager.
  - c. Enter a name for the instance when prompted. In this procedure, assume that you entered KMQ1. Click **OK**.
  - d. Right-click the KMQ1 instance, and click **Change Startup**.
  - e. In the Startup Type window is displayed. Select **Manual** and click **OK**.
  - f. Edit the configuration file of KMQ1 to configure it to monitor the QM1 queue manager.
  - g. Stop the primary instance of the WebSphere MQ Monitoring agent.

**Remember:** Do not use the primary WebSphere MQ Monitoring agent to monitor queue managers in a cluster environment.

5. Set local variables by doing the following steps on each cluster node:
  - a. Right-click the KMQ1 instance, and click **Advanced > Edit Variables**.
  - b. In the Override Local Variable Settings window, add the variables in Table 16, which specify where data that is saved by the WebSphere MQ Monitoring agent is stored. The value of each variable is the location on the R drive 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_SIT_PATH	The location where situation data is stored.
CTIRA_LOG_PATH	The location where log data is stored.
CTIRA_HIST_DIR	The location where historical data is stored.

For example, you might set the variables as follows:

```
CTIRA_SIT_PATH=R:\WMQ\kmc\QM1\sitpath  
CTIRA_LOG_PATH=R:\WMQ\kmc\QM1\logs  
CTIRA_HIST_DIR=R:\WMQ\kmc\QM1\logs\History\@CanProd\@CanTask@
```

This is illustrated in Figure 30 on page 160.

**Remember:** Variable paths cannot contain spaces. For example, CTIRA\_LOG\_PATH = R:\Websphere MQ\kmc\log is not valid.

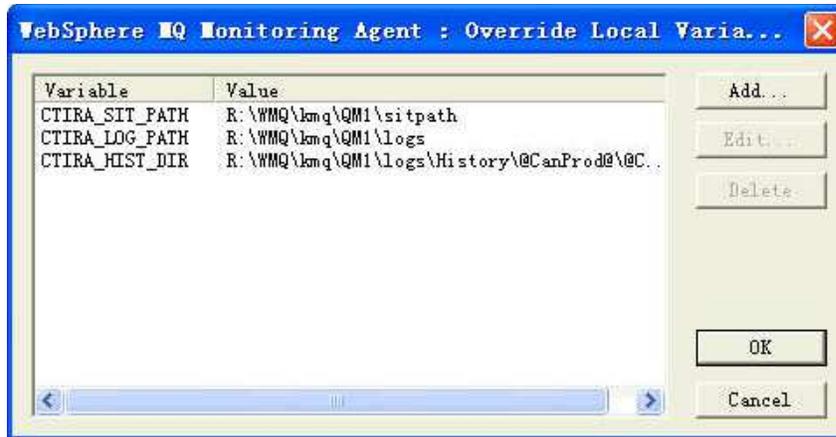


Figure 30. Setting local variables

- c. Click **OK** to close the window.
- d. Change the start mode of the KMQ1 instance to manual startup.
6. Configure the Tivoli Enterprise Portal Server to list agents that are running in cluster groups by cluster name instead of by host system name in Tivoli Enterprise Portal:
  - a. Open Manage Tivoli Enterprise Monitoring Services, and right-click the name of the agent instance.
  - b. Click **Reconfigure** from the displayed menu. The `mq.instance_name.cfg` file is opened, where `instance_name` is the name of the agent instance.
  - c. Add the following line at the bottom of the file:
 

```
SET AGENT NAME($cluster_name)
```

 where `cluster_name` is the name of the MSCS cluster.
  - d. If the Tivoli Enterprise Portal Server is running on a Windows system, do the following steps:
    - 1) Stop the portal server if it is running.
    - 2) In the Manage Tivoli Enterprise Monitoring Service window, right-click the Tivoli Enterprise Portal Server icon, and click **Advanced > Edit Variables**.
    - 3) In the Tivoli Enterprise Portal Server Override Local Variable Setting window, click **Add**.
    - 4) From the **Variable** menu of the Add Environment Setting Override window, look for the **KFW\_TOPOLOGY\_CLUSTER\_LIST** variable. If the variable exists, append `AFF_MVS_MQM` to any existing values, separated by a space. If the variable does not already exist, create it and set its value to `AFF_MVS_MQM`.
    - 5) Reconfigure and recycle the portal server.
  - e. If the Tivoli Enterprise Portal Server is running on a UNIX or Linux system, do the following steps:
    - 1) Stop the portal server if it is running.
    - 2) Navigate to the following directory: `ITM_HOME/config/`, where `ITM_HOME` is the IBM Tivoli Monitoring installation directory.
    - 3) Open the `cq.ini` file in a text editor.

- 4) Look for the **KFW\_TOPOLOGY\_CLUSTER\_LIST** parameter. If the parameter already exists, add **AFF\_MVS\_MQM** to any existing values, separated by a space. If the parameter does not already exist, add the following line to the file:  

```
KFW_TOPOLOGY_CLUSTER_LIST=AFF_MVS_MQM
```
- 5) Save and close the file.
- 6) Reconfigure and recycle the portal server.
7. Use **Cluster Administrator** to add a **Generic Service** type resource with the name **KMQ1** and a **Physical Disk** type resource with the name **R** to cluster group 1.
8. Use **Cluster Administrator** to set the group owner of cluster group 1 to cluster node 1.
9. Use **Cluster Administrator** to start the queue manager and the WebSphere MQ Monitoring agent in cluster group 1 on cluster node 1 or cluster node 2.

The configuration of the WebSphere MQ Monitoring agent to monitor queue managers in a cluster environment is completed.



---

## Chapter 12. Configuring in a cluster environment on AIX systems

You can configure the WebSphere MQ Monitoring agent to run in a cluster environment on AIX<sup>®</sup> systems that are using High Availability Cluster Multi Processing (HACMP<sup>™</sup>). 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 IBM Tivoli Monitoring to run in a cluster environment, see the individual documentation of each product .

The WebSphere MQ Monitoring agent can be configured to run in either an active/active or active/passive environment. See “Active/active clustering” and “Active/passive clustering” on page 165 for configuration information.

---

### Active/active clustering

Before you begin configuring the WebSphere MQ Monitoring 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 product is installed and your HACMP cluster environment is correctly configured.
- Both cluster nodes have access to a minimum of two shared disks, on which historical information that is shared between copies of the WebSphere MQ Monitoring agent that are running on different cluster nodes is stored. You must have a separate shared disk available in your cluster environment for each instance of the agent. If you want to have more than two agents running on each cluster node, increase the number of shared disks accordingly.
- 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 manage are created on both cluster nodes within the HACMP cluster environment. Ensure that failover occurs correctly. See your WebSphere MQ documentation for more information about failover.

An example of a cluster environment is shown in Figure 31 on page 164. 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, so 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 queue managers and an instance of the WebSphere MQ Monitoring agent to monitor each queue manager.

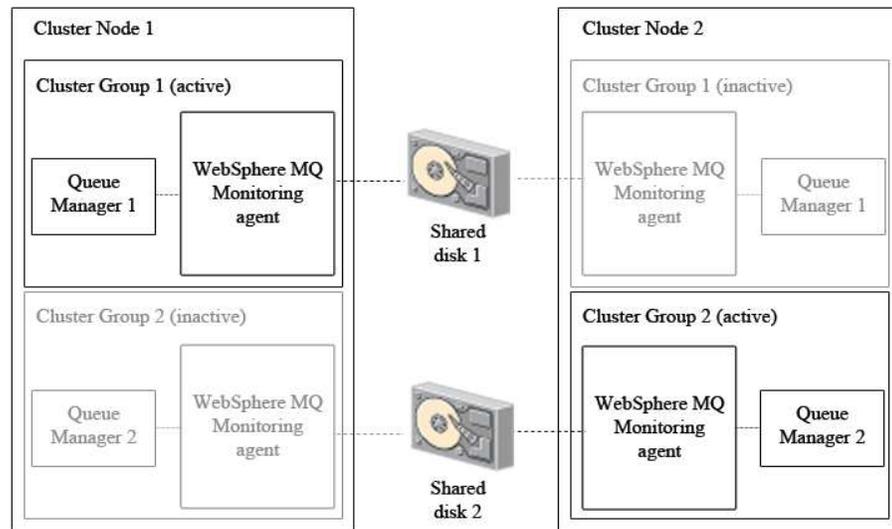


Figure 31. An example active-active cluster environment architecture with one cluster group active on each cluster node

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 31), the copy of cluster group 1 on 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 is started 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, such as historical data files, is stored on a separate disk that can be accessed by all copies of that 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 shared 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 such as historical data files can still be read and written to the disk as if the same copy of the agent was still running.

**Note:** Using a shared disk is preferred over using a Network File System (NFS) mounted file system because results are unpredictable when the NFS mounted file system is not available.

To install and configure the WebSphere MQ Monitoring agent, repeat the procedure in “Configuring the WebSphere MQ Monitoring agent” on page 166 for each instance of the WebSphere MQ Monitoring agent in your environment.

**Remember:** You must repeat this procedure for different copies of the same agent instance that are running on different cluster nodes.

## Active/passive clustering

Before you begin configuring the WebSphere MQ Monitoring 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 product is installed and your HACMP cluster environment is correctly configured.
- Both cluster nodes have access to a shared disk, on which historical information that is shared between copies of the WebSphere MQ Monitoring 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 manage are created on both cluster nodes within the HACMP cluster environment. Ensure that failover occurs correctly. See your WebSphere MQ documentation for more information about failover.

An example of an active/passive cluster environment is shown in Figure 32. 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, so 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 Monitoring agent to monitor each queue manager.

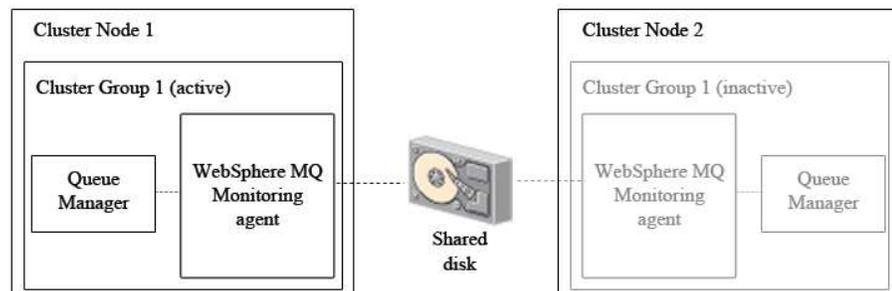


Figure 32. An example active-passive cluster environment architecture

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 32), 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 is started to continue the work of the cluster groups that were active on the node that failed.

Information shared between different copies of the same agent, such as historical data files, 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 is started, shared information such as historical data 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.

**Note:** Using a shared disk is preferred over using a Network File System (NFS) mounted file system because results are unpredictable when the NFS mounted file system is not available.

To install and configure the WebSphere MQ Monitoring agent, repeat the procedure in “Configuring the WebSphere MQ Monitoring agent” for each instance of the WebSphere MQ Monitoring agent in your environment.

**Remember:** You must repeat this procedure for different copies of the same agent instance that are running on different cluster nodes.

---

## Configuring the WebSphere MQ Monitoring agent

To install and configure the WebSphere MQ Monitoring agent for use in an HACMP cluster environment, do the following steps:

1. Install the WebSphere MQ Monitoring agent on the cluster node on which you want the agent to run. See *Installation and Setup Guide* for installation instructions.
2. Create new instances of the WebSphere MQ Monitoring agent for each queue manager that you want to monitor by doing the following steps:
  - a. Navigate to the *ITM\_HOME/config* directory, where *ITM\_HOME* is the directory where the 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 Monitoring agent by copying the *mq.cfg* default configuration file to the *hostname\_mq\_instance\_name.cfg* file, where the *hostname* is the host name of the cluster node and *instance\_name* is the queue manager name.
  - c. Edit each of the newly created configuration files as follows:
    - 1) Locate the **SET MANAGER NAME** parameter and change it as follows:

```
SET MANAGER NAME(instance_name)
```

where *instance\_name* is the name of the queue manager that you want to monitor.
    - 2) Locate the **SET QUEUE NAME** parameter and change it as follows:

```
SET QUEUE NAME(*) MGRNAME(instance_name) QDEFTYPE(PREDEFINED)
```

where *instance\_name* is the name of the queue manager that you want to monitor.
    - 3) Locate the **SET CHANNEL NAME** parameter and change it as follows:

```
SET CHANNEL NAME(*) MGRNAME(instance_name)
```

where *instance\_name* is the name of the queue manager that you want to monitor.
3. Set local variables 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.
  - b. Open the *mq.ini* file.
  - c. Locate the **\$CTIRA\_SIT\_PATH** variable and change it as follows:

```
CTIRA_SIT_PATH=$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/sit$INSTANCE_HISTORY$
```

**Tip:** Using the `$INSTANCE_HISTORY$` variable in the `mq.ini` file distinguishes the instances of the WebSphere MQ Monitoring agent on the cluster node.

- d. Save and close the `mq.ini` file.
4. Create the directories where historical and situation data files are stored by doing the following steps on each cluster node:
  - a. Create the following directory for storing situation data:

```
ITM_HOME/aix523/mq/sit
```

where `ITM_HOME` is the directory in which IBM Tivoli Monitoring is installed. The user ID that is used to run the agent must have write access to this directory.

- b. Create the following directories for storing historical and situation data from each agent instance on the shared disk.
  - For storing historical data: `disk_name/kmq/hist/instance_name`
  - For storing situation data: `disk_name/kmq/sit/instance_name`

where `disk_name` is the name of the shared disk on which historical data is stored and `instance_name` is the name of the queue manager that you want to monitor. The user ID that is used to run the agent must have write access to these directories.

- c. Create a link to the shared disk on which historical data is stored by running the following command:

```
ln -sf disk_name/kmq/hist/instance_name  
ITM_HOME/aix523/mq/hist/instance_name
```

where `disk_name` is the name of the shared disk, `ITM_HOME` is the directory in which IBM Tivoli Monitoring is installed, and `instance_name` is the name of the queue manager that you want to monitor.

**Remember:** The symbolic link definition is used to equate the `mq.ini` specification to a directory on the shared disk on which historical and situation data is stored.

- d. Create a link to the shared disk on which situation data is stored by running the following command:

```
ln -sf disk_name/kmq/sit/instance_name  
ITM_HOME/aix523/mq/sit/instance_name
```

where `disk_name` is the name of the shared disk, `ITM_HOME` is the directory in which IBM Tivoli Monitoring is installed, and `instance_name` is the name of the queue manager that you want to monitor.

**Remember:** The symbolic link definition is used to equate the `mq.ini` specification to a directory on the shared disk on which historical and situation data is stored.

- e. Optional: If you have multi-instance queue managers in your WebSphere MQ environment, create a link to the shared disk where agent data related to the queue manager is stored by running the following command:

```
ln -sf disk_name/kmq/agent/instance_name  
ITM_HOME/aix523/mq/agent/instance_name
```

where `disk_name` is the name of the shared disk, `ITM_HOME` is the directory in which IBM Tivoli Monitoring is installed, and `instance_name` is the name of the queue manager that you want to monitor.

**Remember:** The symbolic link definition is used to equate the mq.ini specification to a directory on the shared disk on which historical and situation data is stored.

5. Configure the Tivoli Enterprise Portal Server to list agents running in cluster groups by cluster name instead of host system name in Tivoli Enterprise Portal:
  - a. Open the agent configuration file. The filename is `hostname_mq_instance_name.cfg`, where `hostname` is the host name of cluster node, `instance_name` is the queue manager name. Add the following line at the bottom of the file:  

```
SET AGENT NAME($cluster_name)
```

where `cluster_name` is the name of the HACMP cluster. This name must be the same as the name that is assigned to the failover agent in the other cluster group.

- b. If the Tivoli Enterprise Portal Server is running on a Windows system, do the following steps:
    - 1) Stop the Tivoli Enterprise Portal Server if it is running.
    - 2) Right-click the Tivoli Enterprise Portal Server icon in Manage Tivoli Enterprise Monitoring Services, and click **Advanced** > **Edit Variables**.
    - 3) In the Tivoli Enterprise Portal Server Override Local Variable Setting window, click **Add**.
    - 4) From the **Variable** menu of the Add Environment Setting Override window, look for the **KFW\_TOPOLOGY\_CLUSTER\_LIST** variable. If the variable exists, append `AFF_MVS_MQM` to any existing values, separated by a space. If the variable does not already exist, create it and set its value to `AFF_MVS_MQM`.
    - 5) Reconfigure and recycle the Tivoli Enterprise Portal Server.
  - c. If the Tivoli Enterprise Portal Server is running on a UNIX or Linux system, do the following steps:
    - 1) Stop the Tivoli Enterprise Portal Server if it is running.
    - 2) Navigate to the `ITM_HOME/config/` directory, where `ITM_HOME` is the IBM Tivoli Monitoring installation directory.
    - 3) Open the `cq.ini` file in a text editor.
    - 4) Look for the **KFW\_TOPOLOGY\_CLUSTER\_LIST** parameter. If the parameter already exists, add `AFF_MVS_MQM` to any existing values, separated by a space. If the parameter does not already exist, add the following line to the file:  

```
KFW_TOPOLOGY_CLUSTER_LIST=AFF_MVS_MQM
```
    - 5) Save and close the file.
    - 6) Reconfigure and recycle the Tivoli Enterprise Portal Server.

6. Create a file containing the startup script that is used to start the agent by doing the following steps:
  - 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 Monitoring agent:  

```
ITM_HOME/bin/itmcmd agent -o instance_name start mq
```

where:

`ITM_HOME` is the directory in which IBM Tivoli Monitoring is installed.

*MC91\_install* is the directory in which WebSphere MQ supportpac MC91 is installed.

*QM\_name* is the name of the queue manager.

*instance\_name* is the name of the WebSphere MQ Monitoring agent instance.

WebSphere MQ supportpac MC91 was installed when you installed WebSphere MQ in the HACMP cluster environment. See your WebSphere MQ documentation for further information about WebSphere MQ supportpac MC91.

- b. Save the file as `kmq_start.sh`.

**Remember:** When writing a startup script, ensure that the queue manager is started before the WebSphere MQ Monitoring agent.

7. Create a file containing 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 Monitoring agent:

```
ITM_HOME/bin/itmcmd agent -o instance_name stop mq
```

- 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.

*MC91\_install* is the directory in which WebSphere MQ supportpac MC91 is installed.

*QM\_name* is the name of the queue manager.

*instance\_name* is the name of the WebSphere MQ Monitoring agent instance.

WebSphere MQ supportpac MC91 was installed when you installed WebSphere MQ in the HACMP cluster environment. See your WebSphere MQ documentation for further information about WebSphere MQ supportpac MC91.

- b. Save the file as `kmq_stop.sh`.
  - c. When writing a shutdown script, ensure that the WebSphere MQ Monitoring agent is stopped before the queue manager.
8. Do the following steps to set the scripts that is used to start and stop the agent in the HACMP environment:
    - a. Open the cluster group in the HACMP cluster software.
    - b. Under Application Server, set the start script as `kmq_start.sh`.
    - c. Under Application Server, set the stop script as `kmq_stop.sh`.

**Remember:** You must repeat this procedure for different copies of the same agent instance that are running on different cluster nodes.

The WebSphere MQ Monitoring agent is configured to operate in an HACMP cluster environment.



---

## 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. Data collection mode

WebSphere MQ Monitoring agent uses two data collection modes: sampling mode and on-demand mode.

In the sampling mode, the agent collects data in the background on an interval basis. Each time that you open a workspace containing a table that is based on sampling data, the data that is displayed in the table was gathered from the most recent interval. For example, if the sampling interval is set to 5 minutes (300 seconds), the displayed data might be collected up to 5 minutes ago. Sampling mode has the advantage of being able to aggregate data and calculate rates because the new sample can be compared to the old sample and deltas can be taken.

In the on-demand mode, the agents collect data at the exact time that a query is issued to it for the data. Each time that you open a workspace containing a table that is based on on-demand data, a query for data collection is issued to the agent and the data is collected in real-time at the time of the query. On-demand mode has the advantage of providing the most current data.

For information about which workspaces use the sampling mode and which use the on-demand mode, see "Sampled and on-demand tables."

---

### Sampled and on-demand tables

Sampled and on-demand tables list the tables that are used in WebSphere MQ Monitoring agent, their data collection mode, and their supported operating systems. Data collection is categorized as follows:

#### Sampled

This data is collected regularly at a specific time interval. Data that is returned by a query that uses sampled data represents values that are recorded during the sampling intervals queried.

#### On-demand

This data is collected by the agent in real-time when the query is issued, and reflects the most recent data values.

#### Background-collected

This data is collected in the background when it is published by the queue manager (in events or accounting and statistics reports). Querying this data results in a maximum of one row of data per event or queue manager report returned (depending on the query parameters). Most of this data is optionally produced by the queue manager according to the parameter settings in the queue manager. Some of the data is produced by the queue manager on an interval basis, and there are parameters for the queue manager that control the length of the interval. See Chapter 4, "Data collection for workspaces," on page 63 for more information about setting queue manager parameters to produce this data.

Table 17. Sampled and on-demand tables

Table name	Data collection type	Supported operating systems
Application Accounting	Background Collected	Distributed systems

Table 17. Sampled and on-demand tables (continued)

Table name	Data collection type	Supported operating systems
Application Connections	On-demand	All
Application Debug Trace	Sampled	z/OS systems
Application Debug Trace Details	Sampled	z/OS systems
Application Debug Trace Selection	Sampled	z/OS systems
Application Long-Term History	Sampled	z/OS systems
Application Statistics	Sampled	z/OS systems
Application Queue Long-Term History	Sampled	z/OS systems
Application Queue Short-Term History	Sampled	z/OS systems
Application Queue Statistics	Sampled	z/OS systems
Application Short-Term History	Sampled	z/OS systems
Application Topology	On-demand	All
Application Transaction/Program Long-Term History	Sampled	z/OS systems
Application Transaction/Program Short-Term History	Sampled	z/OS systems
Application Transaction/Program Statistics	Sampled	z/OS systems
Buffer Manager Long-Term History	Sampled	z/OS systems
Buffer Manager Short-Term History	Sampled	z/OS systems
Buffer Pools	Sampled	z/OS systems
Channel Data	On-demand	All
Channel Definitions	Sampled	All
Channel Definition Details	On-demand	All
Channel Initiator Detail	Sampled	z/OS systems
Channel Long-Term History	Sampled	All
Channel Short-Term History	Sampled	All
Channel Statistics	Sampled	All
Channel Status	On-demand	All
Channel Summary	Sampled	All
Connection Objects	On-demand	All
Current Events	Background-collected	All
Current Queue Manager Status	On-demand	All

Table 17. Sampled and on-demand tables (continued)

Table name	Data collection type	Supported operating systems
Data Manager Long-Term History	Sampled	z/OS systems
Data Manager Short-Term History	Sampled	z/OS systems
Error Log	Background-collected	Distributed systems
Event Archive	Background-collected	All
Event details	Background-collected	All
Event History	Background-collected	All
Listener Status	On-demand	Distributed systems
Log Data Set Status	On-demand	z/OS systems
Log Manager Long-Term History	Sampled	z/OS systems
Log Manager Short-Term History	Sampled	z/OS systems
Managers	Sampled	All
Manager Definition Details	Sampled	All
Message Data	On-demand	All
Message Delete	On-demand	All
Message Details	On-demand	All
Message Manager Long-Term History	Sampled	z/OS systems
Message Manager Short-Term History	Sampled	z/OS systems
Message Retry	On-demand	All
Message Statistics	On-demand	All
Message Summary	On-demand	All
MQSeries Events	Background-collected	All
MQ Action Log	Background-collected	All
MQ Channel Statistics	Background Collected	Distributed systems
MQ Queue Statistics	Background Collected	Distributed systems
MQI Call Statistics Details	Background Collected	Distributed systems
MQI Message Statistics Details	Background Collected	Distributed systems
MQI Statistics	Background Collected	Distributed systems
Namelist	On-demand	All
Object Attribute Details	On-demand	All
Page Sets	Sampled	z/OS systems
Page Set Long-Term History	Sampled	z/OS systems
Page Set Short-Term History	Sampled	z/OS systems
Publish Subscribe Status	On-demand	All
QSG Coupling Facility Structure Backups	Sampled	z/OS systems

Table 17. Sampled and on-demand tables (continued)

Table name	Data collection type	Supported operating systems
QSG Coupling Facility Structure Connections	Sampled	z/OS systems
QSG Coupling Facility Structures	Sampled	z/OS systems
QSG Channels	Sampled	z/OS systems
QSG QMgrs	Sampled	z/OS systems
QSG Queues	Sampled	z/OS systems
Queue Accounting	Background Collected	Distributed systems
Queue Data	On-demand	All
Queue Definition Details	On-demand	All
Queue Definitions	Sampled	All
Queue Handle Status	On-demand	All
Queue Long-Term History	Sampled	All
Queue Short-Term History	Sampled	All
Queue Statistics	Sampled	All
Queue Status	On-demand	All
SMF Data	Sampled	z/OS systems
Subscription Definitions	On-demand	All
Subscription Status	On-demand	All
TCPIP Started Listeners	Sampled	z/OS systems
Topic Definitions	On-demand	All
Topic Manager Long-Term History	Sampled	z/OS systems
Topic Manager Short-Term History	Sampled	z/OS systems
Topic Publishers	On-demand	All
Topic Status	On-demand	All
Topic Subscribers	On-demand	All

---

## Appendix C. Monitoring events on non-supported systems

Always install the WebSphere MQ Monitoring agent on supported systems. However, you can use the following procedure to monitor events *only* on non-supported systems. This procedure causes event data to be stored in a monitored queue manager.

Do the following steps to monitor events on non-supported systems:

1. In the queue manager on the non-supported system, define the system event queues as QREMOTE and as located in your monitored queue manager.
2. In the queue manager on the non-supported system, enable events. Events must be recorded in Coordinated Universal Time (UTC).
3. Enable monitoring of the queue manager on the supported system to which the events on the non-supported system are sent.



## Appendix D. Monitoring remote queue managers

You can set up a WebSphere MQ Monitoring agent to monitor a remote queue manager running on a system that is not currently supported by the agent. Using remote monitoring, you can monitor queue managers that are running on systems on which you cannot install WebSphere MQ Monitoring agent. The following figure shows the architecture that is used when monitoring a remote queue manager.

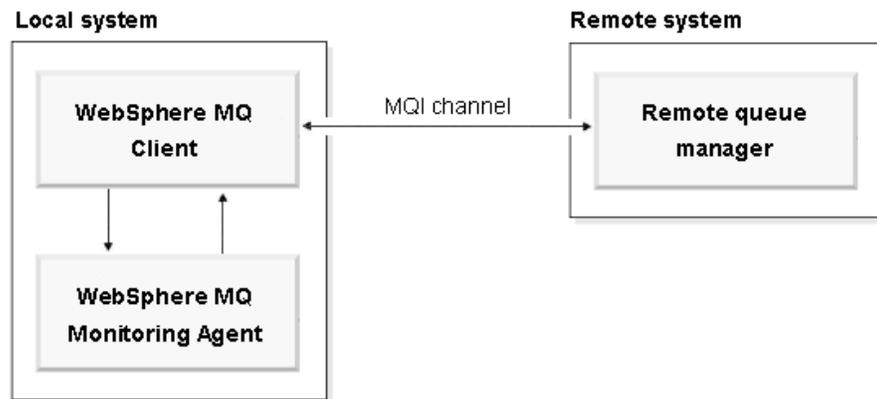


Figure 33. Remote monitoring communications architecture

### Remote monitoring

Remote monitoring is a method of monitoring a queue manager that is deployed on a system with no monitoring agent. When using remote monitoring, a WebSphere MQ Monitoring agent that is on one system monitors queue managers on another system.

If you want to monitor queue managers within your WebSphere MQ environment that are running on operating systems not currently supported by the WebSphere MQ Monitoring agent, such as on Tandem computers, you can use remote monitoring. Table 18 compares monitoring a queue manager locally to monitoring a queue manager remotely.

Table 18. Comparison between monitoring a queue manager locally and remotely

Functionality	Local Monitoring	Remote Monitoring
Monitor queue manager status	✓	✓
Monitor queues	✓	✓
Monitor MQSeries events	✓	✓
Monitor error log	✓	
Monitor dead-letter queues	✓	✓
Monitor channels	✓	✓
Monitor cluster queue managers	✓	✓

Table 18. Comparison between monitoring a queue manager locally and remotely (continued)

Functionality	Local Monitoring	Remote Monitoring
Collect application accounting data	✓	✓
Issue MQSeries Take Action commands	✓	✓
Issue system Take action command	✓	
Monitor multiple queue managers running on different Tandem computers		✓

## Setting up the environment for remote queue manager monitoring

To monitor a remote queue manager, you must configure WebSphere MQ Monitoring agent and define some channels and listeners on the remote host for communication with the monitoring agent.

Before setting up your environment for remote monitoring, you must have a WebSphere MQ Monitoring agent and WebSphere MQ Client running together on a supported AWindows, Linux, or AIX system. See Appendix F, “Check the existence of WebSphere MQ Client,” on page 197 for information about how to check whether WebSphere MQ Client is installed on your computer.

Do the following steps to set up your environment to monitor a remote queue manager running on a system that is not currently supported by the agent:

1. Create an instance of the WebSphere MQ Monitoring agent. For information about how to create an instance of the WebSphere MQ Monitoring agent, see “Creating multiple instances of the WebSphere MQ Monitoring agent” on page 11.
2. Configure the agent instance to connect to the Tivoli Enterprise Monitoring Server.
3. Ensure that the agent instance is stopped.
4. Modify the monitoring file of the agent instance to enable remote monitoring by replacing SET MANAGER NAME(*Qmgr\_remote*) line with the following statements:

```
SET MANAGER NAME(Qmgr_remote) REMOTE(YES)
SET AGENT NAME(agentID)
```

where:

- *Qmgr\_remote* is the name of the remote queue manager.
- *agentID* is the host name or IP address of the remote host.

**Tip:** The monitoring file name of the agent instance is *hostname\_mq\_Qmgr\_remote.cfg*, where *hostname* is the name of the host system; *Qmgr\_remote* is the name of the remote queue manager.

5. Run the following commands on the remote host to define a client channel, a server connection channel, and a listener on the remote queue manager for communication with the monitoring agent:

```
runmqsc Qmgr_remote
> DEFINE LISTENER(Listener) TRPTYPE(TCP) PORT(port_NO)
> DEFINE CHANNEL(Chl_name) CHLTYPE(SVRCONN) TRPTYPE(TCP)
> DEFINE CHANNEL(Chl_name) CHLTYPE(CLNTCONN) TRPTYPE(TCP)-
  CONNAME('Host_IP(port_NO)') QMNAME(Qmgr_remote)
> END
```

where:

- *Qmgr\_remote* is the name of the remote queue manager.
- *Listener* is the name of the listener on the remote queue manager.
- *port\_NO* is the port number used by the listener.
- *Chl\_name* is the name that you assign to the client and server channel.
- *Host\_IP* is the IP address of the remote host.

**Requirement:** The client and server channel must have the same name.

6. Transfer the client channel definition table file (AMQCLCHL.TAB) to the computer where the WebSphere MQ Monitoring agent is installed. Depending on the system on which the WebSphere MQ Monitoring agent is running, the destination directory on the host of the agent is as follows:

- Windows systems (32-bit agent): *install\_dir*\TMAITM6
- Windows systems (64-bit agent): *install\_dir*\TMAITM6\_x64
- UNIX systems: *install\_dir/arch/mq/bin*

where:

- *install\_dir* is the IBM Tivoli Monitoring installation directory.
- *arch* is the architecture code of the operating system. For a complete list of architecture codes, see *Installation and Setup Guide*.

**Tip:** The AMQCLCHL.TAB file is created in the *qmgrs/Qmgr\_remote/@ipcc* directory.

7. Configure the listener to start automatically and then start the listener on the remote queue manager by running the following commands on the remote host:

```
runmqsc Qmgr_remote
> ALTER LISTENER(Listener) TRPTYPE(tcp) CONTROL(QMGR)
> START LISTENER(Listener)
> END
```

where:

- *Qmgr\_remote* is the name of the remote queue manager.
- *Listener* is the name of the listener on the remote queue manager.

8. Make sure that channel authentication settings are configured properly for the user ID that is used to start the agent instance. Note that if you monitor remote queue manager of WebSphere MQ version 8.0.0, you must set proper channel authentication record.

To set the record, you can run the following command:

```
runmqsc Qmgr_remote
> ALTER CHANNEL(chl_name) CHLTYPE(SVRCONN) MCAUSER(non-privileged-user-id)
> SET CHLAUTH(chl_name) TYPE(ADDRESSMAP) ADDRESS(*) USERSRC(CHANNEL) ACTION(ADD)
> END
```

If you want to modify other channel authentications, see SET CHLAUTH in Knowledge Center ([http://www-01.ibm.com/support/knowledgecenter/SSFKSJ\\_8.0.0/com.ibm.mq.ref.adm.doc/q086630\\_.htm](http://www-01.ibm.com/support/knowledgecenter/SSFKSJ_8.0.0/com.ibm.mq.ref.adm.doc/q086630_.htm)) for more information.

9. Start the WebSphere MQ Monitoring agent instance.

**Important:** To monitor the remote queue managers of WebSphere MQ version 8.0.0, you must create a non-privileged user ID on the system where your queue manager is running. After you create the non-privilege user ID, you must follow the Procedure in Appendix F to grant WebSphere MQ OAM authorities to this ID you create.

**Tip:** On Windows systems, all members of the **mqm** group, and all members of the **Administrators** group are privileged users. On UNIX and Linux systems, all members of the mqm group are privileged users.

---

## Monitoring multiple queue managers

By default, the WebSphere MQ Monitoring agent monitors a single queue manager. However, you can remotely monitor multiple queue managers with the same monitoring agent. To do this, you must select one remotely monitored queue manager as the primary one and then configure the primary queue manager to contain other queue manager information.

You must have the required authorities for the MQSC commands and you must know the location of the client channel definition table (AMQCLCHL.TAB) of the primary queue manger.

To remotely monitor multiple queue managers with the same WebSphere MQ Monitoring agent, you cannot copy the AMQCLCHL.TAB files of all remotely monitored queue managers to the system that hosts the WebSphere MQ Monitoring agent, as you can when remotely monitoring a single queue manager (see step 6 on page 181 of “Setting up the environment for remote queue manager monitoring” on page 180). Instead, you must select one remotely monitored queue manager to be the primary queue manager, and configure it so that its AMQCLCHL.TAB contains the correct information for all queue managers.

To configure the remotely monitored queue manager, do the following steps:

1. Create an instance of the WebSphere MQ Monitoring agent for each queue manager that you want to monitor remotely.
2. Modify the configuration file of each agent instance to enable remote monitoring by setting the following parameters:

```
SET MANAGER NAME(queue_manager_name) REMOTE(YES) SET AGENT NAME(agentId)
```

where *queue\_manager\_name* is the name of the remote queue manager and *agentId* is the host name or IP address of the remote host.

3. Create a pair of client and server channels between each queue manager that you want to monitor and the system that hosts the WebSphere MQ Monitoring agents by running the following commands:

```
runmqsc qmgr_remote  
DEFINE CHANNEL(chl_name) CHLTYPE(SVRCONN) TRPTYPE(TCP)  
DEFINE CHANNEL(chl_name) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+  
CONNNAME('host_IP(port_no)') QMNAME(qmgr_remote)  
END
```

where:

- *qmgr\_remote* is the name of the additional queue manager.
- *port\_no* is the port number that is used by the listener.
- *chl\_name* is the name that you want to assign to the client and server channels.

- *host\_IP* is the IP address of the remote host.
4. Create a pair of client and server channels between the primary queue manager and the WebSphere MQ Monitoring agent and between each additional queue manager and the WebSphere MQ Monitoring agent.
    - a. Run the following commands for the primary queue manager, where *qmgr\_primary* is the name of the primary queue manager.
 

```
runmqsc qmgr_primary
DEFINE CHANNEL(chl_name) CHLTYPE(SVRCONN) TRPTYPE(TCP)
DEFINE CHANNEL(chl_name) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
CONNNAME('host_IP(port_no)') QMNAME(qmgr)
```
    - b. Run the following commands for each additional queue manager, where *qmgr* is the name of the queue manager on the remote host.
 

```
DEFINE CHANNEL(chl_name) CHLTYPE(SVRCONN) TRPTYPE(TCP)
DEFINE CHANNEL(chl_name) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
CONNNAME('host_IP(port_no)') QMNAME(qmgr)
```
    - c. Finally, run the following command:
 

```
END
```
- Important:** Run all these commands before you proceed to the next step.
5. Copy the AMQCLCHL.TAB binary file from the system where the primary queue manager is running to the system that hosts the WebSphere MQ Monitoring agent.
  6. Start all listeners for each remotely monitored queue manager and start all the WebSphere MQ Monitoring agent instances.

---

## Limitations of remote queue manager monitoring

Because the WebSphere MQ Monitoring agent cannot access the local file system or issue local commands on the remote host, the following features are unavailable with remote queue manager monitoring:

- Error Log workspace for the remote queue manager.
- Executing Take Action for system commands on the system with the remote queue manager
- The Start Date & Time column in the Queue Manager Status workspace
- Detecting the default queue manager on the remote host



---

## Appendix E. Disk space requirements for historical data tables

*IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* provides the basic disk space requirements for components such as WebSphere MQ Monitoring agent and WebSphere Message Broker Monitoring agent. These requirements do not include disk space that is required for maintaining historical data files. Because of the variations in client distributed systems, system size, number of managed systems, and other items, it is difficult to provide actual disk space requirements for historical data collection. The basic size for each of the tables for which historical data is collected are provided.

---

### Historical data tables

It is a good practice to always collect WebSphere MQ Monitoring agent historical tables at the remote managed system for WebSphere MQ. Product performance is improved by keeping the data at the remote managed system, especially data that applies only to z/OS systems, which can deal with large volumes of data more efficiently.

**Important:** To reduce the performance impact on your system, you can set a longer collection interval for tables that collect a large amount of data. For WebSphere MQ Monitoring agent, the Queue Statistics table collects a large amount of data. For additional information, see the topic “Performance Impact of Historical Data Requests” in the *IBM Tivoli Monitoring Administrator’s Guide*.

The attribute history tables, default file names, default tables collected, and the estimated disk space that is required for each 24-hour period for the historical data that is collected for WebSphere MQ Monitoring agent are listed in Table 19. Total default space is the estimated space that is required for each managed system for each 24-hour period for the default file collection option for all WebSphere MQ systems except z/OS systems; the total default space is based on monitoring 100 queues, 10 channels, and 500 events.

For information that is specific to the historical data collection options of WebSphere MQ Monitoring agent, see “Monitoring options” on page 26.

Table 19. Historical data tables

Attribute history table	File name for historical data
Application Accounting attributes (distributed systems only)	QMMQIACCT
Application Long-Term History attributes (z/OS systems only)	QMCONNAPP
Application Connections attributes*	QM_APAL
Application Queue Long-Term History attributes (z/OS systems only)*	QM_APQL
Application Transaction/Program Long-Term History attributes (z/OS systems only)*	QM_APTL
Buffer Manager Long-Term History attributes (z/OS systems only)*	QMLHBM
Channel Data attributes	QMCH_DATA
Channel Definitions attributes	QMCHANNEL
Channel Initiator Detail attributes (z/OS systems only)*	QMCHANIN

Table 19. Historical data tables (continued)

Attribute history table	File name for historical data
Channel Long-Term History attributes	QMCH_LH
Channel Status attributes	QMCHAN_ST
Channel Summary attributes	QMCHAN_SUM
Connection Objects attributes	QMCONNOBJ
Current Queue Manager Status attributes	QMCURSTAT
Error Log attributes (distributed systems only)**	QMERRLOG
Event Archive attributes	QMEVENTL
Listener Status attributes (distributed systems only)	QMLSSTATUS
Log Data Set Status attributes (z/OS systems only)*	QMDSPUSAGE
Log Manager Long-Term History attributes (z/OS systems only)*	QMLHLM
Message Manager Long-Term History attributes (z/OS systems)*	QMLHMM
Message Statistics attributes	QMMMSG_STAT
MQ Action Log attributes	QMACTLOG
MQ Channel Statistics attributes (distributed systems only)	QMCH_STAT
MQ Queue Statistics attributes (distributed systems only)	QMQ_STAT
MQI Call Statistics Details attributes (distributed systems only)	QMMQICDET
MQI Message Statistics Details attributes (distributed systems only)	QMMQIMDET
MQI Statistics attributes (distributed systems only)	QMMQISTAT
Page Set Long-Term History attributes (z/OS systems only)*	QMPS_LH
QSG Channels attributes (z/OS systems only)*	QSG_CHANS
QSG Coupling Facility Structure Backups attributes (z/OS systems only)*	QSG_CFBKUP
QSG Coupling Facility Structure Connections attributes (z/OS systems only)*	QSG_CFCONN
QSG Coupling Facility Structures attributes (z/OS systems only)*	QSG_CFSTR
QSG QMgrs attributes (z/OS systems only)*	QSG_QMGR
QSG Queues attributes (z/OS systems only)*	QSG_QUEUES
Queue Long Term History attributes	QMQ_LH
Queue Accounting attributes (distributed systems only)	QMQ_ACCT
Queue Data attributes	QMQ_DATA
Queue Definition Details attributes	QMQQUEUE
Queue Handle Status attributes	QMQ_HDL_ST
Queue Status attributes	QMQ_QU_ST
Topic Manager Long-Term History attributes (z/OS systems only)*	QMLHTM
<p><b>Note:</b></p> <ul style="list-style-type: none"> <li>* These tables are available on z/OS systems only. They are not included in the default space estimates.</li> <li>** The Event Log is created for all systems but cannot be configured by using option 3, Customize Historical Collection, on the HDC Main menu. It is included in the table because the data is available for use in the same way as history data. By default, the QMEVENTH file is automatically archived into the CTIRA_HIST_DIR directory when the size of the QMEVENTH file is 10MB. The name of the archive is QMEVENTH.arc.</li> </ul>	

## Historical table record sizes

Table 20. Historical table record sizes

History table	Record size	Frequency
Application Accounting	968 bytes	One record is recorded for each application accounting record.
Application Connections	1164 bytes	During each interval, one record is recorded for each connection.
Application Long-Term History	320 bytes	During each interval, one record is recorded for each monitored application.
Application Queue Long-Term History	412 bytes	During each interval, one record is recorded for each queue used by each transaction or program per monitored application.
Application Transaction/Program Long-Term History	332 bytes	During each interval, one record is recorded for each transaction or program per monitored application.
Buffer Manager Long-Term History	324 bytes	During each interval, one record is recorded for each buffer pool.
Channel Data	1004 bytes	During each interval, one record is recorded for each channel.
Channel Definitions	1072 bytes	During each interval, one record is recorded for each queue.
Channel Initiator Detail	312 bytes	One record is recorded for each z/OS system queue manager.
Channel Long-Term History	960 bytes	During each interval, one record is recorded for each monitored channel that is active.
Channel Status	1604 bytes	During each interval, one record is recorded for each channel.
Connection Objects	1080 bytes	During each interval, one record is recorded for each connection.
Current Queue Manager Status	1712 bytes	During each interval, one record is recorded for the current queue manager.
Error Log	3800 bytes	One record is recorded for each message written to the error log.
Listener Status	1208 bytes	During each interval, one record is recorded for each listener.
Log Data Set Status	344 bytes	During each interval, one record is recorded for each log data set.
Log Manager Long-Term History	584 bytes	During each interval, one record is recorded for each queue manager.
Message Manager Long-Term History	304 bytes	During each interval, one record is recorded for each queue manager.
Message Statistics	560 bytes	One record is recorded for each row returned by active situations that are associated with Message Statistics attribute group.
MQ Action Log	1560 bytes	During each interval, one record is recorded for each action.
MQ Channel Statistics	732 bytes	One record is recorded for each Channel statistics record.
MQ Queue Statistics	580 bytes	One record is recorded for each Queue statistics record.
MQI Call Statistics Details	268 bytes	One record is recorded for each MQI Call Statistics Details record.
MQI Message Statistics Details	236 bytes	One record is recorded for each MQI Message Statistics Details record.

Table 20. Historical table record sizes (continued)

History table	Record size	Frequency
MQI Statistics	608 bytes	One record is recorded for each MQI statistics record.
Page Set Long-Term History	300 bytes	During each interval, one record is recorded for each active page set.
QSG Channels	240 bytes	During each interval, one record is recorded for each shared channel in each QSG.
QSG Coupling Facility Structure Backups	212 bytes	During each interval, one record is recorded for each backup of CF Structure of each QSG.
QSG Coupling Facility Structure Connections	304 bytes	During each interval, one record is recorded for each connection to CF Structure in each QSG.
QSG Coupling Facility Structures	532 bytes	During each interval, one record is recorded for each CF Structure of each QSG.
QSG QMgrs	304 bytes	During each interval, one record is recorded for each queue manager.
QSG Queues	208 bytes	During each interval, one record is recorded for each shared queue in each QSG.
Queue Long-Term History	640 bytes	During each interval, one record is recorded for each monitored queue.
Queue Accounting	752 bytes	One record is recorded for each queue accounting record.
Queue Data	940 bytes	During each interval, one record is recorded for each queue.
Queue Definitions	960 bytes	During each interval, one record is recorded for each queue.
Queue Handle Status	1060 bytes	During each interval, one record is recorded for each queue handle.
Queue Status	392 bytes	During each interval, one record is recorded for each queue.
Topic Manager Long-Term History	324 bytes	During each interval, one record is recorded for each queue manager.

## Historical space requirement worksheets

Use the following worksheets to estimate expected file sizes and additional disk space requirements for your site. A sample calculation is provided for each historical data collection table.

Table 21. Application Accounting (QMMQIACCT) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	968 bytes	$(60/15 \times 24 \times 968 \times 2) / 1024$ for 2 applications	181.5 KBs

Table 22. Application Connections (QMCONNAPP) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1164 bytes	$(60/15 \times 24 \times 1164 \times 5) / 1024$ for 5 monitored applications	546 KBs

Table 23. Application Long-Term History (QM\_APAL) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	320 bytes	$(60/15 \times 24 \times 320 \times 5) / 1024$ for 5 monitored applications	150 KBs

Table 24. Application Queue Long-Term History (QM\_APQL) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	412 bytes	$(60/15 \times 24 \times 412 \times 20) / 1024$ for 20 queues used by monitored applications	773 KBs

Table 25. Application Transaction/Program Long-Term History (QM\_APTL) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	332 bytes	$(60/15 \times 24 \times 332 \times 10) / 1024$ for 10 transaction or programs for monitored applications	311 KBs

Table 26. Buffer Manager Long-Term History (QMLHBM) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	324 bytes	$(60/15 \times 24 \times 324 \times 4) / 1024$ for 4 buffer pools in use	122 KBs

Table 27. Channel Data (QMCH\_DATA) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1004 bytes	$(60/15 \times 24 \times 1004 \times 10) / 1024$ for 10 active monitored channels	942 KBs

Table 28. Channel Definitions (QMCHANNEL) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1072 bytes	$(60/15 \times 24 \times 1072 \times 10) / 1024$ for 10 active monitored channels	1005 KBs

Table 29. Channel Initiator Detail (QMCHANIN) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	312 bytes	$(60/15 \times 24 \times 312 \times 1) / 1024$ for each z/OS system queue manager	29 KBs

Table 30. Channel Long-Term History (QMCH\_LH) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	960 bytes	$(60/15 \times 24 \times 960 \times 10) / 1024$ for 10 active monitored channels	900 KBs

Table 31. Channel Status (QMCHAN\_ST) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1604 bytes	$(60/15 \times 24 \times 1604 \times 10) / 1024$ for 10 active monitored channels	1504 KBs

Table 32. Channel Summary (QMCHAN\_SUM) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	732 bytes	$(60/15 \times 24 \times 408 \times 5) / 1024$ for 5 channel summary	191.25 KBs

Table 33. Connection Objects (QMCONNOBJ) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1080 bytes	$(60/15 \times 24 \times 1080 \times 5) / 1024$ for 5 monitored connections	507 KBs

Table 34. Current Queue Manager Status (QMCURSTAT) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1712 bytes	$(60/15 \times 24 \times 1712 \times 1) / 1024$ for 1 monitored queue manager	160.5 KBs

Table 35. Event Archive (QMEVENTL) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	732 bytes	$(60/15 \times 24 \times 1668 \times 5) / 1024$ for 5 event archives	781.875 KBs

Table 36. Event Log (QMEVENTH) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
Real-time	2776 bytes	$(2776 \times 500) / 1024$ for 500 events	1355 KBs

Table 37. Listener Status (QMLSSTATUS) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1208 bytes	$(60/15 \times 24 \times 1208 \times 1) / 1024$ for 1 monitored listener	114 KBs

Table 38. Log Data Set Status (QMDSPUSAGE) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	344 bytes	$(60/15 \times 24 \times 344 \times 1) / 1024$ for 1 monitored log data set	32 KBs

Table 39. Log Manager Long-Term History (QMLHLM) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	584 bytes	$(60/15 \times 24 \times 584 \times 1) / 1024$ for 1 monitored queue manager	54.75 KBs

Table 40. Message Manager Long-Term History (QMLHMM) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	304 bytes	$(60/15 \times 24 \times 304 \times 1) / 1024$ for 1 monitored queue manager	29 KBs

Table 41. Message Statistics (QMMSG\_STAT) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	560 bytes	$(60/15 \times 24 \times 560 \times 30 \text{ rows}^*) / 1024 *$ Calculated as follows for 10 active situations for a 5-minute situation interval written for 10 queues that all use Queue as the grouping mechanism. A 15-minute historical collection interval divided by the 5-minute situation interval (15/5) equals 3 collection intervals. 10 rows (10 situations per queue) $\times$ 3 collection intervals = 30 rows per 15 minute historical interval.	1.58 MBs

Table 42. MQ Action Log (QMACTLOG) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1560 bytes	$(60/15 \times 24 \times 1560 \times 1) / 1024$ for 1 monitored queue manager	147 KBs

Table 43. MQ Channel Statistics (QMCH\_STAT) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	732 bytes	$(60/15 \times 24 \times 732 \times 5) / 1024$ for 5 channels statistics	343.125 KBs

Table 44. MQ Queue Statistics (QMQ\_STAT) worksheet

Interval	Record Size	Formula	Expected File Size per 24 Hours
15 min.	580 bytes	$(60/15 \times 24 \times 580 \times 5) / 1024$ for 5 queues statistics	271.875 KBs

Table 45. MQI Call Statistics Details (QMMQICDET) worksheet

Interval	Record Size	Formula	Expected File Size per 24 Hours
15 min.	268 bytes	$(60/15 \times 24 \times 268 \times 12) / 1024$ for 12 MQI Call statistics	302 KBs

Table 46. MQI Message Statistics Details (QMMQIMDET) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	236 bytes	$(60/15 \times 24 \times 236 \times 12) / 1024$ for 12 MQI Message statistics	265.5 KBs

Table 47. MQI Statistics (QMMQISTAT) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	608 bytes	$(60/15 \times 24 \times 608 \times 1) / 1024$ for 1 MQI statistics	57 KBs

Table 48. Page Set Long-Term History (QMPS\_LH) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	300 bytes	$(60/15 \times 24 \times 300 \times 10) / 1024$ for 10 active page sets	281 KBs

Table 49. QSG Channels (QSG\_CHANS) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	240 bytes	$(60/15 \times 24 \times 240 \times 10) / 1024$ for 10 monitored channels	225 KBs

Table 50. QSG Coupling Facility Structure Backups (QSG\_CFBKUP) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	212 bytes	$(60/15 \times 24 \times 212 \times 5) / 1024$ for 5 connected queue managers	99 KBs

Table 51. QSG Coupling Facility Structure Connections (QSG\_CFCONN) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	304 bytes	$(60/15 \times 24 \times 304 \times 5) / 1024$ for 5 monitored queue manager connections to DB2	143 KBs

Table 52. QSG Coupling Facility Structures (QSG\_CFSTR) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	532 bytes	$(60/15 \times 24 \times 532 \times 3) / 1024$ for 3 monitored structures	150 KBs

Table 53. QSG QMgrs (QSG\_QMGR) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	304 bytes	$(60/15 \times 24 \times 304 \times 2) / 1024$ for 2 monitored queue managers	57 KBs

Table 54. QSG Queues (QSG\_QUEUES) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	208 bytes	$(60/15 \times 24 \times 208 \times 20) / 1024$ for 20 monitored queues	390 KBs

Table 55. Queue Accounting (QMQ\_ACCT) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	752 bytes	$(60/15 \times 24 \times 752 \times 5) / 1024$ for 5 queues	352.5 KBs

Table 56. Queue Data (QMQ\_DATA) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	940 bytes	$(60/15 \times 24 \times 940 \times 5) / 1024$ for 5 queues	441 KBs

Table 57. Queue Definitions (QMQUEUE) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	960 bytes	$(60/15 \times 24 \times 960 \times 5) / 1024$ for 5 queues	450 KBs

Table 58. Queue Handle Status (QM\_Q\_HDL\_ST) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	1060 bytes	$(60/15 \times 24 \times 1060 \times 1) / 1024$ for 1 queue handle	100 KBs

Table 58. Queue Handle Status (QMQ\_HDL\_ST) worksheet (continued)

Interval	Record size	Formula	Expected file size per 24 hours

Table 59. Queue Long-Term History (QMQ\_LH) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	640 bytes	$(60/15 \times 24 \times 640 \times 10) / 1024$ for 10 monitored queues	600 KBs

Table 60. Queue Status (QMQ\_QU\_ST) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	392 bytes	$(60/15 \times 24 \times 392 \times 5) / 1024$ for 5 queues	184 KBs

Table 61. Topic Manager Long-Term History (QMLHTM) worksheet

Interval	Record size	Formula	Expected file size per 24 hours
15 min.	324 bytes	$(60/15 \times 24 \times 324 \times 1) / 1024$ for 1 monitored queue manager	30 KBs

## Historical disk space summary worksheet

Table 62. Historical disk space summary worksheet

History table	Historical data table size (kilobytes) (24 hours)	Number of archives	Subtotal of the total space required (kilobytes)
Application Accounting			
Application Connections			
Application Long-Term History			
Application Queue Long-Term History			
Application Transaction/Program Long-Term History			
Buffer Manager Long-Term History			
Channel Data			
Channel Definitions			
Channel Initiator Detail			
Channel Long-Term History			
Channel Status			

Table 62. Historical disk space summary worksheet (continued)

History table	Historical data table size (kilobytes) (24 hours)	Number of archives	Subtotal of the total space required (kilobytes)
Channel Summary			
Connection Objects			
Current Queue Manager Status			
Error Log			
Event Archive			
Listener Status			
Log Data Set Status			
Log Manager Long-Term History			
Message Manager Long-Term History			
Message Statistics			
MQ Action Log			
MQ Channel Statistics			
MQ Queue Statistics			
MQI Call Statistics Details			
MQI Message Statistics Details			
MQI Statistics			
Page Set Long-Term History			
QSG Channels			
QSG Coupling Facility Structure Backups			
QSG Coupling Facility Structure Connections			
QSG Coupling Facility Structures			
QSG QMgrs			
QSG Queues			
Queue Long-Term History			
Queue Accounting			
Queue Data			
Queue Definitions			
Queue Handle Status			
Queue Status			
Topic Manager Long-Term History			
Total Disk Space Required			

---

## Appendix F. Check the existence of WebSphere MQ Client

Check if WebSphere MQ Client is already installed on your computer.

---

### Checking the existence of WebSphere MQ Client on Windows systems

WebSphere MQ Client is required for remote queue manager monitoring. Use the Registry Editor on a Windows system to check the existence of WebSphere MQ Client.

You must have the required authorities to view the MQSERIES registry key in Windows Registry.

Do the following steps to check whether WebSphere MQ Client is already installed on a Windows system:

1. Open the Registry Editor by clicking **Start > Run** and typing `regedit`. Click **OK**.
2. Expand the `HKEY_LOCAL_MACHINE` registry key.
3. Expand the `SOFTWARE` registry key.
4. Expand the `IBM` registry key.
5. Expand the `MQSERIES` registry key.
6. Expand the `CurrentVersion` registry key.
7. Expand the `Components` registry key and check if there is an entry named `Local Clients\Windows NT Client` in its subkey list. If there is, WebSphere MQ Client is installed on the Windows system.

---

### Checking the existence of WebSphere MQ Client on AIX systems

WebSphere MQ Client is required for remote queue manager monitoring. Use the `lslpp` command to check the existence of WebSphere MQ Client on an AIX system.

Before you issue the `lslpp` command, log on the system with the root user ID.

Use the following procedure to check whether WebSphere MQ Client is already installed on an AIX system:

1. Run the following command:

```
lslpp -l | grep mqm.client
```
2. Check the returned output by the command. If the following output is displayed, then WebSphere MQ Client is already installed on the AIX system:

```
mqm.client.rte          version COMMITTED WebSphere MQ Client for AIX
```

where *version* is the version number of WebSphere MQ Client.

---

### Checking the existence of WebSphere MQ Client on Linux systems

WebSphere MQ Client is required for remote queue manager monitoring. Use the `rpm` command to check the existence of WebSphere MQ Client on a Linux system.

Before you issue the `rpm` command, log on the system with the root user ID.

Use the following procedure to check whether WebSphere MQ Client is already installed on a Linux system:

1. Run the following command:  
`rpm -qa | grep MQSeriesClient`
2. Check the returned output by the command. If the following output is displayed, then WebSphere MQ Client is already installed on the Linux system:

`MQSeriesClient-version`

where *version* is the version number of WebSphere MQ Client.

---

## Appendix G. Object configuration

If you install the WebSphere MQ Configuration agent and the WebSphere MQ Monitoring agent, you can access some configuration options through the workspaces of WebSphere MQ Monitoring agent.

You can use the configuration options to modify the settings list of an object, or to update an object in your environment from the object in the defined view, without entering the Configuration view in Tivoli Enterprise Portal. Different workspaces provides shortcuts to configure different types of objects, as shown in Table 63.

Table 63. Objects configuration from different workspaces in WebSphere MQ

Workspace	Object that can be Configured
Channel Performance	Channel
Channel Definitions	Channel
Cluster Queue Managers	Channel
Queue Definitions	Queue
Queue Statistics	Queue
Queue Manager Status	Queue Manager

To configure an object from a workspace of the WebSphere MQ Monitoring agent, do the following steps:

1. Navigate to one of the workspaces that are listed in Table 63.
2. In the workspace that contains information about the object that you want to configure, right-click the row.
3. Select **Configure X**, where X is the type of object that you select in the table. For example, if you select a queue manager in the table, select **Configure Queue Manager** from the menu.
4. If you have two or more items with the same name in your defined environment (viewable in the Defined view in the WebSphere MQ Configuration agent), you are prompted to select the one that you want to modify. Select the one that you want to modify.
5. Modify the attributes of the object as you would in the Configuration view.
6. Click **Update Actual and Save** to update your actual environment with any changes that you have made to the object.

**Important:** You can only update your actual environment if the configuration agent is running, otherwise this operation fails.

For more information about the WebSphere MQ Configuration agent and modifying the setting list of an object, see *IBM Tivoli Composite Application Manager Configuration Agent for WebSphere MQ User's Guide*.



---

## Appendix H. Granting WebSphere MQ OAM authorities to a user ID

If the WebSphere MQ queue manager that you want to monitor is version 7.0.1 or later, you can use a non-privileged user ID to start, stop, and run the agent that monitors the queue manager. Before you can do that, you must grant appropriate Object Authority Manager (OAM) authorities to the user ID.

The **setmqaut** control command is used to grant WebSphere MQ OAM authorities to the non-privileged user ID. The user ID that is used to issue this WebSphere MQ control commands must be a member of the **mqm** group.

Do the following steps to grant the user ID appropriate OAM authorities so that the user ID can start, stop and run the agent successfully:

1. Run the following command to grant the user ID the appropriate authorities to access the queue manager that you want to monitor:

```
setmqaut -m QMGR -t qmgr -p UserID +inq +connect +dsp +setid
```

where *QMGR* is the name of the queue manager and *UserID* is the user ID. You must specify the fully qualified user ID for the **-p** option, such as **-p user@domain** or **-p user@host**.

**Tip:** You can replace the **-p** option with the **-g** option in these commands to specify a user group name.

2. Run the following commands to grant the user ID the appropriate authorities to access the system queues of the queue manager:

```
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.COMMAND.QUEUE -p UserID +inq +get +dsp +put +setid
```

(The following line is required only by HLQ statements.)

```
setmqaut -m QMGR -t q -n hlq.IRA.* -p UserID +inq +get +dsp +put
setmqaut -m QMGR -t q -n SYSTEM.DEFAULT.MODEL.QUEUE -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.AUTH.DATA.QUEUE -p UserID +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.QMGR.EVENT -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.PERFM.EVENT -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.CHANNEL.EVENT -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.LOGGER.EVENT -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.CONFIG.EVENT -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.COMMAND.EVENT -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.ACCOUNTING.QUEUE -p UserID +get +inq +dsp
setmqaut -m QMGR -t q -n SYSTEM.ADMIN.STATISTICS.QUEUE -p UserID +get +inq +dsp
```

3. For the workspaces to display data, the user ID of the agent needs display access to various objects. Run the following commands to grant the user ID the appropriate authorities:

```
setmqaut -m QMGR -t q -n "*" -p UserID +dsp
setmqaut -m QMGR -t channel -n "*" -p UserID +dsp
setmqaut -m QMGR -t clntconn -n "*" -p UserID +dsp
setmqaut -m QMGR -t listener -n "*" -p UserID +dsp
setmqaut -m QMGR -t namelist -n "*" -p UserID +dsp
setmqaut -m QMGR -t topic -n "*" -p UserID +dsp
```

4. If you want to use the Take Action facility, and the agent parameters indicate that the user ID of the agent is used to run Take Action commands, you must

grant additional OAM authorities to the user ID. For example, to update a queue with a Take Action command, you must grant the OAM change authority for the queue to the user ID.

5. If you want to use the agent to delete a message from a queue, forward a message to another queue, or purge a queue, you must grant additional OAM authorities to the user ID.

---

## Appendix I. Library for the WebSphere MQ Monitoring agent

The following documents are available in the library for the WebSphere MQ Monitoring 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 Agent for WebSphere MQ User's Guide*  
Provides instructions for using the features of WebSphere MQ Monitoring 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](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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](http://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.

software of a system, subsystem, or network are organized and interconnected.

---

## 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 greater 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

---

## 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

## A

- access control
  - setting authorization level 90
  - settings for different message access levels 91
  - settings for WebSphere MQ messages 89
- accessibility
  - keyboard 171
  - overview 171
  - screen 171
- accessing
  - Dead-Letter Queue Messages workspaces 123
- accounting messages
  - enabling commands 116
  - monitoring workspaces 116
- active/active clustering
  - configuration
    - AIX 166
    - Windows 154
  - configuration prerequisites
    - AIX 163
    - Windows 153
- active/passive clustering
  - configuration
    - AIX 166
    - Windows 158
  - configuration prerequisites
    - AIX 165
    - Windows 157
- ad hoc queries 108
- agent configuration
  - HACMP 166
- agent instances
  - creating
    - i5/OS 12
    - Linux 12
    - UNIX 12
    - Windows 11
- Agent Management Services 7
- Agent Name tag 25
- agent suffixes 12
- Agent tag 26
- agent-server-client architecture 6
- agents
  - remote configuration, from the command line 20
  - remote configuration, from Tivoli Enterprise Portal 20
  - remote configuration, overview 20
- alert
  - description 2
- AMQCLCHL.TAB file 182
- AMQERR01 file 126
- Application Accounting workspace
  - collecting data 63
- Application Accounting workspaces
  - description 116
  - guide for action 117
- Application Connection workspace
  - Application Topology view
    - browse mode 140
    - compact mode 137
    - drill-down modes 138, 139

- application connections
  - to a specific queue 140
  - to queue managers 137, 139
  - to queues 138
- Application Debugging workspace
  - collecting data 64
- Application Debugging workspaces
  - description 118
  - guide for action 118
- Application Statistics workspaces
  - collecting data 65
  - description 118
  - guide for action 119
- Application Topology view
  - browse mode
    - for selected queues 140
  - compact mode
    - for monitored queue managers 137
  - description 137
  - display modes 137
  - displaying
    - specified number of connections 141
  - drill-down modes
    - for a specific application 138
    - for all applications 139
  - predefined links
    - at application nodes 144
    - at queue manager nodes 143
    - at queue nodes 144
    - overview 143
- architecture
  - IBM Tivoli Monitoring 6
  - remote monitoring communications 179
- attributes
  - description 3
  - usage 3
- authorities, OAM
  - granting 201

## B

- buffer managers
  - efficiency 119
  - monitoring 119
    - buffer managers 119
- Buffer Pool Statistics workspaces
  - collecting data 65
  - description 119
  - guide for action 119
- buffer pools
  - improving performance 119

## C

- changing
  - monitoring options
    - i5/OS 17
    - Linux 14
    - UNIX 14
    - Windows 15

- Channel Definitions workspace
  - guide for action 121
- Channel Definitions workspaces
  - description 120
- channel information 120
- Channel Initiator Status workspaces
  - description 121
  - guide for action 121
- Channel Performance Summary chart 122
- Channel Performance workspaces
  - collecting data 66
  - description 122
  - guide for action 122
- channel related workspaces
  - collecting data 66
- Channel Status workspaces
  - collecting data 66
- Channels tag 24
- checking
  - WebSphere MQ Client existence, AIX 197
  - WebSphere MQ Client existence, Linux 197
  - WebSphere MQ Client existence, Windows 197
- clearing a local queue 146
- cluster channel information 123
- cluster environment
  - configuration overview, AIX 163
  - configuration overview, Windows 151
  - configuration, AIX 166
  - configuration, Windows 154, 158
- Cluster Queue Manager Summary chart 123
- Cluster Queue Manager workspaces
  - description 123
  - guide for action 123
- clustering configuration
  - active/active clustering prerequisites
    - Windows 153
  - active/passive clustering prerequisites
    - AIX 165
    - Windows 157
- Cognos reports
  - Broker Elapsed Microseconds report 110
  - Channel Daily Availability report 110
  - Channel Weekly Availability report 110
  - installation 106
  - Queue Full Detail report 110
  - Queue Manager Daily Availability report 110
  - Queue Manager Weekly Availability report 110
  - Top N Queue Full report 110
  - troubleshooting 113
- collecting
  - message statistics 129
- collecting data
  - Application Accounting workspace 63
  - Application Debugging workspace 64
  - Application Statistics workspaces 65
  - Buffer Pool Statistics workspaces 65
  - Channel Performance workspaces 66
  - channel related workspaces 66
  - Channel Status workspaces 66
  - Event Log workspace 67
  - Log Manager workspaces 72
  - Message Manager workspaces 72
  - MQ Channel Statistics workspace 74
  - MQ Queue Statistics workspace 75
  - MQI statistics workspace 73
  - MQSeries Events workspace 73
  - Queue Accounting workspace 68

- collecting data (*continued*)
  - queue related workspaces 76
  - Queue Statistics workspace 69
  - Queue Statistics workspace for z/OS 70
  - Queue Status workspace 71
  - Topic Manager workspaces 77
- commands
  - description, Take Action 60
  - enabling the application accounting messages 116
  - enabling the MQI statistics messages 131
  - executing external customization 48
  - Reset Queue Statistics 95
  - sending 61
  - tacmd 20
  - using, in situations 61
  - WRKOMAMQ 17
- configuration
  - active/active clustering, AIX 166
  - active/active clustering, Windows 154
  - active/passive clustering, AIX 166
  - active/passive clustering, Windows 158
  - cluster nodes, active/active clustering 154
  - cluster nodes, active/passive clustering 158
  - remote agents
    - Agent Name parameters 25
    - Channels parameters 24
    - Event Log parameters 24
    - Event Queues In parameters 24
    - Event Queues Out parameters 25
    - General Agent Settings parameters 21
    - Include File parameters 25
    - Queue Access parameters 23
    - Queue Manager Group parameters 22
    - Queues parameters 24
    - Start Monitoring parameters 25
  - remote agents, from the command line 20
  - remote agents, from Tivoli Enterprise Portal 20
  - remote agents, overview 20
  - WebSphere MQ objects 199
  - WebSphere MQ objects, using Tivoli OMEGAMON DE 8
- configuration prerequisites
  - active/active clustering, AIX 163
- configuring
  - remote agents
    - Agent parameters 26
- creating
  - Take Action command 60
  - workspaces 116
- creating situations 59

## D

- DASD log files 127
- data collection
  - background-collected 173
  - historical 79
  - modes 173
  - on-demand 173
  - sampled 173
- data model
  - Cognos reports 109
- Dead-Letter Queue Messages workspaces
  - accessing 123
  - deleting messages 124
  - description 123
  - forwarding messages 124
  - guide for action 123

- dead-letter queues
  - deleting messages from 124
  - forwarding messages to 124
  - management 123
- debugging trace data
  - sorting 118
  - viewing 118
- deleting
  - messages, from a queue 149
  - messages, from dead-letter queues 124
- delivering failures
  - resolutions 103
- displaying
  - historical data, for a selected time frame 83

## E

- enabling
  - historical data collection, i5/OS 81
  - historical data collection, UNIX and Linux 80
  - historical data collection, Windows 80
  - historical data collection, z/OS 82
  - queue statistics data collection 96
- end user action information 130
- ERRLOGCYCLE parameter 125
- ERRLOGMAX parameter 125
- error log files 126
- Error Log monitoring feature 125
- Error Log workspaces
  - description 125
  - guide for action 126
- error logs
  - collection interval 27, 30
  - default location 125
  - maximum number of messages displayed 27, 30
- error messages
  - KFWITM217E 130
  - KMQMI209E 129
  - KMQMI210E 129
- event indicators
  - description 4
- Event Log tag 24
- Event Log workspace
  - collecting data 67
- Event Queues In tag 24
- Event Queues Out tag 25
- event workspaces 4
- events
  - acknowledgments 6
  - monitoring, on non-supported systems 177

## F

- features
  - Error Log monitoring 125
  - Message Statistics 128
  - Queue Statistics 95
  - queue-sharing group monitoring 148
  - Tivoli OMEGAMON DE 8
- forwarding
  - messages, to dead-letter queues 124
  - messages, to selected queues 150

## G

- General Agent Settings tag 21
- glossary 209
- graphical representation
  - queue manager connections 137

## H

- High Availability Cluster Multi Processing (HACMP) 163
- historical data
  - disks space summary worksheets 195
  - space requirement worksheets 188
  - viewing, for a selected time frame 83
- historical data collection
  - attributes 82
  - enabling, i5/OS 81
  - enabling, UNIX and Linux 80
  - enabling, Windows 80
  - enabling, z/OS 82
  - overview 79
  - starting 82
  - stopping 83
  - table record sizes 187
- historical data tables
  - description 185
  - disk space requirements 185
  - record sizes 187
- HISTORY parameter
  - i5/OS 81
  - Linux 80
  - UNIX 80
  - Windows 80

## I

- IBM Tivoli Monitoring
  - agents 7
  - clients 6
  - information links 9
  - overview 6
  - servers 6
  - Tivoli Enterprise Portal Server 6
- Include File tag 25

## K

- KFW\_TOPOLOGY\_CLUSTER\_LIST variable
  - AIX 166
  - Windows 154, 158
- KFWITM217E error message 130
- KMQ\_HISTCOLL\_DATA\_FLAG 82
- KMQMI209E error message 129
- KMQMI210E error message 129

## L

- legal notices 205
- library 203
- links
  - predefined, at application nodes 144
  - predefined, at queue manager nodes 143
  - predefined, at queue nodes 144
  - predefined, in Application Topology view 143
- local queues
  - clearing 146

- Log Data Set Status workspace
  - description 126
  - guide for action 126
- log data sets 126
- Log Manager Performance workspaces
  - description 126
  - guide for action 127
- Log Manager workspaces
  - collecting data 72
- logging activity workspaces 126

## M

- managed system names 50
- mapping table
  - attribute groups
    - historical workspaces 85
  - historical workspaces
    - attribute groups 85
- MaxRow\_AppTop parameter 139, 141
- message access
  - setting authorization level 90
- message delivery failures
  - resolving 103
- Message Manager Performance workspaces
  - description 127
  - guide for action 127
- Message Manager workspaces
  - collecting data 72
- message manipulation
  - viewing action information 131
- Message Manipulation Access settings 91
- Message Manipulation Account settings 91
- message statistics
  - collecting 129
- Message Statistics feature 128
- message statistics summary 128
- Message Statistics workspaces
  - description 128
  - guide for action 130
- messages
  - access control 89
  - deleting from a local queue 145
  - deleting, from a queue 149
  - deleting, from dead-letter queues 124
  - forwarding to another queue 150
  - manipulation 130
    - overview 89
    - settings for access control 89
  - viewing action information 130
- monitoring
  - events, on non-supported systems 177
  - multi-instance queue managers 18
  - multiple queue managers
    - i5/OS 12
    - Linux 12
    - UNIX 12
    - Windows 11
  - multiple queue managers, on remote systems 182
  - queue depth 98
  - queue managers, on non-supported systems 179
  - remote queue managers
    - limitations 183
    - overview 179
- monitoring agents
  - description 7

- monitoring options
  - activating application debugging, z/OS 53
  - activating application statistics, z/OS 53
  - changing
    - i5/OS 17
    - Linux 14
    - UNIX 14
    - Windows 15
  - controlling message access 90
  - default 26
  - defining queue manager groups 26
  - description 26
  - disabling historical data collection 48
  - enabling external customization commands 48
  - enabling historical data collection 48
  - identifying output queues 46
  - mq.cfg file
    - Linux 14
    - UNIX 14
    - Windows 15
  - specifying applications to be monitored, z/OS 51
  - specifying channels to be monitored 41
  - specifying event log attributes 42
  - specifying event queues to be monitored 43
  - specifying message access rights 36
  - specifying middle qualifiers of managed system names 50
  - specifying queue managers to be monitored 29
  - specifying queue-sharing groups, z/OS 55
  - specifying queues to be monitored 39
  - specifying sampling intervals 48
  - subsystems for application statistics 56
- MQ Action Log workspace
  - description 130
  - guide for action 131
- MQ Channel Statistics workspace
  - collecting data 74
- MQ Queue Statistics workspace
  - collecting data 75
- MQ search 99
- mq.cfg file
  - editing
    - Linux 14
    - UNIX 14
    - Windows 15
- MQI statistics messages
  - enabling commands 131
- MQI Statistics workspace
  - collecting data 73
- MQI Statistics workspaces
  - description 131
  - guide for action 132
- MQSeries Events workspace
  - collecting data 73
- MQSeries Events workspaces
  - description 132
  - guide for action 133
- MQSeries\_Channel\_Out\_Of\_Sync situation 125
- MQSeries\_Delayed\_Message\_Group situation 128
- MQSeries\_High\_Delayed\_Messages situation 128
- MQSeries\_Local\_DestQ\_Depth\_High situation 98
- MQSeries\_No\_Queue\_Messages\_Read situation 95
- MQSeries\_QSG\_\* situation 148
- MQSeries\_Queue\_Depth\_High situation 98, 101
- MSCS clusters
  - overview 151
  - WebSphere MQ clusters 151
- MSGACCESS parameter 89, 90

- MSGACCESS settings
  - working with WebSphere MQ security settings 91
- multi-instance queue manager
  - monitoring requirements 18
- multiple instances
  - creating
    - overview 11
- multiple queue managers
  - remote monitoring 182

## N

- new features 1
- NPMMSGDLV variable 103

## O

- OAM authorities
  - granting 201
- objects
  - configuring 199
- OUTBUFF parameter 127
- overflow alerts 101

## P

- Page Set Statistics workspaces
  - description 134
  - guide for action 134
- page sets
  - storage monitoring 134
- parameters
  - ERRLOGCYCLE 125
  - ERRLOGMAX 125
  - MaxRow\_AppTop 139, 141
  - MSGACCESS 89, 90
  - OUTBUFF 127
  - QDEFTYPE 136
  - remote agent configuration
    - Agent 26
    - Agent Name 25
    - Channels 24
    - Event Log 24
    - Event Queues In 24
    - Event Queues Out 25
    - General Agent Settings 21
    - Include File 25
    - Queue Access 23
    - Queue Manager Group 22
    - Queues 24
    - Start Monitoring 25
  - STATISTICS 96, 118
  - TRACE 118
- PERFORM INCLUDE statement 48
- PERFORM STARTMON statement 48
- performance history 119
- PMSGDLV variable 103
- Policy management 9
- predefined links
  - Application Topology view
    - at application nodes 144
    - at queue manager nodes 143
    - at queue nodes 144
- predefined situations
  - MQSeries\_Channel\_Out\_Of\_Sync 125
  - MQSeries\_Delayed\_Message\_Group 128

- predefined situations (*continued*)
  - MQSeries\_High\_Delayed\_Messages 128
  - MQSeries\_Local\_DestQ\_Depth\_High 98
  - MQSeries\_QSG\_\* 148
  - MQSeries\_Queue\_Depth\_High 98
  - overview 59
- predefined workspaces 115
- preventing
  - queue overflow 101
- primary agents 11
- properties editor 115
- publications 203
- publish subscribe information
  - searching 99
- Publish Subscribe workspaces
  - description 135
  - guide for action 135
- publishing failures
  - cause 103
  - resolving 103
- Purge Queue (MQGET) 145
- purging a local queue 145

## Q

- QDEFTYPE 66, 76
- QDEFTYPE parameter 136
- queries 4
- Query editor 4
- Queue Access tag 23
- Queue Accounting workspace
  - collecting data 68
- Queue Definitions Summary chart 135
- Queue Definitions workspaces
  - description 135
  - guide for action 136
- queue depth
  - monitoring situations 98
- Queue Manager Group tag 22
- Queue Manager Status workspaces
  - Application Topology view 137
  - description 136
  - guide for action 136
- queue managers
  - monitoring events 132
  - monitoring requirements, multi-instance 18
  - monitoring, on non-supported systems 179
  - remote monitoring
    - limitations 183
  - remote monitoring, on non-supported operating systems
    - prerequisites 180
    - usage information 144
- Queue Messages workspace
  - description 148
  - guide for action 149
- queue overflow
  - preventing 101
- queue related workspaces
  - collecting data 76
- queue statistics
  - enabling data collection 96
  - influence on queue service interval events 96
  - monitoring 95
- Queue Statistics
  - overview 95
- Queue Statistics feature
  - coexistence with Application Statistics 96

- Queue Statistics feature (*continued*)
  - influence on queue events 96
- Queue Statistics Summary chart 144
- Queue Statistics workspace 146
  - collecting data 69
  - collecting data, for z/OS 70
- Queue Statistics workspaces
  - description 144
  - guide for action 146
- Queue Status workspace
  - collecting data 71
- queue-sharing group monitoring feature 148
- Queue-Sharing Group workspaces
  - description 147
  - guide for action 147
- queues
  - usage information 144
- Queues tag 24

## R

- remote agents
  - configuration overview 20
  - configuration, from the command line 20
  - configuration, from Tivoli Enterprise Portal 20
- remote configuration
  - command line 20
  - overview 20
  - parameters 21
    - Agent 26
    - Agent Name 25
    - Channels 24
    - Event Log 24
    - Event Queues In 24
    - Event Queues Out 25
    - General Agent Settings 21
    - Include File 25
    - Queue Access 23
    - Queue Manager Group 22
    - Queues 24
    - Start Monitoring 25
  - Tivoli Enterprise Portal 20
- remote monitoring
  - limitations 183
  - non-supported operating systems
    - prerequisites 180
  - overview 179
  - setting up the environment 180
- report package 105
- reports
  - creating, web-based 108
- requirements
  - disk space
    - historical data tables 185
- reset
  - queue statistics 95
- Reset Queue Statistics command 95, 96
- resolving
  - publishing failure 103

## S

- searching
  - subscriptions 99
  - topics 99
  - WebSphere MQ events 134

- secondary agents 11
- security
  - implementing for messages 91
- security checking 119
- sending
  - messages, to another queue 150
  - messages, to dead-letter queues 124
  - Take Action commands 61
- SET AGENT statement 50
- SET APPL statement 51
- SET CHANNEL statement 41
- SET EVENTLOG statement 42
- SET EVENTQIN statement 43
- SET EVENTQOUT statement 46
- SET GROUP statement 26
- SET MANAGER statement 29
- SET MQIMONITOR statement 53
- SET QACCESS statement 36
- SET QSG statement 55
- SET QUEUE 76
- SET QUEUE statement 39
- SET SUBSYSTEM statement 56
- situations
  - creating 59
  - description 7
  - MQSeries\_No\_Queue\_Messages\_Read 95
  - MQSeries\_Queue\_Depth\_High 101
  - predefined
    - MQSeries\_Channel\_Out\_Of\_Sync 125
    - MQSeries\_Delayed\_Message\_Group 128
    - MQSeries\_High\_Delayed\_Messages 128
    - MQSeries\_Local\_DestQ\_Depth\_High 98
    - MQSeries\_QSG\_\* 148
    - MQSeries\_Queue\_Depth\_High 98
  - overview 59
  - queue depth monitoring 98
- sorting
  - debugging trace data 118
- Start Monitoring tag 25
- starting
  - historical data collection 82
- STATISTICS parameter 96, 118
- stopping
  - historical data collection 83
- subscriptions
  - monitoring the queue depth 98
  - preventing queues from overflowing 101
  - searching 99
- topology
  - overview 97
  - viewing 101
- supported WebSphere MQ versions 1

## T

- tables
  - data collection types 173
  - historical data 185
  - supported operating systems 173
- tacmd command 20
- tags
  - Agent 26
  - Agent Name 25
  - Channels 24
  - Event Log 24
  - Event Queues In 24
  - Event Queues Out 25

- tags *(continued)*
  - General Agent Settings 21
  - Include File 25
  - Queue Access 23
  - Queue Manager Group 22
  - Queues 24
  - Start Monitoring 25
- Take Action command
  - creating 60
- Take Action commands
  - description 60
  - sending 61
  - using in situations 61
  - viewing action information 130, 131
- Tivoli Common Reporting
  - creating ad-hoc reports 108
  - creating web-based reports 108
  - data model 109
  - installing Cognos reports 106
  - overview 105
  - prerequisites 105
  - running Cognos reports 107
  - sample reports 110
  - supported attribute groups 105
  - troubleshooting 113
- Tivoli Enterprise Monitoring Server 6
- Tivoli Enterprise Portal
  - attributes 2
  - browser client 6
  - desktop client 6
  - navigator view 2
  - predefined situations 2
  - workspaces 2
- Tivoli OMEGAMON DE
  - access control 8
  - description 7
  - operation details 8
  - prerequisites 8
  - workspaces 8
- Topic Manager Performance workspaces
  - description 150
  - guide for action 150
- Topic Manager workspaces
  - collecting data 77
- topics
  - searching 99
  - viewing the subscription topology for 101
- TRACE parameter 118
- trademarks 207
- trend analysis 119
- troubleshooting
  - delivering failures 103
  - incomplete queue statistics information 96
  - publishing failures 103
  - queue service interval events malfunction 96

## U

- user accounts
  - setting message access authorization level 90
- user interface
  - overview 2
  - Tivoli Enterprise Portal 2
- user-defined situations 59
- user-defined workspaces 116

## V

- variables
  - KFW\_TOPOLOGY\_CLUSTER\_LIST, AIX 166
  - KFW\_TOPOLOGY\_CLUSTER\_LIST, Windows 154, 158
  - NPMMSGDLV 103
  - PMSGDLV 103
- viewing
  - debugging trace data 118
  - historical data 83
  - subscription topology 101
- views
  - description 115

## W

- WebSphere MQ
  - object configuration, using Tivoli OMEGAMON DE 8
  - security settings for different message access levels 91
  - tracing applications 118
  - versions 1
- WebSphere MQ Client
  - existence checking
    - AIX 197
    - Linux 197
    - Windows 197
- WebSphere MQ Configuration agent
  - working with 199
- WebSphere MQ events
  - searching 134
- WebSphere MQ messages
  - access controlling 89
  - setting access authorization level 90
- WebSphere MQ Monitoring agent
  - agent suffixes 12
  - creating multiple instances
    - i5/OS 12
    - Linux 12
    - overview 11
    - UNIX 12
    - Windows 11
  - overview 1, 2
- WebSphere MQ objects
  - configuring 199
- Workflow editor 9
- worksheets
  - historical disk space summary 195
  - historical space requirement 188
- workspaces
  - additional information 150
  - Application Accounting
    - description 116
    - guide for action 117
  - Application Debugging
    - description 118
    - guide for action 118
  - Application Statistics
    - description 118
    - guide for action 119
  - Buffer Pool Statistics
    - description 119
    - guide for action 119
  - Channel Definitions
    - Channel Definitions Summary chart 120
    - description 120
    - guide for action 121

- workspaces (*continued*)
  - Channel Initiator Status
    - description 121
    - guide for action 121
  - Channel Performance
    - description 122
    - guide for action 122
  - Cluster Queue Manager
    - description 123
    - guide for action 123
  - communication systems
    - error detection 121
    - processing capacity improvement 121
  - creating 116
  - customizing time spans 115
  - Dead-Letter Queue Messages
    - accessing 123
    - deleting messages 124
    - description 123
    - forwarding messages 124
    - guide for action 123
  - description 115
  - Enterprise Wide Subscription Definitions workspace 135
  - Error Log
    - description 125
    - guide for action 126
  - event 4
  - event queues
    - exception checking 133
  - Log Data Set Status
    - description 126
    - guide for action 126
  - Log Manager Performance
    - description 126
    - guide for action 127
  - Message Manager Performance
    - API calling frequency 127
    - description 127
    - guide for action 127
  - Message Statistics
    - data availability 129
    - description 128
    - guide for action 130
  - MQ Action Log
    - description 130
    - guide for action 131
  - MQI Statistics
    - description 131
    - guide for action 132
  - MQSeries Events
    - description 132
    - guide for action 133
  - overview 115
  - Page Set Statistics
    - description 134
    - guide for action 134
  - predefined 115
  - publication subscription 150
  - Publish Subscribe
    - description 135
    - guide for action 135
  - Queue Definitions
    - description 135
    - guide for action 136
  - Queue Manager Status
    - Application Topology view 137
    - description 136

- workspaces (*continued*)
  - Queue Manager Status (*continued*)
    - guide for action 136
  - Queue Messages
    - description 148
    - guide for action 149
  - Queue Statistics
    - description 144
    - guide for action 146
  - queue subsets 146
  - Queue-Sharing Group
    - description 147
    - guide for action 147
  - queue-sharing groups
    - viewing status 147
  - SCAN function 146
  - statistics messages 131
  - STR function 146
  - Subscriptions Definitions workspace 135
  - supporting search function 99
  - Tivoli OMEGAMON DE related 8
  - Topic Definitions workspace 135
  - Topic Manager Performance
    - description 150
    - guide for action 150
  - Topic Status workspace 135
  - user-defined 116
  - views 115
- WRKOMAMQ command 17





Printed in USA

SC14-7523-01

