

WebSphere Event Broker



Configuration, Administration, and Security

Version 6 Release 0

WebSphere Event Broker



Configuration, Administration, and Security

Version 6 Release 0

Note

Before using this information and the product it supports, read the information in the Notices appendix.

Fourth Edition (July 2006)

This edition applies to IBM® WebSphere® Event Broker Version 6.0 and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2000, 2006. All rights reserved.

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

Contents

About this topic collection. v

Part 1. Security 1

Security. 3

Security overview 3

Planning for security when you install WebSphere

Event Broker 11

Setting up broker domain security. 11

Setting up z/OS security 28

Publish/subscribe security 32

Securing the publish/subscribe domain 41

Part 2. Configuring the broker domain 49

Configuring the broker domain 51

Designing a broker domain 52

Customizing the z/OS environment 60

Configuring broker domain components. 83

Configuring a broker domain in the workbench 171

Configuring a publish/subscribe topology. 182

Configuring the workbench 199

Changing locales 202

Part 3. Administering the broker domain 209

Administering the broker domain. 211

Connecting to and disconnecting from the broker domain 211

| Connecting to and disconnecting from the broker domain on z/OS 212

Starting and stopping message flows 214

Starting and stopping a broker 214

Starting and stopping a Configuration Manager 216

Starting and stopping the User Name Server 217

Starting a WebSphere MQ queue manager as a Windows service 219

Stopping a WebSphere MQ queue manager when you stop a component 220

Viewing broker domain log information 220

Refreshing broker domain log information. 221

Filtering broker domain log information 222

Saving broker domain log information 223

Clearing broker domain log information 224

Changing Event Log editor preferences. 224

Backing up resources. 225

Part 4. Reference 229

Operations 231

Broker properties 231

Commands 232

z/OS specific information 367

Security requirements for administrative tasks 423

ACL permissions 423

Security requirements for Linux and UNIX platforms. 424

Security requirements for Windows platforms 425

Security requirements for z/OS 428

Part 5. Appendixes 431

Appendix. Notices 433

Trademarks 435

Index 437

About this topic collection

This PDF has been created from the WebSphere Event Broker Version 6.0 (Fix Pack 2 update, July 2006) information center topics. Always refer to the WebSphere Event Broker online information center to access the most current information. The information center is periodically updated on the document update site and this PDF and others that you can download from that Web site might not contain the most current information.

The topic content included in the PDF does not include the "Related Links" sections provided in the online topics. Links within the topic content itself are included, but are active only if they link to another topic in the same PDF collection. Links to topics outside this topic collection are also shown, but these attempt to link to a PDF that is called after the topic identifier (for example, ac12340_.pdf) and therefore fail. Use the online information to navigate freely between topics.

Feedback: do not provide feedback on this PDF. Refer to the online information to ensure that you have access to the most current information, and use the Feedback link that appears at the end of each topic to report any errors or suggestions for improvement. Using the Feedback link provides precise information about the location of your comment.

The content of these topics is created for viewing online; you might find that the formatting and presentation of some figures, tables, examples, and so on are not optimized for the printed page. Text highlighting might also have a different appearance.

Part 1. Security

Security	3
Security overview	3
Authorization for configuration tasks	3
Security for development resources	4
Authorization to access runtime resources	4
Access Control Lists	5
Security exits	8
SSL authentication	8
Tunneling	9
Quality of protection	10
Domain awareness	10
Planning for security when you install WebSphere	
Event Broker	11
Setting up broker domain security	11
Creating user IDs	12
Considering security for the workbench	13
Considering security for a broker	15
Considering security for a Configuration Manager	16
Changing the security domain for the User Name Server	19
Implementing SSL authentication	19
Enabling topic-based security	23
Using security exits	26
Implementing HTTP tunneling	26
Implementing quality of protection	26
Database security	27
Setting up z/OS security	28
Setting up DB2	29
Setting up WebSphere MQ	30
Setting up workbench access on z/OS	31
Creating Publish/Subscribe user IDs	31
Enabling the Configuration Manager on z/OS to	
obtain user ID information	31
Publish/subscribe security	32
Topic-based security	32
Authentication services	37
Message protection	40
Securing the publish/subscribe domain	41
Enabling topic-based security	41
Creating ACL entries	43
Using authentication for real-time connections	43
Using message protection	47
Securing WebSphere MQ resources	47

Security

The topics in this section help you to deal with security in WebSphere Event Broker:

- “Security overview”
- “Planning for security when you install WebSphere Event Broker” on page 11
- “Setting up broker domain security” on page 11
- “Setting up z/OS security” on page 28
- “Publish/subscribe security” on page 32
- “Securing the publish/subscribe domain” on page 41

Security overview

The role of the WebSphere Event Broker system administrator includes customizing and configuring, running utilities, performing problem determination, and collecting diagnostic materials. People involved in these activities need WebSphere Event Broker authorities. There is some security setup that you must do for WebSphere Event Broker to work properly. There is also some security setup that people typically do, for example, protecting queues against unauthorized use.

Security is split into several areas:

- “Authorization for configuration tasks”
- “Security for development resources” on page 4
- “Authorization to access runtime resources” on page 4
- “Security exits” on page 8
- “SSL authentication” on page 8 (for the Real Time node only)
- “Tunneling” on page 9
- “Quality of protection” on page 10
- “Domain awareness” on page 10.

Authorization for configuration tasks

Authorization is the process of granting or denying access to a system resource. For WebSphere Event Broker, authorization is concerned with controlling who has permission to access WebSphere Event Broker resources, and ensuring that users who attempt to work with those resources have the necessary authorization to do so.

Examples of tasks that require authorization are:

- Configuring a broker using, for example, the “mqsicreatebroker command” on page 286.
- Accessing queues, for example, putting a message to the input queue of a message flow.
- Taking actions within the workbench, for example, deploying a message flow to an execution group.
- Publishing topics and subscribing to topics, as described in “Enabling topic-based security” on page 23

Authorization for existing resources

If you want to use the security facilities of Version 6.0, when you require access to a resource that already exists, the user ID with which you work must be included in the Access Control List (ACL) for that resource.

For authorization to create resources, for example brokers, you must be a member of the **Administrator** local group.

The security architecture of WebSphere Event Broker is platform independent. If you are running in a heterogeneous environment, ensure that you limit all the principals you define for WebSphere Event Broker tasks to eight characters or fewer. If you have a Windows-only environment, you can create principals of up to twelve characters, but only use these longer names if you are sure that you will not later include a Linux, UNIX, or z/OS system in your WebSphere Event Broker network.

Security for development resources

Security for development resources must be addressed and defined by the application development organization. No special facilities are provided by WebSphere Event Broker to address this environment over and above those available for a production environment.

Authorization to access runtime resources

Runtime resources are WebSphere Event Broker objects that exist at run time in the broker domain. Each runtime object has an Access Control List (ACL) which determines which users and groups can access the object. The ACL entries for an object can permit a user or group to view the object or view and modify the object from the workbench, the command line, or using the Configuration Manager Proxy (CMP).

ACLs allow or deny access for a user to an object but ACL entries do not secure the object; that is, the ACL entry cannot verify the user's identity.

Using ACL entries, you can control users' access to specific objects in the broker domain. For example, user JUNGLE\MPERRY might be given access to modify BROKERA, but have no access rights to BROKERB. In a further example the same user might have access to deploy to execution group EXEGRP1, but not to EXEGRP2, even though they are both members of BROKERA.

When you try to view or modify an object for which you require permission, the following information is passed to the Configuration Manager:

- Object type
- Object name
- Requested action
- Your user ID.

The Configuration Manager checks the ACL table. If your user ID is included in the ACL entry for the named object, you are authorized to perform the operation.

Refer to Related reference information below for descriptions of the tools that system administrators use to control the ACLs.

ACL entries and groups

In previous versions of WebSphere Event Broker, access to runtime objects was controlled by defining a set of groups and assigning users to those groups. ACL entries enable you to control access with more granularity than groups. ACL entries also enable a single Configuration Manager to manage development, test, and production systems separately by configuring users' access to each broker. Using groups, you would have to place the development, test, and production systems in separate broker domains, each controlled by a separate Configuration Manager.

If you migrate a Configuration Manager from a previous version of WebSphere Event Broker, ACL entries are automatically defined for the following groups:

- mqbrkrs
- mqbrops
- mqbrdevt
- mqbrasgn
- mqbrtpic

Without these ACL entries, users that belong to these groups do not have authority to perform actions on the objects in the domain.

Access Control Lists

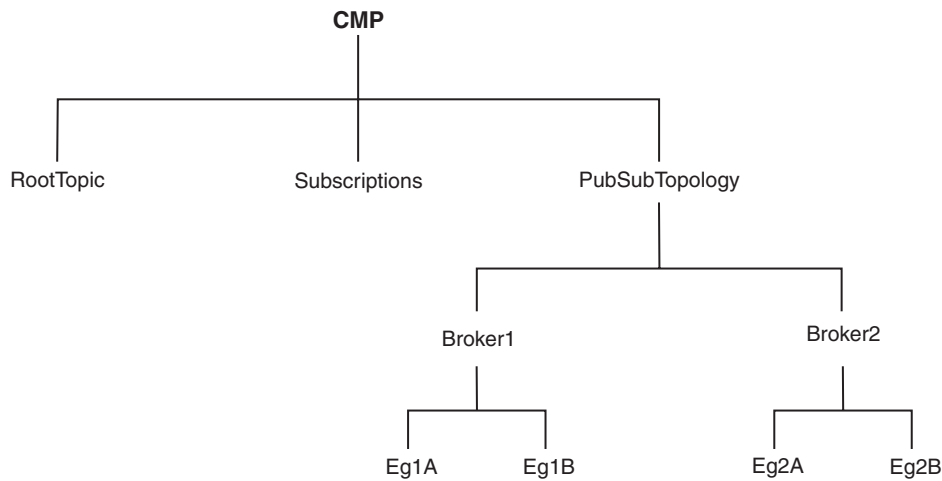
Access Control List (ACL) entries allow or deny a user to access an object. ACL entries do not, however, secure the object because the ACL entry cannot verify the user's identity. An ACL entry contains the user name and can specify a host name or domain name. It is possible, for example, for a user to get access to the objects by creating an account on a computer that has a host name that is the same as an authorized Windows domain name. Use ACL entries to control access to the objects in the broker domain but do not rely on ACL entries to secure your broker domains; use SSL or security exits to secure the channels between components in the broker domain.

WebSphere Event Broker uses Access Control List (ACL) entries to govern which users and groups can manipulate objects in the broker domain. There are four different access levels that can be granted for a user or group: Full, View, Deploy, and Edit. Not all access levels are valid for all object types; see "ACL permissions" on page 423 for a list of the permissions that can be applied to each object type and a summary of the actions that the user or group can perform.

In order to reduce the number of access control entries that a broker administrator must create, the ACL permissions behave in a hierarchical manner. The root of the tree is the ConfigManangerProxy object, which has three children: RootTopic, Subscriptions, and PubSubTopology. The PubSubTopology object has zero or more brokers as children, and each broker can have zero or more execution groups as children. When an ACL entry is added to a given object, that permission is granted to that object and to all objects beneath it in the hierarchy, unless it is overridden by another ACL entry.

On z/OS, you must define an OMVS segment for user IDs and groups, in order for a Configuration Manager to obtain user ID and group information from the External Security Manager (ESM) database.

The following diagram shows an example hierarchy:



The following examples show how this hierarchical behavior works in practice.

Example 1

UserA has no access control entries. Therefore, UserA cannot manipulate any objects in the hierarchy, or see any of the objects defined in the hierarchy.

Example 2

UserB has an ACL entry that gives him Deploy authority to the execution group Eg1A. This gives him implied View authority to PubSubTopology and Broker1. UserB must be able to view PubSubTopology and Broker1 (for example, in the Message Brokers Toolkit) to be able to deploy to Eg1A.

Because UserB does not have any ACL entries for PubSubTopology or Broker1, UserB does not inherit access to the other broker or execution groups in the hierarchy. In practice, this means that UserB can see that there is another execution group defined on the broker Broker1 but cannot see any details (including the execution group's name). Similarly, UserB can see that another broker exists within the topology, but cannot see any details. UserB has no access to RootTopic or to Subscriptions (the subscriptions table).

The following command creates the ACL entry for UserB:

```
mqsicreateaclentry testcm -u UserB -a -x D -b Broker1 -e Eg1A
```

The `mqsilistaclentry` command then displays the following information:

```
BIP1778I: userb -USER - D - Broker1/Eg1A - ExecutionGroup
```

Example 3

UserC has an ACL entry that gives her View authority for the Configuration Manager Proxy (CMP), and an ACL entry that gives her Full authority for Broker1. This gives her the following authorities:

```
CMP View
RootTopic View
```

```
| Subs View
| Topology View
| Broker1 Full
| Eg1A Full
| Eg1B Full
| Broker2 View
| Eg2A View
| Eg2B View
```

The following commands create the ACL entries for UserC:

```
| mqsicreateaclentry testcm -u UserC -a -x V -p
| mqsicreateaclentry testcm -u UserC -a -x F -b Broker1
```

The `mqsilistaclentry` command then displays the following information:

```
| BIP1778I: userc - USER - V - ConfigManagerProxy - ConfigManagerProxy
| BIP1778I: userc - USER - F - Broker1 - Broker
```

Example 4

UserD has an ACL entry that gives him Full authority for the CMP and an ACL entry that gives him View authority for Broker1. By giving UserD View authority to access Broker1, UserD does not inherit Full authority. This use of View ACL entries is useful because it allows users who usually have full control over a given object to reduce their access temporarily in order to prevent accidental deletion or deployment. If the user needs full control of the object, removing the View entry restores Full authority, so that they can perform the operations that they need, then restore the View entry. UserD has the following authorities:

```
| CMP Full
| RootTopic Full
| Subs Full
| Topology Full
| Broker1 View
| Eg1A View
| Eg1B View
| Broker2 Full
| Eg2A Full
| Eg2B Full
```

The following commands create the ACL entries for UserD:

```
| mqsicreateaclentry testcm -u UserD -a -x F -p
| mqsicreateaclentry testcm -u UserD -a -x V -b Broker1
```

The `mqsilistaclentry` command then displays the following information:

```
| BIP1778I: userd - USER - F - ConfigManagerProxy - ConfigManagerProxy
| BIP1778I: userd - USER - V - Broker1 - Broker
```

The following command can then delete the ACL entries for UserD:

```
| mqsdeleteaclentry testcm -u UserD -a -b Broker1
```

To change the access control entries for an object, a user must have Full authority for that object or any parent in the hierarchy. This means that the permission to change the ACLs themselves works in the same way as described above, with the exception that access to the ACLs cannot be removed by granting a lower permission further down the tree; this is necessary because otherwise a user would be able to give themselves a View entry and would not then be able to remove it.

ACL entries can be manipulated using the Java Configuration Manager Proxy API or using the `mqsicreateaclentry`, `mqsdeleteaclentry`, and `mqsilistaclentry` commands.

Security exits

You can use security exit programs to verify that the partner at the other end of the channel is genuine.

When you start the Message Brokers Toolkit, it does not invoke a security exit to monitor its connection to the Configuration Manager by default. If you want to protect access to the Configuration Manager from client programs, you can use the WebSphere MQ channel security exit facility. This works in a standard way for the Configuration Manager end of the connection. You can find information about how to set up the security exit at the server end of the connection in the *WebSphere MQ Intercommunication* manual.

If you want to use a security exit, define when creating a new domain within the Domains view of the Message Brokers Toolkit to provide connection security. These security exits are standard WebSphere MQ security exits, written in Java, and implementing the WebSphere MQ exit interface.

For an overview of security exits, refer to the section "Channel security exit programs" in the chapter "Channel exit programs" in the *WebSphere MQ Intercommunication* manual on the WebSphere MQ library Web page.

SSL authentication

SSL authentication is available for the Real Time node, the HTTP listener, and the WebSphere MQ Java Client.

SSL authentication for the Real Time node

SSL authentication in WebSphere Event Broker supports an authentication protocol known as *mutual challenge-response password authentication*. This is a non-standard variant of the industry standard SSL protocol in which the public key cryptography called for by SSL is replaced by symmetric secret key cryptography. While this protocol is both secure and convenient to administer, it might be better to use the industry standard SSL protocol exactly as defined, especially if a public key cryptography infrastructure is already deployed for other purposes. There are two standardized versions of SSL which are:

Asymmetric SSL

This is used by most Web browsers. In this protocol, only the brokers have public/private key pairs and clients know the brokers' public keys. The SSL protocol establishes a secure connection in which the broker is authenticated to the client using public key cryptography, after which the client can send its password, encrypted by a secure session key, to authenticate itself to the broker.

Symmetric SSL

This is where both participants have public/private key pairs. The SSL protocol uses public key cryptography to accomplish mutual authentication.

In both instances, SSL authentication does not keep the SSL protocol up for the entire lifetime of a connection, because that would incur protection overheads on all messages. The SSL protocol remains in force long enough to accomplish mutual

authentication and to establish a shared secret session key that can be used by message protection (see “Message protection” on page 40). Messages are then individually protected in accordance with the protection level specified for the given topic.

The SSL protocol implementation requires a Public-Key Cryptography Standards (PKCS) file, containing X.509 V3 certificates for the broker’s private key, and possibly the public keys of clients and other brokers. This file, called the key ring file, must contain at least one certificate for the broker and for the trusted certification authority (CA) that issued and signed the broker’s certificate. For the R form of SSL, the key ring file can also have the public keys of clients and other brokers that need to be authenticated, and the certificates supporting those public keys. However, the SSL protocol calls for the exchange of public keys and certificates, so key ring files do not need to be fully primed in this fashion, as long as there are enough commonly-trusted authorities to ensure that authentication completes.

By convention, key ring files are encrypted and protected by a passphrase, which is stored in a second file. The passphrase file requires careful protection using operating system mechanisms to ensure that it is not exposed to unauthorized observers. An observer who learns the passphrase can learn the private keys in the key ring file. However, only the passphrase file needs to be secure in this way and the key ring file is protected by the passphrase. Only private keys are sensitive. Other information in the key ring file, such as the broker’s certificates, can be revealed without compromising security.

For more information on SSL authentication for the Real Time node, see “Enabling SSL for the Real Time node” on page 20.

SSL authentication for the HTTP listener

For information on SSL authentication for the HTTP listener, see Configuring HTTPInput and HTTPReply nodes to use SSL (HTTPS), and Configuring an HTTPRequest node to use SSL (HTTPS).

SSL authentication for the MQ Java Client

For information on SSL authentication for the MQ Java Client, see “Enabling SSL on the WebSphere MQ Java Client” on page 19.

Tunneling

When implementing WebSphere Event Broker, both the clients and their brokers can reside on different intranets, that is, separate organizational entities. This causes problems when a client attempts to connect to a broker. Tunneling addresses this problem where a broker’s firewall has been configured to allow incoming connections from clients. Two options are provided for a client to connect through its own firewall to a broker with both methods achieving the same result, these are:

HTTP tunneling

This is suitable for applets where, due to sandbox security, an attempt to connect explicitly to an HTTP proxy server would be rejected. HTTP tunneling uses the Web support in Web browsers and connects through the proxy as if it were connecting to a Web site.

Activating HTTP tunneling support is configured on each node. Once a node has been configured to use HTTP tunneling, all client connections to that node must use this method of connection. Clients that don't will be rejected when an attempt to connect is made.

HTTP tunneling is not supported in conjunction with SSL authentication.

Connect via proxy

This is not suitable for applets. It is suitable for use where there are no sandbox security restrictions. It connects directly to the proxy and uses Internet protocols to request that the proxy forwards the connection to the broker. This option does not work in applets where the security manager rejects an explicit connection to the proxy.

Quality of protection

In Internet deployments, cryptographically-based protection of messages enhances security by preventing tampering and eavesdropping by hackers. The authentication services provided by WebSphere Event Broker ensure that only legitimate event broker servers and clients can connect to each other. However, a hacker might still be able to observe messages in transit or tamper with messages on established connections. Message protection provides security against these kinds of attacks.

Message protection consumes processor time and can slow system throughput. However, not all messages are equally sensitive, so message protection is configurable on a per-topic basis, so that you get only the protection you really need. Some topics might get no message protection at all, others might get channel integrity (making it impossible for hackers to insert or delete messages undetected), or message integrity (making it impossible for hackers to alter messages undetected), or message privacy (making it impossible for hackers to observe message contents). The protection levels are cumulative. For example, if you request message privacy you get message integrity and channel integrity as well. If you request message integrity you also get channel integrity. The higher levels of protection consume more resources than the lower levels.

You can also set message protection on internal system topics. Unlike user topics this must be either enabled on all topics, or on none.

Domain awareness

Enabling domain awareness means that access to the Message Brokers Toolkit is not restricted to users from one Windows domain.

The Configuration Manager is always domain aware; when the Configuration Manager receives user information, if the Configuration Manager is on Windows, it verifies the user's domain membership.

You can, however, configure whether the Message Brokers Toolkit sends domain aware information about the user to the Configuration Manager. If the user is logged on to a Windows domain and the Message Brokers Toolkit is configured to send domain aware information, the Message Brokers Toolkit sends the user's domain membership information as well as the user's ID. If the user is not logged on to a Windows domain, the Message Brokers Toolkit sends only the user's ID and their computer name.

With domain awareness enabled, users from different Windows domains who are either trusted by the primary domain, or in a Windows 2000 transitive trust relationship, can perform Message Brokers Toolkit tasks, provided that they are in the correct user role definition groups or object level security groups.

When using domain awareness:

- Domain information is retrieved by the Configuration Manager.
- Membership of user role definition/object level security groups is not restricted to users from one domain.
- Nesting in user role definition/object level security groups is supported.

Planning for security when you install WebSphere Event Broker

On Linux and UNIX systems, you must complete security tasks before you install WebSphere Event Broker; these tasks are described in Installation Guide. On Windows systems, security tasks are completed during and after installation.

Always refer to the the Installation Guide for the latest information about installation tasks.

After installation, refer to “Creating user IDs” on page 12 for further security considerations.

For an introduction to various aspects of security, see “Security overview” on page 3.

Setting up broker domain security

This section introduces the things to consider when you are setting up security for a broker configuration running on Windows, Linux, or UNIX platforms.

For an introduction to various aspects of security, see “Security overview” on page 3.

This section does not apply to z/OS. Refer to “Setting up z/OS security” on page 28 and “Summary of required access (z/OS)” on page 372 for information about setting up broker domain security on z/OS.

Before you start setting up security for your broker domain, refer to “Planning for security when you install WebSphere Event Broker,” which contains links to security information that you need before, during, and after installation of WebSphere Event Broker.

You can use the following list of tasks as a security checklist. Each item comprises a list of reminders or questions about the security tasks to consider for your broker configuration. The answers to the questions provide the security information that you need to configure your WebSphere Event Broker components and also give you information about other security controls that you might want to deploy.

- “Creating user IDs” on page 12
- “Considering security for a broker” on page 15
- “Considering security for a Configuration Manager” on page 16
- “Considering security for the workbench” on page 13
- “Enabling topic-based security” on page 23
- “Using security exits” on page 26
- “Database security” on page 27

Creating user IDs

When you are planning the administration of your broker configuration, consider defining user IDs for the following roles:

- Administrator user IDs that can issue mqsi* commands. Refer to:
 - “Deciding which user accounts can execute broker commands” on page 15
 - “Deciding which user accounts can execute User Name Server commands” on page 24
 - “Deciding which user accounts can execute Configuration Manager commands” on page 17
- Service user IDs under which components run. Refer to:
 - “Deciding which user account to use for the broker service ID” on page 15
 - “Deciding which user account to use for the User Name Server service ID” on page 25
 - “Deciding which user account to use for the Configuration Manager service ID” on page 17

On all platforms, you must add broker service user IDs to the **mqbrkrs** local group.

On Windows, there are additional requirements for a runtime component’s service user ID. Because the broker runs as a service, the service user ID must be allowed to log on as a service. If this is not granted, you are able to create the component, but the mqsisstart command fails.

No users are automatically allowed to log on as a service (including those in the Administrators group). The permission needs to be granted separately, and is a requirement for all runtime components’ ServiceUserIds (ConfigMgr, Broker and UserNameServer).

To grant permission, select Control Panel→Administrative Tools→Local Security Policy. Then open Local Policies→User Rights Assignment and change the setting **Log on as a service**. Add the service user IDs to the list. This needs to be done only once for each service ID, but it must be done locally on each machine that runs brokers. So, if you are using a domain ID as the service user ID, the security policy change must be made on each machine in the domain that runs brokers (not only on the domain controller).

- User IDs that access broker databases:
 1. Select the user IDs with which you intend to access the database used by your broker. Ensure that the user ID is not more than eight characters long. When you use a DB2 database, use a local user ID to access the database. If you create brokers in a domain environment where you use a domain user ID for the service user ID, set the database ID to a local ID that is authorized to access databases.
 2. Authorize your selected user IDs to access the broker and Configuration Manager databases. Refer to “Authorizing access to the databases” on page 106 for more information.
 3. When you create your broker, identify the selected user ID using the -u and -p options on the **mqsicreatebroker** command.
- Workbench users.
- Publishers and subscribers. Refer to “Enabling topic-based security” on page 23.

If you are running a Configuration Manager with one user ID and a broker with a different user ID on another system, you might see an error message when you deploy message flows to the broker. To avoid this, complete the following steps:

- Ensure that the broker's user ID is a member of the **mqm** and **mqbrkrs** groups.
- Define the broker's user ID on the system on which the Configuration Manager is running.
- Define the Configuration Manager's user ID on the system on which the broker is running.
- Ensure that all IDs are in lowercase so that they are compatible between computers.

Considering security for the workbench

During this task you consider the factors for deciding which users can take actions within the workbench.

Consider the following:

1. "Are you running with domain awareness enabled?"
2. "Are you running with domain awareness disabled?" on page 14
3. "Securing the channel between the workbench and the Configuration Manager" on page 14

Ensure that the IDs of the users who will run the workbench are not more than eight characters long.

Are you running with domain awareness enabled?

It is recommended that you run with domain awareness enabled. With this option, the domain information for a workbench user is flowed with the userid to the Configuration Manager for increased security. Assume that you are running the Configuration Manager on a computer named WKSTN1, which is a member of a domain named DOMAIN1. Users from DOMAIN2 also want to use the workbench. Perform the following steps:

1. Add any domain users or groups to the local group names that you will be using in your ACLs.
2. When you create the Configuration Manager use the **-m** option on the **mqsicreateaclentry** command to ensure that the domain is considered when verifying the user.

When you start the workbench, it automatically sends the domain information for your user ID to the Configuration Manager. Enable domain awareness in the Configuration Manager to access domain information.

Note: If you are running a Configuration Manager with one user ID and a broker with a different user ID on another computer, you might see an error message when trying to deploy message flows to the broker. To avoid this, do the following:

- Ensure that the broker's user ID is a member of the **mqm** and **mqbrkrs** groups.
- Define the broker's user ID on the computer where the Configuration Manager is running.
- Define the Configuration Manager's user ID on the computer where the broker is running.
- Ensure that all IDs are in lowercase so that they are compatible between computers.

Go to “Securing the channel between the workbench and the Configuration Manager.”

Are you running with domain awareness disabled?

You can set domain awareness to disabled, but running with this option means that the domain information for the workbench user is not flowed with the userid information, thus reducing security. It is therefore recommended that you run with domain awareness enabled.

You can use the `-a` option on the `mqscreateaclentry` command to allow a user to be verified without considering the domain.

To set domain awareness to disabled, answer the following questions:

1. Are your workbench users drawn from a local domain?
 - a. No: Go to the next question.
 - b. Yes: Add any users to the local groups that you will be using in your ACLs. Go to “Securing the channel between the workbench and the Configuration Manager.”
2. Are your workbench users drawn from another domain?
 - a. Yes: Make the other domain a trusted domain of the Configuration Manager’s computer then add the groups and users from the trusted domain to the local groups of the Configuration Manager.

For additional security, run with both domain awareness and security exits enabled. For more information about security exits, refer to “Security exits” on page 8.

Turning off the toolkit domain awareness

The toolkit sends the user and domain name to the Configuration Manager queue manager, regardless of the domain awareness setting on the Configuration Manager. This can cause problems connecting to the queue manager because of the security required to connect, put or get messages.

To turn off the domain awareness on the toolkit, run the toolkit in the following way:

1. Change to the `install_dir\eclipse` directory.
2. Run the toolkit using the command `mqsistudio -vmargs -DDomainAware=0`.

Alternatively, modify the shortcut that runs the toolkit and add on `-vmargs -DDomainAware=0`.

Go to “Securing the channel between the workbench and the Configuration Manager”

Securing the channel between the workbench and the Configuration Manager

Create and enable a pair of security exits to run at the workbench and Configuration Manager ends of the connection. Use these exits to verify workbench users with the Windows security manager on the Configuration Manager computer.

For more information about creating and enabling security exits, refer to “Security exits” on page 8.

Considering security for a broker

Consider the factors for deciding which users can:

- Execute broker commands
- Control security for other broker resources.

Consider the following steps:

1. "Deciding which user accounts can execute broker commands"
2. "Deciding which user account to use for the broker service ID"
3. "Setting security on the broker's queues" on page 16
4. "Enabling topic-based security in the broker" on page 16

Deciding which user accounts can execute broker commands

Decide what permissions are required for the user IDs that:

- Create, change, list, delete, start, and stop brokers
- Display, retrieve, and change trace information.

Answer the following questions:

1. Is your broker installed on a Linux or UNIX operating system?
 - a. No: Go to the next question.
 - b. Yes: Go to "Deciding which user account to use for the broker service ID"
2. Are you executing broker commands under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Assume that your local account is on a computer named, for example, WKSTN1. When you create a broker, ensure that your user ID is defined in your local domain. When you create or start a broker, ensure that your user ID is a member of WKSTN1\Administrators.
Go to "Deciding which user account to use for the broker service ID."
3. Are you executing broker commands under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you create a broker using, for example, DOMAIN1\user1, ensure that DOMAIN1\user1 is a member of WKSTN1\Administrators.
Go to "Deciding which user account to use for the broker service ID."

Deciding which user account to use for the broker service ID

When you set the service ID with the `-i` option on the `mqsicreatebroker` or `mqsichangebroker` command, you determine the user ID under which the broker component process runs.

Answer the following questions:

1. Is your broker installed on a Linux or UNIX operating system?
 - a. No: Go to the next question.
 - b. Yes: Go to "Setting security on the broker's queues" on page 16
2. Do you want your broker to run under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Ensure that your user ID is defined in your local domain and is a member of `mqbrkrs`.

Go to “Setting security on the broker’s queues”

3. Do you want your broker to run under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you run a broker using, for example, DOMAIN1\user1, ensure that: DOMAIN1\user1 is a member of DOMAIN1\Domain mqbrkrs and DOMAIN1\Domain mqbrkrs is a member of WKSTN1\mqbrkrs.

Go to “Setting security on the broker’s queues”

Setting security on the broker’s queues

When you run the mqsicreatebroker command, the mqbrkrs group gets access authority to the following queues:

```
SYSTEM.BROKER.ADMIN.QUEUE  
SYSTEM.BROKER.CONTROL.QUEUE  
SYSTEM.BROKER.EXECUTIONGROUP.QUEUE  
SYSTEM.BROKER.EXECUTIONGROUP.REPLY  
SYSTEM.BROKER.INTERBROKER.QUEUE  
SYSTEM.BROKER.MODEL.QUEUE
```

- If you have created WebSphere Event Broker components to run on different queue managers, set the permissions for the transmission queues that you define to handle the message traffic between the queue managers. Grant put and setall authority to the local mqbrkrs group, or to the service user ID of the component supported by the queue manager on which you defined the transmission queue.
- Ensure that the broker’s service user ID has authority to:
 1. Get messages from each input queue included in a message flow
 2. Put messages to any output, reply, and failure queues included in a message flow.
- Ensure that the user IDs under which applications that interact with the broker run have authority to:
 1. Put messages to each input queue included in a message flow
 2. Get messages from any output, reply, and failure queue included in a message flow.
- Go to “Enabling topic-based security in the broker”

Enabling topic-based security in the broker

Perform this task by responding to the following question:

Do you want to enable topic-based security in the broker?

1. Yes: Go to “Enabling topic-based security” on page 23
2. No: Go to “Considering security for a Configuration Manager”

Considering security for a Configuration Manager

During this task you consider the group membership that is required for:

- Users that execute Configuration Manager commands
- Service IDs
- Access to the Configuration Manager’s queues.

An ACL is associated with the Configuration Manager itself. Users or groups that have full-control membership of the Configuration Manager's ACL implicitly have full-control membership of all other ACLs. Full-control membership of the Configuration Manager's ACL also allows users or groups to modify the ACLs for any object, including the Configuration Manager.

Read the appropriate sections in this list:

1. "Deciding which user accounts can execute Configuration Manager commands"
2. "Deciding which user account to use for the Configuration Manager service ID"
3. "Setting security on the Configuration Manager's queues" on page 18
4. "Running the Configuration Manager in a domain environment" on page 18

Deciding which user accounts can execute Configuration Manager commands

During this task you decide what permissions are required for the user IDs that:

- Create, change, list, delete, start, and stop a Configuration Manager
- Display, retrieve, and change trace information.

Answer the following questions:

1. Are you executing Configuration Manager commands under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Assume that your local account is on a computer named, for example, WKSTN1. When you create a Configuration Manager, ensure that your user ID is defined in your local domain. When you create or start a Configuration Manager, ensure that your user ID is a member of WKSTN1\Administrators.
Go to "Deciding which user account to use for the Configuration Manager service ID"
2. Are you executing Configuration Manager commands under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you create a Configuration Manager using, for example, DOMAIN1\user1, ensure that DOMAIN1\user1 is a member of WKSTN1\Administrators.
Go to "Deciding which user account to use for the Configuration Manager service ID"

Deciding which user account to use for the Configuration Manager service ID

When you set the service ID with the -i option on the mqsicreateconfigmgr or mqsichangeconfigmgr command, you determine the user ID under which the Configuration Manager component process runs.

Answer the following questions:

1. Do you want your Configuration Manager to run under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Ensure that your user ID has the following characteristics:

|

- It is defined in your local domain.
- It is a member of **mqbrkrs**.
- It is a member of **mqm**.
- It is a member of Administrators.

Go to “Setting security on the Configuration Manager’s queues.”

2. Do you want your Configuration Manager to run under a Windows domain account?

a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you run a Configuration Manager using, for example, DOMAIN1\user1, ensure that:

- 1) DOMAIN1\user1 is a member of DOMAIN1\Domain **mqbrkrs**.
- 2) DOMAIN1\user1 is a member of WKSTN1\mqm.
- 3) DOMAIN1\Domain **mqbrkrs** is a member of WKSTN1\mqbrkrs.
- 4) DOMAIN1\user1 is a member of WKSTN1\Administrators.

Alternatively, complete the following steps:

- 1) Define user1 in DOMAIN1.
- 2) Add user1 to the DOMAIN1\Domain **mqm** group.
- 3) Add user1 to the DOMAIN1\Domain **mqbrkrs** group.
- 4) Add the DOMAIN1\Domain **mqm** group to the WKSTN1\mqm group.
- 5) Add the DOMAIN1\Domain **mqbrkrs** group to the WKSTN1\mqbrkrs group.
- 6) Add user1 to the WKSTN1\Administrators group.

Go to “Setting security on the Configuration Manager’s queues.”

Setting security on the Configuration Manager’s queues

When you run the command, the **mqbrkrs** group gets access authority to the following queues:

```
SYSTEM.BROKER.CONFIG.QUEUE
SYSTEM.BROKER.CONFIG.REPLY
SYSTEM.BROKER.ADMIN.REPLY
SYSTEM.BROKER.SECURITY.QUEUE
SYSTEM.BROKER.MODEL.QUEUE.
```

The broker and the User Name Server require access to the Configuration Manager’s queues.

Each group or user for which you create access control lists (ACLs), gets access authority to the following queues:

```
SYSTEM.BROKER.CONFIG.QUEUE
SYSTEM.BROKER.CONFIG.REPLY.
```

Go to “Running the Configuration Manager in a domain environment.”

Running the Configuration Manager in a domain environment

- If you want to enable domain awareness, go to “Are you running with domain awareness disabled?” on page 14.
- If you want to disable domain awareness, go to “Are you running with domain awareness enabled?” on page 13.

Changing the security domain for the User Name Server

You can change the security domain only if you are not using domain awareness. To change the security domain currently in use for your User Name Server, use the “mqsicchangeusernameserver command” on page 279.

Implementing SSL authentication

The following topics contain instructions for implementing SSL authentication:

- “Enabling SSL on the WebSphere MQ Java Client”
- “Enabling SSL for the Real Time node” on page 20
- Configuring HTTPInput and HTTPReply nodes to use SSL (HTTPS)
- Configuring an HTTPRequest node to use SSL (HTTPS)

Enabling SSL on the WebSphere MQ Java Client

The WebSphere MQ Java Client supports SSL-encrypted connections over the SVRCONN channel between the application and the queue manager. This topic tells you how to make use of this SSL support when communicating between the Configuration Manager Proxy (CMP) and the Configuration Manager.

For one-way authentication (with the client (Configuration Manager Proxy) authenticating the server (Configuration Manager) only) perform the following steps:

1. Generate or obtain all the appropriate keys and certificates. This includes a signed pkcs12 certificate for the server and the appropriate public key for the certificate authority that signed the pkcs12 certificate.
2. Add the pkcs12 certificate to the queue manager certificate store and assign it to the queue manager. Use the standard WebSphere MQ facilities, for example, WebSphere MQ Explorer (for WebSphere MQ Version 6) or WebSphere MQ Services (for WebSphere MQ Version 5).
3. Add the certificate of the certificate authority to the JSEE truststore of the Java Virtual Machine (JVM) at the Configuration Manager Proxy end using a tool such as Keytool.
4. Decide which cipher suite to use.
5. Change the properties on the SYSTEM.BKR.CONFIG channel to specify the cipher suite to be used. Use the standard WebSphere MQ facilities (for example, WebSphere MQ Explorer).
6. Add the required parameters (cipher suite, for example) to the Configuration Manager Proxy. If a truststore other than the default is used, its full path must be passed in via the truststore parameter.

When you have performed these steps, the Configuration Manager Proxy will connect to the Configuration Manager if it has a valid signed key that has been signed by a trusted certificate authority.

For two-way authentication (with the Configuration Manager also authenticating the Configuration Manager Proxy) perform the following additional steps:

1. Generate or obtain all the appropriate keys and certificates. This includes a signed pkcs12 certificate for the client and the appropriate public key for the certificate authority that signed the pkcs12 certificate.

2. Add the certificate of the certificate authority to the queue manager certificate store; use the standard WebSphere MQ facilities (for example, WebSphere MQ Explorer for WebSphere MQ Version 6).
3. Set the SYSTEM.BKR.CONFIG channel to always authenticate. You can use SSLCAUTH(REQUIRED) in runmqsc, or WebSphere MQ Explorer.
4. Add the pkcs12 certificate to the JSEE keystore of the JVM at the Configuration Manager Proxy end using a tool such as Keytool.
5. If not using the default keystore, its full path must be passed into the Configuration Manager Proxy via the keystore parameter

When you have performed these steps, the Configuration Manager allows the Configuration Manager Proxy to connect only if the Configuration Manager Proxy has a certificate signed by one of the certificate authorities in its keystore.

Further restrictions can be made using the `sslPeerName` field; for example, you can allow connections only from certificate holders with a specific company or department name in their certificates. In addition, you can invoke a security exit for communications between the Configuration Manager Proxy and the Configuration Manager; see “Using security exits” on page 26.

Enabling SSL for the Real Time node

WebSphere Event Broker authentication services provide an optional facility that is supported between JMS clients and Real-timeInput nodes of WebSphere Event Broker.

In a default configuration, authentication services are disabled.

To configure the product to use the authentication services, complete the following steps.

- Configure and start a User Name Server in a broker domain
- Configure each Real-timeInput node to use authentication and set your chosen authentication protocol in each of the brokers that are to use the authentication services
- Edit a file that specifies client user Ids and passwords
- Specify the names of the files that are required to implement the SSL protocol

Configuring the User Name Server:

The User Name Server distributes to the brokers the information (specifically, passwords) that is required to support these authentication protocols.

To configure the User Name Server to support authentication, two parameters are provided for the `mqscreateusernameserver` and `mqschangeusernameserver` commands.

The first parameter, *AuthProtocolDataSource*, describes the location of an operating system file that contains the information that is required to support the authentication protocols.

The second parameter, the `-jflag`, indicates whether the file pointed to by the *AuthProtocolDataSource* parameter contains group and group membership information as well as password information.

- Set the -j flag if you want to support both authentication and publish/subscribe access control in your broker domain, and you want to draw user and group information from a flat file rather than from the operating system.
- Use the *AuthProtocolDataSource* parameter to specify the source of any protocol-related information. For example, you can specify the name of a file that contains user ID and password information. The user ID and password information in this file must exactly mirror the operating system user ID and password definitions. Make sure that you set the appropriate file system security for this password file.
- The default location of this file is the WebSphere Event Broker home directory. If you store the file somewhere else, give the full path definition of the location of the file.
- For the change to the User Name Server to take effect you must stop and then restart the User Name Server.

The **mqschangeusernameserver** command also supports a-d flag to disable the option.

Configuring a broker:

Configure a broker to support WebSphere Event Broker authentication services. You need to specify two authentication and access control parameters and use the workbench to configure the appropriate Real-timeInput nodes and the sets of protocols that are to be supported on the broker.

The following steps show you how to do this.

- Switch to the Broker Administration perspective.
- For each message flow in the Message Flow Topology:
 1. Right-click the Real-timeInput node.
 2. Click properties.
 3. Check the Authentication box.
- For each broker in the Broker Topology:
 1. Right-click the broker.
 2. Click properties.
 3. Fill in the Authentication Protocol Type field

Choose any combination of the options P, M, S, and R; for example, S, SR, RS, R, PS, SP, PSR, SRM, MRS, and RSMP are all valid combinations of options.

The order in which you specify the options is significant; the broker chooses the first option that the client supports. If you want the broker to always support the strongest protocol that the client supports, choose RSMP.

4. If you have chosen S or R as one of the options in the Authentication Protocol Type field, specify the SSL Key Ring File Name and the SSL Password File Name.
5. Click OK.
6. Use the **mqscreatebroker** or **mqschangebroker** command, with the following two parameters, to configure the broker:

UserNameServerQueueManagerName (-s)

This parameter specifies the name of the queue manager associated

with the User Name Server. This parameter must be specified if you require authentication services, publish/subscribe access control services, or both types of service.

Publish/Subscribe Access Control Flag (-j)

This flag must be set, in addition to specifying the `UserNameServerQueueManagerName` parameter, if you want to use publish/subscribe access control services.

There is no corresponding flag for using the authentication services in the broker; it is enabled at the IP input node level.

Sample password files:

Two sample files, named `password.dat` and `pwgroup.dat`, are shipped with WebSphere Event Broker.

`pwgroup.dat` is a sample file that can be used when you set the `-j` flag.

`password.dat` is a sample file that can be used in the default case.

`password.dat` has the following layout:

```
# This is a password file.

# Each line contains two required tokens delimited by
# commas. The first is a user ID, the second is that user's
# password.

#USERNAME PASSWORD
=====
subscriber,subpw
admin,adminpw
publisher,pubpw
```

This file complements the user and group information drawn by the User Name Server from the operating system. User names that are defined in the file, but not the operating system, are treated as unknown by the broker domain. User names that are defined in the operating system, but are not defined in the password file, are denied access to the system.

`pwgroup.dat` contains group information as well as user and password information. Each user entry includes a list of group names that specify the groups that contain the user.

`pwgroup.dat` has the following layout:

```
#This is a password file.
#Each line contains two or more required tokens delimited by
#commas.The first is a user ID and the second is that user's
#password. All subsequent tokens
#specify the set of groups that the user belongs to.

#USERNAME PASSWORD GROUPS
subscriber,subpw,group1,group2,group3
admin,adminpw,group2
publisher,pubpw,group2,group4
```

As mentioned above, this file can be used to provide the only source of user, group, and password information for the broker domain.

To deploy updated user and password information to the broker network if this information is drawn from an operating system file, stop the User Name Server and brokers, update the file, and then restart the User Name Server and brokers.

If passwords are drawn from the operating system, updates are automatically distributed to the brokers. Use normal operating system management tools to change users or passwords.

Authentication in the JMS client:

For client applications that use WebSphere MQ classes for Java Message Service Version 5.3 before CSD4, the client application always has an authentication protocol level of PM. The client application and broker negotiate on the choice of protocol for a session. Where the broker supports both protocols (that is, you have set PM or MP in the workbench definition of a broker), the first protocol specified in the workbench is chosen.

For client applications that use WebSphere MQ classes for Java Message Service Version 5.3, CSD10 (plus APAR IC47044) or CSD11 or later, the client application supports two levels of authentication.

A *TopicConnectionFactory* can be configured to support either a MQJMS_DIRECTAUTH_BASIC authentication mode or a MQJMS_DIRECTAUTH_CERTIFICATE authentication mode. The MQJMS_DIRECTAUTH_BASIC authentication mode is equivalent to a level of PM and the MQJMS_DIRECTAUTH_CERTIFICATE authentication mode is equivalent to a level of SR.

If authentication services have been successfully configured for a Real-timeInput node, a JMS client application needs to specify its credentials when creating a connection. To do this, the JMS client application supplies a user/password combination to the *TopicConnectionFactory.createTopicConnection* method; for example:

```
factory.createTopicConnection("user1", "user1pw");
```

If credentials are not specified, or are specified incorrectly, the application receives a JMS wrapped exception containing the MQJMS error text.

Enabling topic-based security

If your applications use the publish/subscribe services of a broker, you can apply an additional level of security to the topics on which messages are published and subscribed. This topic-based security is managed by the User Name Server.

Complete the following steps:

1. Before you create a User Name Server, refer to “Considering security for a User Name Server” on page 24.
2. Create a User Name Server. Refer to “Creating a User Name Server” on page 136.
3. Select the -j flag and set the -s parameter to the name of the queue manager for the User Name Server on the mqscreatebroker or mqschangebroker command.
4. Set the -s parameter on the mqscreateconfigmgr or mqschangeconfigmgr command to the name of the queue manager for the User Name Server.

5. Create ACLs for the topics that require additional security. For more information, see “Creating ACL entries” on page 43.
6. Ensure that the broker’s service user ID has authority to:
 - a. Get messages from each input queue included in a message flow
 - b. Put messages to any output, reply, and failure queues included in a message flow.
7. Ensure that the user IDs under which publish and subscribe applications run have sufficient authority to put to and get from message flow queues:
 - a. Authorize publish applications to put messages to the input queue of the message flow.
 - b. Authorize applications that register subscriptions to put to the SYSTEM.BROKER.CONTROL.QUEUE queue.
 - c. Authorize subscribe applications to get from the queue to which messages are published.
 - d. Authorize publish and subscribe applications to get from the reply queue.

If you are issuing publish/subscribe requests from a JMS client, additional security options are available. Refer to “SSL authentication” on page 8, “Quality of protection” on page 10, and “Authentication services” on page 37.

Go to “Considering security for a Configuration Manager” on page 16.

Considering security for a User Name Server

Complete this task by answering the following question:

Have you enabled topic-based security in your broker?

1. No: Go to “Considering security for a Configuration Manager” on page 16.
2. Yes: You need a User Name Server. Go to “Deciding which user accounts can execute User Name Server commands.”

Deciding which user accounts can execute User Name Server commands

During this task you decide what permissions are required for the user IDs that:

- Create, change, list, delete, start, and stop a User Name Server
- Display, retrieve, and change trace information.

Answer the following questions:

1. Is your User Name Server installed on a Linux or UNIX operating system?
 - a. No: Go to the next question.
 - b. Yes: The information about executing User Name Server commands on Linux and UNIX is not yet available.
Go to “Deciding which user account to use for the User Name Server service ID” on page 25.
2. Are you executing User Name Server commands under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Assume that your local account is on a computer named, for example, WKSTN1. When you create a User Name Server, ensure that your user ID is defined in your local domain. When you create or start a User Name Server, ensure that your user ID is a member of WKSTN1\Administrators.

Go to “Deciding which user account to use for the User Name Server service ID.”

3. Are you executing User Name Server commands under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you create a User Name Server using, for example, DOMAIN1\user1, ensure that DOMAIN1\user1 is a member of WKSTN1\Administrators.
Go to “Deciding which user account to use for the User Name Server service ID.”

Deciding which user account to use for the User Name Server service ID

When you set the service ID with the -i option on the mqsicreateusername server or mqsichangeusername server command, you determine the user ID under which the User Name Server component process runs.

Answer the following questions:

1. Is your User Name Server installed on a Linux or UNIX operating system?
 - a. No: Go to the next question.
 - b. Yes: The information about running your User Name Server on Linux and UNIX is not yet available.
Go to “Setting security on the User Name Server’s queues”
2. Do you want your User Name Server to run under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Ensure that your user ID is defined in your local domain and is a member of **mqbrkrs**.
Go to “Setting security on the User Name Server’s queues”
3. Do you want your User Name Server to run under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you run a User Name Server using, for example, DOMAIN1\user1, ensure that:DOMAIN1\user1 is a member of DOMAIN1\Domain **mqbrkrs** and DOMAIN1\Domain **mqbrkrs** is a member of WKSTN1**mqbrkrs**.
Go to “Setting security on the User Name Server’s queues.”

Setting security on the User Name Server’s queues

When you run the **mqsicreateusername server** command, the **mqbrkrs** group gets access authority to the following queues:

SYSTEM.BROKER.SECURITY.QUEUE
SYSTEM.BROKER.MODEL.QUEUE

Only the broker and the Configuration Manager require access to the User Name Server’s queues.

Go to “Running the User Name Server in a domain environment” on page 26.

Running the User Name Server in a domain environment

When the users that issue publish and subscribe commands are domain users, set the `-d` option on the `mqsicreateusernameserver` command to the domain those users come from. All users that issue publish and subscribe commands must come from the same domain.

Using security exits

To invoke a security exit for communications between the Message Brokers Toolkit and the Configuration Manager, one must be defined when the domain connection is created.

1. Click **File** → **New** → **Domain**. The Domain view appears.
2. Enter the queue manager name, host, and port that you wish to use.
3. Optional: Enter the security exit name. This must be a valid Java class name.
4. Optional: Enter the location of the JAR file for the Security Exit require to connect to the WebSphere MQ queue manager. Use the **Browse** button to find the file location.

Note: The location of the JAR file is required if a Security Exit class is entered.

When the connection is attempted, the security exit is invoked.

Alternatively, you can use SSL when communicating between the Configuration Manager Proxy (CMP) and the Configuration Manager; see “Implementing SSL authentication” on page 19.

Implementing HTTP tunneling

HTTP tunneling support in the broker is activated by selecting the Use HTTP Tunneling option within the properties for the Real-timeInput node or Real-timeOptimizedFlow node. Optional settings are also configured using the “`mqsichangeproperties` command” on page 264.

Once set, HTTP tunneling is administered using the “`mqsichangeproperties` command” on page 264 with the `httpProtocolTimeout` and `httpDispatchThreads` options.

Implementing quality of protection

The `enableQoPSecurity` option of the `mqsichangeproperties` command enables quality of protection. By default, quality of protection is enabled if any of the quality of protection settings have been changed from `n` or `none`. The levels of message protection are defined using the `sysQoPLevel` and `isysQoPLevel` options also in the “`mqsichangeproperties` command” on page 264.

From the broker properties window, you can set the values for temporary topics using:

- Temporary Topic Quality of Protection
- Sys Topic Quality of Protection
- ISys Topic Quality of Protection .

The default value is `none`, or you can select one of the following values from each of the drop-down lists:

- Channel Integrity (preventing hackers from inserting or deleting messages without being detected)
- Message Integrity (preventing hackers from changing the content of a message without being detected)
- Encrypted for Privacy (preventing hackers from looking at the content of a message).

The value selected is the same for all users and is independent of the user currently selected.

Database security

The service user ID for the brokers must be authorized to access databases:

- Each broker service user ID must be authorized for create and update tasks on the database that contains the broker internal tables.

In addition to the broker service user ID, this also applies to any data source user ID if defined (using “mqsicreatebroker command” on page 286).

Derby databases, created either by the Default Configuration wizard or by the “mqsicreatedb command” on page 300 on Windows, do not require security authorization. Refer to “Using Derby databases on Windows” on page 89 for more information.

Database security is defined and modified using various commands dependent upon the database that is being used. See the following:

- “mqsicreatebroker command” on page 286
- “mqsicchangebroker command” on page 250

For information relating to specific databases see:

- “Oracle: granting and revoking user access to databases”
- “SQL Server: granting and revoking user access to databases”
- “Sybase: granting and revoking user access to databases”

Oracle: granting and revoking user access to databases

The Oracle database administrator controls user access to Oracle databases. The WebSphere Event Broker does not provide any special commands to administer an Oracle database.

SQL Server: granting and revoking user access to databases

The SQL database administrator controls user access to Microsoft SQL Server databases. WebSphere Event Broker does not provide any special commands to administer a Microsoft SQL Server database.

Sybase: granting and revoking user access to databases

The Sybase database administrator controls user access to Sybase databases. WebSphere Event Broker does not provide any special commands to administer a Sybase database.

Setting up z/OS security

You need to complete some security configuration tasks before WebSphere Event Broker can work correctly. The steps you need to follow are described in this topic and also in the following topics:

- “Setting up DB2” on page 29
- “Setting up WebSphere MQ” on page 30
- “Setting up workbench access on z/OS” on page 31
- “Creating Publish/Subscribe user IDs” on page 31
- “Enabling the Configuration Manager on z/OS to obtain user ID information” on page 31

Decide on the started task names of the broker, Configuration Manager, and User Name Server. These names are used to set up started task authorizations, and to manage your system performance.

Decide on a data set naming convention for your WebSphere Event Broker PDSEs. A typical name might be WMQI.MQP1BRK.CNTL or MQS.MQP1UNS.BIPCNTL, where MQP1 is the queue manager name. You need to give the WebSphere Event Broker, WebSphere MQ, DB2, and z/OS administrators access to these data sets. You can give these professionals control access in several ways, for example:

- Give each user individual access to the specific data set.
- Define a generic data set profile, defining a group that contains the user IDs of the administrators. Grant the group control access to the generic data set profile.

If you intend to use Publish/Subscribe, define a group called MQBRKRS and connect the started task user IDs to this group. Define an OMVS group segment for this group so that the User Name Server can extract information from the External Security Manager (ESM) database to enable you to use Publish/Subscribe security.

Each broker needs a unique ID for its DB2 tables. This can be:

- A unique started task user ID; you could use the broker name as the started task user ID.
A unique group for the broker (for example MQP1GRP) which has defined all necessary DB2 authorities. The broker started task user ID and the WebSphere Event Broker administrator are both members of this group.
- A shared started task user ID and a unique group specified to identify the DB2 tables to be used with the ODBC interface. Use the broker name as the group name.

Define an OMVS segment for the started task user ID and give its home directory sufficient space for any WebSphere Event Broker dumps. Consider using the started task procedure name as the started task user ID. Check that your OMVS segment is defined by using the following TSO command:

```
LU userid OMVS
```

The command output includes the OMVS segment, for example:

```
USER=MQP1BRK NAME=SMITH, JANE OWNER=TSOUSER  
CREATED=99.342 DEFAULT-GROUP=TSOUSER PASSDATE=01.198  
PASS-INTERVAL=30  
.....  
OMVS INFORMATION  
-----  
UID=0000070594
```

```
HOME=/u/MQP1BRK
PROGRAM=/bin/sh
CPUTIMEMAX=NONE
ASSIZEMAX=NONE
FILEPROCMAx=NONE
PROCUSERMAX=NONE
THREADSMAX=NONE
MMAPAREAMAX=NONE
```

The command:

```
df -P /u/MQP1BRK
```

displays the amount of space used and available, where /u/MQP1BRK is the value from HOME above. This command shows you how much space is currently available in the file system. Check with your data administrators that this is sufficient. You need a minimum of 400 000 blocks free; this is needed if a dump is taken.

Associate the started task procedure with the user ID to be used. For example, you can use the STARTED class in RACF®. The WebSphere Event Broker and z/OS administrators must agree on the name of the started task.

WebSphere Event Broker administrators need an OMVS segment and a home directory. Check the setup described above.

The started task user IDs and the WebSphere Event Broker administrators need access to the install processing files, the component specific files, and the home directory of the started task. During customization the file ownership can be changed to alter group access. This might require super user authority.

When the service user ID is root, all libraries loaded by the broker, including all user-written plug-in libraries and all shared libraries that they might access, also have root access to all system resources (for example, file sets). Review and assess the risk involved in granting this level of authorization.

For more information on various aspects of security, see “Security overview” on page 3.

Setting up DB2

This is part of the larger task of setting up security on z/OS.

The user ID of the person running the DB2 configuration jobs needs UPDATE access to the component PDSE, READ/EXECUTE access to the installation directory, and READ/WRITE/EXECUTE access to the broker-specific directory.

A user needs SYSADM or SYSCTRL authority to run the DB2 configuration jobs.

You cannot share DB2 tables between brokers; each broker needs its own DB2 tables. The format of the table names is:

```
table_owner.table_name
```

where table_owner is known as the table owner.

When the broker starts up, the started task user ID is used to connect to DB2 using ODBC. The ODBC statement Set current SQLID is used to set the ID to table_owner; the table owner ID specifies which tables to use. You have two options in setting up the IDs:

1. Make the table owner the same as the started task user ID. This means that each broker must have a different user ID. You need to check that the started task user ID specified has access to SYSIBM tables. From a TSO user with no system administration authority, use SPUFI to issue the following commands:

```
select *      from SYSIBM.SYSTABLES;
select *      from SYSIBM.SYSSYNONYMS;
select *      from SYSIBM.SYSDATABASE;
```

and resolve any problems.

2. Make the table owner different from the started task user ID. For this to work the started task needs to be able to issue the Set current SQLID request. The easiest way to do this is to create a RACF group with the same name as the table owner, and connect the started task user ID to this group.

Check that the group ID specified has access to SYSIBM tables. From a TSO user with no system administration authority, use SPUFI to issue the following commands:

```
SET    CURRENT SQLID='WMQI';
select * from  SYSIBM.SYSTABLES;
select * from  SYSIBM.SYSSYNONYMS;
select * from  SYSIBM.SYSDATABASE;
```

and resolve any problems (WMQI is the name of the group). You might need to connect the TSO user IDs of the DB2 administrators to the group.

If you have a unique group for each broker (and not a unique started task user ID), the started task user ID must be connected to the group for the ODBC request set currentsqlid to work successfully.

The DB2 administrator user ID must have access to one of the programs DSNTDP2 or DSNTIAD, or equivalent.

The started task user ID must be authorized to connect to DB2. The started task user ID needs a minimum of READ access to the subsystem.RRSAP profile in the DSNR class, if present. In this case, subsystem is the DB2 subsystem name. For example, the following RACF command lists all the resources in DSNR class:

```
RLIST DSNR *
```

The started task user ID needs EXECUTE authority to the DSNACLI plan or equivalent.

The DB2 subsystem started task user ID needs authority to create data sets with the high level qualifier specified in the DB2_STOR_GROUP_VCAT value.

Setting up WebSphere MQ

This is part of the larger task of setting up security on z/OS.

The user ID of the person running the create component (BIPCBRK, BIPCRM, and BIPCRUN) jobs needs UPDATE access to the component PDSE, READ/EXECUTE access to the installation directory, and READ/WRITE/EXECUTE access to the component directory. If you do not use queue manager security, you do not need to read the rest of this topic. Topic “Creating the broker component” on page 122 provides detailed statements on how to protect your queues.

The broker, Configuration Manager, and the User Name Server need to be able to connect to the queue manager.

By default, the broker's internal queues, which all have names of the form:
SYSTEM.BROKER.*

should be protected. These names cannot be changed. Restrict access to the broker, Configuration Manager, and User Name Server started task user IDs, and to WebSphere Event Broker administrators.

If you are running a Configuration Manager on z/OS, remote users connecting from either the Message Brokers Toolkit or from a Configuration Manager Proxy application need to be authorized to connect to the queue manager through the channel initiator and require PUT and GET access to
SYSTEM.BROKER.CONFIG.QUEUE and SYSTEM.BROKER.CONFIG.REPLY

If you are using Publish/Subscribe, subscribers need to PUT to
SYSTEM.BROKER.CONTOL.QUEUE.

You can control which applications can use queues used by message flows. Applications need to be able to PUT and GET to queues defined in any nodes.

Setting up workbench access on z/OS

Access to the workbench is controlled from Windows or Linux (x86 platform). The workbench must run on Windows or Linux (x86 platform). See "Considering security for a Configuration Manager" on page 16 for further information.

Creating Publish/Subscribe user IDs

This is part of the larger task of setting up security on z/OS.

A User Name Server can only see user IDs that have been enabled to use UNIX System Services facilities. To ensure that your user or group information can be seen by your User Name Server, you must comply with the following instructions:

- Define user IDs with OMVS(UID(nnnnn)...) and their default group with OMVS(GID(nnnnn)).
- Define groups with OMVS(GID(nnnnn)).

Enabling the Configuration Manager on z/OS to obtain user ID information

This topic lists the steps you need to complete, to enable the Configuration Manager on z/OS to correctly obtain the list of user IDs for a particular group from the External Security Manager (ESM) database.

When connecting to the Configuration Manager, the local user ID on the connecting machine is sent to the Configuration Manager for the purposes of broker domain authorization. This user ID is checked against the Configuration Manager Access Control Lists (ACL) to determine the level of authorization.

For any group ACLs defined, the Configuration Manager queries the local ESM database for a list of user IDs defined to that group. The Configuration Manager then tries to match any user ID connecting to it, with this list, to grant the correct authorization to the broker domain.

For the Configuration Manager on z/OS to obtain this list of user IDs, the group and any user IDs must have an OMVS segment defined.

User IDs

- If you have suitable authorization, you can use the following Security Server (formerly RACF) command to display OMVS information about a user:
LU id OMVS
- If you have suitable authorization, you can use the following Security Server command to give a user ID an OMVS segment:
ALTUSER id OMVS(UID(XXX))

Groups

- If you have suitable authorization, you can use the following Security Server command to display OMVS information about a user:
LG group OMVS
- If you have suitable authorization, you can use the following Security Server command to give a group an OMVS segment:
ALTGROUP id OMVS(GID(XXX))

See the *OS/390 Security Server (RACF) Security Administrator's Guide* (or the appropriate documentation for an external security manager installed on the system) for details.

If the group, or any of the defined user IDs in that group, are not found by the Configuration Manager (either because they do not exist, or because they do not have an OMVS segment), the Configuration Manager is not able to authorize the user attempting the connection.

Publish/subscribe security

The following publish/subscribe security services are provided:

- Topic-based security
Access to messages on particular topics is controlled using access control lists (ACLs).
- Authentication services using real-time nodes
An authentication protocol is used by a broker and a client application to confirm that they are both valid participants in a session.
- Message protection using real-time nodes
Message protection provides security options to prevent messages from being read or modified while in transit.

These services operate independently of each other, but before you can use any of these services you must have a User Name Server.

To use one of these services, use the `mqsicreatebroker` or `mqsichangebroker` command to configure a broker with the `-s` parameter to specify the name of the User Name Server's queue manager.

In addition, to use topic-based security, specify the publish/subscribe access control flag (`-j` parameter) on the `mqsicreatebroker` or `mqsichangebroker` command.

Topic-based security

Use topic-based security to control which applications in your publish/subscribe system can access information on which topics.

For each topic to which you want to restrict access, you can specify which principals (user IDs and groups of user IDs) can publish to the topic, and which principals can subscribe to the topic. You can also specify which principals can request persistent delivery of messages.

Any principal can publish, subscribe, and request persistent delivery of, messages on any topic whose access you do not explicitly restrict.

Topic-based security is managed by a User Name Server that uses the access control lists (ACLs) that you create to decide which authorizations are applied.

Principals and the User Name Server

The User Name Server in WebSphere Event Broker manages the set of principals that are already defined in your network, on behalf of the brokers and the Configuration Manager, for use in publish/subscribe. On Windows, this list of users is taken from the domain specified on the `mqsicreateusername` command.

The User Name Server is made known to both the broker and the Configuration Manager by specifying the User Name Server queue manager on the `mqsicreatebroker` and `mqsicreateconfigmgr` commands.

Message brokers within the broker domain interact with the User Name Server to retrieve the total set of users and groups from which the access control lists are built and against which the publish/subscribe requests are validated. The Configuration Manager interacts with the User Name Server to display the users and user groups in the ACLs that are created using the Topics Hierarchy Editor that is provided in the Broker Administration perspective of the workbench.

Access control lists

Access control lists are used to define, for any topic and principal, the right of that principal to publish on, or subscribe to, that topic, or to request persistent delivery of a publication on that topic.

You can also use the ACL to define the level of message protection that you want to apply to each topic.

Specify these definitions using the Topics Hierarchy Editor in the Broker Administration perspective of the workbench.

Access control can be set explicitly for each individual topic. However, if no explicit ACL is defined for a topic, access control is inherited from an ancestor or parent topic, as defined by the hierarchical structure of the topic tree. If no topic in the hierarchy up to the topic root has an explicit ACL, the topic inherits the ACL of the topic root.

Any defined principal that is known to the User Name Server can be associated with a topic in this way.

Resolving ACL conflicts

If the principals in your broker domain include one or more users in more than one group, the explicit or inherited ACL values might conflict. The following rules indicate how a conflict is resolved:

- If the user has an explicit user ACL on the topic of interest, this always takes priority and the broker verifies the current operation on that basis.

- If the user does not have an explicit user ACL on the topic of interest, but has explicit user ACLs against an ancestor in the topic tree, the closest ancestor ACL for that user takes priority and the broker verifies the current operation on that basis.
- If there are no explicit user ACLs for the user on the topic of interest or its ancestors, the broker attempts to verify the current operation on the basis of group ACLs:
 - If the user is a member of a group that has an explicit group ACL on the topic of interest, the broker verifies the current operation on the basis of that group ACL.
 - If the user is not a member of a group that has an explicit group ACL on the topic of interest, but is a member of a group with explicit group ACLs against an ancestor in the topic tree, the closest ancestor ACL takes priority and the broker verifies the current operation on that basis.
 - If, at a particular level in the topic tree, the user ID is contained in more than one group with an explicit ACL, permission is granted if any of the specifications are positive; otherwise it is denied.

You cannot associate ACLs with topics that include one or more wildcard characters. However, access from your client application is resolved correctly when the subscription registration is made, even when that application specifies a wildcard character in the topic.

PublicGroup authorizations

In addition to the groups that you define, WebSphere Event Broker provides an implicit group, `PublicGroup`, to which all users automatically belong. This implicit group simplifies the specification of ACLs in a topic tree. In particular, this group is used in the specification of the ACL for the topic root. Note that the default setting of the topic root allows publish and subscribe operations for the `PublicGroup`. You can view and change this ACL using the workbench, but you cannot remove it. It determines the default permissions for the entire topic tree. You can specify ACLs for the `PublicGroup` elsewhere in the topic tree, wherever you want to define permissions for all users.

If you have a principal named *Public* defined in your existing security environment, you cannot use this for topic-based security. If you specify this principal within an ACL, it is equated to `PublicGroup` and therefore always allows global access.

mqrbrks authorizations

WebSphere Event Broker grants special publish/subscribe access control privileges to members of the `mqrbrks` group, and to the corresponding Domain `mqrbrks` global group if appropriate.

Brokers need special privileges to perform internal publish and subscribe operations in networks where there is access control. When you create a broker in such a network, you must specify a user ID that belongs to the group `mqrbrks` as the service user ID for the broker. The `mqrbrks` group is given implicit privileges so that its members can publish, subscribe and request the persistent delivery of messages on the topic root (`"/`). All other topics inherit these permissions. If you attempt to configure an ACL for the `mqrbrks` group using the workbench, this ACL is ignored by WebSphere Event Broker.

ACLs and system topics

Messages that are used for internal publish and subscribe operations are published throughout the broker domain using system topics, which begin with the strings "\$SYS" and "\$ISYS".

These topics can only be published from, and subscribed to, members of the mqbrkr group, except for the following two scenarios:

1. If you are migrating topics from WebSphere MQ Publish/Subscribe, you can configure ACLs on topics that begin with the string "\$SYS/STREAM".
2. Clients can subscribe to topics that begin with the string "\$SYS"; this means that applications that provide a management function can subscribe to the broker for administrative events.

Do not configure ACLs on topics that begin with the string "\$ISYS". You are not prevented from doing so, but the ACLs are ignored.

Setting access control on topics

Any user that has an object-level security ACL that gives full control permission to the root topic object, can define and manipulate the ACLs that define which principals can publish on, and subscribe to, which topics. ACLs can also limit delivery of persistent messages, and define the level of message protection.

All defined principals can be associated with any topic; the permissions that can be set are shown in the following table:

Option	Description
Publish	Permits or denies the principal to publish messages on this topic.
Subscribe	Permits or denies the principal to subscribe to messages on this topic.
Persistent	Specifies whether the principal can receive messages persistently. If the principal is not permitted, all messages are sent non-persistently. Each individual subscription indicates whether the subscriber requires persistent messages.
QoS Level	Specifies the level of message protection that is enforced. One of the following four values can be chosen: <ul style="list-style-type: none">• None• Channel Integrity• Message Integrity• Encrypted The default value is 'None'.

Persistent access control behavior is not identical to the publish and subscribe control:

- Clients that are denied Publish access have their publication messages refused.
- Clients that are denied Subscribe access do not receive the publication.
- The persistent access control does not deny the message to subscribers, but denies them persistence, so denied subscribers always receive messages, subject to their subscribe access control, but always have the message sent to them non-persistently, regardless of the persistence of the original message.

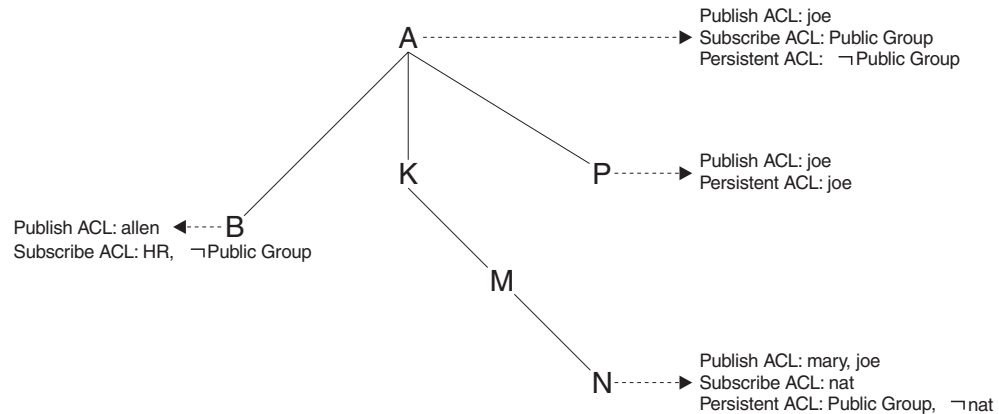
Inheritance of security policies

Typically, topics are arranged in a hierarchical tree. The ACL of a parent topic can be inherited by some or all of its descendent topics that do not have an explicit ACL. Therefore, it is not necessary to have an explicit ACL associated with each

and every topic. Every topic has an ACL policy which is that of its parent. If all parent topics up to the root topic do not have explicit ACLs, that topic inherits the ACL of the root topic.

For example, in the topic tree shown below, the topic root is not shown but is assumed to have an ACL for PublicGroup whose members can publish, subscribe, and receive persistent publications. (The symbol "¬" means "not".)

Inheriting ACLs in a topic tree



The following table shows the ACLs, inherited in some cases, that result from the topic tree shown in the figure:

Topic	Publishers	Subscribers	Persistent
A	only joe	everyone	no-one
A/P	only joe	everyone	only joe
A/K	only joe	everyone	no-one
A/K/M	only joe	everyone	no-one
A/K/M/N	only mary, joe	everyone	everyone except nat
A/B	allen, joe	HR	no-one

Dynamically created topics

Topics that are not explicitly created by the system administrator, but are created dynamically when a client publishes or subscribes to messages, are treated in the same way as those that are created by the system administrator, but they do not have explicitly defined ACLs. That is, the ACLs for dynamically created topics are inherited from the closest ancestor in the topic tree that has an explicit policy. It is therefore not necessary to define leaf topics in the tree if they do not have explicit ACLs.

ACLs and wildcard topics

With WebSphere Event Broker you cannot associate an explicit security policy with a wildcard topic. For example, you cannot associate an ACL with topic "A/+", which represents a two level hierarchy and includes "A/B", "A/K", and "A/P".

However, WebSphere Event Broker does guarantee correct access mediation when a client application subscribes to a wildcard topic.

For example, the topic "A/+" does not, and cannot, have a security policy explicitly associated with it. Therefore, "A/+" inherits its policy from "A". Any user can subscribe to "A/+" because the subscribe ACL includes everyone.

When a message is published on "A/P" or "A/K", the broker delivers it to the user who subscribed to "A/+". However, when a message is published to "A/B", that message is only delivered to subscribers who are in the HR group.

If the system administrator changes the subscribe ACL of any topic that matches "A/+", the broker correctly enforces the ACL when the message is delivered. Subscribing to a wildcard topic has the semantics to deliver messages on all topics that match the wild card, and for which the subscriber has authorization to receive that message.

ACLs and subscription resolution

The broker enforces access control through the topic of the message to be delivered. Messages are delivered only to those clients that have not had subscribe access to that topic denied, either explicitly or through inheritance. Because a subscription can contain a wildcard character, the actual match against the topic namespace, and hence the topic ACLs, cannot be made when the subscription is received. The decision to deliver a message to a subscriber is made only when a specific message with a topic is being processed by the message broker.

Activating topic ACL updates

Updates to a topic ACL do not become active until deployed and activated across the broker domain from the WebSphere Event Broker workbench.

You must have an object-level security ACL that gives full control permission to the root topic object.

Authentication services

Authentication services are supported only between client applications that use the WebSphere MQ Real-time Transport and WebSphere Event Broker Real-timeInput and Real-timeOptimizedFlow nodes.

The WebSphere Event Broker authentication services verify that a broker and a client application are who they claim they are, and can therefore participate in a publish/subscribe session.

Each participant in the session uses an authentication protocol to prove to the other that they are who they say they are, and are not an intruder impersonating a valid participant.

The WebSphere Event Broker product supports the following four protocols:

- P - simple telnet-like password authentication
- M - mutual challenge-response password authentication
- S - asymmetric SSL
- R - symmetric SSL

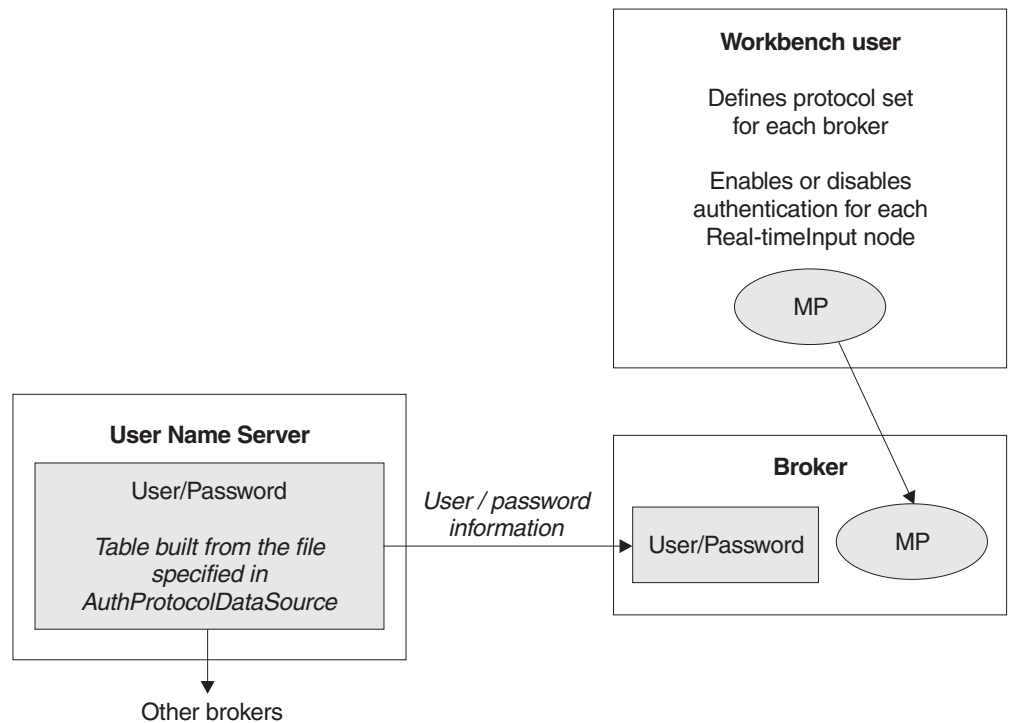
The first two of these protocols and their infrastructure requirements are described in "Simple telnet-like password authentication" on page 39 and "Mutual challenge-response password authentication" on page 40 respectively. Asymmetric and symmetric SSL protocols are described in "SSL authentication" on page 8.

The protocols vary in strength, in terms of providing protection against participants that are not valid participants in the session; P is the weakest and R is the strongest.

Configuring authentication protocols

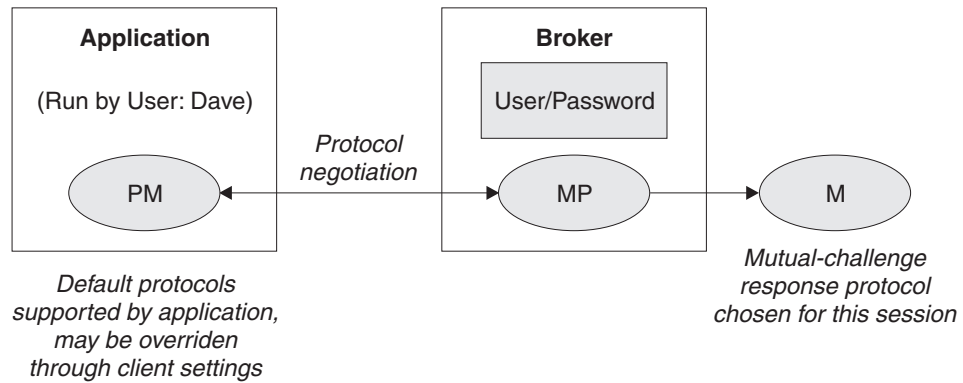
The set of protocols that can be supported by a specific broker in the broker domain can be configured using the workbench. One or more protocols can be specified for each broker. Use the workbench to enable or disable authentication on each Real-timeInput node that is defined for a particular broker. When authentication is enabled at a Real-timeInput node, that node supports the full set of protocols specified for its corresponding broker. The configuration options are illustrated in the following diagrams:

Overview of authentication configuration

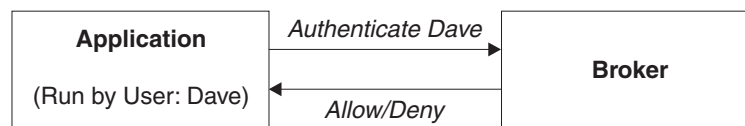


Two-stage runtime authentication process

Stage 1 - Determine protocol for session



Stage 2 - Drive chosen protocol



Simple telnet-like password authentication

This protocol can also be described as *password in the clear* because the password passes un-encrypted over the network. The client application connects to the Real-timeInput node using TCP/IP. The input node requests that the client identify itself. The client sends its "userid" and its password.

This simple protocol relies on both the client and the broker knowing the password associated with a user ID. In particular, the broker needs access to a repository of user and password information. The user ID and password information is distributed by the User Name Server to all the brokers in a WebSphere Event Broker product's domain. The User Name Server extracts user and password information from an operating system file.

The User Name Server approach allows for the centralized maintenance of the source of users and passwords, with automatic distribution of the information to brokers, and automatic refreshes of the information if required. It also provides availability benefits, because user and password information is maintained persistently at each broker.

Each client application must know its own user ID and keep its password secret. When creating a connection, a client specifies its credentials as a name/password combination.

This protocol provides relatively weak security. It does not compute a session key, and should only be used in environments where there are no "eavesdroppers" and no untrusted "middle-men".

In the case where user and password information is stored in a flat file on the User Name Server system, the passwords are stored and distributed "in-the-clear".

The computational load on the client and server is very light.

Mutual challenge-response password authentication

This is a more sophisticated and secure protocol that involves the generation of a secret session key. Both the client and the server compute this key using the client's password. They prove to each other that they know this secret through a challenge and response protocol.

The client must satisfy the server's challenge before the server satisfies the client's challenge. This means that an attacker impersonating a client can gather no information to mount an "offline" password guessing attack. Both the client and the server prove to each other that they know the password, so this protocol is not vulnerable to "impersonation" attacks.

As in the case of the simple telnet-like password protocol, the broker must have access to user and password information. Information about the user ID and password is distributed by the User Name Server to all the brokers in the domain. The User Name Server extracts user and password information from an operating system file.

Each client application must know its own user ID and keep its password secret. When creating a connection, a client specifies its credentials as a name/password combination.

Computational demands on both client and server are fairly modest.

Message protection

The authentication services provided by WebSphere Event Broker ensure that only legitimate message brokers and client applications can connect to each other. However, a hacker might still be able to observe messages in transit or interfere with messages on established connections. Message protection provides security options to protect your messages against such activities.

You cannot use message protection if you are using 'simple telnet-like password authentication'.

Because the use of message protection can have an adverse affect on the performance of your publish/subscribe system, and because security is not equally important for all messages, you might want to define different levels of message protection for different messages. You do this by assigning a Quality of Protection (QoP) value to each topic in your publish/subscribe system.

There are four QoP values. They give the following levels of protection:

- n** This is the default value. It gives no message protection.
- c** This provides channel integrity. With this level of protection, hackers are unable to insert or delete messages without being detected.
- m** This provides message integrity. With this level of protection, hackers are unable to change the content of a message without being detected.
- e** This provides message encryption. With this level of protection, hackers are unable to look at the content of a message.

The protection levels are cumulative. For example, if you specify message encryption, you also get message integrity and channel integrity; if you request message integrity, you also get channel integrity.

If any QoS settings are made, all clients that connect to the broker must use a security level that supports message integrity or message encryption.

Securing the publish/subscribe domain

The following topics describe how to secure your publish/subscribe domain:

- “Enabling topic-based security” on page 23
- “Creating ACL entries” on page 43
- “Enabling SSL for the Real Time node” on page 20
- “Using message protection” on page 47
- “Securing WebSphere MQ resources” on page 47

For more information, see “Publish/subscribe security” on page 32 and “Security overview” on page 3.

Enabling topic-based security

If your applications use the publish/subscribe services of a broker, you can apply an additional level of security to the topics on which messages are published and subscribed. This topic-based security is managed by the User Name Server.

Complete the following steps:

1. Before you create a User Name Server, refer to “Considering security for a User Name Server” on page 24.
2. Create a User Name Server. Refer to “Creating a User Name Server” on page 136.
3. Select the `-j` flag and set the `-s` parameter to the name of the queue manager for the User Name Server on the `mqsicreatebroker` or `mqsichangebroker` command.
4. Set the `-s` parameter on the `mqsicreateconfigmgr` or `mqsichangeconfigmgr` command to the name of the queue manager for the User Name Server.
5. Create ACLs for the topics that require additional security. For more information, see “Creating ACL entries” on page 43.
6. Ensure that the broker’s service user ID has authority to:
 - a. Get messages from each input queue included in a message flow
 - b. Put messages to any output, reply, and failure queues included in a message flow.
7. Ensure that the user IDs under which publish and subscribe applications run have sufficient authority to put to and get from message flow queues:
 - a. Authorize publish applications to put messages to the input queue of the message flow.
 - b. Authorize applications that register subscriptions to put to the `SYSTEM.BROKER.CONTROL.QUEUE` queue.
 - c. Authorize subscribe applications to get from the queue to which messages are published.
 - d. Authorize publish and subscribe applications to get from the reply queue.

If you are issuing publish/subscribe requests from a JMS client, additional security options are available. Refer to “SSL authentication” on page 8, “Quality of protection” on page 10, and “Authentication services” on page 37.

Go to “Considering security for a Configuration Manager” on page 16.

Considering security for a User Name Server

Complete this task by answering the following question:

Have you enabled topic-based security in your broker?

1. No: Go to “Considering security for a Configuration Manager” on page 16.
2. Yes: You need a User Name Server. Go to “Deciding which user accounts can execute User Name Server commands” on page 24.

Deciding which user accounts can execute User Name Server commands

During this task you decide what permissions are required for the user IDs that:

- Create, change, list, delete, start, and stop a User Name Server
- Display, retrieve, and change trace information.

Answer the following questions:

1. Is your User Name Server installed on a Linux or UNIX operating system?
 - a. No: Go to the next question.
 - b. Yes: The information about executing User Name Server commands on Linux and UNIX is not yet available.
Go to “Deciding which user account to use for the User Name Server service ID” on page 25.
2. Are you executing User Name Server commands under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Assume that your local account is on a computer named, for example, WKSTN1. When you create a User Name Server, ensure that your user ID is defined in your local domain. When you create or start a User Name Server, ensure that your user ID is a member of WKSTN1\Administrators.
Go to “Deciding which user account to use for the User Name Server service ID” on page 25.
3. Are you executing User Name Server commands under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you create a User Name Server using, for example, DOMAIN1\user1, ensure that DOMAIN1\user1 is a member of WKSTN1\Administrators.
Go to “Deciding which user account to use for the User Name Server service ID” on page 25.

Deciding which user account to use for the User Name Server service ID

When you set the service ID with the -i option on the mqsicreateusername server or mqsichangeusername server command, you determine the user ID under which the User Name Server component process runs.

Answer the following questions:

1. Is your User Name Server installed on a Linux or UNIX operating system?
 - a. No: Go to the next question.

- b. Yes: The information about running your User Name Server on Linux and UNIX is not yet available.
Go to “Setting security on the User Name Server’s queues” on page 25
2. Do you want your User Name Server to run under a Windows local account?
 - a. No: Go to the next question.
 - b. Yes: Ensure that your user ID is defined in your local domain and is a member of **mqbrkrs**.
Go to “Setting security on the User Name Server’s queues” on page 25
3. Do you want your User Name Server to run under a Windows domain account?
 - a. Yes: Assume that your computer named, for example, WKSTN1, is a member of a domain named DOMAIN1. When you run a User Name Server using, for example, DOMAIN1\user1, ensure that:DOMAIN1\user1 is a member of DOMAIN1\Domain **mqbrkrs** and DOMAIN1\Domain **mqbrkrs** is a member of WKSTN1\mqbrkrs.
Go to “Setting security on the User Name Server’s queues” on page 25.

Setting security on the User Name Server’s queues

When you run the **mqsicreateusername** command, the **mqbrkrs** group gets access authority to the following queues:

```
SYSTEM.BROKER.SECURITY.QUEUE
SYSTEM.BROKER.MODEL.QUEUE
```

Only the broker and the Configuration Manager require access to the User Name Server’s queues.

Go to “Running the User Name Server in a domain environment” on page 26.

Running the User Name Server in a domain environment

When the users that issue publish and subscribe commands are domain users, set the -d option on the **mqsicreateusername** command to the domain those users come from. All users that issue publish and subscribe commands must come from the same domain.

Creating ACL entries

You must create an access control list (ACL) for each new topic. See “Adding a new topic” on page 198 for more information about doing this.

Using authentication for real-time connections

WebSphere Event Broker authentication services provide an optional facility that is supported between JMS clients and Real-timeInput nodes of WebSphere Event Broker.

In a default configuration, authentication services are disabled.

To configure the product to use the authentication services, complete the following steps.

- Configure and start a User Name Server in a broker domain

- Configure each Real-timeInput node to use authentication and set your chosen authentication protocol in each of the brokers that are to use the authentication services
- Edit a file that specifies client user Ids and passwords
- Specify the names of the files that are required to implement the SSL protocol

Configuring the User Name Server

The User Name Server distributes to the brokers the information (specifically, passwords) that is required to support these authentication protocols.

To configure the User Name Server to support authentication, two parameters are provided for the **mqscreateusername** and **mqschangeusername** commands.

The first parameter, *AuthProtocolDataSource*, describes the location of an operating system file that contains the information that is required to support the authentication protocols.

The second parameter, the *-j* flag, indicates whether the file pointed to by the *AuthProtocolDataSource* parameter contains group and group membership information as well as password information.

- Set the *-j* flag if you want to support both authentication and publish/subscribe access control in your broker domain, and you want to draw user and group information from a flat file rather than from the operating system.
- Use the *AuthProtocolDataSource* parameter to specify the source of any protocol-related information. For example, you can specify the name of a file that contains user ID and password information. The user ID and password information in this file must exactly mirror the operating system user ID and password definitions. Make sure that you set the appropriate file system security for this password file.
- The default location of this file is the WebSphere Event Broker home directory. If you store the file somewhere else, give the full path definition of the location of the file.
- For the change to the User Name Server to take effect you must stop and then restart the User Name Server.

The **mqschangeusername** command also supports a *-d* flag to disable the option.

Configuring a broker

Configure a broker to support WebSphere Event Broker authentication services. You need to specify two authentication and access control parameters and use the workbench to configure the appropriate Real-timeInput nodes and the sets of protocols that are to be supported on the broker.

The following steps show you how to do this.

- Switch to the Broker Administration perspective.
- For each message flow in the Message Flow Topology:
 1. Right-click the Real-timeInput node.
 2. Click properties.
 3. Check the Authentication box.

- For each broker in the Broker Topology:
 1. Right-click the broker.
 2. Click properties.
 3. Fill in the Authentication Protocol Type field

Choose any combination of the options P, M, S, and R; for example, S, SR, RS, R, PS, SP, PSR, SRM, MRS, and RSMP are all valid combinations of options.

The order in which you specify the options is significant; the broker chooses the first option that the client supports. If you want the broker to always support the strongest protocol that the client supports, choose RSMP.
 4. If you have chosen S or R as one of the options in the Authentication Protocol Type field, specify the SSL Key Ring File Name and the SSL Password File Name.
 5. Click OK.
 6. Use the **mqsicreatebroker** or **mqsichangebroker** command, with the following two parameters, to configure the broker:

UserNameServerQueueManagerName (-s)

This parameter specifies the name of the queue manager associated with the User Name Server. This parameter must be specified if you require authentication services, publish/subscribe access control services, or both types of service.

Publish/Subscribe Access Control Flag (-j)

This flag must be set, in addition to specifying the UserNameServerQueueManagerName parameter, if you want to use publish/subscribe access control services.

There is no corresponding flag for using the authentication services in the broker; it is enabled at the IP input node level.

Sample password files

Two sample files, named password.dat and pwgroup.dat, are shipped with WebSphere Event Broker.

pwgroup.dat is a sample file that can be used when you set the -j flag.

password.dat is a sample file that can be used in the default case.

password.dat has the following layout:

```
# This is a password file.

# Each line contains two required tokens delimited by
# commas. The first is a user ID, the second is that user's
# password.

#USERNAME PASSWORD
=====
subscriber,subpw
admin,adminpw
publisher,pubpw
```

This file complements the user and group information drawn by the User Name Server from the operating system. User names that are defined in the file, but not

the operating system, are treated as unknown by the broker domain. User names that are defined in the operating system, but are not defined in the password file, are denied access to the system.

pwgroup.dat contains group information as well as user and password information. Each user entry includes a list of group names that specify the groups that contain the user.

pwgroup.dat has the following layout:

```
#This is a password file.
#Each line contains two or more required tokens delimited by
#commas.The first is a user ID and the second is that user's
#password. All subsequent tokens
#specify the set of groups that the user belongs to.

#USERNAME PASSWORD GROUPS
subscriber,subpw,group1,group2,group3
admin,adminpw,group2
publisher,pubpw,group2,group4
```

As mentioned above, this file can be used to provide the only source of user, group, and password information for the broker domain.

To deploy updated user and password information to the broker network if this information is drawn from an operating system file, stop the User Name Server and brokers, update the file, and then restart the User Name Server and brokers.

If passwords are drawn from the operating system, updates are automatically distributed to the brokers. Use normal operating system management tools to change users or passwords.

Authentication in the JMS client

For client applications that use WebSphere MQ classes for Java Message Service Version 5.3 before CSD4, the client application always has an authentication protocol level of PM. The client application and broker negotiate on the choice of protocol for a session. Where the broker supports both protocols (that is, you have set PM or MP in the workbench definition of a broker), the first protocol specified in the workbench is chosen.

For client applications that use WebSphere MQ classes for Java Message Service Version 5.3, CSD 5 or later, the client application supports two levels of authentication.

A *TopicConnectionFactory* can be configured to support either a MQJMS_DIRECTAUTH_BASIC authentication mode or a MQJMS_DIRECTAUTH_CERTIFICATE authentication mode. The MQJMS_DIRECTAUTH_BASIC authentication mode is equivalent to a level of PM and the MQJMS_DIRECTAUTH_CERTIFICATE authentication mode is equivalent to a level of SR.

If authentication services have been successfully configured for a Real-timeInput node, a JMS client application needs to specify its credentials when creating a connection. To do this, the JMS client application supplies a user/password combination to the *TopicConnectionFactory.createTopicConnection* method; for example:

```
factory.createTopicConnection("user1", "user1pw");
```

If credentials are not specified, or are specified incorrectly, the application receives a JMS wrapped exception containing the MQJMS error text.

Using message protection

To use message protection (sometimes known as Quality of Protection (QoP)), set the `enableQopSecurity` parameter of the `mqsichangeproperties` command to true. The default value of this parameter is false.

To define a level of message protection for \$SYS topics, use the `sysQopLevel` parameter of the `mqsichangeproperties` command.

To define a level of message protection for \$ISYS topics, use the `isysQopLevel` parameter of the `mqsichangeproperties` command.

Choose one of the following values for these parameters:

- n** This is the default value. It gives no message protection.
- c** This provides channel integrity. With this level of protection, hackers cannot insert or delete messages without being detected.
- m** This provides message integrity. With this level of protection, hackers cannot change the content of a message without being detected.
- e** This provides message encryption. With this level of protection, hackers cannot look at the content of a message.

Securing WebSphere MQ resources

Secure the WebSphere MQ resources that your configuration requires.

This section does not apply to z/OS.

WebSphere Event Broker depends on a number of WebSphere MQ resources to operate successfully. You must control access to these resources to ensure that the product components can access the resources on which they depend, and that these same resources are protected from other users.

Some authorizations are granted on your behalf when commands are issued. Others depend on the configuration of your broker domain.

- When you issue the command `mqsicreatebroker`, it grants put and get authority on your behalf to the group `mqrbrkrs` for the following queues:
 - SYSTEM.BROKER.ADMIN.QUEUE
 - SYSTEM.BROKER.CONTROL.QUEUE
 - SYSTEM.BROKER.EXECUTIONGROUP.QUEUE
 - SYSTEM.BROKER.EXECUTIONGROUP.REPLY
 - SYSTEM.BROKER.INTERBROKER.QUEUE
 - SYSTEM.BROKER.MODEL.QUEUE
- When you issue the command `mqsicreateconfigmgr` it grants put and get authority on your behalf to the group `mqrbrkrs` for the following queues:
 - SYSTEM.BROKER.CONFIG.QUEUE
 - SYSTEM.BROKER.CONFIG.REPLY
 - SYSTEM.BROKER.ADMIN.REPLY
 - SYSTEM.BROKER.SECURITY.REPLY
 - SYSTEM.BROKER.MODEL.QUEUE

- When you issue the command `mqsicreateusername`, it grants put and get authority on your behalf to the group `mqbrkrs` for the following queues:
 - SYSTEM.BROKER.SECURITY.QUEUE
 - SYSTEM.BROKER.MODEL.QUEUE
- When you issue the command `mqsicreateaclentry`, it grants put and get authority on your behalf to the resource or user that you have specified for the command parameters `-p` or `-u` for the following queues:
 - SYSTEM.BROKER.CONFIG.QUEUE
 - SYSTEM.BROKER.CONFIG.REPLY
- If you have created WebSphere Event Broker components to run on different queue managers, the transmission queues that you define to handle the message traffic between the queue managers must have put and setall authority granted to the local `mqbrkrs` group, or to the service user ID of the component supported by the queue manager on which the transmission queue is defined.
- When you start the workbench, it connects to the Configuration Manager using a WebSphere MQ client/server connection. For details of WebSphere MQ channel security refer to "Setting up WebSphere MQ client security" in the *WebSphere MQ Clients* book.
- When you create and deploy a message flow, grant:
 1. get and inq authority to each input queue identified in an MQInput node, for the broker's ServiceUserID.
 2. put and inq authority to each output queue identified in an MQOutput node, or by an MQReply node, for the broker's ServiceUserID.
 3. get authority to each output queue identified in an MQOutput node or an MQReply node to the user ID under which a receiving or subscribing client application runs.
 4. put authority to each input queue identified in an MQInput node to the user ID under which a sending or publishing client application runs.

Part 2. Configuring the broker domain

Configuring the broker domain	51	Removing a broker from a broker domain	178
Designing a broker domain	52	Removing deployed children from a broker	179
Considering resource naming conventions	52	Adding an execution group to a broker.	179
Designing the WebSphere MQ infrastructure	54	Copying an execution group	180
Considering performance in the domain.	58	Modifying execution group properties	181
Customizing the z/OS environment	60	Renaming an execution group.	181
z/OS customization overview	62	Deleting an execution group	181
Customizing UNIX System Services on z/OS	71	Removing deployed children from an execution	182
DB2 planning on z/OS	73	group	182
WebSphere MQ planning for z/OS	76	Configuring a publish/subscribe topology.	182
Resource Recovery Service planning on z/OS	77	Setting up the broker domain for	183
Defining the started tasks to z/OS Workload	77	publish/subscribe	183
Manager (WLM).	77	Operating a publish/subscribe domain.	197
Mounting file systems.	78	Configuring the workbench	199
Checking the permission of the installation	78	Changing workbench preferences.	199
directory	78	Changing Broker Administration preferences	200
Checking the level of Java on z/OS	79	Changing palette preferences	200
Checking APF attributes of bipimain on z/OS.	79	Configuring CVS to run with the Message	202
Collecting broker statistics on z/OS	80	Brokers Toolkit	202
Configuring an execution group address space as	80	Changing locales	202
non-swappable on z/OS	80	Changing your locale on UNIX and Linux	203
Creating WebSphere Event Broker components	80	systems	203
on z/OS	80	Changing your locale on Windows	204
Configuring broker domain components.	83	Changing your locale on z/OS	205
Configuring component databases.	85	Code page converters	206
Creating a broker	108		
Adding an execution group to a broker using	123		
the command line	123		
Adding an execution group to a broker on z/OS	124		
Creating a Configuration Manager	125		
Enabling a User Name Server	135		
Creating a User Name Server	136		
Using the Default Configuration wizard	150		
Using the Command Assistant wizard	151		
Verifying components	153		
Connecting components	153		
Modifying a broker	155		
Modifying a Configuration Manager	158		
Modifying a User Name Server	161		
Modifying component database access	164		
Moving from WebSphere Event Broker on a	164		
distributed platform to z/OS	164		
Deleting an execution group from a broker	165		
using the command line.	165		
Deleting a broker	166		
Deleting a Configuration Manager	167		
Disabling a User Name Server.	169		
Deleting a User Name Server	169		
Configuring a broker domain in the workbench	171		
Creating a domain connection.	172		
Modifying domain connection properties	173		
Deleting a domain connection	174		
Adding a broker to a broker domain	175		
Copying a broker	176		
Modifying broker properties	177		
Renaming a broker	177		

Configuring the broker domain

A broker domain is a collection of brokers that share a common configuration, together with a single Configuration Manager that controls them. A domain can also include a User Name Server that interfaces with operating system facilities to determine valid users and groups for publish/subscribe applications. Review the conceptual information provided in the WebSphere Event Broker Version 6.0 technical overview for an overview of the broker domain and the broker domain components.

Design your broker domain before you create and configure its components. Consider the factors described in “Designing a broker domain” on page 52 to create a broker domain that best suits its components and the required functionality.

Creating the broker domain is a two-stage process. You create the physical components using the command line, and then configure the physical components using the workbench or programmatically using the Configuration Manager Proxy Java API.

On Windows, you can create, modify, and delete physical components “Using the Command Assistant wizard” on page 151.

If you require a default broker domain configuration on Linux or Windows, you can use the Default Configuration wizard. The Default Configuration wizard creates all the components you need to start exploring WebSphere Event Broker and run the supplied samples. See “Using the Default Configuration wizard” on page 150.

Before you configure a broker domain, review the information in “Authorization for configuration tasks” on page 3 and “Setting up broker domain security” on page 11 to ensure that you have the correct authorization and permission to create and access WebSphere Event Broker resources.

The following set of tasks takes you through the process for creating and configuring the broker domain (depending on the configuration that you require, and the platform that you are using):

- “Designing a broker domain” on page 52
- “Customizing the z/OS environment” on page 60
- “Configuring broker domain components” on page 83
- “Configuring a broker domain in the workbench” on page 171
- “Configuring a publish/subscribe topology” on page 182

This section also provides information about setting preferences within the workbench in “Configuring the workbench” on page 199, and about system locale settings in “Changing locales” on page 202.

Designing a broker domain

When you plan a new WebSphere Event Broker domain, you must first have considered your resource naming conventions, the design of the WebSphere MQ infrastructure, and any performance issues. The following topics describe these considerations:

- “Considering resource naming conventions”
- “Designing the WebSphere MQ infrastructure” on page 54
- “Considering performance in the domain” on page 58

When you are designing a broker domain consider the following elements.

1. **Brokers:** The number of brokers that you need in your domain depends on the following factors:
 - a. **Performance:** What is the required message throughput? (Refer to “Optimizing message flow throughput” on page 58). What is the size of the messages that are being processed? Larger messages take longer to process. A small number of brokers handling many messages might impact the broker domain’s performance. Refer to “Considering performance in the domain” on page 58.
 - b. Do you need to isolate applications from each other? You might want to separate applications that serve different functions, for example personnel and finance.
 - c. Do the brokers need to handle publish/subscribe? Refer to Developing publish/subscribe applications.
2. **User Name Server:** Consider the following if you have a User Name Server in your broker domain:
 - a. **Performance:** If you have a large number of brokers in your broker domain, the requests that they send the User Name Server can be handled more quickly if there is more than one User Name Server. More than one User Name Server might also be beneficial (in terms of network traffic) if your broker domain is complex.
 - b. **Resilience:** Although no standby mechanism is provided by WebSphere Event Broker, you might want to be able to redirect requests to a second User Name Server if a system error occurs on the system of your first User Name Server.
3. **Configuration Manager:** This acts as an interface between the configuration repository and the set of brokers in the domain and the workbench. It uses WebSphere MQ messages to communicate with the brokers, and thus a large number of brokers in a broker domain (if poorly designed) can cause congestion at the Configuration Manager. To solve this, consider dividing the brokers into more than one domain where related brokers are kept together. You can then establish connections with each domain (refer to “Creating a domain connection” on page 172).

Considering resource naming conventions

When you plan a new WebSphere Event Broker network, one of your first tasks must be to establish a convention for naming the resources that you create within this network. There are three aspects to this:

- Product component naming conventions
- WebSphere MQ naming conventions

- Database naming conventions

Product component naming conventions

A naming convention for WebSphere Event Broker resources throughout your network ensures that names are unique, and that users creating new resources can be confident of not introducing duplication or confusion.

The resources you must create and name within an WebSphere Event Broker network are:

Configuration Managers

When you create a Configuration Manager, give it a name that is unique on your system. Names must be unique between Configuration Managers and between Configuration Managers and brokers. Configuration Manager names are case sensitive on UNIX systems.

Brokers

When you create a broker, give it a name that is unique within your broker domain. You must use the same name for that broker when you create it on the system in which it is installed (using the command **mqsicreatebroker**) and when you create a reference to that broker in the broker domain topology in the workbench. The latter is a representation of the physical broker (created by **mqsicreatebroker**) in the configuration repository, and this single name links the two. Broker names are case-sensitive except on Windows platforms.

Execution groups

Each execution group name must be unique within a broker.

Message flows and message processing nodes

Each message processing node must be unique within the message flow it is assigned to. For example, if you include two MQOutput nodes in a single message flow, provide a unique name for each.

Message flow names must be unique within the broker domain. Any reference to that name within the broker domain is always to the same message flow. You can assign the same message flow to many brokers.

Message sets and messages

Each message name must be unique within the message set to which it belongs.

Message set names must be unique within the broker domain. Any reference to that name within the broker domain is always to the same message set. You can therefore assign the same message set to many brokers.

The User Name Server is not allocated a name when you create it. It is identified only by the name of the WebSphere MQ queue manager that hosts the services it provides.

WebSphere MQ naming conventions

All WebSphere Event Broker resources have dependencies on WebSphere MQ services and objects. You must therefore also consider what conventions to adopt for WebSphere MQ object names. If you already have a WebSphere MQ naming convention, use a compatible extension of this convention for WebSphere Event Broker resources.

When you create a broker or a Configuration Manager, you must specify a queue manager name. This queue manager is created for you if it does not already exist. Because the broker and Configuration Manager each use a unique set of WebSphere MQ queues, they can share one queue manager, if appropriate. However, every broker must have a dedicated queue manager.

If you set up a User Name Server in your broker domain, this also uses a unique set of WebSphere MQ queues. The User Name Server can therefore also share a queue manager with a broker, or the Configuration Manager, or both.

Ensure that every queue manager name is unique within your network of interconnected queue managers, whether or not every queue manager is in your WebSphere Event Broker network. This ensures that each queue manager can unambiguously identify the target queue manager to which any given message must be sent, and that WebSphere Event Broker applications can also interact with basic WebSphere MQ applications.

WebSphere MQ supports a number of objects defined to queue managers. These objects (queues, channels, and processes) also have naming conventions and restrictions.

In summary, the restrictions are:

- All names must be a maximum of 48 characters in length (channels have a maximum of 20 characters).
- The name of each object must be unique within its type (for example, queue or channel).
- Names for all objects starting with the characters SYSTEM. are reserved for use by IBM.

There are a few restrictions for naming resources: see “Naming conventions for WebSphere Event Broker for z/OS” on page 370.

Database naming conventions

Consider the naming conventions you use for databases, both for databases that you create for WebSphere Event Broker product and for databases that you create for application use.

Database tables used for brokers can be unique and local to the broker, or can be *shared*, because the rows of the tables specific to each individual broker incorporate the name of the broker. You might need to align the naming of all these databases with other databases that are in use in your broker domain.

Also ensure that the databases used for application data (accessed through message flows) are uniquely named throughout your network, so that there is no opportunity for confusion or error.

Designing the WebSphere MQ infrastructure

WebSphere Event Broker depends on the WebSphere MQ transport services to support internally-generated communications between components. Some of these resources are created for you, when you create WebSphere Event Broker components that depend on them. Others depend on the exact setup of your broker domain; you must create these resources yourself.

Communications between WebSphere Event Broker components are protocol-independent, with the exception of the connection between every instance of the workbench and the Configuration Manager. This must be a TCP/IP connection, as must connections to the WebSphere MQ Everyplace and SCADA nodes. Other connections can use any of the protocols supported by the WebSphere MQ messaging product for the operating system for your WebSphere Event Broker product.

Except for WebSphere MQ Everyplace and SCADA applications, applications that use broker services must also use WebSphere MQ to send and receive all messages. The resources required by your applications (queues and client connection and server connection channels) are application specific; you must create these resources yourself.

The information here concentrates on the specific requirements that WebSphere Event Broker imposes on a WebSphere MQ network. For a full description of designing and connecting a WebSphere MQ network, see *WebSphere MQ Intercommunication*, which covers the basics, such as setting up transmission queues and channels, in detail.

For further information see:

- “WebSphere MQ resources for the broker”
- “WebSphere MQ resources for the Configuration Manager” on page 56
- “WebSphere MQ resources for the User Name Server” on page 57

WebSphere MQ resources for the broker

Each broker depends on a number of WebSphere MQ resources: some must be available, others depend on the broker domain setup. Some of these resources are created for you: you must define others yourself.

WebSphere MQ resources created for you

When you create a broker, the following WebSphere MQ resources are created for you:

- The broker’s queue manager. Each broker must be associated with a queue manager. Specify a queue manager name when you create the broker. If this queue manager does not exist, it is created for you. (For WebSphere Event Broker on z/OS, you must create a queue manager in WebSphere MQ for your broker. See “Creating a broker on z/OS” on page 116 for more details.) This can be shared with the Configuration Manager and User Name Server
- Fixed-name queues on the broker’s queue manager. These allow information to be exchanged with other components in the broker domain.

WebSphere MQ resources that you must create yourself

Depending on the setup of your broker, you might need to create some WebSphere MQ resources yourself. You can create WebSphere MQ resources using commands and utilities such as runmqsc and the PCF interface, or you can use WebSphere MQ Services (with WebSphere MQ Version 5) or WebSphere MQ Explorer (with WebSphere MQ Version 6).

- For WebSphere Event Broker on z/OS, you must create a queue manager in WebSphere MQ for your broker. See “Creating a broker on z/OS” on page 116 for more details.

- If the broker and Configuration Manager do not share a queue manager, you must define the channels and transmission queues to support communication between the broker's queue manager and the Configuration Manager's queue manager.
- If the broker and User Name Server do not share a queue manager, you must define the channels and transmission queues to support communication between the broker's queue manager and the Configuration Manager's queue manager.
- You must define listener connections on the broker's queue manager. You must define one listener connection for every protocol used.
- For connection between brokers, you must define the channels and transmission queues to permit two-way communication between them.

For more information about creating WebSphere MQ resources, see *WebSphere MQ Intercommunication*, available on the WebSphere MQ library Web page.

WebSphere MQ resources for the Configuration Manager

Each Configuration Manager depends on a number of WebSphere MQ resources: some must be available, others depend on the broker domain setup. Some of these resources are created for you: you must define others yourself.

WebSphere MQ resources created for you

When you create a Configuration Manager, the following WebSphere MQ resources are created for you:

- The Configuration Manager's queue manager. Each Configuration Manager must be associated with a queue manager. Specify a queue manager name when you create the Configuration Manager. If this queue manager does not exist, it is created for you. (For WebSphere Event Broker on z/OS, you must create a queue manager in WebSphere MQ for your Configuration Manager. See "Creating a Configuration Manager on z/OS" on page 130 for more details.)
- Fixed-name queues on the Configuration Manager's queue manager. These allow information to be exchanged with other components in the broker domain.
- A server connection for use by the Workbench.

WebSphere MQ resources that you must create yourself

Depending on the setup of your Configuration Manager, you might need to create some WebSphere MQ resources yourself. You can create WebSphere MQ resources using commands and utilities such as `runmqsc` and the PCF interface, or you can use WebSphere MQ Services (with WebSphere MQ Version 5) or WebSphere MQ Explorer (with WebSphere MQ Version 6).

- For WebSphere Event Broker on z/OS, you must create a queue manager in WebSphere MQ for your Configuration Manager. See "Creating a Configuration Manager on z/OS" on page 130 for more details.
- You must define the transmission queues and channels between the Configuration Manager and every broker in the domain (apart from the broker that shares a queue manager with the Configuration Manager).
- If the Configuration Manager and User Name Server do not share a queue manager, you must define the channels and transmission queues to support communication between the broker's queue manager and the Configuration Manager's queue manager.

- You must define listener connections on the Configuration Manager's queue manager for the Workbench and other components and clients that do not share the Configuration Manager's queue manager. You must define one listener connection for every protocol used.

For more information about creating WebSphere MQ resources, see *WebSphere MQ Intercommunication*, available on the WebSphere MQ library Web page.

WebSphere MQ resources for the User Name Server

Each User Name Server depends on a number of WebSphere MQ resources: some must be available, others depend on the broker domain setup. Some of these resources are created for you: you must define others yourself.

WebSphere MQ resources created for you

When you create a User Name Server, the following WebSphere MQ resources are created for you:

- The User Name Server's queue manager. Each User Name Server must be associated with a queue manager. Specify a queue manager name when you create the User Name Server. If this queue manager does not exist, it is created for you. (For WebSphere Event Broker on z/OS, you must create a queue manager in WebSphere MQ for your User Name Server. See "Creating a User Name Server on z/OS" on page 139 for more details.)
- Fixed-name queues on the User Name Server's queue manager. These allow information to be exchanged with other components in the broker domain.

WebSphere MQ resources that you must create yourself

Depending on the setup of your User Name Server, you might need to create some WebSphere MQ resources yourself. You can create WebSphere MQ resources using commands and utilities such as `runmqsc` and the PCF interface, or you can use WebSphere MQ Services (with WebSphere MQ Version 5) or WebSphere MQ Explorer (with WebSphere MQ Version 6).

- For WebSphere Event Broker on z/OS, you must create a queue manager in WebSphere MQ for your User Name Server. See "Creating a User Name Server on z/OS" on page 139 for more details.
- If the Configuration Manager and User Name Server do not share a queue manager, you must define the channels and transmission queues to support communication between them.
- You must define the transmission queues and channels between the User Name Server and every broker in the domain (apart from the broker that shares a queue manager with the User Name Server).
- You must define listener connections on the User Name Server's queue manager for components that do not share its queue manager. You must define one listener connection for every protocol used.

For more information about creating WebSphere MQ resources, see *WebSphere MQ Intercommunication*, available on the WebSphere MQ library Web page.

Considering performance in the domain

When you design your broker domain, and the resources associated with its components, there are several areas where decisions that you make can affect the performance of your brokers and applications:

Message flows

A message flow includes an input node that receives a message from an application over a particular protocol (for example WebSphere MQ).

You need to consider how you split your business logic; how much work should the application do, and how much should the message flow do? Every interaction between an application and a message flow involves I/O and message parsing and therefore adds to processing time. Design your message flows, and design or restructure your applications, to minimize these interactions.

For more information about these factors, see *Optimizing message flow response times*.

Messages

The type, format, and size of the messages that are processed can have a significant effect on the performance of a message flow. For example, if you process persistent messages, these have to be stored for safekeeping.

For more information about these factors, see *Optimizing message flow response times*.

Broker configuration and domain topology

You can configure your broker domain to include multiple brokers, multiple systems, multiple execution groups, and so on. These can play a part in how message flows perform, and how efficiently messages can be processed.

For more information about these factors, see *“Optimizing message flow throughput”* and *Performance considerations for Real-time transport*.

All these factors are examined in more detail in the *Designing for Performance SupportPac (IP04)*.

For a description of common performance scenarios, review *Resolving problems with performance*.

For further articles about WebSphere Event Broker and performance, review these sources:

- The Business Integration Zone on developerWorks. This has a search facility; enter "performance" and review the links that are returned.
- The developerWorks article on message flow performance.
- The developerWorks article on monitoring resource use.
- A developerWorks article that describes other available resources including best practices, tools, and performance data.

Optimizing message flow throughput

Each message flow that you design must provide a complete set of processing for messages received from a certain source. However, this might result in very complex message flows that include large numbers of nodes and cause a

performance overhead and potential bottlenecks. Increasing the number of message flows that process your messages provides the opportunity for parallel processing and therefore improved throughput.

You can also consider the way in which the actions taken by the message flow are committed, and the order in which messages are processed.

Consider the following options for optimizing message flow throughput:

Multiple threads processing messages in a single message flow

When you deploy a message flow, the broker automatically starts an instance of the message flow for each input node that it contains. This is the default behavior. However, if you have a message flow that handles a very large number of messages, the input source (for example, a WebSphere MQ queue) might become a bottleneck.

You can update the *Additional Instances* property of the deployed message flow in the bar file: the broker starts additional copies of the message flow on separate threads, providing parallel processing. This is the most efficient way of handling this situation, if you are not concerned about the order in which messages are processed.

If the message flow receives messages from a WebSphere MQ queue, you can influence the order in which messages are processed to some extent by setting the *Order Mode* property of the MQInput node:

- If you set *Order Mode* to By User ID, the node ensures that messages from a specific user (identified by the *UserIdentifier* field in the MQMD) are processed in guaranteed order. A second message from one user is not processed by an instance of the message flow if a previous message from this user is currently being processed by another instance of the message flow.
- If you set *Order Mode* to By Queue Order, the node processes one message at a time to preserve the order in which the messages are read from the queue. Therefore, this node behaves as though you have set the *Additional Instances* property of the message flow to zero.

For publish/subscribe applications that communicate with the broker over any supported protocol, messages for any given topic are published by brokers in the same order as they are received from publishers (subject to reordering based on message priority, if applicable). This normally means that each subscriber receives messages from a particular broker, on a particular topic, from a particular publisher, in the order that they are published by that publisher.

However, it is possible for messages, occasionally, to be delivered out of order. This can happen, for example, if a link in the network fails and subsequent messages are routed by another link.

If you need to ensure the order in which messages are received, you can use either the *SeqNum* (sequence number) or *PubTime* (publish time stamp) parameter on the **Publish** command for each published message, to calculate the order of publishing.

For more information about the techniques recommended for all MQI and AMI users, see the *WebSphere MQ Application Programming Guide* for programs written to the MQI, and *WebSphere MQ Application Messaging Interface* (available as SupportPac MA0F from the WebSphere MQ SupportPacs Web page) for programs written to the AMI.

WebSphere MQ Everyplace and SCADA applications use a different method of message ordering as described in WebSphere MQ Mobile Transport and WebSphere MQ Telemetry Transport respectively. The broker does not provide message ordering for messages received across WebSphere MQ Real-time Transport or WebSphere MQ Multicast Transport.

Multiple copies of the message flow in a broker

You can also deploy several copies of the same message flow to different execution groups in the same broker. This has similar effects to increasing the number of processing threads in a single message flow, although usually provides less noticeable gains.

This option also removes the ability to determine the order in which the messages are processed. This is because, if there is more than one copy of the message flow active in the broker, each copy can be processing a message at the same time, from the same queue. The time taken to process a message might vary, and multiple message flows accessing the same queue could therefore read messages from the input source in a random order. The order of messages produced by the message flows might not correspond to the order of the original messages.

Ensure that the applications that receive message from these message flows can tolerate out-of-order messages.

Copies of the message flow in multiple brokers

You can deploy several copies of the same message flow to different brokers. This solution requires changes to your configuration, because you must ensure that applications that supply messages to the message flow can put their messages to the right input queue or port. You can often make these changes when you deploy the message flow by setting the message flow's configurable properties.

Customizing the z/OS environment

Although you might be installing only one broker initially, you should consider how the product will be used in your organization in a few years' time. Planning ahead makes developing your WebSphere Event Broker configuration easier.

You should consider creating the Configuration Manager on z/OS to manage the broker domain. If you are migrating from an earlier version of WebSphere Event Broker you should consider migrating the Configuration Manager that was previously on Windows.

If you want to run a Configuration Manager on z/OS, you can either:

- Connect to the Message Brokers Toolkit directly, if you have the optional WebSphere MQ Client Attach feature installed; see "Connecting directly to a Configuration Manager on z/OS" on page 82, or
- Connect through an intermediate queue manager (for example, on Windows) and define the necessary WebSphere MQ components to communicate with the z/OS queue manager; see "Connecting to a z/OS Configuration Manager through an intermediate queue manager" on page 82.

If you are using publish/subscribe with security, you also need a User Name Server. The User Name Server can be on z/OS or on another platform. The queue managers need to be interconnected so that information from the User Name Server can be distributed to the brokers on other queue managers.

A broker requires access to a queue manager and to DB2. A Configuration Manager and User Name Server require access to a queue manager only. A broker cannot share its queue manager with another broker, but a broker can share a queue manager with a Configuration Manager and User Name Server.

You cannot use WebSphere MQ shared queues to hold data related to WebSphere Event Broker as SYSTEM.BROKER queues, but you can use shared queues for your message flow queues.

You can find details of the DB2 database user tables and the WebSphere MQ queues created and used by WebSphere Event Broker on z/OS in the topic “mqsicreatebroker command” on page 286.

When planning to work in a z/OS environment, you must complete the following tasks:

- Create started task procedures for the broker, User Name Server, and Configuration Managers that you plan to use. These procedures need to be defined, in the started task table, with an appropriate user ID.
- Decide on your recovery strategy. As part of your systems architecture, you should have a strategy for restarting systems if they end abnormally. Common solutions are to use automation products like NetView or the Automatic Restart Manager (ARM) facility. You can configure WebSphere Event Broker to use ARM.
- Plan for corequisite products, including UNIX System Services, Resource Recovery Services, DB2, WebSphere MQ, and Java.
- Ensure that the runtime library system (RTLS) for the broker is turned off in the language environment default options for the system. This is because the broker code is compiled using XPLINK, and XPLINK applications cannot be started while RTLS is active.
- Collect broker statistics on z/OS

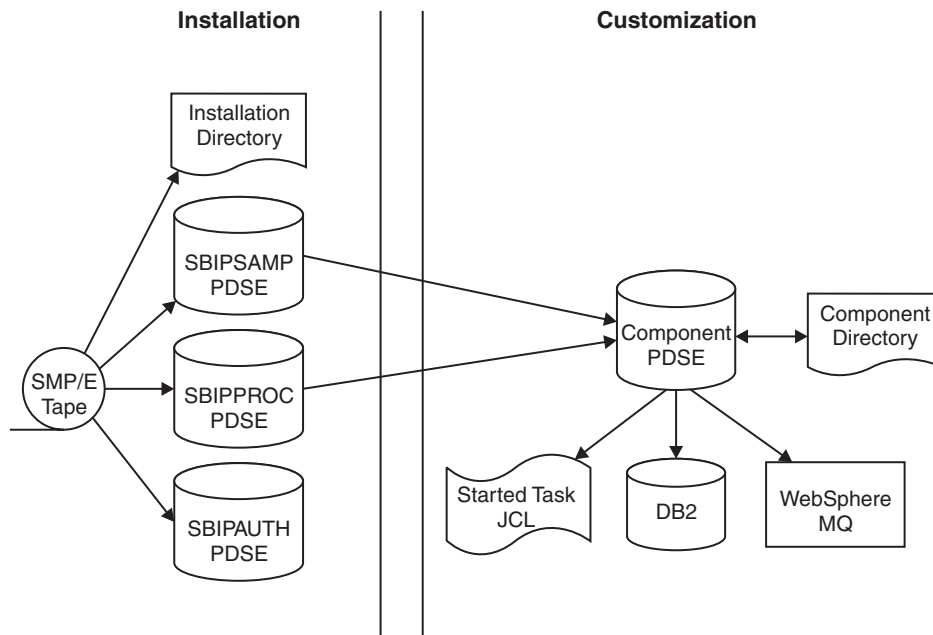
See the following topics for more information:

- “z/OS customization overview” on page 62
- “Customizing UNIX System Services on z/OS” on page 71
- “DB2 planning on z/OS” on page 73
- “WebSphere MQ planning for z/OS” on page 76
- “Resource Recovery Service planning on z/OS” on page 77
- “Defining the started tasks to z/OS Workload Manager (WLM)” on page 77
- “Mounting file systems” on page 78
- “Checking the permission of the installation directory” on page 78
- “Checking the level of Java on z/OS” on page 79
- “Checking APF attributes of bipimain on z/OS” on page 79
- “Collecting broker statistics on z/OS” on page 80
- “Configuring an execution group address space as non-swappable on z/OS” on page 80

For an overview of how to create WebSphere Event Broker components, see “Creating WebSphere Event Broker components on z/OS” on page 80

z/OS customization overview

After you have used SMP/E to install WebSphere Event Broker for z/OS, the installed executable code is located inside the file system. JCL samples are located in the PDS <h1q>.SBIPSAMP, the JCL procedures are located in the PDS <h1q>.SBIPPROC, and load module for synchronizing statistics with SMF are located in the PDS <h1q>.SBIPAUTH. The following diagram gives an overview of the post-installation process.



To perform the customization, update and submit the required JCL. All necessary JCL is supplied to create the runtime environments of your broker, Configuration Manager, and User Name Server. You start the broker, Configuration Manager, or User Name Server using one of the supplied JCL files, which is run as a started task.

For more information, see:

- “Installation directory on z/OS”
- “Components on z/OS” on page 63
- “Component directory on z/OS” on page 63
- “Component PDSE on z/OS” on page 64
- “XPLink on z/OS” on page 64
- “Binding a DB2 plan to use data-sharing groups on z/OS” on page 64
- “Using the file system on z/OS” on page 65
- “Event log messages on z/OS” on page 65
- “Security considerations on z/OS” on page 65
- “Overview of message serialization on z/OS” on page 66

Installation directory on z/OS

On z/OS, the SMP/E installation places all the product executable files into a directory of a file system under UNIX System Services (USS).

For further information on mounting file systems and allocating space see “Mounting file systems” on page 78

Components on z/OS

A *component* is a set of runtime processes that perform a specific set of functions, and can be a broker, a Configuration Manager, or a User Name Server.

A broker processes messages, a Configuration Manager acts as an interface between the configuration repository and the set of brokers in the domain, and a User Name Server extracts information from a security product and makes it available to brokers and the workbench.

A broker that is running has a control address space and one additional address space for each deployed execution group. When the control address space is started, the broker component is started automatically. This behavior can be changed by an optional start parameter in the started task.

A Configuration Manager and User Name Server each have a single address space. When the address space is started, the components are started automatically. This behavior can be changed by an optional start parameter in the started task.

The *component name* is the external name of the component and is used, for example, in the WebSphere Event Broker workbench.

Each component requires a name, which is usually the name of the started task that runs the component. This is typically the queue manager name with a suffix of the facility; for example:

- MQP1BRK for the broker
- MQP1UNS for the User Name Server
- MQP1CMGR for the Configuration Manager

You only need a User Name Server if you are using publish/subscribe security. This User Name Server can exist anywhere in the network, including z/OS.

Each component has its own runtime environment in UNIX System Services and needs its own WebSphere MQ queue manager, although a broker, Configuration Manager, and User Name Server can share a single queue manager. A broker component also needs access to a database.

Component directory on z/OS

The *component directory* is the root directory of the component’s runtime environment.

The *component directory* is also referred to as `ComponentDirectory` in some instances within the code. Both the WebSphere Event Broker administrator and the component require read and write access to the component directory. An example directory for each of the three components follows:

- `/mqsi/brokers/MQP1BRK` for the broker
- `/mqsi/uns/MQP1UNS` for the User Name Server
- `/mqsi/configmgrs/MQP1CMGR` for the Configuration Manager

For further information on mounting file systems and allocating space see “Mounting file systems” on page 78

Component PDSE on z/OS

On z/OS, the *component PDSE* contains jobs customized for a single component. These jobs are used to create and administer the component.

The members specific to a component type are copied from <hlq>.SBIPSAMP and <hlq>.SBIPPROC to the component PDSE. These are then customized for the component.

The broker started-task user ID requires read access to its component PDSE at runtime.

XPLink on z/OS

XPLink is a z/OS technology used by the C and C++ compilers to reduce the cost of function calling for programs written in these languages.

Many products, including WebSphere Event Broker for z/OS, use XPLink technology to improve their performance. To ensure the highest possible performance gains, WebSphere Event Broker requires as many as possible of the software components it uses to be XPLink-compliant. These include the broker, Java runtime, ODBC, and z/OS Language Environment.

The WebSphere Event Broker broker has been compiled by IBM to use XPLink technology and has been link-edited within the SMP/E environment to call the appropriate XPLink routines of the software components it uses. Normally, these XPLink-enabled components are configured during their customization, and the broker needs only to locate the appropriate libraries to become XPLink-enabled.

Binding a DB2 plan to use data-sharing groups on z/OS

During customization, you can specify which plan name to use, or use the default DSNACLI. If you are using XPLink, the default plan is called DSNACLX. If you want your broker to access DB2 data-sharing groups other than its own, the DSNACLI plan must be bound in a special way. If the broker uses one data-sharing group, but might want to access tables on DSNONE and DSNTWO, which are in different data-sharing groups, amend the DB2 supplied job DSNTIJCL so that it looks like this:

```
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLICS) ISOLATION(CS)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLINC) ISOLATION(NC)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIRR) ISOLATION(RR)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIRS) ISOLATION(RS)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIUR) ISOLATION(UR)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIC1)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIC2)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIF4)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIMS)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIQR)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLICS) ISOLATION(CS)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLINC) ISOLATION(NC)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIRR) ISOLATION(RR)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIRS) ISOLATION(RS)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIUR) ISOLATION(UR)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIC1)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIC2)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIF4)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIMS)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIQR)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLICS) ISOLATION(CS)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLINC) ISOLATION(NC)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIRR) ISOLATION(RR)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIRS) ISOLATION(RS)
```



```

BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIUR) ISOLATION(UR)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIC1)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIC2)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIF4)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIMS)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIQR)
BIND PLAN(DSNACLI)-
PKLIST(*.DSNAOCLI.DSNCLICS -
*.DSNAOCLI.DSNCLINC -
*.DSNAOCLI.DSNCLIRR -
*.DSNAOCLI.DSNCLIRS -
*.DSNAOCLI.DSNCLIUR -
*.DSNAOCLI.DSNCLIC1 -
*.DSNAOCLI.DSNCLIC2 -
*.DSNAOCLI.DSNCLIF4 -
*.DSNAOCLI.DSNCLIMS -
*.DSNAOCLI.DSNCLIQR )

```

Using the file system on z/OS

This is part of the larger task of customizing your z/OS environment.

If you have more than one MVS™ image, consider how you will use the file system. You can share files in a file system across different members of a sysplex. The file system is mounted on one MVS image and requests to the file are routed to the owning system using XCF from systems which do not have it mounted.

Moving a broker, User Name Server, or Configuration Manager from one image to another is straightforward and the files for each component can be shared.

However, there is a performance overhead when using files shared between images in a file system because the data flows through the Coupling Facility (this is true for trace and other diagnostic data).

For further information on mounting file systems and allocating space see “Mounting file systems” on page 78

Space requirements:

For details of the disk space required, see “Disk space requirements on z/OS” on page 376.

Event log messages on z/OS

This is part of the larger task of customizing your z/OS environment.

On z/OS, all address spaces have a job log where BIP messages issued by WebSphere Event Broker appear. Additionally, all messages appear on the syslog and important operator messages are filtered to the console using MPF (Message Processing Facility).

To prevent the operator’s console receiving unnecessary BIP messages, you must configure MPF to suppress all BIP messages, with the exception of important messages. Note that you do not need to have the USS SYSLOG configured.

Security considerations on z/OS

This is part of the larger task of customizing your z/OS environment.

The role of the WebSphere Event Broker administrator includes customizing and configuring, running utilities, performing problem determination, and collecting diagnostic materials. People involved in these activities need WebSphere Event Broker authorities. You must set up some security for WebSphere Event Broker to work properly. The information that you need to do this is in “Setting up z/OS security” on page 28.

Overview of message serialization on z/OS

Some messaging transactions depend upon the exact sequence of messages from a queue, and for that sequence to be maintained in the event of a failure of the queue manager. In these instances you must serialize the access to those messages.

Serialization of messages is achieved through the use of specialized connection options, and a unique connection token when the application that empties the messages from a queue issues a connect call to the WebSphere MQ queue manager that owns that queue.

A typical situation in which WebSphere Event Broker can exploit this feature is the case where multiple brokers, with multiple execution groups, are each running message flows that empty from a shared input queue. If one broker queue manager fails, then the message flow can be automatically started on another broker while maintaining the transactional integrity and original sequencing of the messages on the shared queue.

The following examples demonstrate how these features can be applied:

1. “Serialization of input between separate brokers on z/OS”
2. “Serialization of input between separate execution groups running on the same broker on z/OS” on page 68
3. “Serialization of input within an execution group on z/OS” on page 69

Note the following:

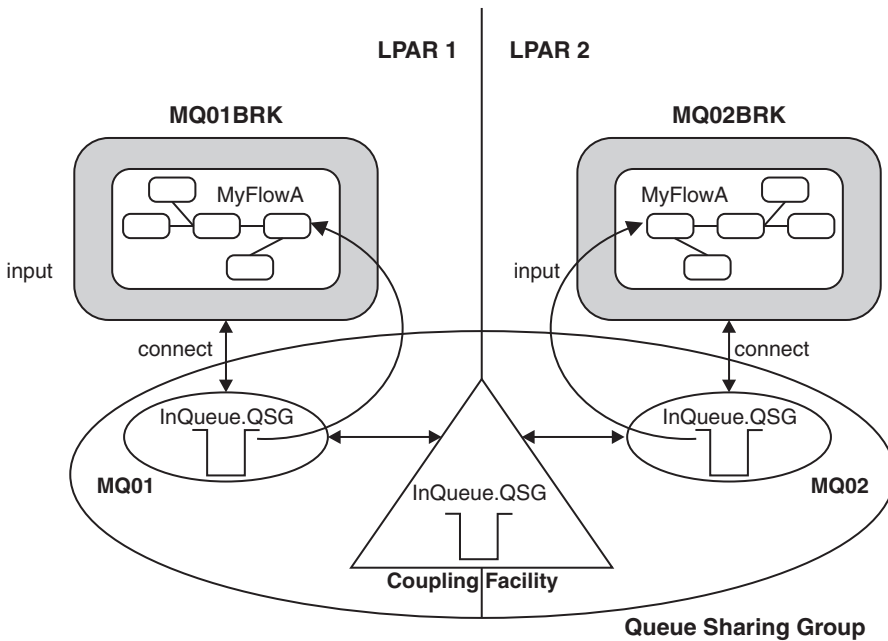
- In each of the first two examples there are two brokers configured, referred to as MQ01BRK and MQ02BRK; the broker’s respective queue managers are called MQ01 and MQ02.
- The queue managers participate in the same queue sharing group. Each queue manager has a shared queue INQueue.QSG that has been defined with a disposition of QSG, and a local queue called INQueue
- The queue managers can be running in the same Logical Partition (LPAR) or separate LPARs.
- The Coupling Facility shown in the following diagrams is a zSeries component that allows z/OS WebSphere MQ queue managers in the same system image, or different system images, to share queues.

Serialization of input between separate brokers on z/OS: This example demonstrates that only one input node at a time takes messages from a shared queue when the same serialization token is used by message flows running on separate brokers.

An identical message flow MyFlowA is deployed to an execution group called MYGroupA on each broker. Note that the message flows do not have to be identical; the significant point is that an identical serialization token is used in both flows.

The simple message flow in this example consists of an MQInput node connected to an MQOutput node. The MQInput node in both message flows gets messages from the shared queue INQueue.QSG; the node attribute Serialization Token is configured as MyToken123ABC in both MQInput nodes.

The message flow property additional Instances takes the default value of zero in both message flows, which ensures that input is serialized within the flow.



A typical sequence of events for this example follows:

1. The first broker MQ01BRK starts and runs message flow MyFlowA in execution group MyGroupA. The input node MyInputNode connects to queue manager MQ01 using a serialization token MyToken123ABC. The input node successfully opens shared queue INQueue.QSG and gets input messages.
2. The second broker MQ02BRK starts and begins to run its copy of message flow MyFlowA in execution group MyGroupA. The Input node MyInputNode attempts to connect to queue manager MQ02, also using a serialization token MyToken123ABC.

The following SDSF console message is logged:

```
BIP2656I MQ02BRK MyGroupA 17 UNABLE TO OPEN QUEUE
'INQueue.QSG' ON WEBSphere BUSINESS INTEGRATION QUEUE
MANAGER 'MQ02': COMPLETION CODE 2; REASON CODE 2271.
:ImbCommonInputNode(759) BECAUSE SERIALIZATION TOKEN
MyToken123ABC is already in use. NO USER ACTION REQUIRED.
```

Note that this message is output every 30 minutes.

Message flow MyFlowA in execution group MyGroupA running on broker MQ02BRK is unable to process input because the serialization token it has passed is already in use within the queue sharing group. This is indicated by the reason code 2271 (MQRC_CONN_TAG_IN_USE) in message bip2623.

3. Broker MQ01BRK stops. Message flow MyFlowA in execution group MyGroupA in broker MQ02BRK2 is now able to get messages from the shared queue INQueue.QSG.

A sequence of SDSF console messages is logged, of which the following two are relevant:

```

BIP2091I MQ02BRK MyGroupA 17 THE BROKER HAS
RECONNECTED TO WEBSphere BUSINESS INTEGRATION
SUCCESSFULLY : ImbCommonInputNode(785)
BIP9142I MQ01BRK 0 THE COMPONENT HAS STOPPED. :
ImbControlService(594)

```

The preceding sequence of events also occurs should broker MQ01BRK fail, rather than stop through a request from the operator, or if a new broker configuration is deployed to MQ01BRK that deletes or modifies message flow MyFlowA.

This arrangement can also be used where the requirement is to migrate message processing between brokers running in different z/OS system images that are attached to the same Coupling Facility.

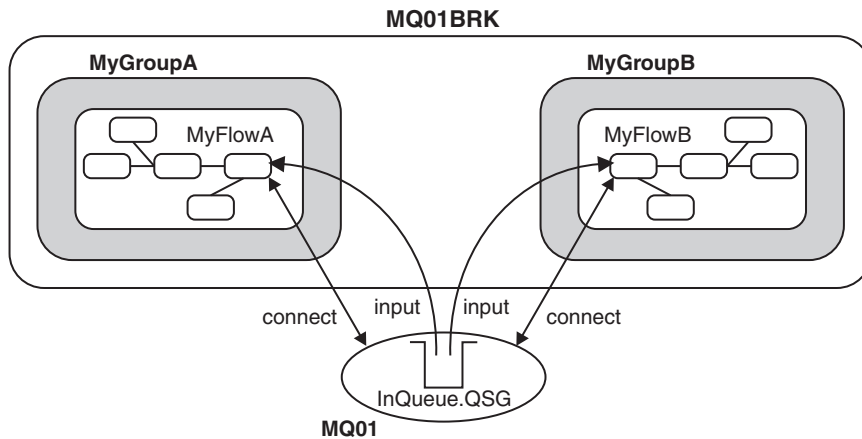
Serialization of input between separate execution groups running on the same broker on z/OS: This example demonstrates that only one MQInput node at a time is allowed to take messages from a shared queue when the same serialization token is used by message flows running in separate execution groups on the same broker.

An identical message flow MyFlowA is deployed to two execution groups called MYGroupA and MYGroupB on broker MQ01BRK.

In this case it is not a requirement that the queue manager participates in a queue sharing group. The input queue INQueue is defined as local with disposition QMGR.

As in “Serialization of input between separate brokers on z/OS” on page 66:

- Note that the message flows do not have to be identical; the significant point is that an identical serialization token is used in both flows.
- The simple message flow in this example consists of an MQInput node connected to an MQOutput node. The MQInput node in both message flows gets messages from the shared queue INQueue.QSG; the node attribute Serialization Token is configured as MyToken123ABC in both MQInput nodes.
- The message flow property additional Instances takes the default value of zero in both message flows, which ensures that input is serialized within the flow.



A typical sequence of events for this example follows:

1. Broker MQ01BRK starts and the first message flow to begin is MyFlowA in execution group MyGroupA. The MQInput node MyInputNode connects to queue manager MQ01 using the serialization token MyToken123ABC. The MQInput node successfully opens shared queue INQueue and gets input messages.
2. The second execution group MyGroupB starts and message flow MyFlowA in execution group MyGroupB begins. The MQInput node MyInputNode now attempts to connect to queue manager MQ01 using serialization token MyToken123ABC. The following SDSF console message is logged:

```
BIP2656I MQ01BRK MyGroupB 11 UNABLE TO OPEN QUEUE  
'INQueue' ON WEBSHERE BUSINESS INTEGRATION QUEUE  
MANAGER 'MQ01': BECAUSE SERIALIZATION TOKEN  
MyToken123ABC is already in use. NO USER ACTION REQUIRED
```

Message flow MyFlowA in execution group MyGroupB is unable to process input because the serialization token it has passed is already in use within the queue manager (by the MQInput node in message flow MyFlowA in execution group MyGroupA). This is indicated by the reason code 2271 (MQRC_CONN_TAG_IN_USE) in message bip2623.

3. The first execution group is deleted or cancelled.

If the first execution group is cancelled by the operator, abends, or is deleted during a redeployment of the broker configuration, then the input node in the second execution group is now able to get input messages from queue INQueue.

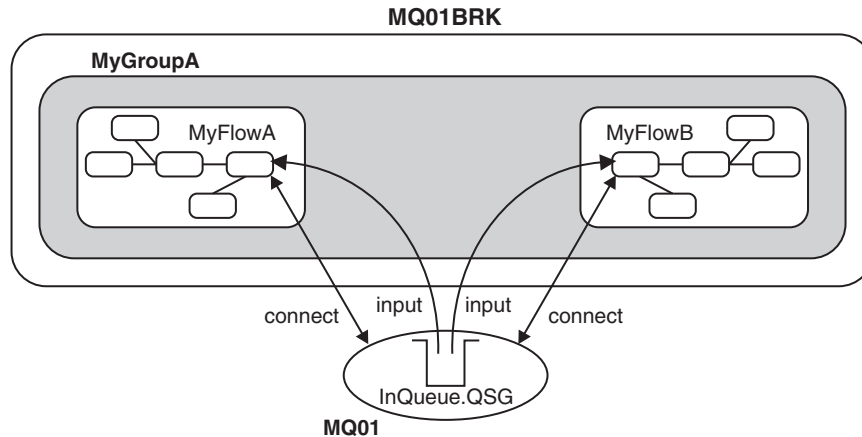
A sequence of SDSF console messages is logged, of which the following one is relevant:

```
BIP2091I MQ01BRK MyGroupB 11 THE BROKER HAS  
RECONNECTED TO WEBSHERE BUSINESS INTEGRATION  
SUCCESSFULLY : ImbCommonInputNode(785)
```

Message flow MyFlowA in execution group MyGroupB is now able to recover processing of messages from the shared queue INQueue.QSG.

Note that, although serialization of input can be achieved in a similar manner by configuring the input queue for exclusive input, this does not ensure message integrity during a recovery situation. This can be achieved only through the use of the serialization token as described in this example.

Serialization of input within an execution group on z/OS: To allow concurrent processing within a message flow, while still serializing messages between message flows in separate execution groups, the scope of the serialization token is restricted within a single execution group.



This example demonstrates that the serialization token is restricted within a single execution group running on a broker::

- Two MQInput nodes in separate message flows (in this case MyFlowA and MyFlowB) are running within the same execution group MyGroupA. Both MQInput nodes concurrently get messages from the shared input queue even though they are using the same serialization token.
- If serialization is required within a single message flow then the message flow attribute `additional instances` must be set to zero which is the default setting. However, if greater throughput is required and serialization of input within the flow is not important, you can set `additional instances` to a value greater than zero.
- The use of the serialization token attribute on the MQInput node does not serialize input between message flows operating within the same execution group. However, setting the attribute has no adverse affect on the processing within that execution group
- In this way it is possible to maximize throughput in a message flow on one broker while still serializing input between brokers. This is useful where the requirement is to have one or more brokers acting as an immediate standby, should the currently active broker need to be stopped for servicing, or fail unexpectedly.

Serialization token - user tasks on z/OS:

This topic gives an overview of the steps needed to:

- Configure a shared input queue for message flows
- Define a serialization token

Configure a shared input queue for message flows

The WebSphere Event Broker broker makes use of WebSphere MQ queue-sharing groups on z/OS.

Queue managers that can access the same set of shared queues form a group called a queue-sharing group (QSG) and they communicate with each other by means of a coupling facility (CF) that stores the shared queues. A shared queue is a type of local queue whose messages can be accessed by one or more queue managers that are in a QSG.

To further enhance the availability of messages in a QSG, WebSphere MQ detects if another queue manager in the group disconnects from the CF in an unusual way, and completes pending units of work for that queue manager where possible; this is known as peer recovery.

To understand more fully the concepts of shared-queues and queue-sharing groups, see the *WebSphere MQ for z/OS Concepts and Planning Guide* and perform the following steps:

- Add a QSG to the DB2 tables
- Add a queue manager to a QSG
- Create the shared queue as a member of the QSG

Define a serialization token

Define the same value for the serialization token attribute for each MQInput node that is required to access the shared queue.

For the situations described in the preceding text to work you must:

- Ensure that the Coupling Facility Structure is at CFLEVEL(3) or above and that you set RECOVER=YES.

If you do not do this, when an MQInput node attempts to get a message from the shared queue, the action fails with the WebSphere MQ return code 2048(MQRC_PERSISTENT_NOT_ALLOWED)

- Set the Backout Threshold for the shared queue to at least 2.

This is to avoid input messages that are in progress being sent to the Dead Letter Queue because, during recovery, a message is restored to the input queue before another broker is able to get it and resume processing.

Customizing UNIX System Services on z/OS

This is part of the larger task of customizing your z/OS environment.

WebSphere Event Broker requires the setup of some UNIX System Services system characteristics. You can use the SETOMVS operator command for dynamic changes or the BPXPRMxx PARMLIB member for permanent changes. See the *z/OS UNIX System Services Planning* manual for more information.

Do not include the broker addresses if you use the IEFUSI exit to limit the region size of OMVS address spaces.

Set the UNIX System Services characteristics as follows:

Description	Parameter	Value
The maximum core dump file size (in bytes) that a process can create. Allow an unlimited size.	MAXCORESIZE	2 147 483 647
The CPU time (in seconds) that a process is allowed to use. Allow an unlimited CPU time	MAXCPU TIME	2 147 483 647

The address space region size. Set to the size of the biggest address space.	MAXASSIZE	> 1 GB A minimum of 375 MB is required.
Specifies the maximum number of threads that a single process can have active. Depends on the definitions of message flows.	MAXTHREADS MAXTHREADTASKS	The value of MAXTHREADS and MAXTHREADTASKS depends on your application. You can calculate the value needed for WebSphere Event Broker as follows: For each message flow: <ol style="list-style-type: none"> 1. Multiply the number of input nodes by the number of instances (additional threads +1). 2. Sum the values of all message flows and add 10 to the resultant sum. 3. Add in the number of threads used for each HTTP listener.

Deploying a message flow, that starts an Execution Group in a new address space, uses USS Semaphore and SharedMemorySegment resources. In particular, each new address space uses a semaphore and SharedMemorySegment. The SharedMemorySegment is deleted immediately after the new address space has started, but the semaphore remains for the life of the new address space.

Certain USS system parameters can affect the start of a new Execution Group address space, if you set them incorrectly. These include:

- IPCSEMNIDS
- IPCSHMNIDS
- IPCSHMNSEGS

You need a minimum of three semaphores for each Execution Group address space started.

You must set IPCSEMNIDS to a value four times the number of potential Execution Group address spaces on a system.

You need one SharedMemorySegment for each Execution Group address space started. You must set IPCSEMNIDS to a value that exceeds the number of potential Execution Group address spaces on a system.

A control address space (BIPSERVICE and BIPBROKER processes) can be attached to many SharedMemorySegments - potentially, one for each Execution Group address space started for that broker. You must set IPCSHMNSEGS to a value that exceeds the potential number of Execution Groups for each broker.

Ensuring sufficient space for temporary files

The environment variable TMPDIR is the path name of the directory being used for temporary files. If it is not set, the z/OS shell uses /tmp.

When starting WebSphere Event Broker components, sufficient space is required in the directory referenced by TMPDIR. In particular, Java needs sufficient space to hold all JAR files required by WebSphere Event Broker.

If you do not allocate sufficient space, the execution group address spaces will abend with a 2C1 code.

Allow at least 50 MB of space in this directory for broker components and 10 MB of space for Configuration Manager components. More space might be needed if you deploy large user-defined nodes or other JARs to the broker component.

Defining WebSphere Event Broker files as shared-library programs

If you plan to deploy to more than one execution group on z/OS, the amount of storage required by the execution group address spaces can be reduced by setting the shared-library extended attribute on the following WebSphere Event Broker files:

```
/usr/lpp/mqsi/bin/*
/usr/lpp/mqsi/lib/*
/usr/lpp/mqsi/lib/wbirf/*
/usr/lpp/mqsi/lib/wbimb/*
/usr/lpp/mqsi/lib/wbieb/*
```

To set the shared-library attribute, use the `extattr` command with the `+l` option. For example:

```
extattr +l /usr/lpp/mqsi/bin/*
```

To find out if the shared-library extended attribute has been set, use the `ls -E` command.

Using `ls -E bipimain` results in, for example:

```
-rwxr-x--- a-s- 1 USER  GROUP  139264 Mar 15 10:05 bipimain
```

where `s` shows that the program is enabled to run in a shared address space.

Use the following command to see if you have enough `SHRLIBRGNSIZE` to contain all of the shared-library programs that are to be used on the system.

```
/D OMVS,LIMITS
```

DB2 planning on z/OS

This is part of the larger task of customizing your z/OS environment and is relevant only to the broker component. The Configuration Manager and User Name Server do not require access to DB2.

WebSphere Event Broker for z/OS accesses DB2 tables using ODBC. To connect to DB2 using ODBC, the location name of the DB2 subsystem is used. See the *DB2 UDB for OS/390® and z/OS V7 Data Sharing: Planning and Administration* manual for more details.

You need to give certain user IDs access to DB2 resources and these are summarized below:

- DB2 systems administrator
 1. Create database, storage groups and table spaces (BIPCRDB).

- 2. Drop database (BIPDLDB)
- Administrator for the broker database (DBA). This should be the WebSphere Event Broker administrator.
 - 1. Create tables and indexes (BIPCRBK)
 - 2. Create tables, drop tables and create indexes (BIPMGCMP)
- Broker started task user Id:
 - 1. SQL to select, insert, and delete rows from the broker database tables, and select from DB2 system tables.
- WebSphere Event Broker administrator and other users
 - 1. SQL to select, insert, and delete rows from the broker database tables, and select from DB2 system tables.

When your DB2 system starts up there should be a message DSNL004I DDF START COMPLETE. The location name is displayed just after this message. When you customize a broker component on z/OS you create a dsnaoini file called BIPDSNAO in the broker PDSE. It contains necessary information to establish the ODBC connection. See the *DB2 UDB for OS/390 and z/OS V7 ODBC Guide and Reference* manual for more details.

You should avoid using a data source name that is the same as the subsystem ID or data sharing ID. If the same name is used, this might affect the granularity of directives on connection with the database.

If you choose to use the same value for the data source name and subsystem ID, you must edit BIPDSNAO in the broker PDSE so that the Datasource and Subsystem keywords are in one section.

See the *DB2 UDB for OS/390 and z/OS V7 ODBC Guide and Reference* manual for more information on customizing this file.

During customization you can specify which plan name to use, or use the default DSNACLI. If you want your broker to access DB2 data-sharing groups other than its own, the DSNACLI plan must be bound in a special way. Check the wildcard location is specified by using SPUIFI and issuing the following command:

```
select * from SYSIBM.SYSPACKLIST where planname = 'DSNACLI';
```

You should rebind if the location column is blank and not '*'.

You should also check that DSNACLI is in the SYSIBM.SYSPLAN table.

You will get significant performance benefits from using the CACHE DYNAMIC SQL facility of DB2, because this eliminates the need to reprocess DB2 statements. See CACHEDYN=YES in the *DB2 UDB for OS/390 and z/OS V7 Installation Guide*.

If your user database is configured to use a comma as a decimal separator using the DSNHDECP module, you will find there is a restriction. If there is a mismatch between DB2 and the locale settings of the user ID under which the broker runs (specifically LC_NUMERIC), your user database updates can be unpredictable. LC_NUMERIC is set through the LC_ALL setting in the BIPBPROF member, and therefore the environment file. The following list details the four possibilities:

- If DB2 is configured to use a period as a decimal point and LC_NUMERIC is set to a value that indicates a period decimal point; user database updates should work correctly.

- If DB2 is configured to use a comma as a decimal point and LC_NUMERIC is set to a value that indicates a comma decimal point; user database updates should work correctly.
- If DB2 is configured to use a period as a decimal point and LC_NUMERIC is set to a value that indicates a comma decimal point; user database updates can lead to unpredictable behavior.
- If DB2 is configured to use a comma as a decimal point and LC_NUMERIC is set to a value that indicates a period decimal point; user database updates can lead to unpredictable behavior.

You can use the DB2 security mechanism, or if on z/OS 1.5 and DB2 Version 8 use an external security manager, for example, RACF.

DB2 security mechanism

The most practical way of managing access to a broker's DB2 resources is to define two RACF groups and connect users to these groups. For example, RACF groups MQP1ADM and MQP1USR are defined for broker MQP1BRK as follows:

- For group MQP1ADM
 1. Grant this group DBADM authority for the broker database.
 2. Typically owned by the WebSphere Event Broker administrator; user Ids must be added to this group who need to submit BIPCRBK to create a broker, or BIPMGCMP to migrate a broker.
- For group MQP1USR
 1. Give this group access to manipulate rows in the broker tables and allow select access to DB2 system tables. For example:

```
GRANT DELETE, INSERT, SELECT, UPDATE
  ON TABLE
    DB2_TABLE_OWNER.BSUBSCRIPTIONS
    ,DB2_TABLE_OWNER.BPUBLISHERS
    ,DB2_TABLE_OWNER.BCLIENTUSER
    ,DB2_TABLE_OWNER.BTOPOLOGY
    ,DB2_TABLE_OWNER.BNBRCONNECTIONS
    ,DB2_TABLE_OWNER.BRETAINEDPUBS
    ,DB2_TABLE_OWNER.BACLENTRIES
    ,DB2_TABLE_OWNER.BMQPSTOPOLOGY
    ,DB2_TABLE_OWNER.BUSERNAME
    ,DB2_TABLE_OWNER.BGROUPNAME
    ,DB2_TABLE_OWNER.BUSERMEMBERSHIP
    ,DB2_TABLE_OWNER.BROKERA
    ,DB2_TABLE_OWNER.BROKERAEG
    ,DB2_TABLE_OWNER.BROKERRESOURCES
    ,DB2_TABLE_OWNER.BRMINFO
    ,DB2_TABLE_OWNER.BRMRTDINFO
    ,DB2_TABLE_OWNER.BRMRTDDEPINFO
    ,DB2_TABLE_OWNER.BRMWFDINFO
    ,DB2_TABLE_OWNER.BRMPHYSICALRES
    ,DB2_TABLE_OWNER.BAGGREGATE
    ,DB2_TABLE_OWNER.BMULTICASTTOPICS
  TO MQP1USR;

GRANT SELECT
  ON TABLE
    SYSIBM.SYSTABLES
    ,SYSIBM.SYSSYNONYMS
    ,SYSIBM.SYSDATABASE
  TO MQP1USR;
```

2. Connect the broker started task user Id and the WebSphere Event Broker administrator to this group, and connect any other users who might need access to the tables, for example those submitting BIPRELG to run the mqsireadlog command.

Note the following:

- When accessing DB2 resources, you specify a CURRENT SQLID as a DB2 command, or through the BIPDSNA0 member.
If this Id is a group, then DB2 checks to see if your user Id is connected to this group, and if it is, you inherit the access from the group; if the user Id is not in the group, you get SQL code -551.
If your Id is in multiple groups, then the highest authorities are used.
- For BIPCRDB and BIPDLDB the CURRENT SQLID is specified as a command in the JCL. For all other JCL it is specified in BIPDSNA0.
- If you do not use groups to define permissions, but use a specific user Id to define the permissions to individual user Ids, then, if the granting user Id is removed from DB2 any permissions that it gave are also removed. This can prevent other users working.
- When the BIPDLDB job drops the broker DB2 database, it also deletes any Image Copy references to itself that you currently have. If you restore the broker in future you need to reinstate the Image Copy references.

If this Id is a group, then DB2 checks to see if your user Id is connected to this group, and if it is, you inherit the access from the group; if the user Id is not in the group, you get SQL code -551. If your Id is in multiple groups, then the highest authorities are used.

If you do not use groups to define permissions, but use a specific user ID to define the permissions to individual user Ids, then, if the granting user Id is removed from DB2 any permissions that it gave are also removed. This can prevent other users working.

See z/OS utility jobs for further information on the WebSphere Event Broker for z/OS jobs that are supplied.

WebSphere MQ planning for z/OS

This is part of the larger task of customizing your z/OS environment.

You are required to have a separate WebSphere MQ queue manager for each broker, User Name Server (although you would typically have only one User Name Server in your environment), and Configuration Manager. A broker, User Name Server, and Configuration Manager however, can share the same queue manager. All WebSphere Event Broker for z/OS system queues are defined during customization.

Your queue manager needs a dead-letter queue. Check this by using the WebSphere MQ command:

```
+cpf DIS QMGR DEADQ
```

Check the queue exists by using the command:

```
+cpf DIS QL(name) STGCLASS
```

Then use the:

```
+cpf DIS STGCLASS(...)
```

to check the STGCLASS value is valid. If the queue manager does not have a valid dead-letter queue, you must define one.

Set up your channel initiator to use distributed queuing. You need channels between the z/OS queue manager and the queue manager of your Configuration Manager (if not on z/OS). If you are using Publish/Subscribe security, you also need access to the queue manager used by the User Name Server, which can be on z/OS or on another platform. You should be able to successfully start channels between the various queue managers before you can test that the broker is working. When configuring the transmission queues between the brokers on z/OS and the Configuration Manager, ensure you set the maximum message size of the queues to 100 MB. This allows large reply messages concerning deployment to be returned to the Configuration Manager. See “Creating a domain connection” on page 172 for details.

Creating and deleting components on z/OS requires the command server on the WebSphere MQ queue manager to be started, which is normally done automatically (refer to the *WebSphere MQ for z/OS System Administration Guide* for more details).

This requires a reply-to queue based on SYSTEM.COMMAND.REPLY.MODEL; by default, this model queue is defined as permanent dynamic. However, if you leave the queue defined in this way, each time you run a create or delete component command these reply-to queues remain defined to the queue manager. To avoid this you can set the SYSTEM.COMMAND.REPLY.MODEL queue as temporary dynamic.

Resource Recovery Service planning on z/OS

This is part of the larger task of customizing your z/OS environment.

WebSphere Event Broker for z/OS uses Resource Recovery Service (RRS) to coordinate changes to WebSphere MQ and DB2 resources. Ensure it is configured and active on your system, because your broker cannot connect to DB2 unless RRS is active.

Refer to the following manuals for detailed information about RRS: *z/OS V1R5.0 MVS Setting Up a Sysplex* and *z/OS V1R5.0 MVS Programming: Resource Recovery SA22-7616*.

Defining the started tasks to z/OS Workload Manager (WLM)

This is part of the larger task of customizing your z/OS environment.

If you are running z/OS in Workload mode, change the classification rules to add the started task names of the brokers, User Name Server, and Configuration Manager to the Started Task Control (STC) subsystem types, for example MQP1BRK, MQP1UNS, and MQP1CMGR to the OMVS subsystem types.

If you are running in compatibility mode, add the broker and User Name Server address spaces to the IEAICSxx member in SYS1.PARMLIB. For example, for a broker MQP1BRK, use the commands:

```

SUBSYS=STC
..
TRXNAME=MQP1BRK,PGN=35,RPGN=2010
..
SUBSYS=OMVS
..
TRXNAME=MQP1BRK%(1),PGN=35,RPGN=2011
  ../ * Broker address spaces*/

```

The %(1) represents jobs beginning with MQP1BRK with one character following it. Define the priority of the broker lower than DB2 and WebSphere MQ.

Mounting file systems

For directories such as ++HOME++, ++COMPONENTDIRECTORY++, and ++INSTALL++ you must either create a directory, or mount a file system of this name, before using the directory.

To create a directory in an already mounted file system use the `mkdir` command. For example:

```
mkdir -p /mqsi/brokers/MQP1BRK
```

To mount a new file system, follow the instructions given in the *z/OS UNIX System Services Planning* manual.

From USS, use the following instruction:

```
mkdir -p /mqsi/brokers/MQP1BRK
```

From TSO, use the following instructions:

```

ALLOCATE DATASET('MQSI.BROKER.MQP1BRK') DSNTYPE(HFS) SPACE(5,5) DIR(1) CYL
FREE DATASET('MQSI.BROKER.MQP1BRK')
MOUNT FILESYSTEM('MQSI.BROKER.MQP1BRK') TYPE(HFS)
  MOUNTPOINT('/mqsi/brokers/MQP1BRK')

```

Note that the preceding `ALLOCATE` command is an example; the dataset should be allocated the correct amount of storage as described in “Disk space requirements on z/OS” on page 376

Checking the permission of the installation directory

This is part of the larger task of customizing your z/OS environment.

You must ensure that the appropriate user IDs, for example, the WebSphere Event Broker Administrator and any component Started Task user IDs have `READ` and `EXECUTE` permission to the WebSphere Event Broker installation directory.

You are recommended to set these permissions using the group access control.

1. Display the permissions on the installation directory using the `ls` command.

```
ls -l /usr/lpp/mqsi
```

This command displays lines similar to the following:

```
drwxr-xr-x  2 TSouser MQM      8192 Jun 17 09:54 bin
```

In this example, `MQM` is the group associated with the directory. Those user IDs requiring permission to the directory must be a member of this group.

This example also shows the permissions defined for the directory. User TS0USER has rwx (READ, WRITE and EXECUTE), group MQM has rx, and any other user ID has rx.

2. Ensure that the user IDs requiring permission have a group that matches that of the installation directory. Use the following command, where `userid` is the ID you want to check:

```
id <userid>
```

3. If the installation directory does not have a valid group, use the command `chgrp` to set the group of the directory:

```
chgrp -R <group> <pathname>
```

For example:

```
chgrp -R MQSI /usr/lpp/mqsi
```

You have to be the owner of the group or have superuser authority to use this command.

4. If the installation directory does not have the correct permissions for the group (READ / EXECUTE), use the command `chmod` to change the permissions:

```
chmod -R g=rx <pathname>
```

For example:

```
chmod -R g=rx /usr/lpp/mqsi
```

Checking the level of Java on z/OS

This is part of the larger task of customizing your z/OS environment.

To check your version of Java, enter `java -version` from an OMVS window. You obtain a response similar to the following:

```
java version "1.4.2"  
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2)  
Classic VM (build 1.4.2 J2RE 1.4.2 IBM z/OS Persistent Reusable VM build cm142-20040917  
(JIT enabled: jitc))
```

This indicates that the level of Java is 1.4.2, which is the minimum required level for this platform.

Checking APF attributes of bipimain on z/OS

This is part of the larger task of setting up your z/OS environment.

Use the `extattr` command to display the attributes of the object `bipimain`. For example:

```
extattr /usr/lpp/mqsi/bin/bipimain
```

It should show APF authorized = YES. If it does not, use `extattr +a bipimain` to set this attribute. For example:

```
extattr +a /usr/lpp/mqsi/bin/bipimain
```

Note that you need the appropriate authorization to issue this command.

Collecting broker statistics on z/OS

If you need to write broker statistics to SMF, you need to have the library <HLQ>.SBIPAUTH in your STEPLIB.

This library and all the libraries in the STEPLIB concatenation need to be APF authorized.

You can use the “mqsichange flowstats command” on page 260 with o=SMF for this purpose.

Configuring an execution group address space as non-swappable on z/OS

Because broker execution groups run as processes in UNIX System Services they cannot be set as NOSWAP in the PPT.

Instead, you can set the following environment variables in the broker environment file so that some, or all, of the address spaces of the broker execution groups request that they become non-swappable by the system; see “Creating the environment file” on page 120 for further information on adding an environment variable to a broker.

```
MQSI_NOSWAP=yes
```

sets the address spaces of all the execution groups to be non-swappable.

```
MQSI_NOSWAP_egname=yes
```

issues a request to the system, for each execution group labelled egname, that the address space be set as non-swappable.

```
MQSI_NOSWAP_uid=yes
```

issues a request to the system, for each execution group with the UUID labelled uuid, that the address space be set as non-swappable.

In order for the above requests to succeed, the broker’s started task ID needs READ access to the BPX.STOR.SWAP facility class through their external security manager, for example, RACF.

When an application makes an address space non-swappable, it can cause additional real storage in the system to be converted to preferred storage. Because preferred storage cannot be configured offline, using this service can reduce the installation’s ability to re-configure storage in the future.

Creating WebSphere Event Broker components on z/OS

This is an overview of how you create WebSphere Event Broker components on z/OS.

Before you start

Before starting this task, you must have installed:

- WebSphere MQ for z/OS, with the optional JMS feature applied; for example, mounted at /usr/lpp/mqm.

- WebSphere Event Broker for z/OS, with a broker file system mounted, for example, /usr/lpp/mqsi.

Note: If you want to connect a Message Brokers Toolkit directly to the Configuration Manager on z/OS, you *must* install the optional WebSphere MQ Client Attach feature.

If you do not have the WebSphere MQ Client Attach feature installed you can connect the Message Brokers Toolkit through an intermediate queue manager.

You should also read through all the sub topics in the “Customizing the z/OS environment” on page 60 section, and follow any recommendations within those topics.

1. Determine the customization information for your environment. The following list of topics contains tables of information that needs to be gathered before you can proceed with creating a broker domain on z/OS. Complete the information that your enterprise requires.

If necessary, discuss the requirements with your system, DB2, and WebSphere MQ administrators.

- Broker:

- “Installation information - broker and User Name Server” on page 117
- “DB2 information” on page 117
- “Component information - broker” on page 118

- Configuration Manager:

- “Installation information - Configuration Manager” on page 130
- “Component information - Configuration Manager” on page 131

- User Name Server:

- “Installation information - broker and User Name Server” on page 117
- “Component information - User Name Server” on page 140

2. Set up security for the started task user IDs. Start with “Setting up z/OS security” on page 28.
3. Plan your DB2 requirements; start with “DB2 planning on z/OS” on page 73
4. Create the broker by carrying out the tasks listed in “Creating a broker on z/OS” on page 116. Start at “Creating the broker PDSE” on page 118.
5. Create the Configuration Manager by carrying out the tasks listed in “Creating a Configuration Manager on z/OS” on page 130. Start at “Creating the Configuration Manager PDSE” on page 131
 - a. Set up the connections between the Message Brokers Toolkit and the Configuration Manager .
 - If you are using the WebSphere MQ Client Attach feature, see “Connecting directly to a Configuration Manager on z/OS” on page 82.
 - If you are connecting through an intermediate queue manager, see “Connecting to a z/OS Configuration Manager through an intermediate queue manager” on page 82.
6. Optionally, create the User Name Server by carrying out the tasks listed in “Creating a User Name Server on z/OS” on page 139. Start at “Creating the User Name Server PDSE” on page 141.

Connecting directly to a Configuration Manager on z/OS

Connection to the z/OS Configuration Manager directly, can be from:

- The Message Brokers Toolkit.
- A Configuration Manager Proxy (CMP) application.
- One of the WebSphere Event Broker commands used for the Configuration Manager, for example `mqsicreateexecutiongroup`.

All of these connect through the WebSphere MQ server connection channel, `SYSTEM.BKR.CONFIG`. You can connect directly to this channel only if you have the optional WebSphere MQ Client Attach feature installed.

An alternative is to connect through an intermediate queue manager; see “Connecting to a z/OS Configuration Manager through an intermediate queue manager.”

Before you start

Before starting this task, you must have set up your system components as described in “Creating WebSphere Event Broker components on z/OS” on page 80.

Set up the connections between the Message Brokers Toolkit and the Configuration Manager by carrying out the following tasks:

1. Verify that your queue manager and channel initiator are running and that the channel initiator is listening on the appropriate port.
For more information see your WebSphere MQ documentation.
2. Ensure that your Configuration Manager is running; see “Starting and stopping a Configuration Manager on z/OS” on page 217.
3. Ensure that your user ID has been given the appropriate authorization on the z/OS Configuration Manager.

In SDSF, grant FULL domain access to user Id `test1`. For all machines enter:

```
'/F WMQxCFG CA U=test1,A=YES,P=YES,X=F'
```

To grant access to a specific machine for user `test1`, enter:

```
'/F WMQxCFG CA U=test1,M=mymachine,P=YES,X=F'
```

4. Create a new domain connection; see “Creating a domain connection” on page 172.

Connecting to a z/OS Configuration Manager through an intermediate queue manager

This procedure enables you to connect a Message Brokers Toolkit to a z/OS Configuration Manager without the need for the WebSphere MQ Client Attach feature.

You do this by using an intermediate queue manager on another platform, for example, Windows.

When carrying out this task, see your WebSphere MQ documentation for more information.

Before you start

Before starting this task, you must have set up your system components as described in “Creating WebSphere Event Broker components on z/OS” on page 80

1. Set up the connections between the Message Brokers Toolkit and the Configuration Manager by carrying out the following tasks:
 - a. Verify that your queue manager and channel initiator are running and that the channel initiator is listening on the appropriate port.
For more information see your WebSphere MQ documentation.
 - b. Ensure that your user ID has been given the appropriate authorization on the z/OS Configuration Manager.
In SDSF, grant FULL domain access to user Id test1. For all machines enter:

```
'/F WMQxCFG CA U=test1,A=YES,P=YES,X=F'
```


To grant access to a specific machine for user test1, enter:

```
'/F WMQxCFG CA U=test1,M=mymachine,P=YES,X=F'
```
2. Connect the Windows queue manager to the z/OS queue manager using WebSphere MQ channels and a transmission queue. The connection must be bidirectional.
3. Ensure that you have started all the channels.
4. Create a server connection on the Windows queue manager called SYSTEM.BKR.CONFIG for the WebSphere Event Broker client connection. The Message Brokers Toolkit connects to a server connection of this name on the identified queue manager.
5. Start the Configuration Manager on z/OS; see “Starting and stopping a Configuration Manager on z/OS” on page 217.
6. Start the Message Brokers Toolkit on Windows.
7. Create a new domain connection ; see “Creating a domain connection” on page 172.
8. Enter the following connection parameters for the domain connection :
hostname = (windows machine name, for example, localhost)
port = (listener port for Windows queue manager, for example, 1414)
queue manager = (z/OS queue manager, for example, MQ05)
9. Right click on **Domain** and select **Connect** to connect the Message Brokers Toolkit to the z/OS Configuration Manager.

Configuring broker domain components

Before you start:

Ensure that the following requirements are met:

- Your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423.
- On Windows platforms, you have created a new user ID, the service user ID. This is specified during component creation and is used to run the component (the Configuration Manager, broker, and User Name Server).
- Refer to “Planning for security when you install WebSphere Event Broker” on page 11 for more information on user ID authorization and creation.
- You have initialized the command environment on distributed systems. See Setting up a command environment.

To create, modify, or delete a WebSphere Event Broker component:

- Select the task for the component and action that you require from the following list.
- Select the platform that you require from within the task.

or

- From within the Table of Contents, select the top-level container for the component and action that you require.
- Expand the container.
- Select the platform that you require from the list.

On Windows, you can create, modify, and delete physical components “Using the Command Assistant wizard” on page 151.

If you require a default broker domain configuration on Linux or Windows, you can use the Default Configuration wizard. The Default Configuration wizard creates all the components you need to start exploring WebSphere Event Broker and run the supplied samples. See “Using the Default Configuration wizard” on page 150.

When you have created your physical components you can configure the broker domain using either the workbench, or programmatically using the Configuration Manager Proxy Java API.

The following set of tasks describes creating and configuring component databases, and creating, modifying, and deleting the physical broker domain components and associated resources using the command line. For information on the using the Configuration Manager Proxy Java API, see Developing applications using the CMP.

This collection of tasks uses specific resource names, user IDs, and so on. These names are examples only; if you want to use your own names, make a note of the changes that you want to make, and remember to apply them. Follow existing naming conventions for WebSphere MQ and other resources.

- “Configuring component databases” on page 85
- “Creating a broker” on page 108
- “Adding an execution group to a broker using the command line” on page 123
- “Adding an execution group to a broker on z/OS” on page 124
- “Creating a Configuration Manager” on page 125
- “Enabling a User Name Server” on page 135
- “Creating a User Name Server” on page 136
- “Using the Default Configuration wizard” on page 150
- “Using the Command Assistant wizard” on page 151
- “Verifying components” on page 153
- “Connecting components” on page 153
- “Modifying a broker” on page 155
- “Modifying a Configuration Manager” on page 158
- “Modifying a User Name Server” on page 161
- “Modifying component database access” on page 164
- “Moving from WebSphere Event Broker on a distributed platform to z/OS” on page 164
- “Deleting a broker” on page 166

- “Deleting an execution group from a broker using the command line” on page 165
- “Deleting a Configuration Manager” on page 167
- “Disabling a User Name Server” on page 169
- “Deleting a User Name Server” on page 169

Configuring component databases

Review and complete these tasks to configure the databases required by your broker domain components:

- “Creating the databases”
- “Customizing DB2 databases” on page 92
- “Connecting to the databases” on page 92
- “Authorizing access to the databases” on page 106
- “Using retained publications with a Sybase database” on page 108

For information about setting up databases on z/OS, see “DB2 planning on z/OS” on page 73 and “Customizing the z/OS environment” on page 60.

Creating the databases

WebSphere Event Broker requires a database for each broker. This topic provides information about these databases and links to topics that tell you how to create them in your chosen database system.

On Windows, if you use the Default Configuration wizard, it automatically creates a broker database for the default broker, either in DB2 or in Derby. The following information also applies to databases created by the wizard.

The broker database

A broker stores configuration and control information in its database. You must define the database before you create the broker (because creating the broker creates tables within the specified database), and you must authorize access to the database for specific users. The broker database is also known as the broker’s local persistent store. Choose a unique name for the broker database, for example WBRKKBKDB, and keep a note of it for when you create the broker.

If you create a broker on Linux or UNIX, depending on your operating system, you can create the broker database in DB2, Oracle, or Sybase, or an SQL Server database on a Windows machine. On Windows, you can create the broker database in DB2, Oracle, Sybase, SQL Server, or Derby. See Supported databases to check which databases are supported on your operating system.

The Configuration Manager database

The Configuration Manager also stores configuration and control information in its database, which is known as the internal configuration repository. It is created and managed automatically by the Configuration Manager.

Database sharing

You can create a database for each broker, or you can use one database for multiple brokers if the platforms are compatible. The tables for each broker are identified with the broker name; these identifiers separate the data for each broker.

Database size

There is no fixed size requirement for the broker database; the size required depends on the complexity of your message flows. If you develop message flows that support many publishers or subscribers, you might need to increase your initial sizings.

Database schema

When you create a broker, the database tables required by that component are created in the default schema associated with the user ID used to access that database. You specify this user ID on the create command (`mqsicreatebroker`).

- For DB2 and Oracle, the default behavior is for the schema name to default to the user ID used to access the database.
- For Sybase and SQLServer, the typical behavior is to use the database owning schema (`dbo`).

WebSphere Event Broker does not require a particular schema or set of tablespaces; you can configure the database and access privileges of the user ID to choose your own values.

1. On UNIX systems, complete the setup procedures defined in “Preparing databases on UNIX systems” before you create the database. You do not have to complete this task if your database is on Windows or Linux.
2. Create the database. Instructions are provided for DB2 in “Creating a DB2 database on Windows” on page 87 and “Creating a DB2 database on Linux and UNIX systems” on page 88.

To create a Derby database, see the “`mqsicreatedb` command” on page 300. Derby database support is described in “Using Derby databases on Windows” on page 89.

For another database, refer to the documentation for that database. The commands that you can use in relation to databases are described in “Issuing database commands on Windows” on page 90.

3. If your database is DB2, customize it for WebSphere Event Broker use. Customization is described in “Customizing DB2 databases” on page 92.
4. Establish connections to the database. Refer to “Connecting to the databases” on page 92.
5. Authorize access to the database. This task is described in “Authorizing access to the databases” on page 106.

Preparing databases on UNIX systems:

If you are creating an Oracle database on a UNIX system, you must complete the following extra setup tasks before you create the database. You are recommended to complete this setup after you have installed your database, but you can complete it before database installation if you correctly specify the intended database installation directory during this setup.

Unless your database is Oracle, you do not have to complete this task..

Issue the following command:

```
mqsi_setupdatabase database_type <database_install_directory>
```

where `database_type` is `oracle9`, or `oracle10`, and `<database_install_directory>` is the directory in which the database is (or will be) installed.

You can now create the broker database. For DB2, see “Creating a DB2 database on Windows” or “Creating a DB2 database on Linux and UNIX systems” on page 88. For Oracle and Sybase, refer to the database product documentation for information about how to do this.

When you issue the command that creates the broker, tables are created within the database to hold the information required.

If you are creating a Sybase database for your broker, and you expect heavy use of retained publications with multiple topics, you are recommended to apply row-level locking to the retained publications table in the database. See “Using retained publications with a Sybase database” on page 108.

If you are using Sybase on AIX, ensure that you run the Sybase profile before the mqsiprofile.

Creating a DB2 database on Windows:

Use the **mqsicreatedb** command to create a DB2 or Derby database for the broker. Alternatively, you can use the DB2 Control Center to create a DB2 database. If you prefer, you can use any other method supported by DB2 (including command line or batch files); refer to the DB2 documentation for details of how to do this.

When you create a broker, you specify the user ID and password that are used to connect to the database. The user ID must be known to the database and must own the tables that are being accessed. When you create the database, ensure that you create them for the right user ID. DB2 authenticates the user ID using operating system user management, you do not have to define the user ID to DB2 itself.

1. If you want to create a database with the **mqsicreatedb** command, enter the command at the command line, specifying the appropriate parameters. You must provide a userID and password known to DB2. Indicate whether you want to create a DB2 database, or a Derby database. For more information about these and other parameters, refer to the **mqsicreatedb** command.
If you want to use the Control Center instead of the **mqsicreatedb** command, complete step 2.
2. Start the DB2 Control Center. For each database you want to create:
 - a. Expand All Systems in the object tree in the DB2 Control Center until you find Databases. Right-click Databases and click **Create Database** → **Standard**.
 - b. Enter a name and alias for your database. If you have a naming convention for databases, choose a compatible name. The alias name can be the same as the database name. Database names are limited to eight characters. For example, enter WBRKBKDB.
 - c. Click **Done**.
3. You must increase the database heap size to ensure it is sufficient for the broker. This task is described in “Customizing DB2 databases” on page 92.
4. When you have completed these steps for every database you have created, click **OK**.

If you use the DB2 command line to create the databases, you must bind the db2cli package to the database. You do not have to do this if you used the DB2 Control Center wizard, the **mqsicreatedb** command, or if you created the broker with the Default Configuration wizard.

1. Open a DB2 Command Line Processor window.

2. Connect to the broker database:
db2cmd db2 CONNECT to <YourBrokerDatabaseName>
3. Enter the following commands, where c:\ is the drive on which you installed DB2. You must enter your full DB2 installation path; do not use spaces or quotes.
db2 bind C:\SQLLIB\BND\@db2ubind.lst GRANT PUBLIC
db2 bind C:\SQLLIB\BND\@db2cli.lst GRANT PUBLIC
4. Repeat the previous two steps for every broker database.

Creating a DB2 database on Linux and UNIX systems:

When you create a broker, you specify the user ID and password that are used to connect to the broker database. The user ID must be known to the database and must own the tables that are being accessed. When you create the database, ensure that you create them for the right user ID. DB2 authenticates the user ID using operating system user management, you do not have to define the user ID to DB2 itself.

1. Logon as root.
2. Create a database instance. Use the commands shown here for guidance for the different platforms.

a. On AIX:

```
/usr/lpp/db2_08_01/instance/db2icrt -u fence_userID username
```

b. On Linux, Solaris, or HP-UX:

```
/opt/IBM/db2/V8.1/instance/db2icrt -u fence_userID username
```

The *username* that you specify on this command determines the nominated owner of the database instance. You are recommended to log on as this user whenever you perform any actions against the database instance (for example, creating or modifying a database). The command examples that are used in this help assume that you are logged on as *username*, and use the tilde (~) character to indicate this user ID in the DB2 commands issued.

If you are not logged on as the user that owns the database instance, you must modify the commands shown to specify explicit ownership by specifying the owner user ID *username* following the ~ character wherever it is used in the examples.

The *fence_userID* refers to the user ID under which stored procedures execute. You can specify a different ID to the instance owner ID for the database for extra security and protection, which is achieved because the stored procedure runs under a different ID, and therefore in a different process, to the database instance itself.

For further explanation of database ownership, refer to the DB2 library, accessible on the Web.

3. Logon as *username*
4. Create a database (in this example called WBRKBKDB) using the following commands (on some platforms, an explicit path name is required).

Note: You must insert a space between the starting period and the tilde character in the first command shown here:

```
. ~/sqllib/db2profile
db2start
db2 create database WBRKBKDB
db2 connect to WBRKBKDB
db2 bind ~/sqllib/bnd/@db2cli.lst grant public CLIPKG 5
```


5. You must increase the database heap size to ensure it is sufficient for the broker. This task is described in “Customizing DB2 databases” on page 92.

If you are using a 64-bit DB2 instance, ensure that you add <DB2 instance directory>/sql/lib/lib32 to the start of the library search path environment variable. If you are using a 64-bit Oracle instance, ensure that you add \$ORACLE_HOME/lib32 to the start of the library search path environment variable. If you are using 64-bit execution groups, ensure that you set the environment variable MQSI_LIBPATH64 to include the regular 64-bit database libraries.

When you issue the command that creates the broker, tables are created within the database to hold the information required.

Using Derby databases on Windows: Derby refers to IBM Cloudscape Version 10.0, a database product that is built on the Derby database from the Apache Software Foundation. Cloudscape does not modify Derby in any way, but provides additional function including installers. Derby database support is embedded in the broker component on Windows only.

This topic describes the processes, services, IP ports, and database files used to support Derby on Windows.

Security

With the current implementation of Derby in WebSphere Event Broker, no security controls are available, and no optimizations have been performed. For these reasons, it is strongly recommended that you do not use Derby in a production environment.

DB2 Run-Time Client use

WebSphere Event Broker uses ODBC to connect to Derby databases. Derby is a native Java database engine without ODBC support. The DB2 Run-Time Client provides the drivers that allow ODBC to access Derby databases. The DB2 Run-Time Client is used only for providing and managing the ODBC connection between WebSphere Event Broker and the Derby databases. It does not provide a DB2 database and therefore does not consume the resources that a full DB2 installation normally requires.

Database Instance Manager (managing, creating, deleting, and running databases)

A running network server is required for WebSphere Event Broker to be able to access Derby databases through ODBC. The network server provides access to Derby databases from external programs. When you create the first Derby database using the **mqsicreatedb** command, a Windows service is also created. The service is called IBM MQSeries Broker DatabaseInstanceMgr6 and starts automatically when Windows starts, under the user name that you supplied with the **mqsicreatedb** command. The service is referred to as DatabaseInstanceMgr component, and starts the network server. DbInstMgr is the internal component name of the Database Instance Manager.

All Derby databases that you create using the **mqsicreatedb** command are served by one instance of the DatabaseInstanceMgr and network server. Before the network server can function, it requires a TCP/IP port number. The default port number for Derby is 1527 (use this when creating the Derby database). You can

specify a different port number when you issue the **mqscreatedb** command to create a Derby database for the first time. However, you cannot subsequently change the port number after a network server has been set up, without first using **mqsdeletedb** to remove all Derby databases.

Issue the **mqsilist DatabaseInstanceMgr** command to produce a list all of the databases that have been created by the **mqscreatedb** command. You can remove the DatabaseInstanceMgr and the network server after the last Derby database has been deleted, using the **mqscreatedb** command. If the password of the user name under which the Windows service runs is changed, use the **mqsichangedbimgr** command to update the service with the new password. You can also use the **mqsichangedbimgr** command to change the user name of the service. Use the **mqsistart** and **mqsistop** commands to start and stop the DatabaseInstanceMgr component.

Multiplicity (brokers, dbiMgrs, installations, databases)

There is no limit to the number of databases that you can create with the **mqscreatedb** command. A maximum of one DatabaseInstanceMgr is created irrespective of how many databases have been created. If there are multiple simultaneous installations of WebSphere Event Broker Version 6.0, these use a single instance of the DatabaseInstanceMgr component.

Uninstall broker description, and considerations

Use the **mqsdeletedb** command to clear all resources created by the **mqscreatedb** command. When the last Derby database is deleted, the DatabaseInstanceMgr and network server are also stopped and removed. If the database files cannot be deleted using the **mqsdeletedb** command, it is possible to delete them manually.

Issuing database commands on Windows: On Windows, WebSphere Event Broker provides commands for creating and deleting databases for use by a broker, or by applications. Only DB2 and Derby databases are supported. The commands are:

- “mqscreatedb command” on page 300
- “mqsdeletedb command” on page 315
- “mqsichangedbimgr command” on page 259

The **mqsilist** command lists the databases that have been created using the **mqscreatedb** command. Only databases created using the **mqscreatedb** command can be deleted using the **mqsdeletedb** command.

The Default Configuration wizard and the Prepare Samples wizard use the **mqscreatedb** command to create the databases for the broker and the samples, using the default database engine. Therefore, you can list these databases using the **mqsilist DatabaseInstanceMgr** command.

The **mqssetdbparms** command is used to manage the access security for user databases only. It has no effect on Derby databases, which have no access security protection, nor on broker databases in general, which are governed by the access security settings in the broker itself. The rest of this page applies only to the **mqscreatedb**, **mqsdeletedb**, and **mqsichangedbimgr** commands.

Supported database engines

If DB2 version 8.1 Fix Pak 7 or later is installed, both DB2 and Derby databases can be created and used. If DB2 Run-time Client Version 8.2 is installed, only Derby databases are supported. If an earlier version of DB2 is installed, only DB2 databases can be created.

The `mqscreatedb` command has an option to select the database engine to use (either DB2 or Derby). The default for this option depends on which database engines are installed. If DB2 Run-time Client Version 8.2 is installed, the default is Derby, otherwise the default is DB2.

Database Instance manager

The databases that are created by `mqscreatedb` are managed by a component called the Database Instance manager. This component exists only on Windows. The component stores a list of all the databases created and which database engine is used for each database. Normally there is no process or Windows service required for the Database Instance manager component, and if you start the component it will not be recognized.

The first time a Derby database is created, a Windows service called IBM MQSeries Broker DatabaseInstanceMgr6 is created and started. This service is required in order to access Derby databases. This service can be started or stopped by the `mqsistart` and `mqsistop` commands, and automatically starts when Windows is started, if necessary. The service is deleted when the last Derby database is deleted. There is at most one Database Instance manager Windows service, even if you install WebSphere Event Broker Version 6.0 more than once on your Windows computer (multiple installed instances).

The database commands affect all the databases created in any installed instance on your Windows computer, regardless of the instance under which they are created. For example, the `mqsilist DatabaseInstanceMgr6` command lists all the databases that have been created using the `mqscreatedb` command on this Windows computer. The `mqsichangedbimgr` command is used to change the user name and password under which the Database Instance manager Windows service is run. This is required only if passwords change or if user names are updated after the initial installation and configuration. For more information, see "Using Derby databases on Windows" on page 89.

Creating and deleting databases

The command `mqscreatedb` is used to create databases for broker use or for application use. The Prepare Samples wizard and the Default Configuration wizard, for example, use the `mqscreatedb` command to create their databases on Windows. Not only is the database itself created (in either DB2 or Derby), but the ODBC data source name (DSN) is also created (with the same name).

Because the data source names and the instance manager component are system wide, you cannot create two databases with the same name, on the same Windows computer, even if they are for brokers on different installed instances of WebSphere Event Broker Version 6.0. The `mqscreatedb` command warns you if this is attempted. Any database created using the `mqscreatedb` command can be deleted by the `mqsdeletedb` command, even if that database is in use by a broker. See the links to the command descriptions for more information.

Customizing DB2 databases

If you create broker databases in DB2, you must ensure that the Database Heap Size is set to 900 (4 KB pages).

To change the Heap Size on Windows:

1. Start the DB2 Control Center.
2. For each database you have created:
 - a. Right-click the database name in the object tree and select **Configure Parameters**.
 - b. In the window that opens, select **Performance** → **DBHEAP**. You can reset this within the range 32 to 60000, but are recommended to choose a value of at least 900.
 - c. Click **OK**.

To change the Heap Size on UNIX platforms:

1. Open a command window.
2. Enter the db2 command with the parameters shown, specifying the number of pages required:

```
db2 update database configuration for WBRKBDDB using dbheap 900
```

Connecting to the databases

The broker uses ODBC to access its database so you must set up an ODBC data source name (DSN) definition on each broker system. At any one time there can be multiple connections using the same DSN definition.

For more information about the connections that a broker database needs, see “Broker database connections” on page 93.

If you are using the Default Configuration Wizard or the database commands to create a broker or a database on Windows, the ODBC DSNs are automatically created for you.

To define the DSN explicitly, click the appropriate links for your operating system and data source type:

- For Windows, follow the instructions in Defining an ODBC connection on Windows.

- For Linux and UNIX platforms:

- Set up the 32-bit ODBC data source to the broker database. This DSN is always required.

If you have 32-bit execution groups in the broker that access user databases, you must also set up 32-bit DNS for each of these databases.

This task is described in “Defining an ODBC connection to a 32-bit database on Linux and UNIX” on page 95.

- If you are using WebSphere MQ Version 6 and XA coordination, or if you have created 64-bit execution groups, you must also set up a 64-bit ODBC DSN for each database. This task is described in “Defining a connection to a 64-bit database on UNIX” on page 100.
- If you have defined 64-bit execution groups for a broker, you must define both 32-bit and 64-bit DSNs for the broker database.

When you have configured your ODBC data source names (DSN), you must also configure the environment for issuing console commands and for running the

broker so that it can access the required database libraries. For more information, see “Setting your environment to access databases” on page 106.

Broker database connections: The number of connections required by the broker to its database depend to some extent on the actions of the message flows it is processing. The following connections are required for each broker:

- Five by internal broker threads.
- One for each Publish/Subscribe neighbor, if the topology has been deployed.
- One for each message flow thread that contains a publication node.
- One for each message flow thread that parses MRM messages.
- A further number if you are using SCADA nodes with WebSphere MQ Everyplace. The exact number to add depends on whether thread pooling is being used (determined by the Use Thread Pooling property of the SCADAInput node):
 - If Use Thread Pooling is not selected (the default setting) add the number of SCADA clients that will connect to the SCADAInput node.
 - If Use Thread Pooling is selected, add the value in the Max Threads property of the SCADAInput node. The default value is 500.

If you are using the same database for several brokers, you must take account of all brokers in your calculations.

The connections for neighbors and publication nodes are only required if you are using retained publications.

When you start a broker, it opens all connections that it requires to the broker database for its own operation. When you stop the broker, it releases all current database connection handles.

If you are using DB2 for your database, the default action taken by DB2 is to limit the number of concurrent connections to a database to the value of the *maxappls* configuration parameter. The default for *maxappls* is 40. If you believe the connections that the broker might require exceed the value for *maxappls*, increase this and the associated parameter *maxagents* to new values based on your calculations.

Defining an ODBC connection to a database on Windows:

Configure an ODBC data source using the ODBC Data Source Administrator; click **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Data Sources (ODBC)**, then click the **System DSN** tab. When you define a new data source, select the appropriate driver for your database and complete the dialog that is displayed. Refer to your relevant database product documentation for more information.

Setup considerations specific to WebSphere Event Broker are described below for the supported databases.

DB2 UDB

When you define a data source for DB2 UDB you must choose the driver named IBM DB2 ODBC DRIVER. Enter the data source name (DSN) and description, and select the correct database alias from the drop-down list. You must register the data source as a system data source.

You might find it easier to use the Configuration Assistant:

1. Open the DB2 Configuration Assistant.

2. Right-click the database, and select **Change Database**.
3. Select **Data Source**.
4. Select **Register this database for ODBC** and select the system data source option.
5. Click **Finish**.
6. The **Test Connection** dialog opens automatically and you can test the various connections.

Informix Dynamic Server

When you define a data source for Informix Dynamic Server, choose the driver:

- IBM INFORMIX ODBC DRIVER

Complete these steps to configure the driver:

1. On the **Connection** tab, specify:
 - the Informix server name
 - the machine host name
 - the Informix network service name (as defined in the services file)
 - the network protocol (for example, olsotcp)
 - the Informix data source name
 - the user identifier to access the data source within
 - the password for that user identifier
2. Click **Apply**.
3. Click **Test Connection** to check your supplied values.
4. Click **OK** to finish.

Microsoft SQL Server

When you define a data source for Microsoft SQL Server you must choose the driver named SQL Server. The driver level must be Version 3.60 or later. Specify a name and description, and select the correct server from the drop-down list.

Oracle

When you define a data source for Oracle, choose the driver:

- MQSeries DataDirect Technologies 5.00 32-BIT Oracle

Complete these steps to configure the driver:

1. Enter the DSN name, description, and server name (where the server name is the "Service Name" that resolves to a "Connect Descriptor", for example through a mapping in the TSNames.ORA file).
2. Select the appropriate Oracle client version from the drop-down list.
3. Ensure that the **Enable SQLDescribeParam** box is checked. This parameter is on the **Advanced** tab of the driver settings.
4. Create a new registry subkey for each of your DSNs that reference an Oracle database. Use REGEDIT to navigate to the correct location:


```
HKEY_LOCAL_MACHINE
  SOFTWARE
    ODBC
      ODBC.INI
```
5. Right-click the DSN, and select **New** → **String Value**. Specify **WorkArrounds** for the string, and set the value to 536870912.

Sybase Adaptive Server Enterprise

When you define a data source for Sybase Adaptive Server Enterprise, choose the driver:

- MQSeries DataDirect Technologies 5.00 32-BIT Sybase Wire Protocol

Complete these steps to configure the driver:

1. Enter the DSN name, description, network address of the server (for a description of the format of this address, see the explanation for `NetworkAddress=` in “Editing the `.odbc.ini` parameters” on page 103).
2. Ensure the **Enable Describe Parameter** box is checked. This parameter is on the **Advanced** tab.
3. Ensure the **Prepare Method** setting is 1 - Partial. This parameter is on the **Performance** tab.
4. Create a new registry subkey for each of your DSNs that reference an Sybase database. Use REGEDIT to navigate to the correct location:

```
HKEY_LOCAL_MACHINE
  SOFTWARE
    ODBC
      ODBC.INI
```

5. Right-click the DSN, and select **New** → **String Value**. Specify **SelectUserName** for the string, and set the value to 1.

You have now configured your ODBC data source names on Windows. Next, you must configure the environment for issuing console commands, and for running the broker, so that it can access the required database libraries. For more information, see “Setting your environment to access databases” on page 106.

Defining an ODBC connection to a 32-bit database on Linux and UNIX:

In the Linux and UNIX environments, there is no ODBC Administrator or Driver Manager. To configure an ODBC data source name (DSN) definition for DataDirect, you must edit the required system information, which is held in a plain text file called `.odbc.ini` (note that the name of this file starts with a period).

Set the `ODBCINI` environment variable to point to the file, specifying a full path and file name. If you do not set this variable, the path defaults to `$MQSI_REGISTRY/odbc/.odbc.ini` for a 32-bit execution group, which is created when WebSphere Event Broker is installed. The file must have file permissions of `mqm:mqbrkrs`.

A sample template is provided in the file `install_dir/merant/odbc.ini` which contains examples of how to configure a DSN residing in each of the databases supported by WebSphere Event Broker. The example stanzas for the supported platforms are displayed below. The examples show the recommended configuration for the supported databases.

The entries in the stanzas that you must configure to match your local requirements are shown in italics (descriptions of these entries are provided in “Editing the `.odbc.ini` parameters” on page 103). You must retain all the entries shown, but you can remove a complete stanza if you do not require it for your configuration (for example, if you are using an Oracle database, you can remove the stanzas shown for DB2 and Sybase).

Ensure that the appropriate library search path environment variable is set to reflect the database products to be used. For example, the variable is `LD_LIBRARY_PATH` on Solaris and Linux (x86 platform). Refer to your database product documentation for more details.

If you are using Linux (zSeries platform) or Linux (POWER platform), you do not need to define an ODBC connection. Instead, the data source name used in the message flow is the same as the DB2 alias of the database.

If you have a 64-bit database package installed, or have created 64-bit execution groups:

- If you are using a 64-bit DB2 instance, ensure that you add *DB2 instance directory*/sql/lib/lib32 to the start of the library search path environment variable.

This addition might prevent you from running DB2 commands such as `db2create` from the command line in this environment shell. If you want to enter DB2 commands, start a separate environment shell and run `db2profile` for the relevant database instance, but do not run `mqsiprofile`.

- If you are using a 64-bit Oracle instance, ensure that you add `$ORACLE_HOME/lib32` to the start of the library search path environment variable.
- If you are using 64-bit execution groups, ensure that you set the environment variable `MQSI_LIBPATH64` to include the regular 64-bit database libraries.

If you are using WebSphere MQ Version 6, refer to the section 'Implications of a 64-bit queue manager' in the *WebSphere MQ Quick Beginnings* book for your operating environment.

On AIX, if you are using DB2 as your database, a maximum of 10 connections using shared memory are allowed from a single process. This means that if you deploy more than one or two message flows at the same time, you might see connection failures characterized by the DB2 error message `SQL1224N`. The connection errors are reported in the system log from the broker's execution group. To avoid this problem, you can use TCP/IP mode to connect to DB2. For detailed instructions on how to do this, see `DB2 error message SQL1224N` is issued when you connect to DB2.

Here is the sample `.odbc.ini` information:

AIX

```
[ODBC Data Sources]
WBRKBKDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
ORACLEDB=DataDirect 5.0 Oracle
SYBASEDB=DataDirect 5.0 Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 SQL Server Wire Protocol
INFORMIXDB=IBM Informix ODBC Driver

[WBRKBKDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.a
Description=WBRKBKDB DB2 ODBC Database
Database=WBRKBKDB

[MYDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.a
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your_install_directory>/merant/lib/UKor820.so
Description=DataDirect 5.0 Oracle
EnableDescribeParam=1
OptimizePrepare=1
ServerName=<Your Oracle host>
WorkArounds=536870912
ProcedureRetResults=1
```



```

[SYBASEDB]
Driver=<Your_install_directory>/merant/lib/UKase20.so
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your Database Name>
ServerName=<YourServerName>
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

[SQLSERVERDB]
Driver=<Your_install_directory>/merant/lib/UKmsss20.so
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your SQLServer Host>,<Your SQLServer server port>
Database=<Your Database Name>
AnsiNPW=Yes
QuoteId=No

[INFORMIXDB]
Driver=<Your Informix Client Directory>/lib/cli/iclit09b.so
Description=IBM Informix ODBC Driver
ServerName=<YourServerName>
Database=<Your Datasource>

[ODBC]
Trace=0
TraceFile=<A Directory with plenty of free space>/odbctrace.out
TraceDll=<Your_install_directory>/merant/lib/odbctrac.so
InstallDir=<Your_install_directory>/merant
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8

```

HP-UX

```

[ODBC Data Sources]
WBRKKBDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
ORACLEDB=DataDirect 5.0 Oracle
SYBASEDB=DataDirect 5.0 Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 SQL Server Wire Protocol
INFORMIXDB=IBM Informix ODBC Driver

[WBRKKBDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.s1
Description=WBRKKBDB DB2 ODBC Database
Database=WBRKKBDB

[MYDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.s1
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your_install_directory>/merant/lib/UKor820.s1
Description=DataDirect 5.0 Oracle
EnableDescribeParam=1
OptimizePrepare=1
ServerName=<Your Oracle Host>
WorkArrounds=536870912
ProcedureRetResults=1

[SYBASEDB]
Driver=<Your_install_directory>/merant/lib/UKase20.s1
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your Database Name>
ServerName=<YourServerName>
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

```

```

[SQLSERVERDB]
Driver=<Your_install_directory>/merant/lib/UKmsss20.sl
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your_SQLServer_host>,<Your_SQLServer_server_port>
AnsiNPW=Yes
Database=<Your_Database_Name>
QuoteId=No

[INFORMIXDB]
Driver=<Your_Informix_Client_Directory>/lib/cli/iclit09b.sl
Description=IBM Informix ODBC Driver
ServerName=<YourServerName>
Database=<Your_Datasource>

[ODBC]
Trace=0
TraceFile=<A_Directory_with_plenty_of_free_space>/odbctrace.out
TraceDll=<Your_install_directory>/merant/lib/odbctrac.sl
InstallDir=<Your_install_directory>/merant
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8

```

Linux (x86 platform)

```

[ODBC Data Sources]
WBRKBKDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
ORACLEDB=DataDirect 5.0 Oracle
SYBASEDB=DataDirect 5.0 Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 SQL Server Wire Protocol
INFORMIXDB=IBM Informix ODBC Driver

[WBRKBKDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.so
Description=WBRKBKDB DB2 ODBC Database
Database=WBRKBKDB

[MYDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.so
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your_install_directory>/merant/lib/UKor820.so
Description=DataDirect 5.0 Oracle
EnableDescribeParam=1
OptimizePrepare=1
ServerName=<Your_Oracle_Host>
WorkArounds=536870912
ProcedureRetResults=1

[SYBASEDB]
Driver=<Your_install_directory>/merant/lib/UKase20.so
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your_Database_Name>
ServerName=<YourServerName>
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

[SQLSERVERDB]
Driver=<Your_install_directory>/merant/lib/UKmsss20.so
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your_SQLServer_host>,<Your_SQLServer_server_port>
Database=<Your_Database_Name>
AnsiNPW=Yes
QuoteId=No

```

```

[INFORMIXDB]
Driver=<Your Informix Client Directory>/lib/cli/iclit09b.so
Description=IBM Informix ODBC Driver
ServerName=<YourServerName>
Database=<Your Datasource>

[ODBC]
Trace=0
TraceFile=<A Directory with plenty of free space>/odbctrace.out
TraceDll=<Your_install_directory>/merant/lib/odbctrac.so
InstallDir=<Your_install_directory>/merant
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8

```

Solaris (SPARC platform) and Solaris (x86-64 platform)

```

[ODBC Data Sources]
WBRKBDDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
ORACLEDB=DataDirect 5.0 Oracle
SYBASEDB=DataDirect 5.0 Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 SQL Server Wire Protocol
INFORMIXDB=IBM Informix ODBC Driver

[WBRKBDDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.so
Description=WBRKBDDB DB2 ODBC Database
Database=WBRKBDDB

[MYDB]
Driver=<Your_DB2_installation_directory>/lib/libdb2.so
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your_install_directory>/merant/lib/UKor820.so
Description=DataDirect 5.0 Oracle
EnableDescribeParam=1
ProcedureRetResults=1
ServerName=<Your Oracle Host>
WorkArounds=536870912
OptimizePrepare=1

[SYBASEDB]
Driver=<Your_install_directory>/merant/lib/UKase20.so
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your Database Name>
ServerName=<YourServerName>
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

[SQLSERVERDB]
Driver=<Your_install_directory>/merant/lib/UKmsss20.so
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your SQLServer host>,<Your SQLServer server port>
AnsiNPW=Yes
Database=<Your Database Name>
QuoteId=No

[INFORMIXDB]
Driver=<Your Informix Client Directory>/lib/cli/iclit09b.so
Description=IBM Informix ODBC Driver
ServerName=<YourServerName>
Database=<Your Datasource>

[ODBC]
Trace=0
TraceFile=<A Directory with plenty of free space>/odbctrace.out
TraceDll=<Your_install_directory>/merant/lib/odbctrac.so

```

```
InstallDir=<Your_install_directory>/merant
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8
```

You have now configured your 32-bit ODBC data source names on UNIX. Next, you must configure the environment for issuing console commands, and for running the broker, so that it can access the required database libraries. For more information, see “Setting your environment to access databases” on page 106.

Defining a connection to a 64-bit database on UNIX:

If you are using WebSphere MQ Version 6 and XA coordination, or if you have created 64-bit execution groups, you need to configure a 64-bit ODBC data source name (DSN). Ensure that you set the environment variable MQSI_LIBPATH64 to include the regular 64-bit database libraries. For example, if you are using a 64-bit DB2 instance, ensure that you add *DB2_instance_directory/sqlib/lib64* to the start of the library search path environment variable.

The XA-coordinated databases must appear in the ODBCINI64 stanza file so that WebSphere MQ can perform the XA coordination. WebSphere MQ Version 6 supports a 64-bit environment.

In the UNIX environment, there is no ODBC Administrator or Driver Manager. To configure an ODBC DSN definition, you must edit the required system information, which is held in a plain text file called *odbc64.ini*.

If you are using Linux (zSeries platform) or Linux (POWER platform), you do not need to define an ODBC connection. Instead, the data source name used in the message flow is the same as the DB2 alias of the database.

For the UNIX platforms, set the ODBCINI64 environment variable to point to the file, specifying a full path and file name. If you do not set this variable, the path defaults to *\$MQSI_REGISTRY/odbc/odbc64.ini*. You must copy your *odbc64.ini* file to this directory and set file ownership to *mqm:mqbrkrs*.

A sample template is provided in the file *install_dir/DD64/odbc64.ini* which contains examples of how to configure a DSN residing in each of the databases supported by WebSphere Event Broker. The example stanzas for the supported platforms are displayed below. The examples show the recommended configuration for the supported databases.

The entries in the stanzas that you must configure to match your local requirements are shown in italics (descriptions of these entries are provided in “Editing the *odbc64.ini* parameters” on page 105). You must retain all the entries shown, but you can remove a complete stanza if you do not require it for your configuration (for example, if you are using an Oracle database, you can remove the stanzas shown for DB2 and Sybase).

Make a copy of the default file, set ODBCINI64 to point to this copy, and make any changes to the copied file rather than to the default.

Ensure that the appropriate library search path environment variable (for example, *LD_LIBRARY_PATH* on Solaris) is set to reflect the database products to be used. Refer to your database product documentation for more details.

On AIX, if you are using DB2 as your database, a maximum of 10 connections using shared memory are allowed from a single process. This means that if you deploy more than one or two message flows at the same time, you might see connection failures characterized by the DB2 error message SQL1224N. The connection errors are reported in the system log from the broker's execution group. To avoid this problem, you can use TCP/IP mode to connect to DB2. For detailed instructions on how to do this, see DB2 error message SQL1224N is issued when you connect to DB2.

Here is the sample odbc64.ini information:

AIX

```
[ODBC Data Sources]
WBRKKBDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
ORACLEDB=DataDirect 5.0 64bit Oracle Wire Protocol
SYBASEDB=DataDirect 5.0 64bit Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 64bit SQL Server Wire Protocol

[WBRKKBDB]
Driver=libdb2Wrapper64.so
Description=WBRKKBDB DB2 ODBC Database
Database=WBRKKBDB

[MYDB]
Driver=libdb2Wrapper64.so
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your install directory>/DD64/lib/UKora20.so
Description=DataDirect 5.0 Oracle Wire Protocol
HostName=<Your Oracle Server Machine Name>
PortNumber=<Port on which Oracle is listening on HostName>
SID=<Your Oracle SID>
CatalogOptions=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
EnableDescribeParam=1
OptimizePrepare=1
WorkArounds=536870912
ProcedureRetResults=1

[SYBASEDB]
Driver=<Your install directory>/DD64/lib/UKase20.so
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your Database Name>
ApplicationsUsingThreads=1
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

[SQLSERVERDB]
Driver=<Your install directory>/DD64/lib/UKmsss20.so
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your SQLServer host>,<your SQLServer server port>
AnsiNPW=Yes
Database=<Your Database Name>
QuoteId=No

[ODBC]
Trace=0
TraceFile=<A Directory with plenty of free space>/odbctrace.out
TraceDll=<Your install directory>/DD64/lib/odbctrac.so
```

```
InstallDir=<Your install directory>/DD64
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8
```

HP-UX

```
[ODBC Data Sources]
WBRKKBDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
ORACLEDB=DataDirect 5.0 64bit Oracle Wire Protocol
SYBASEDB=DataDirect 5.0 64bit Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 64bit SQL Server Wire Protocol

[WBRKKBDB]
Driver=libdb2Wrapper64.s1
Description=WBRKKBDB DB2 ODBC Database
Database=WBRKKBDB

[MYDB]
Driver=libdb2Wrapper64.s1
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your install directory>/DD64/lib/UKora20.s1
Description=DataDirect 5.0 Oracle Wire Protocol
HostName=<Your Oracle Server Machine Name
PortNumber=<Port on which Oracle is listening on HostName
SID=<Your Oracle SID>
CatalogOptions=0
ProcedureRetResults=1
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
EnableDescribeParam=1
OptimizePrepare=1
WorkArounds=536870912

[SYBASEDB]
Driver=<Your install directory>/DD64/lib/UKase20.s1
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your Database Name>
ApplicationUsingThreads=1
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

[SQLSERVERDB]
Driver=<Your install directory>/DD64/lib/UKmsss20.s1
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your SQLServer host>,<your SQLServer server port>
AnsiNPW=Yes
Database=<Your Database Name>
QuoteId=No

[ODBC]
Trace=0
TraceFile=<A Directory with plenty of free space>/odbctrace.out
TraceDll=<Your install directory>/DD64/lib/odbctrac.s1
InstallDir=<Your install directory>/DD64
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8
```

Solaris (SPARC platform)

```
[ODBC Data Sources]
WBRKKBDB=IBM DB2 ODBC Driver
MYDB=IBM DB2 ODBC Driver
```

```

ORACLEDB=DataDirect 5.0 64bit Oracle Wire Protocol
SYBASEDB=DataDirect 5.0 64bit Sybase Wire Protocol
SQLSERVERDB=DataDirect 5.0 64bit SQL Server Wire Protocol

[WRKKBKDB]
Driver=libdb2Wrapper64.so
Description=WRKKBKDB DB2 ODBC Database
Database=WRKKBKDB

[MYDB]
Driver=libdb2Wrapper64.so
Description=MYDB DB2 ODBC Database
Database=MYDB

[ORACLEDB]
Driver=<Your install directory>/DD64/lib/UKor820.so
Description=DataDirect 5.0 Oracle Wire Protocol
HostName=<Your Oracle Server Machine Name>
PortNumber=<Port on which Oracle is listening on HostName>
SID=<Your Oracle SID>
CatalogOptions=0
ProcedureRetResults=1
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
EnableDescribeParam=1
OptimizePrepare=1
WorkArounds=536870912

[SYBASEDB]
Driver=<Your install directory>/DD64/lib/UKase20.so
Description=DataDirect 5.0 Sybase Wire Protocol
Database=<Your Database Name>
ServerName=<YourServerName>
ApplicationUsingThreads=1
EnableDescribeParam=1
OptimizePrepare=1
SelectMethod=0
NetworkAddress=<YourServerName>,<YourPortNumber>
SelectUserName=1

[SQLSERVERDB]
Driver=<Your install directory>/DD64/lib/UKmsss20.so
Description=DataDirect 5.0 SQL Server Wire Protocol
Address=<Your SQLServer host>,<your SQLServer server port>
AnsiNPW=Yes
Database=<Your Database Name>
QuoteId=No

[ODBC]
Trace=0
TraceFile=<A Directory with plenty of free space>/odbctrace.out
TraceDll=<Your install directory>/DD64/lib/odbctrac.so
InstallDir=<Your install directory>/DD64
UseCursorLib=0
IANAAppCodePage=4
UNICODE=UTF-8

```

You have now configured your 64-bit ODBC data source names on UNIX. Next, you must configure the environment for issuing console commands, and for running the broker, so that it can access the required database libraries. For more information, see “Setting your environment to access databases” on page 106.

Editing the .odbc.ini parameters:

Configure the template files by updating the following list of configurable parameters. Some parameters are not applicable to all databases, as shown.

[ODBC Data Sources]

This stanza describes the data source names (DSNs) for the databases that

are configured in the `.odbc.ini` file. You must configure this stanza to show all your databases, and you must include a stanza for each one.

Address (SQL Server wire protocol definitions)

Specify the network address of your server (this is required for local and remote databases). Specify an IP address as follows:

`<servername or IP address>, <portnumber>`

Driver

- If you are using DB2, specify the location of the 32-bit driver library that matches your DB2 installation.
- If you are using any other database, add your installation directory structure to complete the fully qualified path to the driver shown.

Description

You can change this if you choose. This is a text field for information only and has no bearing on operation.

Database (DB2, Sybase, SQL Server accessed from UNIX, Informix)

- If you are using DB2, specify the database alias. The data source name must be the same as the database alias name. If you are using a remote DB2 database, you must set up your client-server connection to resolve this alias to the correct database. For more information, see the DB2 documentation.
- If you are using Sybase or SQL Server accessed from UNIX, specify the name of the database to which you want to connect by default. If you do not specify a value, the default is the database defined by your system administrator for each user.
- If you are using Informix, specify the name of the database on the IDS server.

NetworkAddress (Sybase only)

Specify the network address of your Sybase server (this is required for local and remote databases). Specify an IP address as follows:

`<servername or IP address>, <portnumber>`

For example `Sybaseserver, 5000`. You can also specify the IP address directly, for example `199.226.224.34, 5000`. You can find the port number in the Sybase interfaces file which is typically named `interfaces`, `interfac`, or `sql.ini`, depending on the operating system.

ServerName (Sybase, Oracle, Informix)

- If you are using Oracle, specify the "Service Name" that resolves to a "Connect Descriptor", for example through a mapping in the `TSNAMES.ORA` file. This is applicable only to the 32-bit client driver.
- If you are using Sybase, specify the name of the Sybase database server that you have defined on the server computer.
- If you are using Informix, specify the name of the Informix IDS server.

Trace This value controls whether the DataDirect ODBC trace is turned on or off. To start trace, set the value to 1; to stop trace, set the value to 0.

TraceFile

This value shows the path and the name of the trace file to which the ODBC trace is written. Trace files can become quite large; specify a directory with plenty of free disk space.

TraceDll

Add your installation directory structure to complete the fully qualified path to the ODBC trace DLL.

InstallDir

Add your installation directory structure to complete the fully qualified path to the ODBC trace directory.

Editing the odbc64.ini parameters:

Configure the template files by updating the following list of configurable parameters. Some parameters are not applicable to all databases, as shown.

[ODBC Data Sources]

This stanza describes the data source names (DSNs) for the databases that are configured in the `odbc64.ini` file. You must configure this stanza to show all your databases, and you must include a stanza for each one.

Driver

- If you are using DB2, use the value exactly as shown.
- If you are using any other database, add your installation directory structure to complete the fully qualified path to the driver shown.

Description

You can change this if you choose. This is a text field for information only and has no bearing on operation.

Database (DB2, Sybase, SQL Server accessed from UNIX)

- If you are using DB2, specify the database alias. The data source name must be the same as the database alias name. If you are using a remote DB2 database, you must set up your client-server connection to resolve this alias to the correct database. For more information, see the DB2 documentation.
- If you are using Sybase or SQL Server accessed from UNIX, specify the name of the database to which you want to connect by default. If you do not specify a value, the default is the database defined by your system administrator for each user.

HostName (Oracle 64-bit wire protocol)

Specify the IP address on which the Oracle database is running.

NetworkAddress (Sybase only)

Specify the network address of your Sybase server (this is required for local and remote databases). Specify an IP address as follows:

<servername or IP address>, <portnumber>

For example `Sybaseserver, 5000`. You can also specify the IP address directly, for example `199.226.224.34, 5000`. You can find the port number in the Sybase interfaces file which is typically named `interfaces`, `interfac`, or `sql.ini`, depending on the operating system.

Address (SQL Server wire protocol definitions)

Specify the network address of your server (this is required for local and remote databases). Specify an IP address as follows:

<servername or IP address>, <portnumber>

PortNumber (Oracle 64-bit wire protocol)

Specify the port number on which the Oracle database is running.

ServerName (Sybase)

- If you are using Sybase, specify the name of the Sybase database server that you have defined on the server computer.

SID (Oracle 64-bit wire protocol)

Specify the Oracle System Identifier of the database on that server.

TraceFile

This value shows the fully qualified path and file name of the trace file to which the ODBC trace is written. Trace files can become quite large so specify a directory with plenty of free disk space.

TraceDll

Add your installation directory path to complete the fully qualified path to the ODBC trace library.

InstallDir

Add your installation directory path to complete the fully qualified path to the database drivers directory.

Setting your environment to access databases:

When you have configured your ODBC data source names, you must also configure the environment for issuing console commands, and for running the broker, so that it can access the required database libraries. For example, if you have a DB2 broker database, you must add the DB2 client libraries to your library search path.

On Windows platforms, this is likely to have been done for you when you installed the database product. On UNIX systems, and Linux, you need to run a profile for each database you need to access. For example, on DB2 you must run `db2profile`; other database vendors have similar profiles.

If you are using a 64-bit DB2 instance, ensure that you add `<DB2 instance directory>/sql1lib/lib32` to the start of the library search path environment variable after running `db2profile`. If you are using a 64-bit Oracle instance, ensure that you add `$ORACLE_HOME/lib32` to the start of the library search path environment variable. If you are using 64-bit execution groups, ensure that you set the environment variable `MQSI_LIBPATH64` to include the regular 64-bit database libraries.

Additionally, ensure that you access the correct set of libraries (32-bit) because this might not be the default.

If you are using WebSphere MQ Version 6, refer to the section 'Implications of a 64-bit queue manager' in *WebSphere MQ Quick Beginnings* for your operating environment.

Authorizing access to the databases

When you have created a broker database, you must authorize the owning component to access it. When you invoke the `mqsicreatebroker` command, you must specify at least one ID for runtime authorization; you can specify a second ID specifically for database connect authorization. If you do not specify the second ID, the component uses its runtime ID (the service user ID) for database access as well.

You specify the service user ID and its password with the `-i` and `-a` flags, and the optional database connection ID and password with the `-u` and `-p` flags.

The way that you authorize access depends on the database you are using, and the platform on which you have created it.

DB2 authorization:

To authorize access to a DB2 database on Windows:

1. Start the DB2 Control Center, if it is not already active.
2. Expand the object tree until you find the database you created for the broker.
3. Expand the tree under this database and select the **User and Group Objects** folder. The **DB Users** and **DB Groups** folders are displayed in the right pane.
4. Right-click the **DB Users** folder in the right pane and select **Add**. The Add User notebook opens.
5. Select the user ID you want to authorize to access the database (for example, `mqsuid`) from the drop-down list. The ID you select must be the user ID that you specify to be used for database access when you create the broker. The drop-down list contains all user IDs that are defined to Windows. If you cannot see the user ID you specified in the command, you must define it before you can give it authority.
6. Select the appropriate options from the choices in the box labelled **Choose the appropriate authorities to grant to the selected user** for the database. These are:
 - Connect database
 - Create tables
 - Create packages
 - Register functions to execute in database manager's process
7. Click **OK**. The authorities are granted. The dialog closes.
8. Close the DB2 Control Center.

If you prefer, you can use the command line commands shown below for UNIX platforms (for a broker database); the commands are the same on Windows.

To authorize access to a DB2 database on Linux and UNIX:

1. Connect to the database with a user ID that has DB2 system administration (SYSADM or DBADM) authority (substitute the correct database and ID in this command):
2. Issue the following command to grant the required privileges to the user ID that the broker will use to connect to the database (substitute the correct ID for your broker in this command if you are not using the sample `mqsuid`):

```
db2 grant connect, createtab, bindadd, create_external_routine on database to user mqsuid
```

If you need further guidance about any of these tasks, use the online help facility of the DB2 Control Center. Your database administrator might also be able to offer advice and assistance.

Oracle authorization:

To authorize access to an Oracle database:

1. Logon to the database using SQL*Plus as the Oracle DBA (database administrator).
2. Modify the privileges of the user ID that you have specified for database connection to ensure that the broker can successfully access the database. The

user ID needs quota in its tablespaces and sufficient privilege to allow the creation of, and updates to, the broker tables:

```
GRANT CREATE SESSION TO dbid;  
GRANT CREATE TABLE TO dbid;
```

For further information, refer to the Oracle documentation, or consult your database administrator.

Using retained publications with a Sybase database

If you have created a broker that uses a Sybase database, and you expect extensive use of retained publications with multiple topics, you are recommended to apply row-level locking to the retained publications table in the database. If you do not plan to use retained publications, or expect their use to be infrequent, you do not have to make this change.

If you do not apply row-level locking, and your use of retained publications is too great, the broker will experience deadlock problems.

To apply row-level locking:

1. At a command prompt enter the following command:

```
isql -Umqsiuid -Pmqsipw
```

If you have authorized another user ID and password for broker access to this database, substitute your values for `mqsiuid` and `mqsipw` in that command.

2. Connect to the broker database with this command:

```
use WBRKBKDB
```

If you have created your broker database with a different name, substitute your name for `WBRKBKDB` in that command.

3. Update the retained publications table to use row-level locking with this command:

```
alter table mqsiuid.BRETAINEDPUBS lock datarows
```

If the owner of this database instance is not `mqsiuid`, substitute the correct schema name in that command.

4. Apply the change with this command:

```
go
```

You can check that the change has been successfully applied by entering the commands:

```
sp_help BRETAINEDPUBS  
go
```

The locking scheme is displayed: `lock scheme datarows`.

If the change has **not** completed, it is displayed as: `lock scheme allpages`.

Creating a broker

Before you start:

You must complete the following tasks:

- Ensure that your ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423.

- For platforms other than z/OS, see “Considering security for a broker” on page 15 for information about security matters relevant to a broker during the configuration task.
- Create and configure the broker database. Configure ODBC to allow the broker to access its database. Refer to “Configuring component databases” on page 85 for information on all these tasks.
- Create a new user ID to access the broker database tables (persistent store).
- If you want to configure a broker on Windows, UNIX systems, or Linux as a WebSphere MQ trusted application, refer to “Using WebSphere MQ trusted applications” before creating the broker. Using trusted (fastpath) applications allows the broker and the WebSphere MQ queue manager agent to run in the same process, thus improving overall performance.
- If you want to add a User Name Server to your broker domain, create the broker with the additional `-s` and `-j` parameters on the **mqsicreatebroker** command. These parameters allow the broker to communicate with the User Name Server. See “Enabling a User Name Server” on page 135 for details of the parameters to specify.
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before creating a broker, by running the product profile or console; refer to Setting up a command environment.
- On Windows, UNIX systems, and Linux, you must set up any required database profiles, for example, running `db2profile` for DB2.

Create a broker using the command line on the system where the broker component is installed. On Windows, you can also use the Command Assistant to complete this task.

The broker must be given a name that is unique within the broker domain. Broker names are case-sensitive on all supported platforms, except the Windows platforms. The broker’s name and its queue manager name are required when creating the broker reference in the workbench.

To create a broker, follow the link for the appropriate platform:

- AIX
- HP-UX
- Linux
- Solaris
- Windows
- z/OS

Using WebSphere MQ trusted applications

Before you start:

You must complete the following tasks:

- Ensure that your user ID is a member of the **mqm** group. On HP-UX and Solaris, specify the user ID **mqm** as the service user ID when you create the broker. On Windows, use any service user ID that is a member of **mqm**. Refer to “Security requirements for administrative tasks” on page 423.
- Review the restrictions that WebSphere MQ places on trusted applications that apply to your environment. See the section “Connection to a queue manager using the MQCONN call” in the *WebSphere MQ Application Programming Guide*, available on the WebSphere MQ library Web page.

You can configure a broker to run as a trusted (fastpath) application on all supported platforms, with the exception of z/OS where the option is not applicable. If the broker is configured as a trusted application, it runs in the same process as the WebSphere MQ queue manager agent, and all broker processes benefit from an improvement in the overall system performance.

A broker does not run as a trusted application by default; you either create a trusted application using the “**mqsicreatebroker command**” on page 286, or modify an existing broker using the “**mqsichangebroker command**” on page 250.

Configuring a broker as a trusted application does not affect the operation of WebSphere MQ channel agents or listeners. For more information about running these as trusted applications, see the section “Running channels and listeners as trusted applications” in *WebSphere MQ Intercommunication*, available on the WebSphere MQ library Web page.

Take care when deploying user-defined nodes or parsers. Because a trusted application (the broker) runs in the same operating system process as the queue manager, a user-defined node or parser might compromise the integrity of the queue manager. Consider fully the restrictions that apply to your environment and test user-defined nodes and parsers in a non-trusted environment before deploying them in a trusted broker.

You can either configure a new broker to run as a trusted application, or modify an existing broker.

- To configure a new broker, on a command line run the **mqsicreatebroker** command with the **-t** flag,, which specifies that the broker is created as a trusted application.

For example, enter the following command to create a broker called **WBRK_BROKER** as a trusted application:

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw  
-q WBRK_QM -n WBRKBKDB -u wbrkuid -p wbrkpw -t
```

Refer to “Creating a broker” on page 108 for more detailed information about how to create a broker for your platform.

- To modify an existing broker:
 1. Run the **mqsistop** command on the command line to stop the broker.
 2. Run the **mqsichangebroker** command with the **-t** flag. For example, enter the following command to modify a broker called **WBRK_BROKER** to run as a trusted application:

```
mqsichangebroker WBRK_BROKER -t
```

You might need to change the service user ID and password if you did not originally create the broker to use an appropriate service user ID.

Refer to “Modifying a broker” on page 155 for more detailed information on how to modify a broker for your platform.

3. Restart the broker using the **mqsistart** command. The broker restarts with fastpath set.

Creating a broker on AIX

If you expect your broker to handle a heavy load (running a large number of message flows, or interacting with a number of databases), it might exceed the default memory limits that you configured during AIX installation. If the broker experiences memory problems, check the maximum size of the data segment for

the user under which your broker is running (the ServiceUserID), and consider increasing its value. The size is defined in /etc/security/limits.

To create a broker:

1. Log on using your service user ID. If you use the su command to switch user you must ensure that you invoke that user's profile.
 - a. Enter su - <user ID> to run a different user's profile.
2. Run '. <install_dir>/bin/mqsiprofile' to source the mqsiprofile script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
3. Ensure that the broker database instance profile has been run. Invoke the SQL profile that was created when the broker database was created.
4. Enter the following command to create the broker:

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw  
-q WBRK_QM -n WBRKKBDB -u dbuid -p dbpw
```

If you are using different names or values for any parameter on this command, you **must** replace the appropriate values with your own.

In the command above:

WBRK_BROKER

Is the broker name.

wbrkuid

Is the service user ID that is used to run the broker.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that the broker will use. This queue manager is created if it does not exist.

WBRKKBDB

Is the name of the existing broker database, the broker tables will be created within this database.

dbuid Is the user ID that has read, write and create access permissions for the database. This is the user ID that will be used to read and update the broker's persistent store.

dbpw Is the password that is associated with the database user ID, dbuid.

On completion of this task, you have:

- Created a broker called WBRK_BROKER.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the broker, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqsicreatebroker** command.

Note: Note that this command does **not** start the listener

- Ensured that all database tables required by the broker have been created in the database WBRKKBDB.

Now that you have created a physical broker, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.
2. Add the broker to the broker domain.
 - To add the broker using the workbench, see “Adding a broker to a broker domain” on page 175.
 - To add the broker using the Configuration Manager Proxy Java API, see Creating domain objects using the Configuration Manager Proxy

Creating a broker on HP-UX

To create a broker:

1. Log on using your service user ID. If you use the su command to switch user ensure that you invoke that user’s profile.
 - a. Enter su - <user ID> to run a different user’s profile.
2. Run '. <install_dir>/bin/mqsiprofile' to source the mqsiprofile script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
3. Ensure that the broker database instance profile has been run. Invoke the SQL profile that was created when the broker database was created.
4. Enter the following command to create the broker:

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw
-q WBRK_QM -n WBRKBKDB -u dbuid -p dbpw
```

If you are using different names or values for any parameter on this command, you **must** replace the appropriate values with your own.

In the command above:

WBRK_BROKER

Is the broker name.

wbrkuid

Is the service user ID that is used to run the broker.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that the broker will use. This queue manager is created if it does not exist.

WBRKBKDB

Is the name of the existing broker database, the broker tables will be created within this database.

dbuid Is the user ID that has read, write and create access permissions for the database. This is the user ID that will be used to read and update the broker’s persistent store.

dbpw Is the password that is associated with the database user ID, dbuid.

On completion of this task, you have:

- Created a broker called WBRK_BROKER.
- Created and started a WebSphere MQ queue manager called WBRK_QM.

- Created and set up the WebSphere MQ resources required by the broker, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqsicreatebroker** command.

Note: Note that this command does **not** start the listener

- Ensured that all database tables required by the broker have been created in the database WBRKBKDB.

Now that you have created a physical broker, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.
2. Add the broker to the broker domain.
 - To add the broker using the workbench, see “Adding a broker to a broker domain” on page 175.
 - To add the broker using the Configuration Manager Proxy Java API, see Creating domain objects using the Configuration Manager Proxy

Creating a broker on Linux

Follow the steps detailed in this task for creating a broker on Linux platforms.

To create a broker:

1. Log on using your service user ID. If you use the su command to switch user you must ensure that you invoke that user’s profile.
 - a. Enter `su - <user ID>` to run a different user’s profile.
2. Run `' . <install_dir>/bin/mqsiprofile'` to source the mqsiprofile script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
3. Ensure that the broker database instance profile has been run. Invoke the SQL profile that was created when the broker database was created.
4. Enter the following command to create the broker:

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw
-q WBRK_QM -n WBRKBKDB -u dbuid -p dbpw
```

Note: The service user ID you use on the mqsicreatebroker command line **must** be the user ID that you use to invoke the mqsicreatebroker command, or root.

If you are using different names or values for any parameter on this command, replace the appropriate values with your own.

In the command above:

WBRK_BROKER

Is the broker name.

wbrkuid

Is the service user ID that is used to run the broker.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that the broker will use. This queue manager is created if it does not exist.

WBRKKBDB

Is the name of the existing broker database, the broker tables will be created within this database.

dbuid Is the user ID that has read, write and create access permissions for the database. This is the user ID that will be used to read and update the broker's persistent store.

dbpw Is the password that is associated with the database user ID, dbuid.

On completion of this task, you have:

- Created a broker called `WBRK_BROKER`.
- Created and started a WebSphere MQ queue manager called `WBRK_QM`.
- Created and set up the WebSphere MQ resources required by the broker, and defined these on the queue manager. This includes the default dead letter-queue (DLQ), which is automatically enabled by running the `mqsicreatebroker` command.

This command does **not** start the listener; you must do that yourself.

- Ensured that all database tables required by the broker have been created in the database `WBRKKBDB`.

Now that you have created a physical broker, you are ready to complete the next actions:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to "Connecting components" on page 153
2. Add the broker to the broker domain.
 - To add the broker using the workbench, see "Adding a broker to a broker domain" on page 175.
 - To add the broker using the Configuration Manager Proxy Java API, see Creating domain objects using the Configuration Manager Proxy

Creating a broker on Solaris

To create a broker:

1. Log on using your service user ID. If you use the `su` command to switch user you must ensure that you invoke that user's profile.
 - a. Enter `su - <user ID>` to run a different user's profile.
2. Run `'. <install_dir>/bin/mqsiprofile'` to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
3. Ensure the broker database instance profile has been run. Invoke the SQL profile that was created when the broker database was created.
4. Enter the following command to create the broker: If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw  
-q WBRK_QM -n WBRKKBDB -u dbuid -p dbpw
```

where:

- WBRK_BROKER is the broker name.
- wbrkuid is the service user ID that is used to run the broker.
- wbrkpw is the password for the service user ID.
- WBRK_QM is the name of the WebSphere MQ queue manager that the broker will use. This queue manager is created if it does not exist.
- WBRKBKDB is the name of the existing broker database, the broker tables will be created within this database.
- dbuid is the user ID that has read, write and create access permissions for the database. This is the user ID that will be used to read and update the broker's persistent store.
- dbpw is the password that is associated with the database user ID, dbuid.

On completion of this task, you have:

- Created a broker called WBRK_BROKER.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the broker, and defined these on the queue manager. This includes the default dead letter queue (DLQ) which is automatically enabled by running the **mqsicreatebroker** command.

Note: Note that this command does **not** start the listener

- Ensured that all database tables required by the broker have been created in the database WBRKBKDB.

Now that you have created a physical broker, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers and Configuration Manager). This allows components in your broker domain, that are supported by different queue managers, to exchange messages and communicate effectively. Refer to "Connecting components" on page 153
2. Add the broker to the broker domain.
 - To add the broker using the workbench, see "Adding a broker to a broker domain" on page 175.
 - To add the broker using the Configuration Manager Proxy Java API, see Creating domain objects using the Configuration Manager Proxy

Creating a broker on Windows

To create a broker:

1. Open a WebSphere Event Broker command prompt for the desired runtime.
2. Enter the following command to create the broker:

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw  
-q WBRK_QM -n WBRKBKDB -u dbuid -p dbpw
```

If you are using different names or values for any parameter on this command, you **must** replace the appropriate values with your own.

In the command above:

WBRK_BROKER

Is the broker name.

wbrkuid

The broker runs as a Windows service. A service needs to log on with some credentials; "wbrkuid" is the user id for the credentials.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that the broker will use. This queue manager is created if it does not exist.

WBRKKBDB

Is the name of the existing broker database, the broker tables will be created within this database.

dbuid Is the user ID that has read, write and create access permissions for the database. This is the user ID that will be used to read and update the broker's persistent store.

dbpw Is the password that is associated with the database user ID, dbuid.

On completion of this task, you have:

- Created a broker called WBRK_BROKER.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the broker, and defined these on the queue manager. This includes the default dead letter-queue (DLQ), which is automatically enabled by running the **mqsicreatebroker** command.

Note: Note that this command does **not** start the listener

- Ensured that all database tables required by the broker have been created in the database WBRKKBDB.

Now that you have created a physical broker, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to "Connecting components" on page 153
2. Add the broker to the broker domain.
 - To add the broker using the workbench, see "Adding a broker to a broker domain" on page 175.
 - To add the broker using the Configuration Manager Proxy Java API, see Creating domain objects using the Configuration Manager Proxy

Creating a broker on z/OS

The process for creating a broker involves the following tasks:

1. "Collecting the information required to create a broker" on page 117
2. "Creating the broker PDSE" on page 118
3. "Customizing the broker component data set" on page 119
4. "Customizing the broker JCL" on page 119
5. "Creating the environment file" on page 120
6. "Priming DB2" on page 121
7. "Creating the broker component" on page 122

8. "Copying the broker started task to the procedures library" on page 122
9. "Creating the broker directory on z/OS" on page 122

Collecting the information required to create a broker:

This is part of the larger task of creating a broker on z/OS.

You need to complete the information in each of the tables, at the following links, before continuing:

- "Installation information - broker and User Name Server"
- "DB2 information"
- "Component information - broker" on page 118

Installation information - broker and User Name Server:

Collect the information shown in the Description column and complete the values you require for your particular system. You can see a complete list of variables you can customize in "z/OS JCL variables" on page 382.

Description	JCL variable	Example installation value	Your installation value
Fully qualified name of the product's SBIPPROC dataset	N/A	<hlq>.SBIPPROC	
Fully qualified name of the product's SBIPSAMP dataset	N/A	<hlq>.SBIPSAMP	
File system directory where the product has been installed	++INSTALL++	/usr/lpp/mqsi	
WebSphere MQ high-level qualifier	++WMQHLQ++	MQM.V531	
Location of Java installation	++JAVA++	/usr/lpp/java/IBM/J1.4	
Location of IBM XML Toolkit installation	++XMLTOOLKIT++	/usr/lpp/ixm/IBM/xml4c-5_5	
Locale of environment where commands are run by submitting JCL	++LOCALE++	C	
Time zone of environment where commands are run by submitting JCL	++TIMEZONE++	GMT0BST	

DB2 information:

Collect the information explained in the Description column and complete the values you require for your particular system. You can see a complete list of variables that you can customize in "z/OS JCL variables" on page 382.

Description	JCL variable	Example installation value	Your installation value
DB2 high-level qualifier	++DB2HLQ++.	SYS2.DB2.V710	
DB2 run library value	++DB2RUNLIB++	DSN710PK.RUNLIB.LOAD	
DB2 subsystem identifier	++DB2SUBSYSTEM++	DFK4	
DB2 plan name	++DB2DSNACLIPLAN++	DSNACLI	

DB2 program value	++DB2SAMPLEPROGRAM++	DSNTEP2	
DB2 plan value	++DB2SAMPLEPROGRAMPLAN++	DSNTEP71	
DB2 location value of the DB2 subsystem	++DB2LOCATION++	DSN710PK	
DB2 converter	++DB2CONVERSION++	SINGLE	
DB2 user ID for the component and commands	++DB2CURRENTSQLID++	MQPIBRK	
DB2 table owner user ID	++DB2TABLEOWNER++	MQP1BRK	

Component information - broker:

Collect the information shown in the Description column and complete the values you require for your particular system. You can see a complete list of variables you can customize in “z/OS JCL variables” on page 382.

Description	JCL variable	Example component value	Your component value
Home directory of the file system for the broker’s user ID	++HOME++	/u/mqp1brk	
Queue Manager associated with the broker	++QUEUEMANAGER++	MQP1	
File system directory where the broker is to exist	++COMPONENTDIRECTORY++	/mqsi/brokers/MQP1BRK	
Broker name	++COMPONENTNAME++	MQP1BRK	
Data set where all JCL relevant to the broker is saved	++COMPONENTDATASET++	TESTDEV.BROKER.MQP1BRK	
Profile name	++COMPONENTPROFILE++	BIPBPROF	BIPBPROF
Name of the Started Task JCL; can be a maximum of 8 characters	++STARTEDTASKNAME++	MQP1BRK	
Name of the broker DB2 database	++DB2DATABASE++	DMQP1BRK	
Name of the broker DB2 storage group	++DB2STORAGEGROUP++	MQP1STOR	
Name of the broker DB2 bufferpool	++DB2BUFFERPOOL++	BP0	
DB2 index bufferpool	++DB2INDEXBP++	BP0	
DB2 LOB table bufferpool	++DB2LOBBP++	BP0	
mqsicreatebroker options	++OPTIONS++	Any additional optional parameters for the mqsicreatebroker command	

Creating the broker PDSE:

This is part of the larger task of creating a broker on z/OS.

Each broker requires a PDSE or a PDS. A PDSE is preferable to a PDS because free space is available without the need to compress the data set.

Create the broker PDSE, for example using option 3.2 on ISPF. The name of the PDSE must be the same as the JCL variable ++COMPONENTDATASET++. Allocate a data set with:

- Eight directory blocks
- 15 tracks (or 1 cylinder) of 3390 DASD with a record format of fixed blocked 80
- A suitable block size (for example 27920)
- A data set type of library

Customizing the broker component data set:

This is part of the larger task of creating a broker on z/OS.

Before you start

Before starting this task, you must have completed “Collecting the information required to create a broker” on page 117.

Create the broker data set in TSO, identified by ++COMPONENTDATASET++, as instructed below:

1. Copy the members specified in “Broker PDSE members originating in <hlq>.SBIPSAMP” on page 378 from <hlq>.SBIPSAMP to ++COMPONENTDATASET++. Ensure that you copy only the listed files.
2. Copy the members specified in “Broker PDSE members originating in <hlq>.SBIPPROC” on page 378 from <hlq>.SBIPPROC to ++COMPONENTDATASET++. Ensure that you copy only the listed files.
3. Customize the JCL.

Customizing the broker JCL:

This is part of the larger task of creating a broker on z/OS.

Before you start

Before starting this task, you must have completed “Customizing the broker component data set.”

All JCL has a standard header, comprising:

- A brief description of its function.
- A description where further information can be found, relating to the function of the JCL.
- If appropriate, a topic number.
- The section listing the JCL variables themselves.

Each JCL file defines its own STEPLIB. Some JCL files, for example BIPRELG, might require DB2 defined in the STEPLIB for a broker component. This must be removed from the JCL if the component is either a Configuration Manager or User Name Server, because it is not required.

You can customize the files using an ISPF edit macro that you have to tailor, or you can make changes to each of the PDSE members manually.

BIPEDIT is a REXX program that you can use to help you customize your JCL. After you have customized BIPEDIT you can run this REXX program against the other JCL files to change their JCL variables.

1. Customize the renamed BIPEDIT file. Use the information you collected in:
 - “Installation information - broker and User Name Server” on page 117
 - “DB2 information” on page 117
 - “Component information - broker” on page 118
2. Activate the renamed BIPEDIT file before you customize any other JCL files. Do this by running the following TSO command:

```
ALTLIB ACTIVATE APPLICATION(EXEC) DA('COMPONENTDATASET')
```

where 'COMPONENTDATASET' is identical to ++COMPONENTDATASET++.

This command is active for the local ISPF session for which it was issued. Note that if you have split screen sessions, the other sessions are not able to use this. If you use ISPF option 6 to issue the command, use ISPF option 3.4 to edit the data set; this enables you to use the edit command.

3. Edit each JCL file. Run the renamed BIPEDIT exec by typing its name on the command line (for example MQ01EDBK). Instead of editing a member, you might want to View it until you have resolved any problems in your REXX program. Alternatively, you can Cancel the Edit session instead of saving it.

You must set a value for all the variables listed in the JCL; if you do not do so, the JCL will not work correctly.

Some JCL files include ++OPTIONS++ for a command; you must replace them with additional optional parameters specific to the command on z/OS, or remove them. It is likely that you will have to do this in addition to running BIPEDIT. If you do not require any additional options, remove ++OPTIONS++ using the following command:

```
"c ++OPTIONS++ ' ' all"
```

where ' ' represents two single quotation marks.

Save the edit macro and run this macro against all of the members except the edit macro itself.

If the user ID submitting the BIPCBRK command has the appropriate DB2 and WebSphere MQ authorities, you can ignore the optional **mqsicreatebroker** parameters -1, -2, and -3.

If you intend to have different administrators create the DB2 and WebSphere MQ resources, you can consider using one of these optional parameters; see “mqsicreatebroker command” on page 286 for further information.

When you update BIPBPROF (the broker profile), the changes are not accessible until you run BIPGEN to copy the profile to the file system and create the ENVFILE. You must do this each time you update BIPBPROF for the changes to take effect.

You need to be aware that another process might be using the current ENVFILE, so you need to consider whether updating the current ENVFILE in the file system will have any impact.

Creating the environment file:

This is part of the larger task of creating a broker on z/OS.

Before you start

Before starting this task, you must have completed “Customizing the broker JCL” on page 119

1. Review the BIPBPROF member. If you define parameters for all users, you can configure BIPBPROF to use these parameters.

For example, if the time zone option TZ is set as a system-wide parameter for all users, you can remove it from BIPBPROF.

2. Submit member BIPGEN. Review the job output and make sure the environment file in the output contains the parameters you expect.

If you change BIPBPROF, or system-wide parameters, you must submit BIPGEN again to pick up the changes.

Priming DB2:

This is part of the larger task of creating a broker on z/OS. The broker uses DB2 tables to hold its internal data. These tables are defined in table spaces, which in turn, are defined within a DB2 database.

Data from tables is accessed through in-memory buffer pools, and typically you have different buffer pools for:

- Different applications
- Indexes
- Tables
- LOB tables

The DASD volumes that can be used by a database are defined using a storage group (STOGROUP). Your DB2 systems administrator will tell you which buffer pools and storage groups to use.

The BIPCRDB job issues commands that require the following authorities:

- CREATESG - to create a storage group
- CREATEDBA - to create the database

Note that you might also need authority to grant use of a buffer pool.

If you have any problems with this job, you can edit and customize member BIPDLDB to delete the database. You can run the BIPCRDB job again when you have resolved the problems.

Before you start

Before starting this task, you must have completed “Creating the environment file” on page 120.

1. Edit the BIPCRDB job.
2. Review and change the BUFFERPOOL and INDEXBP buffer pools on the CREATE DATABASE statement
3. Change the buffer pool specification on the CREATE LOB TABLESPACE statements to a value suitable for your enterprise.
4. Submit BIPCRDB from your broker PDSE. You need the authority described earlier to submit the DB2 job.

BIPCRDB creates the DB2 StorageGroup, Database, and Table Spaces but does not create any tables or indexes.

The steps in the BIPCRDB job must complete with return code zero.

Creating the broker component:

This is part of the larger task of creating a broker on z/OS.

Before you start

Before starting this task, you must have completed “Priming DB2” on page 121.

If the user ID submitting the BIPCRBK command has the appropriate DB2 and WebSphere MQ authorities, you can ignore the optional **mqsicreatebroker** parameters -1, -2, and -3. If it is your intention to have different administrators create the DB2 and WebSphere MQ resources, you can consider using one of these optional parameters; see “mqsicreatebroker command” on page 286 for further information.

1. Submit job BIPCRBK with option -1. This job creates the files and directories that are placed in the default storage group. You must run this job first, and to do this you need authority to access the broker root directory.
2. Edit BIPCRBK and submit the job with option -2. This job creates the WebSphere MQ queues. If you do not have the requisite authority, ask your WebSphere MQ system administrator to run the job.
3. Edit BIPCRBK and submit the job with option -3. This job creates the DB2 queues. If you do not have the requisite authority, ask your DB2 system administrator to run the job.
4. Ensure that the jobs have run successfully by:
 - Checking the STDOUT stream in the JOBLOG.
 - Viewing STDOUT for any errors and checking for BIP8071I: Successful command completion.

If you encounter any problems, delete the broker and recreate it using the following procedure. Note that you need the appropriate authority to run the jobs.

1. Edit and configure job BIPDLBK.
2. Run job BIPDLBK with the same option, or options, that caused the problems when you ran the BIPCRBK job.
3. Correct the problems and run the BIPCRBK job again.

Copying the broker started task to the procedures library:

This is part of the larger task of creating a broker on z/OS.

Before you start

Before starting this task, you must have completed “Creating the broker component.”

1. Ensure that the user ID for the broker started task is defined and that the broker procedure is associated with the user ID. If you are using a security manager, for example RACF, update the started class for your broker. See “Setting up z/OS security” on page 28 and “Summary of required access (z/OS)” on page 372 for more information.
2. Copy the Started Task JCL (BIPBRKP) to the procedures library, for example USER.PROCLIB.

Creating the broker directory on z/OS:

This is part of the larger task of creating a broker on z/OS .

Before you start

Before starting this task, you must have completed “Collecting the information required to create a broker” on page 117 and “Creating the broker PDSE” on page 118.

1. Use the TSO command OMVS to get into OMVS.
2. Create the broker root directory using the command:

```
mkdir -p <ComponentDirectory>
```

The name of the directory must be the same as the JCL variable ++COMPONENTDIRECTORY++.

3. Display the contents of the directory, which is currently empty, using the command:

```
ls -dl /var/wmqi/MQP1BRK
```

4. Display the permissions on the directory using the command:

```
ls -l /var/wmqi/MQP1BRK
```

5. Ensure that the user ID of the person doing the customization has a group that matches the group of the directory. Use the command, where `userid` is the ID you want to check:

```
id <userid>
```

6. Check that the directory has a valid group and that the group has `rxw` permissions. If they do not, use the command to set the group of the directory:

```
chgrp <group> <pathname>
```

For example:

```
chgrp WMQI /var/wmqi/MQP1BRK
```

You have to be the owner of the group or have superuser authority to use this command.

7. To give the group `READ`, `WRITE`, and `EXECUTE` access, use the command:

```
chmod g=rwx <pathname>
```

For example:

```
chmod g=rwx /usr/wmqi/MQP1BRK
```

8. To display the amount of space used and available, use the command:

```
df -P /var/wmqi/MQP1BRK
```

Adding an execution group to a broker using the command line

Before you start:

You must complete the following tasks:

- “Adding a broker to a broker domain” on page 175

When you create a broker, it has a default execution group. If you want additional execution groups, you must create them explicitly.

For more details about why you might want to create multiple execution groups, see Execution groups.

Instead of employing the Message Brokers Toolkit, you can use this task as an alternative method of creating an execution group .

For more details on creating an execution group from the Message Brokers Toolkit see “Adding an execution group to a broker” on page 179

To add an execution group to a broker using the command line on Windows, UNIX systems, and Linux:

1. Open a command prompt that has the environment configured for WebSphere Event Broker Version 6.0.
2. Enter the following command to add the execution group:
`mqsicreateexecutiongroup -i host -p 1414 -q QMGR -b BROKER -e EG1`

where

host Is the host name or IP address of the Configuration Manager for the domain on which the broker resides.

1414 Is the port on which the Configuration Manager’s queue manager is listening.

QMGR Is the name of the Configuration Manager’s queue manager.

BROKER Is the name of the broker.

EG1 Is the name of the execution group that you want to create.

On completion of this task, you have requested that the Configuration Manager creates an execution group on the broker when it is next deployed.

Adding an execution group to a broker on z/OS

Before you start:

You must complete the following tasks:

- “Adding a broker to a broker domain” on page 175

When you create a broker, it has a default execution group. If you want additional execution groups, you must create them explicitly.

For more details about why you might want to create multiple execution groups, see Execution groups.

Instead of employing the Message Brokers Toolkit, you can use this task as an alternative method of creating an execution group .

For more details on creating an execution group from the Message Brokers Toolkit see “Adding an execution group to a broker” on page 179

To add an execution group to a broker on z/OS:

Configure and run the BIPCREG job to create an execution group. Note that you need to create the broker in the Configuration Manager before you run the BIPCREG job.

On completion of this task, you have requested that the Configuration Manager creates an execution group on the broker when it is next deployed.

Creating a Configuration Manager

Before you start:

You must complete the following tasks:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423.
- For platforms other than z/OS, see “Considering security for a Configuration Manager” on page 16 for information about security matters relevant to a Configuration Manager during the configuration task.

To create a Configuration Manager, follow the link for the appropriate platform.

- Create a Configuration Manager using the command line on the system where the Configuration Manager component is installed. On Windows, you can also use the Command Assistant to complete this task.
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before creating a Configuration Manager, by running the product profile or console; refer to Setting up a command environment.
- AIX
- HP-UX
- Linux
- Solaris
- Windows
- z/OS

Creating a Configuration Manager on AIX

The following steps show you how to create a Configuration Manager.

1. Run '`. <install_dir>/bin/mqsiprofile`' to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. Log on using your user ID. If you use the `su` command to switch user from root, enter `su - <user ID>` to run your user profile.
3. Enter the following command to create the Configuration Manager:

```
mqsicreateconfigmgr CMGR01 -i wbrkuid -a wbrkpw -q WBRK_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

CMGR01

Is the name of the Configuration Manager that you are creating.

wbrkuid

Is the service user ID that is used to run the Configuration Manager.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that will host the Configuration Manager. This is created if it does not exist.

On completion of this task, you have:

- Created a Configuration Manager.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the Configuration Manager, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqsicreateconfigmgr** command.
- Set up the authorizations that the Configuration Manager requires to access WebSphere MQ resources.

Now that you have created the Configuration Manager, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.
2. Create a broker domain connection using the workbench. Refer to “Creating a domain connection” on page 172.

Creating a Configuration Manager on HP-UX

The following steps show you how to create a Configuration Manager.

1. Run '`<install_dir>/bin/mqsiprofile`' to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. Log on using your user ID. If you use the `su` command to switch user from `root`, enter `su - <user ID>` to run your user profile.
3. Enter the following command to create the Configuration Manager:

```
mqsicreateconfigmgr CMGR01 -i wbrkuid -a wbrkpw -q WBRK_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

CMGR01

Is the name of the Configuration Manager that you are creating.

wbrkuid

Is the service user ID that is used to run the Configuration Manager.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that will host the Configuration Manager. This is created if it does not exist.

On completion of this task, you have:

- Created a Configuration Manager.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the Configuration Manager, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqsicreateconfigmgr** command.

- Set up the authorizations that the Configuration Manager requires to access WebSphere MQ resources.

Now that you have created the Configuration Manager, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.
2. Create a broker domain connection using the workbench. Refer to “Creating a domain connection” on page 172.

Creating a Configuration Manager on Linux

Follow the steps detailed in this task for creating a Configuration Manager on Linux platforms.

To create a Configuration Manager.

1. Run '`<install_dir>/bin/mqsiprofile`' to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. Log on using your user ID. If you use the `su` command to switch user from root, enter `su - <user ID>` to run your user profile.
3. Enter the following command to create the Configuration Manager:

```
mqsicreateconfigmgr CMGR01 -i wbrkuid -a wbrkpw -q WBRK_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

CMGR01

Is the name of the Configuration Manager that you are creating.

wbrkuid

Is the service user ID that is used to run the Configuration Manager.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that will host the Configuration Manager. This is created if it does not exist.

On completion of this task, you have:

- Created a Configuration Manager.
- Created and started a WebSphere MQ queue manager called `WBRK_QM`.
- Created and set up the WebSphere MQ resources required by the Configuration Manager, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the `mqsicreateconfigmgr` command.
- Set up the authorizations that the Configuration Manager requires to access WebSphere MQ resources.

Now that you have created the Configuration Manager, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers,

and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.

2. Create a broker domain connection using the workbench. Refer to “Creating a domain connection” on page 172.

Creating a Configuration Manager on Solaris

The following steps show you how to create a Configuration Manager.

1. Run '`<install_dir>/bin/mqsiprofile`' to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. Log on using your user ID. If you use the `su` command to switch user from `root`, enter `su - <user ID>` to run your user profile.
3. Enter the following command to create the Configuration Manager:

```
mqsicreateconfigmgr CMGR01 -i wbrkuid -a wbrkpw -q WBRK_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

CMGR01

Is the name of the Configuration Manager that you are creating.

wbrkuid

Is the service user ID that is used to run the Configuration Manager.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that will host the Configuration Manager. This is created if it does not exist.

On completion of this task, you have:

- Created a Configuration Manager.
- Created and started a WebSphere MQ queue manager called `WBRK_QM`.
- Created and set up the WebSphere MQ resources required by the Configuration Manager, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the `mqsicreateconfigmgr` command.
- Set up the authorizations that the Configuration Manager requires to access WebSphere MQ resources.

Now that you have created the Configuration Manager, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.
2. Create a broker domain connection using the workbench. Refer to “Creating a domain connection” on page 172.

Creating a Configuration Manager on Windows

You create a Configuration Manager using the command line. Create the Configuration Manager on the system where the Configuration Manager component is installed.

Use the **mqsicreateconfigmgr** command. The parameters on this command provide the Configuration Manager with all the additional information it requires to be ready for action as soon as it is started.

To create a Configuration Manager:

1. Open a WebSphere Event Broker command prompt for the desired runtime.
2. Enter the following command to create the Configuration Manager:

```
mqsicreateconfigmgr CMGR01 -i wbrkuid -a wbrkpw -q WBRK_QM
```

If you are using different names or values for any parameter on this command, you **must** replace the appropriate values with your own.

In the command above:

CMGR01

Is the name of the Configuration Manager that you are creating. This is an optional parameter; if you do not specify it, the default is 'ConfigMgr'.

wbrkuid

is the service user ID used to run the Configuration Manager.

This ID must be a member of the `mqm`, `mqbrkrs` and `Administrators` groups.

wbrkpw

Is the password for the service user ID.

WBRK_QM

Is the name of the WebSphere MQ queue manager that will host the Configuration Manager. This is created if it does not exist.

On completion of this task, you have:

- Created a Configuration Manager and added its Windows service to the Services (viewable from the Control Panel).
- Created and started a WebSphere MQ queue manager called `WBRK_QM`.
- Created and set up the WebSphere MQ resources required by the Configuration Manager, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqsicreateconfigmgr** command.
- Set up the authorizations that the Configuration Manager requires to access WebSphere MQ resources.
- Defined a service user ID `wbrkuid`, and database password `wbrkpw`.

Now that you have created the Configuration Manager, you are ready to:

1. Create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to "Connecting components" on page 153.

2. Create a broker domain connection using the workbench. Refer to “Creating a domain connection” on page 172.

Creating a Configuration Manager on z/OS

To create your Configuration Manager, perform the following tasks in order.

1. “Collecting the information required to create a Configuration Manager on z/OS”
2. “Creating the Configuration Manager PDSE” on page 131
3. “Creating the Configuration Manager directory on z/OS” on page 131
4. “Customizing the Configuration Manager component data set” on page 132
5. “Customizing the Configuration Manager JCL” on page 132
6. “Creating the Configuration Manager component” on page 133
7. “Copying the Configuration Manager started task to the procedures library” on page 135

Collecting the information required to create a Configuration Manager on z/OS:

This is part of the larger task of creating a Configuration Manager on z/OS.

You need to complete the information in each of the following tables before continuing:

- “Installation information - Configuration Manager”
- “Component information - Configuration Manager” on page 131

Installation information - Configuration Manager:

Collect the information shown in the Description column and complete the values you require for your particular system. You can see a complete list of variables you can customize in “z/OS JCL variables” on page 382.

Description	JCL variable	Example installation value	Your installation value
Fully qualified name of the product's SBIPPROC dataset	N/A	<hlq>.SBIPPROC	
Fully qualified name of the product's SBIPSAMP dataset	N/A	<hlq>.SBIPSAMP	
File system directory where the product has been installed	++INSTALL++	/usr/lpp/mqsi	
WebSphere MQ high-level qualifier	++WMQHLQ++	MQM.V531	
Location of Java installation	++JAVA++	/usr/lpp/java/IBM/J1.4	
Location of IBM XML Toolkit installation	++XMLTOOLKIT++	/usr/lpp/ixm/IBM/xml4c-5_5	
Locale of environment where commands are run by submitting JCL	++LOCALE++	C	
Time zone of environment where commands are run by submitting JCL	++TIMEZONE++	GMT0BST	
WebSphere MQ file system install directory	++MQPATH++	/usr/lpp/mqm	

Component information - Configuration Manager:

Collect the information shown in the Description column and complete the values you require for your particular system. You can see a complete list of variables you can customize in “z/OS JCL variables” on page 382.

Description	JCL variable	Example component value	Your component value
Configuration Manager name	++COMPONENTNAME++	MQP1CMGR	
Configuration Manager’s user ID file system home directory	++HOME++	/u/mqp1cmgr	
File system directory where the Configuration Manager is to exist	++COMPONENTDIRECTORY++	/mqsi/configmgrs/ MQP1CMGR	
Data set where all JCL relevant to the Configuration Manager is saved	++COMPONENTDATASET++	TESTDEV.CMGR.MQP1CMGR	
Profile name	++COMPONENTPROFILE++	BIPCPROF	BIPCPROF
Name of the Started Task JCL; can be a maximum of 8 characters	++STARTEDTASKNAME++	MQP1CMGR	
mqsicreateconfigmgr options	++OPTIONS++	Any additional optional parameters for the mqsicreateconfigmgr command	

Creating the Configuration Manager PDSE:

This is part of the larger task of creating a Configuration Manager on z/OS.

Create the Configuration Manager PDSE, for example using option 3.2 on ISPF. The name of the PDSE must be the same as the JCL variable ++COMPONENTDATASET++. Allocate a data set with:

- Eight directory blocks
- 15 tracks (or 1 cylinder) of 3390 DASD with a record format of fixed blocked 80
- A suitable block size (for example 27920)
- A data set type of library

Creating the Configuration Manager directory on z/OS:

This is part of the larger task of creating a Configuration Manager on z/OS.

Before you start

To complete this task, you must have completed the following tasks:

- “Collecting the information required to create a Configuration Manager on z/OS” on page 130
- “Creating the Configuration Manager PDSE”

Create the Configuration Manager directory manually using:

```
mkdir <ComponentDirectory>
```

The name of the directory must be the same as the JCL variable ++COMPONENTDIRECTORY++.

Use the chmod command to set the required authorizations. See “Creating the broker directory on z/OS” on page 122 for more information.

Customizing the Configuration Manager component data set:

This is part of the larger task of creating a Configuration Manager on z/OS.

Before you start

Before starting this task, you must have completed “Collecting the information required to create a Configuration Manager on z/OS” on page 130.

Create the Configuration Manager data set in TSO, identified by ++COMPONENTDATASET++, as instructed below:

1. Copy BIPCPR0F from <hlq>.SBIPSAMP to ++COMPONENTDATASET++.
2. Copy the members specified in “Configuration Manager PDSE members originating in <hlq>.SBIPPROC” on page 381 from <hlq>.SBIPPROC to ++COMPONENTDATASET++. Ensure that you copy only the listed files.
3. Customize the JCL.

Customizing the Configuration Manager JCL:

This is part of the larger task of creating a Configuration Manager on z/OS.

Before you start

Before starting this step, you must have completed “Customizing the Configuration Manager component data set.”

- A brief description of its function.
- A description where further information can be found, relating to the function of the JCL.
- If appropriate, a topic number.
- The section listing the JCL variables themselves.

Each JCL file defines its own STEPLIB. Some JCL files, for example BIPRELG, might require DB2 defined in the STEPLIB for a broker component. This must be removed from the JCL if the component is either a Configuration Manager or User Name Server, because it is not required.

You can customize the files using an ISPF edit macro that you have to tailor, or you can make changes to each of the PDSE members manually.

BIPEDIT is a REXX program that you can use to help you customize your JCL. After you have customized BIPEDIT you can run this REXX program against the other JCL files to change their JCL variables.

1. Customize the renamed BIPEDIT file. Use the information you collected in:
 - “Installation information - Configuration Manager” on page 130
 - “Component information - Configuration Manager” on page 131
2. Activate the renamed BIPEDIT file before you customize any other JCL files. Do this by running the following TSO command:

```
ALTLIB ACTIVATE APPLICATION(EXEC) DA('COMPONENTDATASET')
```

where 'COMPONENTDATASET' is identical to ++COMPONENTDATASET++.

This command is active for the local ISPF session for which it was issued. Note that if you have split screen sessions, the other sessions are not able to use this. If you use ISPF option 6 to issue the command, use ISPF option 3.4 to edit the data set; this enables you to use the edit command.

3. Edit each JCL file. Run the renamed BIPEDIT exec by typing its name on the command line (for example MQ01EDCM). Instead of editing a member, you might want to View it until you have resolved any problems in your REXX program. Alternatively, you can Cancel the Edit session instead of saving it.

You must set a value for all the variables listed in the JCL; if you do not do so, the JCL will not work correctly.

Some JCL files include ++OPTIONS++ for a command; you must replace them with additional optional parameters specific to the command on z/OS, or remove them. It is likely that you will have to do this in addition to running BIPEDIT. If you do not require any additional options, remove ++OPTIONS++ using the following command:

```
"c ++OPTIONS++ ' ' all"
```

where ' ' represents two single quotation marks.

Save the edit macro and run this macro against all of the members except the edit macro itself.

Do not set either of the optional pass parameters (-1 or -2) in BIPCRCM at this time because you want to create the registry and the WebSphere MQ queues.

When you update BIPCPR0F (the Configuration Manager profile), the changes are not accessible until you run BIPGEN to copy the profile to the file system and create the ENVFILE. You must do this each time you update BIPCPR0F for the changes to take effect, which happens when you restart the Configuration Manager.

You need to be aware that another process might be using the current ENVFILE, so you need to consider whether updating the current ENVFILE in the file system will have any impact.

Creating the Configuration Manager component:

This is part of the larger task of creating a Configuration Manager on z/OS.

Before you start

Before starting this task, you must have completed "Customizing the Configuration Manager JCL" on page 132.

If the user ID submitting the BIPCRCM command has the appropriate WebSphere MQ authorities, you can ignore the optional **mqsicreateconfigmgr** parameters -1 and -2. If it is your intention to have a different administrator create the WebSphere MQ resources, you can consider using one of these optional parameters; see the "mqsicreateconfigmgr command" on page 296 for further information.

1. Submit job BIPCRCM with option -1. This job creates the Configuration Manager together with the files and directories that are placed in the registry. You must run this job first, and to do this you need authority to access the Configuration Manager.
2. Edit BIPCRCM and submit the job with option -2. This job creates the WebSphere MQ queues. If you do not have the requisite authority, ask your WebSphere MQ system administrator to run the job.
3. Ensure that the jobs have run successfully by:
 - Checking the STDOUT stream in the JOBLOG.
 - Viewing STDOUT for any errors and checking for BIP8071I: Successful command completion.

If you encounter any problems, delete the Configuration Manager and recreate it using the following procedure. Note that you need the appropriate authority to run the jobs.

1. Edit and configure job BIPDLCM.
2. Run job BIPDLCM with the same option, or options, that caused the problems when you ran the BIPCRCM job.
3. Correct the problems and run the BIPCRCM job again.

If you want to migrate the Configuration Manager from another platform to z/OS, for example, migrating a Version 5 Configuration Manager from Windows XP, you need to do some additional customization to include JDBC into the BIPCRCM job.

1. Locate the JDBC classes in your USS environment; for example the file db2jcc.jar can be in /usr/lpp/db2710/db2710/jcc/classes/.
2. Edit the BIPCPR0F file and add the following lines before the line containing export CLASSPATH=, so that the file looks like this:


```
DB2=/usr/lpp/db2710/db2710
CP=$CP:$DB2/jcc/classes/sqlj.zip
CP=$CP:$DB2/jcc/classes/db2jcc.jar
CP=$CP:$DB2/jcc/classes/db2jcc_javax.jar
CP=$CP:$DB2/jcc/classes/db2jcc_license_cisuz.jar
export CLASSPATH=$CP
```
3. Before the line containing export LIBPATH=\$LP insert the following lines to add the files to the LP, as follows:


```
LP = $LP:$DB2/jcc/lib
export LIBPATH=$LP
```
4. After the final export PATH statement add the following line:


```
export PATH=$PATH:$DB2/jcc/bin
```
5. Save the file, submit the BIPGEN job, and check the output to make sure the changes you just made are present.
6. Edit the BIPCRCM job to define the remote database, user ID, and password for the remote database you want to use; for example:

```
mqsicreateconfigmgr -
VCP2CMGR -
-q VCP2 -
-n //kbyn176.alpha.ibm.com:50000/WBIV5CFG -
-u fred -p xxxxxxx
```

In the preceding example:

- VP2CMGR is the Configuration Manager name
- -n is the location of the remote database
- //kbyn176.alpha.ibm.com is the machine containing the DB2 instance

- 50000 is the port number
- WBIV5CFG is the database name on that DB2 instance; this information is passed to the JDBC connect call
- -u is the Windows user ID, in this case fred
- -p is the password value

You can determine the port number as follows:

1. From the UDB control center, right-click on the DB2 instance.
2. Select **Setup Communications...**
3. Enter the user ID and password, if required.

The properties box contains the address and port number for this DB2 instance.

Note that the BIPCRCM job can take several minutes to run, depending on the content of the remote database.

Copying the Configuration Manager started task to the procedures library:

This is part of the larger task of creating a Configuration Manager on z/OS.

Before you start

Before starting this task, you must have completed “Creating the Configuration Manager component” on page 133.

Copy the Started Task JCL (BIPCMGRP) to the procedures library, for example USER.PROCLIB.

Enabling a User Name Server

If you require a User Name Server as a component of your broker domain, you must create the necessary connections between the broker, Configuration Manager, and User Name Server, so that they can communicate effectively.

Specify additional parameters on the **mqsicreatebroker** and **mqsicreateconfigmgr** commands, before you create the User Name Server. The following steps show you how to do this.

1. Create a broker with the additional -s and -j parameters on the **mqsicreatebroker** command. These parameters allow the broker to communicate with the WebSphere MQ queue manager for the User Name Server, and also enable the broker for publish/subscribe access control.
If you have created the broker without these parameters, modify the broker, defining the -s and -j parameters. Refer to “Modifying a broker” on page 155.
2. Create a Configuration Manager with the additional -s parameter on the **mqsicreateconfigmgr** command. This parameter allows the Configuration Manager to communicate with the WebSphere MQ queue manager for the User Name Server.
If you have created the Configuration Manager without this parameter, modify the Configuration Manager, defining the -s parameter. Refer to “Modifying a Configuration Manager” on page 158.

Now that you have made the required changes to the broker and Configuration Manager, you can create the User Name Server, and thus enable publish/subscribe services.

Creating a User Name Server

Before you start:

You must complete the following tasks:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423.
- Create a broker and Configuration Manager, with the additional parameters on the **mqsicreatebroker** and **mqsicreateconfigmgr** commands to allow them to communicate with the User Name Server. Refer to “Enabling a User Name Server” on page 135.
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before creating a User Name Server, by running the product profile or console; refer to Setting up a command environment

Create a User Name Server using the command line on the system where the User Name Server component is installed. On Windows, you can also use the Command Assistant to complete this task.

To create a User Name Server, follow the link for the appropriate platform.

- AIX
- HP-UX
- Linux
- Solaris
- Windows
- z/OS

Creating a User Name Server on AIX

The following steps show you how to create a User Name Server.

1. Log on using your user ID. If you use the su command to switch user from root, enter `su - <user ID>` to run your user profile.
2. Enter the following command to create the User Name Server:

```
mqsicreateusernameserver -i wbrkuid -a wbrkpw -q WBRK_UNQ_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

wbrkuid

Is the service user ID that is used to run the User Name Server.

wbrkpw

Is the password for the service user ID.

WBRK_UNQ_QM

Is the name of the WebSphere MQ queue manager for the User Name Server. This is created if it does not exist.

On completion of this task, you have:

- Created a User Name Server.
- Created a default startup status of manual for the User Name Server.
- Created and started a WebSphere MQ queue manager called WBRK_QM.

- Created and set up the WebSphere MQ resources required by the User Name Server, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqscreateusernameserver** command.

Now that you have created the User Name Server, you are ready to create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.

Creating a User Name Server on HP-UX

The following steps show you how to create a User Name Server.

1. Log on using your user ID. If you use the su command to switch user from root, enter `su - <user ID>` to run your user profile.
2. Enter the following command to create the User Name Server:

```
mqscreateusernameserver -i wbrkuid -a wbrkpw -q WBRK_UNQ_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

wbrkuid

Is the service user ID that is used to run the User Name Server.

wbrkpw

Is the password for the service user ID.

WBRK_UNQ_QM

Is the name of the WebSphere MQ queue manager for the User Name Server. This is created if it does not exist.

On completion of this task, you have:

- Created a User Name Server.
- Created a default startup status of manual for the User Name Server.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the User Name Server, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqscreateusernameserver** command.

Now that you have created the User Name Server, you are ready to create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.

Creating a User Name Server on Linux

Follow the steps detailed in this task for creating a User Name Server on Linux platforms.

1. Log on using your user ID. If you use the su command to switch user from root, enter `su - <user ID>` to run your user profile.

2. Enter the following command to create the User Name Server:

```
mqsicreateusernameserver -i wbrkuid -a wbrkpw -q WBRK_UNQ_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

wbrkuid

Is the service user ID that is used to run the User Name Server.

wbrkpw

Is the password for the service user ID.

WBRK_UNQ_QM

Is the name of the WebSphere MQ queue manager for the User Name Server. This is created if it does not exist.

On completion of this task, you have:

- Created a User Name Server.
- Created a default startup status of manual for the User Name Server.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the User Name Server, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the **mqsicreateusernameserver** command.

Now that you have created the User Name Server, you are ready to create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.

Creating a User Name Server on Solaris

The following steps show you how to create a User Name Server.

1. Log on using your user ID. If you use the su command to switch user from root, enter su - <user ID> to run your user profile.
2. Enter the following command to create the User Name Server:

```
mqsicreateusernameserver -i wbrkuid -a wbrkpw -q WBRK_UNQ_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

wbrkuid

Is the service user ID that is used to run the User Name Server.

wbrkpw

Is the password for the service user ID.

WBRK_UNQ_QM

Is the name of the WebSphere MQ queue manager for the User Name Server. This is created if it does not exist.

On completion of this task, you have:

- Created a User Name Server.
- Created a default startup status of manual for the User Name Server.

- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the User Name Server, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the `mqscreateusernameserver` command.

Now that you have created the User Name Server, you are ready to create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.

Creating a User Name Server on Windows

The following steps show you how to create a User Name Server.

1. Open a command prompt.
2. Enter the following command to create the User Name Server:

```
mqscreateusernameserver -i wbrkuid -a wbrkpw -q WBRK_UNQ_QM
```

If you are using different names or values for any parameter on this command, you must replace the appropriate values with your own.

In the command above:

wbrkuid

Is the service user ID that is used to run the User Name Server.

wbrkpw

Is the password for the service user ID.

WBRK_UNQ_QM

Is the name of the WebSphere MQ queue manager for the User Name Server. This is created if it does not exist.

On completion of this task, you have:

- Created a User Name Server.
- Created a default startup status of manual for the User Name Server.
- Created and started a WebSphere MQ queue manager called WBRK_QM.
- Created and set up the WebSphere MQ resources required by the User Name Server, and defined these on the queue manager. This includes the default dead-letter queue (DLQ), which is automatically enabled by running the `mqscreateusernameserver` command.

Now that you have created the User Name Server, you are ready to create and start the WebSphere MQ queue manager channels that are required to connect WebSphere Event Broker components (brokers, User Name Servers, and Configuration Manager). This allows components in your broker domain that are supported by different queue managers to exchange messages and communicate effectively. Refer to “Connecting components” on page 153.

Creating a User Name Server on z/OS

To create your User Name Server, perform the following tasks in order.

1. “Collecting the information required to create a User Name Server on z/OS” on page 140
2. “Creating the User Name Server PDSE” on page 141

3. "Creating the User Name Server directory on z/OS" on page 141
4. "Creating the User Name Server runtime environment on z/OS" on page 141
5. "Customizing the User Name Server component data set" on page 142
6. "Customizing the User Name Server JCL" on page 143
7. "Creating the User Name Server component" on page 144
8. "Copying the User Name Server started task to the procedures library" on page 144

Collecting the information required to create a User Name Server on z/OS:

This is part of the larger task of creating a User Name Server on z/OS.

You need to complete the information in each of the following tables before continuing:

- "Installation information - broker and User Name Server" on page 117
- "Component information - User Name Server"

Installation information - broker and User Name Server:

Collect the information shown in the Description column and complete the values you require for your particular system. You can see a complete list of variables you can customize in "z/OS JCL variables" on page 382.

Description	JCL variable	Example installation value	Your installation value
Fully qualified name of the product's SBIPPROC dataset	N/A	<hlq>.SBIPPROC	
Fully qualified name of the product's SBIPSAMP dataset	N/A	<hlq>.SBIPSAMP	
File system directory where the product has been installed	++INSTALL++	/usr/lpp/mqsi	
WebSphere MQ high-level qualifier	++WMQHLQ++	MQM.V531	
Location of Java installation	++JAVA++	/usr/lpp/java/IBM/J1.4	
Location of IBM XML Toolkit installation	++XMLTOOLKIT++	/usr/lpp/ixm/IBM/xml4c-5_5	
Locale of environment where commands are run by submitting JCL	++LOCALE++	C	
Time zone of environment where commands are run by submitting JCL	++TIMEZONE++	GMT0BST	

Component information - User Name Server:

Collect the information shown in the Description column and complete the values you require for your particular system. You can see a complete list of variables you can customize in "z/OS JCL variables" on page 382.

Description	JCL variable	Example component value	Your component value

User Name Server's user ID file system home directory	++HOME++	/u/mqp1uns	
File system directory where the User Name Server is to exist	++COMPONENTDIRECTORY++	/mqsi/uns/MQP1UNS	
Data set where all JCL relevant to the User Name Server is saved	++COMPONENTDATASET++	TESTDEV.UNS.MQP1UNS	
Profile name	++COMPONENTPROFILE++	BIPUPROF	BIPUPROF
Name of the Started Task JCL; can be a maximum of 8 characters	++STARTEDTASKNAME++	MQP1UNS	
mqsicreateusername server options	++OPTIONS++	Any additional optional parameters for the mqsicreateusername command	

Creating the User Name Server PDSE:

This is part of the larger task of creating a User Name Server on z/OS.

Create the User Name Server PDSE, for example using option 3.2 on ISPF. The name of the PDSE must be the same as the JCL variable ++COMPONENTDATASET++. Allocate a data set with:

- Eight directory blocks
- 15 tracks (or 1 cylinder) of 3390 DASD with a record format of fixed blocked 80
- A suitable block size (for example 27920)
- A data set type of library

Creating the User Name Server directory on z/OS:

This is part of the larger task of creating a User Name Server on z/OS.

Before you start

To complete this task, you must have completed the following tasks:

- "Collecting the information required to create a User Name Server on z/OS" on page 140
- "Creating the User Name Server PDSE"

Create the User Name Server directory manually using:

```
mkdir <ComponentDirectory>
```

The name of the directory must be the same as the JCL variable ++COMPONENTDIRECTORY++.

Use the chmod command to set the required authorizations. See "Creating the broker directory on z/OS" on page 122 for more information.

Creating the User Name Server runtime environment on z/OS:

This is part of the larger task of creating a User Name Server on z/OS

Before you start

To complete this task, you must have completed the following task:

- “Creating the User Name Server directory on z/OS” on page 141.

Use the **mqsicreateusernameserver** command to create a User Name Server and its runtime environment. The command syntax is:

```
mqsicreateusernameserver -q QueueManagerName [-r RefreshInterval] [-1] [-2]
```

where:

-q *QueueManagerName*

is a required parameter and is the name of the WebSphere MQ queue manager associated with your User Name Server, for example MQP1.

-r *RefreshInterval*

is an optional parameter and is the interval, specified in seconds, at which the User Name Server interrogates the security subsystem for changes to user or group attributes. If an interval is not specified, the User Name Server default interval of 60 seconds is used.

-1 is an optional parameter and is the registry pass; this creates only the User Name Server registry.

-2 is an optional parameter and is the WebSphere MQ pass; this creates only the User Name Server WebSphere MQ queues.

You will be asked to confirm that the parameters you enter are correct. Enter Y to confirm, or N to change the parameters. If you choose to change the parameters, run **mqsicreateusernameserver** again.

Check that you are using the correct installation path, particularly if you are customizing the system after applying maintenance to an alternate set of WebSphere MQ Event Broker libraries. If you are applying service to the broker, you might want a different installation path.

The functionality of this command is not the same as on distributed platforms, because no WebSphere MQ-related definitions are performed. You have to follow further steps to complete the User Name Server creation and customization.

Customizing the User Name Server component data set:

This is part of the larger task of creating a User Name Server on z/OS.

Before you start

Before starting this task, you must have completed “Collecting the information required to create a User Name Server on z/OS” on page 140.

Create the User Name Server data set in TSO, identified by ++COMPONENTDATASET++, as instructed below:

1. Copy BIPUPROF from <hlq>.SBIPSAMP to ++COMPONENTDATASET++.
2. Copy the members specified in “User Name Server PDSE members originating in <hlq>.SBIPPROC” on page 380 from <hlq>.SBIPPROC to ++COMPONENTDATASET++. Ensure that you copy only the listed files.
3. Customize the JCL.

Customizing the User Name Server JCL:

This is part of the larger task of creating a User Name Server on z/OS.

Before you start

Before starting this task, you must have completed “Customizing the User Name Server component data set” on page 142.

All JCL has a standard header, comprising:

- A brief description of its function.
- A description where further information can be found, relating to the function of the JCL.
- If appropriate, a topic number.
- The section listing the JCL variables themselves.

Each JCL file defines its own STEPLIB. Some JCL files, for example BIPRELG, might require DB2 defined in the STEPLIB for a broker component. This must be removed from the JCL if the component is either a Configuration Manager or User Name Server, because it is not required.

You can customize the files using an ISPF edit macro that you have to tailor, or you can make changes to each of the PDSE members manually.

BIPEDIT is a REXX program that can be used to assist you in customizing your JCL. Once you have customized BIPEDIT you can run this REXX program against the other JCL files to change their JCL variables.

1. Customize the renamed BIPEDIT file. Use the information you collected in:
 - “Installation information - broker and User Name Server” on page 117
 - “Component information - User Name Server” on page 140
2. Activate the renamed BIPEDIT file before you customize any other JCL files. Do this by running the following TSO command:

```
ALTLIB ACTIVATE APPLICATION(EXEC) DA('COMPONENTDATASET')
```

where 'COMPONENTDATASET' is identical to ++COMPONENTDATASET++.

This command is active for the local ISPF session for which it was issued. Note that if you have split screen sessions, the other sessions are not able to use this. If you use ISPF option 6 to issue the command, use ISPF option 3.4 to edit the data set; this enables you to use the edit command.

3. Edit each JCL file. Run the renamed BIPEDIT exec by typing its name on the command line (for example MQ01EDUN). Instead of editing a member, you might want to View it until you have resolved any problems in your REXX program. Alternatively, you can Cancel the Edit session instead of saving it.

You must set a value for all the variables listed in the JCL; if you do not do so, the JCL will not work correctly.

Some JCL files include ++OPTIONS++ for a command, these **must** be replaced with additional optional parameters specific to the command on z/OS, or removed. It is likely that you will have to do this in addition to running BIPEDIT. If you do not require any additional options, remove ++OPTIONS++ using the following command:

```
"c ++OPTIONS++ ' ' all"
```

where ' ' represents two single quotation marks.

Save the edit macro and run this macro against all the members except the edit macro itself.

Do not set either of the optional pass parameters (-1 or -2) in BIPCRUN at this time because you want to create the registry and the WebSphere MQ queues.

When you update BIPUPROF (the User Name Server profile), the changes are not accessible until you run BIPGEN to copy the profile to the file system and create the ENVFILE. You must do this each time you update BIPUPROF for the changes to take effect.

You need to be aware that another process might be using the current ENVFILE, so you need to consider whether updating the current ENVFILE in the file system will have any impact.

Creating the User Name Server component:

This is part of the larger task of creating a User Name Server on z/OS.

Before you start

Before starting this task, you must have completed “Customizing the User Name Server JCL” on page 143.

If the user ID submitting the BIPCRUN command has the appropriate WebSphere MQ authorities, you can ignore the optional **mqsicreateusernameserver** parameters -1 and -2. If it is your intention to have a different administrator create the WebSphere MQ resources, you can consider using one of these optional parameters; see “mqsicreateusernameserver command” on page 305 for further information.

1. Submit job BIPCRUN with option -1. This job creates the User Name Server together with the files and directories which are placed in the registry. You must run this job first, and to do this you need authority to access the User Name Server.
2. Edit BIPCRUN and submit the job with option -2. This job creates the WebSphere MQ queues. If you do not have the requisite authority, ask your WebSphere MQ system administrator to run the job.
3. Ensure that the jobs have run successfully by:
 - Checking the STDOUT stream in the JOBLOG.
 - Viewing STDOUT for any errors and checking for BIP8071I: Successful command completion.

If you encounter any problems, delete the User Name Server and recreate it using the following procedure. Note that you need the appropriate authority to run the jobs.

1. Edit and configure job BIPDLUN.
2. Run job BIPDLUN with the same option, or options, that caused the problems when you ran the BIPCRUN job.
3. Correct the problems and run the BIPCRUN job again.

Copying the User Name Server started task to the procedures library:

This is part of the larger task of creating a User Name Server on z/OS.

Before you start

Before starting this task, you must have completed “Creating the User Name Server component” on page 144

Copy the Started Task JCL (BIPUNSP) to the procedures library, for example USER.PROCLIB.

Connecting the User Name Server to the WebSphere Event Broker network

This is part of the larger task of creating a User Name Server.

Before you start

On z/OS, to complete this task, you must have completed the following task:

- “Starting and stopping the User Name Server on z/OS” on page 219.

To enable communication between all the components, define and start WebSphere MQ channels between the following components:

- Configuration Manager, queue manager and the User Name Server queue manager.
- Configuration Manager and the broker queue manager.
- User Name Server queue manager and the broker queue managers.
- All brokers used in publish/subscribe.

You connect a User Name Server to another component in the same way as you connect the Configuration Manager to another component. This task is described in detail in “Connecting components” on page 153.

The Configuration Manager requests user IDs and group information from the User Name Server. The WebSphere Event Broker administrator defines Access Control Lists (ACLs) on the workbench. These ACLs are sent to each broker using WebSphere MQ channels following a deploy.

For further details of connecting your User Name Server to a broker and enabling Publish/Subscribe, refer to “Configuring Publish/Subscribe security.”

Configuring Publish/Subscribe security:

Refer to the following tasks:

- “Connecting the User Name Server to a broker”
- “Connecting the User Name Server to a broker on z/OS” on page 146
- “Starting the WebSphere MQ channels and listeners” on page 147
- “Enabling applications to use Publish/Subscribe” on page 149
- “Enabling applications to use Publish/Subscribe security on z/OS” on page 149

Connecting the User Name Server to a broker:

Before you start:

To complete this task, you must have completed the following task:

- “Creating a User Name Server” on page 136

You need to make the broker known to the User Name Server. You can do this using either of the following methods.

- Create a broker and specify `s=UserNameServerQueueManagerName` on the **mqscreatebroker** command.
- Change an existing broker using the **mqschangebroker** command.

If the User Name Server is not connected to the broker's queue manager, you need channels between the broker's queue manager and the User Name Server's queue manager. You need channels between the Configuration Manager queue manager and the broker's queue manager to receive message flows and Access Control Lists.

Change the Configuration Manager to use the queue manager name used by the User Name Server. You can use the **mqscreateconfigmgr** or **mqschangeconfigmgr** commands to set this value.

On the Topics panel in the workbench, you can view user information sent from the User Name Server.

Check that the User Name Server has registered the Configuration Manager. For more information on implementing topic-based security using the workbench, see "Enabling topic-based security" on page 23.

Example startup messages:

When a broker starts for the first time, and a User Name Server queue manager has been specified, and no response has ever been received from the User Name Server, you will receive the following message:

```
+BIP9141W  UserNameServer 0 The component was started.
```

When the User Name Server starts and indicates that it has registered with the broker, you will receive the following message:

```
18:17:18.54 BIP9141W: The component was started.
18:17:18.57 BIP2001I: The WebSphere Event Broker service has started, process ID 196827.
18:17:24.31 BIP8201I: User Name Server starting with refresh interval 60.
18:17:28.21 BIP8204I: User Name Server is registering a client with UUID
                  12345678-1234-1234-1234-123456789abc, and cache version 0.
```

Connecting the User Name Server to a broker on z/OS:

Before you start:

To complete this task, you must have completed the following task:

- "Creating a User Name Server on z/OS" on page 139

You need to make the broker known to the User Name Server. You can do this using either of the following methods.

- Create a broker and specify `-s UserNameServerQueueManagerName` on the **mqscreatebroker** command.
- Change an existing broker using the **mqschangebroker** command.

If the User Name Server is not connected to the broker's queue manager, you need channels between the broker's queue manager and the User Name Server's queue

manager. You need channels between the Configuration Manager queue manager and the broker's queue manager to receive message flows and Access Control Lists.

Check the z/OS console for the message BIP8204, which is issued when the User Name Server has successfully registered a client.

Change the Configuration Manager to use the queue manager name used by the User Name Server on z/OS, or another supported platform. You can use the **mqscreateconfigmgr** or **mqschangeconfigmgr** commands to set this value.

On the Topics panel in the workbench, you can view user information sent from the User Name Server.

Check that the User Name Server has registered the Configuration Manager. Also, check the z/OS console for message BIP8204, which is issued when the User Name Server has successfully registered a client. For more information on implementing topic-based security using the workbench, see "Enabling topic-based security" on page 23.

Example startup messages:

When a broker starts for the first time, and a User Name Server queue manager has been specified, and no response has ever been received from the User Name Server, you will receive the following message:

```
+BIP9141W  UserNameServer 0 The component was started.
```

When the User Name Server starts and indicates that it has registered with the broker, you will receive the following message:

```
18:17:18.54 BIP9141W: The component was started.
18:17:18.57 BIP2001I: The WebSphere Event Broker service has started, process ID 196827.
18:17:24.31 BIP8201I: User Name Server starting with refresh interval 60.
18:17:28.21 BIP8204I: User Name Server is registering a client with UUID
12345678-1234-1234-1234-123456789abc, and cache version 0.
```

Starting the WebSphere MQ channels and listeners:

This topic tells you how to start the channels and listeners on Linux, UNIX systems and Windows platforms.

To complete the connection between two components that are supported by different queue managers, start the server channels that you created in "Connecting the User Name Server to a broker on z/OS" on page 146.

Before you can do that, you need to start the WebSphere MQ listeners that are to receive the messages sent out from these channels.

Note: All the examples use port 1414, the default WebSphere MQ port. You **must** ensure that you use the port space in the channel definition and that this port is not in use by another application.

UNIX systems:

1. To start a listener enter the following command in a shell window:

```
runmqtsr -t tcp -p 1414 -m WBRK_QM
```
2. To start a sender channel, enter the following command in a shell window:

```
runmqchl -c BROKER.CONFIG -m WBRK_QM
```

LINUX systems:

- If you are using WebSphere MQ Version 6.0, listeners and channels can be started using the WebSphere MQ Explorer, in the same way as with Windows platforms, as described in “Windows platforms using WebSphere MQ Version 6.”
- If you are using WebSphere MQ Version 5, listeners and channels must be started by entering commands in a shell window, as described in this section.
 1. To start a listener, enter the following command in a shell window:

```
runmqtsr -t tcp -p 1414 -m WBRK_QM
```
 2. To start a sender channel, enter the following command in a shell window:

```
runmqchl -c BROKER.CONFIG -m WBRK_QM
```

Windows platforms using WebSphere MQ Version 6:

If you are using WebSphere MQ Version 6.0, start listeners and channels using WebSphere MQ Explorer.

1. To start a listener as a background task:
 - a. Click **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**.
 - b. In the left pane expand the queue manager, expand **Advanced**, and select **Listeners**
 - c. Right-click **Listeners** → **New** → **TCP Listener...**, enter a name for the listener, then click **Finish**. A new listener is created with transport type TCP and (default) port number 1414.
 - d. Right-click the new listener and click **Start** to start it.
2. To start the sender channels as background tasks using WebSphere MQ Explorer expand the queue manager, expand **Advanced**, and select **Channels**.
3. If you prefer, you can start listeners and channels as foreground tasks:
 - a. To start a listener, enter the following command on the command line:

```
runmqtsr -t tcp -p 1414 -m WBRK_CONFIG_QM
```
 - b. To start channels, enter the following commands:

```
runmqchl -m WBRK_UNQ_QM -c WBRK_UNQ_TO_BR
```

```
runmqchl -m WBRK_QM -c WBRK_BR_TO_UNQ
```

Windows platforms using WebSphere MQ Version 5:

If you are using WebSphere MQ Version 5, start the listeners using WebSphere MQ Services, and start channels by entering commands on the command line.

1. To start a listener as a background task:
 - a. Click **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Services**.
 - b. Expand the left pane and select the queue manager WBRK_CONFIG_QM to display its services in the right pane.
 - c. If the listener is displayed, right-click and select **All Tasks** → **Start** to start the listener.
 - d. If the listener is not displayed:
 - 1) Right-click the queue manager and select **New** → **Listener**. A new listener is created with (default) transport type TCP and (default) port number 1414.
 - 2) Right-click the new listener and select **Start** to start it.
2. If you prefer, you can start a listener as a foreground task. Enter the following command on the command line:

```
runmqtsr -t tcp -p 1414 -m WBRK_CONFIG_QM
```

3. To start the channels as foreground tasks, enter the following commands:

```
runmqchl -m WBRK_UNQ_QM -c WBRK_UNQ_TO_BR
```

```
runmqchl -m WBRK_QM -c WBRK_BR_TO_UN
```

Enabling applications to use Publish/Subscribe:

If WebSphere MQ queue security is enabled, users who want to subscribe need UPDATE authority to put to the SYSTEM.BROKER.CONTROL.QUEUE on the User Name Server's queue manager. Publish/Subscribe users also need UPDATE authority to allow them to use input and output queues in message flow nodes.

Enabling applications to use Publish/Subscribe security on z/OS:

This topic lists the steps that you need to complete to enable applications to use Publish/Subscribe security on z/OS.

- For the User Name Server on z/OS to extract user ID and group information from the External Security Manager (ESM) database, user IDs and groups must have an OMVS segment defined.
- To use publish/subscribe security, you need to have an ESM group defined called **mqbrkrs**. This group needs to have an OMVS segment defined. The user ID of the started task needs to be in this group.
- If you are using RACF, use the LG group OMVS command. For example:
LG MQBRKRS OMVS

User IDs:

- If you have suitable authorization, you can use the following RACF command to display OMVS information about a user:
LU id OMVS
- To give a user ID an OMVS segment, you can use the following RACF command if you have suitable authorization:
ALTUSER id OMVS(UID(XXX))

Groups:

- You can use the following RACF command to display OMVS information about a group if you have suitable authorization:
LG group OMVS
- To give a group an OMVS segment you can use the following RACF command if you have suitable authorization:
ALTGROUP id OMVS(GID(XXX))
Refer to the *OS/390 Security Server (RACF) Security Administrator's Guide* (or the appropriate documentation for an external security manager installed on the system) for details.

If an application tries to use publish/subscribe with security, and the user ID is not found by the User Name Server (either because the user ID does not exist or the user ID does not have an OMVS segment), the message BIP7017W is written to the SYSLOG.

If an application tries to use publish/subscribe with security, and the user ID is found by the User Name Server, but an access control list denies access to the topic, either of the following messages are written to SYSLOG:

```
BIP7025 User does not have permission to subscribe to a topic.
```

```
BIP7026 User does not have publish permission on a topic.
```

Using the Default Configuration wizard

Before you run the Default Configuration wizard:

- The Message Brokers Toolkit and all runtime components must be installed on this system. The Default Configuration wizard is available through the Message Brokers Toolkit, and is therefore available on Linux (x86 platform) and Windows only.
- You must have administration privileges on Windows, and your user ID must be a local ID (not a domain ID).
- A database must be available, and your user ID must be authorized to create databases:
 - On Linux (x86 platform) this must be DB2 Enterprise Server.
 - On Windows, this can be Derby or DB2 Enterprise Server.

The Default Configuration wizard allows you to set up a simple configuration on your local machine so that you can explore the product and run the samples that are supplied in the Samples Gallery. It also allows you to remove the default configuration, if it already exists, that has been set up on your logon account.

This topic contains the following sections:

- “Creating the default configuration”
- “Removing the default configuration” on page 151

Creating the default configuration

The wizard creates the following resources:

- A broker domain
 - A sample broker
 - A database to be used by the broker. The wizard defaults to whatever database manager is available and you are informed of the database manager used after it has been created in the **Default Configuration Summary** page. Details of the database manager are also written to the wizard’s log file.
 - A WebSphere MQ queue manager
1. On Windows, the Default Configuration wizard starts automatically at the end of the installation of WebSphere Event Broker. You can launch the wizard manually from the Message Brokers Toolkit **Welcome** page, which is displayed the first time that you launch the Message Brokers Toolkit. If the **Welcome** page is not displayed, open it in the Message Brokers Toolkit by clicking **Help** → **Welcome**.
 2. The **Welcome** panel of the wizard describes what is about to happen. Enter your password to log on and click **Next** to continue. You can click **Cancel** at any time to cancel the creation of the default configuration.
The wizard checks that the default configuration is not already installed.
 3. The **Default Configuration Summary** panel lists the resources that will be created. The information field in this panel confirms whether or not Derby has been set as the default broker database. It also suggests an alternative option of installing and configuring an enterprise database server instead. Click **Next** to continue.
 4. The **Default Configuration Progress** panel lists the background configuration actions as they happen and indicates successful completion. You can cancel the creation of the default configuration at this point by clicking **Cancel**. The wizard backs out all configuration tasks and the displays the progress and

success of the process. The configuration process is written to a log file in the Eclipse workspace directory *install_dir/eclipse/workspace/defaultConfiguration.log*.

If the default configuration is set up successfully, you see an appropriate message. If there are errors during the setup of the default configuration, you see an appropriate message and the wizard backs out all configuration tasks. If an error occurs during the back out process, the wizard displays a list of resources that you must remove manually.

5. You can use the samples to verify the default configuration. The **Launch Samples Wizard when finished** check box is selected by default. Click **Finish** to launch the Prepare the Samples wizard.

If you do not need to launch the Prepare the Samples wizard, clear the **Launch Samples Wizard when finished** check box before clicking **Finish**.

If you are viewing this information from within the Message Brokers Toolkit, launch the samples manually by clicking Soccer Results sample. Alternatively, click **Help** → **Samples Gallery**, and expand **Application samples** → **Message Broker - Getting Started samples**.

Removing the default configuration

1. Launch the Default Configuration wizard from the Message Brokers Toolkit **Welcome** page, which is displayed after you launch the Message Brokers Toolkit. If the **Welcome** page is not displayed, open it in the Message Brokers Toolkit by clicking **Help** → **Welcome**.

2. The **Welcome** panel of the wizard describes what is about to happen. Enter your password to log on and click **Next** to continue. You can click **Cancel** at any time to cancel the removal of the default configuration.

The wizard checks that the default configuration is already installed.

3. The **Remove Default Configuration Summary** panel lists the resources that will be removed. Click **Next** to continue.

4. The **Default Configuration Progress** panel lists the removal actions as they happen and indicates successful completion. The removal process is written to a log file in the Eclipse workspace directory *install_dir/eclipse/workspace/defaultConfiguration.log*.

5. A message confirms that the default configuration has been removed successfully. Click **Finish** to close the wizard.

If errors occur during the removal of the default configuration, the wizard displays the errors and also writes them to the log file. Follow the advice in the log and retry each step.

If you experience problems using the wizard to remove the default configuration, you might need to remove the default configuration manually.

Using the Command Assistant wizard

Before you start:

- The Message Brokers Toolkit and all runtime components must be installed on this system. The Command Assistant wizard is available through the toolkit, and is available on Windows only.
- You must have administration privileges.

Use the Command Assistant wizard to create, modify, and delete the following physical runtime components:

- Brokers

- Configuration Managers
- User Name Servers

Using the wizard, you access the equivalent command line command through a graphical interface:

- “mqsicreatebroker command” on page 286, “mqsicreateconfigmgr command” on page 296, and “mqsicreateusernameserver command” on page 305
- “mqsichangebroker command” on page 250, “mqsichangeconfigmgr command” on page 256, and “mqsichangeusernameserver command” on page 279
- “mqsideletebroker command” on page 311, “mqsideleteconfigmgr command” on page 313, and “mqsideleteusernameserver command” on page 318

The wizard consists of a series of panels that lead you through the task you want to complete. The wizard provides help in the banner at the top of each panel, which indicates what actions you should take to complete the panel and continue. Not every optional parameter on each of these commands is supported through the wizard; if you are using some of the more advanced features (for example, setting or modifying LDAP directory access for a broker), you must use the command line interface.

Use the buttons displayed at the bottom of each panel to move **Back** to the previous panel, to move to the **Next** panel, to **Finish** working with the wizard, or to **Cancel** the current action and end the wizard.

1. Switch to the Broker Application Development perspective or the Broker Administration perspective.
2. Select **File** → **New** → **Other**. The **New** dialog opens.
3. Select **Command Assistant Wizard** within the **Broker Administration - Getting Started** category and click **Next**. The wizard opens and displays its first panel.
4. Select the type of component that you want to work with. The wizard checks which components have been installed on this system. You must select a value from the available list; you cannot enter a different value.
5. Navigate to the **Name** input field. If the wizard has found any existing components of the type you entered, it shows these in this field. If there are no existing components of this type, or you want to create a new component, enter a new unique name in this field, following the naming restrictions enforced by the product and any naming conventions that are in use in your environment.

The name of a resource is case insensitive. If a resource of the same name exists, but with characters in a different case to those you typed into this field, the name you typed is overwritten with the existing name.

6. Navigate to the **Action** input field and choose the action you want to complete. The wizard prevents you from entering an invalid action for the resource you have entered in the **Name** field. For example, if you have entered a name that the wizard has not found on this system, you can only choose to create a new resource. If the resource already exists, you can choose to modify it or to delete it.
7. If you have more than one installation of the product on this system, you must also select the correct value in the **Location** field. This field displays the home directory of the installation identified by the wizard:
 - If there is only one installation on this system, the directory is displayed and the field is greyed out.

- If you have specified an existing, uniquely named, resource in the **Name** field, the wizard displays the location of the installation associated with that resource and the field is greyed out.
 - If more than one installation exists, and could be the target for your request, you must select the correct location in this field,
8. Click **Next**. The wizard displays the next panel, the content of which depends on your choices so far.
Use the help displayed by the wizard on each panel, and navigate through the entry fields, selecting or entering text where appropriate.
If you enter a password, the characters are displayed as asterisk characters in the entry field to increase security.
 9. When you have completed the entry field on the panel, click **Next**. The wizard displays a summary that shows you the commands that will be invoked, and any additional actions that will be taken.
 10. Check the information in the summary; if it is correct, click **Next**.
If you want to change anything, click **Back** to return to a previous panel and change your input.
 11. The wizard starts processing your request. If the action succeeds, the wizard displays messages in the summary panel.
If an action fails, the wizard reports the error in a message dialog. If you know what is causing the error, and can fix it, correct the error and click **Yes**. The wizard reissues the command.
If you do not know what is causing the error, or you cannot fix it, click **No**. The wizard backs out any actions that have already completed and returns your system to its initial state.
 12. Click **Finish** to end the wizard, or click **Next** to return to the first page and select another task to complete.

Verifying components

To verify that the WebSphere Event Broker components that you have created exist, use the **mqsilist** command. On the command line type:

```
mqsilist
```

Note, that on z/OS it is not possible to display all the components.

If you do not specify any parameters when you issue this command, a list of components and queue manager names is displayed for each component created on this system, in the form:

```
BIP8099I: Broker: brokername - queuemanagename
BIP8099I: UserNameServer: UserNameServer - queuemanagename
BIP8099I: ConfigMgr: configmgrname - queuemanagename
BIP8071I: Successful command completion
```

Connecting components

Before you start:

To complete this task, you must have completed the following tasks:

- “Creating a Configuration Manager” on page 125
- “Creating a broker” on page 108
- “Creating a User Name Server” on page 136

Complete the steps below to make connections between the Configuration Manager, brokers, and the User Name Server.

If components in your broker domain are supported by different queue managers, establish WebSphere MQ connections between those queue managers to enable messages to be exchanged. It is important that each broker is able to exchange messages with the User Name Server that provides user name services for the broker.

If your broker domain components all run on the same system, and use a single queue manager, you do not need to create any WebSphere MQ connections between your brokers.

To achieve the required connection, complete the following steps. All the steps here are illustrated with MQSC examples. You can use any appropriate method for defining these resources. These examples assume that the queue managers are called COMP1 and COMP2.

The value of 104857600 for `maxmsgl` in the following steps is merely an example. You are recommended to check the appropriate WebSphere MQ documentation to confirm the value for `maxmsgl` that you can use on your particular platforms.

In addition, note that you have to set the `maxmsgl` attribute only on the transmission queue that sends messages from the Configuration Manager's queue manager to the broker's queue manager.

1. Define a transmission queue on each component's queue manager. These queues will collect messages ready for transmission between components. Give the transmission queue the same name as the queue manager to which it transmits messages (that is COMP1 and COMP2 for this example). In addition, set the `maxmsgl` attribute to its maximum value.

For example, on queue manager COMP1:

```
define qlocal('COMP2') usage(XMITQ) maxmsgl (104857600) replace
```

and on queue manager COMP2:

```
define qlocal('COMP1') usage(XMITQ) replace
```

2. Define the channels for the connection. Use sender-receiver pairs of channels for all two-way communications between queue managers that host WebSphere Event Broker components.

- a. Define the sender channel on the first component's queue manager (Sender(3)). This will transport messages sent by the first component to the second component.

Allocate connection names according to your WebSphere MQ network conventions, and specify the protocol that you are using for this connection and the port on which the listener is listening.

For example, on queue manager COMP1:

```
define channel('COMP1_TO_COMP2') chltype(sdr) trptype(tcp)
conname('WBRKSYS1(1415)') xmitq('COMP2')
maxmsgl (104857600) replace
```

- b. Define a receiver channel on the first component's queue manager (Receiver(2)). Messages sent by the second component to the first will be received by this channel.

This receiver channel must have the same name as the sender channel on COMP2, defined in Step 2c. For example, on queue manager COMP1:

```
define channel('COMP2_TO_COMP1') chltype(rcvr) trptype(tcp)
maxmsgl (104857600) replace
```

- c. Define the sender channel on the second component's queue manager (Sender(1)). This will transport messages sent by the second component to the first component.

Allocate connection names according to your WebSphere MQ network conventions, and you must specify the protocol you are using for this connection.

For example, on queue manager COMP2:

```
define channel('COMP2_TO_COMP1') chltype(sdr) trdtype(tcp)
conname('WBRKSYS1(1414)') xmitq('COMP1')
maxmsgl (104857600) replace
```

- d. Define a receiver channel on the second component's queue manager (Receiver(4)). Messages sent by the first component to the second will be received by this channel.

This receiver channel must have the same name as the sender channel on COMP2, defined in Step 2a. For example, on queue manager COMP2:

```
define channel('COMP1_TO_COMP2') chltype(rcvr) trdtype(tcp)
maxmsgl (104857600) replace
```

3. Create and start a listener for each protocol in use.
4. Start the sender channels (1) and (3) on the respective queue managers. You can set up channel initiators for these channels. This reduces overhead by allowing the channels to stop when there is no message traffic, but ensures automatic startup when there are messages to transport.

You can set up a single receiver channel on the Configuration Manager's queue manager to support all sender channels created for the brokers. This requires a single definition on the Configuration Manager and a single sender definition on each broker, which must have the same name on each broker. You can also use this receiver channel on the Configuration Manager to support communications from the User Name Server.

All WebSphere MQ connections between WebSphere Event Broker components, and between clients and WebSphere Event Broker components, can be set up using any of the communications protocols supported by WebSphere MQ (TCP/IP and SNA on all operating systems; also, NetBIOS and SPX on Windows).

Modifying a broker

Before you start:

You must complete the following tasks:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to "Security requirements for administrative tasks" on page 423
- "Creating a broker" on page 108
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before performing this task, by running the product profile or console; refer to Setting up a command environment

Modify a broker using the command line on the system where the broker component is installed. On Windows, you can also use the Command Assistant to complete this task.

The parameters you can change on the broker affect the physical broker, created using the command line.

You can also modify the broker reference in the workbench, where it is possible to change broker properties, such as multicast properties.

Follow the link for the appropriate platform.

- “Modifying a broker on Linux and UNIX systems”
- “Modifying a broker on Windows” on page 157
- “Modifying a broker on z/OS” on page 158

Modifying a broker on Linux and UNIX systems

To modify a broker on Linux and UNIX systems:

1. Stop the broker using the **mqsistop** command.
2. Enter the **mqsichangebroker** command with the parameters that you want to change: `mqsichangebroker brokername <<-i ServiceUserID> -a ServicePassword> <-p DatabaseSourcePassword> <-s UserNameServerQueueManagerName> <-j | -d> <-t | -n> <-l UserLilPath> <-g ConfigurationTimeout> <-k ConfigurationDelayTimeout> <-v StatisticsMajorInterval> <-P HttpPort>` where:

brokername

Is the broker name.

- i** Is the service user ID that is used to run the broker.
- a** Is the password for the broker user ID.
- p** Is the password for the broker’s database user ID.
- s** Is the WebSphere MQ queue manger for the User Name Server
- j** Indicates that publish/subscribe access control is to be enabled for this broker.
- d** Indicates that publish/subscribe access control is to be disabled for this broker.
- t** Indicates that the broker runs as a WebSphere MQ trusted application (not supported on AIX)
- n** Indicates that the broker should cease to run as a WebSphere MQ trusted application.
- l** Indicates from where LIL (loadable implementation libraries) files are loaded.
- g** Is the maximum time (in seconds) to allow a broker to process a deployed message.
- k** Is the maximum time (in seconds) to allow a broker to process a minimum size deployed message.
- v** Is the time (in minutes) for the duration of the interval for collecting statistics archive records.
- P** Is the port that the broker HTTP listener will use.

For example, to change the user ID that is used to run the broker, enter the following command at the command prompt:

```
mqsichangebroker WBRK_BROKER -i wbrkuid -a wbrkpw
```

3. Restart the broker using the **mqsistart** command. The broker restarts with the new properties.

If you cannot change a property using **mqsichangebroker**, delete the broker and then create a new one with the new properties.

Modifying a broker on Windows

To modify a broker on Windows:

1. Stop the broker using the **mqsistop** command.
2. Enter the **mqsichangebroker** command with the parameters that you want to change:

```
mqsichangebroker brokername <<-i ServiceUserID> -a ServicePassword>  
<-p DatabaseSourcePassword> <-s UserNameServerQueueManagerName>  
<-j | -d> <-t | -n> <-l UserLilPath> <-g ConfigurationTimeout>  
<-k ConfigurationDelayTimeout> <-v StatisticsMajorInterval> <-P HttpPort>
```

where:

brokername

Is the broker name.

- i** Is the service user ID that is used to run the broker.
- a** Is the password for the broker user ID.
- p** Is the password for the broker's database user ID.
- s** Is the WebSphere MQ queue manger for the User Name Server
- j** Indicates that publish/subscribe access control is to be enabled for this broker.
- d** Indicates that publish/subscribe access control is to be disabled for this broker.
- t** Indicates that the broker runs as a WebSphere MQ trusted application.
- n** Indicates that the broker should cease to run as a WebSphere MQ trusted application.
- l** Indicates from where LIL (loadable implementation libraries) files are loaded.
- g** Is the maximum time (in seconds) to allow a broker to process a deployed message.
- k** Is the maximum time (in seconds) to allow a broker to process a minimum size deployed message.
- v** Is the time (in minutes) for the duration of the interval for collecting statistics archive records.
- P** Is the port that the broker HTTP listener will use.

For example, to change the user ID that is used to run the broker, enter the following command at the command prompt:

```
mqsichangebroker WBRK_BROKER -i wbrkuid -a wbrkpw
```

3. Restart the broker using the **mqsistart** command. The broker restarts with the new properties.

If you cannot change a property using **mqsichangebroker**, delete the broker and then create a new one with the new properties.

Modifying a broker on z/OS

Before you start:

To complete this task, you must have completed the following task:

- “Creating a broker on z/OS” on page 116

To modify a broker:

1. Ensure that the broker is running
2. Stop the broker components by issuing the command `/F BROKERNAME, PC`.
3. When it has stopped, use the MVS `MODIFY` command with the `changebroker` parameters that you want to change. For example:

```
/F <BROKERNAME>,cb g=100,k=200
```

4. Restart the broker components by issuing the following command `/F BROKERNAME, SC`

The broker now uses the changed parameters.

You cannot change all the parameters with which you created a broker. If you cannot modify a parameter that you need to change using the `changebroker` command, delete the broker and then create a new one. This will allow you to redefine all the parameters.

The parameters that you can change are:

g	ConfigurationTimeOut
k	ConfigurationDelayTimeout
s	UserNameServerQueueManagerName
l	UserLilPath
v	StatisticsArchiveInterval
P	HTTPPort

See “`mqsichangebroker` command” on page 250 for further information on these parameters.

Modifying a Configuration Manager

Before you start:

You must complete the following tasks:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423
- “Creating a Configuration Manager” on page 125
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before performing this task, by running the product profile or console; refer to Setting up a command environment

Modify a Configuration Manager using the command line on the system where the Configuration Manager component is installed. On Windows, you can also use the Command Assistant to complete this task.

Parameters that are required in order to start, stop and migrate the Configuration Manager (such as the service user ID and password, and the connection parameters to a configuration database for migration) can be modified only by using the command line on the system where the Configuration Manager component is installed.

Parameters that control a running Configuration Manager or domain (such as the set of broker references stored in the Configuration Manager) can be modified using the Message Brokers Toolkit or a Configuration Manager Proxy application, which might or might not be on the same machine as the Configuration Manager component.

Follow the link for the appropriate platform.

- “Modifying a Configuration Manager on Linux and UNIX systems”
- “Modifying a Configuration Manager on Windows” on page 160
- “Modifying a Configuration Manager on z/OS” on page 160

If you need to transfer the Configuration Manager onto another queue manager, follow the steps described in “Moving the Configuration Manager to a new queue manager” on page 161.

Modifying a Configuration Manager on Linux and UNIX systems

The following steps show you how to modify a Configuration Manager’s service user ID, service password, database password, User Name Server queue manager, and the maximum JVM heap size, on Linux and UNIX systems:

1. Stop the Configuration Manager using the **mqsistop** command.
2. Enter the **mqsichangeconfigmgr** with the parameters you want to change:

```
mqsichangeconfigmgr configmgrName <<-i ServiceUserID> -a ServicePassword>  
<-p DatabasePassword> <-s UserNameServerQueueManagerName> <-j MaxJVMHeapSize>
```

where:

configmgrName

Is the Configuration Manager name.

-i Is the service user ID that is used to run the Configuration Manager.

-a Is the password for the Configuration Manager user ID.

-p If an existing DB2 database from a previous version of the product has not yet been migrated, use this option to set the password used to access the database.

-s Is the WebSphere MQ queue manger for the User Name Server.

-j Is the maximum Java virtual machine heap size, in megabytes (minimum 64).

For example, to modify the Configuration Manager so that it can communicate with the User Name Server, enter the following command at the command prompt:

```
mqsichangeconfigmgr CMGR01 -s WBRK_UNQ_QM
```

3. Restart the Configuration Manager using the **mqsistart** command. The Configuration Manager restarts with the new properties.

If you cannot change a property, delete the Configuration Manager then create a new one with the new property. Creating a new Configuration Manager does not

cause any loss of data as long as the previous Configuration Manager's database tables were not deleted (for example, by specifying the **-n** parameter on the **mqsdeleteconfigmgr** command).

Modifying a Configuration Manager on Windows

The following steps show you how to modify a Configuration Manager's service user ID, service password, database password, User Name Server queue manager, and the maximum JVM heap size, on Windows:

1. Stop the Configuration Manager using the **mqsistop** command.
2. Enter the **mqsichangeconfigmgr** with the parameters you want to change:
`mqsichangeconfigmgr configmgrName <<-i ServiceUserID> -a ServicePassword>
<-p DatabasePassword> <-s UserNameServerQueueManagerName> <-j MaxJVMHeapSize>`

where:

configmgrName

Is the Configuration Manager name. This is optional.

- i** Is the service user ID that is used to run the Configuration Manager.
- a** Is the password for the Configuration Manager user ID.
- p** If an existing DB2 database from a previous version of the product has not yet been migrated, use this option to set the password used to access the database.
- s** Is the WebSphere MQ queue manager for the User Name Server.
- j** Is the maximum Java virtual machine heap size, in megabytes (minimum 64).

For example, to modify the Configuration Manager so that it can communicate with the User Name Server, enter the following command at the command prompt:

```
mqsichangeconfigmgr CMGR01 -s WBRK_UNQ_QM
```

3. Restart the Configuration Manager using the **mqsistart** command. The Configuration Manager restarts with the new properties.

If you cannot change a property, delete the Configuration Manager then create a new one with the new property. Creating a new Configuration Manager does not cause any loss of data as long as the previous Configuration Manager's database tables were not deleted (for example, by specifying the **-n** parameter on the **mqsdeleteconfigmgr** command).

Modifying a Configuration Manager on z/OS

Before you start:

To complete this task, you must have completed the following task:

- "Creating a Configuration Manager on z/OS" on page 130

The following steps show you how to modify a Configuration Manager's database password, User Name Server queue manager, and the maximum JVM heap size:

1. At the command prompt, issue the **stopcomponent** command to stop the Configuration Manager.
2. When it has stopped, use the **MODIFY** command with the **changeconfigmgr** parameters that you want to change. Note that you can abbreviate **changeconfigmgr** to **cc**. For example:

```
MODIFY <configurationmanagername>,changeconfigmgr s=WBRK_UNQ_QM
```

3. At the command prompt issue the `startcomponent` command.
The Configuration Manager now uses the changed parameters.

You cannot change all the parameters with which you created a Configuration Manager. If you cannot modify a parameter that you need to change using the `changeconfigmgr` command, delete the Configuration Manager and then create a new one. This will allow you to redefine all the parameters.

The parameters that you can change are:

- s=** Is the WebSphere MQ queue manager for the User Name Server.
- j=** Is the maximum Java virtual machine heap size, in megabytes (minimum 64).

See “`mqsichangeconfigmgr` command” on page 256 for further information on these parameters.

Moving the Configuration Manager to a new queue manager

The following steps show you how to move the Configuration Manager to a new queue manager that is on the same computer or on a different computer:

1. Use the `mqsicreateconfigmgr` command to create a new Configuration Manager that uses the new queue manager. Do not specify a database name.
2. If possible, stop all brokers in the domain using the `mqsistop` command.
3. Stop the original Configuration Manager using the `mqsistop` command.
4. Back up the original Configuration Manager using the `mqsibackupconfigmgr` command.
5. On the computer that contains the new Configuration Manager, use the `mqsirestoreconfigmgr` command to overwrite the new Configuration Manager’s repository with the one that you backed up.
6. Start the new Configuration Manager using the `mqsistart` command.
7. Perform a complete deployment of the topology, using the Message Brokers Toolkit, the `mqsideploy` command, or the Configuration Manager Proxy. This tells all the brokers in the domain to associate themselves with the new Configuration Manager.
8. If you stopped the brokers in the domain in Step 2, start them using the `mqsistart` command as soon as deployment is initiated, so that the deployments can now be processed.
9. If it was not possible to stop the brokers in Step 2, ensure that any messages on the original Configuration Manager’s queue manager’s `SYSTEM.BROKER.ADMIN.QUEUE` are transferred manually to the new Configuration Manager’s queue manager’s `SYSTEM.BROKER.ADMIN.QUEUE`. This is the queue that brokers use to communicate their status to the Configuration Manager and if any status change event occurred between stopping the original Configuration Manager in Step 3 and the complete deployment in Step 7, any messages that report a change in status will have been sent to the old Configuration Manager.

Modifying a User Name Server

Before you start:

You must complete the following tasks:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423
- “Creating a User Name Server” on page 136
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before performing this task, by running the product profile or console; refer to Setting up a command environment

Modify a User Name Server using the command line on the system where the User Name Server component is installed. On Windows, you can also use the Command Assistant to complete this task.

Follow the link for the appropriate platform.

- “Modifying a User Name Server on Linux and UNIX systems”
- “Modifying a User Name Server on Windows” on page 163
- “Modifying a User Name Server on z/OS” on page 163

Modifying a User Name Server on Linux and UNIX systems

To modify a User Name Server on Linux and UNIX systems; AIX, HP-UX, Linux (zSeries platform), Linux (x86 platform) and Solaris:

1. Stop the User Name Server using the **mqsistop** command.
2. Enter the **mqsichangeusernameserver** command with the parameters that you want to change: `mqsichangeusernameserver <<-i ServiceUserID> <-a ServicePassword> <-d SecurityDomainName> <-r RefreshInterval> <-g AuthProtocolDataSource> <-j` | -o> where:`

- i** Is the service user ID that is used to run the User Name Server
- a** Is the password for the User Name Server user ID.
- d** Is the security domain that the User Name Server uses on the Windows platform.
- r** Is the number of seconds between each refresh of the User Name Server internal cache.
- j** Indicates that groups and group memberships are defined in the data source for the authentication protocol, rather than being drawn from the operating system.
- o** Indicates that groups and group memberships are drawn from the operating system, rather than being defined in the data source for the authentication protocol.
- g** Is the name of the data source required by the authentication protocol.

For example, to change the number of seconds between each refresh of the User Name Server internal cache, enter the following command at the command prompt:

```
mqsichangeusernameserver -r 2000
```

3. Restart the User Name Server using the **mqsistart** command. The User Name Server restarts with the new properties.

If you cannot change a property using **mqsichangeusernameserver**, delete the User Name Server and then create a new one with the required properties.

Modifying a User Name Server on Windows

To modify a User Name Server:

1. Stop the User Name Server using the **mqsistop** command.
2. Enter the **mqsichangeusernameserver** command with the parameters you want to change:

```
mqsichangeusernameserver <<-i ServiceUserID> <-a ServicePassword>  
<-d SecurityDomainName> <-r RefreshInterval> <-k AuthProtocolType>  
<-j AuthProtocolModule> <-g AuthProtocolDataSource>
```

where:

- i Is the service user ID that is used to run the User Name Server
- a Is the password for the User Name Server user ID.
- d Is the security domain that the User Name Server uses.
- r Is the number of seconds between each refresh of the User Name Server internal cache.
- k Indicates that the authentication protocol is supported by brokers.
- j Indicates that the authentication services product library is to be used.
- g Indicates the name and location of the password file used to source any protocol related information.

For example, to change the number of seconds between each refresh of the User Name Server internal cache, enter the following command at the command prompt:

```
mqsichangeusernameserver -r 2000
```

3. Restart the User Name Server using the **mqsistart** command. The User Name Server restarts with the new properties.

If you cannot change a property using **mqsichangeusernameserver**, delete the User Name Server and then create a new one with the new properties.

Modifying a User Name Server on z/OS

Before you start:

To complete this task, you must have completed the following task:

- “Creating a User Name Server on z/OS” on page 139

To modify a User Name Server.

1. At the command prompt issue the stopcomponent command to stop the User Name Server.
2. When it has stopped, use the MODIFY command with the changeusernameserver parameters that you want to change. For example:

```
MODIFY <usernameserver>,changeusernameserver r=2000
```
3. At the command prompt issue the startcomponent command.
The User Name Server now uses the changed parameters.

You cannot change all the parameters with which you created the User Name Server: if you cannot modify a parameter that you need to change using the changeusernameserver command, delete the User Name Server and then create a new one. This will allow you to redefine all the parameters.

Modifying component database access

Set the user ID through which a broker accesses its database tables by using the `DataSourceUserID` parameter on the `mqsicreatebroker` command.

You cannot modify this parameter once the component has been created. Therefore you must save the database tables, delete the component, and create a new one, specifying the new user ID. The new component uses the data in the saved tables, with the updated database user ID.

To ensure that you preserve the data held in these databases, follow the steps detailed in the following task.

“Modifying broker database access”

Modifying broker database access

Set the user ID through which the broker accesses its database tables by using the `DataSourceUserID` parameter on the `mqsicreatebroker` command.

You cannot modify this parameter using the `mqsichangebroker` command. You have to delete the broker and create a new one, specifying the new user ID.

To ensure that you do not lose any of the data in the broker database when performing this task, complete the following steps.

- Back up the database tables. These are listed in “`mqsicreatebroker` command” on page 286.
- Delete the broker, following the “Deleting a broker” on page 166 task.
- Restore the database tables to the new location.
- Create a new broker, following the “Creating a broker” on page 108 task. Specify the new user ID when you create the new broker.

The new broker uses the database tables with the new user ID

Moving from WebSphere Event Broker on a distributed platform to z/OS

Recommendations on how to define resources for WebSphere Event Broker for z/OS are given in the following topics:

- “z/OS customization overview” on page 62
- “Customizing the z/OS environment” on page 60
- “Creating a broker on z/OS” on page 116
- “Creating a User Name Server on z/OS” on page 139
- “Creating a Configuration Manager on z/OS” on page 130
- “Administration in z/OS” on page 368

Taking these into account, recreate your broker and User Name Server resources on z/OS and deploy your message flows and execution groups to a WebSphere Event Broker for z/OS broker. If you have extended WebSphere Event Broker in a distributed environment with user-defined parsers or message processing nodes, port them to run under z/OS.

Also consider the following points:

- Floating point conversion: z/OS runs under z/OS floating point format, so floating point operations on z/OS run in a different range and accuracy from distributed platforms.
- Administration commands are partially implemented as console commands and partially as JCL commands.
- Event log messages: All address spaces have a JOBLOG where messages appear. In addition to this, all messages appear on the SYSLOG, with important operator messages being filtered to the console through MPF (Message Processing Facility).

Moving user applications

You can write your own applications to work with WebSphere Event Broker. If these applications use the common subset of functionality of all WebSphere Event Broker brokers, no migration is necessary. If you are using functionality that is available on some WebSphere Event Broker platforms only, for example message segmentation and WebSphere MQ message groups, be aware that WebSphere Event Broker for z/OS does not provide support for this migration.

Deleting an execution group from a broker using the command line

Before you start:

You must complete the following tasks:

- “Adding an execution group to a broker using the command line” on page 123

Instead of employing the Message Brokers Toolkit, you can use this task as an alternative method of deleting an execution group .

For more details on deleting an execution group from the Message Brokers Toolkit see “Deleting an execution group” on page 181

To delete an execution group from a broker using the command line:

1. Open a command prompt that has the environment configured for WebSphere Event Broker Version 6.0.
2. Enter the following command to delete the execution group:
`mqsideleteexecutiongroup -i host -p 1414 -q QMGR -b BROKER -e EG1`

where

host Is the host name or IP address of the Configuration Manager for the domain on which the broker resides.

1414 Is the port on which the Configuration Manager’s queue manager is listening.

QMGR Is the name of the Configuration Manager’s queue manager.

BROKER Is the name of the broker.

EG1 Is the name of the execution group that you want to delete.

On completion of this task, the execution group is no longer running on the specified broker. In addition, any message flows that were running on the execution group are no longer running.

Deleting a broker

Before you start:

You must complete the following tasks:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423
- Remove the broker from the broker domain in the workbench (“Removing a broker from a broker domain” on page 178).

Delete a broker using the command line on the system where the broker component is installed. On Windows, you can also use the Command Assistant to complete this task.

On Windows, UNIX systems, and Linux, you must set up your command-line environment before deleting a broker, by running the product profile or console; refer to Setting up a command environment.

You can remove the broker from the broker topology using the workbench, but the physical broker will not be deleted until the broker is physically deleted from the command line.

Follow the link for the appropriate platform.

- “Deleting a broker on Linux and UNIX systems”
- “Deleting a broker on Windows”
- “Deleting a broker on z/OS” on page 167

Deleting a broker on Linux and UNIX systems

To delete a broker on Linux and UNIX systems:

1. Stop the broker using the **mqsistop** command.
2. Enter the following command to delete the broker:

```
mqsdeletebroker WBRK_BROKER
```

where:

WBRK_BROKER is the broker name.

On completion of this task, you have:

- Removed the broker’s data from the database.
- Removed the record for the component in the broker registry. It is therefore removed from the list of components displayed by issuing the **mqsilist** command.

Deleting a broker on Windows

To delete a broker:

1. Stop the broker using the **mqsistop** command.
2. Enter the following command to delete the broker:

```
mqsdeletebroker WBRK_BROKER
```

where:

WBRK_BROKER is the broker name.

On completion of this task, you have:

- Stopped the Windows service that runs the broker.
- Removed the broker's data from the database.
- Removed the record for the component in the broker registry. It is therefore removed from the list of components displayed by issuing the **mqsilist** command.

Deleting a broker on z/OS

To delete a broker:

1. Remove the broker from the broker domain, in the workbench. Refer to "Removing a broker from a broker domain" on page 178.
2. Stop the broker, by stopping the started task.
3. Customize and submit the following delete jobs in your component PDSE to delete WebSphere MQ and DB2 definitions:

Delete jobs	Description
BIPDLBK	Delete component including WebSphere MQ broker queues and channels and rows in the DB2 database
BIPDLDB	Drop the broker DB2 database, storage group and table spaces.

Note:

- a. Not all files are deleted from the component directory in the file system.
- b. When the BIPDLDB job drops the broker DB2 database, it also deletes any Image Copy references to itself that you currently have. If you restore the broker in future you need to reinstate the Image Copy references.

Deleting a Configuration Manager

Before you start:

Ensure that your user ID has the correct authorizations to perform the task. Refer to "Security requirements for administrative tasks" on page 423

Delete a Configuration Manager using the command line on the system where the Configuration Manager component is installed. On Windows, you can also use the Command Assistant to complete this task.

On Windows, UNIX systems, and Linux, you must set up your command-line environment before deleting a Configuration Manager, by running the product profile or console; refer to Setting up a command environment.

Follow the link for the appropriate platform:

- "Deleting a Configuration Manager on Linux and UNIX systems" on page 168
- "Deleting a Configuration Manager on Windows" on page 168

- “Deleting a Configuration Manager on z/OS” on page 169

Deleting a Configuration Manager on Linux and UNIX systems

You delete the Configuration Manager using the command line. The Configuration Manager can be deleted only from the system where the Configuration Manager component is installed.

You can delete a Configuration Manager without also deleting your domain connection parameters in the workbench. If you want to delete a Configuration Manager and create a new one, you can keep your connection parameters in the workbench, even if you specify different parameters when creating the new Configuration Manager. When you reconnect to your domain in the workbench your new settings are displayed.

To delete a Configuration Manager on Linux and UNIX systems:

1. Stop the Configuration Manager using the “mqsisstop command” on page 362 command.
2. Delete the Configuration Manager using the “mqsideleteconfigmgr command” on page 313 command.

On completion of this task, you have:

- Removed the record for the component in the broker registry. It is therefore removed from the list of components displayed by issuing the “mqsilist (list resources) command” on page 328 command.
- Preserved all internal data associated with the Configuration Manager, unless you specify the -n parameter on the “mqsideleteconfigmgr command” on page 313 command.

Deleting a Configuration Manager on Windows

You delete the Configuration Manager using the command line. The Configuration Manager can be deleted only from the system where the Configuration Manager component is installed.

You can delete a Configuration Manager without also deleting your domain connection parameters in the workbench. If you want to delete a Configuration Manager and create a new one, you can keep your connection parameters in the workbench, even if you specify different parameters when creating the new Configuration Manager. When you reconnect to your domain in the workbench your new settings will be displayed.

To delete a Configuration Manager:

1. Stop the Configuration Manager using the “mqsisstop command” on page 362 command.
2. Delete the Configuration Manager using the “mqsideleteconfigmgr command” on page 313 command.

On completion of this task, you have:

- Stopped the Windows service that runs the Configuration Manager.
- Removed the record for the component in the broker registry. It is therefore removed from the list of components displayed by issuing the “mqsilist (list resources) command” on page 328 command.

- Preserved all internal data associated with the Configuration Manager, unless you specify the `-n` parameter on the “`mqsdeleteconfigmgr` command” on page 313 command.

Deleting a Configuration Manager on z/OS

To delete a Configuration Manager:

1. Stop the Configuration Manager, by stopping the started task.
2. Customize and submit the following delete jobs in your component PDSE to delete WebSphere MQ definitions:

Delete jobs	Description
BIPDLCM	Delete component including WebSphere MQ broker queues and channels.

Note that not all files are deleted from the component directory in the file system.

Disabling a User Name Server

When you delete a User Name Server you disable publish/subscribe services within the broker domain.

To delete a User Name Server from the broker domain, remove the connections between the broker, Configuration Manager, and User Name Server. This ensures that the broker and Configuration Manager do not continue to communicate with the User Name Server.

Modify the broker and Configuration Manager using the `mqsichangebroker` and `mqsichangeconfigmgr` commands, before you delete the User Name Server. The following steps show you how to do this.

- Modify the broker by removing the reference to the queue manager for the User Name Server. Use the `mqsichangebroker` command to modify the `-s` and `-d` parameters:
 1. Specify an empty string (two double quotation marks, `""`) on the `-s` parameter.
 2. Specify the `-d` parameter to disable publish/subscribe access for the broker. This ensures that the broker does not try to communicate with the User Name Server.
- Modify the Configuration Manager by removing the reference to the queue manager for the User Name Server. Use the command to modify the `-s` parameter, by specifying an empty string (two double quotation marks, `""`). This ensures that the Configuration Manager does not try to communicate with the User Name Server.

Now that you have made the required changes to the broker and Configuration Manager, you can delete the User Name Server, and thus disable publish/subscribe services.

Deleting a User Name Server

Before you start:

You must complete the following task:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423
- Modify the broker and Configuration Manager so that they do not continue to communicate with the User Name Server. See “Disabling a User Name Server” on page 169 for details of the changes you must make.

Delete a User Name Server using the command line on the system where the User Name Server component is installed. On Windows, you can also use the Command Assistant to complete this task.

On Windows, UNIX systems, and Linux, you must set up your command-line environment before deleting a User Name Server, by running the product profile or console; refer to Setting up a command environment.

Follow the link for the appropriate platform.

- “Deleting a User Name Server on Linux and UNIX systems”
- “Deleting a User Name Server on Windows”
- “Deleting a User Name Server on z/OS”

Deleting a User Name Server on Linux and UNIX systems

To delete a User Name Server on Linux and UNIX systems; AIX, HP-UX, Linux (zSeries platform), Linux (x86 platform) and Solaris:

1. Stop the User Name Server using the **mqsistop** command.
2. Enter the following command to delete the User Name Server:

```
mqsdeleteusenameserver
```

On completion of this task, you have:

- Deleted the queue associated with the User Name Server on the local queue manager
- Removed the record for the component in the broker registry. It is therefore removed from the list of components displayed by issuing the **mqsilist** command.

Deleting a User Name Server on Windows

To delete a User Name Server:

1. Stop the User Name Server using the **mqsistop** command.
2. Enter the following command to delete the User Name Server:

```
mqsdeleteusenameserver
```

On completion of this task, you have:

- Stopped the Windows service that runs the User Name Server.
- Deleted the queue associated with the User Name Server on the local queue manager.
- Removed the record for the component in the broker registry. It is therefore removed from the list of components displayed by issuing the **mqsilist** command.

Deleting a User Name Server on z/OS

To delete a User Name Server:

1. Stop the User Name Server, by stopping the started task.

2. Customize and submit the following delete job manually to delete WebSphere MQ definitions:

Delete jobs	Description
BIPDLUN	Deletes components WebSphere MQ queues and channels

Note that not all files are deleted from the component directory in the file system.

Configuring a broker domain in the workbench

Before you start:

You must have created the physical broker domain components. Refer to “Configuring broker domain components” on page 83.

Configuring a broker domain using the workbench is only possible on Windows and Linux (x86 platform). It is the second part of the two-stage process to create and configure your broker domain.

The workbench allows you to configure and administer the broker domain components as you require. You can launch the workbench in the following ways:

- Using the shortcut added to your desktop during installation, labelled ‘WebSphere Message Brokers Toolkit’.
- From the Start Menu (Windows only) **Start** → **Programs** → **IBM WebSphere Message Brokers 6.0** → **WebSphere Message Brokers Toolkit**
- Using the following commands in a command prompt from their location in either the RAD root directory (if Rational products such as Rational Application Developer were installed on your system before WebSphere Event Broker was installed), or the WebSphere Event Broker installation directory (if no Rational products were installed on your system before WebSphere Event Broker was installed).

On Windows:

```
wmbt.exe
```

On Linux (x86 platform):

```
wmbt.bin
```

See the following tasks for instructions on how to configure a broker domain in the workbench:

- “Creating a domain connection” on page 172
- “Modifying domain connection properties” on page 173
- “Deleting a domain connection” on page 174
- “Adding a broker to a broker domain” on page 175
- “Modifying broker properties” on page 177
- “Removing a broker from a broker domain” on page 178
- “Removing deployed children from a broker” on page 179
- “Adding an execution group to a broker” on page 179
- “Deleting an execution group” on page 181
- “Removing deployed children from an execution group” on page 182

When configuring your broker domain, you are prompted to deploy all changes to the Configuration Manager. It is possible to set your user preferences to not prompt you to deploy after each change. Refer to “Changing Broker Administration preferences” on page 200.

When you make changes to the broker domain, and deploy to the Configuration Manager, there can be a short delay until the workspace is updated and the Configuration Manager tells you that the deploy has worked. The delay depends on the network configuration, or the number of changes to make to the configuration of the broker domain during the deployment.

Creating a domain connection

Before you start:

You must complete the following tasks:

- “Creating a Configuration Manager” on page 125
- Create and start a listener for the Configuration Manager

Create a domain connection in the workbench using the Create a New Domain Connection wizard. Enter a set of parameters to create a `.configmgr` file. The parameters contained within the `.configmgr` file are used to connect to the Configuration Manager, where you can view and edit your broker domain.

To create a domain connection:

1. Switch to the Broker Administration perspective.
 2. Right-click in the Domains view, and click **New** → **Domain**
 3. In the Create a New Domain Connection wizard, enter:
 - a. The name of the WebSphere MQ queue manager that the Configuration Manager is using. This property is mandatory.
 - b. The host name or IP address of the machine on which the Configuration Manager is running (the default is `localhost`). This property is mandatory.
 - c. The TCP port on which the WebSphere MQ queue manager is listening (the default is 1414). This property must be a valid positive number.
 - d. Optional: The name of the Security Exit required to connect to the WebSphere MQ queue manager. This property must be a valid Java classname, but you can leave this box blank if it does not apply to your domain connection.
 - e. Optional: The location of the JAR file for the Security Exit required to connect to the WebSphere MQ queue manager. Use the Browse button to find the file location. You can leave this box blank if it does not apply to your domain connection.
- Note:** The location of the JAR file is required if a Security Exit class is entered.
- f. Optional: The cipher suite, distinguished names, CRL name list, key store, and trust store parameters required when enabling SSL (see “Implementing SSL authentication” on page 19 for more information). The cipher suite field displays available cipher suites. Click **More** to configure a custom cipher suite in the Broker Administration preferences window. If a cipher suite is not specified, all other fields in the SSL section are unavailable.

You can configure several domain connections in your workspace. Each domain connection has to address a different Configuration Manager, which

needs to have a different WebSphere MQ queue manager, host name, or TCP port number. An error message is displayed in the wizard, if you try to create a second broker domain using the same queue manager, host name, and port number.

4. Click **Next** to begin the domain connection to the Configuration Manager.
You cannot connect to a Version 2.1 Configuration Manager. An error is thrown, and you will not be able to populate the domain with brokers or topics, or connect to it using the workbench.
5. If you click **Cancel**, the Create a New Domain Connection wizard closes and a forced disconnection from the domain occurs.
6. After the domain connection has been made, enter:
 - a. The name of your Server Project. This is the container for your domain connection. If you have not already created a server project, you can specify the name of a new project here. The server project is created with the domain connection.
 - b. The Connection Name. This is the name you give to the `.configmgr` file that contains the parameters to connect to the Configuration Manager.
7. Click **Finish** to create the domain connection.
The new domain connection is added to the Broker Administration Navigator view, under Domain Connections. Here the server project holds the `.configmgr` domain connection file.

The view of the broker domain is displayed in the Domains view.

Modifying domain connection properties

Before you start:

To complete this task, you must have completed the following tasks:

- “Creating a domain connection” on page 172
- Disconnect from the broker domain. Refer to “Connecting to and disconnecting from the broker domain” on page 211.

Modify the parameters of the `.configmgr` domain connection file that are used to connect to the Configuration Manager.

To modify the domain connection properties.

1. Switch to the Broker Administration perspective.
2. In the Broker Administration Navigator view, expand Domain Connections, and open your server project.
3. Right-click the `.configmgr` domain connection file and click **Open With** → **Domain Connection Editor**. From here you can change:
 - a. The name of the WebSphere MQ queue manager that the Configuration Manager is using. This property is mandatory.
 - b. The host name or IP address of the machine on which the Configuration Manager is running. This property is mandatory.
 - c. The TCP port on which the WebSphere MQ queue manager is listening. This property must be a valid positive number.
 - d. Optional: The name of the Security Exit required to connect to the WebSphere MQ queue manager. This property must be a valid Java class name, but it is not mandatory and you can leave it blank, if it does not apply to your domain connection.

- e. Optional: The location of the JAR file for the Security Exit required to connect to the WebSphere MQ queue manager. Use the Browse button to find the file location. You can leave this box blank if it does not apply to your domain connection.

Note: The location of the JAR file is required if a Security Exit class is entered.

- f. Optional: The cipher suite, distinguished names, CRL name list, key store, and trust store parameters required when enabling SSL (see “Implementing SSL authentication” on page 19 for more information). The cipher suite field displays available cipher suites. Click **More** to configure a custom cipher suite in the Broker Administration preferences window. If a cipher suite is not specified, all other fields in the SSL section are unavailable.
4. Close the editor.
 5. You are prompted to save the changes; click **Yes**. If the broker domain is connected, you are prompted to disconnect before you can save your changes. The `.configmgr` domain connection file is updated with the new parameters.

You can also change the domain connection parameters for a disconnected domain, from the Domains view. Right-click the disconnected domain and click **Edit Parameters**. This opens the Domain Connection editor. Follow steps 3 to 5 above to make the changes you require.

Deleting a domain connection

Before you start:

You must complete the following task:

- “Creating a domain connection” on page 172

To delete a domain connection, delete the corresponding `.configmgr` file from your server project.

The configuration of the broker domain is stored in the Configuration Manager and is not affected by deleting the domain connection. If you create a new domain connection to the same Configuration Manager, the broker domain will be configured and available for use.

The following steps show you how to delete a domain connection.

1. Switch to the Broker Administration perspective.
2. In the Broker Administration Navigator view:
 - a. Expand Domain Connections
 - b. Open the servers project (called Servers by default).
3. Right-click the domain connection file(<connection name>.configmgr) and click **Delete**.
4. Click **OK** at the prompt, to confirm that you want to delete the domain connection.

If the broker domain in the Domains view is connected, you are prompted to disconnect from the broker domain before it can be deleted. Click **Yes** to disconnect from the broker domain. Clicking **Cancel** at this prompt, cancels deletion of the domain connection.

On completion of this task:

- The `.configmgr` file is removed from the server project.
- The view of the broker domain and its hierarchy is removed from the Domains view.

Adding a broker to a broker domain

Before you start:

You must have completed the following tasks:

- Create a physical broker. On Windows and UNIX platforms, you do this using the command line. Refer to “Creating a broker” on page 108. To create a physical broker on z/OS, refer to “Creating a broker on z/OS” on page 116.
- Connect to the broker domain. Refer to “Connecting to and disconnecting from the broker domain” on page 211.

Adding a broker to the broker topology creates a reference to the broker in the configuration repository; it does not create the physical broker. When you add a broker, be sure to use the same name that you used to create the broker.

To add a broker to a broker domain:

1. Switch to the Broker Administration perspective.
2. Right-click in the Domains view, and click **New** → **Broker**.
3. In the **Create a Broker** wizard:
 - a. Select the broker domain to which you want to add the broker. If the selected broker domain is not connected, you are prompted to connect to the domain. Click **OK**. If you click **Cancel** at this prompt, the wizard remains open.
 - b. Enter the name of the broker.
 - c. Enter the name of the WebSphere MQ queue manager that the broker uses.

Note:

- 1) If the WebSphere MQ queue manager is on a separate machine, make sure that you have performed the steps listed in “Connecting components” on page 153.
 - 2) You can associate a WebSphere MQ queue manager with only one broker, even if the brokers are in different broker domains.
4. Click **Next**.
 5. Optional: Enter a short or long description for the broker.
 6. Click **Finish** to add the broker to the broker domain.
 7. You are, by default, prompted to deploy the updated publish/subscribe topology configuration.

You only need to deploy the topology (either **Complete** or **Delta**) if you are using publish/subscribe and want to share publications or subscriptions.

If you are *not* using publish/subscribe, click **None**. A deployment now (to associate the broker with the Configuration Manager), is not necessary; the broker is automatically associated with the Configuration Manager the first time a bar file is deployed.

You can set user preferences so that you are not prompted to deploy the publish/subscribe topology. Instead, you can choose for either a complete or

delta deployment to be performed automatically. Alternatively, if you are not using publish/subscribe, you might prefer to set the preference so that *no* automatic deployment takes place.

In the Domains view, the broker is added to the broker domain and a default execution group is added to the broker.

Adding a broker to the broker topology creates security ACL groups, which give the user ID full control of the broker and its default execution group. These ACL groups exist until this broker is removed from the broker domain. This means that the user ID can be removed from the **mqbr*** groups, but the user still has the full control access level for the broker and its default execution group.

Next:

Continue to add further execution groups to the broker if necessary. Then create, modify, or reuse message flows, message sets and other required files, and add them to the broker archive for deploying to the broker.

Copying a broker

Before you start:

You must complete the following task:

- “Adding a broker to a broker domain” on page 175

You can copy a broker that you have previously added to a broker domain. The new broker reference can be pasted within the same broker domain only.

The new broker inherits the same short and long description as the original broker, and the same execution groups are added; the message flows under the execution groups of the original broker are not inherited by the new broker’s execution groups. All other broker properties and multicast properties are not inherited by the new broker.

The new broker is automatically given a unique broker name, and queue manager name.

The following steps show you how to copy a broker.

1. Switch to the Broker Administration perspective.
2. In the Domains view, open the broker domain and right-click the broker that you want to copy. Click **Copy**.
3. In the broker domain right-click the Broker Topology and click **Paste**.
4. You are prompted to deploy the updated topology configuration. Click **Delta** to perform a delta deploy. If user preferences are not set to *prompt*, the topology deploy is automatic.

The new broker reference is added to the broker domain. It inherits the short and long description and the same execution groups as the original broker.

The new broker is given a unique name in the broker domain, and a new queue manager name.

The newly-created broker does not necessarily reference a physical broker correctly. The workbench does not check if a physical broker exists for the new broker reference.

To ensure that the broker reference does not contain any errors, rename the broker and the broker's queue manager to be exactly the same names as those specified on the **mqsicreatebroker** command when the physical broker was created:

- To rename the broker, refer to "Renaming a broker."
- To rename the broker's queue manager, refer to "Modifying broker properties."

Modifying broker properties

Before you start:

To complete this task, you must have completed the following tasks:

- "Adding a broker to a broker domain" on page 175
- Start the broker. Refer to "Starting and stopping a broker" on page 214.

You can modify broker properties by adding a long or short description and , customizing the broker or multicast properties.

To modify the broker properties:

1. Switch to the Broker Administration perspective.
2. In the Domains view, right-click the broker that you want to modify, and click **Properties**. In the properties window you can modify:
 - a. The broker properties.
Click **Broker** in the left panel of the properties window. Refer to "Broker properties" on page 231 for details of all the broker properties.
 - b. The multicast properties.
Click **Multicast** in the left panel of the properties window and expand it.
Click **Advanced** to access the advanced multicast properties.
Refer to "Setting up a multicast broker" on page 189 for details of all the multicast properties.
 - c. The description for the broker.
Click **Description** in the left panel of the properties window. Add a short or long description for the broker.
3. Click **OK** to save all modifications to the broker.
An automatic broker configuration deploy is immediately performed to take into account the broker properties changed, except for the broker queue manager name and the short and long descriptions, for which this deploy is not needed to update the broker properties.

Renaming a broker

Before you start:

You must complete the following tasks:

- "Adding a broker to a broker domain" on page 175

You might need to rename a broker (and possibly its queue manager; refer to "Modifying broker properties") if your original attempt at creating a broker reference contained an error.

Renaming a broker is simpler than deleting and re-creating it.

The following steps show you how to rename a broker:

1. Switch to the Broker Administration perspective.
2. In the Domains view, right-click the broker and click **Rename**. The **Rename Broker** dialog is displayed.
3. In the **New name** field, type the new name of the broker.
The name must be exactly the same name as that specified on the **mqsicreatebroker** command.
4. Click **Finish** to rename the broker.

The broker's name is updated in the Domains view, and in the Topology editor.

Removing a broker from a broker domain

Before you start:

You must complete the following task:

- “Adding a broker to a broker domain” on page 175

Removing a broker from a broker domain deletes its broker reference in the configuration repository. The broker is not deleted from the system when you perform this task; it simply marks the broker as logically deleted from the configuration repository.

If you want to move a broker from one topology to another, you need to delete and recreate the broker physically (using the **mqsdeletebroker** and **mqsicreatebroker** commands) even if the Configuration Manager in both domains are at the same product and service release level. See “Deleting a broker” on page 166 for further information.

The following steps show you how to remove a broker from a broker domain.

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the broker domain to reveal the broker that you want to remove.
To remove more than one broker from the same broker domain, select each broker while holding down the Ctrl key.
3. Right-click the broker and click **Delete**.
4. Click **OK** at the prompt to confirm that you want to remove the broker from the broker domain.
5. You are, by default, prompted to deploy the updated publish/subscribe topology configuration.

You only need to deploy the topology if you are using publish/subscribe and want to share publications or subscriptions.

If you are *not* using publish/subscribe, click **None**, as a deployment is not necessary; when removing a broker from the domain, the Configuration Manager automatically requests the broker component to stop message flows that are running and to tidy up any resources being used. (Although if this operation fails for any reason, you can again request the broker to tidy up by deploying a delta topology.)

You can set user preferences so that you are not prompted to deploy the publish/subscribe topology. Instead, you can choose for either a complete or

delta deployment to be performed automatically. Alternatively, if you are not using publish/subscribe, you might prefer to set the preference so that *no* automatic deployment takes place.

The broker and its execution groups are removed as components of the broker domain. Confirmation of the broker's deletion is in two places:

- The broker is removed from the Domains view.
- The broker icon is removed from the Broker Topology editor. If the broker was connected to another broker, this connection is also removed.

To delete the physical broker after you have removed the broker from the domain, refer to "Deleting a broker" on page 166.

Removing deployed children from a broker

Remove the deployed children from a broker if the synchronization between the broker and the Configuration Manager falls into an inconsistent state. Removing the deployed children removes all the message flows and message sets from all execution groups on the specific broker. It also deletes all execution groups, except the default execution group, which is automatically re-created.

The message flows and message sets are not deleted by removing deployed children from a broker. They remain in the development workspace, but their reference is removed from the broker.

To remove the deployed children from a broker:

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the broker domain to reveal the broker with which you want to work.
3. Right-click the broker, and click **Remove Deployed Children**.
4. Click **OK** at the prompt to confirm that you want to delete all execution groups on the broker.

This will remove all message flows and message sets from all execution groups, and delete all execution groups. An automatic broker configuration deploy is immediately performed for the broker to save the changes.

A BIP08921 information message is displayed, to show that the request was received by the Configuration Manager. Verify the results of the deployment by opening the Event Log.

Adding an execution group to a broker

Before you start:

You must complete the following tasks:

- "Adding a broker to a broker domain" on page 175
- Connect to the broker domain. Refer to "Connecting to and disconnecting from the broker domain" on page 211.

When you create a broker, it has a default execution group. If you want additional execution groups, you must create them explicitly.

For more details about why you might want to create multiple execution groups, see Execution groups.

If you prefer, you can create an execution group using the command line; see “Adding an execution group to a broker using the command line” on page 123.

To add an execution group to a broker:

1. Switch to the Broker Administration perspective.
2. Right-click in the Domains view, and click **New** → **Execution Group**.
3. In the Create an Execution Group wizard:
 - a. Select the broker to which you want to add the execution group.
If the selected broker domain is not connected, a Confirm Connection dialog prompts you to connect to the domain. If you click **OK**, the domain is connected and populated with the defined brokers. If you click **Cancel** at this prompt, the wizard remains open.
 - b. Enter the name of the execution group.
 - c. Select the processor architecture for this execution group to specify if the execution group process runs as a 32-bit or as a 64-bit application. You can change the default value for this option, which is initially set to 32-bit; click **Window** → **Preferences** → **Broker Administration** and update the setting for *Execution Group Platform Processor Architecture*.
4. Click **Next**.
5. Optional: Enter a short or long description for the execution group.
6. Click **Finish** to add the execution group to the broker.

In the Domains view, the execution group is added to the appropriate broker.

Copying an execution group

Before you start:

You must complete the following tasks:

- “Adding an execution group to a broker” on page 179
- “Adding a broker to a broker domain” on page 175

You can copy an existing execution group from a broker to another broker within the same broker domain. The new execution group inherits the same short and long description as the original execution group, and is automatically given a new name. The new execution group does not inherit any other properties of the original execution group. The message flows in the original execution group are not copied to the new execution group.

To copy an execution group:

1. Switch to the Broker Administration perspective.
2. In the Domains view, right-click the name of the execution group that you want to copy, then click **Copy**.
3. Right-click the name of the broker to which you want to copy the execution group, then click **Paste**. The broker must be in the same broker domain as the original execution group.

A copy of the execution group is created on the broker; the new execution group has a unique name.

Modifying execution group properties

You can add a long or short description to an execution group. This can be an execution group that you have added to the broker, or the default execution group.

The following steps show you how to modify execution group properties.

1. Switch to the Broker Administration perspective.
2. In the Domains view, right-click the execution group broker that you want to modify, and click **Properties**. The **Execution Group Properties** dialog is displayed.
3. Add a long or short description to the execution group.
4. Click **OK** to add the description.

Renaming an execution group

Before you start:

You must complete the following task:

- “Adding an execution group to a broker” on page 179

You can rename any execution group that you have added to a broker.

To rename an execution group:

1. Switch to the Broker Administration perspective.
2. In the Domains view, right-click the execution group and click **Rename**. The **Rename Execution Group** dialog is displayed.
3. In the **New name** field, type the new name of the execution group.
4. Click **Finish**.
5. Deploy a bar file to the execution group to apply the change to the execution group. You can use any valid bar file to do this. For more information about deploying bar files, see Deploying a broker archive file. If you do not deploy a bar file to the execution group, the changes that you made in the Message Brokers Toolkit are not applied to the runtime execution group.

The name of the execution group is updated in the Domains view.

Deleting an execution group

Before you start:

You must complete the following task:

- “Adding an execution group to a broker” on page 179

You can delete an execution group from the broker to which it belongs.

A broker must always have at least one execution group; you cannot delete the last group belonging to a broker.

Instead of employing this method, you can delete an execution group using the command line; see “Deleting an execution group from a broker using the command line” on page 165.

The following steps show you how to delete an execution group from a broker.

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain to reveal the execution group that you want to delete.
To delete more than one execution group from the same broker domain, select each execution group while holding down the Ctrl key.
3. Right-click the execution group and click **Delete**.
4. Click **OK** at the prompt to confirm that you want to delete the execution group from the broker.

An automatic broker configuration deploy is immediately performed for the broker parent.

A BIP08921 information message is displayed to show that the request was received by the Configuration Manager. Verify the results of the deployment by opening the Event Log.

No message flows or message sets are deleted from the development workspace. The execution group and its assigned message flows and message sets are deleted from the Domains view. However, the messages flows and message sets remain in the Broker Administration Navigator view.

Their assignment reference to the execution group is removed from the configuration repository.

Removing deployed children from an execution group

Removing deployed children from an execution group removes all message flows and message sets without deleting them from the development workspace.

To remove the deployed children from a broker:

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the broker domain to reveal the execution group with which you want to work.
3. Right-click the execution group, and click **Remove Deployed Children**.
4. Click **OK** at the prompt to confirm that you want to remove all message flows and message sets from the execution group.

An automatic broker configuration deploy is immediately performed for the broker parent.

A BIP08921 information message is displayed to show that the request was received by the Configuration Manager. Verify the results of the deployment by opening the Event Log.

Configuring a publish/subscribe topology

To configure a publish/subscribe topology, you need to do the following things:

1. Design and configure your broker domain.
For further information, refer to “Designing a broker domain” on page 52 and “Configuring broker domain components” on page 83
2. Define the topic trees that you require.
For further information, refer to Topics and “Adding a new topic” on page 198.
3. Decide which security options to use.

For further information, refer to “Publish/subscribe security” on page 32 and “Securing the publish/subscribe domain” on page 41.

Setting up the broker domain for publish/subscribe

Refer to the following topics:

“Creating a broker” on page 108

“Modifying a broker” on page 155

“Adding a broker to a broker domain” on page 175

“Configuring broker domain components” on page 83

Publish/subscribe topologies

A *publish/subscribe topology* consists of the brokers, the collectives, and the connections between them, that support publish/subscribe applications in the broker domain.

A publish/subscribe application can consist of a network of brokers connected together. The brokers can all be on the same physical system, or they can be distributed over several physical systems. By connecting brokers together, publications can be received by a client on any broker in the network.

This provides the following benefits:

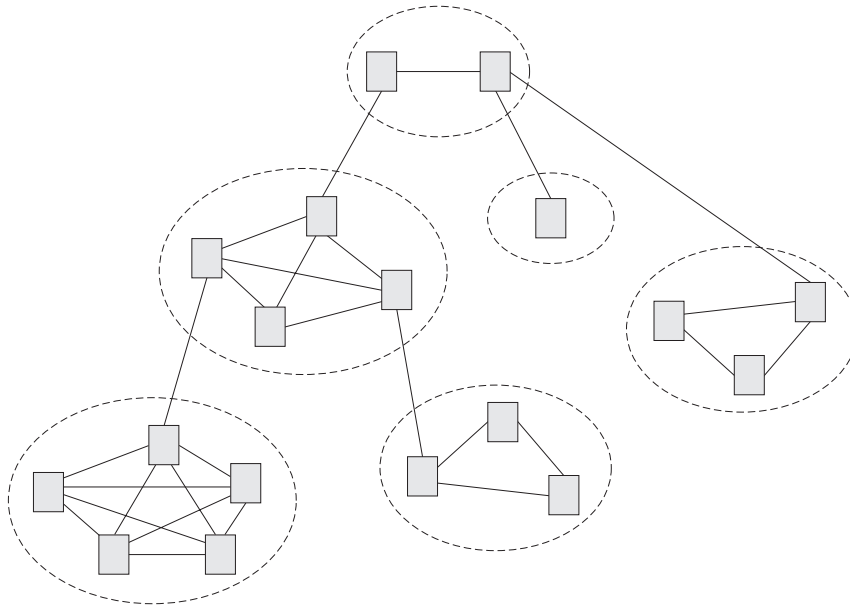
- Client applications can communicate with a nearby broker rather than with a distant broker, thereby getting better response times.
- By using more than one broker, more subscribers can be supported.

Publications are sent only to brokers that have subscribers that have expressed an interest in the topics being published. This helps to optimize network traffic.

Broker networks: There are three ways of connecting brokers together to make a broker domain:

- Brokers can be simply joined together.
- Brokers can be grouped together into collectives, where a collective is a set of one or more brokers that are directly connected to each other.
- Collectives can be joined together; this is a combination of the previous two ways of grouping brokers together.

The following diagram shows a network of six collectives.

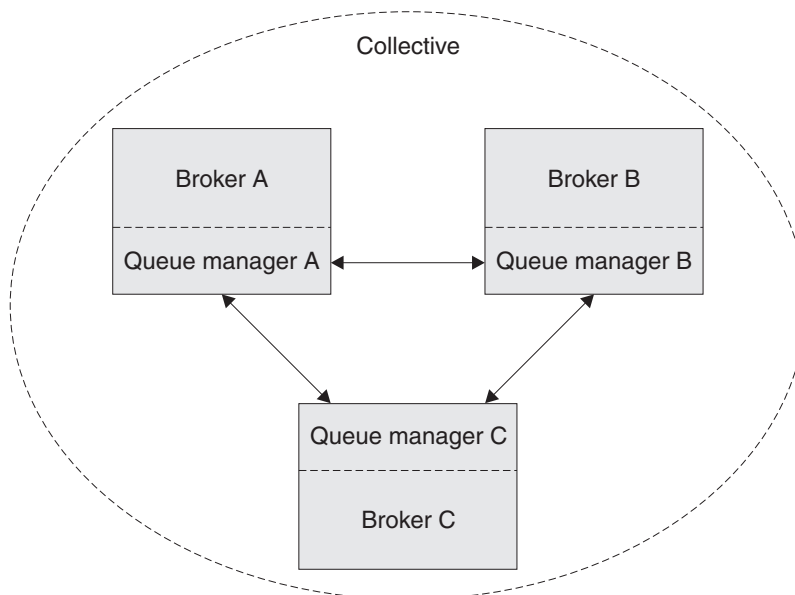


Collectives: A *collective* is a set of brokers that are fully interconnected and form part of a multi-broker network for publish/subscribe applications.

A broker cannot belong to more than one collective. Brokers within the same collective can exist on physically separate computers. However, a collective cannot span more than one broker domain.

Each pair of broker queue managers must be connected together by a pair of WebSphere MQ channels.

The following figure shows a simple collective of three brokers:



A collective provides the following benefits:

- Messages destined for a specific broker in the same collective are transported directly to that broker and do not need to pass through an intermediate broker.

This improves broker performance and optimizes inter-broker publish/subscribe traffic, in comparison with a hierarchical tree configuration.

- If your clients are geographically dispersed, you can set up a collective in each location, and connect the collectives (by joining a single broker in each collective) to optimize the flow of publications and subscription registrations through the network.
- You can group clients according to the shared topics that they publish and to which they subscribe.

Clients that share common topics can connect to brokers within a collective. The common publications are transported efficiently within the collective, because they pass through only brokers that have at least one client with an interest in those common topics.

- A client can connect to its nearest broker, to improve its own performance. The broker receives all messages that match the subscription registration of the client from all brokers within the collective.

The performance of a client application is also improved for other services that are requested from this broker, or from this broker's queue manager. A client application can use both publish/subscribe and point-to-point messaging.

- The number of clients per broker can be reduced by adding more brokers to the collective to share workload within that collective.

When you create a collective, the workbench ensures that the connections that you make to other collectives and brokers are valid. You are prevented from making connections that would cause messages to cycle forever within the network. You are also prevented from creating a collective of brokers that does not have the required WebSphere MQ connections already defined.

The queue manager of each broker in a collective must connect to every other queue manager in the collective by a pair of WebSphere MQ channels.

Each broker in the collective maintains a list of its neighbors.

A neighbor can be one of the following:

- a broker in the same collective
- a broker outside its collective to which it has an explicit connection; that is, for which it is acting as a gateway

The complete list of neighboring brokers forms a broker's neighborhood.

Multicast publish/subscribe: In a publish/subscribe system there are client applications, some of which are publishers and some of which are subscribers, that are connected to a network of message brokers that receive publications on a number of topics, and send the publications on to the subscribers for those topics.

Normally, a separate message is sent to each subscriber of a publication. However, with *multicast*, regardless of how many subscribers to a topic there are on a subnet, only one message is sent. This improves network utilization.

The more subscribers there are in your publish/subscribe system, the greater the improvement to network utilization there might be if you use multicast.

The subscriber must be a JMS client if you want to use Multicast publish/subscribe.

To use multicast, you must change some of the properties of the broker. Some of these properties apply to specific topics, but some properties apply to all Multicast messages that are controlled by that broker.

For each topic, you can define whether the topic can be multicast, and the IP address to which Multicast messages are sent.

You can also change those properties in the broker that define, for example, the following things:

- The multicast protocol type
- The port that is used for Multicast messages
- A 'Time To Live (TTL)' setting that determines how far from its source a Multicast packet can be sent
- The size of a Multicast packet
- Whether there is a maximum transmission rate and, if there is, its value
- What interface to use for Multicast transmissions

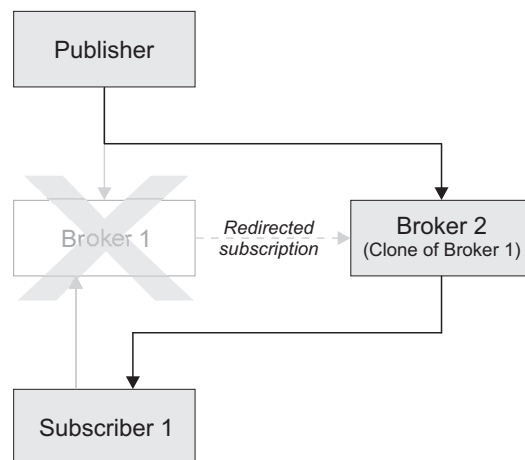
These properties apply to all Multicast messages.

Cloned brokers: A *cloned broker* is a broker for which you have defined one or more clones; the subscription table of a cloned broker is replicated to all other brokers with which it is cloned.

When a subscriber requests a subscription from a cloned broker, the subscription is also sent to each of the clones of that broker.

Use cloned brokers to improve the availability of your publish/subscribe system. By defining cloned brokers on different computers, you make sure that a publication is delivered to a subscriber even when one of the computers is unavailable.

The diagram shows what happens when Subscriber 1 sends a subscription to Broker 1, but Broker 1 becomes unavailable; because Broker 1 and Broker 2 have been defined as clones, the subscription is redirected to Broker 2 and Subscriber 1 gets the publication from Broker 2 instead of Broker 1.



If two brokers are clones within a collective, duplicate messages might be sent to subscribers that are registered with brokers inside that collective.

Use the `mqsichangeproperties` command to define cloned brokers; the property `clonedPubSubBrokerList` is used to do this.

Migrated topologies: If you have a WebSphere MQ Publish/Subscribe broker network, you can continue to use this network unchanged. The introduction of WebSphere Event Broker to your environment, and the creation of brokers in that broker domain, does not affect your WebSphere MQ Publish/Subscribe broker domain until you take specific action to connect the two networks.

If you want to have two separate, independent networks, you do not have to do anything. You can retain your existing WebSphere MQ Publish/Subscribe network, and install and configure a WebSphere Event Broker network, without any interaction.

Heterogeneous networks: A *heterogeneous network* is a network of brokers, some of which form a WebSphere MQ Publish/Subscribe network and some of which belong to the WebSphere Event Broker product.

With the WebSphere Event Broker product, there are two ways in which a broker can be joined to the WebSphere MQ Publish/Subscribe network; it can be joined as a leaf node or as a parent node.

Leaf node: When a broker is joined as a leaf node, it is joined as a child broker of another broker in the WebSphere MQ Publish/Subscribe network.

Adding the broker as a leaf node rather than as a parent node causes the new broker to receive only some of the WebSphere MQ Publish/Subscribe message traffic that is directed to the brokers for which this new broker is a child broker.

Parent node: When a broker is joined as a parent node, it is joined as a parent broker of one or more brokers in the WebSphere MQ Publish/Subscribe network.

Adding the broker as a parent node rather than as a leaf node causes the new broker to receive all the WebSphere MQ Publish/Subscribe message traffic that is directed to the child brokers for which this new broker is the parent broker.

Changing Broker Topology editor properties

After you have launched the Broker Topology editor in the editor area, you can change or remove the default background image displayed in the editor area.

The following steps show you how to change the properties of the Broker Topology editor.

1. Switch to the Broker Administration perspective.
2. In the **Domains** view, expand the appropriate broker domain to display its contents.
3. Double-click **Broker Topology** to launch the Broker Topology editor.
4. Right-click the editor, then click **Properties** to display the Broker Topology editor properties.
5. On the **Editor** page, you can change the background image file, and modify its scale factor in a range of 1 to 5. The default value is 3. Alternatively, you can choose to not display a background image.
6. Optional: On the **Description** page, you can provide a description for the background image file.
7. Click **OK** to save your changes and close the Properties dialog.

Any changes you made to the background image are displayed when the Properties dialog closes.

Connecting brokers in a collective

A *collective* is a set of brokers that are fully interconnected and form part of a multi-broker network for publish/subscribe applications.

You connect brokers in a collective by using either the Message Brokers Toolkit or the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit.

For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.CollectiveProxy*.

The following steps show you how to connect brokers in a collective.

1. Define the WebSphere MQ channels between the queue managers of each pair of the brokers in the collective; use the standard WebSphere MQ facilities (for example, WebSphere MQ Explorer).
2. Assign the brokers as members of the collective using the Broker Topology editor in the workbench; the brokers do not have to be connected together using the connect function.

Tip: Compare the use of collectives with the use of WebSphere MQ cluster queues, as described in *Developing applications using the CMP*.

Deleting a collective

You can delete a collective by using either the Message Brokers Toolkit or the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit.

For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.CollectiveProxy*.

The following steps show you how to delete a collective.

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click the Topology item to open the Broker Topology editor.
4. Right-click the collective that is to be deleted and select Delete, or select the collective that is to be deleted and press the Delete key, or select Delete from the Edit menu.

The collective is deleted locally, but the delete operation is not completed until you save or close the editor.

Connecting a broker to a collective

You can connect a broker to a collective using either the Message Brokers Toolkit or the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit.

For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.CollectiveProxy*.

The following steps show you how to connect a broker to a collective.

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click the Topology item to open the Broker Topology editor.
4. In the Broker Topology editor, click the Connection tool.
5. Click the broker to be connected and then click the collective that you want to connect the broker to.

The connection is added locally, but the connection is only effective after you have saved, or closed the editor.

Removing a broker from a collective

You can remove a broker from a collective using either the Message Brokers Toolkit or the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit.

For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.CollectiveProxy*.

The following steps show you how to remove a broker from a collective.

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click the Topology item to open the Broker Topology Editor.
4. Right-click the connection that you want to delete and select Delete.

Setting up a multicast broker

You can set up a multicast broker by either using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.BrokerProxy.MulticastParameterSet*.

To make a broker capable of handling multicast requests:

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click the Topology item to open the Broker Topology editor.
4. In the Broker Topology editor, right-click the broker that you want to modify, and select **Properties**.
5. In the left panel of the properties window, select **Multicast**.
6. Select the **Multicast Enabled** check box.
7. Optional: Modify the properties that are listed below; any properties that are not modified take the default value.

Protocol Type

The multicast protocol type.

Valid values are "PTL", "PGM/IP", and "UDP encapsulated PGM". The default value is "PTL".

See "Multicast protocol types" on page 194 for an explanation of these multicast protocol types.

Min Address

The lowest IP address that the broker can use for its multicast transmissions.

This must be in the range 224.0.0.0 through 239.255.255.255. The default value is 239.255.0.0.

Max Address

The highest IP address that the broker can use for its multicast transmissions.

This must be in the range 224.0.0.0 through 239.255.255.255, and must not be lower than the value of Min Address. The default value is 239.255.255.255.

Data Port

The UDP data port through which multicast packets are sent and received.

The default value is 34343.

Broker Packet Size

The size, in bytes, of multicast packets.

This can be in the range 500 through 32000. The default value is 7000.

Broker Heartbeat Timeout

The broker sends a control packet periodically, approximately every second, to each client. This packet is used to send various control information, and to keep the heartbeat. The heartbeat timeout value is made known to the clients to help the clients detect a transmitter or network failure. If a control packet does not arrive within a number, defined as twice the value specified by this property, of seconds of the previous control packet's arrival, a client can suspect that there has been a transmitter failure or a network failure.

The default value is 20.

Broker Multicast TTL

The maximum number of hops that a multicast packet can make between the client and the broker. This value is one more than the maximum number of routers that there can be between the client and the broker.

The default value is 1, which means that the multicast packet must remain local to its originator and does not pass through any routers. The maximum value is 255.

Do not use a value of 0. In some operating systems, this might have the effect of preventing messages from being received, but in other operating systems (for example, Windows 2000, Windows XP, and Linux), a value of 0 does not have this effect.

Broker Network Interface

The name of the network interface over which multicast packets are transmitted. This is only relevant when the broker is running on a host with more than one network interface.

This can be a host name or an IP address. The default is 'None'. If the default value is chosen, the network interface that is used is operating system dependent.

Overlapping Multicast Topic Behavior

Choose Accept, Reject, or Revert.

The Overlapping Multicast Topic Behavior property controls the behavior of the broker when a client requests a multicast subscription for a topic that is part of a topic hierarchy containing topics that are explicitly disabled for multicast.

For example, consider a topic hierarchy where multicast is a topic with two children, *foo* that is enabled for multicast, and *bar* that is not enabled for multicast.

The three possible settings are:

Accept

A matching multicast subscription is accepted and all publications matching the topic, except those that are specifically excluded, are multicast. In the example shown above, a multicast subscription to *multicast/#* receives messages published on *foo* over multicast, but does not receive any messages published on *bar*.

Reject A multicast subscription to a topic with children that are disabled for Multicast is rejected by the broker. Subscriptions to *multicast/#* are rejected.

Revert Subscriptions to a topic that is disabled for multicast, or has children that are disabled for multicast, result in unicast transmission. A multicast subscription to *multicast/#* receives messages published on *foo* and *bar*, but the messages are sent unicast rather than multicast.

The default value is *Accept*.

Maximum Key Age

The maximum age, in minutes, of a topic encryption key before it must be redefined.

The default value is 360.

8. Optional: Click the + next to Multicast and click **Advanced**. You can now modify the following additional properties:

Broker Transmission Rate Limit Activation

Use the Broker Transmission Rate Limit Activation property in conjunction with Broker Transmission Rate Limit Value to control network congestion. Choose one of the following values from the drop-down menu:

Disabled

Multicast data is transmitted as fast as possible. If the rate at which messages are submitted to be multicast exceeds the machine or network limits (that is, the speed of Ethernet or the host CPU becomes the bottleneck), these limits define the maximum transmission rate, and message submissions are stopped until all previously submitted messages have been sent.

Static The transmission rate is limited by the value that is specified in Broker Transmission Rate Limit Value.

Dynamic

The limit on the transmission rate can vary during run time, depending on congestion conditions and data losses reported by clients. But the rate never exceeds the Broker Transmission Rate Limit Value.

The default is *Disabled*. If you choose *Static*, you can also choose a value for the property Broker Transmission Rate Limit Value.

Broker Transmission Rate Limit Value

This limits the overall transmission rate, in kilobits per second, of multicast packets. This parameter is effective only if the Broker Transmission Rate Limit Activation property is *Static*. This property must not exceed the capabilities of the machine or network.

This value can be in the range 10 through 1,000,000.

Client NACK Back Off Time

The maximum time, in milliseconds, that a client listens for another's NACKs before sending its own NACK.

This value can be in the range 0 through 1000. The default value is 100.

Client NACK Check Period

The time, in milliseconds, between periodic checks of reception status and sequence gap detection for NACK building.

This value can be in the range 10 through 1000. The default value is 300.

Client Packet Buffer Number

The number of memory buffers that are created at startup for packet reception. Having a high number of buffers available improves the reception performance and minimizes packet loss at high delivery rates, but requires increased memory use. Each buffer is 33 KB; having 500 buffers (the default value) uses approximately 15 MB of main memory.

If memory use is important, try using different values for this property and look at the effect on the overall performance of your application when transmission rates are high.

This value can be in the range 1 through 5000. The default value is 500.

Client Socket Buffer Size

The size, in kilobytes, of the client's socket receiver buffer. Increasing this value reduces the number of data packets that might be dropped by the client receiver.

This value can be in the range 65 through 10000. The default value is 3000.

Broker History Cleaning Time

The time, in seconds, that is defined for cleaning the retransmission buffer.

This value can be in the range 1 through 20. The default value is 7.

Note: This property is not used in Version 6.

Broker Minimal History Size

The minimum size, in kilobytes, of a buffer that is allocated as an archive for all transmitted packets. This buffer is shared by all reliable topics, and can be used to recover lost packets.

This value can be in the range 1000 through 1,000,000. The default value is 60,000.

Broker NACK Accumulation Time

The time, in milliseconds, that NACKs are aggregated in the broker before recovered packets are sent.

This value can be in the range 50 through 1000. The default value is 500.

Maximum Client Memory Size

The maximum amount of memory, in kilobytes, that can be used by reception buffers in the client.

This property is applicable only to PGM multicast protocols. The default value is 262,144 which represents 256 MB.

Important: Be aware that by increasing the values of properties such as Broker Minimal History Size you increase the amount of memory that is required by the Java Virtual Machine (JVM). This might cause a "JVM Out of Memory" error when a subscription to the broker is attempted for the first time after this change. If this error occurs, either increase your JVM heap size or reduce the value of the property (such as Broker Minimal History Size) that you have just increased.

9. Click OK.
10. Restart the broker; you must do this for the changes that you have made to take affect.

Before you can use multicast, you must define some topics as capable of being multicast.

The recommended way of changing the broker's multicast configuration is to use the workbench. However, you can also use the command `mqsichangeproperties` to change the broker's properties.

The following table relates the properties described above to the corresponding names of the parameters on the `mqsichangeproperties` command that support multicast. Full details of the `mqsichangeproperties` command is in "mqsichangeproperties command" on page 264.

Property name	mqsichangeproperties parameter
Multicast Enabled	multicastEnabled
Protocol Type	multicastProtocolType
Min Address	multicastAddressRangeMin
Max Address	multicastAddressRangeMax
Data Port	multicastDataPort
Broker Packet Size	multicastPacketSizeBytes
Broker Heartbeat Timeout	multicastHeartbeatTimeoutSec

Property name	mqsichangeproperties parameter
Broker Multicast TTL	multicastMCastSocketTTL
Broker Network Interface	multicastMulticastInterface
Overlapping Multicast Topic Behavior	multicastOverlappingTopicBehavior
Maximum Key Age	multicastMaxKeyAge
Broker Transmission Rate Limit Activation	multicastLimitTransRate
Broker Transmission Rate Limit Value	multicastTransRateLimitKbps
Client NACK Back Off Time	multicastBackoffTimeMillis
Client NACK Check Period	multicastNackCheckPeriodMillis
Client Packet Buffer Number	multicastPacketBuffers
Client Socket Buffer Size	multicastSocketBufferSizeKbytes
Broker History Cleaning Time (deprecated in V6)	N/A
Broker Minimal History Size	multicastMinimalHistoryKBytes
Broker NACK Accumulation Time	multicastNackAccumulationTimeMillis
Maximum Client Memory Size,	multicastMaxMemoryAllowedKBytes

To enable multicast for the broker WBRK_BROKER use the following command:

```
mqsichangeproperties WBRK_BROKER -o DynamicSubscriptionEngine -n multicastEnabled -v true
```

This enables the broker for multicast, but does not change any other properties of the broker.

To enable multicast for the broker WBRK_BROKER, and to restrict the transmission rate to 50,000 kilobits per second, use the following command:

```
mqsichangeproperties WBRK_BROKER -o DynamicSubscriptionEngine -n multicastEnabled,
multicastLimitTransRate,multicastTransRateLimitKbps -v true,Static,50000
```

None of the other properties of the broker are changed.

Note the use of commas to separate the properties that are being changed, and also their values.

For the changes to be effective, you must restart the broker.

Warning: Any changes to the broker configuration made using `mqsichangeproperties` are overwritten with the configuration that is held in the Configuration Manager whenever the broker configuration is deployed.

Multicast protocol types: WebSphere Event Broker supports three different types of multicast protocol:

- PTL (Packet Transfer Layer)
- PGM/IP
- PGM UDP encapsulated

PTL provides backward compatibility with WebSphere Business Integration Event Broker Version 5.0, where it is the only multicast protocol that is supported. For new multicast deployments, use one of the two PGM multicast protocols.

The broker supports two implementations of the PGM multicast protocol, PGM/IP and PGM UDP encapsulated. Which of the two PGM protocol types that you should choose, depends on the complexity of your network topology.

If your network topology consists of two or more subnets with many receiver clients in each subnet, use PGM/IP. PGM/IP takes advantage of PGM router assist support.

For a simpler network topology, use the PGM UDP encapsulated implementation, which does not use PGM router assist.

Important: To use PGM/IP, both the broker and the client applications must run with superuser authority. Because of the security risks that are associated with running with superuser authority, it is recommended that no other work should be run on the broker.

Making topics multicast:

To make individual topics, or groups of topics, capable of being multicast you need to make changes to the topic hierarchy:

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click on the Topics item to open the Topics Hierarchy editor.
4. In the Topics Hierarchy editor, right-click the topic, or group of topics, that you want to make capable of being multicast, and select properties.
5. In the left panel of the properties window, select **Multicast**.
6. Choose the **Multicast Enabled** required.

For the topic root, the choice is either **Enabled** or **Disabled**. The default is **Disabled**.

For a child topic root, the choice can be **Inherit**, **Enabled**, or **Disabled**. The default is **Inherit**.

7. Check the **Automatic Multicast Address** box, or type in the name of the **MC Group Address**.
8. Choose the **Quality of Service** required. The choice is between **Reliable** or **Unreliable**. The default is **Reliable**.
9. Optional: Select the **Encrypted** check box.
10. Click OK.

Handling high-volume publish/subscribe activity on z/OS:

Brokers that handle large numbers of retained subscriptions or publications can use up all the IRLM storage that is allocated by default for DB2 locks. This might cause problems when you try to restart the broker.

The following actions might help stop this happening.

1. Tune the publish/subscribe topology:
 - a. Balance execution groups across more brokers; this means that fewer execution groups need to start at the same time and have concurrent locks for the same DB2 subsystem.

- b. Put the brokers in publish/subscribe collectives; this reduces the number of subscriptions in a single broker table and reduces the amount of concurrent access to DB2. See “Publish/subscribe topologies” on page 183 for more information about this.
2. Increase the IRLM storage that is available:
 - a. Set the value of MAXCSA so high that the ECSA that is required by the IRLM never reaches this value. Because IRLM gets storage only when it needs it, choose a value that is higher than you expect IRLM to need.
 - b. If you are unable to choose a value of MAXCSA sufficiently high that it cannot be exceeded by the ECSA that is required by the IRLM, use the option PC=YES on the START irlmproc command. This causes the IRLM to place in its private address space the control block structures that relate to locking. There is more information about this in the DB2 Redbook *DB2 UDB for OS/390 Version 7 Performance Topics*, SG24-5351.

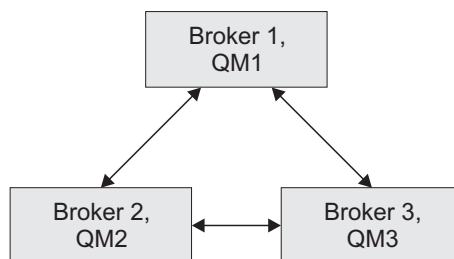
Note: There might be a slight (approximately 1 to 2 percent) performance degradation when you run with PC=YES. See *DB2 Universal Database for OS/390 and z/OS Version 7 Administration Guide*, SC26-9931 for more information.

Setting up cloned brokers

Each broker that is to be cloned with other brokers must be told which brokers are to be its clones.

To set up three brokers (broker1 with queue manager QM1, broker2 with queue manager QM2, and broker3 with queue manager QM3) to be clones of each other, as shown in the diagram below, use the `mqsichangeproperties` command for each of the brokers:

1. `mqsichangeproperties broker1 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"broker2,QM2,broker3,QM3\"`
2. `mqsichangeproperties broker2 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"broker1,QM1,broker3,QM3\"`
3. `mqsichangeproperties broker3 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"broker1,QM1,broker2,QM2\"`



Adding a cloned broker

To add a broker to a set of cloned brokers, use the `mqsichangeproperties` command to define the brokers that are its clones, and to tell each of the other brokers that it has a new clone.

To add broker4 (with queue manager QM4) to a set of three cloned brokers (broker1 with queue manager QM1, broker2 with queue manager QM2, and broker3 with queue manager QM3), use the following **mqsichangeproperties** commands:

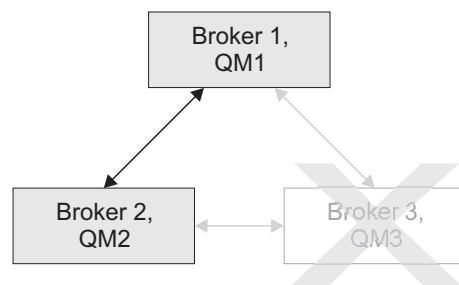
1. `mqsichangeproperties broker4 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"broker1,QM1,broker2,QM2,broker3,QM3\"`
2. `mqsichangeproperties broker1 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"+broker4,QM4\"`
3. `mqsichangeproperties broker2 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"+broker4,QM4\"`
4. `mqsichangeproperties broker3 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"+broker4,QM4\"`

Deleting a cloned broker

To delete a broker from a set of cloned brokers, use the **mqsichangeproperties** command to delete the brokers that were its clones, and to tell each of the other brokers that one of its clones has been deleted.

To delete broker3 from a set of three cloned brokers (broker1 with queue manager QM1, broker2 with queue manager QM2, and broker3 with queue manager QM3), as shown in the diagram below, use the following **mqsichangeproperties** commands:

1. `mqsichangeproperties broker1 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"-broker3\"`
2. `mqsichangeproperties broker2 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"-broker3\"`
3. `mqsichangeproperties broker3 -e default -o DynamicSubscriptionEngine -n clonedPubSubBrokerList -v \"\"`



Operating a publish/subscribe domain

After you have set up your publish/subscribe broker domain, you might want to create or delete topics, or view the current status of your subscriptions.

For information about how to do this, refer to the following topics:

- “Adding a new topic” on page 198
- “Deleting a topic” on page 198
- “Querying subscriptions” on page 199

Adding a new topic

You can define a new topic explicitly by using either the Message Brokers Toolkit or the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit.

For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.TopicProxy*.

You can define a new topic implicitly by sending to the message broker a Publish command that specifies the new topic.

However, to define a new topic explicitly, do the following:

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click on the Topics item to open the Topics Hierarchy editor.
4. Right-click **Topics** in the topics hierarchy that is displayed by the Topics Hierarchy Editor.
5. From the menu shown, click **Create Topic**; a topic window opens that shows the topic hierarchy.
6. In the topic hierarchy, select the topic that you want to be the parent topic of the topic that you are creating. In the lower pane of the topic window, type the name of your new topic.
7. Click **Next**; the next wizard page opens. The pane on the left of this window shows all the principals (groups and users) that are defined.
8. Select the groups and users that you want to relate to your new topic and click the > icon between the two panes of the window; the pane on the right of the window is updated with the groups and users that you have chosen.
9. For each principal selected in the right-hand pane, you can set **Publish**, **Subscribe**, and **Persistent** attributes by choosing a value from the corresponding list.
By selecting more than one principal, you can choose values for a set of principals.

10. Click **Finish** to insert the topic into the topic hierarchy and update the access control list (ACL) for the topic. The ACL is in a table with four columns that are entitled Principal, Publish, Subscribe, and Persistent. The rows of the table show the properties of each principal that is relevant to the topic.

The topic is created locally, but the change is not effective until you have saved or closed the editor.

When saving or closing the editor, you might be prompted to deploy the new topics hierarchy or the deployment might be automatic, depending on the **Perform topics deploy after change** preference.

Deleting a topic

You can delete a topic by either using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.TopicProxy*.

To delete a topic:

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the appropriate broker domain.
3. Double-click **Topics** to open the Topics Hierarchy Editor.
4. In the Topics Hierarchy editor, right-click the topic that you want to delete, and select **Delete**; alternatively, select the topic that you want to delete and press the Delete key, or select Delete from the Edit menu.

The topic is deleted locally, but the delete is not effective until you do a save.

Querying subscriptions

You can query a subscription either by using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class com.ibm.broker.config.proxy.TopicProxy*.

To query a subscription:

1. Switch to the Broker Administration perspective.
2. In the **Domains** view, click **Subscriptions** from the list of domain objects shown; the Subscriptions Query Editor opens in the workbench.

You can also open the editor by double-clicking the **Subscriptions** item in the tree, or by right-clicking the **Subscriptions** item and clicking **Open**, or by clicking the **Subscriptions** item and clicking **Enter**.

3. Fill in the fields that are required to generate your subscriptions query.
To generate your query, you might not need to fill in all the fields shown.
4. Click **Query**. The results of your query are displayed in the lower part of the edit window.

Configuring the workbench

The following topics show you how to configure aspects of the workbench. A minimum display resolution of at least 1024 x 768 is required for some dialogs, such as the Preferences dialog.

- “Changing workbench preferences”
- “Changing Broker Administration preferences” on page 200
- “Changing palette preferences” on page 200
- “Configuring CVS to run with the Message Brokers Toolkit” on page 202

Changing workbench preferences

The workbench has a large number of preferences that you can change to suit your requirements. Some of these are specific to the product plug-ins that you have installed within the workbench, including those for WebSphere Event Broker. Others control more general options, such as the colors and fonts in which information is displayed.

To access the workbench preferences:

1. Select **Window** → **Preferences**.
2. Click the plus sign associated with **Workbench**, typically the first entry in the left pane. An expanded list of options appears, Select the aspect of the workbench that you want to modify. These options might be of interest:

Startup and shutdown

Switch on, or off, the prompt at toolkit startup that asks you to confirm the workspace location. Typically you switch this prompt off, so that it does not appear, but you can force it to appear next time you start the workbench if you want to specify a different location.

Here you can also choose to display, or not display, the dialog that asks you to confirm shutdown of the workbench.

Colors and fonts

Change the default fonts and colors that appear in the workbench.

Perspectives

On this dialog, your choices include the option to open a new perspective in a new window.

3. When you have made your changes, click **OK** to close the Preferences dialog.

Below the Workbench category in the Preference dialog are items that refer specifically to WebSphere Event Broker resources, such as message flows. Review the following topics for information about setting preferences and other values that are specific to your use of these resources:

- Message flow preferences
- Changing trace settings

Changing Broker Administration preferences

You can change the following Broker Administration preferences:

- Show empty projects in the Navigator views.
- Show ACL restricted objects in the Navigator views.
- Warn before deleting alerts.
- Prompt to perform a topology deploy after changes. You can change this to never deploy, always a delta deploy, or always a complete deploy.
- Prompt to perform a topics deploy after changes. You can change this to never deploy, always a delta deploy, or always a complete deploy.

To change Broker Administration preferences:

1. Switch to the **Broker Administration perspective**.
2. Click **Window** → **Preferences**.
3. Expand the **Broker Administration** category in the left pane.
4. Make your selections.
5. Click **OK**.

Changing palette preferences

You can change the palette preferences in the Message Brokers Toolkit . The changes that you can make are described in the following topics.

- “Changing the palette layout” on page 201
- “Changing the palette settings” on page 201
- “Customizing the palette” on page 201

Changing the palette layout

You can change the layout of the palette in the Message Flow editor and the Broker Topology editor using the Message Brokers Toolkit.

1. Right-click the palette to display the pop-up menu.
2. Click **Layout**.
3. Click one of the available views:

Columns

Displays named icons in one or more columns. Change the number of columns by clicking on the right edge of the palette and dragging.

List Displays named icons in a single-column list. This is the default layout.

Icons Only

Displays a list of icons only.

Details

Displays a detailed list of icons.

Changing the palette settings

In Message Brokers Toolkit you can change the palette settings in the Message Flow editor and Broker Topology editor using the **Palette Settings** dialog.

1. Right-click the palette to display the pop-up menu.
2. Click **Settings**. The **Palette Settings** dialog opens.
3. Use the dialog to change the appropriate setting:
 - Click the **Change** button to change the font on the palette.
 - Click the **Restore Default** button to restore the default palette settings.
 - In the **Layout** list, tick the appropriate radio button to change the palette layout. (See “Changing the palette layout” for more information.)
 - Tick the **User large icons** check box to toggle between large and small icons in the palette.
 - In the **Drawer options** list, tick the appropriate radio button to change the way that drawers are handled in the palette. A drawer is a container for a list of icons, such as the **Built-in nodes** drawer on the Message Flow editor’s palette or the **Entity** drawer on the Broker Topology editor’s palette.

Customizing the palette

In Message Brokers Toolkit you can customize the palette for the Message Flow editor using the **Customize Palette** dialog.

1. Right-click the palette to display the pop-up menu.
2. Click **Customize**. The **Customize Palette** dialog opens.
3. To change the order of entries and drawers in the palette, click the appropriate item in the list to highlight it, then click the **Move Down** or **Move Up** button.
4. To hide an entry or drawer, click the appropriate item in the list to highlight it, then tick the **Hide** check box.
5. To create a new separator, click **New** → **Separator**.
6. To create a new drawer:
 - a. Click **New** → **Drawer**.
 - b. Type a name and description for the drawer.
 - c. If required, tick the **Open drawer at start-up** check box.

- d. If required, tick the **Pin drawer open at start-up** check box.

Configuring CVS to run with the Message Brokers Toolkit

Install CVS as a normal program by following the usual prompts. Not all versions of *CVSNT* are supported by Eclipse.

1. Configure CVS by carrying out the following tasks:
 - a. Create a directory on your computer, for example, on Windows - `c:\CVSRepository`.
 - b. Start the *CVSNT* control panel. Select `Start->Programs->CVSNT` to see the icon on the desktop.
 - c. Stop both the CVS Service and the CVS Lock Service.
 - d. Select the Repositories tag, click **Add** and create a new repository. Note that no entry appears on the screen the first time that you do this.
 - e. Use the `...` button on the next window to select the directory that you created in step 1a and click **OK**. Note that when CVS has finished formatting its repository the backslash in the directory name is changed to a forward slash.
 - f. Select the Service Status tab and restart both the CVS Service and the CVS Lock Service.
2. Enable the CVS Revision tag to be populated in the Eclipse Version fields in the Message Brokers Toolkit. To do this on Windows:
 - a. Select `Window->Preferences`
 - b. Expand the Team section and click **CVS**
 - c. Use the drop down in the **Default keyword substitution:** field and set the value to ASCII with keyword expansion(-kkv)
3. Add the WebSphere Event Broker file types to the Eclipse CVS configuration. To do this:
 - a. Select **File Content** in the Team section of the window you opened in step 2
 - b. Click **Add** and add `msgflow` as an allowable file extension. Ensure that the value is set to ASCII.
 - c. Repeat the above procedure for the following file extensions that the broker uses:
 - `esql`
 - `mset`
 - `mxsd`

If you use CVS to store other file types, for example, COBOL copybooks add the appropriate file types as well.
- d. Click **OK** when you have finished.

Changing locales

You can change the locale for the system on which a runtime component is installed.

The way in which you do this depends on the operating system:

- “Changing your locale on UNIX and Linux systems” on page 203
- “Changing your locale on Windows” on page 204
- “Changing your locale on z/OS” on page 205

WebSphere Event Broker uses code page converters to support character sets from different environments. “Code page converters” on page 206 describes what a code page converter is, and how to generate new converters.

Changing your locale on UNIX and Linux systems

You can change your system locale on UNIX and Linux systems.

There are many environment variables that control the locale. These can be defined system-wide, in your environment, or on a per-session basis:

LC_ALL

Overrides all LC_* environment variables with the given value

LC_CTYPE

Character classification and case conversion

LC_COLLATE

Collation (sort) order

LC_TIME

Date and time formats

LC_NUMERIC

Non-monetary numeric formats

LC_MONETARY

Monetary formats

LC_MESSAGES

Formats of informative and diagnostic messages, and of interactive responses

LC_PAPER

Paper size

LC_NAME

Name formats

LC_ADDRESS

Address formats and location information

LC_TELEPHONE

Telephone number formats

LC_MEASUREMENT

Measurement units (Metric or Other)

LC_IDENTIFICATION

Metadata about the locale information

LANG

The default value. This is used when either LC_ALL is not set, or an applicable value for LC_* is not set

NLSPATH

Delimited list of paths to search for message catalogues

TZ Time zone

LC_MESSAGES and NLSPATH are the most important variables to the broker. These variables define the language and location of response messages that the broker uses. The broker profile file, mqsiprofile, sets NLSPATH. Either you, or your system must set LC_MESSAGES. The value set in LC_MESSAGES must be a value that the

broker recognizes. LC_CTYPE is also important to the broker because it defines the character conversion that the broker performs when interacting with the local environment.

If you use common desktop environment (CDE), use this to set the locale instead of setting LANG and LC_ALL directly. The NLSPATH variable respects either method. Before setting the code page, check that it is one of the Supported code pages.

For example, to set WebSphere Event Broker to run in a UTF-8 environment set the following values in the profile:

```
LANG=en_US.utf-8
LC_ALL=en_US.utf-8
```

Where en_US sets the language, and utf-8 sets the code page.

You can use the executable `locale` to show your current locale. The command `locale -a` displays all the locales currently installed on the machine. Make sure that the locale you select for LANG and LC_ALL is in the list that `locale -a` returns. The values that `locale` uses and returns are case-sensitive, so copy them exactly when assigning them to an environment variable.

When you start a broker component, the locale of that component is inherited from the shell in which it is started. The broker component uses the LC_MESSAGES environment variable as the search path in the NLSPATH environment variable (LC_MESSAGES is set when variable LC_ALL is exported).

Messages are sent to the syslog in the code page set by this locale. If you have multiple brokers that write to this syslog, their messages are in the code page of the locale in which they were started, for example:

locale	syslog code page	ccsid
pt_BR	iso8859-1	819
Pt_BR	ibm-850	850
PT_BR	utf-8	1208

Set the locale of the user ID that runs the syslog daemon to one that is compatible with the locales of all brokers that write to the syslog on that system, for example, utf-8. You can do this by setting the default locale. On Solaris, set the LANG and LC_ALL variables in `/etc/default/init`. On AIX and Linux, these variables are in `/etc/environment`. This task is not required on HP-UX.

For full time zone support in the broker, set the TZ variable using Continent/City notation. For example set TZ to Europe/London to make London, England the time zone, or set it to America/New_York to make New York, America the time zone.

If you want to add a new locale, refer to the operating system documentation for information on how to complete that task. If the code page of the new locale is not supported by WebSphere Event Broker you must add it by “Generating a new code page converter” on page 206.

Changing your locale on Windows

You can change your system locale on Windows.

The product components are started as services on Windows and are therefore influenced by the system locale. The command line functions are influenced by the user's locale. WebSphere Event Broker on Windows has all its locale information installed by default. However, you might need to install additional locale packages if prompted to do so by Windows.

To change locale, you can do one of the following:

- Install a locale-specific operating system.
- Alter the system or user locale by selecting *Regional Settings* in the Control Panel.

Messages are sent to the Event Log in the code page set by the current locale.

You can use the `chcp` command to change the active console code page. Enter the command at a command prompt; if you enter `chcp` without a parameter, it displays the current setting. If you enter it with a code page, it changes to that code page.

For example, to check the current code page setting:

```
C:\>chcp
Active code page: 437
```

The current page is displayed (437 is US-ASCII). If you want to change this to GB18030, enter:

```
C:\>chcp 54936
Active code page: 54936
```

Before using a code page, search for `windows-number` where *number* is the active code page you want to use in the list of Supported code pages. If the code page is not in the list, either use a code page that is in the list, or generate a new code page converter.

Changing your locale on z/OS

You can change your system locale on z/OS.

If you want to change your system locale on z/OS, set the `LANG`, `LC_ALL`, and `NLS_PATH` variables. See "Installation information - broker and User Name Server" on page 117 and "Installation information - Configuration Manager" on page 130 for further information.

The locale is set in the appropriate component profile (`BIPBPROF` for the broker, `BIPCPRF` for the Configuration Manager, `BIPUPROF` for the User Name Server) and you must run `BIPGEN` to create the component `ENVFILE`.

You can use the UNIX System Services (USS) executable `locale` to show your current locale. The command `locale -a` displays all the locales currently installed on the machine. Refer to the operating system documentation for information about adding new locales. If you add a new locale after you have installed WebSphere Event Broker, install that locale's message catalogs from the original install media.

You can set WebSphere Event Broker to operate with a specific code page. Set the code page after a period in the `LANG` and `LC_ALL` variable. This example sets the locale to `En_us` and the code page to `IBM-1140` (EBCDIC `En_us` with euro):

```
LANG=En_us.IBM-1140
LC_ALL=En_us.IBM-1140
```

Make sure that the selected code page is one of the Supported code pages. If the code page is not in the list, either use a code page that is in the list, or generate a new code page converter.

Code page converters

WebSphere Event Broker performs string operations in Universal Character Set coded in 2 octets (UCS-2). If incoming strings are not encoded in UCS-2, they must be converted to UCS-2. The broker uses international components for Unicode (ICU) code page converters to do this. The Unicode Consortium has further information on Unicode.

A code page converter is a mapping from the byte sequence in one code page to a serialized representation of UCS-2, known as UCS Transformation Format 16 bit form (UTF-16). A code page converter allows the broker to create a UCS-2 representation of an incoming string.

An example of the use of code page converter is:

- A message comes in on a queue from z/OS, with the MQ CCSID field set to 1047 (LATIN-1 Open Systems without euro). The broker looks up `ibm-1047` and uses the resulting converter to create a UCS-2 representation for internal use.

WebSphere Message Broker currently supports the code pages listed in Supported code pages. If you need support for an additional code page, or if you require a different variant of a code page, you can extend the broker to support this code page.

Generating a new code page converter

Before you start:

- “Code page converters” provides information about what a code page converter is, and about the code pages that WebSphere Event Broker supports.

If you need to support a code page that is not in the default set of code pages that WebSphere Event Broker supports, you can generate a new code page converter.

1. Create or find a mapping data file with the file extension `.ucm` for the converter you require. You can download many `.ucm` files from the ICU Character set mapping files archive. These mapping data files are available and modifiable without restriction. An example mapping data file is `ibm-1284_P100-1996.ucm`.
2. Rename the `.ucm` to a file name with the format `ibm-number.ucm` where *number* is a number you choose to identify the code page. Make sure this number is not already used in one of the Supported code pages. An example of this is renaming `ibm-1284_P100-1996.ucm` to `ibm-1284.ucm`.
3. Go to ICU downloads and download the binary distribution for your platform. An exact match is not important as long as the binaries can run. If you have problems building the converter, see the ICU user guide.
4. Extract the files from the binary distribution archive in to a temporary directory.
5. Copy the library and binary files to a directory within the environment path and `libpath`. Alternatively, copy the library and binary files to directory that is not temporary and modify the environment path and `libpath` to include this directory.

6. Use the `makeconv` tool from the extracted files to convert the mapping data file (.ucm files) into a binary converter file (.cnv file). Enter the following command to do this:

```
makeconv -p ICUDATA mapping_file.ucm
```

where

mapping_file.ucm

is the mapping data file that you are using.

The name of the binary converter file that `makeconv` produces is:

```
icudt32<platform-suffix>_<mapping_file>.cnv
```

where

<platform-suffix>

is one of the following:

- *l* for little-endian ASCII platforms
- *b* for big-endian ASCII platforms
- *e* for EBCDIC platforms

<mapping_file>

is the name of the mapping data file that was converted.

To make the .cnv file for `ibm-1284.ucm`, use the following command:

```
makeconv -p ICUDATA ibm-1284.ucm
```

7. Copy the file with the file extension .cnv for the code page you need into a directory that WebSphere Event Broker can access. On UNIX an example directory is `/var/mqsi/converters`.
8. Associate the broker with the code page converter by entering the name of the *directory* where the converter is stored:
 - To create a new broker associated with the converter enter the following at a command prompt: `mqsicreatebroker -c directory`
 - To alter an existing broker to recognize the converter enter the following at a command prompt: `mqsichangebroker -c directory`
 - To affect all the products and the broker command-line tools using ICU, add the *directory* to the `ICU_DATA` environment variable. If you have already used either the `mqsicreatebroker` command or the `mqsichangebroker` to specify the code page converter to be used, the broker ignores the `ICU_DATA` value.

You have now created a code page converter, and associated the converted with a broker.

Using converters from a previous level of the product

Before you start:

- “Code page converters” on page 206 provides information about what a code page converter is, and about the code pages that WebSphere Event Broker supports.

If you have applications that require a code page that is not in the default set of code pages that WebSphere Event Broker Version 6.0 supports, you can use a code page from an earlier version of WebSphere Event Broker. Because the changes in converters between the previous level of the broker and WebSphere Event Broker

Version 6.0 is significant, the set of converters from the previous level has been included with WebSphere Event Broker Version 6.0.

To use one of these converters follow these steps:

1. Extract the list of WebSphere Business Integration Event Broker Version 5.0 code page converters from your installation directory to a temporary directory:
 - On Windows: extract "install_dir\sample\converters\mqsicconverters-v5.zip".
 - On Linux: extract install_dir/sample/converters/mqsiconverters-v5.tar.bz2.
 - On Unix: extract install_dir/sample/converters/mqsiconverters-v5.tar.gz.

Where install_dir is the home directory of your WebSphere Event Broker installation.

2. Copy the .cnv file for the desired codepage to a directory accessible to the broker. For example, on UNIX platforms: /var/mqsi/converters and on Windows:c:\documents and setting\all users\application data\IBM\MQSI\converters If you want to make sure that there is no conflict with an existing converter, the file can be renamed to something unique. To check the file will not cause a conflict of filenames, make sure the number is not already used in one of the Supported code pages. Remember that if the converter is to be usable by ESQL it must be of the form ibm-<ccsid>. This is because converters are referenced through their numeric CCSID, not their name.
3. Associate the broker with the code page converter by entering the name of the directory where the converter is stored:
 - To create a new broker associated with the converter, enter the following in a command prompt: mqsicreatebroker -c directory
 - To alter an existing broker to recognize the converter, enter the following at a command prompt: mqsichangebroker -c directory
 - To affect all the products and the broker command-line tools using ICU, add the directory to the ICU_DATA environment variable.

If you have already used either the mqsicreatebroker command or the mqsichangebroker to specify the code page converter to be used, the broker ignores the ICU_DATA value.

The entire set of converters (*.cnv) and aliases (*.icu) can be copied to reproduce the behavior of the previous level of the product.

Part 3. Administering the broker domain

Administering the broker domain	211
Connecting to and disconnecting from the broker domain	211
Connecting to and disconnecting from the broker domain on z/OS	212
Starting and stopping message flows	214
Starting and stopping a broker	214
Starting and stopping a broker on Linux and UNIX systems	215
Starting and stopping a broker on Windows	215
Starting and stopping a broker on z/OS	216
Starting and stopping a Configuration Manager	216
Starting and stopping a Configuration Manager on Linux and UNIX systems	216
Starting and stopping a Configuration Manager on Windows.	217
Starting and stopping a Configuration Manager on z/OS	217
Starting and stopping the User Name Server	217
Starting and stopping the User Name Server on Linux and UNIX systems	218
Starting and stopping the User Name Server on Windows.	218
Starting and stopping the User Name Server on z/OS	219
Starting a WebSphere MQ queue manager as a Windows service	219
Stopping a WebSphere MQ queue manager when you stop a component	220
Viewing broker domain log information	220
Refreshing broker domain log information.	221
Filtering broker domain log information	222
Saving broker domain log information	223
Clearing broker domain log information	224
Changing Event Log editor preferences.	224
Backing up resources	225
Backing up the broker domain on distributed systems	225
Backing up the broker domain on z/OS	227
Backing up the Message Brokers Toolkit workspace	228

Administering the broker domain

Administering the broker domain includes the tasks that you operate frequently to activate and run your broker domain. These are listed below:

- “Connecting to and disconnecting from the broker domain”
- “Starting and stopping message flows” on page 214
- “Starting and stopping a broker” on page 214
- “Starting and stopping a Configuration Manager” on page 216
- “Starting and stopping the User Name Server” on page 217
- “Starting a WebSphere MQ queue manager as a Windows service” on page 219
- “Stopping a WebSphere MQ queue manager when you stop a component” on page 220
- “Viewing broker domain log information” on page 220
- “Refreshing broker domain log information” on page 221
- “Filtering broker domain log information” on page 222
- “Saving broker domain log information” on page 223
- “Clearing broker domain log information” on page 224
- “Changing Event Log editor preferences” on page 224
- “Backing up resources” on page 225

These tasks can be performed using one, or more, of the administrative techniques available with WebSphere Event Broker:

- The Message Brokers Toolkit
- The WebSphere Event Broker commands
- The Configuration Manager Proxy Java API

For each task, the administrative techniques that can be used are identified.

Connecting to and disconnecting from the broker domain

Before you start:

You must complete the following task:

- “Creating a domain connection” on page 172

You can connect to, and disconnect from, the broker domain by either using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy, see [Connecting to the Configuration Manager using the Configuration Manager Proxy](#).

Use a domain connection to connect to the broker domain in the workbench.

The following steps show you how to connect to the broker domain and how to disconnect from the broker domain.

1. To connect to the broker domain:
 - a. Switch to the Broker Administration perspective.

- b. In the Domains view, right-click the broker domain to which you want to connect, and click **Connect**. This starts the domain connection to the Configuration Manager.

When connected, the workbench status line is changed (for example *WBRK_QM@localhost:1414* is connected). The Broker Topology and Topics are populated, and the broker domain and broker topology icons change to reflect the connected state.

On successful connection, the Configuration Manager name is shown in the Domains view in the form ConfigurationManagerName on QMgrName@Hostname:PortNumber.

Note: If you click **Cancel** while the connection is being attempted, the connection that is in progress stops and the domain returns to its initial unconnected state.

2. To disconnect from the broker domain:
 - a. Switch to the Broker Administration perspective.
 - b. In the Domains view, right click the broker domain from which you want to disconnect, and click **Disconnect**. The connection to the Configuration Manager is broken.

When disconnected, the workbench status line is changed (for example *WBRK_QM@localhost:1414* is not connected). All brokers and topics are removed from the domains navigator tree, and the broker domain and broker topology icons change to reflect the disconnected state.

Connecting to and disconnecting from the broker domain on z/OS

Before you start:

You must complete the following task:

- “Creating a Configuration Manager on z/OS” on page 130
- Create and start a listener for the Configuration Manager

Ensure that your toolkit machine and user ID has the appropriate authorization on the z/OS Configuration Manager.

In SDSF, grant access to your user ID.

1. For this to work on all machines, enter:

```
'/F <started task name> CA U=<userID>,A=YES,P=YES,X=F'
```

or to grant access to your user ID for a specific machine, enter:

```
'/F <started task name> CA U=<userID>,A=YES,M=<machine name>,P=YES,X=F'
```

2. Verify the above by entering:

```
/F <configmgrname>,LA
```

Create a domain connection in the workbench using the Create a New Domain Connection wizard. Enter a set of parameters to create a `.configmgr` file. The parameters contained within the `.configmgr` file are used to connect to the Configuration Manager, where you can view and edit your broker domain.

To create a domain connection:

1. Switch to the Broker Administration perspective.
2. Right-click in the Domains view, and click **New** → **Domain**

3. In the Create a New Domain Connection wizard, enter:
 - a. The name of the WebSphere MQ queue manager that the Configuration Manager is using. This property is mandatory.
 - b. The host name or IP address of the machine on which the Configuration Manager is running (the default is localhost). This property is mandatory.
 - c. The TCP port on which the WebSphere MQ queue manager is listening (the default is 1414). This property must be a valid positive number.
 - d. Optional: The name of the Security Exit required to connect to the WebSphere MQ queue manager. This property must be a valid Java classname, but you can leave this box blank if it does not apply to your domain connection.
 - e. Optional: The location of the JAR file for the Security Exit required to connect to the WebSphere MQ queue manager. Use the Browse button to find the file location. You can leave this box blank if it does not apply to your domain connection.

Note: The location of the JAR file is required if a Security Exit class is entered.

- f. Optional: The cipher suite, distinguished names, CRL name list, key store, and trust store parameters required when enabling SSL (see “Implementing SSL authentication” on page 19 for more information). The cipher suite field displays available cipher suites. Click **More** to configure a custom cipher suite in the Broker Administration preferences window. If a cipher suite is not specified, all other fields in the SSL section are unavailable.

You can configure several domain connections in your workspace. Each domain connection has to address a different Configuration Manager, which needs to have a different WebSphere MQ queue manager, host name, or TCP port number. An error message is displayed in the wizard, if you try to create a second broker domain using the same queue manager, host name, and port number.
4. Click **Next** to begin the domain connection to the Configuration Manager.
5. If you click **Cancel**, the Create a New Domain Connection wizard closes and a forced disconnection from the domain occurs.
6. After the domain connection has been made, enter:
 - a. The name of your Server Project. This is the container for your domain connection. If you have not already created a server project, you can specify the name of a new project here. The server project is created with the domain connection.
 - b. The Connection Name. This is the name you give to the .configmgr file that contains the parameters to connect to the Configuration Manager.
7. Click **Finish** to create the domain connection.

The new domain connection is added to the Broker Administration Navigator view, under Domain Connections. Here the server project holds the .configmgr domain connection file.

The view of the broker domain is displayed in the Domains view.

Starting and stopping message flows

You can start and stop a message flow by either using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy, see Navigating broker domains using the Configuration Manager Proxy.

From the workbench you can start and stop:

- All message flows in all execution groups, assigned to a specific broker.
 - All message flows in a specific execution group.
 - A single message flow.
1. To start a message flow:
 - a. Switch to the Broker Administration perspective.
 - b. In the Domains view, expand your broker domain to locate your message flow:
 - To start all message flows in all execution groups for a broker, right-click the broker and click **Start Message Flows**.
 - To start all message flows in a specific execution group, right click the execution group and click **Start Message Flows**.
 - To start a single message flow, right-click the message flow and click **Start**.

The Configuration Manager sends a message to the broker to start the specified message flows.

A BIP0892I information message is displayed to show that the Configuration Manager has received the request. Verify the results of the deployment by opening the Event Log.

There might be a short delay for the Configuration Manager to respond.

The alert Message Flow is not running is removed from the Alert Viewer.

2. To stop a message flow:
 - a. Switch to the Broker Administration perspective.
 - b. In the Domains view, expand your broker domain to locate your message flow:
 - To stop all message flows in all execution groups for a broker, right-click the broker and click **Stop Message Flows**.
 - To stop all message flows in a specific execution group, right click the execution group and click **Stop Message Flows**.
 - To stop a single message flow, right-click the message flow, and click **Stop**.
 - c. Open the Event Log for the broker domain. A BIP0892I information message is displayed to show that the Configuration Manager has received the request.

There might be a short delay for the Configuration Manager to respond.

The alert Message Flow is not running is added to the Alert Viewer.

Starting and stopping a broker

Before you start:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to “Security requirements for administrative tasks” on page 423.
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before performing this task, by running the product profile or console; refer to Setting up a command environment.

To start and stop a broker, use the **mqsistart** and **mqsistop** commands from the command line.

Follow the link for the appropriate platform.

- “Starting and stopping a broker on Linux and UNIX systems”
- “Starting and stopping a broker on Windows”
- “Starting and stopping a broker on z/OS” on page 216

Starting and stopping a broker on Linux and UNIX systems

The following steps show you how to start and stop a broker.

1. Run '`<install_dir>/bin/mqsiprofile`' to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.

2. To start a broker, enter the following command on the command line:

```
mqsistart WBRK_BROKER
```

Substitute your own broker name for `WBRK_BROKER`. The broker and its associated queue manager are started. Check the syslog to ensure that the broker has initialized successfully.

3. To stop a broker, enter the following command on the command line:

```
mqsistop WBRK_BROKER
```

Substitute your own broker name for `WBRK_BROKER`.

You can also request that the broker’s queue manager is stopped by this command. Refer to “Stopping a WebSphere MQ queue manager when you stop a component” on page 220.

Starting and stopping a broker on Windows

The following steps show you how to start and stop a broker.

1. Run the `<install_dir>/bin/mqsiprofile` command to set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.

2. To start a broker, enter the following command on the command line:

```
mqsistart WBRK_BROKER
```

Substitute your own broker name for `WBRK_BROKER`.

You can also request that the broker’s queue manager is started as a Windows service. Refer to “Starting a WebSphere MQ queue manager as a Windows service” on page 219.

The broker and its associated queue manager are started. The command initiates the startup of the broker’s Windows service. Check the Application Log of the Windows Event Viewer to ensure that the broker has initialized successfully.

3. To stop a broker, enter the following command on the command line:

```
mqsistop WBRK_BROKER
```

Substitute your own broker name for WBRK_BROKER.

You can also request that the broker's queue manager is stopped by this command. Refer to "Stopping a WebSphere MQ queue manager when you stop a component" on page 220.

Starting and stopping a broker on z/OS

The following steps show you how to start and stop a broker.

1. From SDSF, start the component by using the command `/S <broker name>`. If MQP1BRK is the name of the broker, this command produces, for example, the following output:
+BIP9141I MQP1BRK 0 The component was started
2. To stop a broker use the command:
`/P <broker name>`

Starting and stopping a Configuration Manager

Before you start:

- Ensure that your user ID has the correct authorizations to perform the task; refer to "Security requirements for administrative tasks" on page 423.
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before performing this task, by running the product profile or console; refer to Setting up a command environment.

To start and stop a Configuration Manager, use the **mqsistart** and **mqsistop** commands from the command line.

Follow the link for the appropriate platform.

- "Starting and stopping a Configuration Manager on Linux and UNIX systems"
- "Starting and stopping a Configuration Manager on Windows" on page 217
- "Starting and stopping a Configuration Manager on z/OS" on page 217

Starting and stopping a Configuration Manager on Linux and UNIX systems

Use the **mqsistart** and **mqsistop** commands from the command line.

The following steps show you how to start and stop a Configuration Manager.

1. Run `'. <install_dir>/bin/mqsiprofile'` to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. To start a Configuration Manager, enter the following command:
`mqsistart CMGR01`
Substitute your own Configuration Manager name for CMGR01. The Configuration Manager and its associated queue manager are started.
3. To stop a Configuration Manager, enter the following command on the command line:
`mqsistop CMGR01`
Substitute your own Configuration Manager name for CMGR01.

You can also request that the Configuration Manager's queue manager is stopped by this command. Refer to "Stopping a WebSphere MQ queue manager when you stop a component" on page 220.

Starting and stopping a Configuration Manager on Windows

Use the **mqsistart** and **mqsistop** commands from the command line.

The following steps show you how to start and stop a Configuration Manager.

1. Run the `<install_dir>/bin/mqsiprofile` command to set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.

2. To start a Configuration Manager, enter the following command:

```
mqsistart CMGR01
```

Substitute your own Configuration Manager name for CMGR01. If you do not specify a name, the default of `configmgr` is used. The Configuration Manager and its associated queue manager are started. The command initiates the startup of the Configuration Manager's Windows service. Check the Application Log of the Windows Event Viewer to ensure that the Configuration Manager has initialized successfully.

You can also request that the Configuration Manager's queue manager is started as a Windows service. Refer to "Starting a WebSphere MQ queue manager as a Windows service" on page 219.

3. To stop a Configuration Manager, enter the following command on the command line:

```
mqsistop CMGR01
```

Substitute your own Configuration Manager name for CMGR01. If you do not specify a name, the default of `configmgr` is used.

You can also request that the Configuration Manager's queue manager is stopped by this command. Refer to "Stopping a WebSphere MQ queue manager when you stop a component" on page 220.

Starting and stopping a Configuration Manager on z/OS

The following steps show you how to start and stop a Configuration Manager.

1. From SDSF, start the component by using the command `/S <Configuration Manager name>`. If MQP1CMGR is the name of the Configuration Manager, this command produces, for example, the following output:

```
| +BIP9141I MQP1CMGR 0 The component was started
```

2. To stop a Configuration Manager use the command:

```
| /P <Configuration Manager name>
```

Starting and stopping the User Name Server

Before you start:

- Ensure that your user ID has the correct authorizations to perform the task. Refer to "Security requirements for administrative tasks" on page 423.
- On Windows, UNIX systems, and Linux, you must set up your command-line environment before performing this task, by running the product profile or console; refer to Setting up a command environment.

To start and stop a User Name Server use the **mqsistart** and **mqsistop** commands from the command line.

Follow the link for the appropriate platform.

- “Starting and stopping the User Name Server on Linux and UNIX systems”
- “Starting and stopping the User Name Server on Windows”
- “Starting and stopping the User Name Server on z/OS” on page 219

Starting and stopping the User Name Server on Linux and UNIX systems

1. Run '`. <install_dir>/bin/mqsiprofile`' to source the `mqsiprofile` script and set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. To start a User Name Server enter the following command on the command line:

```
mqsistart UserNameServer
```

The User Name Server and its associated queue manager are started. Check the syslog to ensure that the User Name Server has initialized successfully.

3. To stop a User Name Server enter the following command on the command line:

```
mqsistop UserNameServer
```

You can also request that the User Name Server's queue manager is stopped by this command. Refer to “Stopping a WebSphere MQ queue manager when you stop a component” on page 220.

Starting and stopping the User Name Server on Windows

The following steps show you how to start and stop a User Name Server.

1. Run the `<install_dir>/bin/mqsiprofile` command to set up the environment for a single targeted runtime. You must do this before you can run any of the WebSphere Event Broker commands.
2. To start a User Name Server:
 - a. Enter the following command on the command line:

```
mqsistart usernameserver
```

The User Name Server and its associated queue manager are started. The command initiates the startup of the User Name Server's Windows service. Check the Application Log of the Windows Event Viewer to ensure that the User Name Server has initialized successfully.

You can also request that the User Name Server's queue manager is started as a Windows service. Refer to “Starting a WebSphere MQ queue manager as a Windows service” on page 219.

3. To stop a User Name Server enter the following command on the command line:

```
mqsistop usernameserver
```

You can also request that the User Name Server's queue manager is stopped by this command. Refer to “Stopping a WebSphere MQ queue manager when you stop a component” on page 220.

Starting and stopping the User Name Server on z/OS

The following steps show you how to start and stop a User Name Server.

1. From SDSF, start the component by using the command `/S <User Name Server name>`. If MQP1UNS is the name of the User Name Server, this command produces, for example, the following output:
+BIP9141I MQP1UNS 0 The component was started
2. To stop a User Name Server, use the command:
`/P <User Name Server name>`

Starting a WebSphere MQ queue manager as a Windows service

Before you start:

You must complete the following task:

- Stop the queue manager for the WebSphere Event Broker component, using the `endmqm` command. If you prefer, you can use WebSphere MQ Version 5 Services or WebSphere MQ Version 6 Explorer.

When you start a WebSphere Event Broker component (broker, Configuration Manager, or User Name Server), the “`mqsistart` command” on page 357 starts the associated queue manager if it is not already running. When you start any of these components on Windows, it starts as a service on Windows, but the associated queue manager does not. You can change the properties of the queue manager service to set the startup type to automatic to enable the queue manager to run as a Windows service.

This change ensures that the operation of the queue manager is independent of the logged-on status of the user that starts the WebSphere Event Broker component.

To start a WebSphere MQ Version 5 queue manager as a Windows service:

1. Click **Start** → **Programs** → **IBM** → **IBM WebSphere MQ** → **WebSphere MQ Services**.
2. Right-click the queue manager and select **Properties**, and the **General** tab.
3. Change the **Startup Type** to *Automatic*. This setting ensures that the queue manager is started whenever the WebSphere MQ Service (a Windows service) is started.
4. (Optional) Change the properties of the WebSphere MQ Services service by updating its **Startup Type** to *Automatic* using the Control Panel. This setting starts WebSphere MQ Services when Windows itself starts and isolates the operation of the WebSphere MQ Services service from any logged on user.
5. Restart the queue manager for the WebSphere Event Broker component using the `strmqm` command or WebSphere MQ Services. The changes to the queue manager’s startup type take effect when you restart Windows.
6. Start the component using the “`mqsistart` command” on page 357.

To start a WebSphere MQ Version 6 queue manager as a Windows service:

1. Click **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**.
2. In the left pane, right-click the queue manager and select **Properties**. The Properties dialog opens. The General properties are displayed.
3. Find the Startup property and set it to *Automatic*.

4. Click **OK**. The Properties dialog closes and the change is applied.
5. Restart the queue manager for the WebSphere Event Broker component using the `strmqm` command or WebSphere MQ Explorer. The changes to the queue manager's startup type take effect when you restart Windows.
6. Start the component using the "`mqsistart` command" on page 357.

Stopping a WebSphere MQ queue manager when you stop a component

Before you start:

You must complete the following task:

- If you are using a single queue manager to support more than one WebSphere Event Broker component (a single broker can also be defined on the same queue manager as a Configuration Manager, or the User Name Server, or both), you are recommended to specify the `-q` flag only on the final stop command, having stopped the other components first. The `-q` flag initiates a queue manager termination regardless of any other component currently using that queue manager.

If you are preparing to stop a broker, Configuration Manager or User Name Server, you can stop the component's WebSphere MQ queue manager at the same time.

You can specify a `-q` parameter on the **`mqsistop`** command to initiate a controlled shutdown of the queue manager for a WebSphere Event Broker component.

To stop a WebSphere MQ queue manager enter the following command on the command line:

```
mqsistop WBRK_BROKER -q
```

where:

`WBRK_BROKER` is the name of the component.

`-q` stops the WebSphere MQ queue manager associated with the component.

The command cannot complete until shutdown of the queue manager has completed.

Viewing broker domain log information

You can view broker domain log information by either using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP and Class `com.ibm.broker.config.proxy.LogProxy`*.

Broker domain log information is written to the Event Log editor in the `workbench`.

The Event Log contains information about events that occur within your broker domain. These events can be information, errors, or warnings and relate to your own actions. To view events for a particular broker, look for the name of the broker in the Source column.

Each event contains the following information:

- Message: The event number.
- Source: Where the event has come from (within the broker domain).
- TimeStamp: The date and time that the event occurred. TimeStamps are taken from the computer that is hosting the Configuration Manager.
- Details: What has caused the event and what action is needed to rectify it.

The following steps show how to view broker domain log information.

1. Switch to the Broker Administration perspective.
2. In the Domains view, expand the broker domain with which you want to work, to reveal the Event Log.
3. Double-click the Event Log. All broker domain log information specific to the broker domain with which you are working is displayed in the Event Log editor.

If the broker domain is not connected, you are prompted to connect to the broker domain before the Event Log is opened.

The Event Log editor has two panes called Logs and Details. The top half of the view lists all the events, in date and time order. The bottom half of the view shows the details of a specific selected event. You can maximize and minimize each pane, and toggle between them.

4. Click the event that you want to view in more detail from the top half of the Event Log view. The details of this event can then be viewed in the bottom half of the view.

When you filter information, as described in “Filtering broker domain log information” on page 222, a note appears next to the view label to indicate that a filter has been applied.

Refreshing broker domain log information

Messages about events that occur in the broker domain are created in the Event Log editor.

To refresh the Event Log editor with new messages:

1. Switch to the **Broker Administration perspective**.
2. In the **Domains** view, expand the appropriate domain to display its components.
3. Double-click on **Event Log** to launch the Event Log editor in the editor area.
4. Right-click in the **Logs** pane and click **Revert** from the pop-up menu. **Revert** does not remove or overwrite existing messages in the Event Log editor or the configuration repository.

Filtering broker domain log information

Broker domain log information is written to the Event Log editor in the workbench. The Event Log contains information about events that occur in a broker domain. For each event, the Event log records the following details:

- Event type (whether the event is information, an error or a warning)
- Event source (what caused the event, and where it originates within the broker domain, for example the configuration manager, and specified message brokers)
- Event timestamp (the date and time when the event occurred)

You can filter on the type, the source and the timestamp of the message, to restrict the number of log entries that are displayed in the Event Log editor. You can also filter events, event by event, to view a particular set of events in the Event log editor. The filter settings you define are kept for your next session. A note also appears next to the view label to indicate that a filter has been applied.

To filter entries, use the Filter Event Log dialog:

1. Switch to the Broker Administration perspective.
2. In the Domains view, open the Event Log for the appropriate broker domain.
3. From the Event Log editor menu, click **Event Log editor > Filter Log ...**. This action opens the Filter Log dialog.

The Filter Log dialog has the following controls:

- A check box for each of the three message types (information, error or warning)
- A check box for each of the possible message sources for all known entries so far
- Under the source check boxes, a **Select All** button to select all sources and a **Deselect All** button to deselect all sources
- A non-editable drop-down list containing each possible timestamp of all known entries so far
- A table of check box items for each log entry, with a vertical scroll bar to access additional entries
- Under the table, a **Select All** button to select all events, and a **Deselect All** button to deselect all events from this table
- A **Restore Defaults** button

In the default view of the Log Filter, all message type check boxes are selected, indicating that messages of all three types are displayed. All message source check boxes are also selected by default, indicating that messages of all sources are displayed. The timestamp is the one for the oldest known event so far. All events are selected in the table.

To restore the default settings, click **Restore Defaults** (the defaults are: all types selected, all sources selected, timestamp set to oldest event one, all events selected).

To discard all changes, click **Cancel**.

To save the current filter settings, click **OK**. This applies the settings to the opened editor (event filtering is based on the new settings, and the editor is refreshed).

Using the Event Log Filter, you can filter broker domain log information in the following ways:

- Filter by message type, so that the log only displays messages of a particular type:
 - a. Clear the check boxes for all three event types.
 - b. Check the check box of the event type that you want to view (you can view more than one type by selecting the appropriate check boxes). All events with the selected types are selected in the filter dialog table of entries.
 - c. Click OK to activate the filter. All events with the selected types are displayed in the editor.
- Filter by message source, so that the log only displays messages from one source:
 - a. Deselect all sources, click the **Deselect All** button under the source check boxes, or clear the check boxes for all sources.
 - b. Check the check box of the event source that you want to view (you can view more than one source by selecting the appropriate check boxes). You can also view all sources click by clicking the **Select All** button under the source check boxes. All events with the selected sources are selected in the filter dialog table of entries.
 - c. Click **OK** to activate the filter. All events with the selected sources are displayed in the editor.
- Filter by timestamp, so that the log hides messages generated before a specified timestamp:
 - a. Open the **Hide Events generated before** drop-down list by clicking the down arrow. Select the timestamp you want to filter on. All events generated before this timestamp are deselected in the filter dialog table of entries.
 - b. Click **OK** to activate the filter. All events generated before the reference timestamp are hidden in the editor. All other events are displayed.

You can combine filtering options (type, source, time stamp). The combinations you select are identified in the table (entries are automatically ticked or non-ticked to indicate the choices you make). The editor is also updated based on the events tables which combines all filtering options. Ticked entries are displayed, non-ticked entries are hidden. For incoming new events, the filtering options based on type, source, timestamp are applied.

Saving broker domain log information

Broker domain log information is written to the Event Log Editor in the workbench.

Event Log information is deleted automatically from the Configuration Manager after 72 hours.

To save broker domain log information:

1. Switch to the Broker Administration perspective.
2. Open the Event Log for the appropriate broker domain.
3. Right-click in the Event Log view and click **Save Log As...**
4. You are prompted to save the log information to an appropriate directory. By default the log is saved as log.txt. However, you can change the name of this text file.

The file can also be saved using XML format, with .xml file extension.

Each message recorded in the event log is written to the text file with the same information that is detailed in the event log itself.

To view the log, open the log.txt file in an appropriate text editor.

Clearing broker domain log information

You can clear broker domain log information by either using the Message Brokers Toolkit or by using the Configuration Manager Proxy Java API. This topic describes how to use the Message Brokers Toolkit. For information about how to use the Configuration Manager Proxy (CMP), see *Developing applications using the CMP* and Class `com.ibm.broker.config.proxy.LogProxy`.

To clear all the broker domain log information from the Event Log:

1. Switch to the **Broker Administration** perspective.
2. Open the Event Log for the appropriate broker domain.
3. In the Event Log editor menu, click **Event Log Editor** → **Clear Log ...**

If you have set user preference to warn before deleting events, a prompt asks you to confirm deletion. Click **OK**.

If you have not set user preferences to warn before deleting events, the event log is cleared automatically.

When you clear the event log, all recorded events that are in view are deleted from the repository.

Changing Event Log editor preferences

You can change the following preferences for the Event Log editor:

- Choose not to display a warning before deleting log events. The default is to display a warning.
- Change the color for each type of event (Warning, Information, and Error). You can choose from a palette of basic colors or define custom colors. The default color for all events is black.
- Define the style and size of the font used for event details. The default is *Tahoma*, regular, 8 point.

To change preferences:

1. Switch to the **Broker Administration** perspective.
2. Click **Window>Preferences**.
3. Expand the **Broker Administration** category in the left pane.
4. Click **Event Log Editor** within the expanded **Broker Administration** category to open the Event Log editor preferences page.
5. Make your selections.
6. Click **OK**.

Backing up resources

Brokers rely on a database manager to maintain and control their configuration data. Brokers, the Configuration Manager, and the User Name Server rely on WebSphere MQ to transport and guarantee messages between components. You must establish a backup process that includes these sources of information to preserve the integrity and consistency of your broker domain.

It is important that you maintain regular backups of your broker domain and associated databases. You should refer to the information supplied with the database you are using for details of the relevant database backup procedures.

Consult your database administrator and agree upon the:

- Frequency of backups
- Quiesce backup points to take

Depending upon your workflow, this can be hourly or daily or weekly.

You should aim to always be in a position to recover to a specific point in time, whatever happens. For example, take a backup of the broker domain and quiesce of the broker databases before installing a new application.

The following topics tell you how to back up and restore brokers, the Configuration Manager and the Message Brokers Toolkit workspace:

- “Backing up the broker domain on distributed systems”
- “Backing up the broker domain on z/OS” on page 227
- “Backing up the Message Brokers Toolkit workspace” on page 228

Backing up the broker domain on distributed systems

These steps tell you how to back up a broker domain so that it can be restored for migration purposes or, in the event of an unrecoverable failure. The backup and restoration of a broker needs to extend to every broker that is deployed to by the Configuration Manager. All the topics that you need to carry out these steps are listed in the ‘Related information’ section at the end of this topic.

To back up the components:

1. Stop each broker.
2. Stop the Configuration Manager.
3. Back up the Configuration Manager data repository using the **mqsibackupconfigmgr** command.
4. If you plan to restore the Configuration Manager data repository on distributed systems, you must take a copy of the file:

```
| <data directory>/components/<Configuration  
| Manager name>/<directory name>/service.properties
```

The <data directory> is platform specific:

- On Windows the directory is:
C:\Documents and Settings\All Users\Application Data\IBM\MQSI
- On the other distributed platforms the directory is:
/var/mqsi

This needs to be kept with the zip file produced by the `mqsibackupconfigmgr` command, and must be copied to the equivalent place in the restored Configuration Manager data repository after running the `mqsirestoreconfigmgr` command.

5. Back up each broker database.

For example, for a DB2 broker database use the Backup wizard in the DB2 Control Center, or a command similar to:

```
DB2 BACKUP DATABASE <broker db> TO "<backup directory>"
```

6. Back up the system work path.

The work path is platform specific:

- On Windows the directory is:
C:\Documents and Settings\All Users\Application Data\IBM\MQSI
- On the other distributed platforms the directory is:
/var/mqsi

and any broker-specific work paths. These paths are the ones specified by the `-w` flag on the `mqsicreatebroker` command.

To restore the components:

1. **Stop and remove the existing components in the Configuration Manager domain.**
 - a. Disconnect from the domain on the Message Brokers Toolkit.
 - b. Stop each broker.
 - c. Stop the Configuration Manager.
 - d. Delete each broker using the `mqsdeletebroker` command, specifying the `-w` parameter, which is an optional parameter on Windows and UNIX platforms that deletes from the work path all files related to these brokers.
 - e. Delete the Configuration Manager using the `mqsdeleteconfigmgr` command, specifying the `-w` and `-n` parameters. The `-n` parameter deletes all data in the configuration repository.
2. **Recreate the components.**
 - a. Create the Configuration Manager.
 - b. Create each broker.
3. **Restore the components.**
 - a. Restore any work paths.
 - b. Restore the Configuration Manager repository using the `mqsirestoreconfigmgr` command.
Replace the previously backed-up `service.properties` file
 - c. Restore each broker database.
For example, for a DB2 broker database use the Restore wizard in the DB2 Control Center, or a command similar to:

```
DB2 RESTORE DATABASE <broker db> FROM "<backup directory>" TAKEN AT <datetime>
```
 - d. Start the Configuration Manager.
 - e. Start each broker.
 - f. Connect to the Configuration Manager on the Message Brokers Toolkit. This re-imports the broker topology, excluding execution groups and flows, from the Configuration Manager.

- g. Deploy the topology configuration on the Message Brokers Toolkit. This causes the Configuration Manager to give the UUIDs to the brokers. Note that if you are working on a platform other than Windows, this step is unnecessary.

Backing up the broker domain on z/OS

These steps tell you how to back up a broker domain so that it can be restored for migration purposes or, in the event of an unrecoverable failure. The backup and restoration of a broker needs to extend to every broker that is deployed to by the Configuration Manager. All the topics that you need to carry out these steps are listed in the 'Related information' section at the end of this topic.

To back up the components:

1. Stop each broker.
2. Note the BrokerUUID value from the following file: <broker directory>/registry/<broker name>/CurrentVersion/BrokerUUID.
3. Stop the Configuration Manager.
4. Back up the Configuration Manager data repository using the **mqsibackupconfigmgr** command, or JCL job BIPBUCM.
5. Back up each broker database.

To restore the components:

1. **Stop and remove the existing components in the Configuration Manager domain.**
 - a. Disconnect from the domain on the Message Brokers Toolkit.
 - b. Stop each broker.
 - c. Stop the Configuration Manager.
 - d. Delete each broker.
 - e. Delete the Configuration Manager.
2. **Recreate the components.**
 - a. Create the Configuration Manager repository.
 - b. Create each broker.
3. **Restore the components.**
 - a. Restore the Configuration Manager repository using the **mqsirestoreconfigmgr** command, or JCL job BIPRSCM.
 - b. Restore each broker database.
 - c. Set the BrokerUUID by editing the following file: <broker directory>/registry/<broker name>/CurrentVersion/BrokerUUID.
 - d. Start the Configuration Manager.
 - e. Start each broker.
 - f. Connect to the Configuration Manager on the Message Brokers Toolkit. This re-imports the broker topology, excluding execution groups and flows, from the Configuration Manager.
 - g. Deploy the topology configuration on the Message Brokers Toolkit. This causes the Configuration Manager to give the UUIDs to the brokers.

Backing up the Message Brokers Toolkit workspace

The Message Brokers Toolkit workspace contains your personal settings and data, such as message flow and message set resources. On Windows, the default workspace directory is created at `C:\Documents and Settings\user\IBM\wmbt6.0\workspace`, and on Linux, the default workspace directory is created at `/home/user/IBM/wmqi6.0/workspace`, where *user* is the user name with which you are logged on.

You can have multiple workspaces in different locations and you can have references to projects that are in other locations as well, so consider all of these locations when you back up your resources.

The workspace directory contains a directory called `.metadata`, which contains your personal settings and preferences for the Message Brokers Toolkit. If the `.metadata` directory gets corrupted, you lose these settings and the Message Brokers Toolkit reverts to the default layout and preferences; if you have not backed up the `.metadata` directory, you must manually set any preferences again and import any projects, such as message flow projects, that were displayed in the Resource Navigator view. To back up the `.metadata` directory, just take a copy of the directory.

In addition to the `.metadata` directory, in the workspace, there is a directory for each project that you have created in the Message Brokers Toolkit, including message flow projects, message set projects, and server projects. These directories contain your data, which should be backed up. There are various ways that you can back up the data in your workspace, including the following three methods:

- Export the projects from within the Message Brokers Toolkit. You can export the projects directly as a zip file. For instructions, see *Exporting in the Eclipse Workbench User Guide*.
- Copy the project directories from the workspace directory to another location.
- When you add resources to a broker archive (`bar`) file ready for deployment, you can select the **Include source files** check box which adds the message flow and message set source files, as well as the compiled files, to the `bar` file. You can then take copies of the `bar` file to back up its contents.

To restore the resources, copy the directories back to your workspace directory and import the projects. For instructions, see *Importing in the Eclipse Workbench User Guide*.

Part 4. Reference

Operations	231
Broker properties	231
Commands	232
Summary of commands on Windows platforms, Linux, UNIX systems, and z/OS	233
Syntax diagrams: available types	236
Characters allowed in commands.	240
Rules for using commands	241
Responses to commands.	242
Message Brokers Toolkit commands	242
Runtime commands	248
z/OS specific information	367
Administration in z/OS	368
z/OS customization	370
z/OS JCL variables	382
z/OS sample files supplied.	385
Security requirements for administrative tasks	423
ACL permissions	423
Security requirements for Linux and UNIX platforms.	424
Security requirements for Windows platforms	425
Security requirements for z/OS	428

Operations

Follow the links below for more information:

- “Broker properties”
- “Commands” on page 232
- “z/OS specific information” on page 367

Broker properties

The following table is a reference for the broker properties.

Property	Meaning
Queue Manager Name	The name of the WebSphere MQ queue manager being used by the broker. The name must be exactly the same name specified for this broker’s queue manager on the mqsicreatebroker command.
Interbroker Host Name	Interbroker host name to use.
Interbroker Port Number	Interbroker port number to use.
Authentication Protocol Type	The authentication protocols that the broker supports. There are four authentication protocols: P Password in the clear M Mutual Challenge and response S Asymmetric SSL R Symmetric SSL
SSL Key Ring File Name	The filename (including path) to the SSL Key Ring file. This is required for authentication when using the Asymmetric and Symmetric (S and R) authentication protocols. The file name and path refer to the path accessible from the broker and not necessarily the tooling, if on different machines.
SSL Password File Name	The SSL key ring file is encrypted and requires a passphrase to decode it. This field is used to specify the filename containing the passphrase required. The file name and path refer to the path accessible from the broker and not necessarily the tooling, if on different machines.
SSL HTTP Listener	Use the “mqsicreateusernameeserver command” on page 305 or “mqsichangeusernameeserver command” on page 279 to enable the SSL HTTP Listener authentication options.

The following three properties:

- Temporary Topic Quality Of Protection
- Sys Topic Quality Of Protection
- ISys Topic Quality Of Protection

refer to the Message Protection feature (QoP) on the “mqsichangeproperties command” on page 264. See “Implementing quality of protection” on page 26 for details on setting these for temporary topics.

Commands

This topic lists the Message Brokers Toolkit commands, followed by the other commands grouped by function, provided by WebSphere Event Broker on distributed systems.

The “Summary of commands on Windows platforms, Linux, UNIX systems, and z/OS” on page 233 lists the comparable commands on WebSphere Event Broker for z/OS.

WebSphere Event Broker Toolkit commands

mqsicreatebar	“mqsicreatebar command” on page 242
mqsimigratemsgflows	“mqsimigratemsgflows command” on page 245
mqsireadbar	“mqsireadbar command” on page 247

WebSphere Event Broker commands

Broker commands

mqsicreatebroker	“mqsicreatebroker command” on page 286
mqsichangebroker	“mqsichangebroker command” on page 250
mqsideletebroker	“mqsideletebroker command” on page 311
mqsicreateexecutiongroup	“mqsicreateexecutiongroup command” on page 302
mqsideleteexecutiongroup	“mqsideleteexecutiongroup command” on page 316
mqsireload	“mqsireload command” on page 346
mqsicbrreport	“mqsicbrreport command” on page 249

Database commands

mqsicreatedb	“mqsicreatedb command” on page 300
mqsichangedbimgr	“mqsichangedbimgr command” on page 259
mqsidedetedb	“mqsidedetedb command” on page 315
mqsi_setupdatabase	“mqsi_setupdatabase command” on page 356

Configuration Manager commands

mqsicreateconfigmgr	“mqsicreateconfigmgr command” on page 296
mqsichangeconfigmgr	“mqsichangeconfigmgr command” on page 256
mqsideleteconfigmgr	“mqsideleteconfigmgr command” on page 313
mqsibackupconfigmgr	“mqsibackupconfigmgr command” on page 248
mqsirestoreconfigmgr	“mqsirestoreconfigmgr command” on page 354

User Name Server commands

mqsicreateusernameserver	“mqsicreateusernameserver command” on page 305
mqsichangeusernameserver	“mqsichangeusernameserver command” on page 279
mqsideleteusernameserver	“mqsideleteusernameserver command” on page 318

Start and stop commands

mqsistart	“mqsistart command” on page 357
mqsistop	“mqsistop command” on page 362

	<code>mqsistartmsgflow</code>	“mqsistartmsgflow command” on page 359
	<code>mqsistopmsgflow</code>	“mqsistopmsgflow command” on page 365
List and trace commands		
	<code>mqsilist</code>	“mqsilist (list resources) command” on page 328
	<code>mqsichangetrace</code>	“mqsichangetrace command” on page 274
	<code>mqsiformatlog</code>	“mqsiformatlog command” on page 325
	<code>mqsireadlog</code>	“mqsireadlog command” on page 342
	<code>mqsireporttrace</code>	“mqsireporttrace command” on page 351
WebSphere MQ Publish/Subscribe interoperability commands		
	<code>mqsiclearmqpubsub</code>	“mqsiclearmqpubsub command” on page 282
	<code>mqsijoinmqpubsub</code>	“mqsijoinmqpubsub command” on page 327
	<code>mqsilistmqpubsub</code>	“mqsilistmqpubsub command” on page 335
Migration commands		
	<code>mqsimigratecomponents</code>	“mqsimigratecomponents command” on page 337
Properties commands		
	<code>mqsichangeproperties</code>	“mqsichangeproperties command” on page 264
	<code>mqsireportproperties</code>	“mqsireportproperties command” on page 349
Statistics commands		
	<code>mqsichangeflowstats</code>	“mqsichangeflowstats command” on page 260
	<code>mqsireportflowstats</code>	“mqsireportflowstats command” on page 347
Miscellaneous commands		
	<code>mqsicreateaclentry</code>	“mqsicreateaclentry command” on page 283
	<code>mqsicreateexecutiongroup</code>	“mqsicreateexecutiongroup command” on page 302
	<code>mqsideleteaclentry</code>	“mqsideleteaclentry command” on page 308
	<code>mqsideleteexecutiongroup</code>	“mqsideleteexecutiongroup command” on page 316
	<code>mqsideploy</code>	“mqsideploy command” on page 320
	<code>mqsilistaclentry</code>	“mqsilistaclentry command” on page 330
	<code>mqsisetsecurity</code>	“mqsisetsecurity command” on page 355

Summary of commands on Windows platforms, Linux, UNIX systems, and z/OS

The following table summarizes the *runtime* commands available on Windows platforms, Linux, and UNIX systems and provides the z/OS equivalent, where it is available.

Command on Windows platforms, Linux, and UNIX systems	z/OS equivalent: type	z/OS equivalent	z/OS References
<code>mqsibackupconfigmgr</code>	Utility JCL	BIPBUM	“Contents of the Configuration Manager PDSE” on page 380
<code>mqsicbrreport</code>	N/A.	-	-

mqsichangebroker	1. Console command: modify 2. Utility JCL	1. changebroker 2. BIPCHBK	1. "mqsichangebroker command" on page 250 2. "Contents of the broker PDSE" on page 378
mqsichangeconfigmgr	1. Console command: modify 2. Utility JCL	1. changeconfigmgr 2. BIPCHCM	1. "mqsichangeconfigmgr command" on page 256 2. "Contents of the Configuration Manager PDSE" on page 380
mqsichangedbimgr	N/A	-	-
mqsichangeflowstats	1. Console command: modify 2. Utility JCL	1. changeflowstats 2. BIPCHMS	1. "mqsichangeflowstats command" on page 260 2. "Contents of the broker PDSE" on page 378
mqsichangeproperties	Utility JCL	BIPCHPR	"Contents of the broker PDSE" on page 378
mqsichangetrace	console command: modify	changetrace	"mqsichangetrace command" on page 274
mqsichangeusernameserver	1. Console command: modify 2. Utility JCL	1. changeusernameserver 2. BIPCHUN	1. "mqsichangeusernameserver command" on page 279 2. "Contents of the User Name Server PDSE" on page 379
mqsiclearmqpubsub	Utility JCL	BIPCLMP	"Contents of the broker PDSE" on page 378
mqsicreateaclentry	1. Console command: modify 2. Utility JCL	1. createaclentry 2. BIPCRACL	1. "mqsicreateaclentry command" on page 283 2. "Contents of the Configuration Manager PDSE" on page 380
mqsicreatebroker	UNIX System Services command	"mqsicreatebroker command" on page 286	"mqsicreatebroker command" on page 286
mqsicreateconfigmgr	Utility JCL	BIPRCRM	"Contents of the Configuration Manager PDSE" on page 380
mqsicreateexecutiongroup	Utility JCL	BIPCREG	"Contents of the Configuration Manager PDSE" on page 380
mqsicreateusernameserver	UNIX System Services command	"mqsicreateusernameserver command" on page 305	"mqsicreateusernameserver command" on page 305
mqsideleteaclentry	1. Console command: modify 2. Utility JCL	1. deleteaclentry 2. BIPDLACL	1. "mqsideleteaclentry command" on page 308 2. "Contents of the Configuration Manager PDSE" on page 380
mqsideletebroker	Utility JCL	BIPDLBK	"Contents of the broker PDSE" on page 378

mqsdeleteconfigmgr	Utility JCL	BIPDLCM	"Contents of the Configuration Manager PDSE" on page 380
mqsdeleteexecutiongroup	Utility JCL	BIPDLEG	"Contents of the Configuration Manager PDSE" on page 380
mqsdeleteusernameserver	Utility JCL	BIPDLUN	"Contents of the User Name Server PDSE" on page 379
mqsdeploy	1. Console command: modify 2. Utility JCL	1. deploy 2. BIPDPLY	1. "mqsdeploy command" on page 320 2. "Contents of the broker PDSE" on page 378
mqsifformatlog	Utility JCL	BIPFMLG	"Contents of the broker PDSE" on page 378
mqsijoinmqpubsub	Utility JCL	BIPJNMP	"Contents of the broker PDSE" on page 378
mqsilist	1. Console command: modify 2. Utility JCL	1. list 2. BIPLIST	1. "mqsilist (list resources) command" on page 328 2. "Contents of the Configuration Manager PDSE" on page 380
mqsilistaclentry	1. Console command: modify 2. Utility JCL	1. listaclentry 2. BIPLIACL	1. "mqsilistaclentry command" on page 330 2. "Contents of the Configuration Manager PDSE" on page 380
mqsilistmqpubsub	Utility JCL	BIPLSMP	"Contents of the broker PDSE" on page 378
mqsimigratecomponents	Utility JCL	BIPMGCMP	"mqsimigratecomponents command" on page 337
mqsireadlog	Utility JCL	BIPRELG	"Contents of the broker PDSE" on page 378
mqsireload	console command: modify	reload	"mqsireload command" on page 346
mqsireportflowstats	1. Console command: modify 2. Utility JCL	1. reportflowstats 2. BIPRPMS	1. "mqsireportflowstats command" on page 347 2. "Contents of the broker PDSE" on page 378
mqsireportproperties	Utility JCL	BIPRPPR	"Contents of the broker PDSE" on page 378
mqsireporttrace	console command: modify	reporttrace	"mqsireporttrace command" on page 351
mqsirestoreconfigmgr	Utility JCL	BIPRSCM	"Contents of the Configuration Manager PDSE" on page 380
mqsisetdbparms	Utility JCL	BIPSDBP	mqsisetdbparms command
mqsisetsecurity	N/A	-	-

mqsistart	1. Console command: start 2. console command: modify	1. standard MVS start command 2. startcomponent	1. - 2. "mqsistart command" on page 357
mqsistartmsgflow	Utility JCL	BIPSTMF	"Contents of the Configuration Manager PDSE" on page 380
mqsistop	1. console command: stop 2. console command: modify	1. standard MVS stop command 2. 'p' stopcomponent	1. - 2. "mqsistop command" on page 362
mqsistopmsgflow	Utility JCL	BIPSPMF	"Contents of the Configuration Manager PDSE" on page 380

Syntax diagrams: available types

The syntax for commands is presented in the form of a diagram. The diagram tells you what you can do with the command, and indicates relationships between different options and, sometimes, different values of an option. There are two types of syntax diagrams: railroad diagrams and dotted decimal diagrams. Railroad diagrams are a visual format suitable for sighted users. Dotted decimal diagrams are text-based diagrams that are more helpful for blind or partially-sighted users.

To select which type of syntax diagram you use, click the appropriate button above the syntax diagram in the topic that you are viewing.

The following topics describe how to interpret each type of diagram:

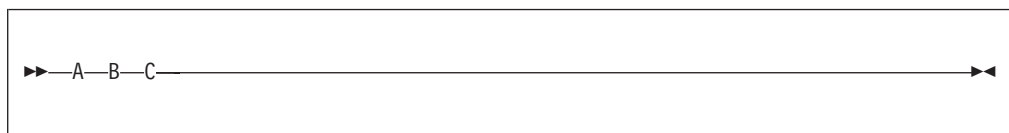
- "How to read railroad diagrams"
- "How to read dotted decimal diagrams" on page 238

How to read railroad diagrams

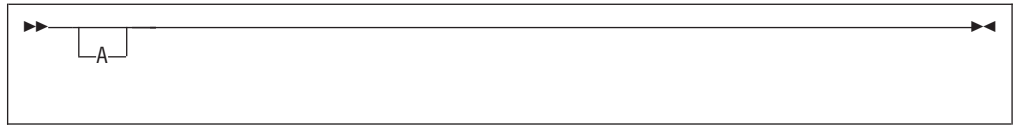
Each railroad diagram begins with a double right arrow and ends with a right and left arrow pair. Lines beginning with a single right arrow are continuation lines. You read a railroad diagram from left to right and from top to bottom, following the direction of the arrows.

The following examples show other conventions used in railroad diagrams.

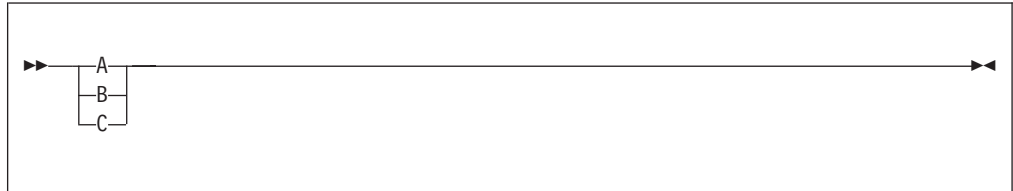
This example shows that you must specify values A, B, and C. Required values are shown on the main line of a railroad diagram:



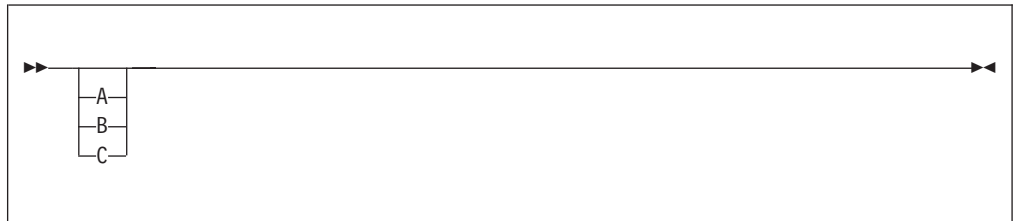
This shows that you can specify value A. Optional values are shown below the main line of a railroad diagram:



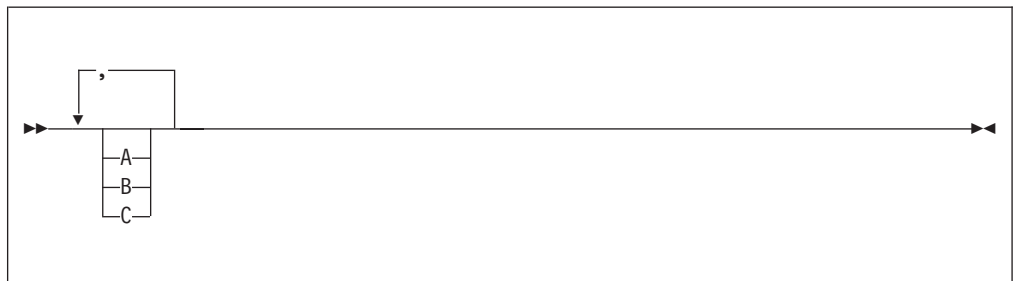
The next example specifies that values A, B, and C are options, one of which you must specify:



Values A, B, and C are options in this example, one of which you can specify:



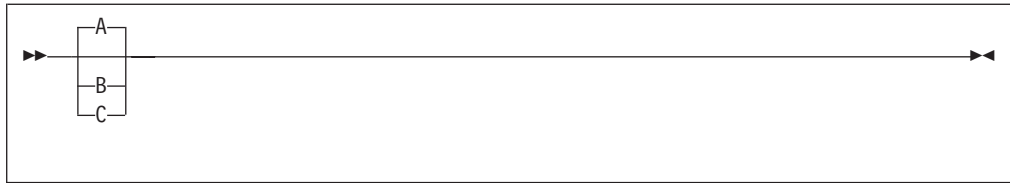
The next example shows that you can specify one or more of the values A, B, and C. Any required separator for multiple or repeated values (in this example, the comma (,)) is shown on the arrow:



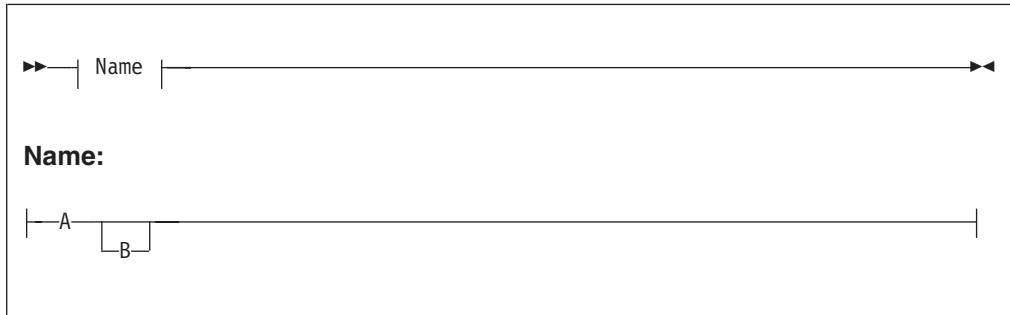
In this example, you can specify value A multiple times. The separator in this example is optional:



Values A, B, and C are alternatives in the next example, one of which you can specify. If you specify none of the values shown, the default A (the value shown above the main line) is used:



The last example shows the use of a syntax fragment Name, which is shown separately from the main railroad diagram. This technique is used to simplify the diagram, or help fit it into the page of text. The fragment could be used multiple times in the railroad diagram:



Punctuation and uppercase values must be specified exactly as shown.

Lowercase values (for example, *name*) indicate where to type your own text in place of the *name* variable.

How to read dotted decimal diagrams

In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line, because they can be considered as a single compound syntax element.

Each line starts with a dotted decimal number, for example 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that your screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. For example, if you hear the lines 3.1 USERID, 3.1 SYSTEMID, you know that your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with the dotted decimal number 3 is followed by a series of syntax elements with the dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Characters such as commas that are used to separate a string of syntax elements are shown in the syntax just before the items that they separate. They can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line might also show another symbol giving information about the syntax elements; all these symbols are explained below. For example, the lines 5.1* , , 5.1 LASTRUN, 5.1 DELETE mean that if you use more than one of the syntax elements LASTRUN and DELETE, they must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, this indicates a reference that is defined elsewhere. The string following the % is the name of a syntax fragment, rather than a literal. For example, the line 2.1 %OP1 means that, at this point, you must refer to the separate syntax fragment OP1. OP1, in the syntax from which this example was taken, gave a list of further options.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the escape character, which is a \ (backslash). For example, the * symbol can be used next to a dotted decimal number to mean that this syntax element can be repeated. If a syntax element actually starts with the * symbol, for example a syntax element * FILE with the dotted decimal number 3, it is given in the format 3 * FILE. If the format is 3* FILE, this means that there is a syntax element FILE, which can be repeated. If the format is 3* * FILE, this means that there is a syntax element * FILE, which can be repeated.

The words and symbols used next to the dotted decimal numbers are as follows:

- **? means an optional syntax element.** If a dotted decimal number is followed by the ? symbol, this means that all the syntax elements with that dotted decimal number, and any subordinate syntax elements that they each have, are optional. If there is only one syntax element with that dotted decimal number, the ? symbol appears on the same line as the syntax element, for example 5? NOTIFY. If there is more than one syntax element with that dotted decimal number, the ? symbol appears on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional; you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.
- **! means a default syntax element.** If a dotted decimal number is followed by the ! symbol, appended to the last digit of the dotted decimal number, this means that this syntax element is the default of all the elements with the same dotted decimal number. Only one of the syntax elements that share the same dotted decimal number can specify a !. For example, if you hear the lines 2? FILE, 2.1! (KEEP), 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. If you include the FILE keyword, but do not state your choice of option, the default option KEEP is applied. As well as the particular syntax element marked with the ! symbol, the default also applies to the next higher dotted decimal number. In the example above, the default applies to 2? FILE as well as to 2.1! (KEEP), meaning that, if you omit the word FILE, the default FILE(KEEP) is used. However, you might instead hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), 2.1.1 (DELETE). As the default only applies to the next higher dotted decimal number, which in this case is 2.1, it does not apply to 2? FILE. In this case, if you omit the word FILE, nothing is used.
- *** means a syntax element that is optional and can be repeated.** If a dotted decimal number is followed by the * symbol, this means that this syntax element is optional, and can be repeated. For example, if you hear the line 5.1* data-area, you know that you can include more than one data area, or you can include none. If you hear the lines 3*, 3 HOST, 3 STATE, you know that you can include HOST, STATE, both, or nothing. If a dotted decimal number has an asterisk next to it, and there is only one item with that dotted decimal number, you can repeat that same item more than once. If a dotted decimal number has an asterisk next to it, and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than

once each. In the example above, you could write HOST STATE, but you could not write HOST HOST. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

- **+ means a syntax element that must be included at least once, and can be repeated.** If a dotted decimal number is followed by the + symbol, this means that this syntax element must be included at least once, and can be repeated. For example, if you hear the line 6.1+ data-area, you know that you must include at least one data area, and you can include more than one. If you hear the lines 2+, 2 HOST, 2 STATE, you know that you must include HOST, STATE, or both. As for the + symbol, you can only repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Characters allowed in commands

There are a few rules you must adhere to when you provide names or identifiers for the components and resources in your broker domain.

The components of the broker domain are:

- Brokers
- The Configuration Manager
- The User Name Server (this component is optional)

The broker resources are:

- Execution groups
- Message sets and messages
- Message flows
- Topics

The character set that you can use to name brokers, Configuration Managers, execution groups, and message identifiers is as follows:

- Uppercase A-Z
- Lowercase a-z
- Numerics 0-9
- Any special characters supported by the underlying file system:
 - The following special characters are accepted on Windows platforms:

\$	%	' (apostrophe)	' (quote)
- (dash)	_ (underscore)	@	~ (tilde)
!	()	{
}	[]	&
#	&	+	, (comma)
;	=	(space)	

- The following special characters, with the exception of a space, are accepted on UNIX platforms:

.(dot)	%	- (dash)	_ (underscore)
@	~ (tilde)	!	{
}	[]	&
#	, (comma)	=	(space)

In general, you can use characters **A** through **Z**, **a** through **z**, and **0** through **9**, plus any Unicode character with a decimal value greater than 127 (hexadecimal X'7F'), provided that your operating system can recognize the characters chosen.

If you expect to trace the operation of an execution group, restrict the name of the execution group to include only the valid alphabetic and numeric characters listed. The trace commands do not support the use of special characters for an execution group name.

For all other resources, any characters that are supported by the database configuration are supported.

Broker names, Configuration Manager names, and fixed names (UserNameServer) are not case sensitive on the Windows platforms. For example, broker names Broker1 and BROKER1 refer to the same broker.

On Linux and UNIX systems, broker names and Configuration Manager names are case sensitive, and the examples above would refer to different brokers. You must use UserNameServer as shown.

There are additional rules for naming message service folders within the MQRFH2 header.

Rules for using commands

Observe the following rules when using the WebSphere Event Broker commands on distributed systems. If you are using commands on z/OS, refer to the section on z/OS commands in "Commands" on page 232.

- Each command must be issued on the system on which the resource it relates to is defined (or is to be created).
- Each command starts with a primary keyword (the executable command name) followed by one or more blanks.
- Following the primary keyword, flags (parameters) can occur in any order.
- Flags are shown in this book in the form `-t`, for example. In all cases, the character `/` can be substituted for the `-` character.
- If a flag has a corresponding value, its value must follow the flag to which it relates. A flag can be followed by its value directly or can be separated by any number of blanks.
- Flags can be concatenated if they do not have corresponding values, although the last flag in a concatenated group *can* have a value associated with it. For example, the command:

```
mqsireadlog WBRK_BROKER -u -e default -o trace.xml -f
```

could be entered as:

```
mqsireadlog WBRK_BROKER -ufedefault -o trace.xml
```

where the name of the execution group, `default`, relates to the `-e` flag. For clarity, all examples given in this documentation are shown with separate flags and with a space before any associated value.

- Repeated flags are not allowed.
- Strings that contain blanks or special characters must be enclosed in double quotation marks. For example:

```
mqsireadlog "My Broker" -u -e default -o trace.xml -f
```

Additionally, you can specify a null, or empty, string with a pair of double quotes with nothing between: `""`. For example:

```
mqsichangeconfigmgr -s ""
```

- The case sensitivity of primary keywords and parameters depends on the underlying operating system. On Windows platforms keywords are not case sensitive; `mqsistart`, `mqsISTART`, and `MQSISTART` are all acceptable. On UNIX platforms, you must use lower case; only `mqsistart` is acceptable.

All WebSphere Event Broker commands have dependencies on WebSphere MQ function. You must ensure that WebSphere MQ is available before issuing these commands.

Responses to commands

Responses are issued to the commands as messages. If a command is successful, it returns a return code of zero, and a message with the number BIP8071I (command successful).

Warning and error responses are listed in the command descriptions. If the command is unsuccessful and returns, for example, the message BIP8083, it has an exit code, in this case, of 83.

The following responses are returned by all the commands, and are not listed with each individual command:

- BIP8001 Unknown flag selected
- BIP8002 Selected flags incompatible
- BIP8003 Duplicate flag
- BIP8004 Invalid flags or arguments
- BIP8005 Flag or argument missing
- BIP8006 Mandatory flag missing
- BIP8007 Mandatory argument missing
- BIP8009 Program name not valid
- BIP8083 Invalid component name

Message Brokers Toolkit commands

This topic is a container for the commands that are part of the WebSphere Event Broker Toolkit.

These commands are available only on a machine that has the Toolkit installed.

See “Commands” on page 232 for a list of all the WebSphere Event Broker commands.

mqsicreatebar command

Supported platforms:

- Windows
- Linux (x86 platform)

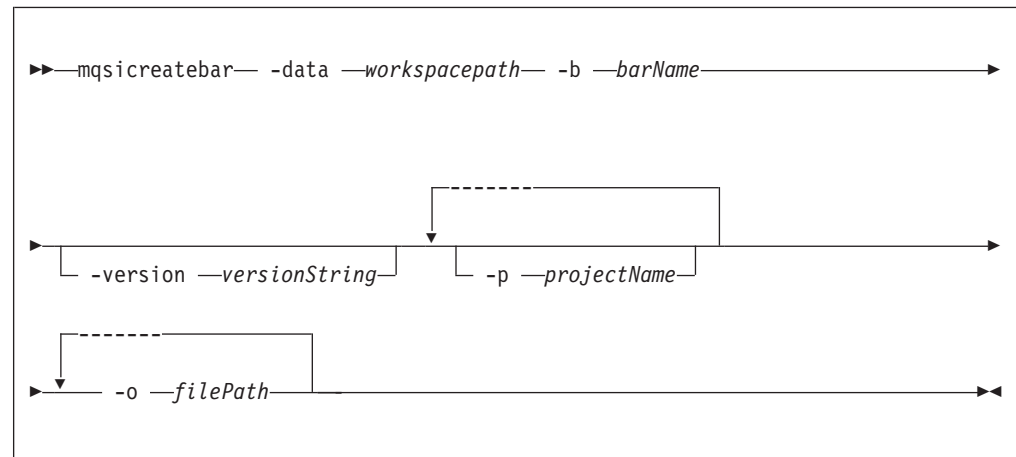
Purpose:

The **mqsicreatebar** command provides a command line compiler that creates deployable broker archive files containing message flows and dictionaries.

Together with the command line repository tools, this enables you to write scripts to repeatedly deploy. Although you are recommended not to perform team development without a repository, a repository is not required.

You can share files using the file system, or using the Eclipse **File>Import...** and **File>Export...** capabilities.

Syntax:



Parameters:

-data workspace

(Required) The path of the workspace in which your projects are created.

The workspace location is also the default location for projects. Relative paths are interpreted as being relative to the directory from which the command was started.

-b barName

(Required) The name of the bar (zip format) archive file where the result is stored. The bar is replaced if it already exists and the META-INF/broker.xml file is created.

-version versionString

(Optional) Append the _ (underscore) character and the value of the versionString to the names of the objects added to the bar, before the file extension.

-p projectName

(Optional) Projects containing files to link. You can specify multiple projects that can be a message flow project, a message set project, or a message flow plug-in node project.

This option allows you to use the command line tool to open existing or closed projects. The specified project is fully built and added to the workspace used to compile the bar file.

-o filePath

(Required) The workspace relative path (including the project) of a msgflow file to add to the broker archive.

The file can be in a message flow project or a message flow plug-in node project.

Note: `msgflow` is the extension of the message flow file that, for example, you can call `myFlow.msgflow`.

You can add more than one deployable file to this command by using the following format `-o filePath1 -o filePath2 -o filePath'n'`

Authorization:

The user ID used to invoke this command must have **Administrator** authority on the local system.

Responses:

This command returns the following responses:

- BIP0956 Unable to start `mqsicreatebar`
- BIP0957 Incorrect arguments supplied to `mqsicreatebar`
- BIP0958 Nothing to do in `mqsicreatebar`
- BIP0959 Incorrect arguments supplied to `mqsicreatebar` (Project name)
- BIP0960 Incorrect arguments supplied to `mqsicreatebar` (Project directory)
- BIP0961 Error opening workspace in `mqsicreatebar` (Project could not be created)
- BIP0962 Error opening workspace in `mqsicreatebar` (Project could not be opened)
- BIP0963 Error saving file in `mqsicreatebar`
- BIP0964 Incorrect `"-o"` argument supplied to `mqsicreatebar`
- BIP0965 Error compiling files in `mqsicreatebar`

Examples:

The following example assumes that you are working from the product installation Eclipse folder and have a workspace in the folder `C:\Workspace`:

```
mqsicreatebar -data C:\Workspace -b myflow.bar -p TestFlowProject -o TestFlowProject\TestFlow\Test.msgflow
```

mqsimigratemfmaps command

Supported platforms:

- Windows
- Linux (x86 platform)

Purpose:

Use the **mqsimigratemfmaps** command to create new `.msgmap` files in the WebSphere Event Broker Version 6.0 format, based on existing `.mfmaps` from WebSphere Business Integration Event Broker Version 5.0.

Note:

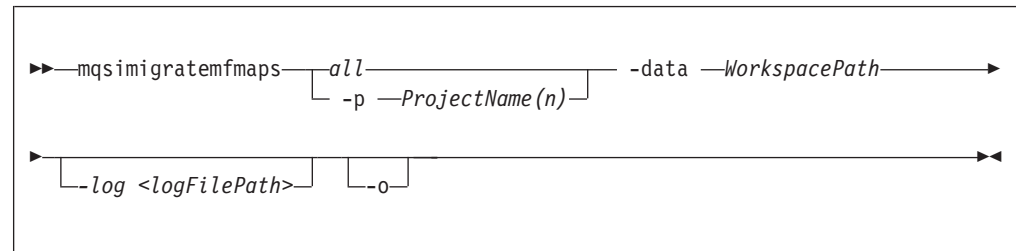
1. The `.mfmap` files are left in the workspace so that the migration can be run again.
2. The `.mfmap` files are not included in builds and are not recognized as valid WebSphere Event Broker development artefacts. They are present in the workspace as simple text files and you can delete them at your

own discretion. The Version 5.0 mfmap editor is no longer available in Version 6.0, so the only way to view the contents of the .mfmap files is through a text-editor.

3. Once the .mfmap files are migrated into .msgmap files, these new files are editable through the new Version 6.0 msgmap editor.

The mqsimigratemfmaps.exe file is located in <toolkit install>/eclipse/.

Syntax:



Parameters:

all (Required) All project names in the workspace are checked and migrated. This must be specified unless you specify specific project names to migrate.

-p *ProjectName(n)* (Required) The specific project name, or names, in the workspace to be checked and migrated. These must be specified only if you do not specify *all*.

-data *WorkspacePath* (Required) The path of the workspace in which your projects are created.

The workspace location is also the default location for projects. Relative paths are interpreted as being relative to the directory from which the command was started.

-log *<filepath>* (Optional) Alternative report file path.

If you do not specify an alternative, this command generates a detailed migration log in the <install_dir>/eclipse/ folder. The log-file has the default name of "mqsimigratemfmaps.report.txt".

-o (Optional) Overwrite files that already exist.

Authorization:

No specific authority is required to invoke this command.

Examples:

```
mqsimigratemfmaps -p sample -data c:\wmqi\test
```

mqsimigratemsgflows command

Supported platforms:

- Windows
- Linux (x86 platform)

Purpose:

Use the **mqsimigratemsgflows** command to create new flows in the WebSphere Event Broker Version 6.0 format, based on existing exported flows from a WebSphere MQ Event Broker Version 2.1 Configuration Manager.

Note:

1. This command is for one way migration to the WebSphere Event Broker Version 6.0 Message Brokers Toolkit from the Version 2.1 release.
2. When you migrate from Version 5.0 to Version 6.0 you need load only the Version 5.0 .msgflow files into the Version 6.0 workspace and when you save the files they are saved in Version 6.0 format.

In addition, you can use this command to deploy exported user-defined node definitions from Version 2.1 to Version 6.0. To recreate the user-defined nodes in Version 6.0 you must manually redefine them.

3. Stop your Message Brokers Toolkit session before you invoke the command.
4. Specify the workspace location using the **-data** flag.

If your path contains spaces, enclose the entire path name in double quotation marks.

On Windows operating systems the mqsimigratemsgflows.exe file is located in the <toolkit install>/eclipse directory. Similarly, on the Linux (x86 platform) operating system, the mqsimigratemsgflows file is located in the <toolkit install>/eclipse directory.

Syntax:

```
►► mqsimigratemsgflows -data WorkspacePath -p ProjectName
► -d DirectoryPath [-rm] [-log <filepath>]
```

Parameters:

-data *WorkspacePath*

(Required) The path of the workspace in which your projects are created.

The workspace location is also the default location for projects. Relative paths are interpreted as being relative to the directory from which the command was started.

-p *ProjectName*

(Required) The project name where the new flows are created. If the project already exists, the flows are added to this project. If the project does not exist, this command creates it.

-d *DirectoryPath*

(Required) The directory path where the exported flows can be found.

A relative path is interpreted from the current working directory. You can specify a full path. All nested directories are ignored.

The flow name becomes the name of the .msgflow file. You can change this name to meet the local file naming conventions.

Duplicate message flows are ignored; any error of this form is reported in the migration report file.

-rm

(Optional) Replace message flow projects if they already exist.

-log <filepath>

(Optional) Report file.

If you do not specify an alternative, this command generates a detailed migration log in the <install_dir>/eclipse/ folder. The log-file has the default name of "mqsimigratemsgflows.report.txt".

For further information on flow migration, see Migrating message flows from Version 2.1.

Authorization:

No specific authority is required to invoke this command.

Examples:

```
mqsimigratemsgflows -p sample -d c:\wmqi\test
```

mqlireadbar command

Supported platforms:

- Windows
- Linux (x86 platform)

Purpose:

The **mqlireadbar** command lists to the console the keywords defined for each deployable file within a deployable broker archive file.

Syntax:

```
►► mqlireadbar -b barName ◀◀
```

Parameters:

-b *barName*

(Required) The name of the bar (zip format) archive file to read.

Authorization:

The user ID used to invoke this command must have **Administrator** authority on the local system.

Responses:

This command returns the following responses:

- BIP2956 Unable to read broker archive file <file name>

Examples:

The following example reads the file `my_bar_file.bar` and displays defined keywords within the given file to the console

```
mqsireadbar -b my_bar_file.bar
```

Runtime commands

This topic is a container for the runtime commands of WebSphere Event Broker.

These commands are available on a machine where any of the runtime components are installed

See “Commands” on page 232 for a list of all the WebSphere Event Broker commands.

mqsibbackupconfigmgr command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS using BIPBUCM; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

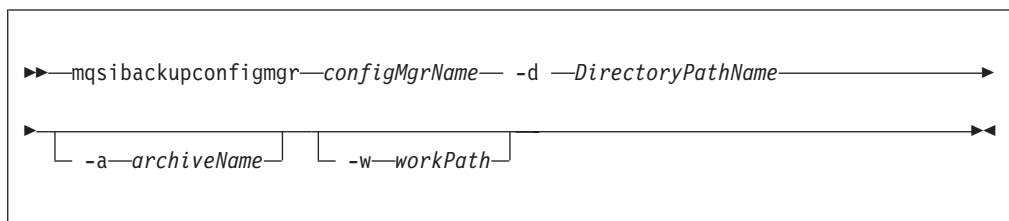
This command backs up the Configuration Manager repository online and uses the Configuration Manager Proxy to communicate with the Configuration Manager in the same way that the existing utility `mqsidesploy` does on Windows platforms.

Note: If you plan to restore the Configuration Manager data repository on z/OS and the platform from which it was originally backed up was not z/OS, or the other way round, you must take a copy of the file:

```
<Configuration  
Manager directory>/components/<component name>/<directory name>/service.properties
```

This needs to be kept with the zip file produced by the `mqsibbackupconfigmgr` command, and must be copied to the equivalent place in the restored Configuration Manager data repository after running the `mqsirestoreconfigmgr` command.

Syntax:



Parameters:

configMgrName

(Required) The name of the Configuration Manager.

- d** *DirectoryPathName*
(Required) The directory where the back up is placed. An error occurs if the directory does not exist.
- a** *archiveName*
(Optional) Specifies the backup archive name; if you do not specify a name, the name takes the form: <configMgrName>_<date>_<time>.zip.
- w** *workPath*
(Optional) Specifies the path for the Configuration Manager repository.

Authorization:

The user ID used to invoke this command must be a member of the Windows **Administrators** group on this local system.

Responses:

This command returns the following responses:

- BIP8056 Unknown queue manager

Examples:

```
mqsicbackupconfigmanager ConfigMgr -d c:\mqsitest\db -a archive1
```

mqsicbrreport command

Supported platforms:

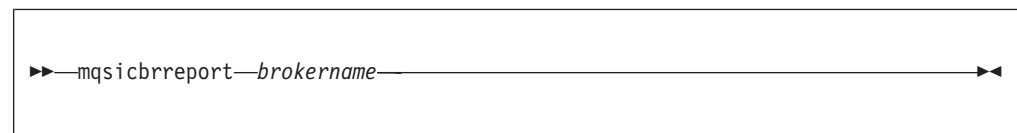
- Windows
- Linux and UNIX systems

Purpose:

Use the **mqsicbrreport** command to help identify applications that use a content-based routing filter. The program inspects a broker’s subscriptions table, and reports any filters it finds that might cause incompatible behavior.

You must invoke on the system on which the program is running and you must be logged on as the service user ID for the broker.

Syntax:



Parameters:

brokername

(Required) The name of the broker to inspect. The output is written to stdout and you must review the report generated so that you can make any necessary changes to your programs.

Note: This utility only identifies and reports possible incompatibilities.

Authorization:

On Windows platforms, the user ID used to invoke this command must have **Administrator** authority on the local system.

On Linux and UNIX systems, the user ID used to invoke this command must be **root**. It must also be a member of the **mqbrkrs** group.

mqchangebroker command

Supported operating systems:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPCHBK; see “Contents of the broker PDSE” on page 378

Purpose:

You must stop the broker before you can issue this command and restart the broker for the changes to take effect.

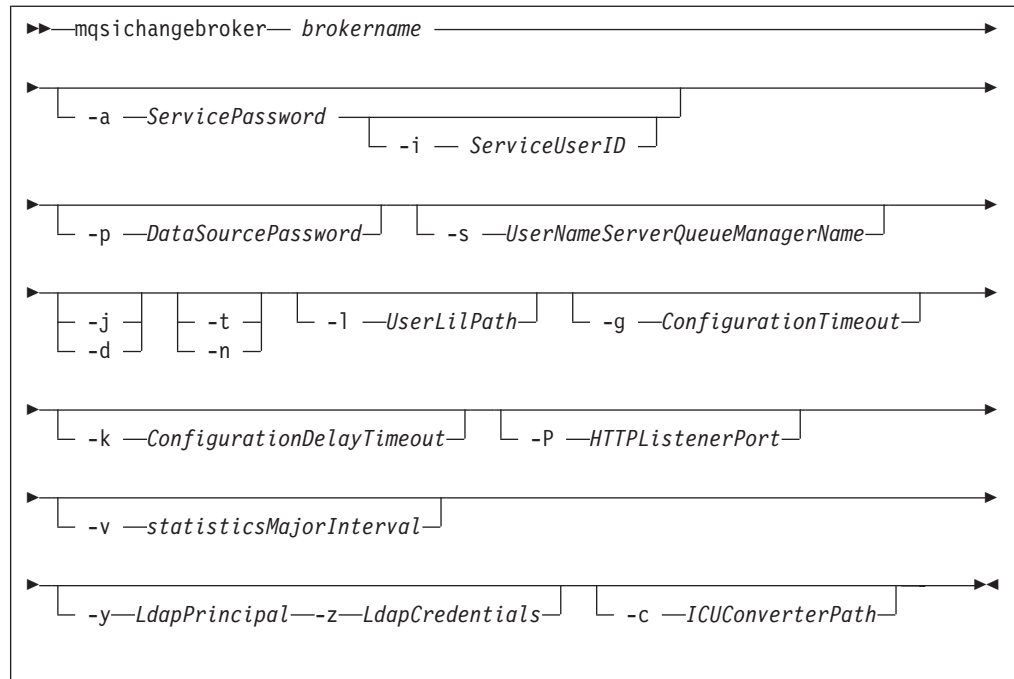
On Windows, Linux, and UNIX systems, use the **mqsisstop** and **mqsisstart** commands.

On z/OS, you must have started the original broker control process using the /S option. You must stop the broker components using the /F broker, PC option, and start the broker components again using the /S broker, SC option.

See “mqsisstop command” on page 362 and “mqsisstart command” on page 357 for more information.

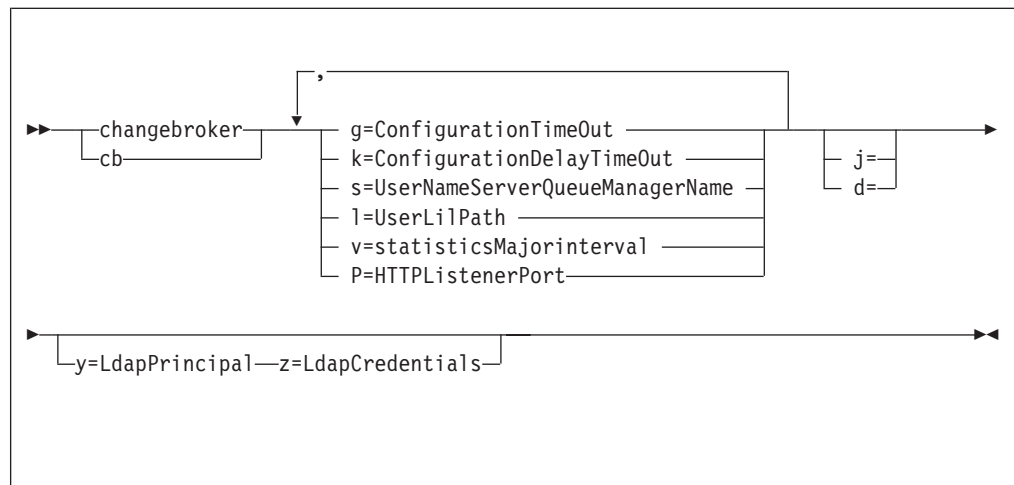
Syntax:

Windows, Linux, and UNIX systems:



z/OS console command:

Synonym: cb



Parameters:

brokername

(Required - Windows, Linux, and UNIX systems) This must be the first parameter. Specify the name of the broker that you want to modify.

-a *ServicePassword*

(Optional - Windows, Linux, and UNIX systems) The password for the *ServiceUserID*.

For compatibility with existing systems, you can still specify *password*.

However, if you do not specify a password with this parameter when you run

the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

On Linux and UNIX systems, **-a** is required for Windows systems compatibility but it is not used in relation to *ServiceUserID*; it is used as a default only if **-p** is not specified. (See the description of the **-p** parameter for further details.)

If you have created this broker to also use this user ID and password for database access (that is, either you omitted the **-u** *DataSourceUserID* and **-p** *DataSourcePassword* parameters, or you included them but provided the same user ID and password for the service user ID using **-a** *ServicePassword* and **-i** *ServiceUserID*), ensure that you update both instances of the password on this command by supplying the **-p** *DataSourcePassword* as well.

To complete a password change successfully, you must:

- Stop the broker.
- Change the password using the appropriate operating system facilities.
- Use this command to update all parameters that reference this same password.
- Restart the broker.

-i *ServiceUserID*

(Optional - Windows, Linux, and UNIX systems) The user ID under which the broker runs. You must also change the password (**-a**) if you change this value.

This can be specified in any valid username syntax. On Windows systems, these are:

- domain\username
- \\server\username
- .\username
- username

On Linux and UNIX systems, only the last format, username, is valid.

If you use the unqualified form for this user ID (username) on Windows systems, the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

The *ServiceUserID* specified must be a member of the local group **mqbrkrs**. On Windows systems, it can be an indirect or direct member of the group. The *ServiceUserID* must also be authorized to access the home directory (where WebSphere Event Broker has been installed), and the working directory (if specified by the **mqsicreatebroker -w** parameter). This ID must also be a member (either direct or indirect) of the local group **mqm**.

The security requirements for the *ServiceUserID* are detailed in “Security requirements for Windows platforms” on page 425 for Windows systems and in “Security requirements for Linux and UNIX platforms” on page 424 for Linux and UNIX systems.

-p *DataSourcePassword*

(Optional -Windows, Linux, and UNIX systems) The password of the user ID with which the databases containing broker tables and user data are to be accessed.

For compatibility with existing systems, you can still specify *password*. However, if you do not specify a password with this parameter when you run

the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

For DB2 on Linux and UNIX systems, **-p** can be specified as an empty string (two double quotation marks, ""). In this case, DB2 grants WebSphere Event Broker the privileges of the *ServiceUserID* which results in a database connection as "already verified". If you specify an empty string for **-a** and **-p**, no passwords are stored by WebSphere Event Broker, creating the most secure configuration.

You must ensure that you change all instances of the use of this password. If you have created (or changed) the broker to use the same user ID and password for its service user ID as well as its database access, you must update both instances at the same time. See the description of the **-a** parameter for further details.

-s *UserNameServerQueueManagerName*

(Optional) The name of the WebSphere MQ queue manager that is associated with the User Name Server. If you want to remove topic-based security, specify an empty string (two double quotation marks, "").

Note that on z/OS this name is case sensitive and you must include the names in single quotes if they contain mixed case characters.

-j (Optional) Publish/subscribe access is enabled for the broker.

-d (Optional) Publish/subscribe access is not enabled for the broker.

-t (Optional - Windows, Linux, and UNIX systems) Requests that the broker runs as a WebSphere MQ trusted application.

For more details about using WebSphere MQ trusted applications, see *WebSphere MQ Intercommunication*.

-n (Optional - Windows, Linux, and UNIX systems) Requests that the broker ceases to run as a WebSphere MQ trusted application.

-l *UserLilPath*

(Optional) Specifies a list of paths (directories) from which the broker loads LILs (loadable implementation libraries) for user-defined message processing nodes.

You must create your own directory for storing your .lil or .jar files. Do not save them in the WebSphere Event Broker install directory.

If you specify more than one additional directory, they must be separated by the default operating system-specific path separator (semicolon (;) on Windows systems, colon (:)) on Linux, UNIX systems, and z/OS).

You cannot include environment variables in this path: if you do so, they are ignored.

Note that on Linux and UNIX systems, and on z/OS, this name is case sensitive and you should include the names in single quotes if they contain mixed case characters.

-g *ConfigurationTimeout*

(Optional) Defines the length of time (in seconds) that an execution group in the broker is allowed to take to apply a change in configuration (for example, an update that you have deployed from the workbench).

When a message flow is processing an application message, it cannot respond to a configuration change. If any one of the message flows within the execution

group that has been requested to change its configuration does not finish processing an application message and apply the configuration change within this timeout, the execution group returns a negative response to the deployed configuration message.

The value that you set for this timeout depends on the system load (including CPU utilization) and on each execution group's load. You can make an initial estimate by deploying the broker's entire configuration. The time taken for this to complete successfully gives you an indication of the minimum value that you should set.

The value is specified in seconds and can range from 10 to 3600. The default value is 300.

The sum of the *ConfigurationTimeout* and the *ConfigurationDelayTimeout* (described below) represents the maximum length of time that a broker is allowed to process a deployed configuration message before it generates a negative response.

-k *ConfigurationDelayTimeout*

(Optional) Defines the length of time (in seconds) that a broker is allowed to take to process a minimal change in configuration (for example, an update that you have deployed from the workbench).

This represents the time it takes for a minimal deployed configuration message to be processed by the broker and its execution groups, and is dependent on queue manager network delays, the load on the broker's queue manager, and system load.

You can estimate this value by issuing a command to request a simple configuration change, for example:

- On Windows, Linux, and UNIX systems:
`mqsireporttrace brokerName -e "Execution Group Name" -u`
- On z/OS:
`F MQP1BRK,reporttrace u=yes,e='exgrp1'`

Note that on z/OS, this name is case sensitive and you should include the names in single quotes if they contain mixed case characters.

The response time of each execution group differs according to system load and the load of its own processes. The value that you set must reflect the longest response time any execution group takes to respond. If the value you set is too low, the broker returns a negative response, and might issue error messages to the local error log.

The value is specified in seconds and can range from 10 to 3600. The default value is 60.

If the broker is on a production system, you are recommended to increase the values for both *ConfigurationTimeout* and *ConfigurationDelayTimeout* to allow for application messages currently being processed by message flows to be completed before the configuration change is applied.

If the broker is on a development or test system, you might want to reduce time-outs (in particular, the *ConfigurationTimeout*) to improve perceived response times, and to force a response from a broker that is not showing expected behavior. However, reducing the timeout values decreases the probability of successfully deploying a configuration change.

-P HTTPListenerPort

(Optional) Enter the number of the port on which the web services support is listening.

Note that this listener is started by the broker when a message flow that includes web services support is started, and has a default value of 7080.

You must ensure that the port you specify has not been specified for any other purpose.

-v statisticsMajorInterval

(Optional) Specify the timer interval in minutes at which WebSphere Event Broker statistics and accounting is notified that archive records should be output. For internal accounting, the valid range is from 10 to 14400 minutes.

An interval of zero minutes indicates that the operating system has an external method of notification and is not using an internal timer within WebSphere Event Broker.

-y LdapPrincipal

(Optional - all operating systems, but mandatory when *LdapCredentials* is provided.) The user principal for access to an optional LDAP directory that holds the JNDI administered Initial Context for the JMS provider.

-z LdapCredentials

(Optional - all operating systems, but mandatory when *LdapPrincipal* is provided.) The user password for access to LDAP.

-c ICUConverterPath

(Optional) A delimited set of directories to search for additional code page converters. On Windows systems, the delimiter is a comma (.). On UNIX and Linux systems, the delimiter is a colon (:). The code page converters must be either of the form *icudt32_codepagename.cnv* or in an ICU data package called *icudt32.dat*.

If you want to change other broker properties, you must delete and recreate the broker, then use the workbench to redeploy the broker's configuration. If you want to change the user ID used for database access, see "Administering the broker domain" on page 211.

Authorization:

On Windows systems, the user ID used to invoke this command must have **Administrator** authority on the local system.

On Linux and UNIX systems, the user ID used to invoke this command must be a member of the **mqbrkrs** group.

On z/OS systems, the user ID used to invoke this command must be a member of a group that has READ and WRITE access to the component directory.

Using LDAP: Ensure that the registry is appropriately secured to prevent unauthorized access. The setting of *LdapPrincipal* and *LdapCredentials* options on **mqchangebroker** is not required for correct operation of the broker. The password is not stored in clear text in the file system.

Responses:

This command returns the following responses:

- BIP2595 Error casting character string '...' to an integer (z/OS only)
- BIP8003 Duplicate flag detected (z/OS only)
- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8018 Component running
- BIP8021 User ID/password incorrect
- BIP8022 Invalid user ID/password
- BIP8023 Password required
- BIP8030 Unable to modify user ID privileges
- BIP8068 Argument ... is not a valid integer value for this flag (z/OS only)
- BIP8073 Invalid broker name (Windows and UNIX systems only)
- BIP8158 Invalid format for command (z/OS only)
- BIP8159 Unknown parameter "..." (z/OS only)

Examples:

Windows, Linux, and UNIX systems:

```
mqschangebroker WBRK_BROKER -s WBRK_UNQ_QM
mqschangebroker WBRK_BROKER -s ""
```

z/OS:

```
F MQP1BRK,cb g=100,k=200
```

mqschangeconfigmgr command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPCHCM; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

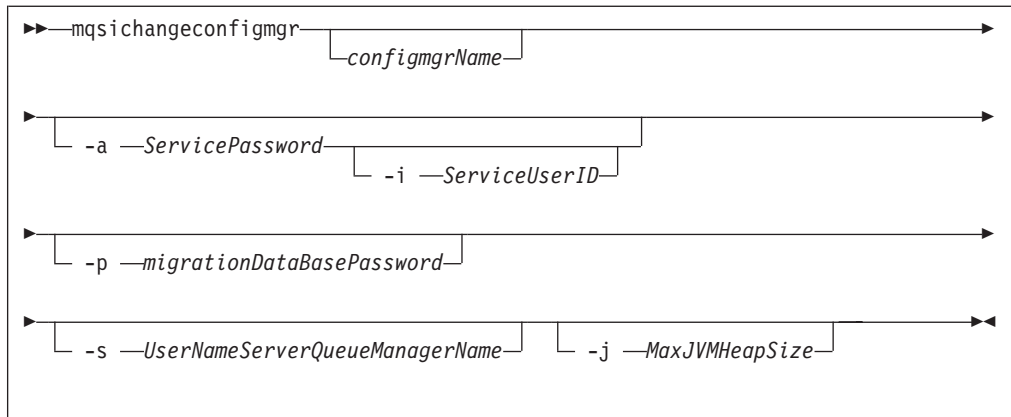
Use the **mqschangeconfigmgr** command to change some of the properties of the Configuration Manager.

You must stop the Configuration Manager, using **mqsistop**, (see “mqsistop command” on page 362).

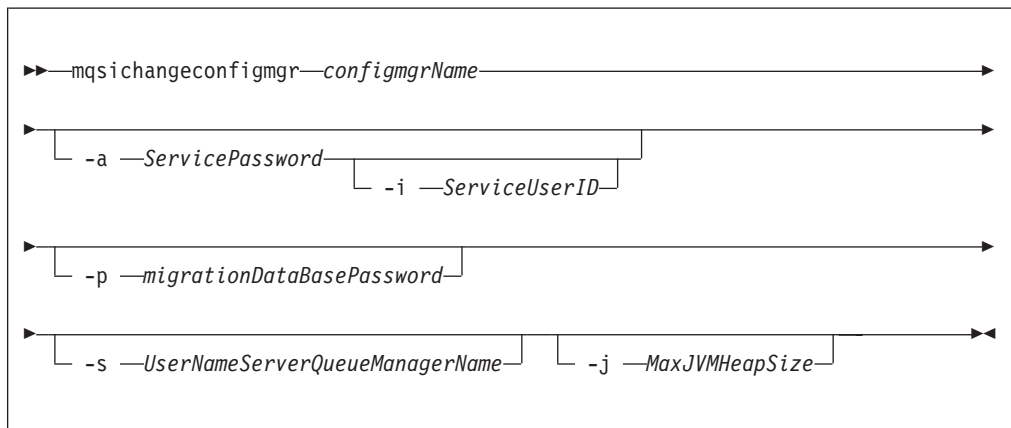
When you restart the Configuration Manager, using **mqsistart**, (see “mqsistart command” on page 357), it uses the changed parameters.

Syntax:

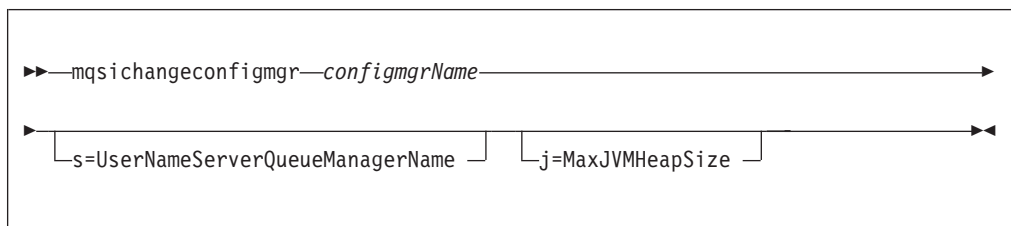
Windows:



Linux and UNIX systems:

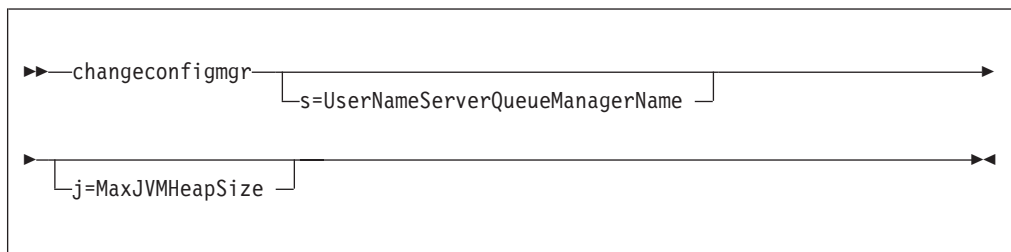


z/OS:



z/OS console command:

Synonym: cc



Parameters:

configmgrName

(Optional - Windows. Required - Linux, UNIX systems, and z/OS) The name of the Configuration Manager that you want to change.

On Linux, UNIX systems and z/OS, this must be the first parameter specified. It is case-sensitive on Linux, UNIX systems and z/OS.

The default name on Windows, if this parameter is not specified, is 'ConfigMgr'.

-a *ServicePassword*

(Optional - Windows platforms, Linux and UNIX systems only) The password for the ServiceUserID.

If you created the Configuration Manager to use this user ID and password for database access as well (that is, you provided the same user ID and password for the service user ID using **-a ServicePassword** and **-i ServiceUserID**), ensure that you update all instances of the password on this command.

To complete a password change successfully, you must:

- Stop the Configuration Manager.
- Change the password using the appropriate operating system facilities.
- Use this command to update all parameters that reference this same password.
- Restart the Configuration Manager.

For compatibility with existing systems, you can still specify `<password>`. However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

-i *ServiceUserID*

(Optional - Windows platforms, Linux and UNIX systems only) The user ID under which the Windows system service runs. You can only change this value if you also change the password.

This can be specified in any valid username syntax for the platform.

If you use the unqualified form for this user ID (username) on Windows systems, the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

The ServiceUserID specified must be a member of the local group **mqbrkrs**. It can be an indirect or direct member of the group. The ServiceUserID must also be authorized to access the home directory (where WebSphere Event Broker has been installed), and the working directory (if specified by the **mqsicreateconfigmgr -w** flag). This ID must also be a member (either direct or indirect) of the local group **mqm**.

The security requirements for the ServiceUserID are detailed in "Security requirements for Windows platforms" on page 425 for Windows platforms and "Security requirements for Linux and UNIX platforms" on page 424 for UNIX platforms.

-p *migrationDataBasePassword*

(Optional - Windows platforms, Linux and UNIX systems only) The password for the DB2 database that you are migrating.

Ensure that you change all instances of the use of this password. If you have created (or changed) the Configuration Manager to use the same user ID and

password for its service user ID as well as its database access, you must update all instances at the same time. See the description of `-a` for further details.

-s *UserNameServerQueueManagerName*

(Optional) The name of the WebSphere MQ queue manager that is associated with the User Name Server. If you want to remove topic security, specify an empty string (two double quotation marks, `""`).

-j *MaxJVMHeapSize*

(Optional) The maximum Java virtual machine (JVM) heap size, in megabytes. The smallest value that you can set is 64. If you do not set this parameter, the default size of 128 MB is used.

If you want to change other properties, you must delete and recreate the Configuration Manager. If you want to change the `DataBaseUserID`, see “Modifying component database access” on page 164 for instructions.

Responses:

This command returns the following responses:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8018 Component running
- BIP8021 User ID/password incorrect
- BIP8022 Invalid user ID/password
- BIP8023 Password required
- BIP8030 Unable to modify user ID privileges

Examples:

```
mqsichangeconfigmgr CMGR01 -i ADMIN
mqsichangeconfigmgr CMGR01 -s ""
```

mqsichangedbimgr command

Supported platforms:

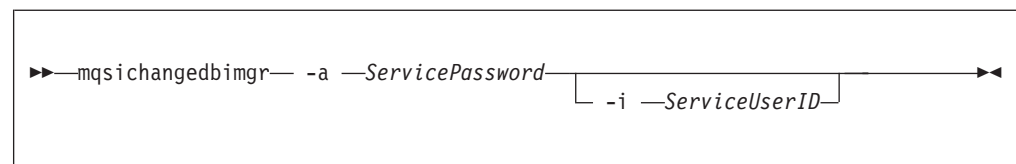
- Windows

Purpose:

The **mqsichangedbimgr** command updates the Windows service that runs the Derby Network Server, with a new user password, a new user ID, or both.

Syntax:

Windows platforms:



Parameters:

-a ServicePassword

(Required) The new password for the ServiceUserID. To complete a password change successfully, you must:

- Stop all the broker components using the **mqsistop** command.
- Change the password using the appropriate Windows facilities.
- Use the appropriate mqsichange commands to update all the components that reference this same ServiceUserID and password.
- Restart all the broker components using the **mqsistart** command.

-i ServiceUserID

(Optional) The user ID under which the default database runs. This can be specified in any valid username syntax. On Windows systems, these are:

- domain\username
- \\server\username
- .\username
- username

If you use the unqualified form for this user ID (username) on Windows systems, the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete. The ServiceUserID specified must be a member of the local group **mqrbrks**. On Windows systems, it can be a direct or indirect member of the group. The ServiceUserID must also be authorized to access the home directory (where WebSphere Event Broker has been installed). The security requirements for the ServiceUserID are detailed in “Security requirements for Windows platforms” on page 425.

Authorization:

The user ID used to invoke this command must have Administrator authority on the local system and be part of the **mqrbrks** group.

Responses:

This command returns the following responses:

- BIP8071 Successful command completion.
- BIP9810 The IBM MQSeries Brokers DatabaseInstanceMgr service was not found.

Examples:

The following example changes the password used for the IBM MQSeries Brokers DatabaseInstanceMgr service:

```
mqsichangedbimgr -a wbrkpw1
```

mqsichangeflowstats command

Supported Platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPCHMS; see “Contents of the broker PDSE” on page 378

Purpose:

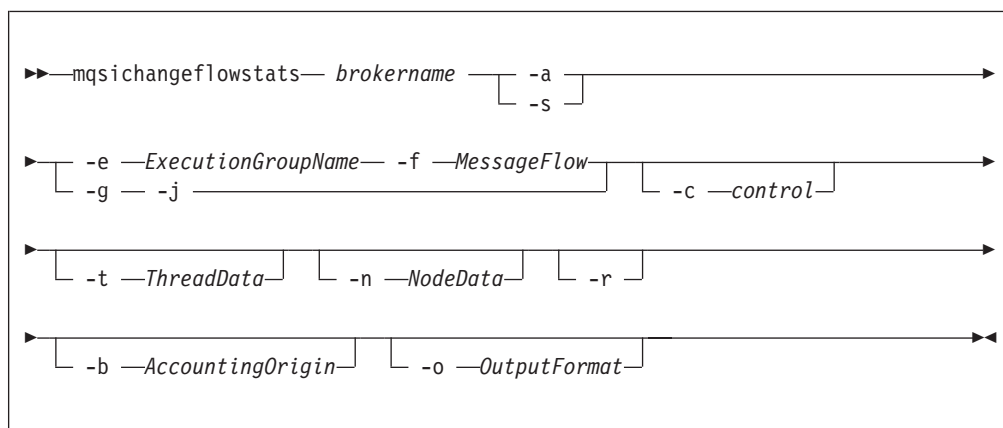
Use the **mqsichangeflowstats** command to:

- Turn on or off accounting and statistics snapshot publication, or archive record output.
- Specify that the command be applied to a specific flow message flow, or all flows in an execution group, or all execution groups belonging to a broker.
- Modify the granularity of the data collected in addition to the standard message flow accounting and statistics. This extra data can include thread related data, node related data, node terminal related data, or a mixture of this data.

The options set using this command remain active until modified by a subsequent **mqsichangeflowstats** command.

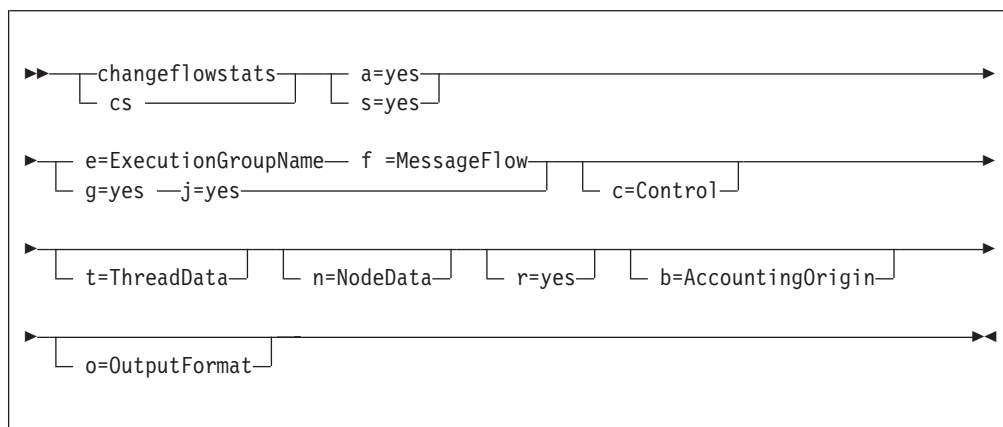
Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS:

Synonym cs



Parameters:

brokername

(Required -Windows platforms, Linux, and UNIX systems) Specify the label of the broker for which accounting and statistics are to be changed.

-a (Required) Specify that the command modifies archive accounting and statistics collection.

Note: You must specify either **-a** or **-s**. If you do not specify one of these arguments you receive a warning message.

-s (Required) Specify that the command modifies snapshot accounting and statistics collection.

Note: You must specify either **-a** or **-s**. If you do not specify one of these arguments you receive a warning message.

-e *ExecutionGroupName*

(Required) Specify the name for the execution group, for which accounting and statistics options are to be changed.

Note: You must specify either **-e** or **-g**. If you do not specify one of these arguments you receive a warning message.

-f *MessageFlow*

(Required) Specify the label for the message flow, for which accounting and statistics options are to be changed.

Note: You must specify either **-f** or **-j**. If you do not specify one of these arguments you receive a warning message.

-g (Required) Specifies that the command applies to **all** execution groups that belong to the broker.

Note: You must specify either **-e** or **-g**. If you do not specify one of these arguments you receive a warning message.

-j (Required) Specifies that the command applies to **all** message flows that belong to the execution group.

Note:

1. You must specify either **-f** or **-j**. If you do not specify one of these arguments you receive a warning message.
2. If you set the **-g** option for all execution groups, you must use **-j** instead of **-f**.

-c *control*

(Optional) Specify the string value that controls the level of the action to be applied to accounting and statistics collection for snapshot or archiving.

Possible values are:

- active - turn on snapshot or archiving
- inactive - turn off snapshot or archiving.

-t *ThreadData*

(Optional) Specify a string value to modify the collection of thread statistics data for a message flow Possible values are:

- none - exclude thread related data from the statistics
- basic - include thread related data in the statistics

-n *NodeData*

(Optional) Specify a string value to modify the collection of node statistics data for a message flow. Possible values are:

- none - exclude node related data in the statistics

- basic - include node related statistics in the statistics
 - advanced - include node related and terminal related data in the statistics
- r** (Optional) Specify that a reset of archive data is required.

Note: This action is only valid for archive data.

This results in the clearing out of accounting and statistics data accumulated so far for this interval, and restarts collection from this point. All archive data for all flows in the execution group, or groups, is reset.

The archive interval timer is only reset if the **-v** option (*statistics archive interval*) of **mqsicreatebroker** or **mqsichangebroker** is non zero. That is, the interval timer is only set if the internal interval notification mechanism is being used, and not an external method for example, ENF on z/OS.

-b *AccountingOrigin*

This parameter has no effect.

-o *OutputFormat*

(Optional) Specify the output destination for the statistics reports. Possible values are:

- usertrace - this is the default and writes "bip" messages to usertrace, which can be post processed in the normal way using the **mqsireadlog** and **mqsiformatlog** commands
- xml - the statistics reports are generated as XML documents and published by the broker running the message flow.

The topic on which the data is published has the following structure:

```
$SYS/Broker/<brokerName>/StatisticsAccounting/<recordType>
/<executionGroupLabel>/<messageFlowLabel>
```

where recordType is set to Snapshot or Archive, and broker, execution group, and message flow names are specified according to the subscriber's requirements.

- smf - (z/OS only). Statistics reports are output as SMF type 117 records.

Authorization:

The user Id used to issue the command must have mqbrkrs authority.

Responses:

This command returns the following responses:

- BIP2226 Request to change attribute in message flow node ' ': message flow does not exist
- BIP8004 Invalid flags and arguments selected
- BIP8013 Component does not exist
- BIP8020 Unable to access the database
- BIP8029 Broker not configured
- BIP8033 Unable to send XML message
- BIP8038 Unsupported command option
- BIP8039 Execution group not available
- BIP8040 Unable to connect to database

Examples:

Turn on snapshot statistics for the message flow "myFlow1" in all execution groups of BrokerA and specify that the data is to be gathered by accounting origin:

```
mqsichangeflowstats BrokerA -s -g -j -b none
```

Turn off the collection of archive statistics for message flow "MyFlow1" in execution group "EGRP2" for BrokerA, and at the same time modify the granularity of data that is to be collected (when next activated) to include thread related data.

```
mqsichangeflowstats BrokerA -a -e "EGRP2" -f MyFlow1 -c inactive -t basic
```

Turn off snapshot data for all message flows in all execution groups for Broker A.

```
mqsichangeflowstats BrokerA -s -g -j -c inactive
```

mqsichangeproperties command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS through the BIPJCHPR utility; see "Contents of the broker PDSE" on page 378

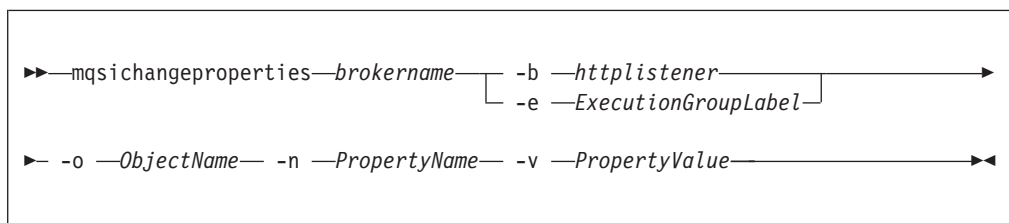
Purpose:

Use the **mqsichangeproperties** command to change properties relating to inter-broker communications and the http listener component, which includes the HTTP and HTTPS (SSL) support for the HTTPInput and HTTPReply nodes.

Start the broker using mqsistart, and then issue the command on the machine running the broker.

If you change any value you **must** stop and restart the broker for the change to take effect.

Syntax:



Parameters:

brokername

(Required) The name of the broker to modify. This must be the first parameter.

-b httplistener

(Optional) The name of the http listener component.

-e ExecutionGroupLabel

(Optional) Reserved

-o ObjectName

(Required) The name of the object whose properties you want to change. This must be set to one of the values listed below.

- n *PropertyName*
(Required) The name of the property being changed.
- v *PropertyValue*
(Required) The supplied *PropertyValue* is assigned to the property specified by *PropertyName*.

More than one name and corresponding value can be specified using commas as separators. For example,
-n Name1, Name2 -v Value1, Value2

For Inter-broker communications, the following *ObjectName* values are available:

- *DynamicSubscriptionEngine*

For the *httplistener* component, which includes the HTTPInput and HTTPReply nodes, the following *ObjectName* values are available:

- *HTTPListener* for controlling the HTTPListener process.
- *HTTPConnector* for controlling HTTP communication with the HTTPInput and HTTPReply nodes.
- *HTTPSConnector* for controlling HTTPS communication with the HTTPInput and HTTPReply nodes.

The *httplistener ComponentName* is required when using the HTTP *ObjectName* settings.

For compatibility mode with previous versions the following *ObjectName* value is available:

- *ComIbmXmlParserFactory*

Inter-broker communications parameter values

Valid property names for inter-broker communications are listed below:

brokerInputQueues

Specifies the maximum number of dispatch queues which are to be used when processing messages from an interbroker connection. Increasing the value might increase the rate at which messages can be transmitted across an interbroker connection:

- Value type - Integer
- Initial value - 1

brokerInputQueueLength

Defines the maximum number of messages that can be stored in each input queue; the higher the value, the higher the number of input messages that can be stored in each input queue. Note that the higher the value of this property, the larger the amount of memory that the broker requires for each queue:

- Value type - Integer
- Initial value - 99

brokerPingInterval

Time in milliseconds between broker initiated ping messages on broker-broker connections. Ping messages ensure that the communications are still open between both sides of the connection, and are generated internally. If the value is 0, the broker does not initiate pings.

- Value type - Integer
- Initial value - 5000

clientPingInterval

Time in milliseconds between broker initiated ping messages on broker-client connections. Ping messages ensure that the communications are still open between both sides of the connection, and are generated internally. If the value is 0, the broker does not initiate pings.

- Value type - Integer
- Initial value - 30000

clonedPubSubBrokerList

The list of brokers in which <brokername> registers to be a clone.

This list takes the format

BrokerName1, BrokerQMName1, BrokerName2, BrokerQMName2. Therefore, if you require to clone three brokers BRKA, BRKB, and BRKC, you must run the following commands:

```
mqsichangeproperties BRKA -e default -o DynamicSubscriptionEngine
-n clonedPubSubBrokerList -v \"BRKB, BRKBQM, BRKC, BRKCQM\"
mqsichangeproperties BRKB -e default -o DynamicSubscriptionEngine
-n clonedPubSubBrokerList -v \"BRKA, BRKAQM, BRKC, BRKCQM\"
mqsichangeproperties BRKC -e default -o DynamicSubscriptionEngine
-n clonedPubSubBrokerList -v \"BRKA, BRKAQM, BRKB, BRKBQM\"
```

It is also possible to remove brokers from a cloned environment. For example, if BRKC is to be removed from the clone use the following commands:

```
mqsichangeproperties BRKA -e default -o DynamicSubscriptionEngine
-n clonedPubSubBrokerList -v \"-BRKC\"
mqsichangeproperties BRKB -e default -o DynamicSubscriptionEngine
-n clonedPubSubBrokerList -v \"-BRKC\"
mqsichangeproperties BRKC -e default -o DynamicSubscriptionEngine
-n clonedPubSubBrokerList -v \"\"
```

Note the minus symbol in the list for BRKA and BRKB. BRKC does not specify any brokers and is, therefore, not a clone. However, BRKA and BRKB remain clones of each other.

- Value type - String
- Initial value - none

enableClientDiscOnQueueOverflow

If true, and if after deleting all possible messages the maxClientQueueSize is still exceeded, the broker disconnects the client.

- Value type - Boolean
- Initial value - False

enableQopSecurity

Enables the level of quality of protection for messages.

By default, Quality of Protection is enabled if either the **isysQopLevel** or **sysQopLevel** value has been changed from the default value of none.

- Value type - string
- Initial value - none

httpDispatchThreads

The value is the number of threads that the broker dedicates to managing HTTP tunneling clients.

- Value type - Integer
- Initial value -32

httpProtocolTimeout

The value is the number of milliseconds in the HTTP protocol timeout interval. You can change this value to update the amount of time a broker is to wait for the next event during any phase of the HTTP tunneling protocol. A value of 0 causes the broker to wait indefinitely

- Value type - Integer
- Initial value -10000

interbrokerHost

Specifies the IP host name of the broker. A single broker configuration can be left to default as null.

```
mqschangeproperties <broker> -o DynamicSubscriptionEngine -n  
interbrokerHost -v <IP host name>
```

- Value type - String
- Initial value - null

If you change the value, the broker must be stopped and restarted. Then you must redeploy the full topology.

interbrokerPort

Port number on which the Broker listens for incoming interbroker connections. If running more than one broker on the same machine, set the **interbrokerPort** property to a different value for each broker. For example:

```
mqschangeproperties <broker> -o DynamicSubscriptionEngine -n  
interbrokerPort -v <port number>
```

If you do not set the **interbrokerPort** value before the topology is deployed, restart the broker.

- Value type - Integer
- Initial value -1507

If you change the value, the broker must be stopped and restarted. Then you must redeploy the full topology.

isysQopLevel

Applies to the system and allows brokers only to publish and subscribe.

- Value type - string
- Initial value - none

maxBrokerQueueSize

Maximum number of bytes that the broker should queue for transmission to another broker. If the maximum is exceeded, the broker deletes all messages queued to that broker, except for the latest message, high-priority messages, and responses. If 0, the broker does not limit the number of bytes queued to another broker:

- Value type - Integer
- Initial value - 1000000

maxClientQueueSize

Maximum number of bytes that the broker should queue for transmission to a client. If the maximum is exceeded, the broker deletes all messages queued to that client, except for the latest message, high-priority messages, and response messages. If 0, the broker does not limit the number of bytes queued to a client.

- Value type - Integer
- Initial value - 100000

The value of this property **must** be greater than, or equal to, the *maxMessageSize* value.

maxConnections

The maximum number of concurrently connected clients which the broker permits. If this limit is reached, the broker denies new connection requests from clients. If this value is less than 0, the number of clients is unlimited.

- Value type - Integer
- Initial value -100

jvmMaxHeapSize

Specifies the size of the Java Virtual Machine (JVM) heap size used with the JVMManager for your Java plug in nodes.

This must be in the range 16 777 216 through 8 589 934 592.

- Value type - Integer
- Initial value - 134 217 728

maxHopCount

Specifies that maximum number of multibroker links over which a message is sent, to ensure that messages never loop in a multibroker network. Set this value large enough to ensure that messages can travel the entire multibroker network.

- Value type - Integer
- Initial value - 20

maxMessageSize

Maximum allowed message size in bytes. If a message exceeding this maximum size is received from a client, that client is disconnected.

- Value type - Integer
- Initial value - 100000

The value of this property **must** be less than, or equal to, the *maxClientQueueSize* value.

multicastAddressRangeMax

The highest IP address that the broker can use for its Multicast transmissions.

This should be in the range 224.0.0.2 through 239.255.255.255

- Value type - String
- Initial value - 239.255.255.255

multicastAddressRangeMin

The lowest IP address that the broker can use for its Multicast transmissions.

This should be in the range 224.0.0.2 through 239.255.255.255

- Value type - String
- Initial value - 224.0.0.2

multicastBackoffTimeMillis

The maximum time, in milliseconds, that a client listens for another's NACKs before sending its own NACK. This value can be in the range 0 through 1000.

- Value type -Integer
- Initial value -100

multicastDataPort

The UDP data port through which Multicast packets are sent and received:

- Value type - Integer
- Initial value - 34343

multicastEnabled

Indicates whether the topics that are defined in the `multicastTopicsConfigFile` are delivered Multicast. If the value is true, the topics in the `multicastTopicsConfigFile` are delivered Multicast.

- Value type - Boolean
- Initial value - false

multicastHeartbeatTimeoutSec

Indicates the time in seconds between the arrival of control packets at each client. If a control packet does not arrive within the number, defined as twice the value specified by this property, of seconds of the previous control packet's arrival an error can be suspected.

- Value type - Integer
- Initial value -20

multicastLimitTransRate

This property can be used in conjunction with the **multicastTransRateLimitKbps** property to control network congestion. Possible values are:

Disabled

Multicast data is transmitted as fast as possible

Static The transmission rate is limited by the value specified in **multicastTransRateLimitKbps**

Dynamic

The transmission rate can vary throughout the process, but never exceeds the value specified in **multicastTransRateLimitKbps**

- Value type - String
- Initial value - Disabled

multicastMaxKeyAge

Maximum age, in minutes, of a topic encryption key before it must be redefined.

- Value type - String
- Initial value - 360

multicastMaxMemoryAllowedKBytes

Maximum memory consumption by client reception buffers, measured in kilobytes.

- Value type - Integer
- Initial value - 262144

This parameter is available *only* if a Pragmatic General Multicast (PGM) protocol is selected.

multicastMCastSocketTTL

The maximum number of hops that a Multicast packet can make between the client and the broker. This value is one more than the maximum number of routers that there can be between the client and the broker.

A value of 1 indicates that the packet reaches all local nodes, but cannot be relayed by routers. The maximum value is 255.

- Value type - Integer
- Initial value - 1

multicastMinimalHistoryKBytes

The minimum size, in kilobytes, of a buffer that is allocated as an archive

for all transmitted packets. This buffer is shared by all reliable topics, and can be used to recover lost packets. This value can be in the range 1000 through 1,000,000.

- Value type - Integer
- Initial value - 60000

multicastMulticastInterface

Indicates what interface to use for Multicast transmissions. You can specify a host name or an IP address. A value of "none" causes the network interface to be operating system dependent.

- Value type - String
- Initial value - "none"

Note: If you have only one network card, the default value of none works because the operating system uses the localhost value. However, if you have more than one network card you **must** set this parameter to ensure that the correct card is used.

multicastNACKAccumulationTimeMillis

The time, in milliseconds, that NACKs are aggregated in the broker, before recovered packets are sent. This value can be in the range 50 through 1000.

- Value type - Integer
- Initial value - 300

multicastNACKCheckPeriodMillis

The time, in milliseconds, between periodic checks of reception status and sequence gap detection for NACK building. This value can be in the range 10 thru 1000

- Value type - Integer
- Initial value - 500

multicastOverlappingTopicBehavior

This property is used to control the behavior of the broker when a client requests a Multicast subscription for a topic, that is part of a topic hierarchy containing topics, explicitly excluded for Multicast. Possible values are:

Accept

A matching Multicast subscription is accepted and all publications matching the topic, except those that are specifically excluded, are multicast.

Reject A Multicast subscription to a topic with children that are not enabled for Multicast is rejected by the broker.

Revert Subscriptions to a topic, or to children of that topic, that are not enabled for Multicast result in unicast transmission.

- Value type - String
- Initial value - Accept

multicastPacketBuffers

The number of memory buffers that are created at startup for packet reception. Having a high number of buffers available improves the reception performance and minimizes packet loss at high delivery rates, at the price of increased memory utilization. Each buffer is 33KB and this value can be in the range 1 through 5000.

- Value type - Integer
- Initial value - 500

multicastPacketSizeBytes

Indicates the size, in bytes, of Multicast packets. This can be in the range 500 through 32000.

- Value type - Integer
- Initial value - 7000

multicastProtocolType

Specifies the protocol type. This must be one of:

- PTL
- PGM/IP
- PGM/UDP
- Value type - String
- Initial value - PTL

multicastSocketBufferSizeKbytes

The size, in kilobytes, of the client's socket receiver buffer. Increasing it leads to lower loss rates. This value can be in the range 65 through 10000.

- Value type - Integer
- Initial value - 3000

multicastTransRateLimitKbps

Limits the overall transmission rate in Kb (kilobits) per second.

This property is only effective if the **multicastLimitTransRate** property is not Disabled. The value of this property should not be set higher than the maximum data transmission rate of the system or the network and can be in the range 10 through 1,000,000.

- Value type - Integer
- Initial value - 9500

nonDurableSubscriptionEvents

Indicates whether the user requires event messages when a non-durable subscriber is created or deleted. A true value causes an event publication to be created, false indicates that no event publications are made.

- Value type - Boolean
- Initial value - False

pingTimeoutMultiple

Number of consecutive clientPngIntervals or brokerPngIntervals without a response that the broker waits before disconnecting a client or broker.

- Value type - Integer
- Initial value - 3

statsInterval

The value is the number of milliseconds between statistics publications. If set to 0, statistics publications are not generated. You do not need to restart the broker after changing this property, however it can take the broker up to a minute to start producing statistics after the value is changed.

This should be in the range 0 through 1000

- Value type - Integer
- Initial value - 0

Note: This value refers to the publish/subscribe statistics interval only.

sysQopLevel

Applies to the system and allows brokers only to publish.

- Value type - string

- Initial value - none

Authorization

On Windows platforms, the user ID used to invoke this command must have **Administrator** authority on the local system.

On UNIX systems, the user ID used to invoke this command must either be **root** or must be the same as that specified in the **-i** parameter of the **mqsicreatebroker** command. It must also be a member of the **mqbrkrs** group.

Additionally, the authority required by the broker for the different protocols is as follows:

PGM/IP

The broker requires:

- Root authority on Linux and UNIX systems
- Administrator authority on Windows platforms
- root authority (UNIX System Services only) on z/OS

PGM/UDP

The broker requires User authority on all supported platforms

PTL The broker requires User authority on all supported platforms

httplistener **component parameter values**

Valid property names for the *HTTPListener* *ObjectName*:

enableSSLConnector

A boolean value which can be used to enable or disable the HTTPS (SSL) connector. This must be set to “true” before the http listener will listen for inbound SSL connections.

- Value type - Boolean
- Initial value - false

Valid property names for the *HTTPConnector* *ObjectName*:

address

For servers with more than one IP address, this value specifies which address is used for listening on the specified port. By default, this port is used on all IP addresses associated with the server. If specified, only one address can be used.

- Value type - string
- Initial value - null

port The TCP port number on which this Connector creates a server socket and awaits incoming connections.

- Value type - integer
- Initial value - 7080

Valid property names for the *HTTPSConnector* *ObjectName*:

address

For servers with more than one IP address, this value specifies which

address is used for listening on the specified port. By default, this port is used on all IP addresses associated with the server. If specified, only one address can be used.

- Value type - string
- Initial value - null

port The TCP port number on which this Connector creates a server socket and awaits incoming connections.

- Value type - integer
- Initial value - 7083

algorithm

The certificate encoding algorithm to be used.

- Value type - string
- Initial value - SunX509 on Solaris and HP-UX, and IbmX509 on other platforms (AIX, z/OS, Linux, Windows).

clientAuth

Set to true if the SSL stack requires a valid certificate chain from the client before accepting a connection. A false value (which is the default) does not require a certificate chain unless the client requests a resource protected by a security constraint that uses CLIENT-CERT authentication.

- Value type - string
- Initial value - false

keystoreFile

The path to the keystore file where the server certificate, which is to be loaded, has been stored. By default the http listener will expect a file called .keystore in the home directory of the user who started the broker.

- Value type - string
- Initial value - *default value* (described above)

keystorePass

The password used to access the server certificate from the specified keystore file.

- Value type - string
- Initial value - changeit

keystoreType

The type of keystore file to be used for the server certificate.

- Value type - string
- Initial value - JKS

sslProtocol

The version of the SSL protocol to use.

- Value type - string
- Initial value - SSLv3

ciphers

A comma separated list of the encryption ciphers that may be used. If not specified (the default), then any available cipher may be used.

- Value type - string
- Initial value - null

The possible values for *keystoreType*, *sslProtocol*, and *ciphers* are JSSE-implementation specific, and these values should be found in the JSSE provider documentation.

Authorization

On Windows platforms, the user ID used to invoke this command must have **Administrator** authority on the local system.

On UNIX systems, the user ID used to invoke this command must either be **root** or must be the same as that specified in the **-i** parameter of the `mqsicreatebroker` command. It must also be a member of the **mqbrkrs** group.

Examples:

Change the `clientPingInterval` to 200

```
mqsichangeproperties TEST -o DynamicSubscriptionEngine -n clientPingInterval -v 200
```

Enable multicast

```
mqsichangeproperties TEST -o DynamicSubScriptionEngine -n multicastEnabled -v true
```

Change the default `ssl` protocol from `SSLv3` to `TLS`

```
mqsichangeproperties TEST -b httpListener -n sslProtocol -v TLS
```

Enable the `HTTPS Connector`

```
mqsichangeproperties TEST -b httpListener -o HTTPListener -n enableSSLConnector -v true
```

mqsichangetrace command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

Use the **mqsichangetrace** command to set the tracing characteristics for a component. This command is valid for:

- User trace. Specify the **-u** option.
- Service trace. Specify the **-t** option. You are recommended to use this option only if directed to do so by the action described in a `BIPxxxx` message, or by your IBM Support Center.

You can initiate, modify, or terminate user tracing for a broker, or initiate, modify, or terminate service tracing for a broker, a Configuration Manager, or the User Name Server (identified by component name). You cannot use this command to initiate service tracing for the workbench.

On Windows platforms, Linux, and UNIX systems, you can also start and stop tracing activity for execution groups and message flows using the facilities of the workbench. See *User trace* for more information.

On z/OS, you can also start, modify, or stop a trace using the console commands or using the facilities of the workbench.

If you specify a broker, or any of its resources (execution group or message flow), you must have deployed them before you can start trace.

The trace output generated by these commands is written to trace files in the `log` subdirectory. When you have completed the work you want to trace, use `mqsireadlog` to retrieve the log as an XML format file. Use either `mqsiformatlog` (to produce a formatted file) or an XML browser to view the XML records.

When you set tracing on, you cause additional processing to be executed for every activity in the component you are tracing. You must expect to see some impact on performance when trace is active.

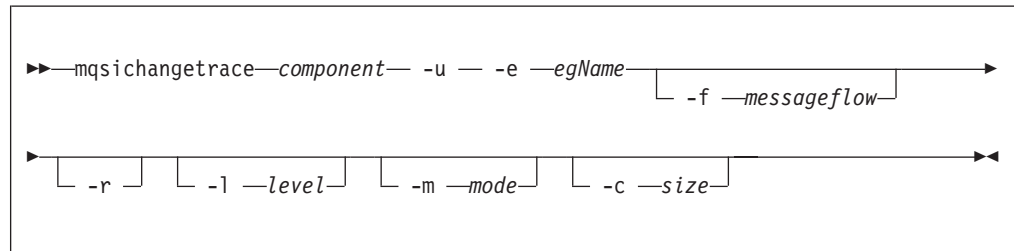
If you want to trace the command processes themselves, set the environment variables `MQSI_UTILITY_TRACE` and `MQSI_UTILITY_TRACESIZE` before you initiate trace.

Ensure that you reset these variables when tracing for the selected command is complete. If you do not do so, all subsequent commands are also traced, and their performance degraded.

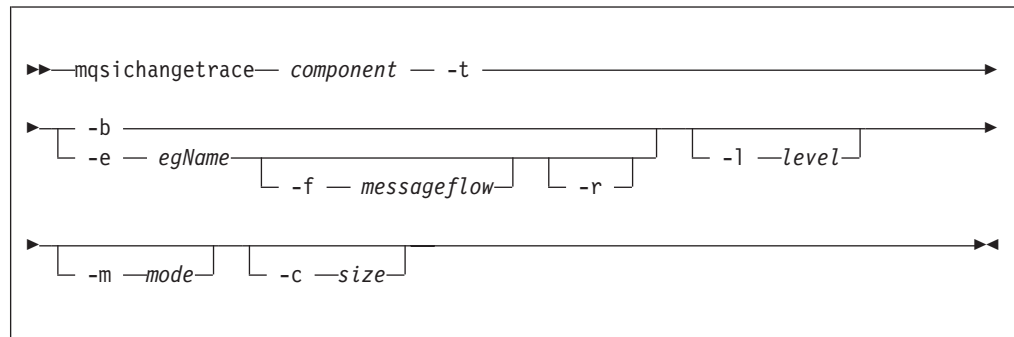
Syntax:

Windows platforms, Linux, and UNIX systems:

User trace:

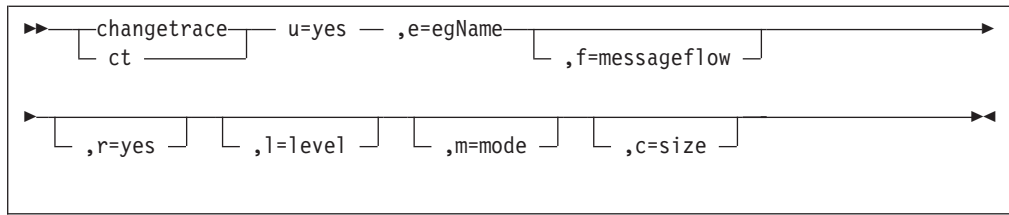


Service trace:

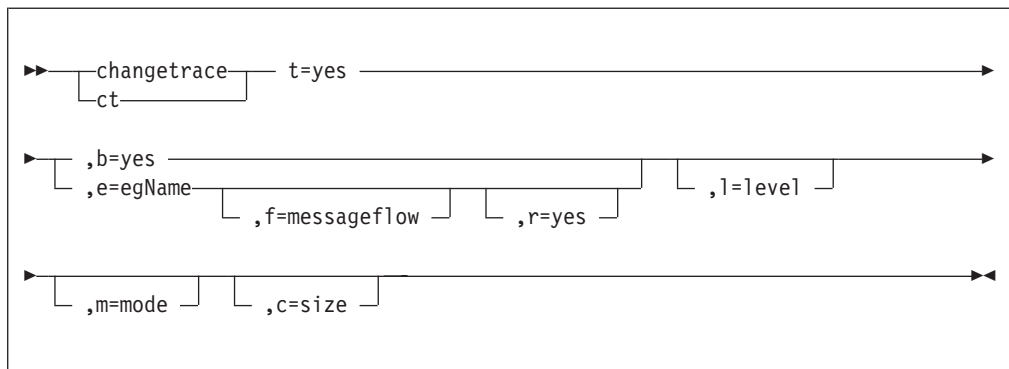


z/OS:

User trace:



Service trace:



Parameters:

component

(Required - Windows platforms, Linux, and UNIX systems) The name of the component for which trace parameters are to be changed. This can either be the name of a broker, or of a Configuration Manager, or the fixed value, `UserNameServer` (all are case sensitive on UNIX systems and on Linux).

Key words `workbench` and `utility` are reserved and must not be used as a component name.

- u** (Required for user trace only if the component is a broker) Specifies that user trace options are to be modified. This option is only valid if you have:
 - Specified a broker name as the component name on Windows platforms, Linux, and UNIX systems.
 - Issued this command against a broker (that is, not a Configuration Manager or User Name Server) on z/OS.

-e *egName*

(Required for user trace; optional for service trace) Identifies the execution group for which trace options are to be modified (for example, started or stopped). This option is only valid for a broker.

On z/OS, this name is case sensitive and you should include the names in single quotes if they contain mixed case characters.

-f *messageflow*

(Optional) Identifies the message flow for which trace options are to be modified. This option is only valid if you have specified an execution group (flag `-e`).

On z/OS, this name is case sensitive and you should include the names in single quotes if they contain mixed case characters.

- r** (Optional) This option requests that the trace log is reset: that is, all current

records are discarded. Use this option when you start a new trace to ensure that all records in the log are unique to the new trace.

This option is only valid if you have specified an execution group (flag `-e`).

-l *level*

(Optional) Set the level of the trace. This must be one of:

- `normal`. This provides a basic level of trace information.
- `none`. This sets tracing off.
- `debug`. This provides a more comprehensive trace.

Each component is created with a default value of `none`. If you do not specify this parameter, the current value is unchanged. Once you successfully change this value, it is persistent.

This is valid for all components.

-m *mode*

(Optional) Indicate the way trace information is to be buffered:

- `safe`. This mode causes trace entries to be written to file when they are generated.
- `fast`. This mode causes trace entries to be buffered, and only written to file in batches.

Each component starts with a default value of `safe`. If you do not specify this parameter, the current value is unchanged.

This option is only valid if the component you have specified is:

- A broker. If you change this value, it affects tracing for the execution group (if you have specified one), or for the agent component (if you have not specified an execution group).
- The User Name Server. If you change this value, it affects tracing for the entire component. (This is only valid for service trace.) Once you successfully change this value, it is persistent.

-c *size*

(Optional) The size of the trace file in KB (kilobytes). If you do not specify this parameter, the current value is left unchanged. Each component starts with a default value of 4096 KB. Specify this option to reset the value. The maximum value you can specify depends on how you subsequently intend to read the log, using the `mqsireadlog` command.

On HP-UX you are recommended to set this value below 500 MB.

- If you use `mqsireadlog` with the `-f` option set, the log file is read directly from the file system. In this case, the maximum value that can be specified here is 2097151, which will allow a trace file up to 2 GB (gigabyte) to be created.
- If you use `mqsireadlog` without setting the `-f` option, a WebSphere MQ message is sent to the broker to retrieve the log. In this case, the trace file size should not exceed 70 MB (megabytes). The maximum value that you can set here, should not be appreciably more than 70000.

However you intend to retrieve the trace file, you are recommended to keep its size as small as possible, either by using a low value for this parameter or by using the reset (`-r`) option on this command to clear the trace log. The benefit of adopting this approach is that the formatting process (`mqsiformatlog`) is much faster and requires less resource to carry out its task.

This option is only valid if the component you have specified is:

- A broker. If you change this value, it affects tracing for the execution group (if you have specified one), or for the agent component (if you have not specified an execution group).
- The User Name Server. If you change this value, it affects tracing for the entire component. (This is only valid for service trace.)

If you change the trace size, the new value is persistent over a restart of the broker or User Name Server.

Additional parameters exclusive to service trace:

Use these options only when directed to do so by your IBM Support Center or by a BIPxxxx message.

- t** (Required) Specifies that service trace options are to be modified.
- b** (Required) Specifies that service trace options for the agent subcomponent of the component specified are to be modified (for example, started or stopped). You can only specify this flag if **-t** is also specified.

Authorization:

The user ID used to issue the command must have **mqlbrkrs** authority.

Responses:

This command returns the following responses:

- BIP2595 Error casting character string '...' to an integer (z/OS only)
- BIP8002 Selected flags incompatible (z/OS only)
- BIP8003 Duplicate flag detected (z/OS only)
- BIP8013 Component does not exist
- BIP8020 Unable to access database
- BIP8029 Broker not configured
- BIP8031 Invalid flag supplied
- BIP8032 Unable to connect to queue
- BIP8033 Message send failure
- BIP8035 Response not received before time-out
- BIP8036 Negative response received
- BIP8037 Unsupported flag
- BIP8039 Execution group not available
- BIP8040 Unable to connect to database
- BIP8045 Message flow not found
- BIP8068 Integer argument required
- BIP8158 Invalid format for command (z/OS only)
- BIP8159 Unknown parameter "..." (z/OS only)

Examples:

Windows platforms, Linux, and UNIX systems:

To collect and process a user trace for the default execution group use the command:

```
mqsichangetrace WBRK_BROKER -u -e default -l normal -c 5000
```

To collect and process a service trace for flow f1 in the default execution group use the command:

```
mqsichangetrace WBRK_BROKER -u -e default -m fast
```

To collect and process a service trace for an agent use the command:

```
mqsichangetrace WBRK_BROKER -t -b -m -l normal
```

z/OS:

To collect and process a user trace for the default execution group use the command:

```
F MQP1BRK,ct u=yes,e='default',l=normal,c=5000
```

and in the PDSE member BIPJLOG, set the option for **mqsireadlog** to

```
-u -e default
```

To collect and process a service trace for flow f1 in the default execution group use the command:

```
F MQP1BRK,ct u=yes,e='default',f='f1',m=fast
```

and in the PDSE member BIPJLOG, set the option for **mqsireadlog** to

```
-t -e default -f f1-
```

To collect and process a service trace for an agent use the command:

```
F MQP1BRK,ct t=yes,b=yes,m=fast,l=debug
```

and in the PDSE member BIPJLOG, set the option for **mqsireadlog** to

```
-t -b agent
```

mqsichangeusernameserver command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPCHUN; see “Contents of the User Name Server PDSE” on page 379

Purpose:

On Windows platforms, Linux, and UNIX systems, use the **mqsichangeusernameserver** command to change various properties of the User Name Server.

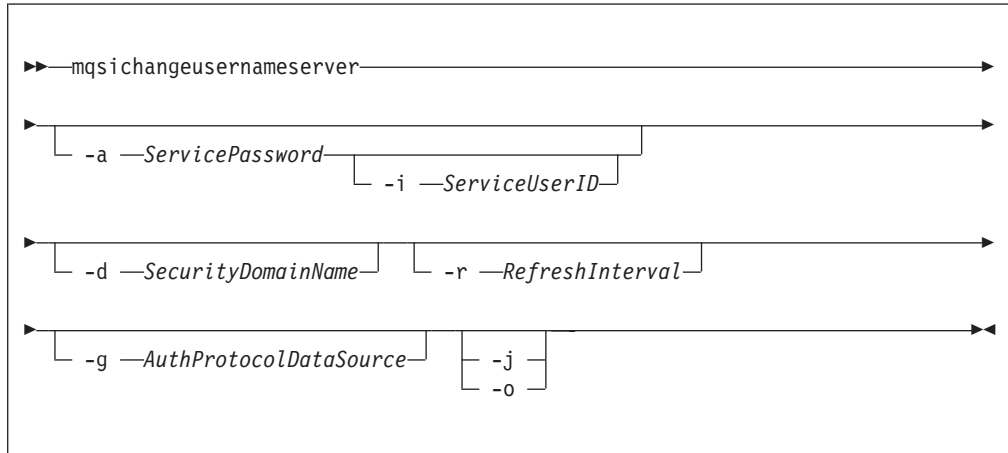
On z/OS, use the **mqsichangeusernameserver** command to change the refresh interval and authentication properties of the User Name Server

You must stop the User Name Server, using **mqsistop** on Windows platforms and UNIX platforms, or **stopcomponent** on z/OS, (see “mqsistop command” on page 362) before you can issue this command.

When you restart the User Name Server, using **mqsistart** on Windows platforms and UNIX platforms, or **startcomponent** on z/OS, (see “mqsistart command” on page 357) it uses the changed parameters.

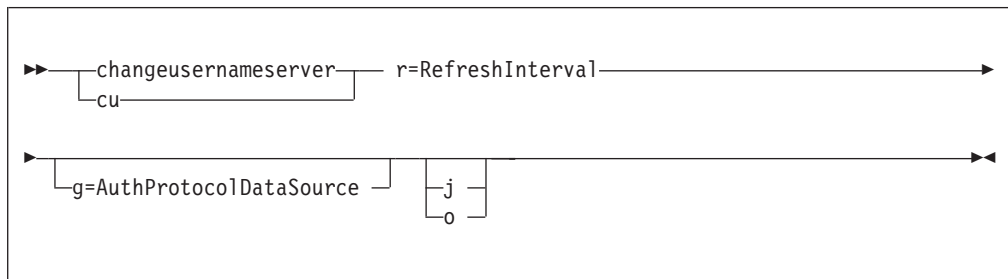
Syntax:

Windows platforms, Linux and UNIX systems:



z/OS console command:

Synonym: cu



Parameters:

-a ServicePassword

(Optional - Windows platforms, Linux, and UNIX systems) The password for the ServiceUserID.

For compatibility with existing systems, you can still specify <password>. However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

On Linux and UNIX systems, -a is required for Windows platforms compatibility but it is not used in relation to ServiceUserID.

-i ServiceUserID

(Optional - Windows platforms, Linux, and UNIX systems) The user ID under which the broker runs. You can only change this value if you also change the password.

This can be specified in any valid username syntax. On Windows platforms, these are:

- domain\username
- \\server\username
- .\username
- username

On Linux and UNIX systems, only the last format, username, is valid.

If you use the unqualified form for this user ID (username) in Windows, the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

The ServiceUserID specified must be a member of the local group **mqbrkrs**. On Windows platforms, it can be an indirect or direct member of the group. The ServiceUserID must also be authorized to access the home directory (where WebSphere Event Broker has been installed), and the working directory (if specified by the **mqsicreateusernameserver -w** flag). This ID must also be a member (either direct or indirect) of the local group **mqm**.

The security requirements for the ServiceUserID are detailed in “Security requirements for Windows platforms” on page 425 for Windows platforms and in “Security requirements for Linux and UNIX platforms” on page 424 for UNIX platforms.

-d *SecurityDomainName*

(Optional - Windows platforms, Linux, and UNIX systems) The name of the security domain on the Windows platform.

-r *RefreshInterval*

(Optional - Windows platforms, Linux, and UNIX systems) (Required - z/OS) The interval, in seconds, at which the User Name Server interrogates the security subsystem for changes to user or group attributes.

-g *AuthProtocolDataSource*

(Optional) Use this parameter to specify the name of the data source required by the authentication protocol.

-j (Optional) Indicates that groups and group memberships are defined in the data source for the authentication protocol, rather than being drawn from the operating system.

-o (Optional) Indicates that groups and group memberships are drawn from the operating system, rather than being defined in the data source for the authentication protocol.

Responses:

This command returns the following responses:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8018 Component running
- BIP8021 User ID/password incorrect
- BIP8022 Invalid user ID/password
- BIP8023 Password required
- BIP8030 Unable to modify user ID privileges

- BIP8068 Integer argument required

Examples:

Windows platforms, Linux, and UNIX platforms:

```
mqsichangeusernameserver -r 2000
```

z/OS:

```
F MQP1UNS,cu r=2000
```

mqsiclearmqpubsub command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS through the BIPCLMP utility; see “Contents of the broker PDSE” on page 378

Purpose:

Use the **mqsiclearmqpubsub** command to remove an WebSphere MQ Publish/Subscribe broker as a neighbor of this WebSphere Event Broker broker.

This command removes knowledge of the WebSphere MQ Publish/Subscribe broker from the WebSphere Event Broker broker identified on this command. To complete this action you must also issue the WebSphere MQ Publish/Subscribe command **clrmqbrk** against the WebSphere MQ Publish/Subscribe broker. When both clear commands have completed, all publish/subscribe traffic between the two brokers ceases.

Use this command only if you are integrating this WebSphere Event Broker broker with an WebSphere MQ Publish/Subscribe broker network. Before you issue this command you must ensure that the WebSphere Event Broker broker is ready to receive and process messages on queue SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS (that is, you must restart the broker after creating this queue.)

Syntax:

```
►►—mqsiclearmqpubsub—brokername— -n —NeighborQueueManagerName—►►
```

Parameters:

brokername

(Required) The name of the broker from which knowledge of an WebSphere MQ Publish/Subscribe neighbor broker is to be removed.

-n NeighborQueueManagerName

(Required) The name of the queue manager that hosts the WebSphere MQ Publish/Subscribe broker for which the association as a neighbor is being removed.

Authorization:

The user ID used to invoke this command must have put and inq authority to the queue SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS.

On Linux and UNIX systems, the user ID must be a member of the **mqbrkrs** group.

Responses:

This command returns the following responses:

- BIP8013 Component does not exist
- BIP8056 Unknown queue manager
- BIP8057 Queue manager error
- BIP8059 Queue manager not available
- BIP8060 Queue error
- BIP8061 No reply received
- BIP8064 Internal broker error
- BIP8066 Invalid broker name
- BIP8070 Database exception
- BIP8072 Database exception

Examples:

```
mqsiclearnmqpubsub WBRK_BROKER -n MQBroker1
```

mqsicreateaclentry command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPCRACL; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

Use the **mqsicreateaclentry** command to create or modify the Configuration Manager data relating to the group or user access control lists that you have defined.

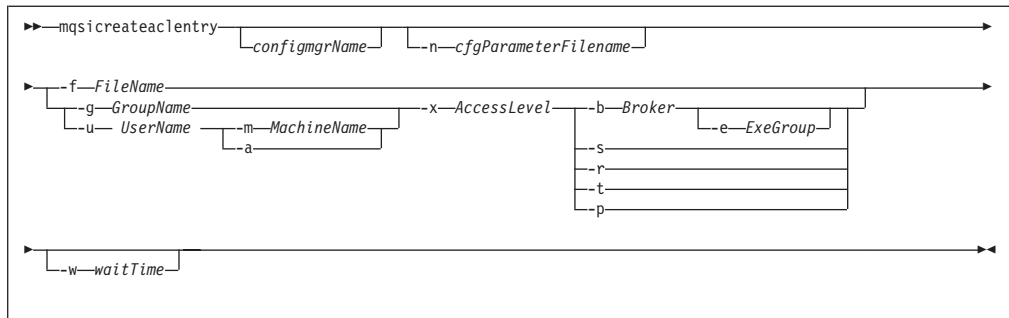
If you create or modify an access control group you must stop and restart the Configuration Manager for the change to take effect.

On z/OS, you must define an OMVS segment for user IDs and groups, in order for a Configuration Manager to obtain user ID and group information from the External Security Manager (ESM) database.

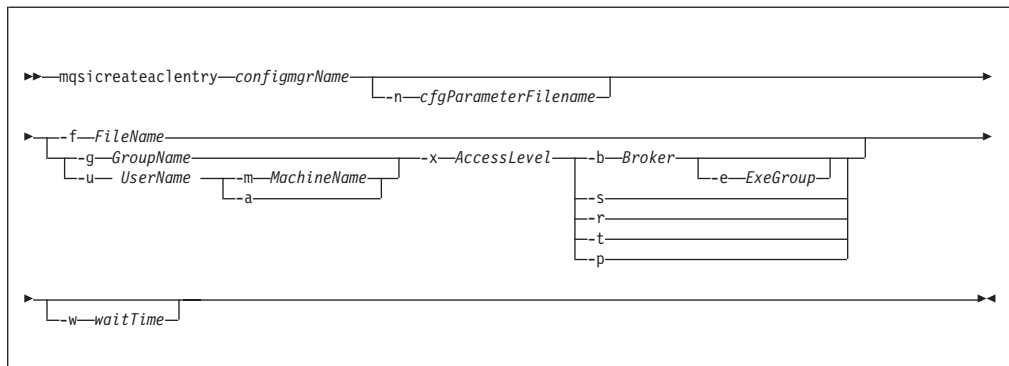
Note that this command does not check for the existence of the specified component in case you want to set up the access control list first.

Syntax:

Windows:

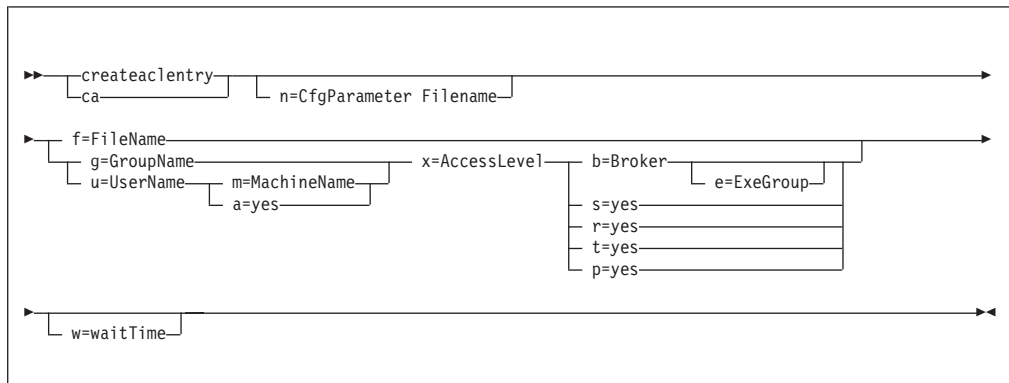


Linux and UNIX systems:



z/OS console command:

Synonym: `ca`



Parameters:

You **must** select either `-f` or

- `-g` or `-u`, and
- `-x`, and
- `-b` and `-e` or `-s` or `-r` or `-t` or `-p`

If you select `-u` you must select either `-m` or `-a`

configmgrName

(Optional - Windows. Required - Linux and UNIX systems.) The name of the Configuration Manager to which the access control lists are to be added.

On Linux and UNIX systems this must be the first parameter specified. It is case-sensitive on Linux and UNIX systems. On z/OS this parameter is implicit because you specify the component you want to MODIFY.

The default name on Windows, if this parameter is not specified, is 'ConfigMgr'.

-ncfg *ParameterFilename*

(Optional) The name of a .configmgr file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the .configmgr format saved by the Eclipse GUI. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
  securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement `encoding="UTF-8"` from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the host attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
  securityExit="test.myExit"/>
```

-f *FileName*

(Optional) File from which to import the configuration. The output of the **mqsilistaclentry** command is the correct format.

-g *GroupName*

(Optional) Local group to which this entry refers. For this reason, the name must adhere to the standard platform convention for group names.

To add a domain group, grant authority to a local group and then add the domain group, or groups, that you want to authorize into that local group. Any members of those domain groups obtain the permissions of the local group indirectly.

-u *UserName*

(Optional) User name to which this entry refers, for example, TEST\ANOTHER.

Note: **-u** and **-g** in this command refer to users and groups within the domain that the Configuration Manager uses for its security. This domain is by default the machine on which the Configuration Manager resides.

-m *MachineName*

(Optional) The name of the machine from which a specified user can connect. This option can not be used with **-a**.

-a (Optional) This signifies that the specified user name can be on any machine. This option can not be used with **-m**.

Note: If you select **-u**, you must select either **-a** or **-m**.

-x *AccessLevel*

(Optional) The required access level given for this group. This can be any one of the following letters:

F Full control

D Deploy

E Edit

V View

-b *Broker*

(Optional) The object is a broker object, and its name is specified as a parameter.

-e *ExeGroup*

(Optional) The object is an execution group and its name is specified as a parameter of the form Broker\ExeGroup. You must specify the **b** flag if you specify this flag.

-s *Subscription*

(Optional) The object is a subscription object, and its name is specified as a parameter.

-r (Optional) The object refers to the root topic.

-t (Optional) The object refers to the main topology.

-p (Optional) The object refers to the "allresources" resource type. The authority that the principal has for this object applies to all objects, including the mqsicreateaclentry, mqsideleteaclentry, and mqsilistaclentry commands themselves.

-w *waitTime*

(Optional) The time in seconds that the command waits for a response from the Configuration Manager. If you do not supply a value the command waits for 30 seconds.

Authorization:

The user ID used to invoke this command must have full control permissions for the object being changed; see "ACL permissions" on page 423 for more information.

When z/OS commands are run through the console, they effectively run as the Configuration Manager's started-task ID. This means that the commands inherit a Full Control root ACL and you can carry out any operation.

If you submit a console command to the Configuration Manager you can change any ACL for that Configuration Manager.

Examples:

Windows, Linux, and UNIX systems:

```
mqsicreateaclentry CMGR01 -f c:\test\mylist  
mqsicreateaclentry CMGR01 -g GROUPA -x F -b MYBROKER
```

z/OS. Note, that on z/OS you must use a comma between each command option. The following example shows the z/OS version of the preceding Windows, Linux, and UNIX systems example:

```
/f CMGR01, ca g='GROUPA', x='F', b='MYBROKER'
```

mqsicreatebroker command

Supported platforms:

- Windows
- Linux and UNIX systems

- z/OS. You can also use BIPCRBK; see “Contents of the broker PDSE” on page 378

Purpose:

The **mqsicreatebroker** command:

- Creates a WebSphere MQ queue manager, except on z/OS, if one does not already exist.

Note:

1. If a WebSphere MQ queue manager is created as a result of using the **mqsicreatebroker** command, the default DLQ provided by WebSphere MQ (SYSTEM.DEAD.LETTER.QUEUE) is automatically enabled. The security settings are the same as those of other broker-specific WebSphere MQ queues.

If you choose to create the queue manager separately, you must set up a dead letter queue (DLQ). The DLQ is referenced by WebSphere Event Broker when errors occur processing messages in message flows.

If a message in either a user-defined message flow or in the publish/subscribe model cannot be processed, it is routed to this DLQ as a last resort. If you prefer to back out the message onto the input queue, effectively halting the message flow until the problem is resolved, disable the DLQ.

The **mqsdeletebroker** command does not delete this queue (unless the queue manager is deleted).

- 2.

If you are using a WebSphere MQ queue manager that has been created independently of the **mqsicreatebroker** command, you can define clusters if you choose. This simplifies your configuration in most cases.

- Starts the WebSphere MQ queue manager, except on z/OS, if it is not already running.

If the queue manager is created by this command, it is not started as a Windows service; it will therefore stop if you log off. To avoid this happening, you must either remain logged on, or change the startup status of the queue manager service. (If you lock your workstation, the WebSphere MQ queue manager does not stop.)

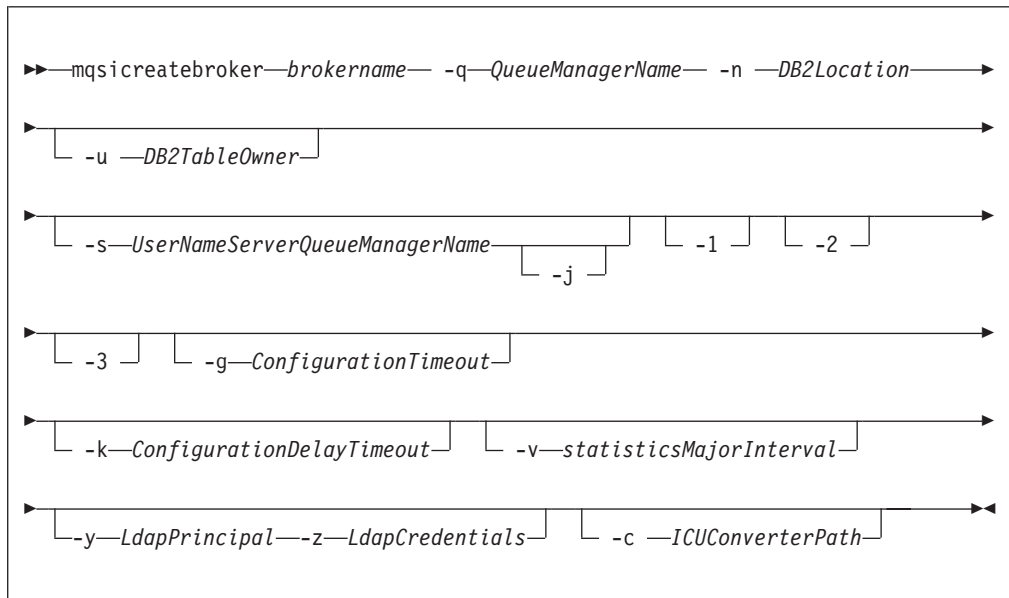
- Creates the broker-specific WebSphere MQ queues, if these do not already exist.
- Creates database tables for the broker, if they do not already exist, or adds rows specific to this broker to existing tables.
- On Windows platforms, installs a service under which the broker will run.
- Creates a record for the component in the broker registry.

Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS console command:



Parameters:

brokername

(Required) The name of the broker that you want to create. This must be the first parameter, and it is case sensitive on Linux and UNIX systems.

On z/OS, if you create an uppercase broker name, you must use this name in uppercase also for your broker in the workbench. For restrictions on the character set that can be used, see "Characters allowed in commands" on page 240.

-i *ServiceUserID*

(Required - Windows platforms, Linux, and UNIX systems) The user ID under which the broker will run.

This can be specified in any valid username syntax. On Windows platforms these are:

- domain\username
- \\server\username
- .\username
- username

On Linux and UNIX systems, only the last format, username, is valid.

If you use the unqualified form for this user ID (username) on Windows platforms, the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

The *ServiceUserID* specified must be a member of the local group **mqbrkrs**. On Windows platforms, it can be a direct or indirect member of the group. The *ServiceUserID* must also be authorized to access the home directory (where WebSphere Event Broker has been installed), and the working directory (if specified by the **-w** flag).

If you specify, on Windows platforms, that the broker is to run as a WebSphere MQ trusted application (flag **-t**), you must also add this user ID to the group **mqm**. On Linux and UNIX systems, specify the *ServiceUserID* as **mqm** if you set the **-t** flag.

The security requirements for the *ServiceUserID* are detailed in “Security requirements for Windows platforms” on page 425.

If you use this user ID for database access (that is, you do not specify a different user ID with the **-u** flag) and you are using SQL Server for your database, you must create this user ID as an SQL Server login ID and give it the correct access before you create the broker (see “Considering security for a broker” on page 15 for further details). If your broker database exists in DB2, and this user ID is not known to DB2, DB2 automatically creates it for you.

-a *ServicePassword*

(Required - Windows platforms, Linux, and UNIX systems) The password for the *ServiceUserID*.

For compatibility with existing systems, you can still specify <password>. However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

On Linux and UNIX systems **-a** is required for Windows platforms compatibility, but is not used in relation to *ServiceUserID*; it is used as a default only if **-p** is not specified. (See notes about the **-p** parameter for further details.)

-q *QueueManagerName*

(Required) The name of the queue manager associated with this broker. Use the same name for your broker and the queue manager to simplify the organization and administration of your network. Queue manager names are limited to 48 characters in length and are case sensitive.

Each broker *must* have its own unique queue manager. A broker cannot share a queue manager with another broker.

If the queue manager does not already exist, it is created by this command. It is not created as the default queue manager; if you want this queue manager to be the default queue manager on this system, you must either create the queue manager before you issue this command, or change the settings of this queue manager to make it the default. Use either the WebSphere MQ Explorer or the WebSphere MQ Services snap-in, depending which version of WebSphere MQ you are using.

The queue manager attribute MAXMSGLN (maximum length of messages that can be put to queues) is updated to 100 MB. This is done whether or not the queue manager is created by this command.

For restrictions on the character set that can be used, see “Characters allowed in commands” on page 240.

-n *DataSourceName*

(Required - Windows platforms, Linux, and UNIX systems) The ODBC data source name (DSN) of the database in which the broker tables are created. This must be the DSN, not the name of the database, if you have not used the same name for both.

This database must already exist. You must create a System DSN ODBC connection for this DSN, if you have not already done so.

If you have a DB2 database on Linux, enter the appropriate DB database alias name; an ODBC DSN is not required.

-u *DataSourceUserID*

(Optional - Windows platforms, Linux, and UNIX systems) The user ID with which databases containing broker tables and user data are to be accessed. If this is not specified, it defaults to the value specified by *-i*.

This user ID must have the authority to create tables within this database, and read from and write to those tables.

On Windows platforms, if your broker database exists in DB2, and this user ID is not known to DB2, it is created for you within DB2. On Linux and UNIX systems, the service user must have previously been granted the correct privilege. If your database is SQL Server, you must create this user ID as an SQL Server login ID and give it the correct access before you create the broker (see “Security requirements for Windows platforms” on page 425 for further details).

If you have an application database in DB2 that was created by this user ID, or to which this user ID has appropriate read, write, or create authority, message flows executing in this broker can access and manipulate the application data held within it without having to specify explicit schema names.

-n *DB2Location*

(Required - z/OS) The location of the database in which the broker tables are created.

-u *DB2TableOwner*

(Required - z/OS) The user ID with which databases containing broker tables and user data are to be accessed.

This user ID must have the authority to create tables within this database, and read from and write to those tables.

| If you have an application database in DB2 that was created by this user ID, or
| to which this user ID has appropriate read, write, or create authority, message
| flows executing in this broker can access and manipulate the application data
| held within it without having to specify explicit schema names.

-p *DataSourcePassword*

(Optional - Windows platforms, Linux and UNIX systems) The password of the user ID with which databases containing broker tables and user data are to be accessed. If not specified, this defaults to the *ServicePassword* specified by **-a**.

For compatibility with existing systems, you can still specify `<password>`. However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

For DB2 on Linux and UNIX systems, **-u** and **-p** can be specified as empty strings (two double quotation marks `""`). In this case, DB2 grants WebSphere Event Broker the privileges of the *ServiceUserID*, which results in a database connection as "already verified". If you specify **-a** as an empty string as well as **-u** and **-p**, no passwords are stored by WebSphere Event Broker, creating the most secure configuration.

-s *UserNameServerQueueManagerName*

(Optional) The name of the WebSphere MQ queue manager that is associated with the User Name Server. You **must** specify this parameter if you require either authentication services or publish/subscribe access control. If this is not specified, the broker assumes that there is no User Name Server defined.

-j (Optional) You **must** specify this flag in conjunction with the **-s** *UserNameServerQueueManagerName* parameter to enable publish/subscribe access control.

-w *Workpath*

(Optional - Windows platforms, Linux, and UNIX systems) The directory in which working files for this broker are stored. If this is not specified, files are stored in the default workpath, specified when the product was installed. If specified, you must create this directory before you start the broker. On Windows platforms, this cannot be on a networked drive.

This directory is also used for trace records created when tracing is active. These are written to a subdirectory *log*, which you must create before you start the broker.

Error logs written by the broker when a process terminates abnormally are stored in this directory. On Windows platforms, use this option, to specify a directory on a drive other than the one on which the product is installed.

The error log is unbounded and continues to grow. Check this directory periodically and clear out old error information.

You cannot change this option using the **mqsichangebroker** command. If you want to specify, or change, the workpath, delete and recreate the broker.

-t (Optional - Windows platforms, Linux, and UNIX systems) The broker is configured to run as a WebSphere MQ trusted application.

If you specify this option on Windows platforms, add the *ServiceUserID* (identified by flag **-i**) to the group **mqm**. If you specify this option on HP-UX and Solaris, specify the *ServiceUserID* as **mqm**. For more details about using WebSphere MQ trusted applications, see *WebSphere MQ Intercommunication*.

-m (Optional -Windows platforms, Linux, and UNIX systems) Migrate an existing WebSphere MQ Publish/Subscribe broker. If you specify this option, the queue manager identified by **-q** must be the queue manager being used by the WebSphere MQ Publish/Subscribe broker.

-l *UserLilPath*

(Optional - Windows platforms, Linux, and UNIX systems) A list of paths (directories) from which the broker loads LILs (loadable implementation libraries) for user-defined message processing nodes.

You must create your own directory for storing your `.lil` or `.jar` files. Do not save them in the WebSphere Event Broker install directory.

If you specify more than one additional directory, they must be separated by the default platform-specific path separator (semicolon (;) on Windows platforms, colon (:)) on Linux and UNIX systems).

You cannot include environment variables in this path: if you do so, they are ignored.

-g *ConfigurationTimeout*

(Optional) The length of time (in seconds) that an execution group in the broker is allowed to take to apply a change in configuration (for example, an update that you have deployed from the workbench).

When a message flow is processing an application message, it cannot respond to a configuration flow change. If any one of the message flows within the execution group that has been requested to change its configuration does not finish processing an application message and apply the configuration change within this timeout, the execution group returns a negative response to the deployed configuration message.

The value that you set for this timeout depends on the system load (including CPU utilization) and on each execution group's load. You can make an initial estimate by deploying the broker's entire configuration. The time taken for this to complete successfully gives you an indication of the minimum value to set.

The value is specified in seconds and can range from 10 to 3600. The default value is 300.

The sum of the *ConfigurationTimeout* and the *ConfigurationDelayTimeout* (described below) represents the maximum length of time that a broker is allowed to process a deployed configuration message before it generates a negative response.

-k *ConfigurationDelayTimeout*

(Optional) The length of time (in seconds) that a broker is allowed to take to process a minimal change in configuration (for example, an update that you have deployed from the workbench).

This represents the time it takes for a minimal deployed configuration message to be processed by the broker and its execution groups, and depends on queue manager network delays, the load on the broker's queue manager, and system load.

You can estimate this value by issuing a command to request a simple configuration change, for example:

- On Windows platforms, Linux, and UNIX systems
`mqsireporttrace brokerName -e "Execution Group Name" -u`
- On z/OS
`F MQP1BRK,reporttrace u=yes,e='exgrp1'`

The response time of each execution group differs according to system load and the load of its own processes. The value that you set must reflect the longest response time that any execution group takes to respond. If the value that you set is too low, the broker returns a negative response, and might issue error messages to the local error log.

The value is specified in seconds and can range from 10 to 3600. The default value is 60.

If the broker is on a production system, increase the values for both *ConfigurationTimeout* and *ConfigurationDelayTimeout* to allow for application messages currently being processed by message flows to be completed before the configuration change is applied.

If the broker is on a development or test system, you might want to reduce time-outs (in particular, the *ConfigurationTimeout*) to improve perceived response times, and to force a response from a broker that is not showing expected behavior. However, reducing the time-out values decreases the probability of successfully deploying a configuration change.

-P *HTTPListenerPort*

(Optional - Windows platforms, Linux, and UNIX systems) Enter the number of the port on which the Web services support is listening.

This listener is started by the broker when a message flow that includes Web services support is started, and has a default value of 7080.

Ensure that the port that you specify has not been specified for any other purpose.

-v *statisticsMajorInterval*

(Optional) The timer interval in minutes at which WebSphere Event Broker statistics and accounting is told to output archive records. For internal accounting, the valid range is from 10 to 14400 minutes.

An interval of zero minutes indicates that the platform has an external method of notification and is not using an internal timer within WebSphere Event Broker.

-1 (Optional - z/OS only) The registry pass, which creates only the broker registry.

-2 (Optional - z/OS only) The WebSphere MQ pass, which creates only the broker WebSphere MQ queues.

-3 (Optional - z/OS only) The DB2 pass, which creates only the broker DB2 tables and indexes.

-y *LdapPrincipal*

(Optional - all platforms, but mandatory when *LdapCredentials* is provided.) The user principal for access to an optional LDAP directory that holds the JNDI administered Initial Context for the JMS provider.

-z *LdapCredentials*

(Optional - all platforms, but mandatory when *LdapPrincipal* is provided.) The user password for access to LDAP.

-c *ICUConverterPath*

(Optional) A delimited set of directories to search for additional code page converters. On Windows systems the delimiter is “;”. On UNIX and Linux

systems, the delimiter is ":". The code page converters must be either of the form `icudt32_codepagename.cnv` or in an ICU data package called `icudt32.dat`.

Authorization:

On Windows systems, the user ID used to invoke this command must have **Administrator** authority on the local system.

On UNIX systems, the user ID used to invoke this command must be a member of the **mqbrkrs** group.

On z/OS systems, the user ID used to invoke this command must be a member of a group that has READ and WRITE access to the component directory.

Using LDAP: Ensure that the registry is appropriately secured to prevent unauthorized access. The setting of *LdapPrincipal* and *LdapCredentials* options on **mqsicreatebroker** is not required for correct operation of the broker. The password is not stored in clear text in the file system.

Websphere MQ queues created:

- SYSTEM.BROKER.ADMIN.QUEUE
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.EXECUTIONGROUP.QUEUE
- SYSTEM.BROKER.EXECUTIONGROUP.REPLY
- SYSTEM.BROKER.INTERBROKER.QUEUE
- SYSTEM.BROKER.INTERBROKER.MODEL.QUEUE
- SYSTEM.BROKER.MODEL.QUEUE
- SYSTEM.BROKER.WS.INPUT
- SYSTEM.BROKER.WS.REPLY
- SYSTEM.BROKER.WS.ACK

Access authority is granted for the WebSphere Event Broker group **mqbrkrs** to all these queues. If the DLQ is enabled, it also has the same authority.

Database tables created:

The database tables that this command creates, or adds to, are described in Database contents.

Responses:

This command returns the following responses:

- BIP8011 Unable to create configuration data
- BIP8012 Unable to connect to system components
- BIP8014 Component cannot be created
- BIP8022 Invalid user ID/password
- BIP8030 Unable to modify user ID privileges
- BIP8040 Unable to connect to database
- BIP8048 Unable to start queue manager
- BIP8050 Unable to create queue manager
- BIP8051 Unable to create queue
- BIP8053 Unable to set security for queue manager

- BIP8054 Unable to set security for queue
- BIP8056 Unknown queue manager
- BIP8070 Database exception
- BIP8072 Database exception
- BIP8073 Invalid broker name
- BIP8084 Unable to create directory
- BIP8086 Queue manager in use
- BIP8087 Component already exists
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping

In some circumstances, you might see the following error message issued by DB2:

```
(51002) [IBM] [CLI Driver] [DB2/NT]SQL0805N
Package "NULLID.SQLLF000" was not found.  SQLSTATE=51002.
```

This error occurs when the bind to the database is not successful.

On Windows platforms, binding is not needed for broker databases, but is required for user databases. If you have created the database using the DB2 Control Center, the bind is completed for you. If you use the command interface, it is not. For the database MYDB, for example, you can create or re-create a bind by entering the following commands at the command prompt:

```
db2 connect to MYDB user db2admin using db2admin
db2 bind X:\sqllib\bnd\@db2cli.lst grant public
db2 connect reset
```

where X: is the drive on which DB2 is installed.

On UNIX platforms, binding is necessary for all databases. For the database WBRKBKDB, for example, you can effect this by entering the following commands at the command prompt (where <user_name> is the user ID under which the database instance was created):

```
db2 connect to WBRKBKDB user db2admin using db2admin
db2 bind ~<user_name>/sqllib/bnd/@db2cli.lst grant public CLIPKG 5
db2 connect reset
```

If you are not using the default DB2 user ID and password (db2admin), you must replace these values in the db2 connect command with the correct values.

If you run the **mqsicreatebroker** command for a second time because of a failure the first time, you receive a series of messages. These indicate any items that cannot be created. There should not be any detrimental effects as a result of this. For example, as long as the reason for the first failure has been resolved, attempting to create a broker which failed the first time should result in a properly created broker.

Examples:

```
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw -q WBRK_QM -s WBRK_UNQ_QM -n WBRKBKDB
mqsicreatebroker WBRK_BROKER -i wbrkuid -a wbrkpw -q WBRK_QM -n WBRKBKDB -t
```

| To create an entire broker on z/OS:

```
| mqsicreatebroker CSQ1BRK -q CSQ1 -u BRKUSER -n DBA0
```

| To create only the DB2 tables and indexes on z/OS:

```
| mqsicreatebroker CSQ1BRK -q CSQ1 -u BRKUSER -n DBA0 -2
```

| **mqsicreateconfigmgr command**

| **Supported platforms:**

- | • Windows
- | • Linux and UNIX systems
- | • z/OS. You can also use BIPCRCM; see “Contents of the Configuration Manager PDSE” on page 380

| **Purpose:**

This command completed the following actions:

- | • Creates a WebSphere MQ queue manager, if one does not already exist.

| **Notes:**

- | 1. If a WebSphere MQ queue manager is created as a result of using the **mqsicreateconfigmgr** command, the default DLQ provided by WebSphere MQ (SYSTEM.DEAD.LETTER.QUEUE) is automatically enabled. The security settings are the same as those of other broker-specific WebSphere MQ queues.

If you choose to create the queue manager separately, set up a dead letter queue (DLQ). The DLQ is referenced by WebSphere Event Broker when errors occur processing messages in message flows.

If a message in either a user-defined message flow or in the publish/subscribe model cannot be processed, it is routed to this DLQ as a last resort. If you would prefer the message to be backed out onto the input queue, effectively halting the message flow until the problem is resolved, disable the DLQ.

The **mqsdeleteconfigmgr** command does not delete this queue (unless the queue manager is deleted).

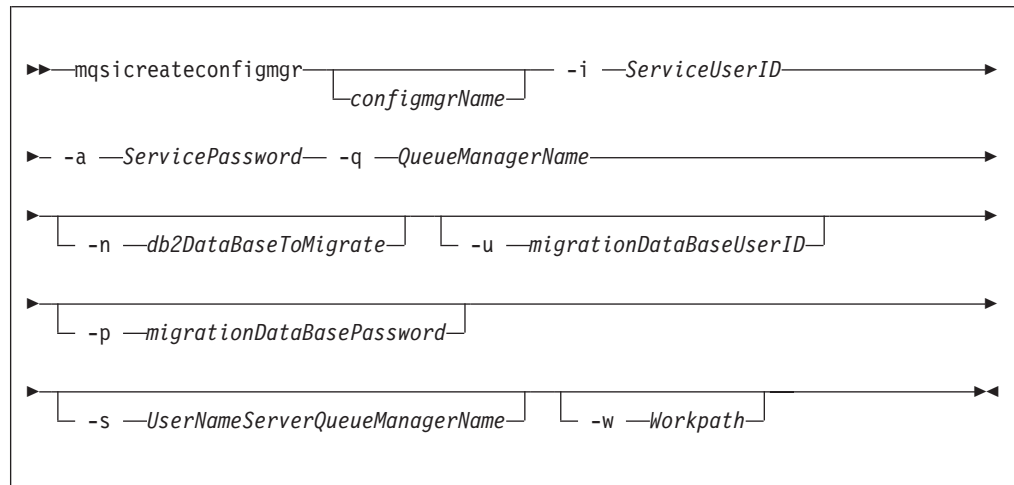
- | 2. If you are using a WebSphere MQ queue manager that has been created independently of the **mqsicreateconfigmgr** command, you can define clusters if you choose. This option simplifies your configuration.
 - | • Starts the WebSphere MQ queue manager, if it is not already running.
 - | • Creates the WebSphere MQ queues and channel that are specific to the Configuration Manager, if they do not already exist.
 - | • Creates database tables for the Configuration Manager in its internal repository. If you need to transfer data from the configuration repository of an earlier release, you can use the *db2DatabaseToMigrate*, *migrationDatabaseUserId*, and *migrationDatabasePassword* parameters.
 - | • If you run this command using the *-n* parameter and then delete the Configuration Manager using **mqsdeleteconfigmgr**, without specifying the *-n* parameter on that command, the new database containing the configuration repository is not deleted.

If you run this command again in this situation, and specify the *-n* parameter, the parameter is ignored because the new database still exists.
 - | • (Windows only) - installs a Windows service, under which the Configuration Manager runs.
 - | • Creates a record for the component in the broker registry.

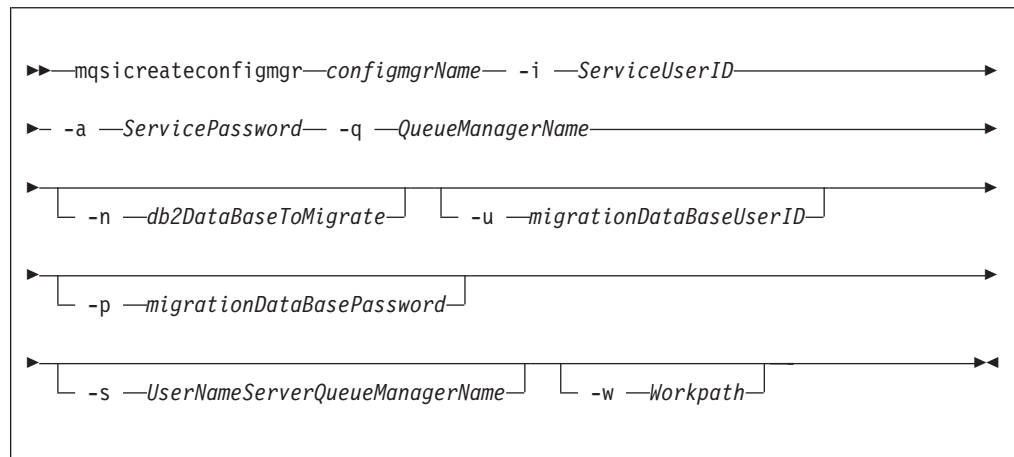
If you have installed VisualAge for Java, and selected the WebSphere MQ Connector as part of that installation, ensure that the CLASSPATH entry for VisualAge for Java appears *after* the CLASSPATH entries for WebSphere MQ for the Windows platform that you are using (server or Java client). This requirement ensures that the Configuration Manager accesses the correct WebSphere MQ classes (not the VisualAge classes) when it is started by the “mqsisstart command” on page 357. If the Configuration Manager detects an error in this area, it writes message BIP1004 to the Windows System Event log.

Syntax:

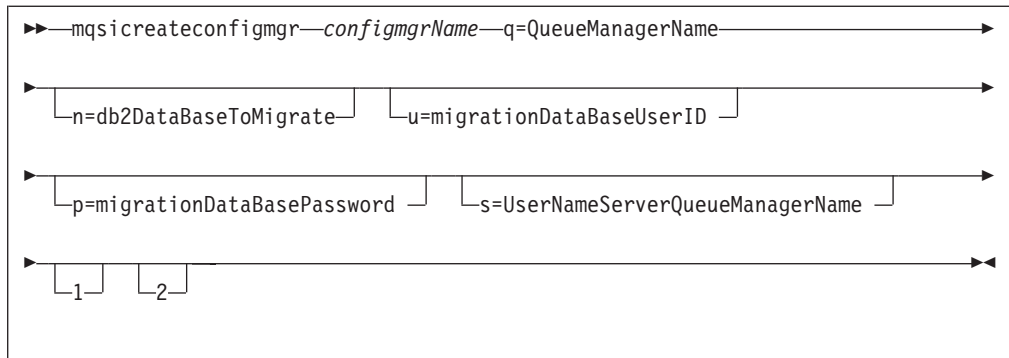
Windows:



Linux and UNIX systems:



z/OS:



Parameters:

configmgrName

(Optional - Windows. Required - Linux, UNIX systems, and z/OS) The name of the Configuration Manager that you want to create.

On Linux, UNIX systems and z/OS, this parameter must be the first specified. It is case-sensitive on Linux, UNIX systems and z/OS.

The default name on Windows, if this parameter is not specified, is 'ConfigMgr'.

-i *ServiceUserID*

(Required) The user ID under which the service runs.

This parameter can be specified in any valid username syntax for the platform.

The *ServiceUserID* specified must be a member (either direct or indirect) of the local group **mqbrkrs**, and must be authorized to access the home directory (where WebSphere Event Broker has been installed), and the working directory (if specified by the **-w** flag).

The security requirements for the *ServiceUserID* are detailed in "Security requirements for Windows platforms" on page 425 for Windows, "Security requirements for Linux and UNIX platforms" on page 424 for UNIX platforms, and "Security requirements for z/OS" on page 428 for z/OS.

If you use the unqualified form for the service user ID (username), on Windows the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

-a *ServicePassword*

(Required) The password for the *ServiceUserID*.

For compatibility with existing systems, you can still specify `<password>`.

However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

-q *QueueManagerName*

(Required) The name of the queue manager associated with the Configuration Manager.

If the queue manager does not already exist, it is created by this command. It is not created as the default queue manager: if you want it to be the default queue manager on this system, create the queue manager before you issue this command.

The queue manager attribute MAXMSGL (maximum length of messages that can be put to queues) is updated to 100 MB. This update is done whether or not the queue manager is created by this command.

-n *db2DatabaseToMigrate*

(Optional) The name of the database that you created at an earlier release to hold the configuration repository tables.

This database must already exist. You do not need to create an ODBC connection for this database, because access is provided by JDBC.

-u *migrationDataBaseUserID*

(Optional) The user ID with which the configuration repository database (created at an earlier release) is to be accessed.

-p *migrationDataBasePassword*

(Optional) The password of the user ID with which the configuration repository database (created at an earlier release) is to be accessed. If not specified, this parameter defaults to the ServicePassword specified by -a.

For compatibility with existing systems, you can still specify <password>. However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

-s *UserNameServerQueueManagerName*

(Optional) The name of the WebSphere MQ queue manager that is associated with the User Name Server. If this parameter is not specified, the Configuration Manager assumes that there is no User Name Server defined, and does not attempt to communicate with one.

-w *Workpath*

(Optional) The directory in which working files for the Configuration Manager are stored. If not specified, the default directory specified when the product was installed is used.

- 1 (Optional - z/OS only) The registry pass that creates only the Configuration Manager registry.
- 2 (Optional - z/OS only) The WebSphere MQ pass that creates only the Configuration Manager WebSphere MQ queues.

Note: This action can be performed only if the Configuration Manager registry exists.

Authorization:

This command changes security privileges for the ServiceUserID; the user ID used to invoke this command must be a member of the Windows **Administrators** group on this local system.

On UNIX systems, the user ID used to invoke this command must be a member of the mqbrkrs group.

On z/OS systems, the user ID used to invoke this command must be a member of a group that has READ and WRITE access to the component directory.

Websphere MQ queues created:

- SYSTEM.BROKER.CONFIG.QUEUE

- SYSTEM.BROKER.CONFIG.REPLY
- SYSTEM.BROKER.ADMIN.REPLY
- SYSTEM.BROKER.SECURITY.REPLY
- SYSTEM.BROKER.MODEL.QUEUE

Access authority is granted for the WebSphere Event Broker group **mqrbrks** to all these queues. If the DLQ is enabled, it also has the same authority.

Websphere MQ channels created:

- SYSTEM.BKR.CONFIG

Database tables created:

The database tables that this command creates are administered by the Configuration Manager.

Responses:

This command returns the following responses:

- BIP8011 Unable to create configuration data
- BIP8012 Unable to connect to system components
- BIP8014 Component cannot be created
- BIP8022 Invalid user ID/password
- BIP8030 Unable to modify user ID privileges
- BIP8048 Unable to start queue manager
- BIP8050 Unable to create queue manager
- BIP8051 Unable to create queue
- BIP8053 Unable to set security for queue manager
- BIP8054 Unable to set security for queue
- BIP8055 Unable to load Java class
- BIP8056 Unknown queue manager
- BIP8074 Unable to create JVM
- BIP8075 Java exception
- BIP8076 Unable to set current directory
- BIP8077 Error initializing configuration data
- BIP8078 Error initializing configuration data
- BIP8084 Unable to create directory
- BIP8087 Component already exists
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping
- BIP8097 Unable to create Java object

Examples:

```
mqsicreateconfigmgr CMGR01 -i wbrkuid -a wbrkpw -q WBRK_CONFIG_QM
```

mqsicreatedb command

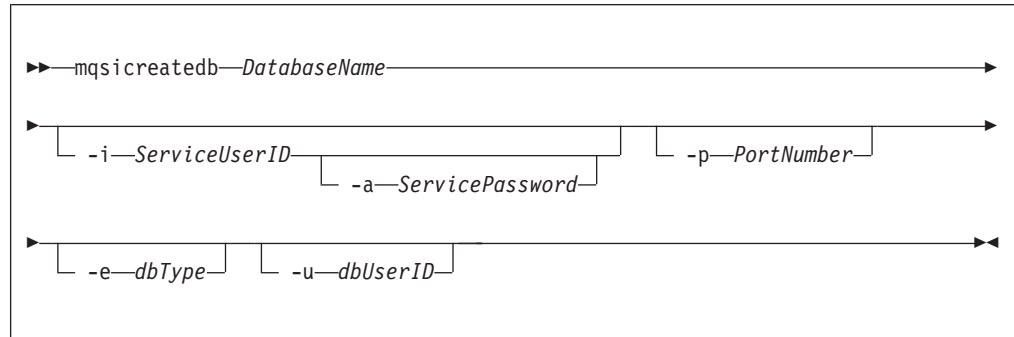
Supported platforms:

- Windows

Purpose:

The `mqsicreatedb` command creates a database and makes it accessible to the broker. The command: creates the database, creates an ODBC data source name, and if necessary, depending on the database type, creates and starts a Windows Service. The command creates at most a single instance of the Windows Service for each installation of a major product version. This command only supports the installed DB2 and Derby database engines.

Syntax:



Parameters:

DatabaseName

(Required) The name of the database you want to create. This must be the first parameter, and is case sensitive. Restrictions might be placed on the permissible length of the database name by the database engine. For restrictions on the character set that can be used, see “Characters allowed in commands” on page 240.

-i ServiceUserID

(Optional, Derby only) The user ID under which the DatabaseInstanceMgr service runs.

This can be specified in any valid username syntax:

- domain\username
- \\server\username
- .\username
- username

If you use the unqualified form for this user ID (username), the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

The ServiceUserID specified must be a member of the local group mqbrkrs. The ID can be a direct or indirect member of the group. The ServiceUserID must also be authorized to access the home directory (where WebSphere Event Broker is installed).

This parameter is ignored if the database engine specified or defaulted for the command is DB2. A ServiceUserID is required for Derby, but only for the first invocation of this command. Subsequent invocations are associated with the existing Windows DatabaseInstanceMgr service that runs under the ServiceUserID specified on the earlier command

The security requirements for the ServiceUserID are detailed in “Security requirements for Windows platforms” on page 425.

- a *ServicePassword*
(Optional, Derby only) The password for the ServiceUserID. Specify this only if you specify ServiceUserID.
- p *PortNumber*
(Optional) The TCP/IP port number that this component will use on the local machine. If not specified, the default value 1527 is used.
- e *dbType*
(Optional) The database engine to be used to create and run the database. Currently supported values are DB2 and Derby. If you do not specify this option, and only one database engine is available, that engine is used. If both are available, the default engine is DB2.
- u *dbUserID*
(Optional, DB2 only) An additional user name that requires access to the database that is created by this command.

Authorization:

The user ID used to invoke this command must have Administrator authority on the local system and be part of the mqbrkrs group.

Responses:

This command returns the following responses:

- BIP9801 No supported database product found
- BIP9802 A database of name xxxx already exists
- BIP9803 The requested database engine, xxxx, could not be found
- BIP9805 A Cloudscape Network Server already running on port number
- BIP9809 Creating database, this may take a while
- BIP9811 The IBM MQSeries Brokers DatabaseInstanceMgr service already exists
- BIP9812 The IBM Cloudscape Network Server failed to start
- BIP9813 External process time out
- BIP9815 The supplied database name xxxx is too many characters in length
- BIP9816 Multiple database engines are installed. Defaulting to the DB2 database engine
- BIP9817 The DB2 database engine was used to create the xxxx database
- BIP9818 The IBM Cloudscape/Apache Derby database engine was used to create xxxx database

Examples:

The following example sets up a database with the name brokerdb on port 1600:
`mqsicreatedb brokerdb -p 1600`

The following example sets up a Derby database with the name derbydb, using port number 1527:

`mqsicreatedb derbydb -i wbrkuid -a wbrkpw -e Derby -p 1527`

mqsicreateexecutiongroup command

Supported platforms:

- Windows

- Linux and UNIX systems
- z/OS. You can also use BIPCREG; see “Contents of the Configuration Manager PDSE” on page 380

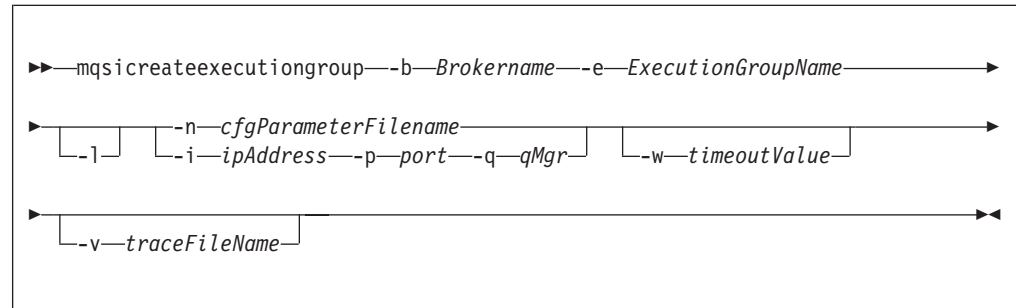
Purpose:

Use the **mqsicreateexecutiongroup** command to add a new execution group to a broker.

You must start the Configuration Manager, using **mqsistart** on Windows platforms, Linux, and UNIX systems, or **startcomponent** on z/OS, (see “mqsistart command” on page 357) before you can issue this command.

The broker must be defined in the Configuration Manager before this command can be used.

Syntax:



Parameters:

- b *BrokerName*
(Required) The name of the broker on which to create the execution group.
- e *ExecutionGroupName*
(Required) The name of the new execution group.
- l (Optional) Create a 64 bit execution group.
- n *cfgParameterFileName*
(Optional) The name of a .configmgr file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the .configmgr format saved by the workbench. For example:

```

<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
  
```

If you are using this file on z/OS you must remove the statement encoding="UTF-8" from the first line, to leave the statement as:

```

<?xml version="1.0"?>
  
```

and remove the value for the host attribute, to leave the statement as:

```

<configmgr host="" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
  
```

Note: If you do not supply this parameter, you must supply the **-i**, **-p**, and **-q** parameters.

-i *ipAddress*

(Optional) The host name or IP address of the Configuration Manager.

If you are using this file on z/OS and want to connect to the local host you must set the value to "".

-p *Port*

(Optional) The port number of the Configuration Manager.

-q *qMgr*

(Optional) The name of the WebSphere MQ queue manager that the Configuration Manager is using.

If you do not supply the **-i**, **-p**, and **-q** parameters, you must specify the **-connection** parameter.

-w *timeoutValue*

(Optional) The time in seconds to wait before the execution group is created; the default value is 60.

-v *TraceFileName*

(Optional) Sends the verbose internal trace to the specified file.

Authorization:

You need to be a member of the 'mqm' group and the command only succeeds if the user Id running the command has the correct authority defined in the Configuration Manager's access control list.

In order to create an execution group, full control authority is required over the broker object; see "ACL permissions" on page 423 for a list of permissions that can be defined in the Configuration Manager.

Responses:

This command returns the following responses:

- 0 (Success) States that the request completed successfully and the execution group has been created successfully in the Configuration Manager's repository. The next time the broker is deployed, the new execution group list is initialized on the broker.
- 2 (Failure) States that the execution group could not be created for any reason.
- 98 States that the Configuration Manager cannot be reached.
- 99 States that the supplied arguments to the utility are not valid.

Examples:

On the domain controlled by the Configuration Manager whose queue manager is called QMGR and is listening on fred.abc.com:1414, create an execution group called 'EG1' on broker 'BROKER'.

```
mqsicreateexecutiongroup -i fred.abc.com -p 1414 -q QMGR -b BROKER -e EG1
```

On the domain specified by the file domain1.configmgr, create an execution group called 'EG2' on broker 'BROKER'.

```
mqsicreateexecutiongroup -n domain1.configmgr -b BROKER -e EG2
```

On the domain specified by the file domain2.configmgr, create an execution group 'EG3' on broker 'FRED'. Wait five minutes for the Configuration Manager to respond and send output to trace.txt.

```
mqsicreateexecutiongroup -n domain2.configmgr -b FRED -e EG3 -w 300 -v trace.txt
```

mqsicreateusernameeserver command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPCRUN; see "Contents of the User Name Server PDSE" on page 379

Purpose:

On Windows platforms, Linux, and UNIX systems, this command:

- Creates a WebSphere MQ queue manager, if one does not already exist.

Note:

1. (Not z/OS) If a WebSphere MQ queue manager is created as a result of using the **mqsicreateusernameeserver** command, the default DLQ provided by WebSphere MQ (SYSTEM.DEAD.LETTER.QUEUE) is automatically enabled. The security settings are the same as those of other broker-specific WebSphere MQ queues.

If you choose to create the queue manager separately, set up a dead letter queue (DLQ). The DLQ is referenced by WebSphere Event Broker when errors occur processing messages in message flows.

If a message in either a user-defined message flow or in the publish/subscribe model cannot be processed, it is routed to this DLQ as a last resort. If you would prefer the message to be backed out onto the input queue, effectively halting the message flow until the problem is resolved, disable the DLQ.

The **mqsdeleteusernameeserver** command does not delete this queue (unless the queue manager is deleted).

- 2.

If you are using a WebSphere MQ queue manager that has been created independently of the **mqsicreateusernameeserver** command, you can define clusters. This simplifies your configuration.

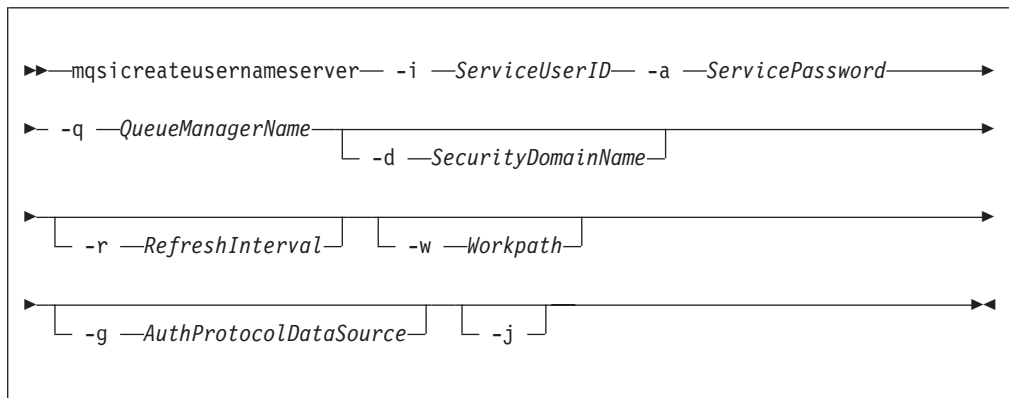
- (Not z/OS) Starts the WebSphere MQ queue manager, if this is not already running.

If the queue manager is created by this command, it is not started as a Windows service; it stops if you log off. To avoid this happening, either remain logged on, or change the start up status of the queue manager service. (If you lock your workstation, the WebSphere MQ queue manager does not stop.)

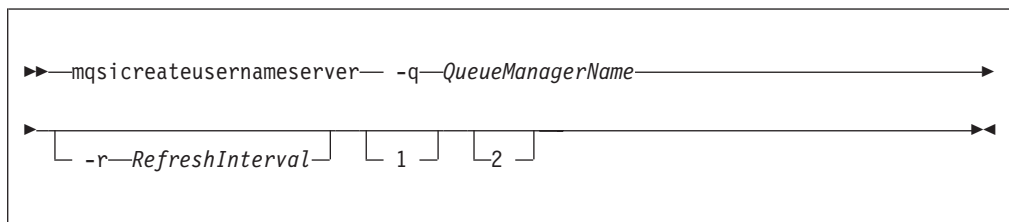
- Creates the User Name Server-specific WebSphere MQ queues, if these do not already exist.
- On Windows, installs a service under which the User Name Server runs.
- Creates a record for the component in the broker registry.

Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS console command:



Parameters:

-i *ServiceUserID*

(Required - Windows platforms, Linux, and UNIX systems) The user ID under which the broker runs.

This can be specified in any valid username syntax. On Windows platforms, these are:

- domain\username
- \\server\username
- .\username
- username

On Linux and UNIX systems, only the last format, username, is valid.

If you use the unqualified form for this user ID (username) on Windows platforms, the operating system searches for the user ID throughout its domain, starting with the local system. This search might take some time to complete.

The *ServiceUserID* specified must be a member of the local group **mqbrkrs**. On Windows platforms, it can be a direct or indirect member of the group. The *ServiceUserID* must also be authorized to access the home directory (where WebSphere Event Broker has been installed).

The security requirements for the *ServiceUserID* are detailed in “Security requirements for Windows platforms” on page 425 for Windows platforms and in “Security requirements for Linux and UNIX platforms” on page 424 for Linux and UNIX systems.

-a *ServicePassword*

(Required - Windows platforms, Linux, and UNIX systems) The password for the ServiceUserID.

For compatibility with existing systems, you can still specify <password>. However, if you do not specify a password with this parameter when you run the command you are prompted to enter a password during its invocation, and to enter the password a second time to verify that you have entered it correctly.

-q *QueueManagerName*

(Required) The name of the queue manager associated with the User Name Server.

On Windows platforms, Linux, and UNIX systems, if the queue manager does not already exist, it is created by this command. It is not created as the default queue manager: if you want it to be the default queue manager on this system, you must create the queue manager before you issue this command.

The queue manager attribute MAXMSGL (maximum length of messages that can be put to queues) is updated to 100 MB. This is done whether or not the queue manager is created by this command.

-d *SecurityDomainName*

(Optional - Windows platforms) The name of the Windows system security domain. If this is not specified, it defaults to the system's local Windows system security domain. For more details about the implementation of security in WebSphere Event Broker, see "Setting up broker domain security" on page 11.

-r *RefreshInterval*

(Optional) The interval, specified in seconds, at which the User Name Server interrogates the security subsystem for changes to user or group attributes. If it is not specified, the User Name Server's default interval of 60 seconds is used.

-w *Workpath*

(Optional - Windows platforms, Linux, and UNIX systems) The directory in which working files for the User Name Server are stored. If not specified, the default value specified when the product was installed is used.

-g *AuthProtocolDataSource*

(Optional - Windows platforms, Linux, and UNIX systems) Use this parameter to specify the name and location of the password file used to source any protocol related information. By default, the file is expected to be found in the home directory. If you store the file in a different location, specify the full path location with file name.

Two samples, password.dat and pwgroup.dat, are provided in the examples/auth directory under the product home directory.

-j (Optional - Windows platforms, Linux, and UNIX systems) Indicates that groups and group memberships are defined in the data source for the authentication protocol, rather than drawn from the operating system.

1 (Optional - z/OS only) The registry pass, which creates only the User Name Server registry.

2 (Optional - z/OS only) The WebSphere MQ pass, which creates only the User Name Server WebSphere MQ queues.

WebSphere MQ queues created:

- SYSTEM.BROKER.SECURITY.QUEUE

- SYSTEM.BROKER.MODEL.QUEUE

Access authority is granted for the WebSphere Event Broker group **mqrbrks** to all these queues.

Responses:

This command returns the following responses:

- BIP8011 Unable to create configuration data
- BIP8012 Unable to connect to system components
- BIP8014 Component cannot be created
- BIP8022 Invalid user ID/password
- BIP8030 Unable to modify user ID privileges
- BIP8048 Unable to start queue manager
- BIP8050 Unable to create queue manager
- BIP8051 Unable to create queue
- BIP8053 Unable to set security for queue manager
- BIP8054 Unable to set security for queue
- BIP8056 Unknown queue manager
- BIP8068 Integer argument required
- BIP8084 Unable to create directory
- BIP8087 Component already exists
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping

Examples:

```
mqsicreateusernameserver -i wbrkuid -a wbrkpw
-q WBRK_QM -r 1000
```

mqsdeleteaclentry command

Supported platforms:

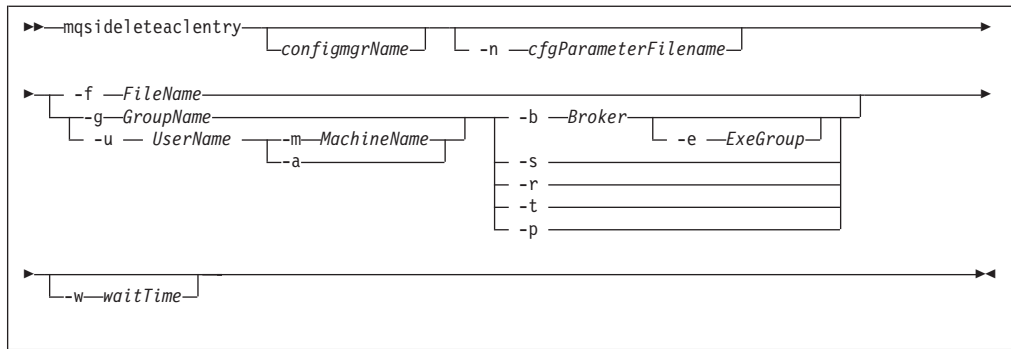
- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPDLACL; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

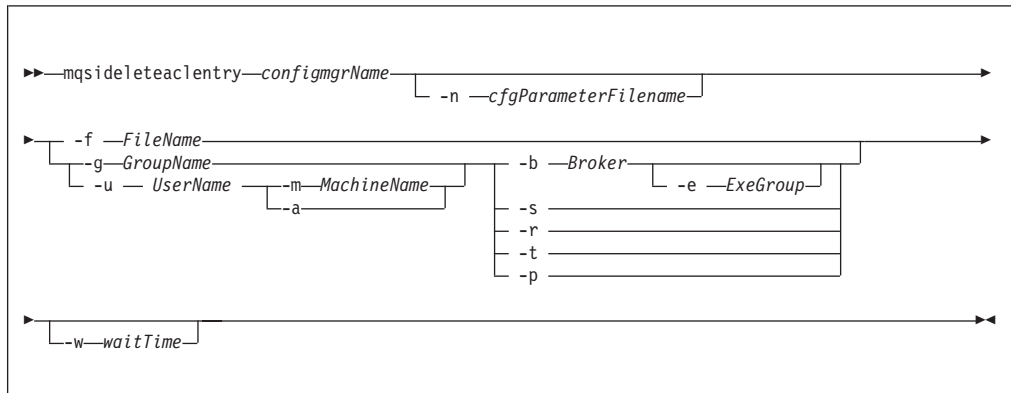
Use the **mqsdeleteaclentry** command to delete the Configuration Manager database table relating to the group or user access control lists that you have defined.

Syntax:

Windows:

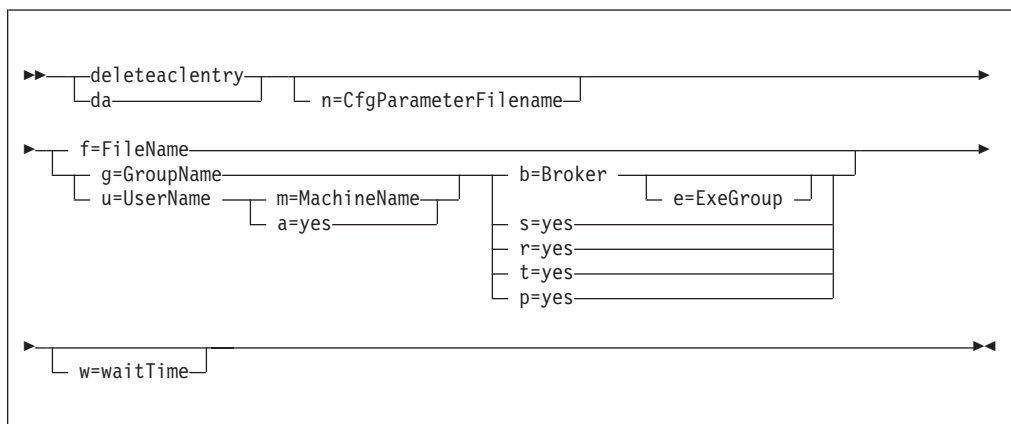


Linux and UNIX systems:



z/OS console command:

Synonym: `da`



Parameters:

You **must** select either `-f` or

- `-g` or `-u`, and
- `-b` and `-e` or `-s` or `-r` or `-t` or `-p`

If you select `-u` you must select either `-m` or `-a`

configmgrName

(Optional - Windows. Required - Linux and UNIX systems.) The name of the Configuration Manager from which the access control lists are to be deleted.

On Linux and UNIX systems this must be the first parameter specified. It is case-sensitive on Linux and UNIX systems. On z/OS this parameter is implicit because you specify the component you want to MODIFY.

The default name on Windows, if this parameter is not specified, is 'ConfigMgr'.

-ncfgParameterFilename

(Optional) The name of a .configmgr file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the .configmgr format saved by the workbench. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
  securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement `encoding="UTF-8"` from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the host attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
  securityExit="test.myExit"/>
```

-f FileName

(Optional) File from which to import the configuration. The output of the **mqsilistaentry** command is the correct format.

-g GroupName

(Optional) Group to which this entry refers. For this reason, the name must adhere to the standard platform convention for group names.

-u UserName

(Optional) User name to which this entry refers, for example, TEST\ANOTHER.

-m MachineName

(Optional) The name of the machine from which a specified user can connect. This option can not be used with **-a**.

-a (Optional) This signifies that the specified user name can be on any machine. This option can not be used with **-m**.

Note: If you select **-u**, you must select either **-a** or **-m**.

-b Broker

(Optional) The object is a broker object, and its name is specified as a parameter.

-e ExeGroup

(Optional) The object is an execution group and its name is specified as a parameter of the form Broker\ExeGroup. You must specify the **b** flag if you specify this flag.

-s (Optional) The object is a subscription object, and its name is specified as a parameter.

- r (Optional) The object refers to the root topic.
- t (Optional) The object refers to the main topology.
- p (Optional) The object refers to the "allresources" resource type. The authority that the principal has for this object applies to all objects, including the mqsicreateaclentry, mqsideleteaclentry, and mqsilistaclentry commands themselves.
- w *waitTime*
(Optional) The time in seconds that the command waits for a response from the Configuration Manager. If you do not supply a value the command waits for 30 seconds.

Authorization:

The user ID used to invoke this command must have full control permissions for the object being changed; see "ACL permissions" on page 423 for more information.

When z/OS commands are run through the console, they effectively run as the Configuration Manager's started-task ID. This means that the commands inherit a Full Control root ACL and you can carry out any operation.

If you submit a console command to the Configuration Manager you can change any ACL for that Configuration Manager.

Examples:

Windows, Linux, and UNIX systems:

```
mqsideleteaclentry CMGR01 -f c:\test\mylist
mqsideleteaclentry CMGR01 -g GROUPA -b MYBROKER
```

z/OS. Note, that on z/OS you must use a comma between each command option. The following example shows the z/OS version of the preceding Windows, Linux, and UNIX systems example:

```
/f CMGR01, da g='GROUPA', b='MYBROKER'
```

mqsideletebroker command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPDLBK; see "Contents of the broker PDSE" on page 378

Purpose:

Use the **mqsideletebroker** command to delete a named broker. The command also deletes the queues on the broker's local queue manager (created when the broker was created), and its data in the broker database. You can also specify that the queue manager is to be deleted.

Even though this command deletes all the data related to this broker from the broker database tables, it does not check if the tables are empty, nor does it delete the tables.

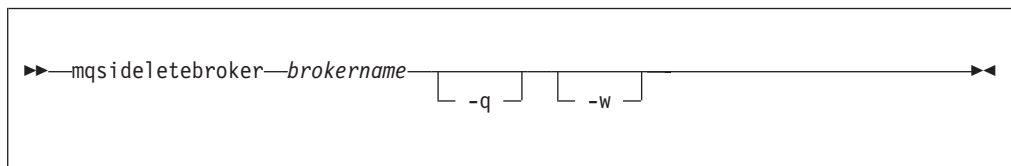
This command:

- On Windows platforms, stops the service that runs the broker.
- Stops and deletes the WebSphere MQ queue manager for the broker, if requested.
- Removes the broker's data from the database.
- Removes the record for the component in the broker registry.

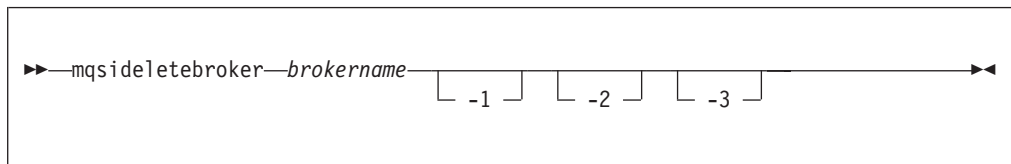
If you delete a broker that has WebSphere MQ publish/subscribe broker neighbors, also invoke the command **clrmqbrk** at each of these neighbors, specifying the WebSphere Event Broker broker that you are deleting with this command.

Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS:



Parameters:

brokername

(Required) The name of the broker that you want to delete. This must be the first parameter.

-q (Optional - Windows platforms, Linux, and UNIX systems) Specifies that the broker's queue manager is deleted. (If this option is not specified, only the WebSphere Event Broker queues and broker's data are deleted.)

If the queue manager hosts another component (the Configuration Manager, or the User Name Server, or both in addition to this broker) that still exists, this command fails.

-w (Optional - Windows platforms, Linux, and UNIX systems) Deletes all files related to this broker from the workpath.

-1 (Optional - z/OS only) Deletes only the broker registry.

-2 (Optional - z/OS only) Deletes only the broker WebSphere MQ queues.

-3 (Optional - z/OS only) Deletes only the broker DB2 tables and indexes.

Responses:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8017 Component cannot be deleted
- BIP8018 Component running

- BIP8040 Unable to connect to database
- BIP8048 Unable to start queue manager
- BIP8049 Unable to stop queue manager
- BIP8052 Unable to delete queue
- BIP8073 Invalid broker name
- BIP8082 Unable to delete queue manager
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping
- BIP8095 Queue manager reserved

Examples:

```
mqsdeletebroker WBRK_BROKER -q
```

|
|
|
|

To delete the broker registry on z/OS for the broker CSQ1BRK, use the following command:

```
mqsdeletebroker CSQ1BRK -l
```

mqsdeleteconfigmgr command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPDLCM; see “Contents of the Configuration Manager PDSE” on page 380

|
|

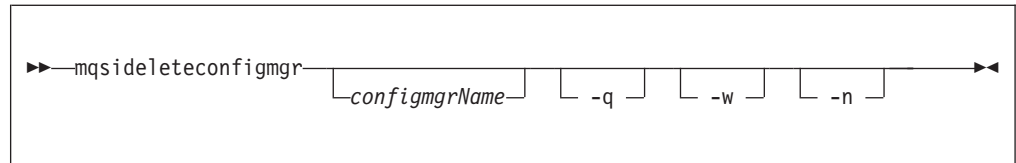
Purpose:

This command:

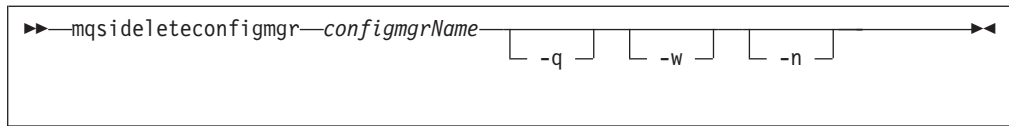
- On the Windows platform, stops the service that runs the Configuration Manager.
- Stops and deletes the WebSphere MQ queue manager for the Configuration Manager, if requested.
- Removes the tables from the configuration repository, if requested.
- Removes the record for the component in the broker registry.

Syntax:

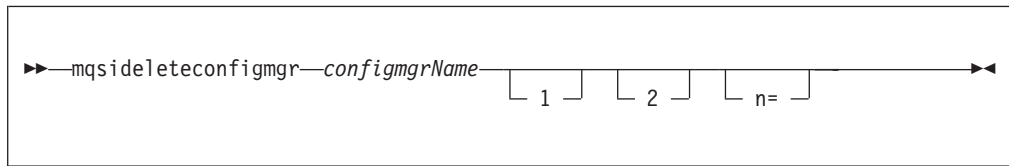
Windows:



Linux and UNIX systems:



z/OS:



Parameters:

configmgrName

(Optional - Windows. Required - Linux, UNIX systems, and z/OS) The name of the Configuration Manager that you want to delete.

On Linux, UNIX systems and z/OS, this must be the first parameter specified. It is case-sensitive on Linux, UNIX systems and z/OS.

The default name on Windows, if this parameter is not specified, is 'ConfigMgr'.

-q (Optional - Windows platforms, Linux, and UNIX systems) Deletes the Configuration Manager's queue manager. (If this option is not specified, only the WebSphere Event Broker queues are deleted.)

If the queue manager hosts another component (a broker, or the User Name Server, or both) that still exists, this command fails.

-w (Optional - Windows platforms, Linux, and UNIX systems) Deletes all files related to the Configuration Manager from the workpath.

-n (Optional) Deletes the configuration repository.

Be very careful using this option. The configuration repository contains the configuration data for the whole broker domain, not just data internal to the Configuration Manager. Deleting this repository destroys all information pertinent to the broker domain, and requires you to recreate every resource within it to recover the broker domain.

If the configuration repository is not deleted as part of deleting the Configuration Manager, and the Configuration Manager is later recreated with the same name, it will continue to use the existing configuration repository.

If you do not specify **-n** to delete the configuration repository data, you can delete it manually later by locating the directory in which the configuration repository is stored and deleting the entire directory. This should be done with extreme caution as all domain information for the Configuration Manager is deleted. To delete the configuration repository manually:

1. Locate the Configuration Manager's working directory. The default location is:
 - For Windows, C:\Documents and Settings\All Users\Application Data\IBM\MQSI
 - For UNIX, /var/mqsi
 - For z/OS, ++COMPONENTDDIRECTORY++

2. Locate the components directory. Delete the directory with the same name as the Configuration Manager.
- 1 (Optional - z/OS only) The registry pass that deletes only the Configuration Manager registry.
- 2 (Optional - z/OS only) The WebSphere MQ pass that deletes only the Configuration Manager WebSphere MQ queues.

Note: This can be performed only if the Configuration Manager registry exists.

Responses:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8017 Component cannot be deleted
- BIP8018 Component running
- BIP8038 Unsupported command option
- BIP8048 Unable to start queue manager
- BIP8049 Unable to stop queue manager
- BIP8052 Unable to delete queue
- BIP8055 Unable to load Java class
- BIP8074 Unable to create JVM
- BIP8075 Java exception
- BIP8076 Unable to set current directory
- BIP8077 Error initializing configuration data
- BIP8078 Error initializing configuration data
- BIP8082 Unable to delete queue manager
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping
- BIP8095 Queue manager reserved
- BIP8097 Unable to create Java object

Examples:

```
mqsdeleteconfigmgr CMGR01 -q
```

mqsdeletedb command

Supported platforms:

- Windows

Purpose:

The **mqsdeletedb** removes a database that has been created by **mqscreatedb**. This includes deleting the database and removing the ODBC data source name. If this is the last database managed by DatabaseInstanceMgr, the Derby Network Server and DatabaseInstanceMgr service are also stopped and removed.

Syntax:



Parameters:

DatabaseName

This must be the only parameter. Specify the name of the database that you want to delete. **Warning:** all the data stored in this database is permanently deleted.

-d DeleteAllDatabases

This must be the only parameter. Specify this option to delete all the databases that have been created by mqsicreatedb. **Warning:** all the data stored in ALL databases is permanently deleted.

Authorization:

The user ID used to invoke this command must have Administrator authority on the local system and be part of the mqbrkrs group.

Responses:

This command returns the following responses:

- BIP9804 No database of name xxx exists, no action taken
- BIP9807 The IBM Derby Network Server on Port number xxxx, has been shutdown
- BIP9810 The IBM MQSeries Brokers DatabaseInstanceMgr service could not be found
- BIP9813 External process time out

Examples:

The following example deletes the database brokerdb:

```
mqsideletedb brokerdb
```

mqsideleteexecutiongroup command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPDLEG; see "Contents of the Configuration Manager PDSE" on page 380

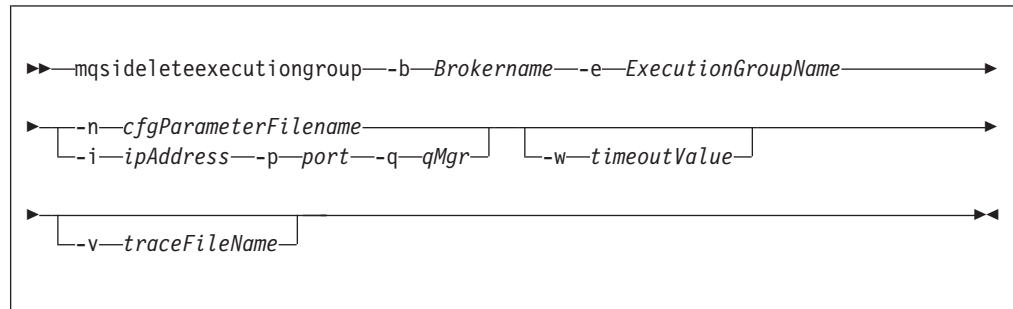
Purpose:

Use the **mqsideleteexecutiongroup** command to delete an execution group from a broker.

You must start the Configuration Manager, using **mqsisstart** on Windows platforms, Linux, and UNIX systems, or **startcomponent** on z/OS, (see "mqsisstart command" on page 357) before you can issue this command.

If you are deleting an execution group to which a deployment has previously been made, you must also start the broker before issuing this command.

Syntax:



Parameters:

- b** *BrokerName*
(Required) The name of the broker on which the execution group resides.
- e** *ExecutionGroupName*
(Required) The name of the execution group to delete.

- n** *cfgParameterFileName*
(Optional) The name of a .configmgr file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the .configmgr format saved by the Eclipse GUI. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement encoding="UTF-8" from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the host attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

Note: If you do not supply this parameter, you must supply the **-i**, **-p**, and **-q** parameters.

- i** *ipAddress*
(Optional) The host name or IP address of the Configuration Manager.

If you are using this file on z/OS and want to connect to the local host you must set the value to "".

- p** *Port*
(Optional) The port number of the Configuration Manager.

- q** *qMgr*
(Optional) The name of the WebSphere MQ queue manager that the Configuration Manager is using.

If you do not supply the **-i**, **-p**, and **-q** parameters, you must specify the **-n** parameter.

-w *timeoutValue*

(Optional) The time in seconds to wait before the execution group is deleted; the default value is 60.

-v *TraceFileName*

(Optional) Sends the verbose internal trace to the specified file.

Authorization:

You need to be a member of the 'mqm' group and the command only succeeds if the user Id running the command has the correct authority defined in the Configuration Manager's access control list.

In order to delete an execution group, full control authority is required over the broker object; see "ACL permissions" on page 423 for a list of permissions that can be defined in the Configuration Manager.

Responses:

This command returns the following responses:

- 0 (Success) States that the request completed successfully and the execution group has been deleted successfully. If the command was to delete an execution group to which a deployment has previously been made, this return code means that the broker has stopped and freed all resources associated with that execution group, for example, message flows.
- 2 (Failure) States that the execution group could not be deleted for any reason.
- 98 States that the Configuration Manager cannot be reached.
- 99 States that the supplied arguments to the utility are not valid.

Examples:

On the domain controlled by the Configuration Manager whose queue manager is called QMGR and is listening on fred.abc.com:1414, delete an execution group called 'EG1' on broker 'BROKER'.

```
mqsideleteexecutiongroup -i fred.abc.com -p 1414 -q QMGR -b BROKER -e EG1
```

On the domain specified by the file domain1.configmgr, delete an execution group called 'EG2' on broker 'BROKER'.

```
mqsideleteexecutiongroup -n domain1.configmgr -b BROKER -e EG2
```

On the domain specified by the file domain2.configmgr, delete an execution group 'EG3' on broker 'FRED'. Wait five minutes for the Configuration Manager to tidy up any resources and send output to trace.txt.

```
mqsideleteexecutiongroup -n domain2.configmgr -b FRED -e EG3 -w 300 -v trace.txt
```

mqsideleteusername server command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPDLUN; see "Contents of the User Name Server PDSE" on page 379

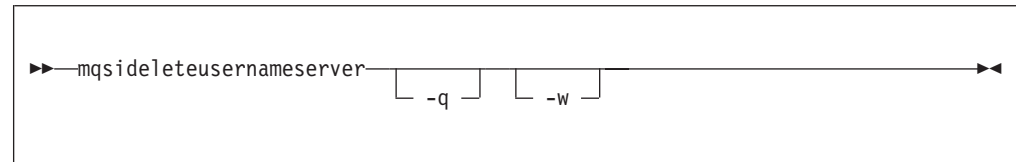
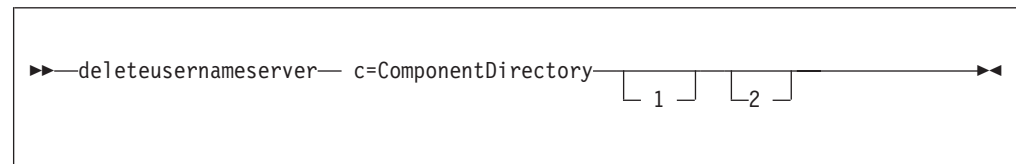
Purpose:

This command:

- Stops the service that runs the User Name Server.
- Stops and deletes the WebSphere MQ queue manager for the User Name Server, if requested.
- Removes the record for the component in the broker registry.

Syntax:

Windows platforms, Linux and UNIX systems:

**z/OS:****Parameters:**

-q (Optional - Windows platforms, Linux, and UNIX systems) Deletes the User Name Server's queue manager when the User Name Server has been deleted. (If this option is not specified, only the WebSphere Event Broker queues are deleted.)

If the queue manager hosts another component (a broker, or the Configuration Manager, or both) that still exists, this command fails.

-w (Optional - Windows platforms, Linux, and UNIX systems) Deletes all files related to the User Name Server from the workpath.

-c *ComponentDirectory*
(Required - z/OS) The name of the component directory. For example /var/wmqi/MQP1UNS

-1 (Optional - z/OS only) Deletes only the User Name Server registry.

-2 (Optional - z/OS only) Deletes only the User Name Server WebSphere MQ queues.

Responses:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8017 Component cannot be deleted
- BIP8018 Component running
- BIP8048 Unable to start queue manager
- BIP8049 Unable to stop queue manager
- BIP8052 Unable to delete queue

- BIP8082 Unable to delete queue manager
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping
- BIP8095 Queue manager reserved

Examples:

```
mqsdeleteusernameserver
```

mqsdeploy command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

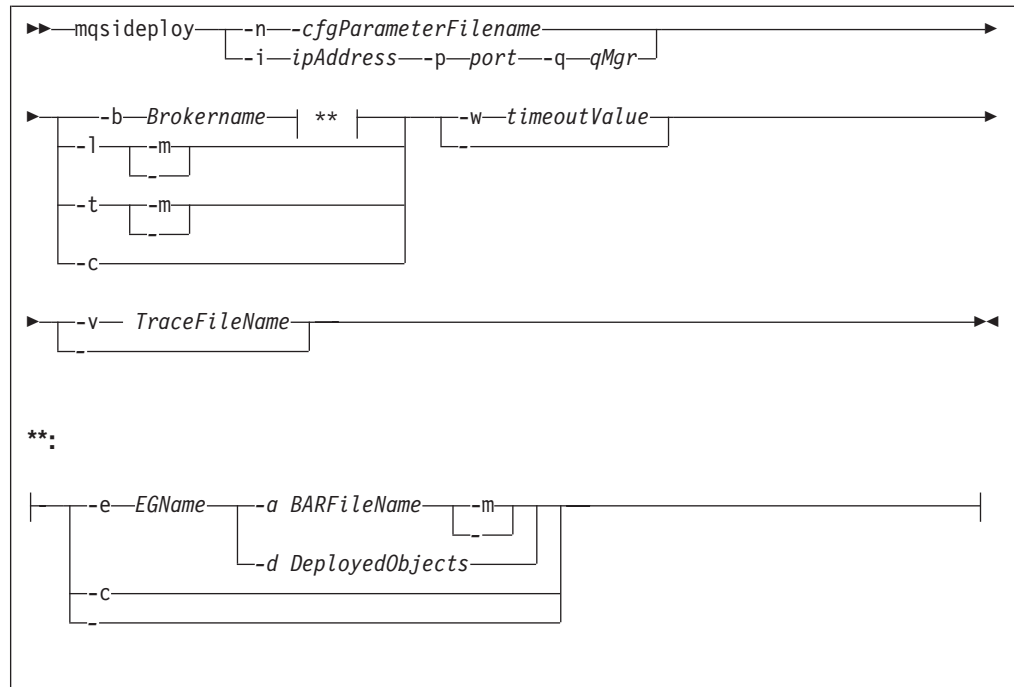
Use the **mqsdeploy** command to make a deployment request to the Configuration Manager. This allows you to make the various flavors of deployment requests from a batch command script, without the need for manual interaction.

The default situation is a delta or incremental deployment. Select **-m** to override the default operation.

mqsdeploy does not require a Configuration Manager name parameter because all of the required connection details can be obtained from the **-n**, **-q**, **-i**, and **-p** parameters.

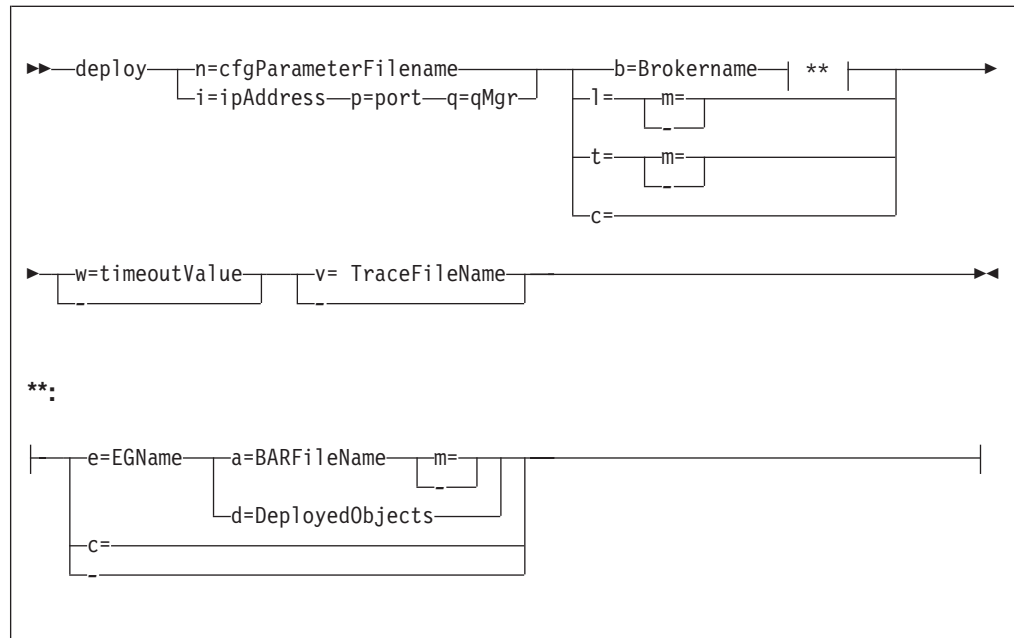
Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS console command:

Synonym: dp



Parameters:

-n *cfgParameterFileName*

(Optional) The name of a .configmgr file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the .configmgr format saved by the Eclipse GUI. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement `encoding="UTF-8"` from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the host attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

Note: If you do not supply this parameter, you must supply the **-i**, **-p**, and **-q** parameters.

-i *ipAddress*

(Optional) The host name or IP address of the Configuration Manager.

If you are using this file on z/OS and want to connect to the local host you must set the value to "".

-p *Port*

(Optional) The port number of the Configuration Manager.

-q *qMgr*

(Optional) The name of the WebSphere MQ queue manager that the Configuration Manager is using.

If you do not supply the **-i**, **-p**, and **-q** parameters, you must specify the **-n** parameter.

-b *Brokername*

(Required) The name of the broker to which to deploy. If either of the **-t** or **-l** flags are specified, the **-b** option is ignored. This is because, when deploying topics or topology, all brokers in the domain are affected. Without the **-e** and **-a** flags, a broker configuration deploy is initiated.

With the **-c** option deployment is cancelled to the specific broker.

-e *EGName*

(Optional) The name of the execution group to which to deploy. The **-b** and **-a** options must also be specified with this option.

-a *BARFileName*

(Optional) The name of the BAR (Broker Archive) file that is to be used for a message flow or message set deploy. The **-b** and **-e** options must also be specified with this option.

On z/OS the BAR file must be in the file system. The BAR file can be anywhere as long as the user ID of the person or Configuration Manager running the command can access the file and read it.

-t (Optional) Deploy all the topics configuration information. Information is deployed to all brokers in the domain.

-l (Optional) This flag specifies that the Topology configuration should be deployed. Information is deployed to all brokers in the domain if the **-m** flag is also set, otherwise the information is deployed only to brokers with a changed topology configuration.

-c (Optional) Tells the Configuration Manager to stop, waiting for responses to previously submitted deployment requests. If used with the **-b** option, the Configuration Manager stops, waiting for outstanding deployment responses

from the specified broker; without the **-b** option, the Configuration Manager stops, waiting for responses to all outstanding deployment requests in the domain.

The **-c** option must be specified with caution. Only use it if there is no possibility that the affected brokers will respond to the deployment request; if a broker subsequently processes a deployment request that had been cancelled, the Configuration Manager ignores the response, and therefore become out of synchronization with the broker.

-w *timeoutValue*

(Optional) The time in seconds that the utility waits for the broker to reply before returning control to the command line. The **mqsidedeploy** command polls the Configuration Manager log records looking for the results of the deploy request that has just been sent. The relevant log records contain information indicating whether the deploy has been successful. The *timeoutValue* is the number of seconds to wait before timing out, in the range 1 - 999 999. If no *timeoutValue* is provided, or a value less than 1 or greater than 999 999 is specified, an error is returned

-d *DeployedObjects*

(Optional) Describes the set of objects to be removed from the execution group. Multiple deployed files can be specified, separated by the ":" character.

Objects of all types can be specified, with the following limitation that, if an ambiguous object name is specified (for example "top", when both "top.dictionary" and "top.cmf" are deployed to the same execution group) the entire command fails with the message BIP1089. In these circumstances, the fully qualified name of the objects to remove must be specified, for example "top.dictionary:top.cmf".

-v *TraceFileName*

(Optional) Sends the internal Configuration Manager Proxy debugging tracing to the specified file.

-m *-complete*

(Optional) Deploy complete information:

- For a **BAR file deploy**, **-m** removes all currently-deployed message flows and message sets from the execution group as part of the deploy. If **-m** is not set, the contents of the BAR file are deployed in addition to what is already deployed on the execution group. In this case, any deployed objects with the same name as an item inside the BAR are replaced by the version inside the BAR.
- For a **topology configuration deploy**, **-m** deploys complete inter-broker configuration information to all brokers. If **-m** is not set, only changed inter-broker configuration is deployed to brokers whose inter-broker configuration has changed.
- For a **broker configuration deploy** this flag is not valid.
- For a **topic tree deploy**, **-m** deploys the entire topic tree to all brokers. If **-m** is not set, only changes to the topic tree are deployed to all brokers.
- For a **remove message flow operation**, the flag is ignored.

Authorization:

In order to successfully deploy, the user ID issuing the command needs to have sufficient authority defined in the Configuration Manager. The permissions required are the same as the permission required to do the equivalent function in

the Message Brokers Toolkit. See “ACL permissions” on page 423 for a list of permissions that can be defined in the Configuration Manager.

Responses:

This command returns the following responses:

- 0 (Success) States that the Configuration Manager issued the deployment request and all relevant brokers responded successfully before the timeout period expired.
- 2 (Failure) States that the Configuration Manager issued the deployment request and at least one broker responded negatively. See the messages output from the utility (or the Configuration Manager’s event log) for more information.
- 3 (Initiated) States that the Configuration Manager has replied, stating that deployment has started, but that no broker responses were received before the timeout occurred.
- 5 (Submitted) States that the deploy message was sent to the Configuration Manager , but that no response was received before the timeout occurred.
- 6 (SuccessSoFar) States that the Configuration Manager issued the deployment request and some, but not all of, the relevant brokers responded successfully before the timeout period expired; no brokers responded negatively.
- 98 States that the Configuration Manager cannot be reached.
- 99 States that the supplied arguments to the utility are not valid.

Examples:

Deploy Publish/Subscribe neighbors using a connection file whose parameters are described in the file `cm1.configmgr`, allow 10 minutes for the broker to reply, and deploy complete inter-broker configuration information:

```
mqsideploy -n cm1.configmgr -m -w 600
```

Deploy Publish/Subscribe neighbors using the **i**, **p**, and **q** parameters to connect to the Configuration Manager, allow 10 minutes for the broker to reply, and deploy complete inter-broker configuration information:

```
mqsideploy -i localhost -p 1414 -q QMNAME -m -w 600
```

Note that you can use the **i**, **p**, and **q** parameters in the following examples instead of the **-n** parameter.

Deploy a topics hierarchy using a connection file whose parameters are described in the file `cm1.configmgr`, allow 10 minutes for the broker to reply, and deploy complete inter-broker configuration information:

```
mqsideploy -n cm1.configmgr -t -m -w 600
```

Deploy a bar file using a connection file whose parameters are described in the file `cm1.configmgr`, allow 10 minutes for the broker to reply, and remove all currently-deployed message flows and message sets from the execution group as part of the deploy:

```
mqsideploy -n cm1.configmgr -b broker1 -e default -a mybar.bar -m -w 600
```

Deploy a broker configuration using a connection file whose parameters are described in the file `cm1.configmgr`, to the specified broker, and allow 15 minutes for the broker to reply:

```
mqsideploy -n cm1.configmgr -b broker1 -w 900
```

Attempt to remove the message flow `top` and the dictionary `bar` from the execution group `default` on broker `b1`, using a connection file whose parameters are described in the file `cm1.configmgr`.

Note that, if there are no other objects called `top` and `bar` deployed to the execution group, the value of the `-d` option can be shortened to `top:bar`.

```
mqsideploy -n cm1.configmgr -b B1 -e default -d top.cmf:bar.dictionary
```

Cancel a deployment using a connection file whose parameters are described in the file `cm1.configmgr`, and allow 15 minutes for the broker to reply. In this example the Configuration Manager stops, waiting for all outstanding deployment requests in the domain. To specify a specific broker on which to cancel a deployment use the `-b` parameter:

```
mqsideploy -n cm1.configmgr -c -w 900
```

mqsideploy command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS through the BIPFMLG utility; see “Contents of the broker PDSE” on page 378

Purpose:

Use the **mqsideploy** command to process the XML log created by **mqsideploylog**. The command retrieves and formats any messages that the XML log contains into a form suitable for the locale of the user invoking the command.

This command interprets an input log file that has been created on any system in a platform-independent code page, `utf-8`. Use it to produce formatted output from input log files transferred from other systems to the system on which you issue the command. If you use this facility, ensure that you use a file transfer program that does not convert the data (for example, by specifying a binary transfer option).

You can direct the output to a file, or to the command shell.

Syntax:

```
mqsideploy -i inputfilename [-o outputfilename]
```

Parameters:

-i *inputfilename*

(Required) The filename of the XML log file that is to be formatted. This file is created by the **mqsideploylog** command; it is encoded in `utf-8`.

-o *outputfilename*

(Optional) The filename of the file into which the formatted log output is to be written. If this is not specified, the formatted log data is written to stdout.

Output written by this command (to file or stdout) is written in a code page suitable for the current user locale.

Authorization:

The user ID used to invoke this command must have read access to the input file, and write access to the output file.

On Linux and UNIX systems, the user ID must be a member of the **mqbrkrs** group.

Responses:

- BIP8041 Unable to open file
- BIP8042 Insufficient memory
- BIP8043 Invalid trace file
- BIP8046 Unable to initialize XML
- BIP8047 Unable to parse data
- BIP8069 Unable to find message
- BIP8079 Unable to locate XML function
- BIP8080 Unable to load resource
- BIP8081 Error processing command

Examples:

```
mqsisformatlog -i trace.xml -o formattrace.log
```

The following extract illustrates the output generated by this command:

Timestamps are formatted in local time, local time is GMT.

```
.  
. .  
2003-02-12 12:57:21.895999 388 UserTrace BIP2638E:  
MQPUT to queue 'SYSTEM.BROKER.EXECUTIONGROUP.REPLY' on queue manager  
'WBRK_QM': MQCC=0, MQRC=0; node ConfigurationMessageFlow.outputNode'.  
The node 'ConfigurationMessageFlow.outputNode' attempted  
to write a message to the specified queue 'SYSTEM.BROKER.EXECUTIONGROUP.REPLY'  
connected to queue manager 'WBRK_QM'.  
The MQCC was 0 and the MQRC was 0.  
No user action required.  
  
2003-02-12 12:57:21.895999 388 UserTrace BIP2622I:  
Message successfully output by output node 'ConfigurationMessageFlow.outputNode'  
to queue 'SYSTEM.BROKER.EXECUTIONGROUP.REPLY' on queue manager  
'WBRK_QM'. The WebSphere  
MQ output node ConfigurationMessageFlow.outputNode'  
successfully wrote an output message to the specified queue  
SYSTEM.BROKER.EXECUTIONGROUP.REPLY connected to queue manager WBRK_QM.  
No user action required.  
. .  
. .  
Threads encountered in this trace: 335 388
```

mqsijoinmqpubsub command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS through the BIPJNMP utility; see “Contents of the broker PDSE” on page 378

Purpose:

Use the **mqsijoinmqpubsub** command to join this WebSphere Event Broker broker to an WebSphere MQ Publish/Subscribe broker network. The command identifies a specific WebSphere MQ Publish/Subscribe broker to be the parent of the WebSphere Event Broker broker.

This is an asynchronous command. Successful completion of this command indicates that the WebSphere Event Broker broker has accepted the request, not that the required action has completed.

Use the **mqsilistmqpubsub** command to monitor the status of the asynchronous actions that result from this command.

Use this command only if you are integrating this WebSphere Event Broker broker with an WebSphere MQ Publish/Subscribe broker network. Before you issue this command, ensure that the WebSphere Event Broker broker is ready to receive and process messages on queue SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS (that is, you must have restarted the broker after creating this queue).

Syntax:

```
►► mqsijoinmqpubsub—brokername— -p —ParentQueueManagerName—◄◄
```

Parameters:

brokername

(Required) The name of the broker that is to be joined to an WebSphere MQ Publish/Subscribe broker.

-p *ParentQueueManagerName*

(Required) The name of the queue manager that hosts the WebSphere MQ Publish/Subscribe broker to which this WebSphere Event Broker broker is to be joined.

Authorization:

The user ID used to invoke this command must have put and inq authority to the queue SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS.

On Linux and UNIX systems, the user ID must be a member of the **mqbrkrs** group.

Responses:

- BIP8013 Component does not exist
- BIP8056 Unknown queue manager
- BIP8057 Queue manager error
- BIP8059 Queue manager not available
- BIP8060 Queue error
- BIP8061 No reply received
- BIP8064 Internal broker error
- BIP8066 Invalid broker name

Examples:

```
mqsjoinmqpubsub WBRK_BROKER -p MQBroker1
```

mqsilist (list resources) command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPLIST; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

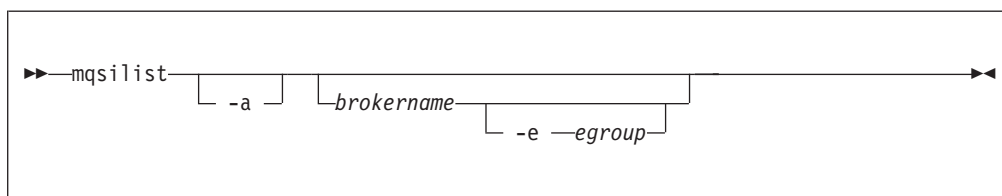
On Windows platforms, Linux, and UNIX systems, use the **mqsilist** command to list all the components installed on the system, all the execution groups defined to a specific broker, or all the message flows contained in a named execution group on a specific broker.

On Windows platforms, Linux, and UNIX systems, the output is directed to stdout.

From a z/OS console, use the **list** command to list all the execution groups defined to a specific broker, or all the message flows contained in a named execution group on a specific broker.

Syntax:

Windows platforms, Linux, and UNIX systems:

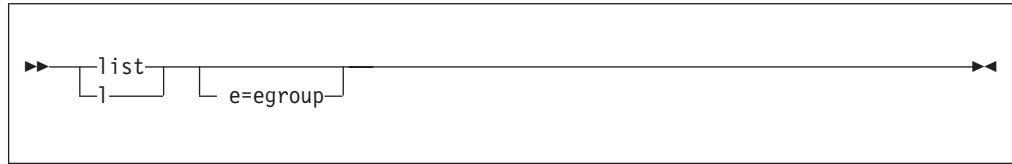


If you do not specify any parameters when you issue this command, a list of components and queue manager names is displayed for each component created on this system, in the form:

```
BIP8099I: Broker: brokername - queuemanagename
BIP8099I: ConfigMgr: configmgrname - queuemanagename
BIP8099I: UserNameServer: UserNameServer - queuemanagename
BIP8071I: Successful command completion
```

z/OS:

Synonym: l



If you do not specify any parameters when you issue this command, a list of the execution groups is displayed.

You issue the **list** command only against a broker task name. For example:

```
F MQP1BRK,list
```

The output is the list of execution groups and process IDs in the form:

```
BIP8130I: Execution Group: <name> -<process ID>  
BIP8071I: Successful command completion
```

If you specify an execution group, for example:

```
F MQP1BRK, list e='exgrp1'
```

the output is a list of message flows in the form:

```
BIP8131I: Messageflow: <MessageFlowName>  
BIP8071I: Successful command completion
```

Parameters:

Windows platforms, Linux, and UNIX systems:

-a (Optional) List all the components installed on the system.

If you use this option on brokers from a previous release of the product, you obtain the following message:

```
BIP8221I: <Component>: <ComponentName> (<Version>) - <Queue Manager>
```

brokername

(Optional) The name of the broker for which you want to list resources. This must be a deployed broker. A list of execution groups configured on this broker and the process ID (pid) of each is displayed.

All platforms:

-e *egroup*

(Optional) Selects an execution group within a broker. Specify the label of the execution group for which you want to list message flows. The command returns a list of message flows assigned to the specified execution group within the broker.

The broker specified must be active for any message flow information to be returned.

Authorization:

On Linux and UNIX systems, the user ID must be a member of the **mqbrkrs** group.

On Windows platforms, if you have specified a broker name and the `-e` flag, the user ID used to invoke this command must have `mqbrkrs` group membership.

Responses:

- BIP8013 Component does not exist
- BIP8020 Unable to access database
- BIP8029 Broker not configured
- BIP8038 Unsupported command option
- BIP8039 Execution group not available
- BIP8040 Unable to connect to database
- BIP8158 Invalid format for command (z/OS only)
- BIP8159 Unknown parameter "... " (z/OS only)

Examples:

Windows platforms, Linux, and UNIX systems:

```
mqsilist WBRK_BROKER -e DefaultEG
mqsilist DatabaseInstanceMgr
```

z/OS

```
F MQP1BRK,list e='exgrp1'
```

mqsilistaclentry command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPLIACL; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

Use the `mqsilistaclentry` command to view or list the currently defined:

- User groups
- Users
- Objects
- Access control lists

If you do not specify any parameters, all the groups, users, and objects are listed.

If you specify *GroupName*, only those access control lists relating to that group are listed.

If you specify *UserName*, only those access control lists relating to that specific user are listed, including any access control lists to which they belong.

If you specify *Broker*, only those groups, users, or access control lists relating to that broker are listed.

The output from this command is a description of the access rights that match the criteria specified in the command line arguments; each line takes the following form:

<principal> - <principaltype> - <accesstype> - <objectname> - <objecttype>

where

- <principal> is the name of the user or group for which a policy has been defined.
- <principaltype> is USER if the principal refers to a user, or GROUP if the principal refers to a group.
- <accesstype> describes the type of authority that has been granted, and can be one of:
 - V View access
 - F Full control
 - D Deploy access
 - E Editor access
- <objectname> applies only to execution groups and brokers, and describes the name of the object that has had a policy defined.
- <objecttype> describes the type of object that has had a policy defined, and can be one of:

Broker

A broker

ConfigManagerProxy

Configuration Manager Proxy

ExecutionGroup

An execution group

PubSubTopology

The topology

Subscription

The list of active subscriptions

TopicRoot

The root topic

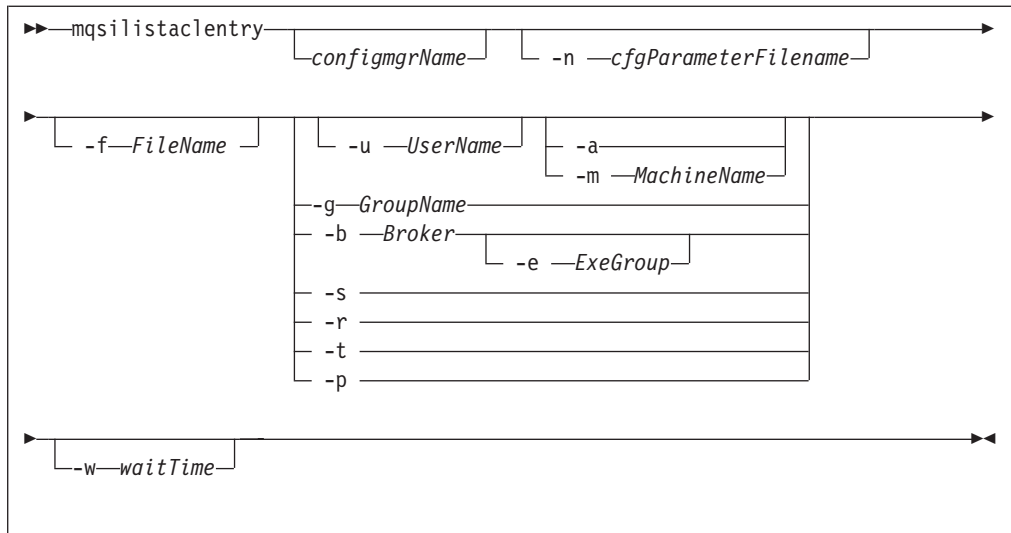
For example:

wrkgrp\ali - USER - F - EXE - BROKER\default

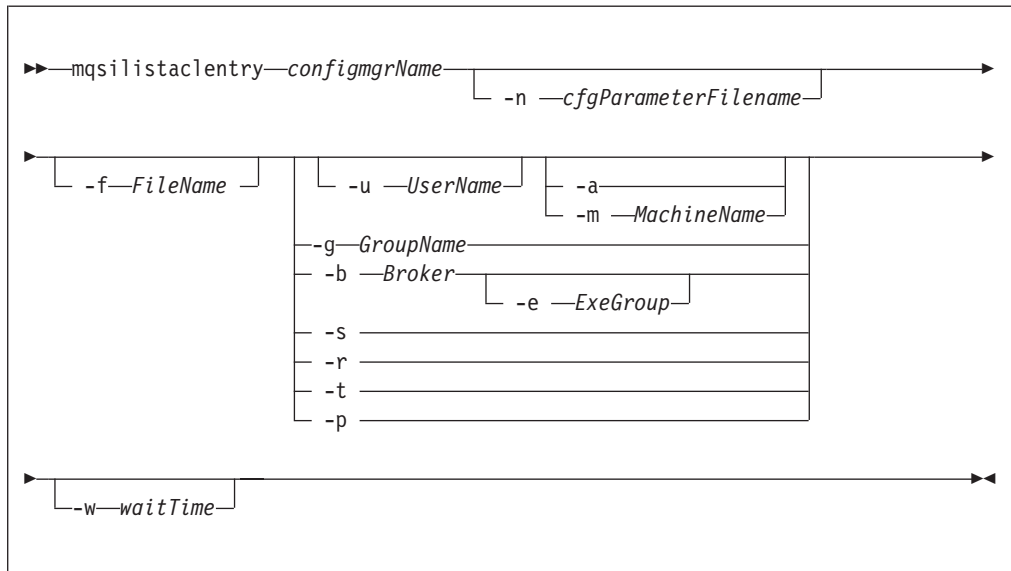
means that user "ali" in domain "wrkgrp" has been granted full control over the execution group default in broker "BROKER".

Syntax:

Windows:

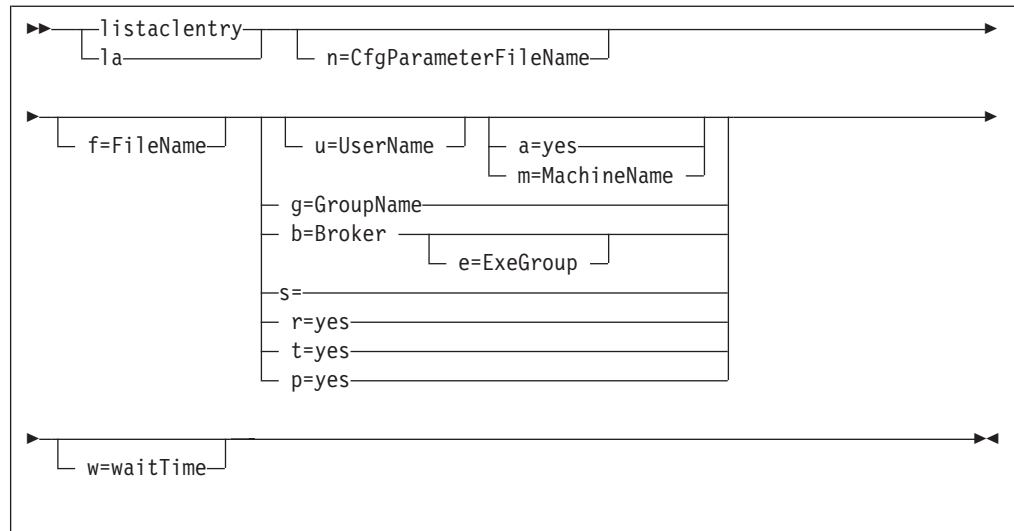


Linux and UNIX systems:



z/OS console command:

Synonym: la



Parameters:

configmgrName

(Optional - Windows. Required - Linux and UNIX systems.) The name of the Configuration Manager for which the access control lists are to be displayed.

On Linux and UNIX systems this must be the first parameter specified. It is case-sensitive on Linux and UNIX systems. On z/OS this parameter is implicit because you specify the component you want to MODIFY.

The default name on Windows, if this parameter is not specified, is 'ConfigMgr'.

-ncfgParameterFilename

(Optional) The name of a .configmgr file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the .configmgr format saved by the Eclipse GUI. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement encoding="UTF-8" from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the host attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

-f FileName

(Optional) Place the results of this command into an XML file.

-u UserName

(Optional) User name to which this entry refers, for example, TEST\ANOTHER.

-a (Optional) Allows a specified user to connect to all machines.

Note: You can select -a or -m.

- m** *MachineName*
(Optional) The name of the machine from which a specified user can connect.
- g** *GroupName*
(Optional) Group to which this entry refers. For this reason, the name must adhere to the standard platform convention for group names.
- b** *Broker*
(Optional) The object is a broker object, and its name is specified as a parameter.
- e** *ExeGroup*
(Optional) The object is an execution group and its name is specified as a parameter of the form 'Broker\ExeGroup'. You must specify the **b** flag if you specify this flag.
- s** *Subscription*
(Optional) The object is a subscription object, and its name is specified as a parameter.
- r** (Optional) The object is referring to the root topic.
- t** (Optional) The object is referring to the main topology.
- p** (Optional) The object refers to the "allresources" resource type. The authority that the principal has for this object applies to all objects, including the `mqsicreateaclentry`, `mqsdeleteaclentry`, and `mqslistaclentry` commands themselves.
- w** *waitTime*
(Optional) The time in seconds that the command waits for a response from the Configuration Manager. If you do not supply a value the command waits for 30 seconds.

Authorization:

The user ID used to invoke this command must have full control permissions for the object being changed; see "ACL permissions" on page 423 for more information.

| When z/OS commands are run through the console, they effectively run as the
| Configuration Manager's started-task ID. This means that the commands inherit a
| Full Control root ACL and you can carry out any operation.

| If you submit a console command to the Configuration Manager you can change
| any ACL for that Configuration Manager.

Examples:

| Windows, Linux, and UNIX systems:
| `mqsilistaclentry CMGR01 -b BROKER01`
| `mqsilistaclentry CMGR01 -e BROKER01\ExeGrp01`
| `mqsilistaclentry CMGR01 -g GROUPA`

| z/OS. Note, that on z/OS you must use a comma between each command option.
| The following example shows the z/OS version of the preceding Windows, Linux,
| and UNIX systems example:

| `/f CMGR01, 1a g='GROUPA'`

mqsilistmqpubsub command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS through the BIPLSMP utility; see “Contents of the broker PDSE” on page 378

Purpose:

Use the **mqsilistmqpubsub** command to display the status of the WebSphere MQ Publish/Subscribe neighbor brokers to the specified WebSphere Event Broker broker.

This command indicates the status of the activity started by a previous join request (see “mqsijoinmqpubsub command” on page 327). The command reports on the status of each neighbor broker, which can be:

Active Broker status is active if the join request has completed successfully.

Inactive

Broker status is inactive if the join has been initiated, but has not completed.

This command also shows the streams that are recognized by both the WebSphere Event Broker broker and its neighbor (on which messages can be published and distributed between the brokers). Stream information is provided only for neighbors with *active* status.

Use this command only if you are integrating with, or migrating from, an WebSphere MQ Publish/Subscribe broker network.

The output generated by this command is directed to stdout.

Syntax:

```
►► mqsilistmqpubsub — brokername —◄◄
```

Parameters:

brokername

(Required) The name of the broker for which you want a list of neighbors.

Authorization:

On Linux and UNIX systems, the user ID must be a member of the **mqbrkrs** group.

On Windows platforms, no authorization is required.

Responses:

- BIP8013 Component does not exist
- BIP8020 Unable to access database

- BIP8029 Broker not configured
- BIP8040 Unable to connect to database
- BIP8064 Internal broker error
- BIP8070 Database exception
- BIP8072 Database exception

Examples:

If there are no WebSphere MQ Publish/Subscribe brokers, and no **mqsijoinmqpubsub** command has been issued, this command returns the following message:

```
BIP8088I: There are no WebSphere MQ Publish/Subscribe neighbors
```

If an **mqsijoinmqpubsub** command has been issued, one of two response messages is displayed:

- For every broker that is an inactive neighbor of WBRK_BROKER (that is, a request has been made, using the **mqsijoinmqpubsub** or **strmqbrk** command, to add the broker to the network, but negotiations for common streams are still in progress), the following message is displayed:

```
BIP8089I: WebSphere MQ Publish/Subscribe neighbor <brokername> is inactive.
```

- For every broker that is an active neighbor of WBRK_BROKER (that is, the two brokers are exchanging publications and subscriptions for each of the common streams), the following message is displayed:

```
BIP8090I: WebSphere MQ Publish/Subscribe neighbor <brokername> is active.
```

Additional messages are displayed for active brokers to indicate the common streams for which publications and subscriptions are exchanged, in the following form:

```
BIP8091I: Common stream streamname
```

For example,

```
mqsilistmqpubsub WBRK_BROKER
```

might return the following responses:

```
BIP8090I: MQSeries Publish/Subscribe neighbor MQPS_BROKER_1 is active.
```

```
BIP8091I: Common stream SYSTEM.BROKER.DEFAULT.STREAM.
```

```
BIP8091I: Common stream STREAM0.
```

```
BIP8090I: MQSeries Publish/Subscribe neighbor MQPS_BROKER_2 is active.
```

```
BIP8091I: Common stream SYSTEM.BROKER.DEFAULT.STREAM.
```

```
BIP8091I: Common stream STREAM150.
```

```
BIP8089I: MQSeries Publish/Subscribe neighbor MQPS_BROKER_3 is inactive.
```

In this example, the WebSphere Event Broker broker has three WebSphere MQ Publish/Subscribe neighbors. Two of these neighbors are active and have been successfully joined to the WebSphere Event Broker broker. The third is inactive and is in the process of being joined.

The list of streams that are common to the WebSphere Event Broker broker and the two active WebSphere MQ Publish/Subscribe brokers are included in the response. For MQPS_BROKER_1, the streams SYSTEM.BROKER.DEFAULT.STREAM and STREAM0 are common. For MQPS_BROKER_2, the streams SYSTEM.BROKER.DEFAULT.STREAM and STREAM150 are common.

If a neighbor is inactive for a long period of time, it is likely that the communication link between the two brokers has been broken. Ensure that the

WebSphere MQ connections between the two brokers (channels and transmission queues) are running, and that the WebSphere Event Broker and WebSphere MQ Publish/Subscribe brokers are both active.

mqsimigratecomponents command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

The **mqsimigratecomponents** command moves a component from one previously installed version (either Version 2.1 or Version 5 only) of the product to another. This command *must* be run from whichever version of the installed product is the later, regardless of whether it is the source version or the target version.

Note:

1. For Version 2.1 of the product, Version 2.1 CSD02 (2.1.0.3) is the earliest release of the product supported. (See Migrating and upgrading for more information.)
2. For Version 5 of the product, Version 5.0.0.4 is the earliest release of the product supported.

You *must* have a Version 6.0 installation of the product with the required component code installed, that is, the broker component is installed if it is needed, and so on.

Before starting migration, stop any debugging sessions in the Control Center. It is not possible to migrate message flows that are being debugged.

You can invoke the command with various options to perform one of the following actions:

- Check on a component, without making any changes, to ensure that the component is suitable for the required migration (-c).
- Move a component to a different version, in full or part (-s and -t).
- Undo a failed migration step (-u).
- Verify that a move has been successful (-v).

The **mqsimigratecomponents** command updates your registry and file system, WebSphere MQ definitions, and database definitions. If the user who is issuing the command does not have the authority to perform all of these steps, the command can be run one part at a time. Different users can run the part for which they are authorized in order to achieve the overall result. This is referred to as *split migration* and is performed using the -1, -2 and -3 parameters.

If you are using the **mqsimigratecomponents** command with a Sybase database, you must modify the database by performing the following actions:

1. Log on to ISQL using a system administrator account.
2. Issue the following series of commands:

```
1> use master
2> go
1> sp_dboption "BROKER1","ddl in tran",TRUE
```

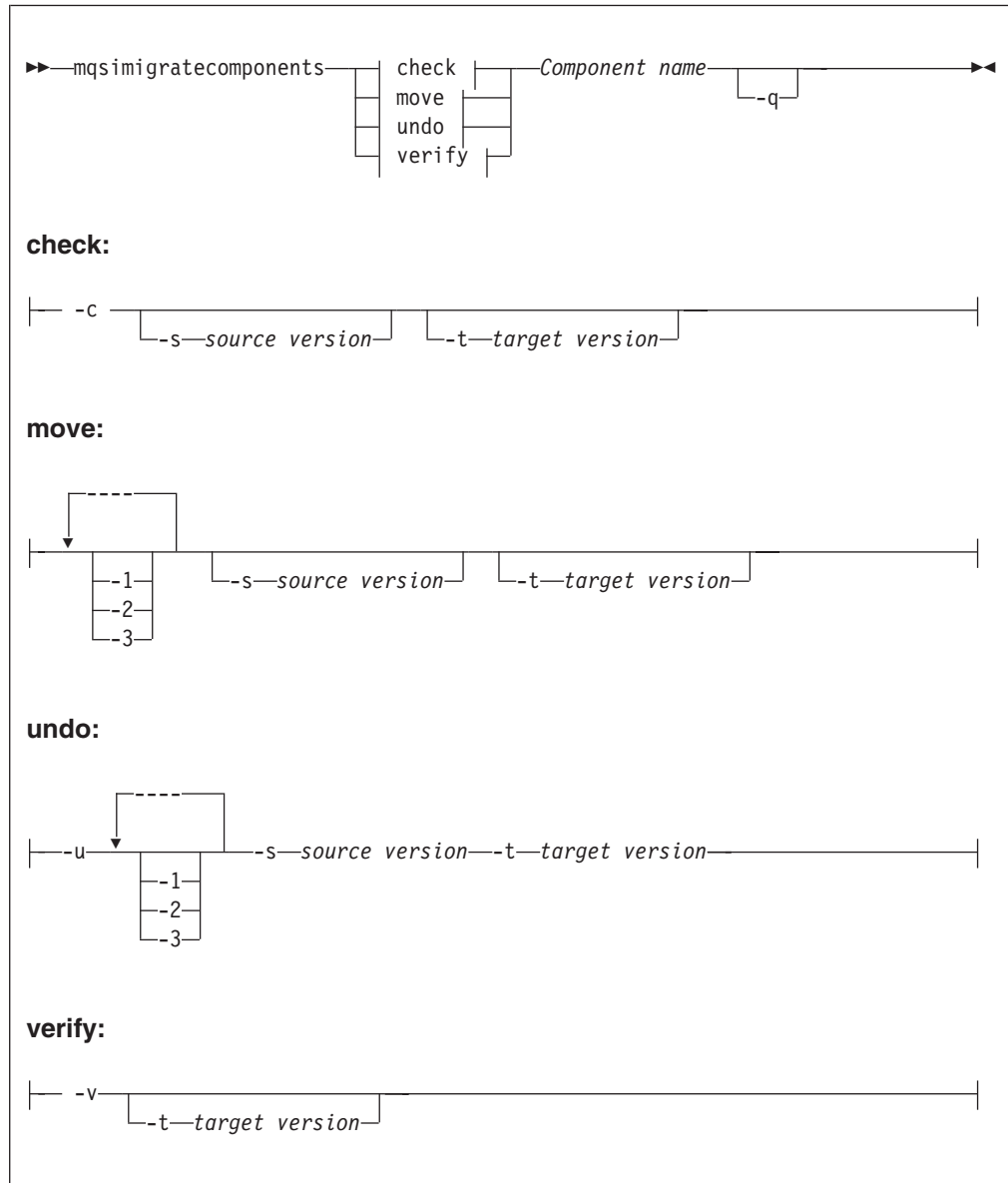
```

2> go
Database option 'ddl in tran' turned ON for database 'BROKER1'.
Run the CHECKPOINT command in the database that was changed.
(return status = 0)
1> use BROKER1
2> go
1> checkpoint
2> go

```

where *BROKER1* is the name of the Sybase broker database.

Syntax:



Parameters:

- c (Optional) Do a pre migration check of a specified component to ensure that:
 - The auto-detected version of the broker matches any version specified on the command line

- There are no 64 bit execution groups, if migrating from Version 6.0 to a previous release
- The database tables to be copied from a previous release do not contain any rows that violate Version 6.0 index requirements.

If a broker that you are migrating shares a database schema with another broker, warning message BIP8678 is issued and the check fails. In this case, all the brokers that share a database schema must be migrated together:

1. Stop all the brokers that are sharing the database schema.
2. Migrate the first broker. This will migrate the database tables for all brokers, as well as the file system and registry, and WebSphere MQ definitions for that broker only; for example:

```
mqsigratecomponents FIRSTBROKER -t 6.0.0.1
```

3. Migrate the file system and registry, and WebSphere MQ parts of each of the other brokers; the database part has already been migrated. Use the **-1** and **-2** parameters to do this, either in one step or two steps:

- In one step:

```
mqsigratecomponents BROKERB -1 -2
```

- In two steps:

```
mqsigratecomponents BROKERB -1
```

```
mqsigratecomponents BROKERB -2
```

The migration check can be run against a running component. This does not impact the component, except for imposing a slight performance penalty. Note that on UNIX systems, the `odbc.ini` file needs to be migrated (that is, a new-format `odbc.ini` file needs to be created with the same set of data sources as the old one) before the check can be run, because the checking command needs to be able to access the broker database.

The check command either succeeds or fails, and prints a message about whether or not the migration should succeed, but no modifications are made during the process.

- v** (Optional) Do a post-migration check of a specified component to ensure that:
 - The correct database tables and queues exist for the specified version.
 - The registry is in the correct format for the specified version.
- q** (Optional) Print fewer status messages during the operation.
- 1** (Optional) Do only registry and file system work.
 - When migrating to Version 6.0, use the **-1** parameter before the **-2** or **-3** parameters.
 - When migrating backwards to a previous version, use the **-2** or **-3** parameters before the **-1** parameter.
- 2** (Optional) Do only WebSphere MQ work.
- 3** (Optional) Do only database work.
- u** (Optional) Undo a failed migration step; you must also specify at least one of **-1**, **-2**, or **-3**. You should only use this option when migration has failed, and also failed to auto-recover (a failure during split migration being one example).
- s** *Source Version*
 (Optional) The previous version of the component.
 - This value is detected automatically if not specified.

- When performing split migration to Version 6.0, the **-s** parameter is mandatory after you run the **mqsigratecomponents** command with the **-1** parameter. This is illustrated in the split migration example.
- See “Purpose” on page 337 for the restrictions to the version numbers of the product that are supported.

-t *Target Version*

(Optional) The destination version of the component.

- This value is assumed to be the current version if not specified.
- When performing split migration from Version 6.0 to a previous version, the **-t** parameter is mandatory. This is illustrated in the split migration example.
- See “Purpose” on page 337 for the restrictions to the version numbers of the product that are supported.

Component Name

(Required) The name of the component to migrate.

Authorization:

When running single-step migration, the user ID used to invoke this command must have the ability to:

- Write to the registry and the file system for the product
- Modify databases associated with the component
- Modify queue definitions

For split migration, the user ID used to invoke this command must always have the ability to read from the registry for the product, and also have specific authorization for each step to succeed:

- **-1** requires the ability to write to the registry and the file system for the product
- **-2** requires the ability to modify queue definitions
- **-3** requires the ability to modify databases associated with the component

Responses:

| This command can produce a large number of possible responses, depending on
 | the results of the various operations. Note that this command differs from other
 | commands in the way it produces messages – they are displayed as needed, rather
 | than being produced in a batch at the end of the program. When migrating
 | database tables, z/OS produces more output than distributed systems.
 |

Examples:

The following example checks for migration of BROKER1 from Version 2.1 to Version 6.0:

```
| mqsigratecomponents -c BROKER1
| BIP8849I: Broker 'BROKER1' (Version 2.1) with Queue Manager 'brkqm1' and Data Source 'brkdb1' specified for migration.
| BIP8791I: Duplicate rows check started.
| BIP8794I: Table BRMINFO has no duplicated rows.
| BIP8794I: Table BRMRTDDEPINFO has no duplicated rows.
| BIP8794I: Table BROKERRESOURCES has no duplicated rows.
| BIP8794I: Table BRMRTDINFO has no duplicated rows.
| BIP8794I: Table BRMWFINFO has no duplicated rows.
| BIP8792I: Duplicate rows check passed.
| BIP8791I: Duplicate rows check started.
| BIP8800W: No invalid topic syntax was detected in table BSUBSCRIPTIONS.
| BIP8800W: No invalid topic syntax was detected in table BPUBLISHERS.
```

```

| BIP8800W: No invalid topic syntax was detected in table BRETAINEDPUBS.
| BIP8797I: Topic syntax check succeeded
| BIP8680I: Pre-migration check succeeded.
| BIP8071I: Successful command completion.

```

The following example does automatic migration of BROKER1 from Version 2.1 to Version 6.0:

```

| mqsigratecomponents BROKER1
| BIP8849I: Broker 'BROKER1' (Version 2.1) with Queue Manager 'BROKER1' and Data Source 'BROKERDB' specified for migration
| BIP8755I: Copied value 'QueueManagerName' into the new location
| BIP8755I: Copied value 'DataSourceName' into the new location
| BIP8755I: Copied value 'DataSourceUserId' into the new location
| BIP8755I: Copied value 'DataSourcePassword' into the new location
| BIP8755I: Copied value 'LilPath' into the new location
| BIP8755I: Copied value 'ConfigurationTimeout' into the new location
| BIP8755I: Copied value 'ConfigurationDelayTimeout' into the new location
| BIP8755I: Copied value 'MigrationNeeded' into the new location
| BIP8755I: Copied value 'MQTrustedQueueManager' into the new location
| BIP8755I: Copied value 'UserNameServerQueueManagerName' into the new location
| BIP8755I: Copied value 'BrokerUUID' into the new location
| BIP8755I: Copied value 'AdminAgentPID' into the new location
| BIP8763I: Deleted value 'QueueManagerName' from the old location
| BIP8763I: Deleted value 'DataSourceName' from the old location
| BIP8763I: Deleted value 'DataSourceUserId' from the old location
| BIP8763I: Deleted value 'DataSourcePassword' from the old location
| BIP8763I: Deleted value 'LilPath' from the old location
| BIP8763I: Deleted value 'ConfigurationTimeout' from the old location
| BIP8763I: Deleted value 'ConfigurationDelayTimeout' from the old location
| BIP8763I: Deleted value 'MigrationNeeded' from the old location
| BIP8763I: Deleted value 'MQTrustedQueueManager' from the old location
| BIP8763I: Deleted value 'UserNameServerQueueManagerName' from the old location
| BIP8763I: Deleted value 'BrokerUUID' from the old location
| BIP8763I: Deleted value 'AdminAgentPID' from the old location
| BIP8768I: Finished registry migration for component 'BROKER1'.
| BIP8654I: Moving filesystem artefacts from '' to 'C:\Documents and Settings\AllUsers\Application Data\IBM\MQSI'
| BIP8670I: Database migration started
| BIP8663I: Creating temporary new tables
| BIP8664I: Migrating from existing tables to temporary new tables
| BIP8665I: Dropping existing tables
| BIP8666I: Creating new tables
| BIP8667I: Copying all rows from temporary new tables to new tables
| BIP8668I: Dropping temporary new tables
| BIP8669I: Database migration successful
| BIP8785I: Starting WebSphere MQ queue migration for component 'BROKER1'.
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.AGGR.REQUEST'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.AGGR.CONTROL'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.AGGR.REPLY'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.AGGR.TIMEOUT'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.AGGR.UNKNOWN'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.TIMEOUT.QUEUE'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.INTERBROKER.MODEL.QUEUE'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.WS.INPUT'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.WS.REPLY'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.WS.ACK'
| The setmqaut command completed successfully.
| BIP8786I: Created WebSphere MQ queue 'SYSTEM.BROKER.IPC.QUEUE'

```

```
| BIP8787I: Cleared WebSphere MQ queue 'SYSTEM.BROKER.ADMIN.QUEUE'  
| BIP8787I: Cleared WebSphere MQ queue 'SYSTEM.BROKER.EXECUTIONGROUP.QUEUE'  
| BIP8787I: Cleared WebSphere MQ queue 'SYSTEM.BROKER.EXECUTIONGROUP.REPLY'  
| BIP8787I: Cleared WebSphere MQ queue 'SYSTEM.BROKER.IPC.QUEUE'  
| BIP8789I: Finished WebSphere MQ queue migration for component 'BROKER1'.  
| BIP8071I: Successful command completion.
```

The following example illustrates a split migration from Version 2.1 to Version 6.0:

```
mqsimigratecomponents BROKER -1  
mqsimigratecomponents BROKER -s 2.1.0.8 -2  
mqsimigratecomponents BROKER -s 2.1.0.8 -3
```

The following example illustrates a split migration from Version 6.0 to Version 2.1:

```
mqsimigratecomponents BROKER -t 2.1.0.8 -2  
mqsimigratecomponents BROKER -t 2.1.0.8 -3  
mqsimigratecomponents BROKER -t 2.1.0.8 -1
```

mqsireadlog command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS through the BIPRELG utility; see “Contents of the broker PDSE” on page 378

Purpose:

Use the `mqsireadlog` command to retrieve the trace log for the specified component. This command is valid for:

User trace

Specify the `-u` option.

Service trace

Specify the `-t` option. You are recommended to use this option only if directed to do so by the action described in a BIPxxxx message, or by your IBM Support Center.

You can specify the output to be directed to file, or to stdout. The trace records returned by this command are in XML format and can be browsed with an XML browser. If you direct output to file, the data is written in code page utf-8. The file is therefore platform-independent, and can be transferred to other systems for browsing or formatting using the `mqsiformatlog` command.

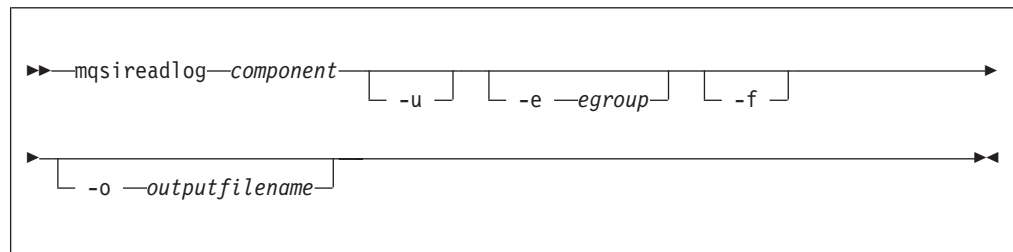
On HP-UX you are recommended to set the size parameter of the `mqsichange` command to be less than 500 MB. Note that the size of the XML generated files is often half as much again as the original trace file, and setting the value of the size parameter to be greater than 500 MB can cause problems.

If you transfer this file to another system, ensure that you use a file transfer program that does not convert the data (for example, by specifying a binary transfer option).

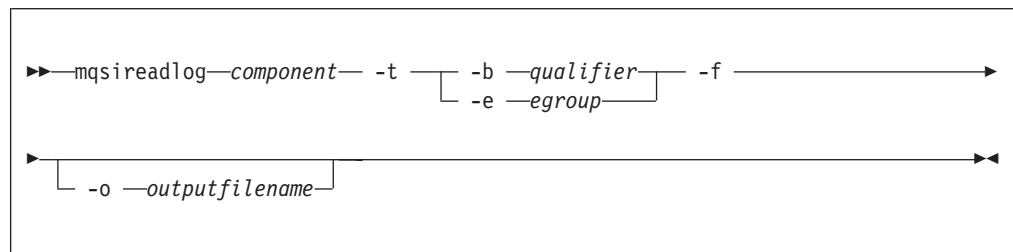
If you specify a broker, or any of its resources (execution group or message flow) you must have deployed them before you can start trace and read the log files.

Syntax:

User trace:



Service trace:



Parameters:

component

(Required) The name of the component for which the log is to be read. This can be either a broker name or Configuration Manager name, or the fixed values , UserNameServer, workbench, or utility (all are case sensitive on Linux and UNIX systems and on z/OS).

-u (Optional) Read the log contents from the user trace log. This is valid **only** if you select the broker component.

-e egroup

(Optional) The label of the execution group for which log information is to be read.

-o outputfilename

(Optional) The name of the file into which to write the log data. If you specify a full pathname, the file is created in the directory specified. If you specify just the filename, the file is created in the current working directory. The contents of the file are written in code page utf-8, which is platform-independent and preserves data such as DBCS characters.

You must specify a file name if you want to format the log using the mqsiformatlog command. If you do not specify a filename, the contents of the log are written to stdout. You are recommended to use a file extension of .xml.

-f (Optional for User trace; required for Service trace). Read the log file directly from the file system. If you do not specify this option, the command sends an XML message to the component to request the log contents. If you have specified **-t** (service trace), you must specify this flag as well. Further details are given in “Additional parameters exclusive to service trace” on page 344.

If you specify this option, stop tracing (using mqsichangetrace) before you use the mqsireadlog command. If the log file is in use when you issue this command with this flag specified, partial XML records might be returned. You can reduce the risk of this happening by specifying **-m safe** on the

mqsichangetrace command. If the component being traced has itself stopped, you do not then need to issue a mqsichangetrace command.

If you do not stop tracing before you issue this command, check the contents of the log file created and remove any partial records from the end using a text editor before using the mqsiformatlog command, as partial records cannot be read by the format command.

Additional parameters exclusive to service trace:

Use these options only when directed to do so by your IBM Support Center or by a BIPxxxx message.

-t (Required) Read the log contents from the service trace log.

-b *qualifier*

(Required) Read the contents of the log for the broker agent, Configuration Manager agent, or User Name Server agent, or for the specified command utility program. This option is valid only if you have specified **-t** (service trace).

The following table shows the valid combinations of *qualifier* and component for service trace.

This option is generally used to trace the commands themselves. If you want to trace a particular command, run that command with environment variable MQSI_UTILITY_TRACE set to debug or normal before you issue this command to read the trace output generated.

Enter these values exactly as shown.

The agent trace is initiated when you specify the **-b** flag on the mqsichangetrace command. Do this only when directed to do so by a WebSphere Event Broker error message or when instructed to do so by your IBM Support Center.

The service trace is initiated when you specify the **-b** flag on the mqsichangetrace command. The format of the command is:

```
mqsireadlog <brokername> -t -b service -f -o service.xml
```

Do this only when directed to do so by a WebSphere Event Broker error message or when instructed to do so by your IBM Support Center.

-f (Required) Read the log file directly from the file system. When used with service trace, this flag has the same characteristics as when used with user trace. It remains optional if the **-e** flag is specified. You must specify this option if you specify the **-b** flag.

Qualifier	Component= <broker_name>	Component= ConfigMgr_name	Component= UserNameServer	Component= workbench	Component= utility
mqsichangebroker	x				
mqsichangeconfigmgr		x			
mqsichangetrace	x	x	x		
mqsichangeusernameserver			x		
mqsiclearmqpubsub	x				
mqsicreateaclentry					x
mqsicreatebroker	x				
mqsicreateconfigmgr		x			

Qualifier	Component= <broker_name>	Component= ConfigMgr_name	Component= UserNameServer	Component= workbench	Component= utility
mqscreateusernameeserver			x		
mqsdeleteaclentry					x
mqsdeletebroker	x				
mqsdeleteconfigmgr		x			
mqsdeleteusernameeserver			x		
mqsifformatlog ¹					x
mqsijoinmqpubsub		x			
mqsilist ²		x			x
mqsilist	x				
mqsilistaclentry					x
mqsireadlog	x	x	x		x
mqsireporttrace		x		x	
mqsistart	x	x	x		
mqsistop	x	x	x		
agent	x	x	x		
service	x	x	x		
workbench				x	
httplistener	x				

Notes:

1. Because this command does not have a component parameter, trace information is recorded in, and retrieved from, the *utility* component trace files. For further details see the mqsichangetrace command.
2. If this command is invoked without a component, trace information is recorded in, and retrieved from, the *utility* trace files in addition to component specific files. For further details see the mqsichangetrace command.

Authorization:

On UNIX platforms, the user ID must be a member of the **mqbrkrs** group. If the -f flag is specified, the user ID used to invoke this command must also have access to the trace file.

On Windows platforms, if the -f flag is specified, the user ID used to invoke this command must have access to the trace file. If the -f flag is not specified, the user ID used to issue the command must have **mqbrkrs** authority.

Responses:

- BIP8020 Unable to access database
- BIP8029 Broker not configured
- BIP8032 Unable to connect to queue
- BIP8033 Unable to send XML message
- BIP8035 Response not received within time-out
- BIP8036 Negative response received

- BIP8037 Unsupported flag selected
- BIP8038 Unsupported command option
- BIP8039 Execution group not available
- BIP8040 Unable to connect to database
- BIP8132 Invalid qualifier

Examples:

User trace for broker WBRK_BROKER:

```
mqsireadlog WBRK_BROKER -u -e default -o trace.xml
```

Service trace for component ConfigMgr:

```
mqsireadlog ConfigMgr -t -b agent -f -o trace.xml
```

Service trace for utility **mqsiformatlog**:

```
mqsireadlog utility -t -b agent -f -o trace.xml
```

You can format the log file (trace.xml in the above examples) using the command **mqsiformatlog**, or view it using an XML editor or viewer.

mqsireload command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

Use the **mqsireload** command to request the broker to stop and restart execution groups.

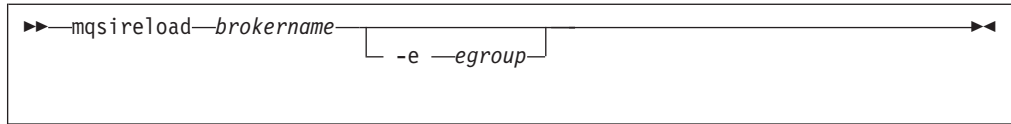
When you issue this command, a message is sent to the broker, which stops and restarts all its execution groups. You can specify a single execution group to be reloaded, but you are recommended to use the default form of this command to reload all execution groups.

Because an execution group does not stop until all message flows within it terminates, the ability of the broker to reload quickly depends on the processing time for the longest running message flow. This affects the performance of this command, and you are recommended to review any long-running message flows.

If you have included a user-defined node or parser within a message flow on the broker, these are deleted by this command, and the relevant termination functions called. When message flows are restarted, the resources used by user-defined nodes and parsers are re-accessed and reacquired. However, you are recommended to ensure that user-defined nodes and parsers provide their own mechanism to reload persistent state and data dynamically, and do not rely on the use of this command.

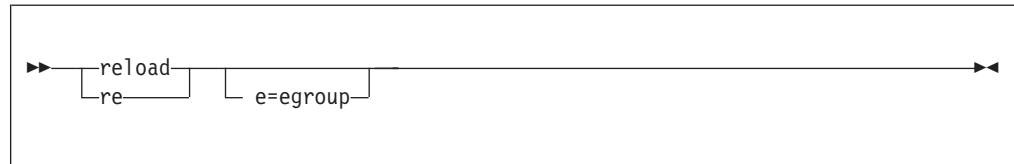
Syntax:

Windows platforms, Linux and UNIX systems:



z/OS:

Synonym: re



Parameters:

brokername

(Required - Windows platforms, Linux, and UNIX systems) The name of the broker to which the reload request is sent.

-e egroup

(Optional) The name of the execution group that is to be reloaded. If this parameter is not specified, all execution groups on the specified broker are stopped and restarted.

Authorization:

The user ID used to issue the command must be a member of the group **mqbrkrs**.

Responses:

No additional responses are returned.

Examples:

Windows platforms and UNIX platforms:

```
mqsireload broker1
```

z/OS:

```
F MQP1BRK,re
```

mqsiportflowstats command

Supported Platforms:

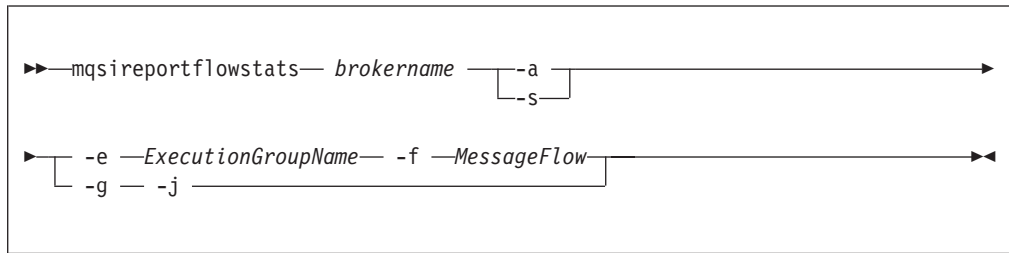
- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPRPMS; see "Contents of the broker PDSE" on page 378

Purpose:

Use the **mqsiportflowstats** command to display the current options for accounting and statistics that have been set using the **mqsichangefflowstats** command.

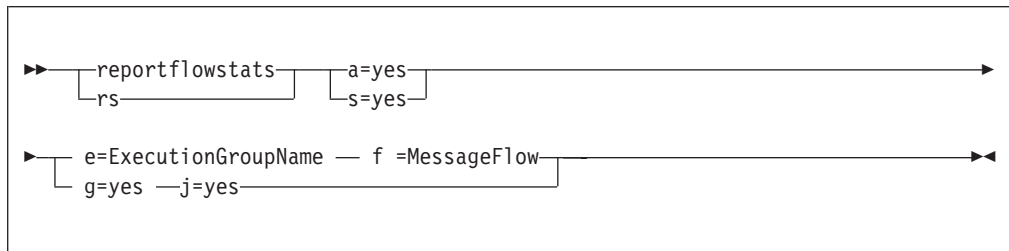
Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS:

Synonym rs



Parameters:

brokername

(Required - Windows platforms, Linux, and UNIX systems) Specify the label of the broker for which the previously stored accounting and statistics options are to be reported.

- a (Required) Specify that the command reports the stored settings for the archive accounting and statistics collection.

Note: You must specify **-a** or **-s**, or both arguments. If you do not specify at least one of these arguments you receive a warning message.

- s (Required) Specify that the command reports the stored settings for the snapshot accounting and statistics collection.

Note: You must specify **-a** or **-s**, or both arguments. If you do not specify at least one of these arguments you receive a warning message.

-e *ExecutionGroupName*

(Required) Specify the name for the execution group, for which accounting and statistics options are to be changed.

Note: You must specify either **-e** or **-g**. If you do not specify one of these arguments you receive a warning message.

-f *MessageFlow*

(Required) Specify the label for the message flow, for which accounting and statistics options are to be changed.

Note: You must specify either **-f** or **-j**. If you do not specify one of these arguments you receive a warning message.

-g (Required) Specifies that the command applies to **all** execution groups that belong to the broker.

Note: You must specify either **-e** or **-g**. If you do not specify one of these arguments you receive a warning message.

-j (Required) Specifies that the command applies to **all** message flows that belong to the execution group.

Note:

1. You must specify either **-f** or **-j**. If you do not specify one of these arguments you receive a warning message.
2. If you set the **-g** option for all execution groups, you must use **-j** instead of **-f**.

Authorization:

The user Id used to issue the command must have mqbrkrs authority.

Responses:

This command returns the following responses:

- BIP2268 Request to report on message flow node ' ': message flow does not exist
- BIP8001 Unknown flag selected
- BIP8004 Invalid flags or arguments missing
- BIP8007 Mandatory argument missing
- BIP8013 Component does not exist
- BIP8020 Unable to access the database
- BIP8029 Broker not configured
- BIP8033 Unable to send XML message
- BIP8038 Unsupported command option
- BIP8039 Execution group not available
- BIP8040 Unable to connect to database
- BIP8071: Successful command completion

Examples:

Request a report for message flow "MyFlow1" in the execution group "default" for broker "BrokerA" for both archive and snapshot statistics collection:

```
mqsireportflowstats BrokerA -s -a -e default -f MyFlow1
```

Request a report of the snapshot options that are currently stored for all message flows in all execution groups for broker "BrokerA" :

```
mqsireportflowstats BrokerA -s -g -j
```

mqsireportproperties command

Supported platforms:

- Windows
- Linux and UNIX systems

- z/OS through the BIPRPP utility; see “Contents of the broker PDSE” on page 378

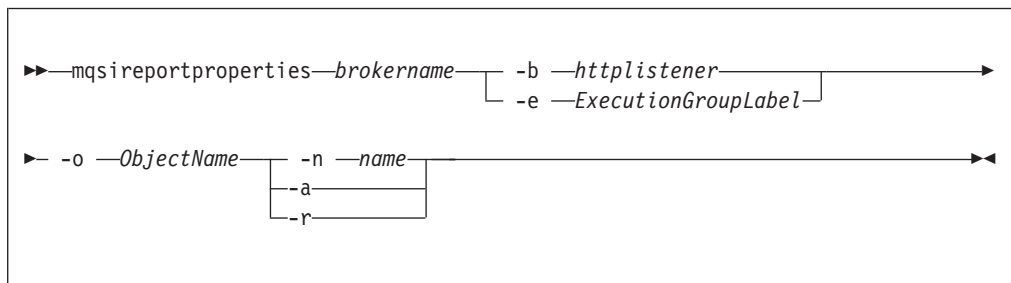
Purpose:

Use the **mqsi**reportproperties command to examine the values of properties set using the **mqsi**changeproperties command.

Start the broker using mqsisstart, and then issue the command on the machine running the broker.

If you change any value (with **mqsi**changeproperties) you **must** stop and restart the broker for the change to take effect.

Syntax:



Parameters:

brokername

(Required) The name of the broker.

-e ExecutionGroupLabel

(Optional) The label of the execution group for which a report is required.

-b httpListener

(Optional) The name of the http listener component.

-o ObjectName

(Required) The name of the object whose properties you want to change. This must be set to one of the values listed below.

-n name

(Optional) Display only the named property

-a (Optional) Indicates that all property values of the object are displayed, and does not recurse into properties that have child values.

-r (Optional) Indicates that all property values of the object are displayed and, additionally, displays the child values for all properties that have child values.

- You **must** select one, and only one, option from **-n**, **-a**, and **-r**.

For a list of the options you can select, see the **mqsi**changeproperties command.

- You **must** select one, and only one, option from **-e** and **-b**.

The *ObjectName* parameter can have a value for inter-broker communications or for the *httpListener* component. For inter-broker communications, use the following value:

- *DynamicSubscriptionEngine*

For the *httplistener* component, which includes the HTTPInput and HTTPReply nodes, the following *ObjectName* values are available:

- *HTTPListener* for controlling the HTTPListener process.
- *HTTPConnector* for controlling HTTP communication with the HTTPInput and HTTPReply nodes.
- *HTTPSConnector* for controlling HTTPS communication with the HTTPInput and HTTPReply nodes.

httplistener is required when using the HTTP *ObjectName* settings.

For the *httplistener* component, **mqsireportproperties** does not report those properties that have not been explicitly set with **mqsichangeproperties**, even if those properties have a default setting. For example, the default HTTPSConnector port that is used (unless it has been changed) is 7083. However this value is not reported by **mqsireportproperties** unless it has been changed from this default with **mqsichangeproperties**. To see the default values for all properties that **mqsireportproperties** can report on, see the documentation for **mqsichangeproperties**.

Authorization:

No specific authority is required to invoke this command.

Examples:

Display all the current HTTPListener settings (that have been changed from their default value)

```
mqsireportproperties TEST -b httplistener -o HTTPListener -a
```

Display the HTTPSConnector port setting (if it has been changed from the default value)

```
mqsireportproperties TEST -b httplistener -o HTTPSConnector -n port
```

Display recursively all the current settings for the inter-broker communication.

```
mqsireportproperties TEST -e default -o DynamicSubscriptionEngine -r
```

mqsireporttrace command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

Use the **mqsireporttrace** command to display the trace options currently in effect. This command is valid for:

- User trace. Specify the **-u** option.
On z/OS, user trace is run against a specific execution group for a broker. You can narrow the command down further to trace a specific message flow.
- Service trace. Specify the **-t** option. Use this option only if directed to do so by the action described in a BIPxxxx message, or by your IBM Support Center.

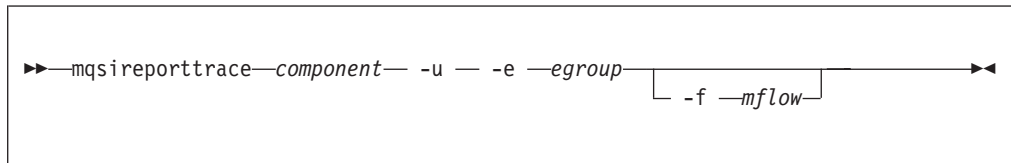
On z/OS, service trace can be run for a specific execution group (like user trace). Unlike user trace, service trace can also be run against an active agent (that is, a broker or User Name Server).

If you specify a broker, or any of its resources (execution group or message flow), you must have deployed them before you can query trace settings.

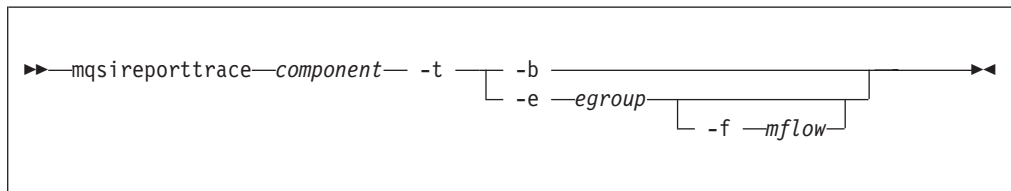
Syntax:

Windows platforms, Linux, and UNIX systems:

User trace:

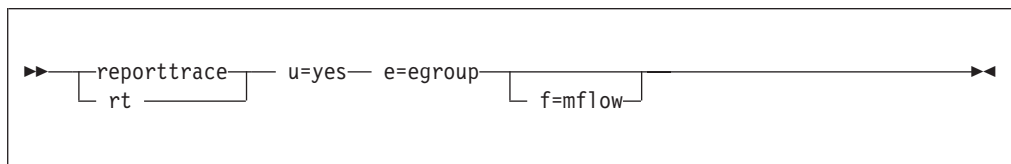


Service trace:

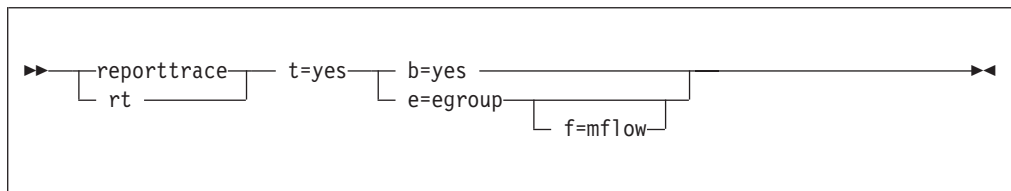


z/OS:

User trace:



Service trace:



Parameters:

component

(Required - Windows platforms, Linux, and UNIX systems) The name of the broker for which options are reported, or the fixed value UserNameServer. Both values are case sensitive on Linux and UNIX systems.

-u (Required for user trace) Derive report information from the user trace.

-e *egroup*

(Required for user trace, otherwise optional) The label of the execution group for which a report is required. This is valid only if you have specified a broker as the component.

On z/OS this name is case sensitive. Include the name in single quotes if it contains mixed-case characters.

-f *mflow*

(Optional) The label of the message flow for which a report is required. This is valid only if you have specified both a broker as the component and an execution group.

On z/OS this name is case sensitive. Include the name in single quotes if it contains mixed-case characters.

Additional parameters exclusive to service trace:

Use these options only when directed to do so by your IBM Support Center or by a BIPxxxx message.

-t (Required for service trace) Derive report information from the service trace.

-b (Alternative to **-e** on all platforms) Request a report for agent function.

Authorization:

The user ID used to issue the command must have **mqbrkrs** authority.

Responses:

- BIP8002 Selected flags incompatible (z/OS only)
- BIP8003 Duplicate flag detected (z/OS only)
- BIP8013 Component does not exist
- BIP8020 Unable to access database
- BIP8029 Broker not configured
- BIP8032 Unable to connect to queue (Windows platforms, Linux, and UNIX systems only)
- BIP8033 Unable to send XML message
- BIP8035 Response not received within time-out
- BIP8036 Negative response received
- BIP8037 Unsupported flag selected
- BIP8038 Unsupported command option
- BIP8039 Execution group not available
- BIP8040 Unable to connect to database
- BIP8045 Message flow not available
- BIP8158 Invalid format for command (z/OS only)
- BIP8159 Unknown parameter "... " (z/OS only)

Examples:

Windows platforms, Linux, and UNIX systems:

```
mqsiporttrace BrokerA -t -e "exgrp1"
```

z/OS:

F MQP1BRK,reporttrace t=yes,e='exgrp1'

mqsirestoreconfigmgr command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPRSCM; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

This command restores a previously backed up Configuration Manager Archive.

Note:

1. It must be run on the same machine as the Configuration Manager and the Configuration Manager must not be running.
2. The command tries to stop the Configuration Manager if it is running before it attempts a backup restore.
3. If you are recovering the Configuration Manager because the configuration repository is damaged, restore the repository from a previously successful backup version using the **mqsirestoreconfigmgr** command.
4. If you plan to restore the Configuration Manager data repository on z/OS and the platform from which it was originally backed up was not z/OS, or the other way round, you need to copy the saved `service.properties` file to:

<Configuration
Manager directory>/components/<component name>/<directory name>/service.properties

after running the **mqsirestoreconfigmgr** command.

Syntax:

Windows platforms, Linux, and UNIX systems:

```
►►mqsirestoreconfigmgr—configMgrName— -d —archiveDirectory—►►
► -a—archiveName— [ -w—workPath— ] ►►
```

z/OS:

```
►►mqsirestoreconfigmgr—configMgrName—d=archiveDirectory—a=archiveName—►►
► [w=workPath—] ►►
```

Parameters:

configMgrName

(Required) The name of the Configuration Manager.

-d *archiveDirectory*

(Required) The directory where the archive is placed.

-a *archiveName*

(Required) Specifies the backup archive name.

-w *workPath*

(Optional) Specifies the path for the Configuration Manager repository.

Authorization:

This command changes security privileges for the ServiceUserID; the user ID used to invoke this command must be a member of the Windows **Administrators** group on this local system.

Responses:

This command returns the following responses:

- BIP8056 Unknown queue manager

Examples:

mqsisetsecurity command

Supported platforms:

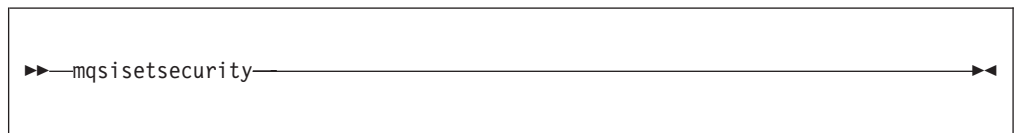
- Windows

Purpose:

Use the **mqsisetsecurity** command to create the Windows groups that WebSphere Event Broker requires for secure access to its runtime libraries and data.

This command runs automatically as part of the installation process of WebSphere Event Broker. If WebSphere MQ is installed after WebSphere Event Broker, you can issue this command to add your account to the MQM group provided you have **Administrator** authority.

Syntax:



Parameters:

None

Authorization:

The user ID used to invoke this command must belong to the **Administrators** group on the local system because creating groups is an administrative task.

Responses:

- BIP8610 User does not have **Administrator** authority
- BIP8611 Unable to create **mqbrkrs** group because the user does not have access to the requested information
- BIP8612 Unable to create **mqbrkrs** group because the computer name is invalid
- BIP8613 Unable to create **mqbrkrs** group because an error occurs when accessing the alias
- BIP8614 The **mqbrkrs** group already exists
- BIP8615 The **mqbrkrs** group has been created successfully
- BIP8616 The current user is already a member of the **mqbrkrs** group
- BIP8617 The **mqbrkrs** group does not exist
- BIP8614 The user could not be added because the account type is invalid

mqsi_setupdatabase command

Supported platforms:

- Linux and UNIX systems

Purpose:

Use the **mqsi_setupdatabase** command if you are setting up a supported database on Linux or UNIX systems. You need to run this command only if your database is Oracle.

This command sets up the required database links for the Oracle database that is used within your WebSphere Event Broker environment. This applies to both broker and user (application) databases.

Note that the command works for a remote database in the same way that it does for a local database.

You must complete this procedure before you create the broker database. You are recommended to do this after you have installed your database, but you can complete this process before database installation if you specify the intended database installation directory correctly during this setup.

Syntax:

```
►—mqsi_setupdatabase— database—database_home_directory—◄◄
```

Parameters:

database

(Required) The database that you are installing. Possible values are :

- oracle9
- oracle10

database_home_directory

(Required) The name of the directory in which the database is (or will be) installed (for example, /usr/lpp/oracle9).

Authorization:

The user ID used to invoke this command must be **root**. It must also be a member of the **mqbrkrs** group.

mqsistart command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

Windows platforms, Linux, and UNIX systems:

Use **mqsistart** to start a WebSphere Event Broker component. If the queue manager associated with this component (defined in the corresponding create command) is not already running, it is also started by this command. However, no listeners, channels, or channel initiators associated with the started component are started. If you have WebSphere MQ Version 6.0 installed, use the WebSphere MQ Explorer to start any required listeners, channels, or channel initiators. For earlier supported versions of WebSphere MQ, use the WebSphere MQ Services snap-in.

Successful completion of this command indicates that the Windows service, or Linux or UNIX daemon has started successfully, and that the component startup has been initiated. Check the Windows system event log or the Linux or UNIX syslog to determine if the component and all related software have started successfully, are initially active, and remain in an active state. Any errors that have prevented successful startup, detected by the component are recorded in the log. Continue to monitor the Windows system event log or Linux or UNIX syslog.

If the queue manager supporting the component specified on this command is not already running, it is started by this command, but on Windows platforms, is not started as a service. On this system, it stops if you log off. To avoid this happening, either remain logged on, or change the startup status of the queue manager service (described in “Creating a Configuration Manager on Windows” on page 129). (If you lock your workstation, the queue manager does not stop.)

z/OS:

The following table distinguishes between the **start (/S)** and **startcomponent** commands, and lists the available options:

- Use the **start (/S)** command to bring a component into a state in which you can run the appropriate **change** command.
- Use the **startcomponent** command to start a broker, Configuration Manager, or User Name Server when its controller (control process) is already running.

Component	Command	Description
Broker	/S <brokerName> /F <brokerName>,SC	Start broker. Starts the broker from a 'stop component' state.
Configuration Manager	/S <configMgrName> /F <configMgrName>,SC	Start Configuration Manager. Starts the Configuration Manager from a 'stop component' state.

User Name Server	/S <User Name ServerName> /F <User Name Server>,SC	Start User Name Server. Starts the User Name Server from a 'stop component' state.
------------------	---	---

When the controller address space is started, this causes the component to start automatically. This behavior can be changed by an optional start parameter in the started task. If the parameter is set to MAN, the component does not start automatically; the default is AUTO.

Issuing commands against the controller means issuing start, stop, or modify commands from the console to the controller address space. There are two scenarios using this command. The first is that the controller is started with the parameter MAN instead of AUTO. The second is that, after a **stopcomponent** command, the component has to be restarted.

Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS:

Synonym: sc



Parameters:

component

(Required - Windows platforms, and Linux and UNIX systems) This must be a broker name, Configuration Manager name, or one of the fixed values UserNameServer or DatabaseInstanceMgr. All the names are case sensitive on Linux and UNIX systems.

You are strongly recommended to only use this command on Windows platforms if you are using the Derby database.

Authorization:

On Windows platforms, the user ID used to invoke this command must have **Administrator** authority on the local system.

On Linux and UNIX systems, the user ID used to invoke this command must either be **root** or must be the same as that specified in the -i parameter when the component was created. It must also be a member of the **mqbrkrs** and **mqm** groups.

When the Windows service, or Linux or UNIX daemon is started, it runs under the user ID specified by the `-i` flag on the appropriate `mqscreatexxxx` command. The component only starts if the ServiceUserID specified is authorized to access the home directory (where WebSphere Event Broker has been installed), and the working directory (if specified by the `-w` flag on the `mqscreatexxxx` command).

The security requirements for using this command are summarized in “Security requirements for Windows platforms” on page 425 and “Security requirements for Linux and UNIX platforms” on page 424.

Responses:

Windows platforms, Linux, and UNIX systems only:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8015 Component cannot be started
- BIP8018 Component running
- BIP8024 Unable to locate executable
- BIP8025 Component disabled
- BIP8026 Unable to start component
- BIP8027 Unable to start WebSphere MQ
- BIP8028 WebSphere MQ unavailable
- BIP8030 Unable to modify user privileges
- BIP8048 Unable to start queue manager
- BIP8056 Unknown queue manager
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping

Examples:

Windows platforms, Linux, and UNIX systems:

```
mqsistart WBRK_BROKER
mqsistart DatabaseInstanceMgr
```

```
z/OS
  F MQ00BRK,sc
```

mqsistartmsgflow command

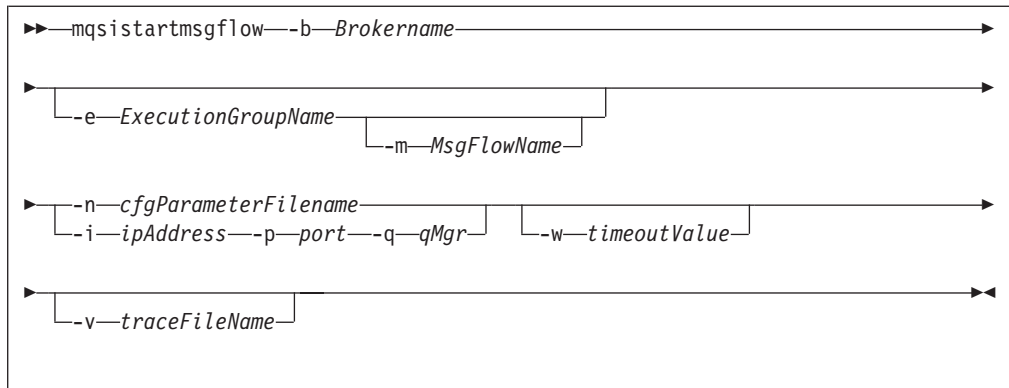
Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPSTMF; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

Use the `mqsistartmsgflow` command to start message flows.

Syntax:



Parameters:

-b *BrokerName*

(Required) The name of the broker on which to start message flows.

If you do not specify the **-e** and **-m** flags, all message flows on the broker are started.

-e *ExecutionGroupName*

(Optional) The name of the execution group on which message flows are started.

-m *msgFlowName*

(Optional) The name of the message flow being started.

You can specify only one message flow in a single command. However, if you do not specify this parameter, all message flows on the execution group or broker are started.

If you specify this flag you must also specify the **-e** flag.

-n *cfgParameterFileName*

(Optional) The name of a `.configmgr` file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the `.configmgr` format saved by the Eclipse GUI. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement `encoding="UTF-8"` from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the host attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
securityExit="test.myExit"/>
```

Note: If you do not supply this parameter, you must supply the **-i**, **-p**, and **-q** parameters.

-i *ipAddress*

(Optional) The host name or IP address of the Configuration Manager.

If you are using this file on z/OS and want to connect to the local host you must set the value to `"`.

- p** *Port*
(Optional) The port number of the Configuration Manager.
- q** *qMgr*
(Optional) The name of the WebSphere MQ queue manager that the Configuration Manager is using.

If you do not supply the **-i**, **-p**, and **-q** parameters, you must specify the **-n** parameter.
- w** *timeoutValue*
(Optional) The time in seconds that the utility waits to ensure that the start command completed; the default value is 60.
- v** *TraceFileName*
(Optional) Sends internal debug trace information to the specified file.

Authorization:

To start message flows you need to have sufficient authority defined in the Configuration Manager's access control list.

The permissions required are the same as the permission required to do the equivalent function in the Message Brokers Toolkit; see "ACL permissions" on page 423 for a list of permissions that can be defined in the Configuration Manager.

Responses:

This command returns the following responses:

- 0** (Success) States that the request completed successfully and the state of all message flows has been updated.
- 2** (Failure) States that at least one message flow can not be put into the correct state for any reason.
- 98** States that the Configuration Manager cannot be reached.
- 99** States that the supplied arguments to the utility are not valid.

Examples:

Starts all message flows on broker B1, which is controlled by the Configuration Manager whose connection details are described in `cm1.configmgr`. Control is returned to the caller when all message flows in the broker are reported as started, or the default time of one minute elapses, whichever is sooner.

```
mqsisstartmsgflow -n cm1.configmgr -b B1
```

Starts all message flows on broker B1, which is controlled by the Configuration Manager whose connection details are described in `cm1.configmgr`. Control is returned to the caller when all message flows in the broker are reported as started, or two minutes elapses, whichever is sooner.

```
mqsisstartmsgflow -n cm1.configmgr -b B1 -w 120
```

Start all message flows on Broker B1, which is controlled by the Configuration Manager. The Configuration Manager is hosted by the queue manager QM1 which is on local host:1414.

```
mqsisstartmsgflow -q QM1 -i localhost -p 1414 -b B1
```

Enter **mqsistartmsgflow** to display usage information:

```
> mqsistartmsgflow
BIP1024I: Starts message flows.

> Syntax:
mqsistartmsgflow (-n cfgParameterFileName | (-i ipAddress -p port -q qMgr))
  -b brokerName [-e executionGroupName [-m flowName]] [-w timeoutValue]
  [-v traceFileName]
Command Options:
'-n cfgParameterFileName' File containing Configuration
Manager connection parameters (.configmgr)
'-i ipAddress' IP address or host name of the Configuration
Manager
'-p port' port number of the Configuration
Manager
'-q qMgr' queue manager of the Configuration
Manager
'-b brokerName' name of the broker on which to start message flows
'-e executionGroupName' name of the execution group on which to start message flows.
If this is not specified, all message flows on the broker will be started.
'-m flowName' name of the message flow to start.
If this is not specified, all message flows on the execution group will be started.
'-w timeoutValue' time to wait (in seconds) for message flows to start (Default=60)
'-v traceFileName' send verbose internal trace to the specified file.
```

mqsistop command

Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS

Purpose:

Use the **mqsistop** command to stop a WebSphere Event Broker component. On z/OS, the controller must be running.

The following table distinguishes between the **stop (/P)** and **stopcomponent** commands, and lists the available options:

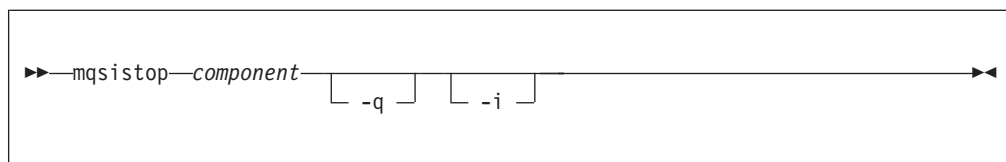
- Use the **stop (/P)** command to bring a component into a state in which you can run the appropriate **change** command.
- Use the **stopcomponent** command to stop a broker, Configuration Manager, or User Name Server when its controller (control process) is already running.

Component	Command	Description
Broker	/P <brokerName> /F <brokerName>,P /F <brokerName>,PC	Stop broker. Stop broker; this is the same as /P. You can also use /F <brokerName>,STOP Stop broker component. This stops the broker process (including any execution group address spaces), but leaves the message broker console command server running inside the controller address space. This allows you to run the "mqsichangebroker command" on page 250 console command. Restart the broker afterwards by running the "mqsistart command" on page 357 (SC) console command.

Configuration Manager	/P <configMgrName> /F <configMgrName>,P /F <configMgrName>,PC	Stop Configuration Manager. Stop Configuration Manager; this is the same as /P. You can also use /F <configMgrName>,STOP Stop Configuration Manager component. This stops the Configuration Manager process, but leaves the message broker console command server running inside the controller address space. This allows you to run the “mqsichangeconfigmgr command” on page 256 console command. Restart the broker afterwards by running the “mqsistart command” on page 357 (SC) console command.
User Name Server	/P <User Name ServerName> /F <User Name Server>,P /F <User Name Server>,PC	Stop User Name Server. Stop User Name Server; this is the same as /P. You can also use /F <User Name Server>,STOP Stop User Name Server component. This stops the User Name Server process, but leaves the message broker console command server running inside the controller address space. This allows you to run the “mqsichangeusernameserver command” on page 279 console command. Restart the broker afterwards by running the “mqsistart command” on page 357 (SC) console command.

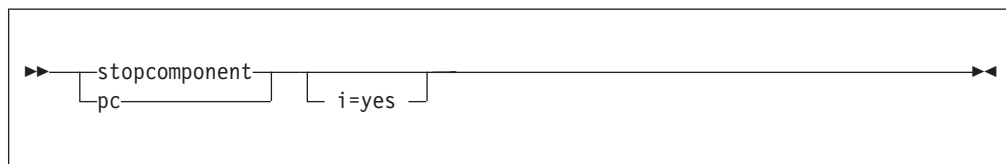
Syntax:

Windows platforms, Linux, and UNIX systems:



z/OS:

Synonym: pc



Parameters:

component

(Required - Windows, Linux, and UNIX systems) This must be a broker name, a Configuration Manager name, or one of the following fixed values:

- UserNameServer or DatabaseInstanceMgr on Windows platforms
- UserNameServer on Linux and UNIX systems

All the names are case sensitive on Linux and UNIX systems.

Do not use this command on a DatabaseInstanceMgr unless you are using the Derby database.

- q (Optional - Windows, Linux, and UNIX systems only) Stop the WebSphere MQ queue manager associated with this WebSphere Event Broker component.

Specify this flag only if the WebSphere Event Broker component is the last (or only) WebSphere Event Broker component active on this queue manager. This command initiates a controlled shutdown of the queue manager, and informs other users of the queue manager that it is closing.

If you do not stop other WebSphere Event Broker components that use this queue manager before you issue this command with this option, stop them afterwards or restart the queue manager.

If you use this option, be aware that any listeners associated with this queue manager are not stopped with the queue manager. Stop these manually after issuing this command.

- i (Optional) Immediately stop the broker.

Only specify this flag if you have already tried, and failed, to stop the broker in a controlled fashion using **mqsistop** without the **-i** flag.

On z/OS this command will be rejected by the Message Broker console command server if a previous stop command has failed to complete. This can occur, for example, if one or more execution group address spaces cannot shutdown.

Authorization:

On Windows platforms, the user ID used to invoke this command must belong to the **Administrators** group.

On Linux and UNIX systems, the user ID used to invoke this command must conform to the following requirements:

- The user ID must be a member of the **mqbrkrs** group.
- The user ID must either be **root**, or the same as that specified in the **-i** parameter when the component was created.
- If you specify the **-q** parameter, the user ID must be a member of the **mqm** group.

The security requirements for using this command are summarized in “Security requirements for Windows platforms” on page 425 and “Security requirements for Linux and UNIX platforms” on page 424.

Responses:

Windows, Linux, and UNIX systems only:

- BIP8012 Unable to connect to system components
- BIP8013 Component does not exist
- BIP8016 Component cannot be stopped
- BIP8019 Component stopped
- BIP8030 Unable to modify user privileges
- BIP8049 Unable to stop queue manager
- BIP8093 Queue manager being created
- BIP8094 Queue manager stopping

Examples:

Windows

To stop the Database Instance manager:

```
mqsistop DatabaseInstanceMgr
```

Windows, Linux, and UNIX systems.

To stop the broker, mybroker, and the WebSphere MQ queue manager associated with it:

```
mqsistop mybroker -q
```

z/OS To stop a broker called MQ00BRK:

```
F MQ00BRK,pc
```

mqsistopmsgflow command

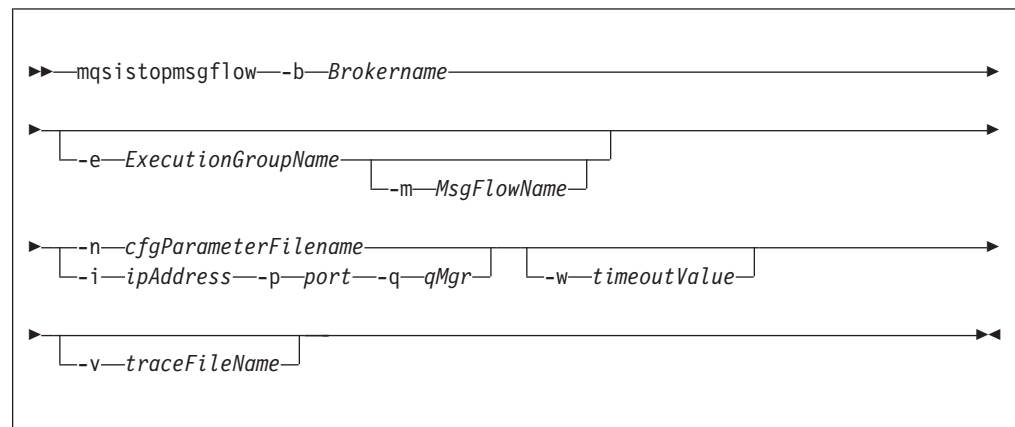
Supported platforms:

- Windows
- Linux and UNIX systems
- z/OS. You can also use BIPSMSE; see “Contents of the Configuration Manager PDSE” on page 380

Purpose:

Use the **mqsistopmsgflow** command to stop message flows.

Syntax:



Parameters:

-b *BrokerName*

(Required) The name of the broker on which to stop message flows.

If you do not specify the **-e** and **-m** flags, all message flows on the broker are stopped.

-e *ExecutionGroupName*

(Optional) The name of the execution group on which message flows are stopped.

-m *msgFlowName*

(Optional) The name of the message flow being stopped.

You can specify only one message flow in a single command. However, if you do not specify this parameter, all message flows on the execution group or broker are stopped.

If you specify this flag you must also specify the **-e** flag.

-n *cfgParameterFileName*

(Optional) The name of a `.configmgr` file that describes the connection parameters to the Configuration Manager.

The file is in XML, using the `.configmgr` format saved by the Eclipse GUI. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configmgr host="localhost" listenerPort="1414" queueManager="QNAME"
  securityExit="test.myExit"/>
```

If you are using this file on z/OS you must remove the statement `encoding="UTF-8"` from the first line, to leave the statement as:

```
<?xml version="1.0"?>
```

and remove the value for the `host` attribute, to leave the statement as:

```
<configmgr host="" listenerPort="1414" queueManager="QNAME"
  securityExit="test.myExit"/>
```

Note: If you do not supply this parameter, you must supply the **-i**, **-p**, and **-q** parameters.

-i *ipAddress*

(Optional) The host name or IP address of the Configuration Manager.

If you are using this file on z/OS and want to connect to the local host you must set the value to `"`.

-p *Port*

(Optional) The port number of the Configuration Manager.

-q *qMgr*

(Optional) The name of the WebSphere MQ queue manager that the Configuration Manager is using.

If you do not supply the **-i**, **-p**, and **-q** parameters, you must specify the **-n** parameter.

-w *timeoutValue*

(Optional) The time in seconds that the utility waits to ensure that the stop command completed; the default value is 60.

-v *TraceFileName*

(Optional) Sends internal debug trace information to the specified file.

Authorization:

To stop message flows you need to have sufficient authority defined in the Configuration Manager's access control list.

The permissions required are the same as the permission required to do the equivalent function in the Message Brokers Toolkit; see "ACL permissions" on page 423 for a list of permissions that can be defined in the Configuration Manager.

Responses:

This command returns the following responses:

- 0 (Success) States that the request completed successfully and the state of all message flows has been updated.
- 2 (Failure) States that at least one message flow can not be put into the correct state for any reason.
- 98 States that the Configuration Manager cannot be reached.
- 99 States that the supplied arguments to the utility are not valid.

Examples:

Stops all message flows on execution group default on broker B1, which is controlled by the Configuration Manager whose connection details are described in cml.configmgr. Control is returned to the caller when all message flows in the execution group are reported as stopped, or the default time of one minute elapses, whichever is sooner.

```
mqsistopmsgflow -n cml.configmgr -b B1 -e default
```

Stops the message flow flow1 on execution group default on broker B1, which is controlled by the Configuration Manager whose connection details are described in cml.configmgr. Control is returned to the caller when the message flow is reported as stopped, or the default time of one minute elapses, whichever is sooner.

```
mqsistopmsgflow -n cml.configmgr -b B1 -e default -m flow1
```

Enter **mqsistopmsgflow** to display usage information:

```
> mqsistopmsgflow
BIP1025I: Stops message flows.

> Syntax:
mqsistopmsgflow (-n cfgParameterFileName | (-i ipAddress -p port -q qMgr))
  -b brokerName [-e executionGroupName [-m flowName]] [-w timeoutValue]
  [-v traceFileName]
Command Options:
'-n cfgParameterFileName' Configuration
Manager connection file (.configmgr)
'-i ipAddress' IP address or host name of the Configuration
Manager
'-p port' port number of the Configuration
Manager
'-q qMgr' queue manager of the Configuration
Manager
'-b brokerName' name of the broker on which to stop message flows
'-e executionGroupName' name of the execution group on which to stop message flows.
If this is not specified, all message flows on the broker will be stopped.
'-m flowName' name of the message flow to start.
If this is not specified, all message flows on the execution group will be stopped.
'-w timeoutValue' time to wait (in seconds) for message flows to stop (Default=60)
'-v traceFileName' send verbose internal trace to the specified file.
```

z/OS specific information

Follow the links below for more information:

- “Administration in z/OS” on page 368
- “z/OS customization” on page 370
- “z/OS JCL variables” on page 382

Administration in z/OS

In the z/OS environment, commands are issued through the console and others in batch jobs.

- *hlq*.SBIPSAMP has all the JCL samples to customize.
- *hlq*.SBIPPROC has all the JCL procedures to customize.

Stepname

The processes BIPSERVICE and BIPBROKER are in the same address space (control address space). After an Execution Group address space is started on z/OS, the stepname of the address space has the following value:

- The last eight characters are taken from the Execution Group label.
- Any lowercase characters are folded to upper case.
- Any non alphanumeric characters are changed to the character @.
- If the first character is not an alpha character, it is changed to A.

The stepname is not guaranteed to be a unique value. However, you are strongly recommended to ensure that the last eight characters of any Execution Group labels that are deployed to a z/OS broker are unique, and contain only alphanumeric characters; note that an Execution Group label has a maximum size of 3000 bytes.

See the following topics for more information:

- “Issuing commands to the z/OS console”
- “Guidance for issuing console commands in z/OS” on page 369
- “START and STOP commands on z/OS” on page 369

Issuing commands to the z/OS console

You operate the broker or User Name Server using the z/OS START, STOP, and MODIFY commands. You can issue commands, and get responses back from:

- The z/OS operator console
- The TSO CONSOLE facility
- The CONSOLE interface from REXX
- Products such as SDSF
- z/OS automation products, such as NetView®

However, you are likely to need to issue commands with mixed case, because execution group names are often in mixed case. You can issue commands with mixed case on the z/OS console, using the REXX CONSOLE interface, with products like SDSF V2.10 and higher, and NetView. Releases of SDSF before V2.10, and the TSO CONSOLE facility, do not support passing mixed case data.

If you do not have support for mixed case, you can submit the commands through a batch job. For example:

```
//MI01CMD JOB MSGCLASS=H
//  COMMAND 'f MQP1BRK,ct t=yes,e='default',l=debug,f='lowmf1''
//STEP1 EXEC PGM=IEFBR14
```

If your product for issuing console commands supports mixed case input, you might need to take special actions to use mixed case. For example in SDSF on OS/390® V2.10 and above, you can enter mixed case keyword values by typing /,

pressing ENTER, and entering the command in the popup window. If you enter / followed by the command, the command is translated to uppercase. In NetView, prefix the command with NETVASIS to get lowercase support.

Guidance for issuing console commands in z/OS

These examples use a broker called MQP1BRK. Start and stop the broker or User Name Server using the MVS START (S) and STOP (P) commands. If you want to pass information to the broker or User Name Server while it is running, use the MVS MODIFY command (F) to issue commands. For example:

```
F MQP1BKR,rt
```

This list summarizes the rules you must follow when issuing console commands:

- Each command starts with a verb followed by zero or more keyword=value pairs.
- There must be one or more blanks between the verb and the first keyword.
- All characters are converted to lowercase, unless they are within quotation marks.
- Multiple keywords are separated by , with no blanks.
- The keyword is always case insensitive.
- The value is case sensitive, unless specified otherwise (for example Yes/No, trace-modes).
- Each keyword must be followed by the equals sign = and parameter value. Enter parameters in any order in the form:

```
flag=value
```

and separate them with commas. Repeated parameters are not allowed.

- Strings that contain blanks or special characters must be enclosed in single quotation marks ('). If the string itself contains a quotation mark, the quotation mark is represented by two single quotation marks.
- The verb and keywords are not case sensitive.
- On mixed case consoles the case of values in single quotation marks (') is not changed.
- For YES/NO flags, all case combinations are allowed.
- The maximum length of the MODIFY command is 126 characters, including
F taskname,

An example console command:

```
F MQP1BRK,changetrace u=Yes,l=normal,e='myExecutionGroup'
```

START and STOP commands on z/OS

These examples use a broker called MQP1BRK. Start and stop the broker or User Name Server using the MVS START (S) and STOP (P) commands. If you want to pass information to the broker or User Name Server while it is running, use the MVS MODIFY command (F) to issue commands. For example:

```
F MQP1BKR,rt
```

The MVS command START (S) starts a broker, Configuration Manager, or User Name Server (server component) on MVS. This initiates the control address space, plus other address spaces as needed, to run that component.

The MVS command STOP (P) stops a server component completely, including its control address space.

For administration purposes you can bring the server component into another state, where the control address space is still running, but all other components are stopped.

For example, this is needed in order to change broker startup parameters, see “mqsicchangebroker command” on page 250. You can do this by using the MODIFY (/F) command on the started component, and using the startcomponent (SC) or stopcomponent (PC) options. See “mqsisstart command” on page 357 and “mqsisstop command” on page 362 for more information.

z/OS customization

This is an introduction topic for a number of reference topics in the area of z/OS customization. See the links under Related reference information.

Naming conventions for WebSphere Event Broker for z/OS

Decide upon a naming convention for your WebSphere Event Broker components to make customizing, operating, and administering easier.

Each broker requires its own queue manager. Base your broker name on the queue manager name. For example, append BRK to the queue manager name of MQP1, to give MQP1BRK. This naming convention has the following advantages:

- It is easy to associate the broker with the queue manager, because they both begin with the same characters.
- The started task name has the same name as the broker.
- You can have the broker name as part of the data set name, which makes it easier to administer.

Similarly, base the Configuration Manager and User Name Server name on the queue manager name. For example, append CMGR or UNS to the queue manager name.

Using this convention, you might have the following component names for a queue manager MQP1.

- A broker called MQP1BRK with:
 - A started task name of MQP1BRK.
 - A started task user ID of MQP1BRK.
 - A PDSE containing definitions called hlq.MQP1BRK.xxx.
 - A UNIX System Services directory structure like /xxx/yyy/MQP1BRK.
 - A DB2 group called MQP1GRP.
- A User Name Server called MQP1UNS with:
 - A started task name of MQP1UNS.
 - A started task user ID of MQP1UNS.
 - A PDSE containing definitions called hlq.MQP1UNS.xxx.
 - A UNIX System Services directory structure like /xxx/yyy/MQP1UNS.
- A Configuration Manager called MQP1CMGR with:
 - A started task name of MQP1CMGR.
 - A started task user ID of MQP1CMGR.

- A PDSE containing definitions called hlq.MQP1CMGR.xxx.
- A UNIX System Services directory structure like /xxx/yyy/MQP1CMGR.

Plan for expansion by selecting names that allow growth.

If your broker name is in uppercase, ensure the broker name is also in uppercase in the workbench.

Customization tasks and roles on z/OS

Systems programmers do most of the customization of WebSphere Event Broker. Tasks that need to be performed by other people in your organization are identified in the table below:

Role	Task
z/OS systems programmer	"Customizing the z/OS environment" on page 60
	"Setting up z/OS security" on page 28
	"Summary of required access (z/OS)" on page 372
	"Customizing UNIX System Services on z/OS" on page 71
	"Creating the broker component" on page 122
	"Starting and stopping a broker on z/OS" on page 216
	"Checking APF attributes of bipimain on z/OS" on page 79
DB2 administrator	"Setting up DB2" on page 29
	"Summary of required access (z/OS)" on page 372
	"DB2 planning on z/OS" on page 73
	"Priming DB2" on page 121
WebSphere MQ administrator	"Setting up WebSphere MQ" on page 30
	"Summary of required access (z/OS)" on page 372
	"WebSphere MQ planning for z/OS" on page 76
	"Creating the broker component" on page 122
	"Defining the started tasks to z/OS Workload Manager (WLM)" on page 77
WebSphere Event Broker administrator	"Setting up workbench access on z/OS" on page 31
	"Summary of required access (z/OS)" on page 372
	"Creating a broker on z/OS" on page 116
	"Creating the broker component" on page 122
	"Checking APF attributes of bipimain on z/OS" on page 79
Performance specialist	"Defining the started tasks to z/OS Workload Manager (WLM)" on page 77
Security administrator	"Setting up z/OS security" on page 28

	"Setting up DB2" on page 29
	"Summary of required access (z/OS)"
	"Creating Publish/Subscribe user IDs" on page 31
Data administrator	"Setting up z/OS security" on page 28
	"Summary of required access (z/OS)"
	"Disk space requirements on z/OS" on page 376
	"Starting and stopping a broker on z/OS" on page 216
	"Using the file system on z/OS" on page 65
	"Binding a DB2 plan to use data-sharing groups on z/OS" on page 377

Some tasks, for example defining queue security, overlap two different roles.

Summary of required access (z/OS):

The following information summarizes the access that the professionals in your organization require.

Authorizations required for the WebSphere Event Broker started-task user ID:

The directory authorizations required for all components are:

- READ/EXECUTE access to <INSTPATH>, where <INSTPATH> is the directory where WebSphere Event Broker for z/OS is installed by SMP/E.
- READ/WRITE/EXECUTE access to the component directory ++COMPONENTDIRECTORY++.
- READ/WRITE access to the home directory.
- READ/WRITE access to the directory identified by ++HOME++.
- In UNIX System Services, the started task user ID and the WebSphere Event Broker administrator user ID must both be members of the groups that have access to the installation and component directories, because they both need privileges over these. The owner of these directories needs to give the appropriate permissions to this group.

The following PDSE and DB2 authorizations are required only for a broker component, that is, not a Configuration Manager or User Name Server

READ access to the component PDSE is required.

DB2 authorizations for the started task user ID and the table owner ID are required:

- If there is a profile for db2subsystem.RRSF in the DSNR class the started task user ID needs access to the profile. For example, the following RACF command shows whether the profile exists:

```
RLIST DSNR (DB2P.RRSF)
```

and the following command gives the required access:

```
PERMIT DB2P.RRSF CLASS(DSNR) ID(WQMITASK) ACCESS(READ)
```

- SELECT privilege on the tables SYSIBM.SYSTABLES, SYSIBM.SYSSYNONYMS, and SYSIBM.SYSDATABASE.
- SELECT, UPDATE, INSERT, and DELETE privileges on all broker system tables.

- DB2_TABLE_OWNER must be a valid authorization ID of the started task user ID.
- EXECUTE authority on the DSNACLI plan, or equivalent for the started task user ID.

WebSphere MQ authorizations:

Enable WebSphere MQ security to protect your WebSphere MQ resources. If all WebSphere MQ security switches are enabled, define the following profiles and give the started task user ID the listed access to each profile. For each profile access listed, <MQ_QMNAME> represents the WebSphere MQ queue manager that the WebSphere Event Broker component is connected to, and TASKID represents the WebSphere Event Broker started-task user ID.

- Connection security: READ access to profile <MQ_QMNAME>.BATCH of class MQCONN. For example, for queue manager MQP1 and started task ID TASKID, use the RACF commands:

```
RDEFINE MQCONN MQP1.BATCH UACC(NONE)
PERMIT MQP1.BATCH CLASS(MQCONN) ID(TASKID) ACCESS(READ)
```

- Queue security: UPDATE access to profile <MQ_QMNAME>.queue of class MQQUEUE for all queues. Consider creating profiles for the following queues:
 - All component queues using the generic profile SYSTEM.BROKER.**
 - Any transmissions queues defined between component queue managers.
 - Any queues defined in message flows.
 - Dead-letter queues.

For example, for queue manager MQP1 and started task ID TASKID, use the following RACF commands to restrict access to the component queues:

```
RDEFINE MQQUEUE MQP1.SYSTEM.BROKER.** UACC(NONE)
PERMIT MQP1.SYSTEM.BROKER.** CLASS(MQQUEUE) ID(TASKID) ACCESS(UPDATE)
```

- Context security: CONTROL access to profile <MQ_QMNAME>.CONTEXT of class MQADMIN. For example, for queue manager MQP1 and started task ID TASKID, use the following RACF commands:

```
RDEFINE MQADMIN MQP1.CONTEXT UACC(NONE)
PERMIT MQP1.CONTEXT CLASS(MQADMIN) ID(TASKID) ACCESS(CONTROL)
```

- Alternate user security: Define the alternate user authority as: UPDATE access to profile <MQ_QMNAME>.ALTERNATE.USER.id of class MQADMIN, where id represents the service ID of the Windows Configuration Manager component. For example, for queue manager MQP1, started task ID TASKID, and configuration service ID CFGID, use the following RACF commands:

```
RDEFINE MQADMIN MQP1.ALTERNATE.USER.CFGID UACC(NONE)
PERMIT MQP1.ALTERNATE.USER.CFGID CLASS(MQADMIN) ID(TASKID) ACCESS(UPDATE)
```

UPDATE access to profile <MQ_QMNAME>.ALTERNATE.USER.id of class MQADMIN, where id represents the user ID of, for example, a Publish/Subscribe request.

- Process and namelist security: If you have WebSphere MQ security switches enabled in your system for process and namelist security, you do not need to define any access profiles in a WebSphere Event Broker default configuration.

For users connecting remotely from either the Message Brokers Toolkit or from a Configuration Manager Proxy application to the Configuration Manager on z/OS the following authorizations are required :

- Connection security: READ access to profile <MQ_QMNAME>.CHIN of class MQCONN. For example, for queue manager MQP1 and started task ID TASKID, use the following RACF commands:

```
RDEFINE MQCONN MQP1.CHIN UACC(NONE)
PERMIT MQP1.CHIN CLASS(MQCONN) ID(TASKID) ACCESS(READ)
```

- Alternate user security: Define the alternate user authority as: UPDATE access to profile <MQ_QMNAME>.ALTERNATE.USER.id of class MQADMIN, where id represents the user ID of the Message Brokers Toolkit or Configuration Manager Proxy application. For example, for queue manager MQP1, started task ID TASKID, and user ID USERID, use the following RACF commands:

```
RDEFINE MQADMIN MQP1.ALTERNATE.USER.USERID UACC(NONE)
PERMIT MQP1.ALTERNATE.USER.USERID CLASS(MQADMIN) ID(TASKID) ACCESS(UPDATE)
```

Authorizations required for the WebSphere Event Broker administrator:

The broker administrator requires the following authorizations:

- ALTER access to the component PDSE.
- READ, WRITE, and EXECUTE access to the component directory ++COMPONENTDIRECTORY++.
- READ/EXECUTE access to <INSTPATH>, where <INSTPATH> is the directory where WebSphere Event Broker for z/OS is installed by SMP/E.
- READ/WRITE access to the directory identified by ++HOME++.
- In UNIX System Services, the started task user ID and the WebSphere Event Broker administrator user ID must both be members of the groups that have access to the installation and component directories, because they both need privileges over these. The owner of these directories needs to give the appropriate permissions to this group.
- To run the DB2 pass when creating and deleting components DBADM authority for the broker database is required.

Authorizations required for the DB2 administrator:

The DB2 administrator needs to have the following authorizations to run the DB2 configuration jobs BIPCRDB and BIPDLDB:

- ALTER access to the component PDSE.
- DB2 authorizations: SYSCTRL or SYSADM authority.
- CREATE STOGROUP, CREATE DATABASE, and CREATE TABLESPACES.
- DROP DATABASE and DROP STOGROUP.

If the DB2 administrator runs the DB2 pass when creating and deleting a component, the administrator user ID also needs the following authorizations. Alternatively, you can grant authorization to the WebSphere Event Broker administrator to run the DB2 pass.

- READ, WRITE, and EXECUTE access to the component directory ++COMPONENTDIRECTORY++.
- READ/EXECUTE access to <INSTPATH>, where <INSTPATH> is the directory where WebSphere Event Broker for z/OS is installed by SMP/E.
- READ/WRITE access to the directory identified by ++HOME++.
- In UNIX System Services, the started task user ID and the WebSphere Event Broker administrator user ID must both be members of the groups that have access to the installation and component directories, because they both need privileges over these. The owner of these directories needs to give the appropriate permissions to this group.

Authorizations required for the WebSphere MQ administrator:

If the WebSphere MQ administrator runs the WebSphere MQ pass when creating a component, the administrator user ID requires the following authorizations. Alternatively WebSphere MQ, you can grant authorization to the WebSphere Event Broker administrator to run the WebSphere MQ pass.

- ALTER access to the component PDSE.
- Directory authorizations:
 - READ/EXECUTE access to <INSTPATH>, where <INSTPATH> is the directory where WebSphere Event Broker for z/OS is installed by SMP/E.
 - READ, WRITE, and EXECUTE access to the component directory ++COMPONENTDIRECTORY++.
 - READ/WRITE access to the directory identified by ++HOME++.

Enable WebSphere MQ security to protect your WebSphere MQ resources. If all WebSphere MQ security switches are enabled, define the following profiles and give the WebSphere MQ administrator the listed access to each profile in order to run the WebSphere MQ configurations jobs. For each profile access listed, MQ_QMNAME represents the WebSphere MQ queue manager that the WebSphere Event Broker component is connected to, and MQADMIN represents the WebSphere MQ administrator ID:

- Connection security: READ access to profile <MQ_QMNAME>.BATCH of class MQCONN. For example, for queue manager MQP1 and WebSphere MQ administrator ID MQADMIN, use the following RACF commands:


```
RDEFINE MQCONN MQP1.BATCH UACC(NONE)
PERMIT MQP1.BATCH CLASS(MQCONN) ID(MQADMIN) ACCESS(READ)
```
- Queue security: UPDATE access to profile <MQ_QMNAME>.queue of class MQQUEUE for component queues created or deleted. You can create a generic profile SYSTEM.BROKER.** For example, for queue manager MQP1 and WebSphere MQ administrator ID MQADMIN, use the following RACF commands to restrict access to the component queues:


```
RDEFINE MQQUEUE MQP1.SYSTEM.BROKER.** UACC(NONE)
PERMIT MQP1.SYSTEM.BROKER.** CLASS(MQQUEUE) ID(MQADMIN) ACCESS(UPDATE)
```
- System command server: UPDATE access to profile <MQ_QMNAME>.queue of class MQQUEUE for SYSTEM.COMMAND.**. For example, for queue manager MQP1 and WebSphere MQ administrator ID MQADMIN, use the following RACF commands to restrict access to the system command server:


```
RDEFINE MQQUEUE MQP1.SYSTEM.COMMAND.** UACC(NONE)
PERMIT MQP1.SYSTEM.COMMAND.** CLASS(MQQUEUE) ID(MQADMIN) ACCESS(UPDATE)
```

UPDATE access to profile <MQ_QMNAME>.queue of class MQQUEUE for some system queues used during the create/delete job. You can create a generic profile <MQ_QMNAME>.**

- Command security:
 - To run the WebSphere MQ pass when creating a component you need:
 - ALTER access to <MQ_QMNAME>.DEFINE.QLOCAL of class MQCMDS.
 - ALTER access to <MQ_QMNAME>.DEFINE.QMODEL of class MQCMDS.
 - ALTER access to <MQ_QMNAME>.DEFINE.CHANNEL of class MQCMDS.
 - To run the WebSphere MQ pass when deleting a component you need:
 - ALTER access to <MQ_QMNAME>.DELETE.QLOCAL of class MQCMDS.
 - ALTER access to <MQ_QMNAME>.DELETE.QMODEL of class MQCMDS.
 - ALTER access to <MQ_QMNAME>.DELETE.CHANNEL of class MQCMDS.

For queue manager MQP1 and WebSphere MQ administrator ID MQADMIN, use the following RACF commands:

```
RDEFINE MQCMDS MQP1.DELETE.QLOCAL UACC(NONE)
PERMIT MQP1.DELETE.QLOCAL CLASS(MQCMDS) ID(MQADMIN) ACCESS(ALTER)
```

- Resource command security: ALTER access to MQP1.QUEUE.queue of class MQADMIN for each queue created or deleted. You can create a generic profile SYSTEM.BROKER.**. For example, for queue manager MQP1 and WebSphere MQ administrator ID MQADMIN, use the RACF commands:

```
RDEFINE MQADMIN MQP1.QUEUE.SYSTEM.BROKER.** UACC(NONE)
PERMIT MQP1.SYSTEM.BROKER.** CLASS(MQADMIN) ID(MQADMIN) ACCESS(ALTER)
```

- Process and namelist security: If you have WebSphere MQ security switches enabled in your system for process and namelist security, you do not need to define any access profiles in a WebSphere Event Broker default configuration.

For a description of how to implement WebSphere MQ security using RACF, see “Setting up WebSphere MQ” on page 30.

Authorizations required for the DB2 subsystem started-task user ID:

DB2 needs ALTER access to the catalog value specified in DB2_STOR_GROUP_VCAT because it creates data sets with this high-level qualifier.

Disk space requirements on z/OS

The WebSphere Event Broker for z/OS installation uses approximately 400 MB of disk space; you should plan on using 500 MB which will also allow for new service to be applied and also for the component directories.

When you apply service, if you do not replace your existing install (for example you apply the new fix pack level alongside your existing install) then you need to plan the same amount of disk space for the higher service level libraries.

If you are transferring the files using tar to package them, you need approximately 200 MB of space for the .tar file.

You can check how much space is used and how much is free in a file system using the OMVS command:

```
df -P /pathname
```

100 MB is 3 276 800 512 byte sectors.

The following table gives guidance on the space required for a minimum installation (base installation and verification test) of WebSphere Event Broker for z/OS components.

Component	Space required	Purpose
DB2 database (broker only)	6 MB	Holds the broker system tables.
Component directory	20 MB	Holds the runtime information and output directories for the component. This includes trace files and other user problem determination data, which can become large.

Component PDSE	1 MB	Holds the customization and administration jobs, procedures, and data for the component. The data set must be allocated with a fixed record length of 80 (LRECL=80) and a format of FB 80. Reserve directory space for 50 members, or use a PDSE if possible.
Started task user ID home directory	8 GB	Collect diagnostic materials, for example dumps. Dumps are usually more than 500MB in size. 8 GB of space needs to be available in the file system, but many user IDs can have their home directory in the file system.
The Component directory and the Started task user ID home directory must be different to ensure that, when dumps are taken in the Started task user ID home directory, they do not cause problems with the runtime broker that still needs to write to the Component directory.		

Binding a DB2 plan to use data-sharing groups on z/OS

During customization, you can specify which plan name to use, or use the default DSNACLI. If you are using XPLINK, the default plan is called DSNACLX. If you want your broker to access DB2 data-sharing groups other than its own, the DSNACLI plan must be bound in a special way. If the broker uses one data sharing group, but might want to access tables on DSNONE and DSNTWO, which are in different data-sharing groups, amend the DB2 supplied job DSNTIJCL to do the following:

```

BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLICS) ISOLATION(CS)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLINC) ISOLATION(NC)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIRR) ISOLATION(RR)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIRS) ISOLATION(RS)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIUR) ISOLATION(UR)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIC1)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIC2)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIF4)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIMS)
BIND PACKAGE (DSNAOCLI)MEMBER(DSNCLIQR)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLICS) ISOLATION(CS)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLINC) ISOLATION(NC)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIRR) ISOLATION(RR)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIRS) ISOLATION(RS)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIUR) ISOLATION(UR)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIC1)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIC2)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIF4)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIMS)
BIND PACKAGE (DSNONE.DSNAOCLI)MEMBER(DSNCLIQR)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLICS) ISOLATION(CS)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLINC) ISOLATION(NC)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIRR) ISOLATION(RR)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIRS) ISOLATION(RS)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIUR) ISOLATION(UR)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIC1)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIC2)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIF4)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIMS)
BIND PACKAGE (DSNTWO.DSNAOCLI)MEMBER(DSNCLIQR)
BIND PLAN(DSNACLI)-
PKLIST(*.DSNAOCLI.DSNCLICS -

```

```

*.DSNAOCLI.DSNCLINC -
*.DSNAOCLI.DSNCLIRR -
*.DSNAOCLI.DSNCLIRS -
*.DSNAOCLI.DSNCLIUR -
*.DSNAOCLI.DSNCLIC1 -
*.DSNAOCLI.DSNCLIC2 -
*.DSNAOCLI.DSNCLIF4 -
*.DSNAOCLI.DSNCLIMS -
*.DSNAOCLI.DSNCLIQR )

```

Customization planning checklist for z/OS

Use the information contained in the following tables to make a note of the values to use when you customize your system variables. For further information, see:

- “Installation information - broker and User Name Server” on page 117
- “Installation information - Configuration Manager” on page 130
- “DB2 information” on page 117
- “Component information - broker” on page 118
- “Component information - Configuration Manager” on page 131
- “Component information - User Name Server” on page 140

Contents of the broker PDSE

Broker PDSE members originating in <hlq>.SBIPSAMP

After successfully customizing the broker, the members in your broker PDSE are as follows:

Description	Name
Broker profile	BIPBPROF
Job to run the broker DB2 database backup	BIPBUDB
Broker DB2 dsnaoini file “Sample BIPDSNAO file” on page 413 lists the shipped BIPDSNAO file.	BIPDSNAO
Job to run the broker DB2 database QUIESCE	BIPQSDB
Job to run the broker DB2 database report	BIPRPDB
Job to run the broker DB2 database restore	BIPRSDB
Job to run the broker DB2 run statistics example	BIPRUNST

Broker PDSE members originating in <hlq>.SBIPPROC

Description	Name
Commented sample job to identify database resources, including tables and table spaces for performance tuning purposes	BIPALDB
Commented sample job to identify WebSphere MQ resources, including queues for performance tuning purposes	BIPALMQ
Job to run mqsibrowse command	BIPBRWS
Job to run the mqsichangebroker command	BIPCHBK
Job to run the mqsichangeflowstats command	BIPCHMS
Job to run the mqsichangeproperties command	BIPCHPR

Removes anMQSeries Publish/Subscribe broker as a neighbor; runs the mqsiclearmqpubsub command	BIPCLMP
Job to run the mqsi createbroker command to: <ul style="list-style-type: none"> • Create the DB2 tables • Create the WebSphere MQ resources • Create the broker registry “Sample BIPCBRK file” on page 394 lists the shipped BIPCBRK file.	BIPCRBK
Job to create the DB2 storage group, database and table spaces. “Sample BIPCRDB file” on page 403 lists the shipped BIPCRDB file.	BIPCRDB
Job to run the mqsi deletebroker command	BIPDLBK
Job to drop the DB2 database and storage groups	BIPDLDB
Edit macro for customization. Rename BIPEDIT to a unique name that identifies it to the current component; for example, MQ01EDBK “Sample BIPEDIT file” on page 414 lists the shipped BIPEDIT file.	BIPEDIT (MQP1BRK)
Job to run the mqsi formatlog command.	BIPFMLG
Job to convert BIPBPROF profile to a valid ENVFILE. “Sample BIPGEN file” on page 415 lists the shipped BIPGEN file.	BIPGEN
Job to run the mqsi joinmqpubsub command	BIPJNMP
Job to run the mqsi list command	BIPLIST
Job to run the mqsi listmqpubsub command	BIPLSMP
Job to change DB2 definitions when migrating from Version 2.1 to Version 6.0	BIPMGTB
Job to run the mqsi readlog command.	BIPRELG
Job to run the mqsi reportflowstats command	BIPRPMS
Job to run the mqsi reportproperties command	BIPRPPR
Job to define a data source, user ID, and password for user data sources.	BIPSDBP
(started task). Rename BIPBRKP to the same as the ++STARTEDTASKNAME++ . “Sample BIPBRKP file” on page 390 lists the shipped BIPBRKP file.	BIPBRKP

Use the standard z/OS IPCS facilities to take a dump. You require access to the following:

- COMPONENT_PDSE
- ComponentDirectory
- SYS1.MIGLIB
- SYS1.SBLSCLI0
- SYS1.PARMLIB
- IPCS

Contents of the User Name Server PDSE

After successfully customizing the User Name Server, the members in your User Name Server PDSE are as follows:

User Name Server PDSE members originating in <hlq>.SBIPSAMP

Description	Name
User Name Server profile "Sample BIPUPROF file" on page 419 lists the shipped BIPUPROF file.	BIPUROF

User Name Server PDSE members originating in <hlq>.SBIPPROC

Description	Name
Commented sample job to identify WebSphere MQ resources, including queues for performance tuning purposes	BIPALMQ
Job to run the mqsichangeusernameserver command.	BIPCHUN
Job to run the mqsicreateusernameserver command to: <ul style="list-style-type: none"> • Create the WebSphere MQ resources • Create the User Name Server registry "Sample BIPCRUN file" on page 411 lists the shipped BIPCRUN file.	BIPCRUN
Job to run the mqsdeleteusernameserver command.	BIPDLUN
Edit macro for customization. Rename BIPEDIT to a unique name that identifies it to the current component; for example, MQ01EDUN. "Sample BIPEDIT file" on page 414 lists the shipped BIPEDIT file.	BIPEDIT
Job to run the mqsiformatlog command.	BIPFMLG
Generate ENVFILE. "Sample BIPGEN file" on page 415 lists the shipped BIPGEN file.	BIPGEN
Job to run the mqsilist command.	BIPLIST
Job to run the mqsireadlog command.	BIPRELG
Started task. Rename BIPUNSP to the same as the ++STARTEDTASKNAME++ . "Sample BIPUNSP file" on page 417 lists the shipped BIPUNSP file.	BIPUNSP

Use the standard z/OS IPCS facilities to take a dump. You require access to the following:

- COMPONENT_PDSE
- ComponentDirectory
- SYS1.MIGLIB
- SYS1.SBLSCLI0
- SYS1.PARMLIB
- IPCS

Contents of the Configuration Manager PDSE

After successfully customizing the Configuration Manager, the members in your Configuration Manager PDSE are as follows:

Configuration Manager PDSE members originating in <hlq>.SBIPSAMP

Description	Name
Configuration Manager profile "Sample BIPCPROF file" on page 398 lists the shipped BIPCPROF file.	BIPCPROF

Configuration Manager PDSE members originating in <hlq>.SBIPPROC

Description	Name
Commented sample job to identify WebSphere MQ resources, including queues for performance tuning purposes	BIPALMQ
Job to run the mqsibackupconfigmgr command	BIPBUCM
Job to run the mqsichangeconfigmgr command	BIPCHCM
Job to run the mqsicreateaclentry command	BIPCRACL
Job to run the mqsicreateconfigmgr command to: <ul style="list-style-type: none"> • Create the WebSphere MQ resources • Create the Configuration Manager registry "Sample BIPCRCM file" on page 401 lists the shipped BIPCRCM file.	BIPCRCM
Job to run the mqsicreateexecutiongroup command	BIPCREG
Job to run the mqsdeleteaclentry command	BIPDLACL
Job to run the mqsdeleteconfigmgr command	BIPDLCM
Job to run the mqsdeleteexecutiongroup command	BIPDLEG
Job to run the mqsdeploy command	BIPDPLY
Edit macro for customization. Rename BIPEDIT to a unique name that identifies it to the current component; for example, MQ01EDCM. "Sample BIPEDIT file" on page 414 lists the shipped BIPEDIT file.	BIPEDIT
Job to run the mqsiformatlog command.	BIPFMLG
Job to convert BIPCPROF profile to a valid ENVFILE. "Sample BIPGEN file" on page 415 lists the shipped BIPGEN file.	BIPGEN
Job to run the mqsilistaclentry command	BIPLIACL
Job to run the mqsilist command	BIPLIST
Job to run the mqsireadlog command.	BIPRELG
Job to run the mqsirestoreconfigmgr command	BIPRSCM
Job to run the mqsistopmsgflow command	BIPSPMF
Job to run the mqsistartmsgflow command	BIPSTMF
Started task. Rename BIPCMGRP to the same as the ++STARTEDTASKNAME++ . "Sample BIPCMGRP file" on page 396 lists the shipped BIPCMGRP file.	BIPCMGRP

Use the standard z/OS IPCS facilities to take a dump. You require access to the following:

- COMPONENT_PDSE
- ComponentDirectory
- SYS1.MIGLIB
- SYS1.SBLSCLI0
- SYS1.PARMLIB
- IPCS

z/OS JCL variables

The following table lists all the JCL variables that you can customize in alphabetical order, together with a description and an example value.

JCL variable	Description	Example value
++ARM++	Specifies if a component should use Automatic Restart Management (ARM).	YES
++ARMNAME++	ARM name. Required if ++ARM++ is set to YES.	Q482BRK
++ARMTYPE++	ARM type. Required if ++ARM++ is set to YES.	SYSWMQI
++COMPONENTDATASET++	The dataset where all JCL relevant to a particular component is saved.	TESTDEV.MQP1BRK.BROKER
++COMPONENTDIRECTORY++	The file system directory where the component exists. This directory includes subdirectories, for example, /log and /registry	mqs/brokers/MQP1BRK
++COMPONENTNAME++	The name you give the component when you create it.	MQP1BRK
++COMPONENTPROFILE++	Profile name.	BIPBPROF, BIPCPROF, or BIPUPROF
++COMPONENTRESOURCE++	Required specifically by BIPBRWS. It represents the resource to be displayed.	BNBRCONNECTIONS
++DB2BUFFERPOOL++	The name of the DB2 buffer pool associated with the component for which the JCL is submitted.	BP0
++DB2CONVERSION++	Specifies the DB2 Converter.	SINGLE
++DB2CURRENTSQLID++	The DB2 user ID for the component and commands.	MQP1BRK

JCL variable	Description	Example value
++DB2DATABASE++	The name of the DB2 database associated with the component for which the JCL is submitted.	DMQP1BRK
++DB2HLQ++	DB2 high-level-qualifier	SYS2.DB2.V710
++DB2INDEXBP++	DB2 index bufferpool	BP0
++DB2LOBBP++	DB2 LOB table bufferpool	BP0
++DB2LOCATION++	The DB2 location value of the DB2 subsystem to which the component connects.	DSN710PK
++DB2PLAN++	The DB2 plan value.	DSNTEP71
++DB2PLANNAME++	The DB2 plan name.	DSNACLI
++DB2PROGRAM++	The DB2 program value.	DSNTEP2
++DB2RUNLIB++	The DB2 run library value.	DSN710PK.RUNLIB.LOAD
++DB2STORAGEGROUP++	The name of the DB2 storage group associated with the component for which the JCL is submitted.	MQP1STOR
++DB2SUBSYSTEM++	The DB2 subsystem ID which the component connects.	DFK4
++DB2TABLEOWNER++	Broker tables schema name.	MQP1BRK
++EXECUTIONGROUPNAME++	The name of an execution group.	Default
++HOME++	The file system home directory for the component's user ID. This is required to dynamically generate the ENVFILE from BIPBPROF, and is also used for STDOUT and STDERR output. You must have the appropriate RACF authorities to write to this file system directory when submitting JCL to run a command.	/u/mqp1brk
++INSTALL++	The directory where you install the product.	/usr/lpp/mqsi

JCL variable	Description	Example value
++JAVA++	Location of Java installation.	/usr/lpp/java/IBM/J1.4
++LANGLETTER++	The letter for the language in which you want messages shown.	E (English)
++LOCALE++	Locale of environment where commands are run by submitting JCL.	C
++MESSAGECASE++	Determines if messages should appear in mixed case.	YES
++MQPATH++	WebSphere MQ location	/usr/lpp/mqm
++NEIGHBOURQUEUEMANAGER++	Required specifically by BIPCLMP for the mqsiclearmqpubsub command. It represents the name of the neighboring QueueManager	MQP1
++OBJECTNAME++	Required specifically by BIPRPPR for the mqsireportproperties command. It represents the name of the object.	DynamicSubscriptionEngine
++OPTIONS++	Many commands submitted by JCL require additional options. See each command's reference material for additional information on options specific to that command.	N/A
++PARENTQUEUEMANAGERNAME++	Required specifically by BIPJNMP for the mqsijoinmqpubsub command. It represents the name of the parent QueueManager.	MQP1
++PROPERTYNAME++	Required specifically by BIPCHPR for the mqsichangeproperties command. It represents the name of the property to be changed.	multicastEnabled

JCL variable	Description	Example value
++PROPERTYVALUE++	Required specifically by BIPCHPR for the mqschangeproperties command. It represents the new value of the property to be changed.	false
++QUEUEMANAGER++	The name of the QueueManager associated with the component for which you submit the JCL.	MQP1
++STARTEDTASKNAME++	Name of the Started Task JCL. This can be a maximum of 8 characters.	MQP1BRK
++TIMEZONE++	Time zone of environment where commands are run by submitting JCL.	GMT0BST
++WMQHLQ++	WebSphere MQ high-level-qualifier	MQM.V531
++XMLTOOLKIT++	IBM XML Toolkit location	/usr/lpp/ixm/IBM/xml4c-5_5

z/OS sample files supplied

The following files are provided as sample source that you can customize:

- “Sample BIPBPROF file”
- “Sample BIPBRKP file” on page 390
- “Sample BIPCBRK file” on page 394
- “Sample BIPCMGRP file” on page 396
- “Sample BIPCPROF file” on page 398
- “Sample BIPCRCM file” on page 401
- “Sample BIPCRDB file” on page 403
- “Sample BIPCRUN file” on page 411
- “Sample BIPDSNAO file” on page 413
- “Sample BIPEDIT file” on page 414
- “Sample BIPGEN file” on page 415
- “Sample BIPUNSP file” on page 417
- “Sample BIPUPROF file” on page 419

Sample BIPBPROF file

```

*****
#*
#* @START_COPYRIGHT@
#*
#* Licensed Materials - Property of IBM;
#* 5655-G97 (c) Copyright IBM Corp. 2004;
#* All Rights Reserved;
#* US Government Users Restricted Rights - use,

```

```

** duplication or disclosure restricted by GSA *
** ADP Schedule Contract with IBM Corp.; *
** See Copyright Instructions *
** *
** @END_COPYRIGHT@ *
** *
*****
** IBM WebSphere Event/Message Brokers *
** *
** Sample profile for a broker. *
** *
*****
** MORE INFORMATION - See: *
** *
** WebSphere Event/Message Brokers Information Centre. *
** *
** IMPORTANT: *
** *
** You must submit BIPGEN each time you update this profile! *
** *
*****
** CUSTOMIZE HERE FOR YOUR INSTALLATION
** YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
** *
** Replace ++INSTALL++
** WBI Brokers installation directory.
** e.g. '/usr/lpp/mqsi'
**
** Replace ++COMPONENTDIRECTORY++
** Broker directory.
** e.g. '/mqsi/brokers/MQ01BRK'
**
** Replace ++COMPONENTDATASET++
** Component dataset.
** e.g. 'BIP.BROKER.MQ01BRK'
**
** Replace ++COMPONENTNAME++
** Broker name.
** e.g. 'MQ01BRK'
**
** Replace ++LOCALE++
** Locale.
** e.g. 'C'
**
** Replace ++TIMEZONE++
** Time zone.
** e.g. 'GMT0BST'
**
** Replace ++JAVA++
** Java location.
** e.g. '/usr/lpp/java/IBM/J1.4'
**
** Replace ++XMLTOOLKIT++
** IBM XML Toolkit location.
** e.g. '/usr/lpp/ixm/IBM/xml4c-5_5'
**
** Replace ++DB2CONVERSION++
** Specifies the DB2 Converter.
** e.g. 'SINGLE'
**
** Replace ++DB2DATABASE++
** Needed by the mqsicreatebroker command to
** determine the DB2 database.
** e.g. 'DMQ01BRK'
**
** Replace ++DB2STORAGEGROUP++
** Needed by the mqsicreatebroker command to

```



```

#*                determine the DB2 storagegroup.
#*                e.g. 'MQ01STOR'
#*
#*****
# 1. Component Settings
#*****
#
# 1.1 MQSI_REGISTRY references the component path. Also needed by
#      commands.
#      e.g. MQSI_REGISTRY=/mqsi/brokers/MQ01BRK
#
# 1.2 MQSI_COMPONENT_NAME is set to the broker name.
#      e.g. MQSI_COMPONENT_NAME=MQ01BRK
#
# 1.3 MQSI_FILEPATH needed by commands to reference the component
#      version install path.
#      e.g. MQSI_FILEPATH=usr/lpp/mqsi/V6R0M0
#
# 1.4 MQSI_LILPATH needed by components to find LILs
#      e.g. MQSI_FILEPATH=usr/lpp/mqsi/V6R0M0/li1
#
export MQSI_REGISTRY=++COMPONENTDIRECTORY++
export MQSI_COMPONENT_NAME=++COMPONENTNAME++
export MQSI_FILEPATH=++INSTALL++
export MQSI_LILPATH=$MQSI_FILEPATH/li1

#*****
# 2. NLS Settings
#*****
#
# 2.1 LANG and LC_ALL determine in which locale the component
#      will run.
#      e.g. LANG=Ja_JP.IBM-939 and LC_ALL=Ja_JP.IBM-939 for
#           japanese locale.
#           LANG=C, LC_ALL=C for US English locale.
#
# 2.2 TZ has the timezone setting in which you are located.
#      e.g. TZ=EST5                for USA Eastern Standard Time
#           TZ=MEZ-1MES,M3.5.0,M10.5.0 for Central Europe
#           TZ=GMT0BST             for the UK
#           Please refer to the IBM Manual
#           "Unix System Services Command Reference SC28-1892.
#
# 2.3 NLSPATH contains the location of the message catalog(s).
#      (NO NEED TO CHANGE FROM DEFAULT!)
#
# 2.4 MQSI_CONSOLE_NLSPATH is used to locate the messages for
#      the console.
#      For Japanese or S-Chinese messages, change En_US to
#      Ja_JP or Zh_CN below. For English messages these can be
#      displayed in mixed or upper case only. (see MC_MESSAGES)
#      Note that MQSI_CONSOLE_NLSPATH does not use %L or %N
#
export LANG=++LOCALE++
export LC_ALL=++LOCALE++
export TZ=++TIMEZONE++
export NLSPATH=$MQSI_FILEPATH/messages/%L/%N
export NLSPATH=$NLSPATH:$MQSI_FILEPATH/nnsy/MIF/messages/%N
export MQSI_CONSOLE_NLSPATH=$MQSI_FILEPATH/messages/En_US

#*****
# 3. Automatic Restart Management (ARM) Settings
#*****
#
# 3.1 MQSI_USE_ARM specifies whether to use ARM.

```

```

# e.g. MQSI_USE_ARM=YES for ARM enabled.
# MQSI_USE_ARM=NO for ARM not enabled.
#
# 3.2 MQSI_ARM_ELEMENTNAME required if ARM enabled.
#
# 3.3 MQSI_ARM_ELEMENTTYPE required if ARM enabled.
#
export MQSI_USE_ARM=NO
export MQSI_ARM_ELEMENTNAME=++COMPONENTNAME++
export MQSI_ARM_ELEMENTTYPE=

#*****
# 4. DB2 Settings
#*****
#
# 4.1 MQSI_DB2_ALWAYS_PREPARE
# (NO NEED TO CHANGE FROM DEFAULT!)
#
# 4.2 MQSI_DB2_CONVERSION specifies the DB2 Converter.
# e.g. MQSI_DB2_CONVERSION=SINGLE
# WBIMB uses a SQL_EBCDIC_SCCSID to determine
# the DB2 converter.
# Note that this setting reflects the current
# WBIMB behavior.
# MQSI_DB2_CONVERSION=MIXED
# WBIMB uses SQL_EBCDIC_MCCSID to determine
# the DB2 converter.
# Note that this setting requires that DB2 is
# configured to accept mixed byte data. This
# setting should be used when the customer
# wants data to be stored in the configured
# DB2 EBCDIC mixed byte code page.
# MQSI_DB2_CONVERSION=LOCAL
# WBIMB uses localConverter identified by
# LC_ALL/LANG settings. This complies to what
# is done on distributed. This setting
# requires that WBIMB and DB2 are using the same
# codepage, otherwise only WBIMB can read DB2
# data correctly, it gets unreadable for other
# ( non-WBIMB ) applications that want to read
# the data.
#
# 4.3 MQSI_DB2_DATABASE needed by the mqsicreatebroker command to
# determine the DB2 database.
# e.g. MQSI_DB2_DATABASE=DMQ01BRK
#
# 4.4 MQSI_DB2_STORAGEGROUP needed by the mqsicreatebroker command
# to determine the DB2 storagegroup.
# e.g. MQSI_DB2_STORAGEGROUP=MQ01STOR
#
# 4.5 DSNA0INI references the component dsnaoini file.
# (NO NEED TO CHANGE FROM DEFAULT!)
#
export MQSI_DB2_ALWAYS_PREPARE=NO
export MQSI_DB2_CONVERSION=++DB2CONVERSION++
export MQSI_DB2_DATABASE=++DB2DATABASE++
export MQSI_DB2_STORAGEGROUP=++DB2STORAGEGROUP++
export DSNA0INI=/'\'+COMPONENTDATASET+\(BIPDSNAO)\'

#*****
# 5. Java Settings
#*****
#
# 5.1 JAVAHOME contains the root directory of the JAVA install.
# e.g. JAVAHOME=/usr/lpp/java/IBM/J1.4
# Note that the Java version must be at least 1.4.1

```

```

#
export JAVAHOME=++JAVA++

#*****
# 6. DistHub Settings
#*****
#
# 6.1 DISTHUB_PATH is the path to DistHub product executables
#     (NO NEED TO CHANGE DEFAULT UNLESS USING A NON-STANDARD
#     INSTALLATION PATH FOR DISTHUB!)
#
export DISTHUB_PATH=$MQSI_FILEPATH

#*****
# 7. Message Broker with Rules and Formatter Extensions Settings
#*****
#
# 7.1 NNSY_ROOT references NNSY executables.
#     (NO NEED TO CHANGE FROM DEFAULT!)
#
# 7.2 NNSY_CATALOGUES references NNSY catalogues.
#     (NO NEED TO CHANGE FROM DEFAULT!)
#
# 7.3 NN_CONFIG_FILE_PATH default location of nnsyreg.dat
#     configuration file.
#     Regardless of where NN_CONFIG_FILE_PATH points, the first
#     place that will be checked for the nnsyreg.dat files, is
#     $MQSI_FILEPATH/bin. Any nnsyreg.dat file in this directory
#     will be used, even if another exists in the location pointed
#     to by the NN_CONFIG_FILE_PATH environment variable. It is
#     recommended that any instances of the nnsyreg.dat in the
#     $MQSI_FILEPATH/bin directory be removed, and placed in
#     environment specific locations, to preserve multi-user
#     capability.
#     e.g. NN_CONFIG_FILE_PATH=/usr/lpp/NNSY/bin
#
# See documentation supplied with Rules and Formatter
# Extensions for further information.
#
export NNSY_ROOT=$MQSI_FILEPATH/nnsy
export NNSY_CATALOGUES=$MQSI_FILEPATH/nnsy/NNSYCatalogues/en_US
export NN_CONFIG_FILE_PATH=

#*****
# 8. WBI Broker Settings
#*****
#
# 8.1 _BPX_BATCH_SPAWN
#     (MUST NOT CHANGE FROM DEFAULT!)
#
# 8.2 MQSI_MC_MESSAGES determines if messages should appear in
#     mixed case or upper case.
#     e.g. MQSI_MC_MESSAGES=YES for mixed case
#         MQSI_MC_MESSAGES=NO for upper case
#
# 8.3 MQSI_COMMAND_DATABASE_ECHO if defined, mqsi commands
#     display information when creating DB2 tables/indexes.
#
# 8.4 MQSI_COMMAND_ZOS_MQ_ECHO if defined, mqsi commands display
#     information returned from the MQ command server when
#     creating/deleting queues.
#
# 8.5 MQSI_COMMAND_ZOS_MQ_ECHO_RC if defined, mqsi commands display
#     reason and return codes from the MQ command server when

```

```

#      creating/deleting queues.
#
# 8.6 MQSI_DEPLOY_PROGRESS if defined, shows deployment progress
#      by the execution group
#
# 8.7 STEPLIB
#      (MUST NOT CHANGE FROM DEFAULT!)
#
export _BPX_BATCH_SPAWN=NO
export MQSI_MC_MESSAGES=NO
export MQSI_COMMAND_DATABASE_ECHO=1
export MQSI_COMMAND_ZOS_MQ_ECHO=1
export MQSI_COMMAND_ZOS_MQ_ECHO_RC=1
export MQSI_DEPLOY_PROGRESS=1
export STEPLIB=CURRENT

#*****
# 9. Other Settings
#*****
#
# NO NEED TO CHANGE FROM DEFAULT!
#
CP=$MQSI_FILEPATH/classes
CP=$CP:$MQSI_FILEPATH/classes/config.jar
CP=$CP:$MQSI_FILEPATH/classes/ConfigManagerProxy.jar
CP=$CP:$MQSI_FILEPATH/classes/ConfigManagerProxySamples.jar
CP=$CP:$MQSI_FILEPATH/classes/configutil.jar
CP=$CP:$JAVAHOME/lib
CP=$CP:$MQSI_FILEPATH/messages
export CLASSPATH=$CP
export ICU_DATA=$MQSI_FILEPATH/nnsy/lib
XMLTOOLKIT=++XMLTOOLKIT++
LP=$MQSI_FILEPATH/lib/wbirf
LP=$LP:$MQSI_FILEPATH/lib/wbimb
LP=$LP:$MQSI_FILEPATH/lib/wbieb
LP=$LP:$MQSI_FILEPATH/lib
LP=$LP:$MQSI_FILEPATH/nnsy/lib
LP=$LP:$MQSI_FILEPATH/nnsy/MIF/lib
LP=$LP:$JAVAHOME/lib
LP=$LP:$JAVAHOME/bin
LP=$LP:$JAVAHOME/bin/classic
LP=$LP:$XMLTOOLKIT/lib
export LIBPATH=$LP
export PATH=$MQSI_FILEPATH/bin
export PATH=$PATH:$MQSI_FILEPATH/nnsy/bin
export PATH=$PATH:/bin
export PATH=$PATH:$JAVAHOME/bin

```

Sample BIPBRKP file

```

| //*****
| //*
| //* @START_COPYRIGHT@
| //*
| //* Licensed Materials - Property of IBM;
| //* 5655-G97 (c) Copyright IBM Corp. 2004;
| //* All Rights Reserved;
| //* US Government Users Restricted Rights - use,
| //* duplication or disclosure restricted by GSA
| //* ADP Schedule Contract with IBM Corp.;
| //* See Copyright Instructions
| //*
| //* @END_COPYRIGHT@
| //*
| //*****
| //*          IBM WebSphere Event/Message Brokers
| //*

```

```

|  /** Sample job to start a broker.                *
|  /**                                              *
|  /*******
|  /** MORE INFORMATION - See:                    *
|  /**                                              *
|  /**      WebSphere Event/Message Brokers Information Centre.
|  /**                                              *
|  /*******
|  /** CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
|  /** YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
|  /**                                              *
|  /**      Replace  ++HOME++
|  /**              Home directory where ENVFILE and STDERR
|  /**              and STDOUT files will be created.
|  /**              e.g. '/u/home'
|  /**
|  /**      Replace  ++INSTALL++
|  /**              WBI Brokers installation directory.
|  /**              e.g. '/usr/lpp/mqsi'
|  /**
|  /**      Replace  ++QUEUEMANAGER++
|  /**              Queue manager name.
|  /**              e.g. 'MQ01'
|  /**
|  /**      Replace  ++COMPONENTDIRECTORY++
|  /**              Broker directory.
|  /**              e.g. '/mqsi/brokers/MQ01BRK'
|  /**
|  /**      Replace  ++STARTEDTASKNAME++
|  /**              Started Task Name (max 8 chars uppercase).
|  /**              e.g. 'MQ01BRK'
|  /**
|  /**      Replace  ++COMPONENTDATASET++
|  /**              Broker dataset.
|  /**              e.g. 'BIP.BROKER.MQ01BRK'
|  /**
|  /**      Replace  ++DB2HLQ++
|  /**              DB2 high-level-qualifier.
|  /**              e.g. 'SYS2.DB2.V710'
|  /**
|  /**      Replace  ++DB2RUNLIB++
|  /**              DB2.
|  /**              e.g. 'DSN710PK.RUNLIB.LOAD'
|  /**
|  /**      Replace  ++WMQHLQ++
|  /**              WebSphere MQ high-level-qualifier.
|  /**              e.g. 'MQM.V531'
|  /**
|  /**      Replace  ++WMBHLQ++
|  /**              WebSphere Message Broker
|  /**              high-level-qualifier.
|  /**
|  /**              ONLY NEEDED IF USING EVENT NOTIFICATION
|  /**
|  /**              e.g. 'MB.V6R0M0'
|  /**
|  /*******
|  /**
|  /** Following variables are changed when starting a DataFlowEngine:
|  /**      STDOUT and STDERR files
|  /**      STDD=OAPPEND (default is OTRUNC)
|  /**      Semaphore ID
|  /**      SE=<Semaphore ID> (default is '')
|  /**      Shared Memory Segment ID
|  /**      SH=<Shared Memory Segment ID> (default is '')
|  /**      Component Unique Name
|  /**      COMPK='' (default is ++STARTEDTASKNAME++)

```

```

|  /*      Start Parameter
|  /*      STRTP=' ' (default is 'AUTO')
|  /*
|  /******
|  /*
|  /*++STARTEDTASKNAME++ PROC INSTP='++INSTALL++',
|  /*      MAINP='bipmain',
|  /*      SRVMP='bipservice',
|  /*      COMPK='++STARTEDTASKNAME++',
|  /*      COMDS='++COMPONENTDATASET++',
|  /*      STRTP='AUTO',
|  /*      COMPDIR='++COMPONENTDIRECTORY++',
|  /*      STDD='OAPPEND',
|  /*      SE=' ',
|  /*      SH=' ',
|  /*      HOME='++HOME++',
|  /*      DB2HLQ='++DB2HLQ++',
|  /*      WMQHLQ='++WMQHLQ++'
|  /*
|  /******
|  /* Copy ENVFILE to SYSOUT
|  /******
|  /*
|  /*COPYENV EXEC PGM=IKJEFT01,
|  /*      PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
|  /*SYSTSPRT DD DUMMY
|  /*BIPFROM DD PATHOPTS=(ORDONLY),
|  /*      PATH='&HOME./ENVFILE'
|  /*ENVFILE DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
|  /*SYSTSIN DD DUMMY
|  /*
|  /******
|  /* Copy DSNAOINI to SYSOUT
|  /******
|  /*
|  /*COPYDSN EXEC PGM=IKJEFT01,
|  /*      PARM='OCOPY INDD(BIPFROM) OUTDD(DSNAOINI)'
|  /*SYSTSPRT DD DUMMY
|  /*BIPFROM DD DISP=SHR,DSN=&COMDS.(BIPDSNAO)
|  /*DSNAOINI DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
|  /*SYSTSIN DD DUMMY
|  /*
|  /******
|  /* Test to see if starting a DataFlowEngine address space.
|  /* Should return RC=0 if starting a Control address space or
|  /* UserNameServer address space, RC=12 if starting a DataFlowEngine
|  /* address space.
|  /******
|  /*
|  /*CHECKDFE EXEC PGM=IKJEFT01,
|  /*      PARM='LISTDS ''&COMDS.&SE. '''
|  /*SYSTSIN DD DUMMY
|  /*SYSTSPRT DD DUMMY
|  /*SYSDUMP DD SYSOUT=*
|  /*
|  /*      IF (RC=0) THEN
|  /*
|  /******
|  /* Broker DB2 and MQ verification
|  /******
|  /*
|  /*VFYDB2MQ EXEC PGM=BXPBATS,REGION=0M,TIME=NOLIMIT,
|  /*      PARM='PGM &INSTP./bin/bipcvp b ++QUEUEMANAGER++'
|  /*
|  /*      DB2 Runtime Libraries
|  /*STEPLIB DD DISP=SHR,DSN=&DB2HLQ..SDSNEXIT
|  /*      DD DISP=SHR,DSN=&DB2HLQ..SDSNLOAD
|  /*      DD DISP=SHR,DSN=&DB2HLQ..SDSNL0D2

```

```

| //          DD DISP=SHR,DSN=++DB2RUNLIB++
| /*          MQSeries Runtime Libraries
| //          DD DISP=SHR,DSN=&WMQHLQ..SCSQANLE
| //          DD DISP=SHR,DSN=&WMQHLQ..SCSQAUTH
| //          DD DISP=SHR,DSN=&WMQHLQ..SCSQLOAD
| //STDENV   DD PATH='&HOME./ENVFILE'
| //STDOUT   DD SYSOUT=*
| //STDERR   DD SYSOUT=*
| //SYSMDUMP DD SYSOUT=*
| //
| //          ENDIF
| //
| //*****
| /* Check RCs from previous steps
| //*****
| //
| //          IF (CHECKDFE.RC NE 0) OR
| //              (VFYDB2MQ.RC EQ 0) THEN
| //
| //*****
| /* Step to delete residual locks
| /* (this is only needed if the broker is ARM enabled)
| //*****
| //
| /*RMLOCKS EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
| /*          PARM='SH rm -f &COMPDIR./common/locks/*'
| //
| //*****
| /* Start either :
| /* Control Address Space (bipimain, bipservice and bipbroker)
| /* DataFlowEngine Address Space (bipimain and DataFlowEngine)
| //*****
| //
| //BROKER   EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
| //          PARM='PGM &INSTP./bin/&MAINP. &SRVMP. &SE. &SH. &COMPK.
| //          &STRTP.'
| //
| /*          DB2 Runtime Libraries
| //STEPLIB DD DISP=SHR,DSN=&DB2HLQ..SDSNEXIT
| //          DD DISP=SHR,DSN=&DB2HLQ..SDSNLOAD
| //          DD DISP=SHR,DSN=&DB2HLQ..SDSNLOD2
| //          DD DISP=SHR,DSN=++DB2RUNLIB++
| //
| /*          MQSeries Runtime Libraries
| //          DD DISP=SHR,DSN=&WMQHLQ..SCSQANLE
| //          DD DISP=SHR,DSN=&WMQHLQ..SCSQAUTH
| //          DD DISP=SHR,DSN=&WMQHLQ..SCSQLOAD
| //
| /*          APF Authorized Library of Message Broker
| //
| /*          Required if using Event Notification
| //
| /*          (All librarys in concatenation
| //
| /*          need to be APF authorized)
| //
| //          DD DISP=SHR,DSN=++WMBHLQ++.SBIPAUTH
| //STDENV   DD PATH='&HOME./ENVFILE'
| //STDOUT   DD PATHOPTS=(OWRONLY,OCREAT,&STDD),
| //          PATHMODE=(SIRWXU,SIRWXG),
| //          PATH='&COMPDIR./output/stdout'
| //STDERR   DD PATHOPTS=(OWRONLY,OCREAT,&STDD),
| //          PATHMODE=(SIRWXU,SIRWXG),
| //          PATH='&COMPDIR./output/stderr'
| //SYSMDUMP DD SYSOUT=*
| //
| //*****
| /* Copy stdout to SYSOUT
| //*****
| //
| //COPYOUT  EXEC PGM=IKJEFT01,COND=EVEN,
| //          PARM='OCOPY INDD(BIPFROM) OUTDD(STDOUT) '
| //SYSTSPRT DD DUMMY
| //BIPFROM  DD PATHOPTS=(ORDONLY),

```

```

| //          PATH='&COMPDIR./output/stdout'
| //STDOUT   DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
| //SYSTSIN  DD DUMMY
| //*
| //*****
| //* Copy stderr to SYSOUT
| //*****
| //*
| //COPYERR  EXEC PGM=IKJEFT01,COND=EVEN,
| //          PARM='OCOPY INDD(BIPFROM) OUTDD(STDERR) '
| //SYSTSPRT DD DUMMY
| //BIPFROM  DD PATHOPTS=(ORDONLY),
| //          PATH='&COMPDIR./output/stderr'
| //STDERR   DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
| //SYSTSIN  DD DUMMY
| //*
| //          ENDIF
| //*
| //*-----
| //          PEND
| //*-----
| //*
| //

```

Sample BIPCBRK file

```

//BIPCBRK JOB
//*****
//*
//* @START_COPYRIGHT@
//*
//* Licensed Materials - Property of IBM;
//* 5655-G97 (c) Copyright IBM Corp. 2004;
//* All Rights Reserved;
//* US Government Users Restricted Rights - use,
//* duplication or disclosure restricted by GSA
//* ADP Schedule Contract with IBM Corp.;
//* See Copyright Instructions
//*
//* @END_COPYRIGHT@
//*
//*****
//*          IBM WebSphere Event/Message Brokers
//*
//* Sample job to create a broker (mqsicreatebroker).
//*
//*****
//* MORE INFORMATION - See:
//*
//*   WebSphere Event/Message Brokers Information Centre.
//*   Topic "an07080"
//*
//*****
//* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
//* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
//*
//*   Replace  ++HOME++
//*           Home directory where ENVFILE and STDERR
//*           and STDOUT files will be created.
//*           e.g. '/u/home'
//*
//*   Replace  ++INSTALL++
//*           WBI Brokers installation directory.
//*           e.g. '/usr/lpp/mqsi'
//*
//*   Replace  ++COMPONENTNAME++
//*           Broker name.
//*           e.g. 'MQ01BRK'

```



```

/**
/** Replace ++QUEUEMANAGER++
/**      Queue manager name.
/**      e.g. 'MQ01'
/**
/** Replace ++DB2TABLEOWNER++
/**      DB2 table owner userid.
/**      e.g. 'MQ01BRK'
/**
/** Replace ++DB2LOCATION++
/**      DB2 location.
/**      e.g. 'DSN710PK'
/**
/** Replace ++OPTIONS++
/**      Options for mqsicreatebroker command.
/**      e.g. '-1'
/**
/**      z/OS specific options are
/**      -1 Registry pass only
/**      This creates the broker directory.
/**      -2 MQ pass only
/**      This creates the broker MQ queues.
/**      -3 DB2 pass only
/**      This creates the broker tables/indexes.
/**
/**      Please see documentation for other options.
/**
/** Replace ++DB2HLQ++
/**      DB2 high-level-qualifier.
/**      e.g. 'SYS2.DB2.V710'
/**
/** Replace ++WMQHLQ++
/**      WebSphere MQ high-level-qualifier.
/**      e.g. 'MQM.V531'
/**
/*******
/**
/*******
/** Copy ENVFILE to SYSOUT
/*******
/**
/**COPYENV EXEC PGM=IKJEFT01,
/**      PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
/**SYSTSPRT DD DUMMY
/**BIPFROM DD PATHOPTS=(ORDONLY),
/**      PATH='++HOME++/ENVFILE'
/**ENVFILE DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
/**SYSTSIN DD DUMMY
/**
/*******
/** Run mqsicreatebroker command
/*******
/**
/**BIPCRBK EXEC PGM=IKJEFT01,REGION=0M
/**      DB2 Runtime Libraries
/**STEPLIB DD DISP=SHR,DSN=++DB2HLQ++.SDSNEXIT
/**      DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOAD
/**      DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOD2
/**      MQSeries Runtime Libraries
/**      DD DISP=SHR,DSN=++WMQHLQ++.SCSQANLE
/**      DD DISP=SHR,DSN=++WMQHLQ++.SCSQAUTH
/**      DD DISP=SHR,DSN=++WMQHLQ++.SCSQLOAD
/**STDENV DD PATHOPTS=(ORDONLY),
/**      PATH='++HOME++/ENVFILE'
/**STDOUT DD SYSOUT=*
/**STDERR DD SYSOUT=*
/**SYSTSPRT DD SYSOUT=*

```

```

//SYSTSIN DD *
BPXBATSL PGM -
  ++INSTALL++/bin/-
mqsicreatebroker -
  ++COMPONENTNAME++ -
  -q ++QUEUEMANAGER++ -
  -u ++DB2TABLEOWNER++ -
  -n ++DB2LOCATION++ -
  ++OPTIONS++
/*
//

```

Sample BIPCMGRP file

```

| //*****
| /*
| /* @START_COPYRIGHT@
| /*
| /* Licensed Materials - Property of IBM;
| /* 5655-G97 (c) Copyright IBM Corp. 2004;
| /* All Rights Reserved;
| /* US Government Users Restricted Rights - use,
| /* duplication or disclosure restricted by GSA
| /* ADP Schedule Contract with IBM Corp.;
| /* See Copyright Instructions
| /*
| /* @END_COPYRIGHT@
| /*
| //*****
| /* IBM WebSphere Event/Message Brokers
| /*
| /* Sample job to start a configmgr.
| /*
| //*****
| /* MORE INFORMATION - See:
| /*
| /* WebSphere Event/Message Brokers Information Centre.
| /*
| //*****
| /* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
| /* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
| /*
| /* Replace ++HOME++
| /* Home directory where ENVFILE and STDERR
| /* and STDOUT files will be created.
| /* e.g. '/u/home'
| /*
| /* Replace ++INSTALL++
| /* WBI Brokers installation directory.
| /* e.g. '/usr/lpp/mqsi'
| /*
| /* Replace ++QUEUEMANAGER++
| /* Queue manager name.
| /* e.g. 'MQ01'
| /*
| /* Replace ++COMPONENTDIRECTORY++
| /* ConfigMgr directory.
| /* e.g. '/mqsi/configmgr/MQ01BRK'
| /*
| /* Replace ++STARTEDTASKNAME++
| /* Started Task Name (max 8 chars uppercase).
| /* e.g. 'MQ01CMGR'
| /*
| /* Replace ++WMQHLQ++
| /* WebSphere MQ high-level-qualifier.
| /* e.g. 'MQM.V531'
| /*
| //*****

```

```

|  /*
|  /*++STARTEDTASKNAME++ PROC INSTP='++INSTALL++',
|  //      MAINP='bipimain',
|  //      SRVMP='bipservice',
|  //      COMPK='++STARTEDTASKNAME++',
|  //      STRTP='AUTO',
|  //      COMPDIR='++COMPONENTDIRECTORY++',
|  //      STDD='OTRUNC',
|  //      HOME='++HOME++',
|  //      WMQHLQ='++WMQHLQ++'
|  /*
|  /******
|  /* Copy ENVFILE to SYSOUT
|  /******
|  /*
|  //COPYENV EXEC PGM=IKJEFT01,
|  //      PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
|  //SYSTSPRT DD DUMMY
|  //BIPFROM DD PATHOPTS=(ORDONLY),
|  //      PATH='&HOME./ENVFILE'
|  //ENVFILE DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
|  //SYSTSIN DD DUMMY
|  /*
|  /******
|  /* ConfigMgr MQ verification
|  /******
|  /*
|  //VFYMQ EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
|  //      PARM='PGM &INSTP./bin/bipcvp c ++QUEUEMANAGER++'
|  /*
|  //STEPLIB DD DISP=SHR,DSN=&WMQHLQ..SCSQANLE
|  //      DD DISP=SHR,DSN=&WMQHLQ..SCSQAUTH
|  //      DD DISP=SHR,DSN=&WMQHLQ..SCSQLOAD
|  //STDENV DD PATH='&HOME./ENVFILE'
|  //STDOUT DD SYSOUT=*
|  //STDERR DD SYSOUT=*
|  //SYSMDUMP DD SYSOUT=*
|  /*
|  /******
|  /* Check RC from previous steps
|  /******
|  /*
|  //      IF (RC=0) THEN
|  /*
|  /******
|  /* Step to delete residual locks
|  /* (this is only needed if the configmgr is ARM enabled)
|  /******
|  /*
|  /*RMLLOCKS EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
|  /*      PARM='SH rm -f &COMPDIR./common/locks/*'
|  /*
|  /******
|  /* Start :
|  /* ConfigMgr Address Space (bipimain, bipservice and bipconfigmgr)
|  /******
|  /*
|  //CMGR EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
|  //      PARM='PGM &INSTP./bin/&MAINP. &SRVMP. &COMPK. &STRTP.'
|  /*
|  //STEPLIB DD DISP=SHR,DSN=&WMQHLQ..SCSQANLE
|  //      DD DISP=SHR,DSN=&WMQHLQ..SCSQAUTH
|  //      DD DISP=SHR,DSN=&WMQHLQ..SCSQLOAD
|  //STDENV DD PATH='&HOME./ENVFILE'
|  //STDOUT DD PATHOPTS=(OWRONLY,OCREAT,&STDD),
|  //      PATHMODE=(SIRWXU,SIRWXG),
|  //      PATH='&COMPDIR./output/stdout'

```

```

| //STDERR DD PATHOPTS=(OWRONLY,OCREAT,&STDD),
| //      PATHMODE=(SIRWXU,SIRWXG),
| //      PATH='&COMPDIR./output/stderr'
| //SYSMDUMP DD SYSOUT=*
| //*
| //*****
| //* Copy stdout to SYSOUT
| //*****
| //*
| //COPYOUT EXEC PGM=IKJEFT01,COND=EVEN,
| //      PARM='OCOPY INDD(BIPFROM) OUTDD(STDOUT)'
| //SYSTSPRT DD DUMMY
| //BIPFROM DD PATHOPTS=(ORDONLY),
| //      PATH='&COMPDIR./output/stdout'
| //STDOUT DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
| //SYSTSIN DD DUMMY
| //*
| //*****
| //* Copy stderr to SYSOUT
| //*****
| //*
| //COPYERR EXEC PGM=IKJEFT01,COND=EVEN,
| //      PARM='OCOPY INDD(BIPFROM) OUTDD(STDERR)'
| //SYSTSPRT DD DUMMY
| //BIPFROM DD PATHOPTS=(ORDONLY),
| //      PATH='&COMPDIR./output/stderr'
| //STDERR DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
| //SYSTSIN DD DUMMY
| //*
| //      ENDIF
| //*
| //*-----
| //      PEND
| //*-----
| //*
| //

```

Sample BIPCPROF file

```

#*****
#*
#* @START_COPYRIGHT@
#*
#* Licensed Materials - Property of IBM;
#* 5655-G97 (c) Copyright IBM Corp. 2004;
#* All Rights Reserved;
#* US Government Users Restricted Rights - use,
#* duplication or disclosure restricted by GSA
#* ADP Schedule Contract with IBM Corp.;
#* See Copyright Instructions
#*
#* @END_COPYRIGHT@
#*
#*****
#*      IBM WebSphere Event/Message Brokers
#*
#* Sample profile for a configmgr.
#*
#*****
#* MORE INFORMATION - See:
#*
#*      WebSphere Event/Message Brokers Information Centre.
#*
#* IMPORTANT:
#*
#*      You must submit BIPGEN each time you update this profile!
#*
#*****

```

```

** CUSTOMIZE HERE FOR YOUR INSTALLATION
** YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
**
**      Replace  ++INSTALL++
**                WBI Brokers installation directory.
**                e.g. '/usr/lpp/mqsi'
**
**      Replace  ++COMPONENTDIRECTORY++
**                Configmgr directory.
**                e.g. '/mqsi/configmgr/MQ01CMGR'
**
**      Replace  ++COMPONENTNAME++
**                ConfigMgr Name.
**                e.g. 'MQ01CMGR'
**
**      Replace  ++LOCALE++
**                Locale.
**                e.g. 'C'
**
**      Replace  ++TIMEZONE++
**                Time zone.
**                e.g. 'GMT0BST'
**
**      Replace  ++JAVA++
**                Java location.
**                e.g. '/usr/lpp/java/IBM/J1.4'
**
**      Replace  ++XMLTOOLKIT++
**                IBM XML Toolkit location.
**                e.g. '/usr/lpp/ixm/IBM/xml4c-5_5'
**
**      Replace  ++MQPATH++
**                MQ location.
**                e.g. '/usr/lpp/mqm'
**
*****
# 1. Component Settings
*****
#
# 1.1 MQSI_REGISTRY references the component path. Also needed by
#      commands.
#      e.g. MQSI_REGISTRY=/mqsi/configmgr/MQ01CMGR
#
# 1.2 MQSI_COMPONENT_NAME is set to the ConfigMgr name.
#      e.g. MQSI_COMPONENT_NAME=MQ01CMGR
#
# 1.3 MQSI_FILEPATH needed by commands to reference the component
#      version install path.
#      e.g. MQSI_FILEPATH=usr/lpp/mqsi/V6R0M0
#
export MQSI_REGISTRY=++COMPONENTDIRECTORY++
export MQSI_COMPONENT_NAME=++COMPONENTNAME++
export MQSI_FILEPATH=++INSTALL++

*****
# 2. NLS Settings
*****
#
# 2.1 LANG and LC_ALL determine in which locale the component
#      will run.
#      e.g. LANG=Ja_JP.IBM-939 and LC_ALL=Ja_JP.IBM-939 for
#           japanese locale.
#           LANG=C, LC_ALL=C for US English locale.
#
# 2.2 TZ has the timezone setting in which you are located.
#      e.g. TZ=EST5             for USA Eastern Standard Time

```

```

#           TZ=MEZ-1MES,M3.5.0,M10.5.0 for Central Europe
#           TZ=GMT0BST           for the UK
#           Please refer to the IBM Manual
#           "Unix System Services Command Reference SC28-1892.
#
# 2.3 NLSPATH contains the location of the message catalog(s).
#      (NO NEED TO CHANGE FROM DEFAULT!)
#
# 2.4 MQSI_CONSOLE_NLSPATH is used to locate the messages for
#      the console.
#      For Japanese or S-Chinese messages, change En_US to
#      Ja_JP or Zh_CN below. For English messages these can be
#      displayed in mixed or upper case only. (see MC_MESSAGES)
#      Note that MQSI_CONSOLE_NLSPATH does not use %L or %N
#
export LANG=++LOCALE++
export LC_ALL=++LOCALE++
export TZ=++TIMEZONE++
export NLSPATH=$MQSI_FILEPATH/messages/%L/%N
export MQSI_CONSOLE_NLSPATH=$MQSI_FILEPATH/messages/En_US

```

```

*****
# 3. Automatic Restart Management (ARM) Settings
*****

```

```

#
# 3.1 MQSI_USE_ARM specifies whether to use ARM.
#      e.g. MQSI_USE_ARM=YES for ARM enabled.
#           MQSI_USE_ARM=NO  for ARM not enabled.
#
# 3.2 MQSI_ARM_ELEMENTNAME required if ARM enabled.
#
# 3.3 MQSI_ARM_ELEMENTTYPE required if ARM enabled.
#
export MQSI_USE_ARM=NO
export MQSI_ARM_ELEMENTNAME=++COMPONENTNAME++
export MQSI_ARM_ELEMENTTYPE=

```

```

*****
# 4. Java Settings
*****

```

```

#
# 4.1 JAVAHOME contains the root directory of the JAVA install.
#      e.g. JAVAHOME=/usr/lpp/java/IBM/J1.4
#      Note that the Java version must be at least 1.4.1
#
export JAVAHOME=++JAVA++

```

```

*****
# 5. WBI Configmgr Settings
*****

```

```

#
# 5.1 _BPX_BATCH_SPAWN
#      (MUST NOT CHANGE FROM DEFAULT!)
#
# 5.2 MQSI_MC_MESSAGES determines if messages should appear in
#      mixed case or upper case.
#      e.g. MQSI_MC_MESSAGES=YES for mixed case
#           MQSI_MC_MESSAGES=NO for upper case
#
# 5.3 MQSI_COMMAND_DATABASE_ECHO if defined, mqsi commands
#      display information when creating DB2 tables/indexes.
#
# 5.4 MQSI_COMMAND_ZOS_MQ_ECHO if defined, mqsi commands display
#      information returned from the MQ command server when

```

```

#      creating/deleting queues.
#
# 5.5 MQSI_COMMAND_ZOS_MQ_ECHO_RC if defined, mqsi commands display
#      reason and return codes from the MQ command server when
#      creating/deleting queues.
#
# 5.6 STEPLIB
#      (MUST NOT CHANGE FROM DEFAULT!)
#
export _BPX_BATCH_SPAWN=NO
export MQSI_MC_MESSAGES=NO
export MQSI_COMMAND_DATABASE_ECHO=1
export MQSI_COMMAND_ZOS_MQ_ECHO=1
export MQSI_COMMAND_ZOS_MQ_ECHO_RC=1
export STEPLIB=CURRENT

#*****
# 6. Other Settings
#*****
#
# NO NEED TO CHANGE FROM DEFAULT!
#
CP=++MQPATH++/java/lib/com.ibm.mq.jar
CP=$CP:++MQPATH++/java/lib/connector.jar
CP=$CP:$MQSI_FILEPATH/classes
CP=$CP:$JAVAHOME/lib
CP=$CP:$MQSI_FILEPATH/classes/config.jar
CP=$CP:$MQSI_FILEPATH/classes/ConfigManagerProxy.jar
CP=$CP:$MQSI_FILEPATH/classes/ConfigManagerProxySamples.jar
CP=$CP:$MQSI_FILEPATH/classes/configutil.jar
CP=$CP:$MQSI_FILEPATH/messages
export CLASSPATH=$CP
XMLTOOLKIT=++XMLTOOLKIT++
LP=++MQPATH++/java/lib
LP=$LP:$MQSI_FILEPATH/lib/wbirf
LP=$LP:$MQSI_FILEPATH/lib/wbimb
LP=$LP:$MQSI_FILEPATH/lib/wbieb
LP=$LP:$MQSI_FILEPATH/lib
LP=$LP:$JAVAHOME/lib
LP=$LP:$JAVAHOME/bin
LP=$LP:$JAVAHOME/bin/classic
LP=$LP:$XMLTOOLKIT/lib
export LIBPATH=$LP
export PATH=$MQSI_FILEPATH/bin
export PATH=$PATH:$JAVAHOME/bin

```

Sample BIPCRCM file

```

| //BIPCRCM JOB
| //*****
| //*
| //* @START_COPYRIGHT@
| //*
| //* Licensed Materials - Property of IBM;
| //* 5655-G97 (c) Copyright IBM Corp. 2004;
| //* All Rights Reserved;
| //* US Government Users Restricted Rights - use,
| //* duplication or disclosure restricted by GSA
| //* ADP Schedule Contract with IBM Corp.;
| //* See Copyright Instructions
| //*
| //* @END_COPYRIGHT@
| //*
| //*****
| //*          IBM WebSphere Event/Message Brokers
| //*
| //* Sample job to create a configmgr (mqsicreateconfigmgr).
| //*

```

```

|  /**
|  /*******
|  /** MORE INFORMATION - See:
|  /**
|  /**   WebSphere Event/Message Brokers Information Centre.
|  /**   Topic "an23000"
|  /**
|  /*******
|  /** CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
|  /** YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
|  /**
|  /**   Replace   ++HOME++
|  /**             Home directory where ENVFILE and STDERR
|  /**             and STDOUT files will be created.
|  /**             e.g. '/u/home'
|  /**
|  /**   Replace   ++INSTALL++
|  /**             WBI Brokers installation directory.
|  /**             e.g. '/usr/lpp/mqsi'
|  /**
|  /**   Replace   ++COMPONENTNAME++
|  /**             ConfigMgr Name.
|  /**             e.g. 'MQ01CMGR'
|  /**
|  /**   Replace   ++QUEUEMANAGER++
|  /**             Queue manager name.
|  /**             e.g. 'MQ01'
|  /**
|  /**   Replace   ++OPTIONS++
|  /**             Options for mqsicreateconfigmgr command.
|  /**             e.g. '-1'
|  /**
|  /**             z/OS specific options are
|  /**             -1 Registry pass only
|  /**               This creates the configmgr directory.
|  /**             -2 MQ pass only
|  /**               This creates the configmgr MQ queues.
|  /**
|  /**             Please see documentation for other options.
|  /**
|  /**   Replace   ++WMQHLQ++
|  /**             WebSphere MQ high-level-qualifier.
|  /**             e.g. 'MQM.V531'
|  /**
|  /*******
|  /**
|  /*******
|  /** Copy ENVFILE to SYSOUT
|  /*******
|  /**
|  /**COPYENV  EXEC PGM=IKJEFT01,
|  /**          PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
|  /**SYSTSPRT DD DUMMY
|  /**BIPFROM  DD PATHOPTS=(ORDONLY),
|  /**          PATH='++HOME++/ENVFILE'
|  /**ENVFILE  DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
|  /**SYSTSIN  DD DUMMY
|  /**
|  /*******
|  /** Run mqsicreateconfigmgr command
|  /*******
|  /**
|  /**BIPCRCM  EXEC PGM=IKJEFT01,REGION=0M
|  /**          MQSeries Runtime Libraries
|  /**STEPLIB  DD DISP=SHR,DSN=++WMQHLQ++.SCSQANLE
|  /**          DD DISP=SHR,DSN=++WMQHLQ++.SCSQAUTH
|  /**          DD DISP=SHR,DSN=++WMQHLQ++.SCSQLOAD

```



```

| //STDENV DD PATHOPTS=(ORDONLY),
| //      PATH='++HOME++/ENVFILE'
| //STDOUT DD SYSOUT=*
| //STDERR DD SYSOUT=*
| //SYSTSPRT DD SYSOUT=*
| //SYSTSIN DD *
| BPXBATSL PGM -
|   ++INSTALL++/bin/-
| mqsicreateconfigmgr -
|   ++COMPONENTNAME++ -
|   -q ++QUEUEMANAGER++ -
|   ++OPTIONS++
| /*
| //

```

Sample BIPCRDB file

```

//BIPCRDB JOB
//*****
//*
//* @START_COPYRIGHT@
//*
//* Licensed Materials - Property of IBM;
//* 5655-G97 (c) Copyright IBM Corp. 2004;
//* All Rights Reserved;
//* US Government Users Restricted Rights - use,
//* duplication or disclosure restricted by GSA
//* ADP Schedule Contract with IBM Corp.;
//* See Copyright Instructions
//*
//* @END_COPYRIGHT@
//*
//*****
//*          IBM WebSphere Event/Message Brokers
//*
//* Create broker storagegroup / database and tablespaces.
//*
//*****
//* MORE INFORMATION - See:
//*
//*   WebSphere Event/Message Brokers Information Centre.
//*
//*
//*****
//* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
//* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
//*
//*   Replace   ++DB2HLQ++
//*             DB2 high-level-qualifier.
//*             e.g. 'SYS2.DB2.V810'
//*
//*   Replace   ++DB2RUNLIB++
//*             DB2.
//*             e.g. 'DSN810PK.RUNLIB.LOAD'
//*
//*   Replace   ++DB2SUBSYSTEM++
//*             DB2 SSID.
//*             e.g. 'DFK4'
//*
//*   Replace   ++DB2LOCATION++
//*             DB2 location.
//*             e.g. 'DSN810PK'
//*
//*   Replace   ++DB2CURRENTSQLID++
//*             SET CURRENT SQLID user ID.
//*             e.g. 'MQ01GRP'
//*
//*   Replace   ++DB2DATABASE++

```

```

/**          DB2 database.
/**          e.g. 'DMQ01BRK'
/**
/**  Replace  ++DB2STORAGEGROUP++
/**          DB2 storagegroup.
/**          e.g. 'MQ01STOR'
/**
/**  Replace  ++DB2BUFFERPOOL++
/**          DB2 base table bufferpool.
/**          e.g. 'BP0'
/**
/**  Replace  ++DB2INDEXBP++
/**          DB2 index bufferpool.
/**          e.g. 'BP0'
/**
/**  Replace  ++DB2LOBBP++
/**          DB2 LOB table bufferpool.
/**          e.g. 'BP0'
/**
/**  Replace  ++DB2SAMPLEPROGRAM++
/**          DB2 sample program name.
/**          e.g. 'DSNTEP2'
/**
/**  Replace  ++DB2SAMPLEPROGRAMPLAN++
/**          DB2 sample program plan name.
/**          e.g. 'DSNTEP81'
/**
/*******
/**
/*******
/** Create broker storagegroup
/*******
/**
/**STORGRP EXEC PGM=IKJEFT01,REGION=0M
/**          DB2 Runtime Libraries
/**STEPLIB DD DISP=SHR,DSN=++DB2HLQ++.SDSNEXIT
/**          DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOAD
/**          DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOD2
/**          DD DISP=SHR,DSN=++DB2RUNLIB++
/**SYSTSPRT DD SYSOUT=*
/**SYSTSIN DD *
DSN SYSTEM(++DB2SUBSYSTEM++)
  RUN -
    PROGRAM(++DB2SAMPLEPROGRAM++) -
    PLAN(++DB2SAMPLEPROGRAMPLAN++)
/**SYSPRINT DD SYSOUT=*
/**SYSUDUMP DD SYSOUT=*
/**SYSIN DD *
  SET CURRENT SQLID='++DB2CURRENTSQLID++';
  CREATE STOGROUP ++DB2STORAGEGROUP++
    VOLUMES('*')
    VCAT ++DB2LOCATION++;
/**
/**
/*******
/** Create broker database
/*******
/**
/**DATABASE EXEC PGM=IKJEFT01,REGION=0M
/**          DB2 Runtime Libraries
/**STEPLIB DD DISP=SHR,DSN=++DB2HLQ++.SDSNEXIT
/**          DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOAD
/**          DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOD2
/**          DD DISP=SHR,DSN=++DB2RUNLIB++
/**SYSTSPRT DD SYSOUT=*
/**SYSTSIN DD *
DSN SYSTEM(++DB2SUBSYSTEM++)

```

```

RUN -
  PROGRAM(++DB2SAMPLEPROGRAM++) -
  PLAN(++DB2SAMPLEPROGRAMPLAN++)
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
  SET CURRENT SQLID='++DB2CURRENTSQLID++';
  CREATE DATABASE ++DB2DATABASE++
    STOGROUP ++DB2STORAGEGROUP++
    INDEXBP ++DB2INDEXBP++;
/*
/**
/*******
/** Create broker tablespaces
/*******
/**
//TABLESPC EXEC PGM=IKJEFT01,REGION=0M
/** DB2 Runtime Libraries
//STEPLIB DD DISP=SHR,DSN=++DB2HLQ++.SDSNEXIT
// DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOAD
// DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOD2
// DD DISP=SHR,DSN=++DB2RUNLIB++
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
DSN SYSTEM(++DB2SUBSYSTEM++)
  RUN -
    PROGRAM(++DB2SAMPLEPROGRAM++) -
    PLAN(++DB2SAMPLEPROGRAMPLAN++)
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
  SET CURRENT SQLID='++DB2CURRENTSQLID++';
  CREATE TABLESPACE BSUBSCRI
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY 7200
      SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ROW
  CLOSE NO;

  CREATE TABLESPACE BPUBLISH
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY 7200
      SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;

  CREATE TABLESPACE BCLIENTU
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY 7200
      SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32

```

```
BUFFERPOOL ++DB2BUFFERPOOL++
LOCKSIZE ANY
CLOSE NO;
```

```
CREATE TABLESPACE BUSERCON
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE     20
  SEGSIZE     32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;
```

```
CREATE TABLESPACE BTOPOLOG
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE     20
  SEGSIZE     32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;
```

```
CREATE TABLESPACE BNBRCONN
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE     20
  SEGSIZE     32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;
```

```
CREATE TABLESPACE BRETAINE
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE     20
  SEGSIZE     32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ROW
  CLOSE NO;
```

```
CREATE TABLESPACE BACLINTR
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE     20
  SEGSIZE     32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
```

```

CLOSE NO;

CREATE TABLESPACE BMQPSTOP
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE      20
  SEGSIZE      32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
CLOSE NO;

```

```

CREATE TABLESPACE BUSERNAM
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE      20
  SEGSIZE      32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
CLOSE NO;

```

```

CREATE TABLESPACE BGROUPNA
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE      20
  SEGSIZE      32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
CLOSE NO;

```

```

CREATE TABLESPACE BUSERMEM
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE      20
  SEGSIZE      32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
CLOSE NO;

```

```

CREATE TABLESPACE BROKERA
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY      7200
    SECQTY      720
  ERASE NO
  FREEPAGE     5
  PCTFREE      20
  SEGSIZE      32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
CLOSE NO;

```

```

CREATE TABLESPACE BROKERAE
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY 7200
    SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;

```

```

CREATE TABLESPACE BROKERRE
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY 7200
    SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;

```

```

CREATE TABLESPACE BRMINFO
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY 7200
    SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;

```

```

CREATE TABLESPACE BRMRTDIN
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY 7200
    SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;

```

```

CREATE TABLESPACE BRMRTDDE
  IN ++DB2DATABASE++
  USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY 7200
    SECQTY 720
  ERASE NO
  FREEPAGE 5
  PCTFREE 20
  SEGSIZE 32
  BUFFERPOOL ++DB2BUFFERPOOL++
  LOCKSIZE ANY
  CLOSE NO;

```

```

CREATE TABLESPACE BRMWFIDIN
  IN ++DB2DATABASE++

```

```

USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY      7200
      SECQTY      720
ERASE NO
FREEPAGE      5
PCTFREE      20
SEGSIZE      32
BUFFERPOOL ++DB2BUFFERPOOL++
LOCKSIZE ANY
CLOSE NO;

CREATE TABLESPACE BRMPHYSI
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY      7200
      SECQTY      720
ERASE NO
FREEPAGE      5
PCTFREE      20
SEGSIZE      32
BUFFERPOOL ++DB2BUFFERPOOL++
LOCKSIZE ANY
CLOSE NO;

CREATE TABLESPACE BAGGREGA
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY      7200
      SECQTY      720
ERASE NO
FREEPAGE      5
PCTFREE      20
SEGSIZE      32
BUFFERPOOL ++DB2BUFFERPOOL++
LOCKSIZE ROW
CLOSE NO;

CREATE TABLESPACE BMULTICA
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY      7200
      SECQTY      720
ERASE NO
FREEPAGE      5
PCTFREE      20
SEGSIZE      32
BUFFERPOOL ++DB2BUFFERPOOL++
LOCKSIZE ANY
CLOSE NO;

CREATE LOB TABLESPACE BSUBLOB1
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY      72000
      SECQTY      7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE LOB;

CREATE LOB TABLESPACE BSUBLOB2
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
      PRIQTY      72000
      SECQTY      7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE LOB;

CREATE LOB TABLESPACE BSUBLOB3

```

```

IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BPULLLOB
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BCLIELOB
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BRETLOB1
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BRETLOB2
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BACLELOB
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BMQPSLOB
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BMULTLOB
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000
    SECQTY    7200
BUFFERPOOL ++DB2LOBBP++
LOCKSIZE   LOB;

CREATE LOB TABLESPACE BROKALOB
IN ++DB2DATABASE++
USING STOGROUP ++DB2STORAGEGROUP++
    PRIQTY    72000

```



```

        SECQTY      7200
    BUFFERPOOL ++DB2LOBBP++
    LOCKSIZE   LOB;

CREATE LOB TABLESPACE BROKRLOB
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
        PRIQTY      72000
        SECQTY      7200
    BUFFERPOOL ++DB2LOBBP++
    LOCKSIZE   LOB;

CREATE LOB TABLESPACE BRMRTLOB
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
        PRIQTY      72000
        SECQTY      7200
    BUFFERPOOL ++DB2LOBBP++
    LOCKSIZE   LOB;

CREATE LOB TABLESPACE BRMPHLOB
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
        PRIQTY      72000
        SECQTY      7200
    BUFFERPOOL ++DB2LOBBP++
    LOCKSIZE   LOB;

CREATE LOB TABLESPACE BAGGRLOB
    IN ++DB2DATABASE++
    USING STOGROUP ++DB2STORAGEGROUP++
        PRIQTY      72000
        SECQTY      7200
    BUFFERPOOL ++DB2LOBBP++
    LOCKSIZE   LOB;

/*
//

```

Sample BIPCRUN file

```

| //BIPCRUN JOB
| //*****
| //*
| //* @START_COPYRIGHT@
| //*
| //* Licensed Materials - Property of IBM;
| //* 5655-G97 (c) Copyright IBM Corp. 2004;
| //* All Rights Reserved;
| //* US Government Users Restricted Rights - use,
| //* duplication or disclosure restricted by GSA
| //* ADP Schedule Contract with IBM Corp.;
| //* See Copyright Instructions
| //*
| //* @END_COPYRIGHT@
| //*
| //*****
| //*          IBM WebSphere Event/Message Brokers
| //*
| //* Sample job to create a usernameserver
| //*          (mqsicreateusernameserver).
| //*
| //*****
| //* MORE INFORMATION - See:
| //*
| //*   WebSphere Event/Message Brokers Information Centre.
| //* Topic "an07200"
| //*
| //*****

```

```

|  /** CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
|  /** YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
|  /**
|  /**      Replace    ++HOME++
|  /**              Home directory where ENVFILE and STDERR
|  /**              and STDOUT files will be created.
|  /**              e.g. '/u/home'
|  /**
|  /**      Replace    ++INSTALL++
|  /**              WBI Brokers installation directory.
|  /**              e.g. '/usr/lpp/mqsi '
|  /**
|  /**      Replace    ++QUEUEMANAGER++
|  /**              Queue manager name.
|  /**              e.g. 'MQ01'
|  /**
|  /**      Replace    ++OPTIONS++
|  /**              Options for mqsicreateusernameserver.
|  /**              e.g. '-1'
|  /**
|  /**              z/OS specific options are
|  /**              -1 Registry pass only
|  /**              This creates the uns directory.
|  /**              -2 MQ pass only
|  /**              This creates the uns MQ queues.
|  /**
|  /**              Please see documentation for other options.
|  /**
|  /**      Replace    ++WMQHLQ++
|  /**              WebSphere MQ high-level-qualifier.
|  /**              e.g. 'MQM.V531'
|  /**
|  /*******
|  /**
|  /*******
|  /** Copy ENVFILE to SYSOUT
|  /*******
|  /**
|  /**COPYENV  EXEC PGM=IKJEFT01,
|  /**          PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE) '
|  /**SYSTSPRT DD DUMMY
|  /**BIPFROM  DD PATHOPTS=(ORDONLY),
|  /**          PATH='++HOME++/ENVFILE'
|  /**ENVFILE  DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
|  /**SYSTSIN  DD DUMMY
|  /**
|  /*******
|  /** Run mqsicreateusernameserver command
|  /*******
|  /**
|  /**BIPCRUN  EXEC PGM=IKJEFT01,REGION=0M
|  /**          MQSeries Runtime Libraries
|  /**STEPLIB  DD DISP=SHR,DSN=++WMQHLQ++.SCSQANLE
|  /**          DD DISP=SHR,DSN=++WMQHLQ++.SCSQAUTH
|  /**          DD DISP=SHR,DSN=++WMQHLQ++.SCSQLOAD
|  /**STDENV   DD PATHOPTS=(ORDONLY),
|  /**          PATH='++HOME++/ENVFILE'
|  /**STDOUT   DD SYSOUT=*
|  /**STDERR   DD SYSOUT=*
|  /**SYSTSPRT DD SYSOUT=*
|  /**SYSTSIN  DD *
|  BPXBATSL PGM -
|  ++INSTALL++/bin/-
|  mqsicreateusernameserver -

```

```

| -q ++QUEUEMANAGER++ -
| ++OPTIONS++
| /*
| //

```

Sample BIPDSNAO file

```

;*****
;*
;* @START_COPYRIGHT@
;*
;* Licensed Materials - Property of IBM;
;* 5655-G97 (c) Copyright IBM Corp. 2004;
;* All Rights Reserved;
;* US Government Users Restricted Rights - use,
;* duplication or disclosure restricted by GSA
;* ADP Schedule Contract with IBM Corp.;
;* See Copyright Instructions
;*
;* @END_COPYRIGHT@
;*
;*****
;*          IBM WebSphere Event/Message Brokers
;*
;* Sample dsnaoini for a broker, usernamerserver or configmgr.
;*
;*****
;* MORE INFORMATION - See:
;*
;*   WebSphere Event/Message Brokers Information Centre.
;*
;*****
;* CUSTOMIZE HERE FOR YOUR INSTALLATION
;* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
;*
;*   Replace  ++COMPONENTDIRECTORY++
;*             Component directory.
;*             e.g. '/mqsi/brokers/MQ01BRK'
;*
;*   Replace  ++DB2SUBSYSTEM++
;*             DB2 SSID.
;*             e.g. 'DFK4'
;*
;*   Replace  ++DB2LOCATION++
;*             DB2 location.
;*             e.g. 'DSN810PK'
;*
;*   Replace  ++DB2CURRENTSQLID++
;*             CURRENT SQLID user ID.
;*             e.g. 'MQ01GRP'
;*
;*   Replace  ++DB2DSNACLIPLAN++
;*             DB2 plan name for dsnacli.
;*             e.g. 'DSNACLI'
;*
;*****
[COMMON]
APPLTRACE=0
APPLTRACEfilename=++COMPONENTDIRECTORY++/output/traceodbc
CONNECTTYPE=2
DIAGTRACE=0
DIAGTRACE_NO_WRAP=0
MAXCONN=0
MULTICONTEXT=0
MVSDEFAULTSSID=++DB2SUBSYSTEM++

; SUBSYSTEM
[++DB2SUBSYSTEM++]

```

MVSATTACHTYPE=RRSAF
PLANNAME=++DB2DSNACLIPLAN++

; DATASOURCES
[++DB2LOCATION++]
CURRENTSQLID=++DB2CURRENTSQLID++

Sample BIPEDIT file

```
| /* REXX */
| /*****
| /*
| /* @START_COPYRIGHT@
| /*
| /* Licensed Materials - Property of IBM;
| /* 5655-G97 (c) Copyright IBM Corp. 2004;
| /* All Rights Reserved;
| /* US Government Users Restricted Rights - use,
| /* duplication or disclosure restricted by GSA
| /* ADP Schedule Contract with IBM Corp.;
| /* See Copyright Instructions
| /*
| /* @END_COPYRIGHT@
| /*
| /*****
| /* IBM WebSphere Event/Message Brokers
| /*
| /* REXX utility to customize JCL.
| /*
| /*****
| /* MORE INFORMATION - See:
| /*
| /* WebSphere Event/Message Brokers Information Centre.
| /*
| /*****
| /*
| /* This edit macro can be used to assist you in configuring your
| /* Broker configuration files.
| /* 1. Edit this file to alter the change commands so the second
| /* parameter is the value for your installaton
| /* 2. Save the file
| /* 3. Rename it to a broker related file, for example VCP1EDIT for
| /* Broker called VCP1BRK
| /* 4. In TSO or TSO command shell ( often ISPF option 6) execute
| /* ALTLIB ACTIVATE APPLICATION(EXEC) DA('WBI.V5.SBIPPROC')
| /* where WBI.V5.SBIPPROC is the name of the PDS containing this
| /* macro
| /* 5. Using the same ISPF session, edit a configuration file
| /* 6. Type the macro name at the commands line and press enter
| /* This will execute the macro.
| /* If you get Command not found, then check you issued the command
| /* in 4. in the same ISPF session
| /* 7. If the macro has any errors, cancel from the file being edited
| /* resolve the errors in the macro and retry
| /*
| /*****
| /* See the product documentation on the meaning of the fields below=
| /*****
| ISREDIT MACRO NOPROCESS
| ADDRESS ISREDIT
| /* All components (Broker , Configuration Manager and User Name Server) */
| "change ++INSTALL++ install_value all"
| "change ++COMPONENTDIRECTORY++ compdir_value all"
| "change ++COMPONENTNAME++ MQ01BRK all"
| "change ++HOME++ /u/mq01brk all"
| "change ++OPTIONS++ options_value all"
| "change ++LOCALE++ C all"
| "change ++TIMEZONE++ GMT0BST all"
```

```

| "change ++JAVA++ /usr/lpp/java/IBM/J1.4          all"
| "change ++WMQHLQ++ MQM.V530                    all"
| "change ++QUEUEMANAGER++ MQ01                  all"
| "change ++COMPONENTDATASET++ componentdataset_value all"
| "change ++STARTEDTASKNAME++ MQ01BRK           all"
| "change ++COMPONENTPROFILE++ componentprofile_value all"
| "change ++XMLTOOLKIT++ /usr/lpp/ixm/IBM/xml4c-5_5 all"
| /* Broker only                                */
| /* (Delete if Configuration Manager or User Name Server) */
| "change ++DB2CONVERSION++ SINGLE              all"
| "change ++DB2SUBSYSTEM++ dbds subsystem_value all"
| "change ++DB2LOCATION++ db2location_value      all"
| "change ++DB2TABLEOWNER++ MQ01GRP            all"
| "change ++DB2CURRENTSQLID++ MQ01GRP          all"
| "change ++DB2DSNACLIPLAN++ dsnac li_value     all"
| "change ++DB2HLQ++ SYS2.DB2.V710             all"
| "change ++DB2RUNLIB++ runlib_value           all"
| "change ++DB2SAMPLEPROGRAM++ sampleprogram_value all"
| "change ++DB2SAMPLEPROGRAMPLAN++ sampleprogramplan_value all"
| "change ++DB2DATABASE++ DMQ01BRK            all"
| "change ++DB2STORAGEGROUP++ MQ01STOR         all"
| "change ++DB2BUFFERPOOL++ BP0                all"
| "change ++DB2INDEXBP++ BP0                  all"
| "change ++DB2LOBBP++ BP0                    all"
| /* Configuration Manager only                  */
| /* (Delete if Broker or User Name Server)     */
| "change ++MQPATH++ /usr/lpp/mqm              all"

```

Sample BIPGEN file

```

//BIPGEN JOB
//*****
//*
//* @START_COPYRIGHT@
//*
//* Licensed Materials - Property of IBM;
//* 5655-G97 (c) Copyright IBM Corp. 2004;
//* All Rights Reserved;
//* US Government Users Restricted Rights - use,
//* duplication or disclosure restricted by GSA
//* ADP Schedule Contract with IBM Corp.;
//* See Copyright Instructions
//*
//* @END_COPYRIGHT@
//*
//*****
//*          IBM WebSphere Event/Message Brokers
//*
//* Copy component profile to the file system and generate an
//* ENVFILE.
//*
//* IMPORTANT:
//*
//*   You must submit BIPGEN each time you update a profile!
//*
//*****
//* MORE INFORMATION - See:
//*
//*   WebSphere Event/Message Brokers Information Centre.
//*
//*****
//* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
//* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
//*
//*   Replace ++HOME++
//*
//*           Home directory where ENVFILE and STDERR
//*           and STDOUT files will be created.
//*
//*           e.g. '/u/home'

```

```

/**
/** Replace ++COMPONENTDATASET++
/**          Component dataset.
/**          e.g. 'BIP.BROKER.MQ01BRK'
/**
/** Replace ++COMPONENTPROFILE++
/**          Component profile name.
/**          e.g. Broker      = 'BIPBPROF'
/**          Usernameserver = 'BIPUPROF'
/**          Configmgr      = 'BIPCPROF'
/**
/*******
/**
/*******
/** Copy BIPBPROF/BIPUPROF/BIPCPROF to file system
/*******
/**
/**COPYPROF EXEC PGM=IKJEFT01,
/**          PARM='OCOPY INDD(BIPFROM) OUTDD(BIPPROF)'
/**SYSTSPRT DD DUMMY
/**BIPFROM  DD DISP=SHR,DSN=++COMPONENTDATASET++(++COMPONENTPROFILE++)
/**BIPPROF  DD PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
/**          PATHMODE=(SIRWXU,SIRWXG),
/**          PATH='++HOME++/bipprof'
/**SYSTSIN  DD DUMMY
/**
/*******
/** Copy BIPPROF to SYSOUT
/*******
/**
/**COPYENV  EXEC PGM=IKJEFT01,
/**          PARM='OCOPY INDD(BIPFROM) OUTDD(BIPPROF)'
/**SYSTSPRT DD DUMMY
/**BIPFROM  DD PATHOPTS=(ORDONLY),
/**          PATH='++HOME++/bipprof'
/**BIPPROF  DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
/**SYSTSIN  DD DUMMY
/**
/*******
/** Create ENVFILE from BIPPROF
/*******
/**
/**CREATENV EXEC PGM=IKJEFT01,REGION=0M
/**SYSTSPRT DD SYSOUT=*
/**SYSTSIN  DD *
/**          BPXBATCH SH -
/**          . ++HOME++/bipprof; -
/**          /bin/printenv > -
/**          ++HOME++/ENVFILE
/**
/*******
/** Copy ENVFILE to SYSOUT
/*******
/**
/**COPYENV  EXEC PGM=IKJEFT01,
/**          PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
/**SYSTSPRT DD DUMMY
/**BIPFROM  DD PATHOPTS=(ORDONLY),
/**          PATH='++HOME++/ENVFILE'
/**ENVFILE  DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
/**SYSTSIN  DD DUMMY
/**
/**

```

Sample BIPUNSP file

```
| //*****  
| //* *  
| //* @START_COPYRIGHT@ *  
| //* *  
| //* Licensed Materials - Property of IBM; *  
| //* 5655-G97 (c) Copyright IBM Corp. 2004; *  
| //* All Rights Reserved; *  
| //* US Government Users Restricted Rights - use, *  
| //* duplication or disclosure restricted by GSA *  
| //* ADP Schedule Contract with IBM Corp.; *  
| //* See Copyright Instructions *  
| //* *  
| //* @END_COPYRIGHT@ *  
| //* *  
| //*****  
| //* IBM WebSphere Event/Message Brokers *  
| //* *  
| //* Sample job to start a usernameserver. *  
| //* *  
| //*****  
| //* MORE INFORMATION - See: *  
| //* *  
| //* WebSphere Event/Message Brokers Information Centre. *  
| //* *  
| //*****  
| //* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION  
| //* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR  
| //* *  
| //* Replace ++HOME++  
| //* Home directory where ENVFILE and STDERR  
| //* and STDOUT files will be created.  
| //* e.g. '/u/home'  
| //*  
| //* Replace ++INSTALL++  
| //* WBI Brokers installation directory.  
| //* e.g. '/usr/lpp/mqsi'  
| //*  
| //* Replace ++QUEUEMANAGER++  
| //* Queue manager name.  
| //* e.g. 'MQ01'  
| //*  
| //* Replace ++COMPONENTDIRECTORY++  
| //* Usernameserver directory.  
| //* e.g. '/mqsi/brokers/MQ01BRK'  
| //*  
| //* Replace ++STARTEDTASKNAME++  
| //* Started Task Name (max 8 chars uppercase).  
| //* e.g. 'MQ01BRK'  
| //*  
| //* Replace ++WMQHLQ++  
| //* WebSphere MQ high-level-qualifier.  
| //* e.g. 'MQM.V531'  
| //*  
| //*****  
| //*  
| //++STARTEDTASKNAME++ PROC INSTP='++INSTALL++',  
| // MAINP='bipimain',  
| // SRVMP='bipservice',  
| // COMPK='++STARTEDTASKNAME++',  
| // STRTP='AUTO',  
| // COMPDIR='++COMPONENTDIRECTORY++',  
| // STDD='OTRUNC',  
| // HOME='++HOME++',  
| // WMQHLQ='++WMQHLQ++'  
| //*  
| //*****
```

```

|  /* Copy ENVFILE to SYSOUT
|  /******
|  /*
|  //COPYENV EXEC PGM=IKJEFT01,
|  // PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
|  //SYSTSPRT DD DUMMY
|  //BIPFROM DD PATHOPTS=(ORDONLY),
|  // PATH='&HOME./ENVFILE'
|  //ENVFILE DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
|  //SYSTSIN DD DUMMY
|  /*
|  /******
|  /* UserNameServer MQ verification
|  /******
|  /*
|  //VFYDB2MQ EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
|  // PARM='PGM &INSTP./bin/bipcvp u ++QUEUEMANAGER++'
|  /*
|  //STEPLIB DD DISP=SHR,DSN=&WMQHLQ..SCSQANLE
|  // DD DISP=SHR,DSN=&WMQHLQ..SCSQAUTH
|  // DD DISP=SHR,DSN=&WMQHLQ..SCSQLOAD
|  //STDENV DD PATH='&HOME./ENVFILE'
|  //STDOUT DD SYSOUT=*
|  //STDERR DD SYSOUT=*
|  //SYSMDUMP DD SYSOUT=*
|  /*
|  /******
|  /* Check RC from previous steps
|  /******
|  /*
|  // IF (RC=0) THEN
|  /*
|  /******
|  /* Step to delete residual locks
|  /* (this is only needed if the broker is ARM enabled)
|  /******
|  /*
|  /**RMLOCKS EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
|  /** PARM='SH rm -f &COMPDIR./common/locks/*'
|  /**
|  /******
|  /* Start :
|  /* UserNameServer Address Space (bipimain, bipservice and bipuns)
|  /******
|  /*
|  //UNS EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
|  // PARM='PGM &INSTP./bin/&MAINP. &SRVMP. &COMPK. &STRTP.'
|  /*
|  //STEPLIB DD DISP=SHR,DSN=&WMQHLQ..SCSQANLE
|  // DD DISP=SHR,DSN=&WMQHLQ..SCSQAUTH
|  // DD DISP=SHR,DSN=&WMQHLQ..SCSQLOAD
|  //STDENV DD PATH='&HOME./ENVFILE'
|  //STDOUT DD PATHOPTS=(OWRONLY,OCREAT,&STDD),
|  // PATHMODE=(SIRWXU,SIRWXG),
|  // PATH='&COMPDIR./output/stdout'
|  //STDERR DD PATHOPTS=(OWRONLY,OCREAT,&STDD),
|  // PATHMODE=(SIRWXU,SIRWXG),
|  // PATH='&COMPDIR./output/stderr'
|  //SYSMDUMP DD SYSOUT=*
|  /*
|  /******
|  /* Copy stdout to SYSOUT
|  /******
|  /*
|  //COPYOUT EXEC PGM=IKJEFT01,COND=EVEN,
|  // PARM='OCOPY INDD(BIPFROM) OUTDD(STDOUT)'
|  //SYSTSPRT DD DUMMY

```



```

| //BIPFROM DD PATHOPTS=(ORDONLY),
| //          PATH='&COMPDIR./output/stdout'
| //STDOUT DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
| //SYSTSIN DD DUMMY
| //*
| //*****
| // Copy stderr to SYSOUT
| //*****
| //*
| //COPYERR EXEC PGM=IKJEFT01,COND=EVEN,
| //          PARM='OCOPY INDD(BIPFROM) OUTDD(STDERR)'
| //SYSTSPRT DD DUMMY
| //BIPFROM DD PATHOPTS=(ORDONLY),
| //          PATH='&COMPDIR./output/stderr'
| //STDERR DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
| //SYSTSIN DD DUMMY
| //*
| //          ENDIF
| //*
| //-----
| //          PEND
| //-----
| //*
| //
| //

```

Sample BIPUPROF file

```

#*****
#*                                                                 *
#* @START_COPYRIGHT@                                           *
#*                                                                 *
#* Licensed Materials - Property of IBM;                       *
#* 5655-G97 (c) Copyright IBM Corp. 2004;                     *
#* All Rights Reserved;                                         *
#* US Government Users Restricted Rights - use,                *
#* duplication or disclosure restricted by GSA                  *
#* ADP Schedule Contract with IBM Corp.;                       *
#* See Copyright Instructions                                    *
#*                                                                 *
#* @END_COPYRIGHT@                                             *
#*                                                                 *
#*****
#*          IBM WebSphere Event/Message Brokers                *
#*                                                                 *
#* Sample profile for a usernameserver.                         *
#*                                                                 *
#*****
#* MORE INFORMATION - See:                                       *
#*                                                                 *
#*   WebSphere Event/Message Brokers Information Centre.       *
#*                                                                 *
#* IMPORTANT:                                                    *
#*                                                                 *
#*   You must submit BIPGEN each time you update this profile! *
#*                                                                 *
#*****
#* CUSTOMIZE HERE FOR YOUR INSTALLATION                         *
#* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR *
#*                                                                 *
#*   Replace ++INSTALL++                                         *
#*           WBI Brokers installation directory.                *
#*           e.g. '/usr/lpp/mqsi'                                *
#*                                                                 *
#*   Replace ++COMPONENTDIRECTORY++                             *
#*           Usernameserver directory.                          *
#*           e.g. '/mqsi/uns/MQ01BRK'                           *
#*                                                                 *
#*   Replace ++LOCALE++                                          *

```

```

#*          Locale.
#*          e.g. 'C'
#*
#*  Replace  ++TIMEZONE++
#*          Time zone.
#*          e.g. 'GMT0BST'
#*
#*  Replace  ++JAVA++
#*          Java location.
#*          e.g. '/usr/lpp/java/IBM/J1.4'
#*
#*  Replace  ++XMLTOOLKIT++
#*          IBM XML Toolkit location.
#*          e.g. '/usr/lpp/ixm/IBM/xml4c-5_5'
#*
#*****
# 1. Component Settings
#*****
#
# 1.1 MQSI_REGISTRY references the component path. Also needed by
#      commands.
#      e.g. MQSI_REGISTRY=/mqsi/uns/MQ01BRK
#
# 1.2 MQSI_COMPONENT_NAME is set to the UserNameServer name.
#      (DO NOT CHANGE FROM DEFAULT!)
#
# 1.3 MQSI_FILEPATH needed by commands to reference the component
#      version install path.
#      e.g. MQSI_FILEPATH=usr/lpp/mqsi/V6ROM0
#
export MQSI_REGISTRY=++COMPONENTDIRECTORY++
export MQSI_COMPONENT_NAME=UserNameServer
export MQSI_FILEPATH=++INSTALL++

#*****
# 2. NLS Settings
#*****
#
# 2.1 LANG and LC_ALL determine in which locale the component
#      will run.
#      e.g. LANG=Ja_JP.IBM-939 and LC_ALL=Ja_JP.IBM-939 for
#           japanese locale.
#           LANG=C, LC_ALL=C for US English locale.
#
# 2.2 TZ has the timezone setting in which you are located.
#      e.g. TZ=EST5           for USA Eastern Standard Time
#           TZ=MEZ-1MES,M3.5.0,M10.5.0 for Central Europe
#           TZ=GMT0BST       for the UK
#           Please refer to the IBM Manual
#           "Unix System Services Command Reference SC28-1892.
#
# 2.3 NLSPATH contains the location of the message catalog(s).
#      (NO NEED TO CHANGE FROM DEFAULT!)
#
# 2.4 MQSI_CONSOLE_NLSPATH is used to locate the messages for
#      the console.
#      For Japanese or S-Chinese messages, change En_US to
#      Ja_JP or Zh_CN below. For English messages these can be
#      displayed in mixed or upper case only. (see MC_MESSAGES)
#      Note that MQSI_CONSOLE_NLSPATH does not use %L or %N
#
export LANG=++LOCALE++
export LC_ALL=++LOCALE++
export TZ=++TIMEZONE++
export NLSPATH=$MQSI_FILEPATH/messages/%L/%N
export MQSI_CONSOLE_NLSPATH=$MQSI_FILEPATH/messages/En_US

```

```

#*****
# 3. Automatic Restart Management (ARM) Settings
#*****
#
# 3.1 MQSI_USE_ARM specifies whether to use ARM.
#     e.g. MQSI_USE_ARM=YES for ARM enabled.
#         MQSI_USE_ARM=NO  for ARM not enabled.
#
# 3.2 MQSI_ARM_ELEMENTNAME required if ARM enabled.
#
# 3.3 MQSI_ARM_ELEMENTTYPE required if ARM enabled.
#
export MQSI_USE_ARM=NO
export MQSI_ARM_ELEMENTNAME=
export MQSI_ARM_ELEMENTTYPE=

#*****
# 4. Java Settings
#*****
#
# 4.1 JAVAHOME contains the root directory of the JAVA install.
#     e.g. JAVAHOME=/usr/lpp/java/IBM/J1.4
#     Note that the Java version must be at least 1.4.1
#
export JAVAHOME=++JAVA++

#*****
# 5. WBI Usernameserver Settings
#*****
#
# 5.1 _BPX_BATCH_SPAWN
#     (MUST NOT CHANGE FROM DEFAULT!)
#
# 5.2 MQSI_MC_MESSAGES determines if messages should appear in
#     mixed case or upper case.
#     e.g. MQSI_MC_MESSAGES=YES for mixed case
#         MQSI_MC_MESSAGES=NO for upper case
#
# 5.3 MQSI_COMMAND_DATABASE_ECHO if defined, mqsi commands
#     display information when creating DB2 tables/indexes.
#
# 5.4 MQSI_COMMAND_ZOS_MQ_ECHO if defined, mqsi commands display
#     information returned from the MQ command server when
#     creating/deleting queues.
#
# 5.5 MQSI_COMMAND_ZOS_MQ_ECHO_RC if defined, mqsi commands display
#     reason and return codes from the MQ command server when
#     creating/deleting queues.
#
# 5.6 STEPLIB
#     (MUST NOT CHANGE FROM DEFAULT!)
#
export _BPX_BATCH_SPAWN=NO
export MQSI_MC_MESSAGES=NO
export MQSI_COMMAND_DATABASE_ECHO=1
export MQSI_COMMAND_ZOS_MQ_ECHO=1
export MQSI_COMMAND_ZOS_MQ_ECHO_RC=1
export STEPLIB=CURRENT

#*****
# 6. Other Settings
#*****

```

```
#
# NO NEED TO CHANGE FROM DEFAULT!
#
CP=$MQSI_FILEPATH/classes
CP=$CP:$MQSI_FILEPATH/classes/config.jar
CP=$CP:$MQSI_FILEPATH/classes/ConfigManagerProxy.jar
CP=$CP:$MQSI_FILEPATH/classes/ConfigManagerProxySamples.jar
CP=$CP:$MQSI_FILEPATH/classes/configutil.jar
CP=$CP:$MQSI_FILEPATH/messages
CP=$CP:$JAVAHOME/lib
export CLASSPATH=$CP
XMLTOOLKIT=++XMLTOOLKIT++
LP=$MQSI_FILEPATH/lib/wbirf
LP=$LP:$MQSI_FILEPATH/lib/wbimb
LP=$LP:$MQSI_FILEPATH/lib/wbieb
LP=$LP:$MQSI_FILEPATH/lib
LP=$LP:$JAVAHOME/lib
LP=$LP:$JAVAHOME/bin
LP=$LP:$JAVAHOME/bin/classic
LP=$LP:$XMLTOOLKIT/lib
export LIBPATH=$LP
export PATH=$MQSI_FILEPATH/bin
export PATH=$PATH:$JAVAHOME/bin
```

Security requirements for administrative tasks

This section contains the following topics:

- “ACL permissions”
- “Security requirements for Linux and UNIX platforms” on page 424
- “Security requirements for Windows platforms” on page 425
- “Security requirements for z/OS” on page 428

ACL permissions

WebSphere Event Broker uses Access Control List (ACL) entries to govern which users and groups can manipulate objects in the broker domain. There are four different access levels that can be granted for a user or group: Full, View, Deploy, and Edit. Not all access levels are valid for all object types. The following table lists the actions which can be performed by a user with a given permission:

Object	Permission	Rights
Topology	Full control	<ul style="list-style-type: none">• Create and delete brokers.• Create and delete collectives.• Add and remove brokers from collectives.• Create and delete connections.• Deploy topology.• All topology View permission rights
	View	<ul style="list-style-type: none">• View topology configuration and managed subcomponents.
Broker	Full control	<ul style="list-style-type: none">• Create and delete execution groups.• Edit all broker properties.• All broker Deploy permission rights.• All execution groups Full control permission rights for contained execution groups.• All broker View permission rights.
	Deploy	<ul style="list-style-type: none">• Deploy broker configuration.• All broker View permission rights.
	View	<ul style="list-style-type: none">• View broker configuration and managed subcomponents.• Implicit view access to Topology.
Execution group	Full control	<ul style="list-style-type: none">• Edit all execution group properties.• Start and stop execution groups.• All execution group Deploy permission rights.• All execution group View permission rights.
	Deploy	<ul style="list-style-type: none">• Deploy execution group configuration.• Start and stop assigned message flows.• Start and stop trace.• All execution group View permission rights.
	View	<ul style="list-style-type: none">• View execution group configuration and managed subcomponents.• Implicit View access to parent broker and topology.

Object	Permission	Rights
Root topic	Full control	<ul style="list-style-type: none"> • Edit "Topic Access Control List". • All root topic Deploy permissions. • All root topic Edit permissions. • All root topic View permissions.
	Deploy	<ul style="list-style-type: none"> • Deploy entire topic configuration. • All root topic View permissions.
	Edit	<ul style="list-style-type: none"> • Create and delete child topics. • All root topic View permissions.
	View	<ul style="list-style-type: none"> • View all topics (including child topics), and any managed subcomponents.
Subscription	Full control	<ul style="list-style-type: none"> • Delete any subscription. • All subscription "View" permissions.
	View	<ul style="list-style-type: none"> • View or query all subscriptions and any managed subcomponents.

Security requirements for Linux and UNIX platforms

This table is a summary of the authorizations in a Linux or UNIX environment.

User is...	Linux or UNIX domain
Creating a component	<ul style="list-style-type: none"> • Member of mqbrkrs and mqm. • In most situations, the component runs under the login ID used to issue the create command. When root is used to issue the create command, it can nominate any user to run the component.
Installing	<ul style="list-style-type: none"> • Superuser.
Uninstalling	<ul style="list-style-type: none"> • Superuser.
Changing a component	<ul style="list-style-type: none"> • Member of mqbrkrs.
Deleting a component	<ul style="list-style-type: none"> • Member of mqbrkrs and mqm.
Starting a component	<ul style="list-style-type: none"> • Member of mqbrkrs. • Member of mqm. • Service user ID.
Stopping a component	<ul style="list-style-type: none"> • Member of mqbrkrs. • Member of mqm if -q is specified. • Service user ID.
Listing a component	<ul style="list-style-type: none"> • Member of mqbrkrs.
Changing, displaying, retrieving trace information.	<ul style="list-style-type: none"> • Member of mqbrkrs.
Running User Name Server (login ID).	<ul style="list-style-type: none"> • Member of mqbrkrs. The User Name Server runs under the login ID specified in the create command.
Running broker (WebSphere MQ non-trusted application) (login ID).	<ul style="list-style-type: none"> • Member of mqbrkrs. The broker runs under the login ID specified in the create command.
Running broker (WebSphere MQ trusted application) (login ID).	<ul style="list-style-type: none"> • Login ID must be mqm. • mqm must be a member of mqbrkrs.
Clearing, joining, listing WebSphere MQ publish/subscribe brokers.	<ul style="list-style-type: none"> • Member of mqbrkrs.

User is...	Linux or UNIX domain
Running publish/subscribe applications.	<ul style="list-style-type: none"> Any user, subject to topic and WebSphere MQ queue access control.

Note: When the service user ID is root, all libraries loaded by the broker, including all user-written plug-in libraries and all shared libraries that they might access, also have root access to all system resources (for example, file sets). Review and assess the risk involved in granting this level of authorization.

Security requirements for Windows platforms

The following table summarizes the security requirements for the WebSphere Event Broker administrative tasks. It illustrates what group membership is required if you are using a local security domain defined on your local system SALONE, or a primary domain named PRIMARY, or a trusted domain named TRUSTED. The contents of this table assume that you have created both the Configuration Manager and the User Name Server with the same security domain.

User is...	Local domain (SALONE)	Primary domain (PRIMARY) / Windows Single domain (PRIMARY)	Trusted domain (TRUSTED) / Windows Parent/Child domain in domain tree (TRUSTED)
Creating a broker, Configuration Manager, User Name Server, or database (with mqsicreatedb)	<ul style="list-style-type: none"> Must be a user ID defined in SALONE Member of Administrators 	<ul style="list-style-type: none"> Must be a user ID defined in PRIMARY Member of SALONE\Administrators 	<ul style="list-style-type: none"> Must be a user ID defined in TRUSTED Member of SALONE\Administrators
Changing a broker, Configuration Manager, User Name Server, DatabaseInstanceMgr	<ul style="list-style-type: none"> Must be a user ID defined in SALONE Member of Administrators 	<ul style="list-style-type: none"> Must be a user ID defined in PRIMARY Member of SALONE\Administrators 	<ul style="list-style-type: none"> Must be a user ID defined in TRUSTED Member of SALONE\Administrators
Deleting a broker, Configuration Manager, User Name Server, or database (with mqsideletedb)	<ul style="list-style-type: none"> Member of Administrators 	<ul style="list-style-type: none"> Member of SALONE\Administrators 	<ul style="list-style-type: none"> Member of SALONE\Administrators
Starting a broker, Configuration Manager, User Name Server, or DatabaseInstanceMgr	<ul style="list-style-type: none"> Member of Administrators 	<ul style="list-style-type: none"> Member of SALONE\Administrators 	<ul style="list-style-type: none"> Member of SALONE\Administrators
Listing a broker, Configuration Manager, User Name Server, or DatabaseInstanceMgr	<ul style="list-style-type: none"> Must be a user ID defined in SALONE User ID must have the authority to query the registry values under <i>WebSphereMQIntegrator</i> entry in the registry. Member of mqbrkrs if issuing the command: mqsilist <broker name><execution group name>. 	<ul style="list-style-type: none"> Must be a user ID defined in PRIMARY User ID must have the authority to query the registry values under <i>WebSphereMQIntegrator</i> entry in the registry. Member of PRIMARY\Domain mqbrkrs if issuing the command: mqsilist <broker name><execution group name>. 	<ul style="list-style-type: none"> Must be a user ID defined in TRUSTED User ID must have the authority to query the registry values under <i>WebSphereMQIntegrator</i> entry in the registry. Member of TRUSTED\Domain mqbrkrs if issuing the command: mqsilist <broker name><execution group name>.
Changing, displaying, retrieving trace information	<ul style="list-style-type: none"> Must be a user ID defined in SALONE Member of mqbrkrs 	<ul style="list-style-type: none"> Must be a user ID defined in PRIMARY Member of PRIMARY\Domain mqbrkrs 	<ul style="list-style-type: none"> Must be a user ID defined in TRUSTED Member of TRUSTED\Domain mqbrkrs

User is...	Local domain (SALONE)	Primary domain (PRIMARY) / Windows Single domain (PRIMARY)	Trusted domain (TRUSTED) / Windows Parent/Child domain in domain tree (TRUSTED)
Running a User Name Server (service user ID)	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE • Member of mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY • Member of PRIMARY\Domain mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED • Member of TRUSTED\Domain mqbrkrs
Running a DatabaseInstanceMgr (service user ID)	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE • Member of mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY • Member of PRIMARY\Domain mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED • Member of TRUSTED\Domain mqbrkrs
Running a Configuration Manager (service user ID)	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE • Member of mqbrkrs • Member of mqm • Member of Administrators 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY • Member of PRIMARY\Domain mqbrkrs • Member of SALONE\mqm (see note 1) • Member of SALONE/Administrators 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED • Member of TRUSTED\Domain mqbrkrs • Member of SALONE\mqm (see note 2) • Member of SALONE/Administrators
Running a broker (WebSphere MQ fastpath off) (service user ID)	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE • Member of mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY • Member of PRIMARY\Domain mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED • Member of TRUSTED\Domain mqbrkrs
Running a broker (WebSphere MQ fastpath on) (service user ID)	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE • Member of mqbrkrs • Member of mqm 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY • Member of PRIMARY\Domain mqbrkrs • Member of SALONE\mqm 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED • Member of TRUSTED\Domain mqbrkrs • Member of SALONE\mqm
Clearing, joining, or listing WebSphere MQ Publish/Subscribe brokers	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE • Member of mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY • Member of PRIMARY\Domain mqbrkrs 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED • Member of TRUSTED\Domain mqbrkrs
Running a Message Brokers Toolkit (see note 3)	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE (see note 4). For example, SALONE\User1 is valid, PRIMARY\User2 and TRUSTED\User3 are not. 	<ul style="list-style-type: none"> • For both domain awareness enabled and domain awareness disabled, when using Message Brokers Toolkit ACLs, user IDs must be members of any local ACL groups created on SALONE. 	<ul style="list-style-type: none"> • For both domain awareness enabled and domain awareness disabled, when using Message Brokers Toolkit ACLs, user IDs must be members of any local ACL groups created on SALONE.
Running publish/subscribe applications	<ul style="list-style-type: none"> • Must be a user ID defined in SALONE. For example, SALONE\User1 is valid, PRIMARY\User2 and TRUSTED\User3 are not. 	<ul style="list-style-type: none"> • Must be a user ID defined in PRIMARY. For example, PRIMARY\User2 is valid, SALONE\User1 and TRUSTED\User3 are not. 	<ul style="list-style-type: none"> • Must be a user ID defined in TRUSTED. For example, TRUSTED\User3 is valid, SALONE\User1 and PRIMARY\User2 are not.

Notes:

1. If you are running in a primary domain, you can also:
 - Define the user ID in the domain PRIMARY.
 - Add this ID to the group **PRIMARY\Domain mqm**.
 - Add the **PRIMARY\Domain mqm** group to the group **SALONE\mqm**.
2. If you are running in a trusted domain, you can also:

- Define the user ID in the domain TRUSTED.
 - Add this ID to the group TRUSTED\Domain **mqm**.
 - Add the TRUSTED\Domain **mqm** group to the group SALONE\mqm .
3. All Message Brokers Toolkit users need read access to the WebSphere MQ java \lib subdirectory of the WebSphere MQ home directory (the default is X:\Program Files \WebSphere MQ , where X: is the operating system disk). This access is restricted to users in the local group **mqm** by WebSphere MQ. WebSphere Event Broker installation overrides this restriction and gives read access for this subdirectory to all users.
 4. If a valid user ID is defined in the domain used by the Configuration Manager (for example, PRIMARY\User4), an identical user defined in a different domain (for example, DOMAIN2\User4) can access the Message Brokers Toolkit with the authorities of PRIMARY\User4.
 5. Ensure that the service user ID has the required access to relevant directories of the product directory tree; for example, write access to the logs directory. If a workpath other than the default has been set for any component, ensure that the services user ID has appropriate access to this location.
 6. If you are running a Configuration Manager with one user ID and a broker with a different user ID on another computer, you might see an error message when trying to deploy message flows to the broker. To avoid this, do the following:
 - Ensure that the broker's user ID is a member of the **mqm** and **mqbrkrs** groups.
 - Define the broker's user ID on the computer where the Configuration Manager is running.
 - Define the Configuration Manager's user ID on the computer where the broker is running.
 - Ensure that all IDs are in lowercase so that they are compatible between computers.

Broker security changes with Windows 2000 and Windows XP

On Windows 2000 and Windows XP, the service user ID must be a member of the mqbrkrs group and optionally a member of the Administrators group. As a member of the Administrators group, the service user ID has permission to access the registry keys of the broker so that it can access broker information. If the service user ID does not belong to the Administrators group, you can edit the Windows registry so that the service user ID can access the registry keys without having Administrators permissions.

To edit the registry on Windows 2000 and Windows XP:

- **Windows 2000**
 1. Run regedt32
 2. Select HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ WebsphereMQSeriesIntegrator
 3. Select **Permissions** from the Security menu in the title bar
 4. Click **Add** on the Permissions for WebsphereMQIntegrator window. From the popup list, select the **mqbrkrs** group and click **Add**. Click **OK**.
 5. Click **Advanced** on the Permissions for WebsphereMQIntegrator window

6. On the Access Control Settings for WebSphereMQIntegrator window, highlight **mqbrkrs** and click **View/Edit**
 7. On the Permission Entry for WebSphereMQIntegrator window, select **Set Value, Create Subkey, and Delete**. Ensure that the **Allow inheritable permissions** box is ticked and then click **OK**
 8. Click **OK** on the remaining screens to exit the editing of the registry
 9. Exit regedt32.
- **Windows XP**
 1. Run regedt32
 2. Select HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebsphereMQSeriesIntegrator
 3. Select **Permissions** by right-clicking on **WebsphereMQSeriesIntegrator**
 4. Click **Add** on the Permissions for WebsphereMQIntegrator window. From the Select Users or Groups window, select **Advanced** and then **Find Now** to list users/groups. From the list, select the **mqbrkrs** group and click **OK** twice
 5. Click **Advanced** on the Permissions for WebsphereMQIntegrator window
 6. On the Advanced Security Settings for WebSphereMQIntegrator window, highlight **mqbrkrs** and click **Edit**
 7. On the Permission Entry for WebSphereMQIntegrator window, select **Set Value, Create Subkey, and Delete**. Ensure the **Inherit from parent** box is ticked and then click **OK**
 8. Click **OK** on the remaining screens to exit the editing of the registry
 9. Exit regedt32.

Security requirements for z/OS

This table is a summary of the UNIX System Services file access authorizations in a z/OS environment.

User is...	File access
Creating broker, User Name Server, Configuration Manager	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS user ID issuing the command • The broker, User Name Server and Configuration Manager run under their z/OS assigned started task ID
Installing	<ul style="list-style-type: none"> • READ and WRITE access to the installation directory by the z/OS user ID installing the product
Uninstalling	<ul style="list-style-type: none"> • READ and WRITE access to the installation directory by the z/OS user ID uninstalling the product
Changing broker, User Name Server, Configuration Manager	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS user ID issuing the command
Deleting broker, User Name Server, Configuration Manager	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS user ID issuing the command
Starting broker, User Name Server, Configuration Manager	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS assigned started task user ID
Stopping broker, User Name Server, Configuration Manager	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS assigned started task user ID
Listing broker, User Name Server, Configuration Manager	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS user ID issuing the command

User is...	File access
Changing, displaying, retrieving trace information.	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS user ID issuing the command
Clearing, joining, listing WebSphere MQ publish/subscribe brokers.	<ul style="list-style-type: none"> • READ and WRITE access to the component directory by the z/OS assigned started task user ID • Member of mqbrkrs group
Running publish/subscribe applications.	<ul style="list-style-type: none"> • Any user, subject to topic and WebSphere MQ queue access control.

Related concepts

“Authorization to access runtime resources” on page 4

Related tasks

“Setting up z/OS security” on page 28

“Setting up broker domain security” on page 11

“Enabling topic-based security” on page 23

Related reference

“Summary of required access (z/OS)” on page 372

“Customization tasks and roles on z/OS” on page 371

Part 5. Appendixes

Appendix. 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 information 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 information. The furnishing of this information does not give 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:

*IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032,
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 may 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 information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information 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 United Kingdom Laboratories,
Mail Point 151,
Hursley Park,
Winchester,
Hampshire,
England
SO21 2JN*

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 information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Programming License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information includes 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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

(C) *(your company name) (year)*. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. *_enter the year or years_*. All rights reserved.

Trademarks

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

AIX	CICS	Cloudscape
DB2	DB2 Connect	DB2 Universal Database
developerWorks	Domino	
Everyplace	FFST	First Failure Support Technology
IBM	IBMLink	IMS
IMS/ESA	iSeries	Language Environment
Lotus	MQSeries	MVS
NetView	OS/400	OS/390
POWER	pSeries	RACF
Rational	Redbooks	RETAIN
RS/6000	SupportPac	S/390
Tivoli	VisualAge	WebSphere
xSeries	z/OS	zSeries

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Index

A

- access control lists 32
 - permissions 423
- administration
 - broker domain 211
 - security requirements 423
 - z/OS 368
- authentication 37
 - implementing 19
 - SSL 8
- authorization for configuration tasks 3

B

- backup
 - broker domain
 - distributed systems 225
 - z/OS 227
 - resources 225
 - Message Brokers toolkit workspace 228
- Broker Administration perspective
 - changing preferences 200
- broker database
 - changing access 164
 - connections 93
 - failure 164
- broker domain
 - adding a broker 175
 - administration 211
 - configuring 51
 - components 83
 - in the workbench 171
 - configuring locales 202
 - code page converters 206
 - generating code page converters 206
 - UNIX 203
 - using converters from a previous product level 207
 - Windows 204
 - z/OS 205
 - connecting and disconnecting 211
 - connecting and disconnecting on z/OS 212
 - default configuration 150
 - designing 52
 - log information
 - clearing 224
 - filtering 222
 - refreshing 221
 - saving 223
 - viewing 220
 - removing a broker 178
- broker domains
 - security 11
- broker networks 183
 - heterogeneous 187
 - migrated 187
- broker statistics, collecting on z/OS 80

- Broker Topology editor
 - changing properties 187
- brokers
 - adding 175
 - changing 155
 - Linux and UNIX systems 156
 - Windows 157
 - z/OS 158
 - cloned 186
 - connecting a user name server 145
 - connecting in a collective 188
 - copying 176
 - creating 108
 - AIX 110
 - HP-UX 112
 - Linux 113
 - Solaris 114
 - Windows 115
 - customizing a new broker on z/OS 116
 - component dataset operations 119
 - Component information 118
 - copying the started task 122
 - creating the broker
 - component 122
 - creating the broker directory 122
 - creating the broker PDSE 118
 - creating the environment file 120
 - customizing the JCL 119
 - DB2 information 117
 - installation information 117, 140
 - JCL variables 382
 - priming DB2 121
 - required information 117
 - sample files 385
 - deleting 166
 - Linux and UNIX systems 166
 - Windows 166
 - z/OS 167
 - execution groups, adding 179
 - execution groups, copying 180
 - modifying 155
 - Linux and UNIX systems 156
 - Windows 157
 - z/OS 158
 - properties 231
 - changing 177
 - removing 178
 - removing deployed children 179
 - renaming 177
 - sample files, z/OS
 - BIPBPROF 385
 - BIPBRKP 390
 - BIPCBRK 394
 - BIPCRDB 403
 - BIPDSNAO 413
 - BIPEDIT 414
 - BIPGEN 415
 - security 15
 - service ID 15
 - starting and stopping 214

- brokers (*continued*)
 - UNIX 215
 - Windows 215
 - z/OS 216
 - user name server, connecting on z/OS 146
 - WebSphere MQ resources 55

C

- c security on z/OS 149
- channels, starting WebSphere MQ 147
- characters allowed in commands 240
- cloned brokers 186
 - adding 196
 - defining 196
 - deleting 197
- code page converters 206
 - new 206
 - using converters from a previous product level 207
- collectives 184
 - adding a broker 188
 - creating 188
 - deleting 188
 - removing a broker 189
- Command Assistant wizard 151
- commands 232
 - characters allowed in 240
 - mqsicreatedb 300
 - responses to 242
 - rules for using 241
 - runtime 248
 - mqsi_setupdatabase 356
 - mqsibackupconfigmgr 248
 - mqsicbrreport 249
 - mqsichangebroker 250
 - mqsichangeconfigmgr 256
 - mqsichangedbimgr 259
 - mqsichangeflowstats 260
 - mqsichangeproperties 264
 - mqsichangetrace 274
 - mqsichangeusernameserver 279
 - mqsiclearmqpubsub 282
 - mqsicreateaclentry 283
 - mqsicreatebroker 286
 - mqsicreateconfigmgr 296
 - mqsicreatedb 300
 - mqsicreateexecutiongroup 302
 - mqsicreateusernameserver 305
 - mqsideleteaclentry 308
 - mqsideletebroker 311
 - mqsideleteconfigmgr 313
 - mqsidedeletedb 315
 - mqsideleteexecutiongroup 316
 - mqsideleteusernameserver 318
 - mqsidedeploy 320
 - mqsiformatlog 325
 - mqsijoinmqpubsub 327
 - mqsilist 328
 - mqsilistaclentry 330

- commands (*continued*)
 - runtime (*continued*)
 - mqsilistmqpubsub 335
 - mqsigratecomponents 337
 - mqsireadlog 342
 - mqsireload 346
 - mqsireportflowstats 347
 - mqsireportproperties 349
 - mqsireporttrace 351
 - mqsirestoreconfigmgr 354
 - mqsisetsecurity 355
 - mqsistart 357
 - mqsistartmsgflow 359
 - mqsistop 362
 - mqsistopmsgflow 365
 - syntax preference 236
 - dotted decimal diagrams 238
 - railroad diagrams 236
 - toolkit 242
 - mqscreatebar 242
 - mqsimigratemfmaps 244
 - mqsimigratemsgflows 245
 - mqsireadbar 247
 - z/OS console
 - guidance on using 369
 - issuing to 368
- components
 - connecting 153
 - definition on z/OS 63
 - directory 63
 - PDSE 64
 - verifying 153
- configuration
 - authorization 3
 - broker database 93
 - broker domain 51
 - components 83
 - in the workbench 171
 - database
 - accessing 106
 - connecting to 92
 - creating 85
 - creating a DB2 database on UNIX systems 88
 - creating a DB2 database on Windows 87
 - customizing 92
 - issuing database commands 90
 - preparing databases on UNIX 86
 - retained publications with a Sybase database 108
 - using Derby databases on Windows 89
 - default 150
 - publish/subscribe topology 182
- Configuration Manager
 - changing 158
 - Linux and UNIX systems 159
 - Windows 160
 - z/OS 160
 - creating 125
 - AIX 125
 - HP-UX 126
 - Linux 127
 - Solaris 128
 - Windows 129
 - creating on z/OS 130

- Configuration Manager (*continued*)
 - component information 131
 - copying the started task 135
 - creating the component 133
 - creating the directory 131
 - creating the PDSE 131
 - Customizing the component data set 132
 - customizing the JCL 132
 - information required 130
 - installation information 130
 - deleting 167
 - Linux and UNIX systems 168
 - Windows 168
 - z/OS 169
 - modifying 158
 - moving to new queue manager 161
 - sample files, z/OS
 - BIPCMGR 396
 - BIPCPROF 398
 - BIPCRCM 401
 - security 16
 - service ID 16
 - starting and stopping 216
 - Linux and UNIX systems 216
 - Windows 217
 - z/OS 217
 - WebSphere MQ resources 56
- creating user IDs 12
- customization
 - z/OS 370
 - broker PDSE, contents of 378
 - Configuration Manager PDSE, contents of 380
 - DB2 using data-sharing groups 377
 - disk space requirements 376
 - naming conventions 370
 - overview 62
 - planning checklist 378
 - summary of required access 372
 - tasks and roles 371
 - User Name Server PDSE, contents of 379
 - z/OS environment 60
 - APF attributes, checking 79
 - DB2 planning 73
 - event log messages 65
 - file system, mounting 78
 - file system, using 65
 - installation directory, checking permission of 78
 - level of Java, checking 79
 - resource recovery service planning 77
 - shared libraries 71
 - temporary directories 71
 - UNIX system services 71
 - z/OS workload manager, defining started tasks to 77
- CVS 202

D

- data-sharing groups, binding a DB2 plan to 64
- database access, changing 164

- database access, changing (*continued*)
 - broker database 164
- database connections
 - broker database 93
 - ODBC drivers 92
- Database Instance Manager 89
- databases
 - accessing 106
 - setting your environment 106
 - broker 164
 - connecting to 92
 - on UNIX (32-bit databases) 95
 - on UNIX (64-bit databases) 100
 - on Windows 93
 - creating 85
 - customizing 92
 - database commands, issuing 90
 - DB2 on UNIX systems, creating 88
 - DB2 on Windows, creating 87
 - Derby databases on Windows, using 89
 - naming conventions 54
 - preparing on UNIX 86
 - security 27
 - Sybase, retained publications 108
- DbInstMgr 89
- Default Configuration wizard 150
- deployment
 - deployed children
 - removing from broker 179
 - removing from execution group 182
- development resources, security for 4
- directories, components 63
- domain awareness 10
 - enabling and disabling 13
- domain connections
 - changing properties 173
 - creating 172
 - deleting 174
 - properties 173
- dotted decimal diagrams, reading 238

E

- editors
 - palette
 - customizing 201
 - layout, changing 201
 - preferences, changing 200
 - settings, changing 201
- error logs
 - broker domain logs
 - clearing 224
 - filtering 222
 - refreshing 221
 - saving 223
 - viewing 220
- Event Log editor
 - changing preferences 224
- execution groups
 - adding 179
 - command line, using 123
 - z/OS 124
 - configuring as non-swappable on z/OS 80
 - copying 180

execution groups (*continued*)
 deleting 181
 deleting through command line 165
 deployed children, removing 182
 properties, changing 181
 renaming 181

F

fastpath applications 109

H

high-volume publish/subscribe on
 z/OS 195
HTTP tunneling 9
 implementing 26

I

installation
 directory 62
 INSTPATH 62
 security 11

L

leaf nodes 187
listeners, starting WebSphere MQ 147
locales
 changing 202
logs
 broker domain logs
 clearing 224
 filtering 222
 refreshing 221
 saving 223
 viewing 220

M

message flows
 starting 214
 stopping 214
 throughput, optimizing 58
message protection 40
 using for Real-time connections 47
message serialization
 input between separate brokers 66
 input between separate execution
 groups 68
 input within an execution group 69
 overview of 66
 user tasks 70
mqbrkrs group 32
multicast brokers
 choosing a protocol 194
 mqsisetproperties command 189
 setup parameters 189
multicast protocols 194
multicast publish/subscribe 185
multicast topics 195

N

National Language Support
 UNIX syslog 203

O

ODBC
 32-bit connection, defining on
 UNIX 95
 64-bit connection, defining on
 UNIX 100
 connection
 defining on Windows 93
 editing .odbc.ini parameters 103
 editing .odbc64.ini parameters 105
Oracle
 granting user access 27
 revoking user access 27
order
 choosing messaging processing
 order 58

P

palette
 customizing 201
 layout, changing 201
 preferences, changing 200
 settings, changing 201
parent nodes 187
password authentication 37
 mutual challenge-response 37
 telnet-like 37
performance
 considerations for design 58
 message flow throughput 58
planning
 database naming conventions 54
 product component naming
 conventions 53
 resource naming conventions 52
 WebSphere MQ naming
 conventions 53
product component naming
 conventions 53
publish/subscribe
 adding a topic 198
 configuring a topology 182
 deleting a topic 198
 enabling applications 149
 multicast 185
 querying a subscription 199
 securing the domain 41
 security 32
 enabling applications on
 z/OS 149
 topic-based 32
 topologies 183

Q

quality of protection 10
 implementing 26
queue managers
 starting as a Windows service 219

queue managers (*continued*)
 stopping 220

R

railroad diagrams, reading 236
Real-time connections, message
 protection 47
repositories, CVS 202
resources
 resource naming conventions 52
responses to commands 242
rules
 using commands 241
runtime resources, controlling access
 to 5
runtime resources, security for 4

S

security 3
 access control list (ACL)
 permissions 423
 Access Control Lists 5
 administrative tasks 423
 broker 15
 broker domain 11
 Configuration Manager 16
 databases 27
 development resources 4
 planning for installation 11
 quality of protection 10
 runtime resources 4
 security domain
 User Name Server, changing
 for 19
 security exits 8
 topic-based 23, 41
 UNIX 424
 User Name Server 23, 41
 Windows 425
 workbench 13
 z/OS 428
security domain
 User Name Server, changing for 19
security exits 8
 invoking 26
SQL server
 granting user access 27
 revoking user access 27
SSL authentication 8
 implementing 19
 MQ Java Client 19
 Real Time node 20
Sybase
 granting user access 27
 revoking user access 27
system topics 32

T

throughput
 optimizing message flows 58
topic-based security 32
 enabling 23, 41

- topics
 - making multicast 195
- trademarks 435
- trusted applications 109
- tunneling 9
 - implementing 26

U

- Unicode 206
- UNIX
 - National Language Support for syslog 203
- User Name Server
 - broker, connecting on z/OS 146
 - broker, connecting to 145
 - changing 161
 - Linux and UNIX systems 162
 - Windows 163
 - z/OS 163
 - configuring publish/subscribe security 145
 - connecting to the network 145
 - creating 136
 - AIX 136
 - HP-UX 137
 - Linux 137
 - Solaris 138
 - Windows 139
 - creating on z/OS 139
 - component information 140
 - copying the started task 144
 - creating the component 144
 - creating the component dataset 142
 - creating the directory 141
 - creating the PDSE 141
 - creating the runtime environment 141
 - customizing the JCL 143
 - information required 140
 - installation information 117, 140
 - deleting 169
 - Linux and UNIX systems 170
 - Windows 170
 - z/OS 170
 - disabling 169
 - enabling 135
 - sample files, z/OS
 - BIPCRUN 411
 - BIPUNSP 417
 - BIPUPROF 419
 - security 23, 41
 - security domain, changing 19
 - starting and stopping 217
 - UNIX 218
 - Windows 218
 - z/OS 219
 - WebSphere MQ resources 57

W

- WebSphere MQ
 - infrastructure
 - designing 54
 - resources for brokers 55

- WebSphere MQ (*continued*)
 - infrastructure (*continued*)
 - resources for the Configuration Manager 56
 - resources for the User Name Server 57
 - naming conventions 53
 - planning for z/OS 76
 - securing resources 47
 - starting
 - channels 147
 - listeners 147
 - trusted applications 109
- wildcard topics 32
- Windows service, starting a queue manager 219
- workbench
 - changing preferences 199
 - configuring a broker domain 171
 - security 13

X

- XPLink 64

Z

- z/OS
 - administration 368
 - Configuration Manager
 - connecting directly to 82
 - connecting through intermediate queue manager 82
 - customization 370
 - broker PDSE, contents of 378
 - Configuration Manager PDSE, contents of 380
 - DB2 using data-sharing groups 377
 - disk space requirements 376
 - naming conventions 370
 - planning checklist 378
 - summary of required access 372
 - tasks and roles 371
 - User Name Server PDSE, contents of 379
 - customization variables, JCL 382
 - customizing the environment 60
 - APF attributes, checking 79
 - DB2 planning 73
 - event log messages 65
 - file system 65
 - installation directory, checking permission of 78
 - level of Java, checking 79
 - mounting file systems 78
 - resource recovery service
 - planning 77
 - shared libraries 71
 - temporary directory space 71
 - TMPDIR 71
 - UNIX system services 71
 - z/OS workload manager, defining started tasks to 77
 - guidance for issuing console commands 369

- z/OS (*continued*)
 - issuing commands to the console 368
 - Message Brokers components, creating 80
 - moving from a distributed environment 164
 - security considerations 65
 - creating Publish/Subscribe user IDs 31
 - enabling the Configuration Manager to obtain user ID information 31
 - setting up DB2 29
 - setting up WebSphere MQ 30
 - setting up workbench access 31
 - setting up z/OS security 28
 - specific information 367
 - START and STOP commands 369
 - WebSphere MQ planning 76



Printed in USA