WebSphere MQ

Migration Information
Some issues affecting migration to IBM WebSphere MQ, Version 6.0

Version 6.0

SC34-6604-01

WebSphere MQ

Migration Information
Some issues affecting migration to IBM WebSphere MQ, Version 6.0

Version 6.0

SC34-6604-01

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

Second edition (October 2005)

This edition applies to IBM WebSphere MQ, Version 6.0 and to all subsequent releases and modifications, unless otherwise indicated in new editions.

Contents

Introduction to WebSphere MQ Version 6.0 migration

This section gives an introduction to the documentation for customers considering migrating to WebSphere® MQ Version 6.0.

The migration process is described, and instructions given, in the *Quick Beginnings* book for your platform, or, for z/OS, in the *WebSphere MQ for z/OS System Setup Guide* and the *Program Directory for WebSphere MQ for z/OS*.

It is not the intention of this document to cover the migration of every possible combination of a WebSphere MQ Version 6.0 installation and associated applications. This would not be possible as the product is so flexible. This document highlights some of the main areas that are believed to impact a customer and give some guidance of the type of action you will need to take to continue 'business as usual'.

Note: Prior to the installation or migration of any software, you are recommended to make a full backup of your system to ensure that you can recreate the system to its original working environment should any problems occur.

Some general considerations

The following lists some of the general issues to consider when making a migration plan.

- Additional migration information is held in the Quick Beginnings book for the platform you are installing on (or the System Setup Guide for z/OS). You are recommended to consult the relevant Quick Beginnings book for any migration information that could affect the installation you are preparing for.
- Develop a backup plan in which you back up the relevant information on the queue manager and server.
- Read the latest README file for the product you are working with. You can find these files on the IBM® home pages for the relevant products.
- Do you need to have the queue manager active all the time? If this is the case, and you are unable to shut down the system running this queue manager, you might need to consider a different migration approach. This will mean performing the migration using the following general steps:
  - Copy all resources from the server concerned to another server.
  - Perform a migration on the duplicate server.
  - Switch over to the new server and queue manager at a convenient time.
- Be prepared to record a number of details about the existing system topology, including such things as the names of the queue managers and their queues, clients, channels and so on.
- This is also a good time to check through all existing queue managers to see whether there are any queues that are no longer needed, and whether there are any queue managers that are no longer required. You might also decide that you want to keep certain queue managers at an earlier level and administer them from a migrated system.
- After you migrate a queue manager to WebSphere MQ Version 6.0, you must start that queue manager to migrate your file system structure before you start

any WebSphere MQ listener associated with that queue manager. Otherwise, you will not be able to start WebSphere MQ listeners after migration.

Migrating from a beta version

If you have previously installed a WebSphere MQ Version 6.0 Beta driver, you MUST uninstall this driver BEFORE you install the GA version of WebSphere MQ Version 6.0.

Supported environments

The supported environments vary according to the changes to the product. Please check each of the sections for details of the environment that is impacted.

Note: Where WebSphere MQ Version 5.3 is stated, it also applies to WebSphere MQ Version 5.3.1 on z/OS.

64-bit queue manager migration information

This section provides you with information regarding the changes that might be necessary for applications to continue working now that WebSphere MQ Version 6.0 has introduced the 64-bit queue manager.

Introduction

Attention: On platforms where there is a 32-bit WebSphere MQ Version 6.0 product, for example, Linux (x86 platform), there is no migration path from 32-bit WebSphere MQ Version 6.0 queue managers to 64-bit WebSphere MQ Version 6.0 queue managers. If you wish to use a 64-bit WebSphere MQ Version 6.0 product on a machine where there was previously a 32-bit WebSphere MQ Version 6.0 installation, you will be prevented from starting any of the existing queue managers. Note however that migration from 32-bit queue managers in previous versions of WebSphere MQ , for example Version 5.3, is supported.

With the queue manager becoming 64-bit for some distributed platforms, it removes many of the 32-bit addressing limitations. It gives a large increase to the amount of memory available for applications and WebSphere MQ, and the number and size of shared storage segments is also increased.

This move to 64-bit queue managers will be transparent to most applications. However, a small number of 32-bit applications will no longer work as they will need some of the files they interact with to be built as 64-bit versions. This migration documentation provides information to help you identify those applications and those files that will be needed as 64-bit.

Where other changes have been made, and where these could have an impact on your current installation without your applications requiring a change (for example, performance), these have also been identified. As a general rule, 32-bit applications will not need to be modified, but 32-bit switches and exits will need to be rebuilt.

Affected environments

The 64-bit queue manager is now supported on the following WebSphere MQ Version 6.0 platforms:

- AIX®
- HP-UX
- Linux® (POWER™ platform)
- Linux (x86-64 platform)
- Sun Solaris

API implications

There are no changes to the API for existing applications to continue to work using 32-bit addressing (as will 64-bit addressing if the 64-bit client SupportPac™ has been installed) as 32-bit libraries are supplied for binary compatibility in WebSphere MQ Version 6.0.

Existing 64-bit client applications will continue to be able to take advantage of using their 64-bit client processes, without changes to the application API being required.

Although the API has not changed, you need to be aware that in WebSphere MQ Version 5.3 and earlier versions, an `MQLONG`, an `int`, a `long`, and a `size_t` were all 32-bit so effectively interchangeable in their use. In WebSphere MQ Version 6.0 this is no longer true as a `long`, and a `size_t` are now 64-bit on at least some platforms.

You also need to be aware that pointers for 64-bit applications and 64-bit MQ exits will be 64-bit. If your user-exits were storing pointers in a WebSphere MQ exit `ExitUserArea`, which is an `MQBYTE16`, you will now only be able to store two pointers. This will not cause you a problem if you have written your user-exit to store a pointer to a block of pointers in the `ExitUserArea`. If your exits have not been written in this way, you will need to rewrite them to use this approach if there is now no longer enough room in `ExitUserArea` to store the pointers that your application needs.

The following table gives you the sizes of the basic 'C' types to aid you to see where similar problems might occur.

Table 1. Data type platform sizes for 32-bit and 64-bit applications (Bracketed figures are for 64-bit size)

Data type	Sun Solaris	HP-UX	AIX	Linux (POWER platform)	Linux (x86-64 platform)	Linux (zSeries 64-bit platform)
char	1 byte (1 byte)	1 byte (1 byte)	1 byte (1 byte)	1 byte (1 byte)	1 byte (1 byte)	1 byte (1 byte)
short	2 bytes (2 bytes)	2 bytes (2 bytes)	2 bytes (2 bytes)	2 bytes (2 bytes)	2 bytes (2 bytes)	2 bytes (2 bytes)
int	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)
long	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)
float	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)
double	8 bytes (8 bytes)	8 bytes (8 bytes)	8 bytes (8 bytes)	8 bytes (8 bytes)	8 bytes (8 bytes)	8 bytes (8 bytes)
long double	16 bytes (16 bytes)[1]	16 bytes (16 bytes)	8 bytes (8 bytes)	8 bytes (8 bytes)	12 bytes (16 bytes)	8 bytes (8 bytes)
pointer	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)
ptrdiff_t	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)
size_t	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)
time_t	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)
clock_t	4 bytes (8 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)	4 bytes (8 bytes)
wchar_t	4 bytes (4 bytes)	4 bytes (4 bytes)	2 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)	4 bytes (4 bytes)

Note: 1. A 32-bit long double on Sun Solaris for x86-64 is 12 bytes.

WebSphere MQ Version 6.0 bindings

Three sets of bindings will be provided for 64-bit applications: isolated; Standard and fastpath bindings. For 32-bit applications only isolated and Standard bindings will be available. If a 32-bit application tries to connect to the queue manager via a fastpath binding it will be silently downgraded to Standard bindings. This will cause a noticeable loss of performance (it has virtually identical performance as when connecting directly with a Standard binding) to anyone currently using fastpath and who is unwilling or unable to port the application to 64-bit. If you require to connect your 32-bit applications using fastpath bindings because performance is an issue, and you intend to keep your applications as 32-bit applications, then you will have to remain with WebSphere MQ Version 5.3.

EXTSHM on WebSphere MQ for AIX

Setting EXTSHM for WebSphere MQ for AIX will no longer allow more than ten MQ shared storage segments to be attached to a 32-bit application process. This is because the WebSphere MQ shared storage segments will have been created by a 64-bit process and these have no concept of EXTSHM. Any setting of EXTSHM has no effect in WebSphere MQ Version 6.0.

32-bit customer WebSphere MQ applications will revert to the pre-WebSphere MQ Version 5.3 limit of ten shared storage segments. If your applications are using standard bindings, you might run into resource problems due to this limitation. This limitation can be avoided by using isolated bindings. Do this by replacing MQCONN calls with MQCONNX, and specifying MQCNO_ISOLATED_BINDING in the MQCNO parameter of the MQCONNX calls.

There is virtually no limit to the number of shared storage segments created using 64-bit applications.

32-bit and 64-bit files

This section provides you with information that will help you identify where you will need to replace your 32-bit files with 64-bit versions.

Executable files and libraries

For WebSphere MQ for AIX, WebSphere MQ for HP-UX,WebSphere MQ for Sun Solaris, and WebSphere MQ for Linux, Version 6.0 (POWER platform), the majority of WebSphere MQ Version 6.0 files are built as 64-bit files.

All the executable files in `/xxx/mqm/bin` and `/xxx/mqm/samp/bin` are 64-bit.

Most of the WebSphere MQ Version 6.0 libraries are 64-bit and put into `/xxx/mqm/lib64` as the Version 5.2 and 5.3 64-bit client SupportPac libraries have been. Like the 64-bit client SupportPacs, there are no symbolic links to the `/xxx/mqm/lib64` directory. Any existing 64-bit client applications will continue to work.

The few libraries that are required by 32-bit applications are installed as usual in `/xxx/mqm/lib` and any current customer 32-bit applications will continue to work (subject to changes needed to exits and switches. See below.) after upgrading to WebSphere MQ Version 6.0.

If you are using 64-bit applications, you might encounter problems if your LIBPATH or LD_LIBRARY_PATH variable includes the /usr/lib directory. The /usr/lib directory contains symbolic links to the 32-bit WebSphere MQ libraries, which do not work with 64-bit applications. Either remove /usr/lib from your library path or remove the symbolic links from /usr/lib. For more information, see the *Quick Beginnings* guide for your platform.

Exits and switch load files

When using 32-bit applications with a 64-bit queue manager, some types of exit and XA switch load files will also need to have a 64-bit version available for use by the queue manager. If the 64-bit version of the exit or XA switch load file is required and is not available, then the relevant MQ API or command will fail.

Two attributes are supported in the mqs.ini and qm.ini files for `ClientExitPath`. These are `ExitsDefaultPath=/var/mqm/exits` and `ExitsDefaultPath64=/var/mqm/exits64`. Using these ensures that the appropriate library can be found. If an exit is used in a WebSphere MQ cluster, this will also ensure that the appropriate library on a remote system will be found.

Where you have used your own directory and use a fully qualified path, you are advised to create a symbolic link from the `ExitsDefaultPath` and `ExitsDefaultPath64` to the appropriate library. Should this not be provided, WebSphere MQ Version 6.0 will search for the library and use the first matching library in the search path. If the library is still not found an error message is generated.

The following table lists the different types of Exit and Switch load files and notes whether 32-bit or 64-bit versions, or both, are required, according to whether 32-bit or 64-bit applications are being used:

File types	32-bit applications	64-bit applications
API crossing exit	32-bit and 64-bit	64-bit
Data conversion exit	32-bit	64-bit
Server Channel exits (all types)	64-bit	64-bit
Client Channel exits (all types)	32-bit	64-bit
Installable service exit	64-bit	64-bit
Service trace module	32-bit and 64-bit	64-bit
Cluster WLM exit	64-bit	64-bit
Pub/Sub routing exit	64-bit	64-bit
Database switch load files	32-bit and 64-bit	64-bit
External Transaction Manager AX libraries	32-bit	64-bit

Communications protocols

The only supported communications protocols for 64-bit applications are TCP and LU 6.2. Applications will require the appropriate communications libraries to be available to them.

- A 32-bit client application will require the 32-bit communication library.

- A 64-bit client application will require the 64-bit communication library.
- On a 64-bit queue manager, the MQ channel processes are 64-bit and will require the 64-bit communication library.

Note: With TCP, SSL is available for both 32-bit and 64-bit applications.

Internal Transactional Manager XA support

WebSphere MQ Version 6.0 no longer supports versions of databases that do not include 64-bit support. You will need to rebuild your switch load files for these databases to support 64-bit processing as well as upgrading the databases to 64-bit versions. If you fail to do this, you will get an error when you start the queue manager and your application will fail to do any work with the database.

COBOL copybooks

This section provides you with information in relation to the changes to the COBOL copybooks supplied with WebSphere MQ Version 6.0.

Due to the size of structures with pointers growing on 64-bit platforms, the lengths defined in some of the COBOL copybooks supplied with earlier versions of WebSphere MQ are incorrect for 64-bit applications. Updated COBOL copybooks are being supplied with WebSphere MQ Version 6.0 as follows:

WebSphere MQ for z/OS®

64-bit COBOL copybooks are not shipped in this release of the product.

WebSphere MQ for AIX

All 32-bit COBOL copy books will be installed in the directory `/usr/mqm/inc/cobcpy32`.

Symbolic links to all the 32-bit COBOL copy books will be created in directory `/usr/mqm/inc`.

All 64-bit COBOL copy books will be installed in the directory `/usr/mqm/inc/cobcpy64`.

All other UNIX® platforms

All 32-bit COBOL copy books will be installed in the directory `/opt/mqm/inc/cobcpy32`.

Symbolic links to all the 32-bit COBOL copy books will be created in directory `/opt/mqm/inc`.

All 64-bit COBOL copy books will be installed in the directory `/opt/mqm/inc/cobcpy64`.

WebSphere MQ for Windows®

All 32-bit COBOL copy books will be installed in the directory `C:\Program Files\IBM\WebSphere MQ\Tools\cobol\copyBook32` and in `C:\Program Files\IBM\WebSphere MQ\Tools\cobol\copyBook`.

Note: `C:\Program Files\IBM\WebSphere MQ` is the default directory for the installation of WebSphere MQ for Windows. If you install it in a different directory, you will adjust the specified path to take this into account.

Internet Protocol Version 6 (IPv6) migration

This section deals with using IPv4 and IPv6 when you are thinking of installing WebSphere MQ Version 6.0

General Introduction

The Internet Protocol Version 6 (IPv6) is designed by the Internet Engineering Task Force (IETF) to replace the current version Internet Protocol, Version 4 (IPv4). IPv4 has been around for over 20 years and is one of the primary methods for machines to communicate to each other over the internet. IPv4 is limited to 32-bit addressing for internet addresses. These addresses are needed by all new machines added to the internet and they are beginning to run out. The IETF is the controlling standards body for the Internet and to meet the growing demand for internet addresses has increased the number of digits used for Internet addresses from 32 to 128 bits. IPv6 offers a far larger number (2^{128}) of internet addresses and should solve the address shortage for the foreseeable future. IPv6 is expected to gradually replace IPv4, with the two protocols coexisting for a number of years while this transition period exists. IPv6 also simplifies header formats and improves support for extensions and options, flow labeling capability, and consolidated authentication and privacy capabilities

WebSphere MQ Version 6.0 introduces the ability for queue managers to communicate using the IPv6 protocol in addition to the existing, IPv4, protocol.

Further information on IPv6 can be found at http://www.ipv6.org/ and http://www.ipv6forum.com/.

WebSphere MQ platforms that support IPv6

This section lists the WebSphere MQ Version 6.0 platforms that support IPv6.

IPv6 is supported on the following WebSphere MQ Version 6.0 platforms:

- WebSphere MQ for AIX (5.2 or later)
- WebSphere MQ for Linux (2.4 or later)
- WebSphere MQ for Sun Solaris (2.8 or later)
- WebSphere MQ for HP-UX (11i or later)
- WebSphere MQ for Windows (XP SP1 or later, Windows 2003 Server)
- WebSphere MQ for iSeries™ (V5R2 or later)
- WebSphere MQ for z/OS (V1R4 or later)

IPv6 is not supported in WebSphere MQ running on Windows 2000 as this platform does not currently have a supported IPv6 protocol implementation.

For the Java™ client, IPv6 is currently supported on the following WebSphere MQ Version 6.0 platforms:

- Sun Solaris 8 or later - Java 2 Platform, Standard Edition 1.4 (J2SE 1.4)
- Linux Kernel 2.4 or later - Java 2 Platform, Standard Edition 1.4 (J2SE 1.4)

Support for additional platforms might also be available in later versions of Java.

Key points in migrating to IPv6 and using WebSphere MQ Version 6.0

This section lists some key points to be aware of when you are thinking of installing WebSphere MQ Version 6.0 and using IPv6.

- WebSphere MQ Version 6.0 now recognizes IPv6 hexadecimal addresses (for example fe80:43e4:0204:acff:fe97:2c34:fde0:3485) as well as IPv4 dotted decimal addresses (for example 9.20.9.30).
- For a system running both IPv4 and IPv6 system, the connection name (CONNAME) you specify for a given channel determines the IP protocol for the channel making a connection.

Considerations when implementing IPv6 in a network

This section lists some things that you should consider when you are thinking of installing WebSphere MQ Version 6.0 on an IPv6 network.

- To ensure consistency across the network, you should plan the introduction of IPv6 for the whole network, especially where clusters are involved. For example, although a queue manager is now IPv6 capable, this doesn't imply that the queue managers it can communicate with are also IPv6 capable.
- When setting the domain name server (DNS) or equivalent, consider whether the system on which the target queue manager is running can resolve to an IPv4 address, an IPv6 address or a dual IPv4 and IPv6 address.
- If the system that you are installing WebSphere MQ Version 6.0 on does not support IPv6, WebSphere MQ Version 6.0 will only be able to connect using IPv4.
- For a queue manager running on an IPv6 enabled system to be able to communicate with a queue manager running on an IPv4 enabled system, the IPv4 enabled system must have a hostname that resolves to an IPv4 address only.
- If there are multiple domain name servers in a WebSphere MQ network, each hostname used in a channel definition must resolve to the same address (or addresses), regardless of which DNS is used.
- If the hostname used in a channel definition resolves to a system which hosts a queue manager from WebSphere MQ Version 5.3 or earlier, the hostname must resolve to an IPv4 address only.

Migrating a queue manager to IPv6

This section deals with migrating a queue manager when you are thinking of installing WebSphere MQ Version 6.0 on an IPv6 network.

The IPv6 protocol can only be utilized by WebSphere MQ Version 6.0 or later. In order to make use of the IPv6 protocol, WebSphere MQ must be installed on a system that is IPv6 capable.

The preferred IP version that two systems use for communicating (if both IPv4 and IPv6 are available) is determined by a new queue manager attribute IPADDRV. This parameter only has an effect if the hostname resolves ambiguously to both an IPv4 address and an IPv6 address.

To migrate a queue manager to use the IPv6 protocol:

1. Configure dual IPv4 and IPv6 protocols on the system where the queue manager to be migrated resides.

2. Install WebSphere MQ Version 6.0.
3. Add an entry to the DNS to resolve the hostname of the system that is to be migrated, to both an IPv4 address and an IPv6 address.
4. Set the IPADDRV parameter to IPv6 (or set the LOCLADDR parameter to resolve to an IPv6 address).

   CAUTION:
   Not all IPv6 software can interpret an IPv4 mapped IPv6 address. If the combination of CONNAME and LOCLADDR results in an IPv4 mapped IPv6 address, ensure that the system hosting the target queue manager is capable of handling this.

   Using mapped addresses can require protocol translators in the IP network.

Migration scenarios (non-cluster topology)

It is possible to come up with a number of different interconnection possibilities, and the following sections aim to help you understand how WebSphere MQ will work in each case.

Non-cluster migration scenario 1

Three systems exist that are IPv4 only capable. Each system hosts a queue manager (QM1, QM2, and QM3) and each queue manager connects to the other two. All CONNAMEs in the cluster channel definitions are made using DNS names rather than IP addresses.

Enable QM1 to be able to use channels running over IPv6 as follows

1. Upgrade the host system to have dual IPv4 and IPv6 stacks.

   Important: A listener is required for each IP stack.
2. Install WebSphere MQ Version 6.0.
3. Update the DNS table so that it has two entries for the system running QM1; one entry for its IPv4 address and one for its IPv6 address. This enables a DNS name request to return both IPv4 and IPv6 addresses for this host.
4. Set the queue manager IPADDRV attribute to IPv6.

Note: Even with these changes made to support IPv6 addressing, QM1 will still be able to communicate with queue managers (both existing and new ones) that are only IPv4 capable.

Enable QM2 to be able to use channels running over IPv6 as for QM1 above.

- Communications between QM1 and QM2 will now be over IPv6.
- Communications between QM1 and QM3 will still be over IPv4.
- Communications between QM2 and QM3 will still be over IPv4.

With the queue manager IPADDRV attribute set to IPv6, the preference has been set for the queue manager to connect using the IPv6 protocol. If a channel from QM1 to QM3 has LOCLADDR set to a host name which resolves to an IPv6 address, or both IPv4 and IPv6 addresses (with the IPADDRV attribute set to IPv6, the IPv6 address will be returned as that is the preference), this channel will attempt to use the IPv6 protocol. If the IPv6 protocol installed on the QM1 host system is capable of using a mapped address then QM1 will communicate with QM3 over IPv6. Otherwise, the channel will fail to resolve CONNAME.

While QM3 remains a WebSphere MQ Version 5.3 or earlier queue manager, you will need to check that all CONNAMEs used to start a channel to QM3 do not resolve to an IPv6 address or dual IPv4 and IPv6 addresses where the IPv6 address could be returned. This would cause QM1 to attempt to start the channel over IPv6 which would fail, as it would be unable to resolve the CONNAME.

It is possible to upgrade a system to have dual IPv4 and IPv6 capability and still run a WebSphere MQ Version 5.3 or earlier queue manager on the system. While it is not recommended to run this type of configuration, as long as the addresses that are returned to this level of queue manager are either IPv4 or an IPv4 mapped version of an IPv6 address, this should work.

Non-cluster migration scenario 2

Three systems exist that are IPv4 only capable. Each system hosts a queue manager (QM1, QM2, and QM3) and each queue manager connects to the other two. All CONNAMEs in the cluster channel definitions are made using IP addresses.

Because addresses have been specified instead of DNS names, to allow a queue manager to connect to another using the IPv6 protocol you will need to duplicate the definitions that use IPv4 addresses between them and provide them with IPv6 addresses instead. The original definitions that use IPv4 addresses will continue to work, but if you intend to take advantage of the IPv6 protocol, you will need to connect using the new definitions.

Enable QM1 to be able to use channels running over IPv6 as follows

1. Upgrade the host system to have dual IPv4 and IPv6 stacks.

   Important: A listener is required for each IP stack.
2. Install WebSphere MQ Version 6.0.
3. Duplicate the channel, transmission queue and, where applicable, any process definitions using IPv6 addresses where required.

Note: Even with these changes made to support IPv6 addressing, QM1 will still be able to communicate with existing queue managers that are only IPv4 capable.

Enable QM2 to be able to use channels running over IPv6 as for QM1 above.

1. Upgrade the host system to have dual IPv4 and IPv6 stacks.

   Important: A listener is required for each IP stack.
2. Install WebSphere MQ Version 6.0.
3. Where necessary amend applications to write to the new remote queue (created above for QM1 with the IPv6 addresses).
4. Verify the channels can be started.

The queue managers can now connect as follows:

- QM1 can now connect with QM2 over either IPv4 or IPv6 depending on the channel the application writes its messages to.
- QM1 still connects with QM3 over IPv4 using the original definitions.

Migrating a cluster to IPv6

This section deals with migrating clusters when you are thinking of installing WebSphere MQ Version 6.0 on an IPv6 capable network.

The following gives an overview of approaches that can be taken when migrating a cluster to WebSphere MQ Version 6.0. Due to the variations that can occur within a cluster, the detail is deliberately general and should only be seen as a guide to the likely course of action you will need to take.

Migration scenarios (cluster topology)

Where an IPv6 capable system is to be added to a WebSphere MQ cluster, all full repository systems in that cluster must be IPv6 capable.

The following scenarios are seen as the ones most likely to occur in customer installations. They describe the changes that are likely to be required.

Scenario 1

A WebSphere MQ Version 5.3 or earlier cluster is installed on IPv4 only capable systems and you need to connect an IPv6 only capable system into the cluster. All CONNAMEs in cluster channel definitions are made using DNS names rather than IP addresses.

When adding a new IPv6 only system to the cluster, identify those queue managers that your new system will communicate with. These include:

- The queue managers your new system will send messages to.
- The queue managers your new system will receive messages from.
- The full repository queue managers

The systems that you have identified must be upgraded before introducing the new system.

Recommended migration procedure:

- Upgrade each of the systems hosting a full repository queue manager as shown in ″Migrating a queue manager to IPv6″ non-cluster scenario 1.
- Upgrade the remaining cluster systems which need to be IPv6 capable as shown in ″Migrating a queue manager to IPv6″ non-cluster scenario 1.

With this configuration:

- The new IPv6 only capable system will communicate with the cluster using IPv6 addressing
- All other IPv4 systems that connect into the cluster will continue to communicate using IPv4 addressing
- The systems in the cluster will be able to connect to each other using either IPv4 or IPv6 addressing. The decision as to which address is used depends on whether you have set IPADDRV to specify IPv4 or IPv6 connections.

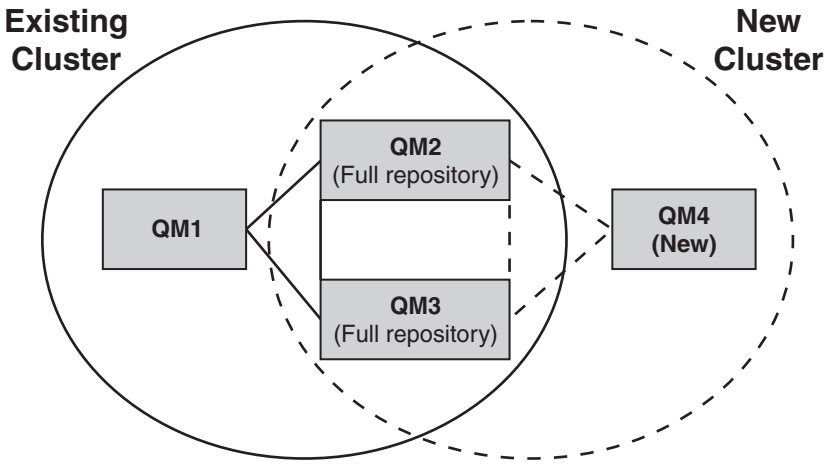
Scenario 2

A WebSphere MQ Version 5.3 or earlier cluster is installed on IPv4 only capable systems and you need to connect an IPv6 only capable system into the cluster. Your network does not support adding both IPv6 and IPv4 addresses using the same hostname or you are using IP addresses rather than DNS names in the cluster channel CONNAMEs.

The problem here is likely to be that all of the systems cannot be switched to IPv6 simultaneously and some at least must remain only IPv4 capable. The systems that your new IPv6 only system communicates with must be IPv4 and IPv6 capable. We do not recommend simply adding a new set of IPv6 channels into the cluster for the IPv6 system to use, as the IPv4 system would also try to use them, resulting in communication errors.

The recommended approach is:

- Define a new cluster which contains the IPv6 only capable system or systems with new IPv6 addresses and channel definitions. The existing cluster remains, and contains the IPv4 only system definitions. The image below gives a pictorial representation of this. QM1, QM2, and QM3 represent the original IPv4 cluster. QM2, QM3, and QM4 represent the new cluster created to allow the IPv6 only capable system (QM4) to connect into your configuration.
- If you are using DNS names, you can give each of the systems separate DNS names for IPv4 and IPv6 (for example system1_IPv4.ibm.com and system1_IPv6.ibm.com).
- Define a new CLUSRCVR channel and any corresponding CLUSSDR channels using the new IPv6 names or IP addresses on each system in the new cluster. In this way the systems with only IPv4 or IPv6 capability do not see channels which they are not able to use and no communications error will result.



Note: There are both IPv4 and IPv6 definitions connecting the full repositories so that definitions for both new and existing cluster definitions are replicated between them. Also be aware that the queue managers QM1 and QM4 cannot communicate directly because they do not share a common network. They could communicate indirectly, for example by using ALIAS queues defined in the queue managers QM2 and QM3. In the configuration shown above you would need to pay attention to the ordering of application messages flowing between QM2 and QM3 because multiple routes exist, if this is relevant you could use BIND_OPEN to fix the route.

Abbreviated migration scenarios

This section gives some abbreviated scenarios for when you are thinking of installing WebSphere MQ Version 6.0.

Abbreviated scenarios: Effects of CONNAME and LOCLADDR settings

The following table provides an overview of what will occur for the different TCP/IP stacks (IPv4 only, IPv6 only and dual IPv4 and IPv6 stacks) and given the settings for CONNAME and LOCLADDR the expected connection result.

Note: Using mapped addresses can require protocol translators in the IP network.

Table 2. Effects of CONNAME and LOCLADDR settings

Stack Type	CONNAME setting	LOCLADDR setting	Connection result
IPv4 only stack	IPv4 address		Channel binds to IPv4 stack
	IPv6 address		Channel fails to resolve CONNAME
	Host name resolves to both IPv4 and IPv6 addresses		Channel binds to IPv4 stack
	IPv4 address	IPv4 address	Channel binds to IPv4 stack
	IPv6 address	IPv4 address	Channel fails to resolve CONNAME
	Host name resolves to both IPv4 and IPv6 addresses	IPv4 address	Channel binds to IPv4 stack
	Any address	IPv6 address	Channel fails to resolve LOCLADDR
	IPv4 address	Host name resolves to both IPv4 and IPv6 addresses	Channel binds to IPv4 stack
	IPv6 address	Host name resolves to both IPv4 and IPv6 addresses	Channel fails to resolve CONNAME
	Host name resolves to both IPv4 and IPv6 addresses	Host name resolves to both IPv4 and IPv6 addresses	Channel binds to IPv4 stack
Dual IPv4 and IPv6 stack	IPv4 address		Channel binds to IPv4 stack
	IPv6 address		Channel binds to IPv6 stack
	Host name resolves to both IPv4 and IPv6 addresses		Channel binds to stack determined by IPADDRV
	IPv4 address	IPv4 address	Channel binds to IPv4 stack
	IPv6 address	IPv4 address	Channel fails to resolve CONNAME
	Host name resolves to both IPv4 and IPv6 addresses	IPv4 address	Channel binds to IPv4 stack
	IPv4 address	IPv6 address	Maps an IPv4 CONNAME to an IPv4 mapped IPv6 address. IPv6 implementations that do not support IPv4 mapped IPv6 addressing fail to resolve CONNAME

Table 2. Effects of CONNAME and LOCLADDR settings (continued)

Stack Type	CONNAME setting	LOCLADDR setting	Connection result
	IPv6 address	IPv6 address	Channel binds to IPv6 stack
	Host name resolves to both IPv4 and IPv6 addresses	IPv6 address	Channel binds to IPv6 stack
	IPv4 address	Host name resolves to both IPv4 and IPv6 addresses	Maps an IPv4 CONNAME to an IPv4 mapped IPv6 address. IPv6 implementations that do not support IPv4 mapped IPv6 addressing fail to resolve CONNAME
	IPv6 address	Host name resolves to both IPv4 and IPv6 addresses	Channel binds to IPv6 stack
	Host name resolves to both IPv4 and IPv6 addresses	Host name resolves to both IPv4 and IPv6 addresses	Channel binds to IPv6 stack
IPv6 only stack	IPv4 address		Maps an IPv4 CONNAME to an IPv4 mapped IPv6 address. IPv6 implementations that do not support IPv4 mapped IPv6 addressing fail to resolve CONNAME
	IPv6 address		Channel binds to IPv6 stack
	Host name resolves to both IPv4 and IPv6 addresses		Channel binds to IPv6 stack
	Any address	IPv4 address	Channel fails to resolve LOCLADDR
	IPv4 address	IPv6 address	Maps an IPv4 CONNAME to an IPv4 mapped IPv6 address. IPv6 implementations that do not support IPv4 mapped IPv6 addressing fail to resolve CONNAME
	IPv6 address	IPv6 address	Channel binds to IPv6 stack
	Host name resolves to both IPv4 and IPv6 addresses	IPv6 address	Channel binds to IPv6 stack
	IPv4 address	Host name resolves to both IPv4 and IPv6 addresses	Maps an IPv4 CONNAME to an IPv4 mapped IPv6 address. IPv6 implementations that do not support IPv4 mapped IPv6 addressing fail to resolve CONNAME
	IPv6 address	Host name resolves to both IPv4 and IPv6 addresses	Channel binds to IPv6 stack
	Host name resolves to both IPv4 and IPv6 addresses	Host name resolves to both IPv4 and IPv6 addresses	Channel binds to IPv6 stack

Abbreviated scenarios: System configurations

Table 4 on page 17 gives a number of abbreviated scenarios based on the configuration of the installed queue managers and the IP configuration they are

running on. The list is not intended to be exhaustive, but to give a number of examples of what to expect based on the configurations shown.

The following table lists the abbreviations used in Table 4. The abbreviations in this table are combined in Table 4 to give the configuration of the systems involved in trying to establish communication. For example:

- v53 + IPv6: Represents a WebSphere MQ Version 5.3 or earlier queue manager on a system with a TCP/IP version 6 stack
- v6 + Dual: Represents a WebSphere MQ Version 6.0 queue manager on system with a dual TCP/IP version 4 and version 6 stack

Table 3. Abbreviations used in system configurations

Abbreviation	Meaning
v53	a WebSphere MQ Version 5.3 or earlier queue manager
v6	WebSphere MQ Version 6.0 queue manager
IPv4	a system using an IPv4 only stack
IPv6	a system using an IPv6 only stack
Dual	a system using both an IPv4 and an IPv6 stack
IPv4DNS	DNS returns an IPv4 address only for hostname of system holding the responding queue manager
IPv6DNS	DNS returns an IPv6 address only for hostname of system holding the responding queue manager
DualDNS	DNS returns an IPv4 and IPv6 address for hostname of system holding the responding queue manager
LOCLADDR4	The LOCLADDR parameter is set to IPv4 addressing
LOCLADDR6	The LOCLADDR parameter is set to IPv6 addressing
IPADDR4	IPADDRV is set to IPv4 addressing
IPADDR6	IPADDRV is set to IPv6 addressing

Table 4. System configurations

Originating queue manager		Responding queue manager			Result
Queue manager and Stack	**LOCLADDR**	**IPADDRV**	**Queue Manager and Stack**	**DNS Return**	
v53 + IPv6	Any	Not applicable			IP Error
v53 + IPv4 or v53 + Dual	Both LOCLADDR4 & LOCLADDR6	Not applicable	v53 + IPv4 or v53 + Dual	IPv4DNS or DualDNS	IPv4 connection can be established
v53 + IPv4 or v53 + Dual	Blank or LOCLADDR4	Not applicable	v53 + IPv4 or v53 + Dual	IPv4DNS or DualDNS	IPv4 connection can be established
v53 + IPv4 or v53 + Dual	Blank or LOCLADDR4	Not applicable	v53 + Dual	IPv6DNS	Unable to resolve CONNAME

Table 4. System configurations (continued)

Originating queue manager		Responding queue manager			Result
Queue manager and Stack	**LOCLADDR**	**IPADDRV**	**Queue Manager and Stack**	**DNS Return**	
v53 + IPv4 or v53 + Dual	Blank or LOCLADDR4	Not applicable	v53 + Dual or v6 + Dual v6 + IPv4	IPv4DNS or DualDNS	IPv4 connection can be established
v53 + IPv4 or v53 + Dual	LOCLADDR6	Not applicable			IP Error
v53 + IPv4 or v53 + Dual	Blank or LOCLADDR4 or both LOCLADDR4 & LOCLADDR6	Not applicable	v6 + IPv6	IPv6DNS	Unable to resolve CONNAME
v6 + IPv4	Blank or LOCLADDR4	Not specified	v53 + IPv4 or v53 + Dual or v6 + IPv4	IPv4DNS or DualDNS	IPv4 connection can be established
v6 + IPv4	LOCADD6	Not specified			Unable to resolve LOCLADDR
v6 + IPv4	Blank or LOCLADDR4	Not specified	v6 + IPv6	IPv6DNS	Unable to resolve CONNAME
v6 + IPv6	Blank or LOCLADDR6	Not specified	v53 + Dual	DualDNS	Attempts to start IPv6 channel and fails as there will be no IPv6 listener available
v6 + IPv6	Blank or LOCLADDR6	Not specified	v53 + IPv4	IPv4DNS	Attempts to start IPv6 channel and fails as there will be no IPv6 listener available
v6 + IPv6 or v6 + Dual	LOCLADDR6	Blank or IPADDR6	v6 + IPv6 or v6 + Dual	IPv6DNS or DualDNS	IPv6 connection can be established
v6 + Dual	LOCLADDR6	IPADDR4	v6 + Dual	IPv4DNS or DualDNS	IPv6 connection can be established where mapped addressing can be used
v6 + Dual	Blank or LOCLADDR4	IPADDR4	v53 + Dual	IPv4DNS or DualDNS	IPv4 connection can be established
v6 + Dual	Both LOCLADDR4 & LOCLADDR6	Blank or IPADDR4	v53 + Dual	IPv4DNS or DualDNS	IPv4 connection can be established
v6 + Dual	LOCLADDR4	IPADDR4			Unable to resolve LOCLADDR
v6 + Dual	LOCLADDR6 or both LOCLADDR4 & LOCLADDR6	Blank or IPADDR6	v6 + IPv6 or v6 + Dual	IPv6DNS or DualDNS	IPv6 connection can be established

Migrating Windows Secure Sockets Layer (SSL) connections

This section deals with migrating Windows Secure Sockets Layer (SSL) connections from WebSphere MQ Version 5.3 to WebSphere MQ Version 6.0.

General Introduction

WebSphere MQ Version 6.0 provides the Global Security Toolkit (GSKit) on Windows platforms for improved SSL (Secure Sockets Layer) support for queue manager and WebSphere MQ client channels. Follow the guidance in this section to determine whether WebSphere MQ Version 5.3 queue managers or clients have been set up to use SSL connections, and to ensure these channels continue to work with WebSphere MQ Version 6.0. The migration process causes a copy of the certificates stored in the WebSphere MQ Certificate Stores used by WebSphere MQ Version 5.3, to be migrated to a GSKit Key database.

Points to consider

- If you are intending to uninstall WebSphere MQ Version 5.3 prior to installing WebSphere MQ Version 6.0, you will need to do the following:
  - Before uninstalling WebSphere MQ Version 5.3 you will need to manually check that the certificate chains are complete. If they are not, use the AMQMCERT utility supplied with WebSphere MQ Version 5.3 to complete the chains.
  - After installing WebSphere MQ Version 6.0 you will need to run the AMQTCERT command from the command line to migrate your certificate stores.

  If you install WebSphere MQ Version 6.0 after uninstalling WebSphere MQ Version 5.3, the certificate chain checker cannot then check the chains and AMQMCERT is no longer available to repair them. This also means that the processes used in the installation to migrate the stores cannot find them and you will need to manually check the chains and manually migrate the stores. See the WebSphere MQ Version 6.0 System Administration Guide for details of these commands.
- The Pre-installation Launchpad is run at the beginning of the installation process. From this the Check WebSphere MQ Certificate Store Wizard can be run. This checks that the certificate chains in the certificate stores are complete, that is, that each certificate in the chain is signed by the entity identified by the next certificate in the chain, terminating with a root CA certificate signed by the CA itself. If you elect not to run the Check WebSphere MQ Certificate Store Wizard, the Post-installation Prepare Wizard will not present any migration panels and your certificate stores can not be scheduled for automatic migration.
- The chain checker application used to verify all the required certificates are there before migrating certificates from the WebSphere MQ for Windows V5.3 store to the GSKit store is available in WebSphere MQ V5.3 Fix Pack 10 (CSD10) or later.
- On client installation, the Check WebSphere MQ Certificate Store Wizard is run from the Install panels directly as there is no launchpad on the client installation to run it from.
- Using the Check WebSphere MQ Certificate Store Wizard and the Post-installation Prepare Wizard for scheduling certificate migration will only be made available if you are migrating from a WebSphere MQ Version 5.3 installation directly to a WebSphere MQ Version 6.0 installation. If you uninstall

WebSphere MQ Version 5.3 and then install WebSphere MQ Version 6.0, the installation process is not aware that the previous version was WebSphere MQ Version 5.3 and will not present the Check WebSphere MQ Certificate Store Wizard or any of the SSL migration panels to you. In this situation, you might consider running the Pre-installation Launchpad and the Check WebSphere MQ Certificate Store Wizard prior to uninstalling WebSphere MQ Version 5.3. This will confirm the completeness of the certificate chains and will allow you to import them using AMQTCERT after installing WebSphere MQ Version 6.0.

- If you are installing WebSphere MQ Version 6.0 silently, there are options which can be passed to the Post-installation Prepare Wizard silently to have it schedule certificate migration for you. If you follow this process, the Check WebSphere MQ Certificate Store Wizard is not run to check the certificate chains. If you are intending to run a silent installation, you should either run the Pre-installation Launchpad and the Check WebSphere MQ Certificate Store Wizard to check the completeness of the certificate chains or check the stores manually using AMQCCERT prior to the installation.

Certificates that are not migrated

A number of certificates are not migrated during this process. These are:

- Certificates that match GSKit's default supplied set. These are not migrated as GSKit provides its own set which are assumed to be the same or more up to date.
- Orphaned certificates that do not have a full valid Certification Authority certificate chain. A certificate can only be imported into a GSkit key database file if a certificate from its certification authority is already present or if it is a root certificate. Certificates can only be added to the GSkit key database starting with the root Certification Authority certificate, proceeding down the chain of intermediate Certification Authority certificates, if any exist, and ending with the personal certificate issued by the lowest member of the Certification Authority chain, again if any exists.
- Certificates that have expired.

Types of certificate migration

There are two types of certificate migration.

- Automatic migration. For a queue manager the actual migration will occur when the queue manager is started for the first time. When the migration has completed, it will not be attempted again even if the migration process failed. The queue manager will attempt to start irrespective of the success or failure of the migration. For a client the actual migration will occur when the client first connects to the queue manager using an SSL channel. If the migration completes successfully then it will not be attempted again. The starting of the client is dependent on the outcome of the migration; if the migration fails then so will the client. Where a certificate store has been successfully validated in the pre-installation phase, the Post-installation Prepare Wizard uses the automatic migration method for each of the queue managers and client stores specified.
- Manual migration. This occurs at the time the new Transfer Certificates (AMQTCERT) control command is run. Manual migration requires you to use AMQTCERT for each queue manager and client. You must specify the location and name stem of the WebSphere MQ Certificate Store and the GSKit key database to be used.

Automatic migration has the advantage that you do not need to specify the location and names for all the WebSphere MQ Certificates Stores and their corresponding GSKit key databases for all the queue managers and the clients as this is derived from the information gathered during the pre-installation processing.

Friendly Name attribute

In the WebSphere MQ Certificate Store file there is one certificate assigned to the queue manager or client. During migration, the copy of this certificate is modified before it is imported into the GSKit database. The modification sets the certificate's Friendly Name attribute to the string `ibmwebspheremq` followed in lower case by the queue manager name or the client logon ID. The previous Friendly Name value, if any, is lost. This Friendly Name value becomes the label of the certificate in the GSKit key database.

Working with migrated certificates

When WebSphere MQ Version 6.0 has been fully installed, and the certificates from the WebSphere MQ Certificate Stores have been migrated to the GSKit database, you can use the IBM Key Management (iKeyman) utility to view and manage your certificates. Full details of the iKeyman utility can be found in the WebSphere MQ Security book.

Determining whether SSL connections have been set up

This section deals with determining whether SSL connections have been set up for WebSphere MQ.

- For channel definitions see the section ″Checking whether channel definitions have been SSL-enabled″.
- For channels set up using client application MQCONNX calls, see the section ″Checking whether client-connection channels set up using MQCONNX calls have been SSL-enabled″.

Checking whether channel definitions have been SSL-enabled

For each queue manager on the computer you are working with, you must check whether any channels have been defined to use SSL. Display the SSLCIPH (CipherSpec) value for each channel defined on the queue manager. To do this you must have the queue manager running and have started the RUNMQSC environment. Enter `DIS CHL(*) CHLTYPE SSLCIPH` to display the channel details. The output should be similar to the following:

```
AMQ8414: Display Channel details.
CHANNEL(SYSTEM.DEF.SENDER) CHLTYPE(SDR) SSLCIPH( )
AMQ8414: Display Channel details.
CHANNEL(SYSTEM.DEF.SERVER) CHLTYPE(SVR) SSLCIPH( )
AMQ8414: Display Channel details.
CHANNEL(TO.QM4) CHLTYPE(CLUSRCVR) SSLCIPH(RC4_MD5_EXPORT)
AMQ8414: Display Channel details.
CHANNEL(TO.QM5) CHLTYPE(CLUSSDR) SSLCIPH(RC4_MD5_EXPORT)
AMQ8414: Display Channel details.
CHANNEL(TO.QM6) CHLTYPE(SVR) SSLCIPH( )
AMQ8414: Display Channel details.
CHANNEL(TO.QM7) CHLTYPE(CLNTCONN) SSLCIPH(NULL_SHA)
AMQ8414: Display Channel details.
CHANNEL(TO.QM7) CHLTYPE(SVRCONN) SSLCIPH(NULL_SHA)
```

Channel definitions that have a value in the brackets after SSLCIPH are SSL channels. If there are any SSL channels the section ″SSL migration steps″ will apply. In the above example, the 'TO.QM4', 'TO.QM5', and both 'TO.QM7' channel definitions have a value for SSLCIPH.

Any client channel definition tables copied from another computer or accessed as a shared file on another computer will also need to be checked for SSLCIPH values. To check these values, either:

- use DIS CHL(*) CHLTYPE SSLCIPH on the queue manager they were defined on
- if your client is running on a system that has a local queue manager, change the MQCHLLIB and MQCHLTAB environment variables which relate to RUNMQSC to specify the directory path and filename of the relevant client channel definition table, then use the DIS CHL(*) CHLTYPE SSLCIPH command on the local queue manager. (Note: You should return the MQCHLLIB and MQCHLTAB settings to their previous values after completing this check.)

Any client-connection channel definitions that have been imported into Active Directory will also need to be checked for non-null SSLCIPH values. Display these definitions using the command `setmqscp -d`.

Checking whether client-connection channels set up using MQCONNX calls are SSL-enabled

For each client application that uses an MQCONNX call, search the MQCD channel definition structure for the optional SSLCipherSpec field, which provides equivalent values to SSLCIPH.

If the value of the SSLCipherSpec field is not null, the MQI channel used by the client application is an SSL channel and the section ″SSL migration steps″ will apply.

SSL migration steps

This section deals with steps for migrating Secure Sockets Layer (SSL) connections to work with WebSphere MQ Version 6.0.

Migrating SSL connections to work with WebSphere MQ version 6.0 consists of several steps:

1. Ensuring WebSphere MQ certificate stores contain complete certificate chains
2. Migrating SSL certificates to Global Security Toolkit key database files
3. Converting Certificate Revocation Lists
4. Ensuring SSLPEER values have correctly ordered OU entries

Step 1: Ensuring WebSphere MQ certificate stores contain complete certificate chains

This section deals with ensuring that complete certificate chains exist in the WebSphere MQ certificate store. This should be completed before installing WebSphere MQ Version 6.0.

WebSphere MQ Version 6.0 uses the Global Security Toolkit (GSKit) to manage SSL certificates. Before installing WebSphere MQ Version 6.0 you must ensure that all WebSphere MQ certificate stores contain complete certificate chains.

In Step 2: Migrating SSL certificates to Global Security Toolkit key database files, it gives guidance on migrating certificates used by WebSphere MQ Version 5.3 queue managers and WebSphere MQ clients into key database files for use with Global Security Toolkit.

As an alternative to Step 1: Ensuring WebSphere MQ certificate stores contain complete certificate chains and Step 2: Migrating SSL certificates to Global Security Toolkit key database files, you can manually configure a key database for each queue manager and WebSphere MQ client and import SSL certificates directly into it without migrating them. See 'Working with the Secure Sockets Layer (SSL) on UNIX and Windows systems' in the WebSphere MQ Version 6.0 Security book for details of how to do this. You will still need to complete Step 3: Ensuring Certificate Revocation Lists are in the correct format and Step 4: Ensuring SSLPEER values have correctly ordered OU entries.

The following sections give the background and necessary steps for "Ensuring WebSphere MQ certificate stores contain complete certificate chains":

- SSL certificates and certificate chains
- Why ensure complete SSL certificate chains exist prior to installation
- How to check WebSphere MQ certificate stores contain complete certificate chains
- Where to locate WebSphere MQ certificate stores
- How to add missing certification authority certificates into WebSphere MQ certificate stores
- What to do if WebSphere MQ version 6.0 has already been installed

SSL certificates and certificate chains

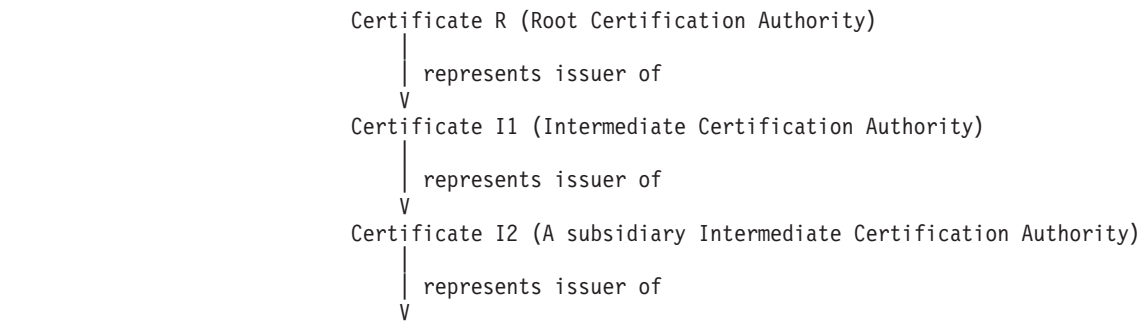
This section explains what SSL certificates are, what a complete certificate chain is and why WebSphere MQ certificate stores need them.

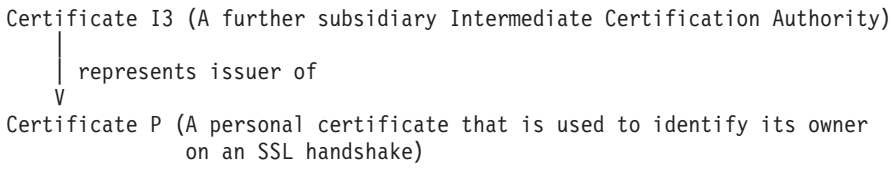
Personal certificates (certificates issued to an individual or a company) can be used by queue managers and WebSphere MQ clients to uniquely identify themselves when they are involved in starting an SSL connection.

Certification authority certificates are used by queue managers and WebSphere MQ clients to verify the authenticity of any personal certificate they receive during an SSL handshake (certification authority certificates are sometimes referred to as Certification Authority (CA) or signer certificates in other WebSphere MQ documentation.)

Each personal certificate has zero or more certificate chains of certification authority certificates that extend back to the root certification authority.

For example:





Certificate chains are used to verify the authenticity of each certificate in that chain, including the personal certificate. Each certificate in the chain is validated using its 'parent' certificate, which in turn is validated using the next certificate up the chain, and so on, from the personal certificate up to the root certification authority certificate.

The Global Security Toolkit (provided by WebSphere MQ Version 6.0) promotes good certificate housekeeping by automatically verifying the authenticity of any personal certificate it manages. For this reason, it requires a complete set (or chain) of certification authority certificates to be stored with each personal certificate.

WebSphere MQ Version 5.3 on Windows allows personal certificates to be held in certificate stores without a complete certificate chain. If you attempt to migrate such certificates to a Global Security Toolkit key database this migration will fail, and your SSL channel connections will no longer work.

Why you must ensure complete SSL certificate chains exist prior to installation

This section details why you must ensure SSL certificate chains are complete prior to the installation of WebSphere MQ Version 6.0.

During the installation of WebSphere MQ Version 6.0, the AMQMCERT command line interface and the Manage SSL Certificates graphical interface that provide access to WebSphere MQ Version 5.3 certificate stores are removed, and you will not be able to add any missing certification authority certificates to these stores after installation.

Where WebSphere MQ certificate stores are located

This section gives details on where you can find the WebSphere MQ certificate stores installed on your systems.

In WebSphere MQ Version 5.3 for Windows, certificates are held in a WebSphere MQ Certificate Store and are stored in a (store) file that has the suffix `.sto`.

The pathname for each of the WebSphere MQ certificate stores can be found by looking in the following attributes and variables:

- for WebSphere MQ queue managers, this is the value of the SSLKEYR attribute
- for WebSphere MQ clients, this is the value of the MQSSLKEYR environment variable
- for applications using MQCONNX calls, this is the value of the KeyRepository field in the MQSCO structure

The store file usually contains the following:

- The certificate assigned to the queue manager or client
- The chain of certification authority certificates
- Any other certificates that were loaded by default
- Any other personal or certification authority certificates.

How to check WebSphere MQ certificate stores contain complete certificate chains

This section details how you can check if the SSL certificate chains that exist in your SSL certificate store are complete.

In WebSphere MQ Version 6.0, a new command is supplied that will check to see if the certificate chains are complete. This command is AMQCCERT (Check Certificate Chains) and can either be run from a command line or batch file, or as part of a wizard. This section will only deal with the use of the wizard. For information on using AMQCCERT from a command line or batch file, see the *WebSphere MQ System Administration Guide*.

The wizard is used to select the queue managers and clients that have certificate stores to migrate. It will run the AMQCCERT command against the certificate stores that have been specified and allows you to check the results of the command. If the wizard has been run previously, any queue managers and clients that were previously selected, will display again.

The wizard also allows you to specify that a queue manager does not use SSL connections and the certificate store (if it exists) will not be checked or migrated.

Identify the queue managers or clients that are using SSL channels. See ″Determining whether SSL connections have been set up″ for guidance on how this is done.

1. Insert the WebSphere MQ Version 6.0 installation CD into the machine where the certificate store to be checked resides.
2. Run the WebSphere MQ Pre-install Launchpad.
3. Select the SSL tab in the WebSphere MQ Pre-install Launchpad.
4. From the WebSphere MQ Pre-install Launchpad, run the Check WebSphere MQ Certificate Store Wizard.
5. Use the Check WebSphere MQ Certificate Store Wizard to check all the certificate chains in your certificate stores. There is help information in the wizard to assist in each of the steps.

When the Check WebSphere MQ Certificate Store Wizard shows which certificate stores have passed and which have failed, the wizard allows you to look at the details of why a certificate store might have failed. The following is an example of the type of information shown when you display the details of why a certificate store might have failed:

```
C:\ssl\client
5724-B41 (C) Copyright IBM Corp. 1994, 2005. ALL RIGHTS RESERVED.
The number of certificates in the Microsoft Certificate Store
                                        'c:\ssl\client' is '13'.

The signer certificate 'GlobalSign Primary Class 1 CA' is missing for
                                          the following certificate.

Microsoft Certificate Store: 'c:\ssl\client'.
Certificate Subject:         'GlobalSign PersonalSign Class 1 CA'.
Certificate Issuer:          'GlobalSign Primary Class 1 CA'.
Certificate Serial Number:   '0400 0000 0000 FA3D EEE9 D9'.
Certificate Valid From:      '22/01/2004' to '28/01/2009'.

The signer certificate 'GlobalSign PersonalSign Class 1 CA' is missing
                                       for the following certificate.

Microsoft Certificate Store: 'c:\ssl\client'.
```

```
Certificate Subject:         'wm.shakespeare@hamlet.com'.
Certificate Issuer:          'GlobalSign PersonalSign Class 1 CA'.
Certificate Serial Number:   '0100 0000 0001 0170 978B 1E'.
Certificate Valid From:      '14/01/2005' to '14/02/2005'.

Certificate chain checking has completed with some failures.
The Check Certificate Chains (amqccert) command has completed.
```

As well as being visible through the wizard, this information, along with other progress information, is also written into a log file. This log file is located in the WebSphere MQ data directory and is named `amqmsccw.txt`.

At this point you have the ability to replace out of date certificates or add missing ones and then go back to the wizard and recheck the stores to ensure they now pass. The wizard will only complete when all the selected certificate stores have been checked and have passed.

Note: If the state `UNTESTED` is displayed for the certificate stores, it indicates that the wizard was unable to launch AMQCCERT to test the given stores. The most likely cause of this is that AMQCCERT or one of its dependent libraries is not available. Check that the WebSphere MQ `bin` directory is available in the path.

Note: AMQMCERT and the Services GUI provided with WebSphere MQ Version 5.3 can be used to work with the certificate stores to correct any errors prior to migrating them.

Adding missing certification authority certificates into WebSphere MQ certificate stores

This section gives the commands necessary to add SSL certificates into WebSphere MQ certificate stores to complete the certificate chains prior to migrating to WebSphere MQ Version 6.0.

Missing certificates can be obtained from the certification authority that issues them. To import a certification authority certificate into a WebSphere MQ certificate store, issue the AMQMCERT command at a command prompt.

- For a queue manager enter:

  `amqmcert -a -s` *`CertificateFilename`* `-m` *`queueManager`*

  To list all certificates in the WebSphere MQ queue manager certificate store, enter:

  `amqmcert -l -m` *`queueManager`*

  Where:

  – CertificateFilename is the fully qualified filename of the file where the certification authority certificate is stored in (certification authority certificates are usually provided in files with extensions .DER, .pb7, or .CER)

  – queueManager is the name of the queue manager that requires the certificate to be added to its certificate store

- For a client (which uses the WebSphere MQ client certificate store identified by the MQSSLKEYR environment variable) enter:

  `amqmcert -a -s` *`CertificateFilename`*

  To list all certificates in the WebSphere MQ client certificate store, enter:

  `amqmcert -l`

  Where:

– CertificateFilename is the fully qualified filename of the file where the certification authority certificate is stored in (certification authority certificates are usually provided in files with extensions .DER, .pb7, or .CER)

- For client applications that use MQCONNX calls enter:

  ```
  amqmcert -a -s CertificateFilename -k KeyRepository
  ```

  To list all certificates in the WebSphere MQ client certificate store, enter:

  ```
  amqmcert -l -k KeyRepository
  ```

  Where:

  – CertificateFilename is the fully qualified filename of the file where the certification authority certificate is stored in (certification authority certificates are usually provided in files with extensions .DER, .pb7, or .CER)

  – KeyRepository is the value (the fully qualified stem name of the repository file) stored in the MQSCO structure

For full details of the AMQMCERT command see the ″WebSphere MQ Version 5.3 System Administration Guide″.

If WebSphere MQ version 6.0 has already been installed

This section deals with the issue of having upgraded to WebSphere MQ Version 6.0 without having complete certificate chains.

If you have installed WebSphere MQ Version 6.0 without completing Step 1: Ensuring WebSphere MQ certificate stores contain complete certificate chains, you will not be able to use AMQMCERT to add any missing certification authority certificates.

You should still use AMQTCERT (Transfer Certificates) command as detailed in Step 2: Migrating SSL certificates to Global Security Toolkit key database files, to attempt certificate migration. Any certificates that have an incomplete certificate chain will fail the migration, and will be copied into a special directory.

If this occurs you will need to:

1. Individually import each certification authority certificate in the failed certificates issuer chain in the correct order
2. Import the failed certificate from the special directory

For more details of these steps, see Reasons and remedies for failed certificate migration.

Step 2: Migrating SSL certificates into Global Security Toolkit database files

This section deals with migrating SSL certificates into Global Security Toolkit key database files and must be performed after installing WebSphere MQ Version 6.0.

The Global Security Toolkit (GSKit) requires SSL certificates to be stored in key database files that it creates and manages. This can be achieved by migrating the SSL certificates held in certificate stores used by WebSphere MQ Version 5.3 queue managers and WebSphere MQ clients into key database files.

This section details how to do this using the Prepare WebSphere MQ Wizard, and the AMQTCERT (Transfer Certificates) command.

Perform Step 1: Ensuring WebSphere MQ certificate stores contain complete certificate chains, prior to installing WebSphere MQ Version 6.0.

The following sections describe the process for migrating your SSL certificates to the GSKit database files:

- Using the Prepare WebSphere MQ Wizard to schedule certificate migration
- Using the AMQTCERT (Transfer Certificates) command

Note: You cannot schedule certificate migration using the Prepare WebSphere MQ Wizard unless you have run the Check WebSphere MQ Certificate Stores Wizard. AMQTCERT can be run without completing Step 1, but you are advised to complete Step 1 prior to moving on to Step 2.

Using the Prepare WebSphere MQ Wizard to schedule certificate migration

This section describes the use of the Prepare WebSphere MQ Wizard which can schedule the migration of your certificate stores and also prompts you to alter other system features for WebSphere MQ Version 6.0 SSL.

The Prepare WebSphere MQ Wizard has two functions in relation to SSL certificate migration:

- It offers to schedule the migration for all certificate stores checked by the Check WebSphere MQ Certificate Stores Wizard during Step 1: Ensuring WebSphere MQ certificate stores contain complete certificate chains
- It also prompts you to check that Step 3: Ensuring Certificate Revocation Lists are in the correct format and Step 4: Ensuring SSLPEER values have correctly ordered OU entries have been completed correctly.

The Prepare WebSphere MQ Wizard is automatically launched at the end of the installation of WebSphere MQ Version 6.0, and can also be launched from the Start Menu.

After starting the Prepare WebSphere MQ Wizard, follow the instructions on each of the panels to schedule the migration or to check that the scheduling of the migration of the certificates has been successful.

Note: The Prepare WebSphere MQ Wizard only offers the certificate stores checked by the Check WebSphere MQ Certificate Stores Wizard. Certificate chains checked manually using AMQCCERT are not presented for selection in the Prepare WebSphere MQ Wizard.

Using the AMQTCERT (Transfer Certificates) command

This section describes the use of the AMQTCERT (Transfer Certificates) command, which can be used to create key database files and transfer existing SSL certificates held in certificate stores used by queue managers and WebSphere MQ clients.

The AMQTCERT (Transfer Certificates) command can be used to schedule migration for the next time the queue manager is started, or the next time the WebSphere MQ client connects to a queue manager using an SSL channel. The migration includes:

- (for queue managers) deriving the names of the source certificate store and target key database file from the queue manager SSLKeyRepository attribute
- creating the target key database file
- attempting to migrate all SSL certificates found in the source certificate store

For details of all the options available for this command, including the options to specify key database filenames, list certificate stores, and cancel scheduled transfers, see the WebSphere MQ Version 6.0 System Administration Guide.

Changing migration state

If you have set a queue manager or client to migrate their stores automatically, it sometimes becomes necessary to migrate the certificate store manually. AMQTCERT can be used to cancel the migration for all or individual queue managers or clients, providing that the migration has not taken place. See the WebSphere MQ Version 6.0 System Administration Guide for details of how to use AMQTCERT to accomplish this.

Automatically transferring SSL certificates used by all queue managers:

This section gives an example of using the AMQTCERT command to automatically transfer the SSL certificates from all WebSphere MQ Version 5.3 queue managers certificate stores (on the current system).

You can schedule the transfer of SSL certificates used by all queue managers on the computer by entering at a command prompt:

```
amqtcert -a -m * -p password -e passwordExpiry
```

Where:

- `password` is the password for all key databases created
- `passwordExpiry` is the number of days until new passwords are required

For details of all the options available for this command, see the WebSphere MQ Version 6.0 System Administration Guide.

Transfer of certificates will occur for each queue manager when it next starts. For each queue manager, the path and stem of where the source WebSphere MQ certificate store and the target GSKit key database file are, is determined by the SSLKeyRepository queue manager attribute.WebSphere MQ client certificate stores will not be transferred by this command.

Automatically transferring SSL certificates used by a specified queue manager:

This section gives an example of using the AMQTCERT command to automatically transfer the SSL certificates from a specified WebSphere MQ Version 5.3 queue manager certificate store.

You can schedule the transfer of SSL certificates used by a specified queue manager on the computer by entering at a command prompt:

```
amqtcert -a -m queueManager -p password -e passwordExpiry
```

Where:

- `queueManager` is the name of the queue manager whose certificate store is to be migrated
- `password` is the password for all key databases created
- `passwordExpiry` is the number of days until new passwords are required

For details of all the options available for this command, see the WebSphere MQ Version 6.0 System Administration Guide.

Transfer of certificates will occur when the queue manager next starts. For the queue manager, the path and stem of where the source WebSphere MQ certificate store and the target GSKit key database file are, is determined by the SSLKeyRepository queue manager attribute.WebSphere MQ client certificate stores will not be transferred by this command.

Automatically transferring SSL certificates used by WebSphere MQ clients:

This section gives an example of using the AMQTCERT command to automatically transfer the SSL certificates from a WebSphere MQ client certificate store.

You can schedule the transfer of SSL certificates used by a WebSphere MQ client on the local system by entering at a command prompt:

```
amqtcert -a -c clientStoreFilename -p password -e passwordExpiry
```

Where:

- `clientStoreFilename` is the fully qualified filename (excluding the .sto suffix) of the WebSphere MQ client certificate store.
- `password` is the password for all key databases created
- `passwordExpiry` is the number of days until new passwords are required

For details of all the options available for this command, see the WebSphere MQ Version 6.0 System Administration Guide.

Transfer of certificates will occur the next time a WebSphere MQ client process which uses a key repository value matching clientStoreFilename connects to a queue manager using an SSL channel.

Manually transferring SSL certificates used by a specified queue manager:

This section gives an example of using the AMQTCERT command to manually transfer the SSL certificates from a WebSphere MQ queue manager certificate store.

You can manually transfer SSL certificates used by a WebSphere MQ queue manager on the computer by entering at a command prompt:

```
amqtcert -m QM1
     -w "C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\SSL\key"
     -g "C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\SSL\key"
     -p MyPassword
```

Where:

- `-m` specifies the name of the queue manager for the certificate store to be migrated
- `-w` specifies the fully qualified filename (excluding the .sto suffix) of the WebSphere MQ Certificate Store
- `-g` specifies the fully qualified filename (excluding the .kdb suffix) of GSKit key database
- `-p` states the password to be set for the GSKit key database

Note:

1. The command should appear on a single line, but has been displayed as above for the purposes of this documentation
2. The GSKit key database must not exist prior to using this command as this command will create it

For details of all the options available for this command, see the WebSphere MQ Version 6.0 System Administration Guide.

Reasons and remedies for failed certificate transfer:

This section gives some reasons and classifications for a failed certificate transfer and how to remedy some of them.

The AMQTCERT command has 2 classifications for why certificates fail to be transferred:

Orphan Certificates

Orphan certificates do not have a complete certificate chain. When the AMQTCERT command detects an orphan certificate, it:

- creates an OrphanCertificates subdirectory in the directory containing the key database file if one doesn't exist already
- exports personal certificates into .pfx files
- exports certification authority certificates into .cer files
- outputs an error message to the `amqerr01.log` for each orphaned certificate, identifying the file, the certificate, and its issuer

To remedy this situation you will need to use the Global Security Toolkit to import the certificates missing from the orphaned certificate chain in strict order from root certification authority to the issuer of the orphaned certificate. Then import the orphan certificate from its file. For more details on how to do this see the WebSphere MQ Version 6.0 Security book.

Failed Certificates

Failed certificates fail to transfer for reasons other than incomplete certificate chains, for example, the certificate having become corrupted. When the AMQTCERT command detects a failed certificate, it:

- creates an ImportFailedCertificates subdirectory in the directory containing the key database file if one doesn't exist already
- exports personal certificates into .pfx files
- exports certification authority certificates into .cer files
- outputs an error message to the `amqerr01.log` for each failed certificate, identifying the file, the certificate, and its issuer

To try to remedy this situation you can get a new copy of the certificate from the certification authority. You will then need to use the Global Security Toolkit to import the certificates in strict order from root certification authority to the personal certificate. For more details on how to do this see *WebSphere MQ Version 6.0 Security*.

Step 3: Converting Certificate Revocation Lists and Authority Revocation Lists

This section describes how to convert the Certificate Revocation Lists and Authority Revocation Lists.

Certificate revocation lists (CRLs) and Authority Revocation Lists (ARLs) are available from Certification Authorities in 2 formats:

- DER-format
- PEM-format

WebSphere MQ Version 5.3 for Windows platforms allows CRLs and ARLs to be in PEM-format. In WebSphere MQ Version 6.0, the Global Security Toolkit requires CRLs and ARLs to be in DER-format and you will need to ensure that any CRLs and ARLs that you have in PEM-format are changed to be in DER-format.

Changing the PEM-format CRLs and ARLs can be performed before or after installing WebSphere MQ Version 6.0.

Changing Certificate Revocation Lists and Authority Revocation Lists into DER-format

Changing PEM-format CRLs and ARLs into DER-format can be achieved in several ways. Two of these are:

- obtain replacement CRLs and ARLs in DER-format from your Certification Authority or authorities
- use a commercial format conversion tool to convert your existing CRLs and ARLs

For each LDAP server that has been configured to hold CRL and ARL information used by WebSphere MQ, you will need to edit the appropriate LDIF file and update the certificateRevocationList; binary field with the DER-format CRL and ARL data. For further information on configuring and updating LDAP servers with CRL and ARL information, see ″Accessing CRLs″ in the WebSphere MQ Security book.

Step 4: Ensuring SSLPEER values have correctly ordered Organizational Unit entries

This section describes how to check that the SSLPEER Organizational Unit (OU) values are in the correct order and how to change them if they are not.

Note: If you have already installed Fix Pack level 8 or higher for WebSphere MQ Version 5.3, you can ignore this step.

SSL-enabled channels that use the optional SSLPEER field to filter Distinguished Names must be checked to ensure multiple Organizational Unit entries (OUs) have been correctly ordered. This section contains information on why this check is needed, and how to do it.

Why you need to check that SSLPEER values have correctly ordered OU entries

This section details why you have to change the order of your SSLPEER values if you are migrating from a WebSphere MQ Version 5.3 Fix Pack 7 or earlier installation.

Every SSL certificate contains a Distinguished Name (DN), used to uniquely identify the person or organization the certificate was issued to. The following attribute types are commonly found in the certificate's Distinguished Name field:

CN Common Name

T Title

O Organization Name

OU Organizational Unit Name

L Locality Name

ST (or SP or S)
State or Province Name

C Country

The certificate Distinguished Name can contain multiple OU attributes, listed in descending hierarchical order. For example, a certificate Distinguished Name could be specified as:

```
CN='QM2', O='IBM', C='GB', L='Hursley', OU='Software Group',
OU='Middleware', OU='MQ'
```

If a WebSphere MQ SSL channel has been configured with an optional SSLPEER value, after an SSL handshake, this value is compared to the Distinguished Name in any certificate received. If these values match then the connection is allowed, otherwise the connection is refused. In WebSphere MQ Version 5.3 Fix Pack 7 or earlier, channel definitions containing SSLPEER values with multiple OUs were entered in ascending hierarchical order on Windows only. All other platforms were in descending hierarchical order. For example on Windows:

```
CN='QM2', O='IBM', C='GB', L='Hursley', OU='MQ', OU='Middleware',
OU='Software Group'
```

These differing approaches to specifying multiple OUs were resolved at Fix Pack 8 - multiple OUs are now always specified in descending hierarchical order in the SSLPEER value on all platforms.

How to display and change SSLPEER values

This section details how you can display the SSLPEER values that you have set and gives an example of how to change them.

Ensure that the queue manager you are changing the SSLPEER values for is running.

1. Start the WebSphere MQ command processor. You can do this by entering `runmqsc queueManager` at a command prompt where queueManager is the name of the queue manager you want to work with.
2. Display the SSLPEER value for each channel defined on the queue manager. You can do this by entering

   ```
   DIS CHL(*) CHLTYPE SSLPEER
   ```

   The output should look similar to this:

   ```
   AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.SENDER) CHLTYPE(SDR) SSLPEER( )
   AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.SERVER) CHLTYPE(SVR) SSLPEER( )
   AMQ8414: Display Channel details.
   CHANNEL(TO.QM7) CHLTYPE(CLNTCONN) SSLPEER(CN='QM7', O='IBM', C='GB',
                   L='Hursley', OU='MQ', OU='Middleware', OU='Software Group')[1]
   AMQ8414: Display Channel details.
   CHANNEL(TO.QM8) CHLTYPE(SVR) SSLPEER(CN='QM2', O='IBM', C='GB',
                   L='Hursley', OU='MQ', OU='Middleware', OU='Software Group')[1]
   ```

3. Where the installation is from WebSphere MQ Version 5.3 Fix Pack 7 or earlier and the SSLPEER values contain multiple organizational unit names (OUs), you will need to reverse the order of these names. You can use the MQSC or the

WebSphere MQ Explorer graphical interface to do this. For example, to change the SSLPEER value for the client-connection channel definition 'TO.QM7' in the above example, at the WebSphere MQ command processor prompt, enter

```
ALTER CHL(TO.QM7) CHLTYPE(CLNTCONN) SSLPEER(CN='QM7', O='IBM', C='GB',
              L='Hursley', OU='Software Group', OU='Middleware', OU='MQ')[1]
```

Note: 1. These lines have been deliberately split to ensure they fit on the page. In the command line interface, all of these should appear on a single line unless the display forces them to wrap on the screen.

SSL Inter-working issue between WebSphere MQ Version 6.0 systems and WebSphere MQ Version 5.3 Windows systems

This section describes an issue in connecting to WebSphere MQ Version 5.3 Windows system from WebSphere MQ Version 6.0 systems using SSL.

In WebSphere MQ Version 6.0 you can renegotiate the secret key on an SSL channel (see WebSphere MQ Security book). If you configure secret key renegotiation on a channel that is connecting to a WebSphere MQ Version 5.3 Windows queue manager, the channel will not connect successfully unless both the following are in place:

- The WebSphere MQ Version 5.3 Windows system has Fix Pack 7 or later installed
- Any of the following operating systems and updates are installed:
  - Windows XP SP2
  - Windows XP SP1 and hotfix Q822541
  - Windows XP and hotfix Q822541
  - Windows 2000 SP4 and hotfix Q822541
  - Windows 2003 is installed

Additional migration information

This section gives additional information that could be of use for customers migrating to WebSphere MQ Version 6.0.

The information in the following topics is provided as guidance to areas that have changed in WebSphere MQ Version 6.0. In some cases you do not need to make any changes to your applications, but it might be beneficial to do so in the future.

Channels implemented as queue manager objects

This section gives information in relation to the move of channels to queue manager objects in WebSphere MQ Version 6.0.

In previous versions of WebSphere MQ, channels on distributed platforms have been stored collectively in a single channel definition file and secured by mqm or QMQMADM permissions. In WebSphere MQ Version 6.0 channels are implemented as queue manager objects in a similar way to objects such as queues and namelists. Two of the main advantages are that channel definitions are now recoverable from media images stored in the queue manager logs and that authority to channel objects can be granted on a per object basis like any other object. To be able to recover a channel from a media image, you must first record an image of the channel. If you issue the rcdmqimg command with the `-t all` parameter, this will happen automatically. If you specify particular types of object, you must add commands to record channel and clntconn objects. There are two new object authorities relevant to channel objects; control (ctrl) and control extended (ctrlx). You must have the appropriate authority in order to start, stop, ping, resolve and reset channels. Any user with ALLADM authority has the required authorities implicitly. Details of changes to media recovery and authority commands to support the new objects can be found in the WebSphere MQ System Administration Guide.

Migration of the channels

Migration to queue manager objects is carried out the first time the queue manager is started after installing WebSphere MQ Version 6.0. A message (AMQ8047) summarizing the total number of channels successfully migrated is displayed and is also written to the queue manager error logs. If channel migration fails, set the AMQ_MIGFORCE_CHANNEL environment variable to force remigration the next time the queue manager is started. Once migration has completed, the channel definition file is renamed from `amqrfcda.dat` to `amqrfcda.old` or from `AMQRFCD4(AMQRFCD4)` to `AMQRFOLD(AMQRFOLD)` on iSeries.

Reverting to a previous version of WebSphere MQ

If you need to uninstall WebSphere MQ Version 6.0 and revert to an earlier version of WebSphere MQ, you will need to rename the channel definition files from `amqrfcda.old` to `amqrfcda.dat` or from `AMQRFOLD(AMQRFOLD)` to `AMQRFCD4(AMQRFCD4)` on iSeries. This will configure your channels to the state that they were in prior to the installation of WebSphere MQ Version 6.0. Any changes made to the channel definitions after the installation of WebSphere MQ Version 6.0 will be lost.

Setting the MQCD Version field

The effect of initializing an MQCD to MQCD_DEFAULT has changed. You might need to change how you set the Version.

In versions of WebSphere MQ before Version 6.0, initializing the MQCD to the macro variables MQCD_DEFAULT or MQCD_CLIENT_CONN_DEFAULT would set the Version field in the MQCD to MQCD_CURRENT_VERSION, which equates to 7 for WebSphere MQ Version 5.3 and 8 for WebSphere MQ Version 6.0.

In WebSphere MQ Version 6.0, MQCD_DEFAULT sets the Version to 6. If you want to take advantage of features of the MQCD introduced in WebSphere MQ Version 5.3 or 6.0, set Version in the MQCD explicitly to 7 or 8, as appropriate, or to MQCD_CURRENT_VERSION. If you intend your applications to be portable between several environments, use a more-recent version MQCD only if all of those environments support that version.

Migrating a queue manager cluster

This section gives information about migrating queue manager clusters to WebSphere MQ Version 6.0.

Migrate the repository queue managers (that is, those queue managers holding a full repository) first, before migrating the other queue managers.

WebSphere MQ Version 6.0 introduces new workload balancing attributes on queues, queue managers, and channels. See Chapter 12 of *WebSphere MQ Queue Manager Clusters* for full details of these attributes. If these parameters are left at their default values, the queue managers will behave as they did before migration.

Use of the new workload balancing parameters in a cluster containing a mixture of Version 5.3 and Version 6.0 queue managers will give unpredictable results.

DCE support in WebSphere MQ

This section gives information in relation to the removal of DCE support in WebSphere MQ Version 6.0.

Support for DCE exits and the DCE name service has been withdrawn from WebSphere MQ and the executables and libraries to allow the use of these will no longer be provided. On HP-UX, the executables and libraries that were built using DCE threads will also no longer be provided.

Consider using SSL (Secure Sockets Layer) or other types of channel exit to secure your channels. For further information see *WebSphere MQ Security*.

External Transaction Manager XA support

This section gives information in relation to changes for external Transaction Manager XA support.

Although there are no migration issues in relation to the support for external Transaction Manager XA, in WebSphere MQ Version 6.0 the WebSphere MQ Server will be brought in line with the enhancements that have been made in earlier

releases to the Extended Transactional Client. For example: a single generic library which supports all transaction managers except CICS®; xa_open string support of QMNAME, TPM and AXLIB.

In WebSphere MQ Version 6.0 a generic XA library is supplied. This is for the server and client, and is in 32-bit form on all UNIX platforms and in 64-bit form in WebSphere MQ for AIX, WebSphere MQ for HP-UX, WebSphere MQ for Sun Solaris, and WebSphere MQ for Linux, Version 6.0 (POWER platform).

The CICS XA libraries will be 32-bit until CICS changes to 64-bit processing.

As the UNIX library is now a shared library and not an archive library you are recommended to rebuild your applications. Not to do so means that you will remain at a level of code from when you last built your applications and will not pick up the changes to the library as it is enhanced through changes to functionality and fixes. To rebuild your applications using this library would be a one time exercise as the applications would then use the library files that are shipped with the product in this and any future releases.

Java archive (JAR) file com.ibm.mqbind.jar

This section gives information in relation to the com.ibm.mqbind.jar file.

The Java archive (JAR) file com.ibm.mqbind.jar has been deprecated and is no longer supplied with WebSphere MQ. If your Java applications have been relying on the contents of this file, you will need to change them to use the file com.ibm.mq.jar when you migrate to WebSphere MQ, Version 6.0.

Queue manager attributes SCHINIT and SCMDSERV

The new queue manager attributes SCHINIT and SCMDSERV control whether the channel initiator and command server should start automatically when the queue manager starts. These will be automatically migrated but you can set them using the ALTER QMGR command.

Starting and stopping services and listeners

You can now start and stop listeners and services using the START and STOP MQSC commands. However, the old commands strmqcsv, endmqcsv, runmqchi, runmqlsr, endmqlsr, and runmqtrm are still supported.

UNIX directory permissions

On UNIX systems, queue manager directory permissions are changed to be stricter in WebSphere MQ Version 6.0 than in Version 5.3. The change will be made automatically when the queue manager is first started after migration. Any user applications which require access to the queue manager directories (e.g. error logs, FDCs) should run under the authority of a user ID in the **mqm** group.

High availability clustering

This section gives information on considerations for migrating high availability (HA) clusters.

To update an HA cluster, plan the order of migration so that a system running WebSphere MQ Version 5.3 code can never access the files for a queue manager

that is already running with Version 6.0 code. Implementing this rolling migration strategy to minimize total downtime will probably require you to disable failover between some systems in the cluster during the upgrade process.

Because channels are objects in WebSphere MQ Version 6.0, the channels and clntconn directories must be replicated between nodes for channel definitions. (The client channel table file is unchanged.)

On Windows HA systems, the certificate stores must be migrated to GSKit on all nodes which host a WebSphere MQ Version 6.0 queue manager.

WebSphere MQ transport for SOAP

This section provides information on WebSphere MQ transport for SOAP.

Prior to WebSphere MQ Version 6.0, support for SOAP (the Simple Object Access Protocol) was provided in SupportPac MA0R. This function is now mostly incorporated into the product, with extensions for asynchronous SOAP messaging in SupportPac MA0V. Full details are given in *WebSphere MQ Transport for SOAP*.

An important change is that the URL for a WebSphere MQ SOAP request now starts with the prefix **jms:** rather than the **wmq:** used previously. Ensure that your applications generate and recognize the correct prefix.

Considerations for migrating WebSphere MQ for AIX

This section gives information on considerations for migrating WebSphere MQ for AIX

Migrating from UDP

The UDP protocol is no longer supported for channels on AIX. Use TCP instead. To migrate channels using UDP, stop the channels at both ends and issue the command `ALTER CHANNEL(CHANNEL.NAME) CHLTYPE(type) TRPTYPE(TCP)`. Change your channel definitions before installing WebSphere MQ for AIX, Version 6.0, as otherwise the UDP channels will not be migrated and will have to be defined again.

Considerations for migrating WebSphere MQ for Linux

This section gives information on considerations for migrating WebSphere MQ for Linux

Migrating from earlier versions of WebSphere MQ for Linux

If you are migrating from a previous version of WebSphere MQ for Linux, you must uninstall your current version before installing WebSphere MQ Version 6.0. See WebSphere MQ for Linux Version 6.0 Quick Beginnings for instructions.

The use of RPM upgrade tools to migrate directly from one version of WebSphere MQ to another is not supported.

If you have already tried to upgrade WebSphere MQ using rpm -U or rpm -F, you might have deleted your old WebSphere MQ package entries from the RPM database without removing the product from your system. You might also have partially installed WebSphere MQ Version 6.0.

To continue upgrading to WebSphere MQ Version 6.0:

1. Find out which WebSphere MQ packages still have entries in your RPM database using: rpm -qa | grep MQSeries®
2. Remove all remaining WebSphere MQ packages of any level from your system using: rpm -e <package name>
3. Remove the /opt/mqm directory by typing: rm -rf /opt/mqm
4. Install WebSphere MQ Version 6.0 using the instructions provided in *WebSphere MQ for Linux Version 6.0 Quick Beginnings*

WebSphere MQ Explorer for Version 6.0 - error connecting to a migrated queue manager

If you cannot connect to a migrated queue manager and see an error like "SYSTEM.MQEXPLORER.REPLY.MODEL not defined", run:

```
strmqm -c
```

on that queue manager.

This command refreshes the default system objects, including creating the queue required by WebSphere MQ Explorer.

Using environment variables

Attention: Misuse of certain environment variables can cause irreparable damage to the RPM database.

You must have the following environment variables set when you attempt to uninstall WebSphere MQ Version 5.3 for Linux for Intel®:

- export LD_ASSUME_KERNEL=2.4.19
- export RPM_FORCE_NPTL=1

If these variables are not set to the specified values when you attempt to uninstall WebSphere MQ V 5.3, it can cause unrecoverable damage to the RPM database. This is due to a known Linux issue, see https://rhn.redhat.com/errata/RHEA-2004-010.html for more information.

WebSphere MQ for Linux (x86 platform), Version 6.0 is not affected by this issue. When you have completed your migration to WebSphere MQ Version 6.0, unset these variables to take advantage of the performance benefits of the Native Linux Posix Thread Library (NPTL).

Considerations for migrating Websphere MQ for Windows

This section gives information on considerations for migrating WebSphere MQ for Windows systems

PL/I support in WebSphere MQ for Windows

This section gives information in relation to PL/I support in WebSphere MQ Version 6.0.

Support for PL/I has been withdrawn from WebSphere MQ for Windows. It continues to be supported for WebSphere MQ for z/OS.

WebSphere MQ service objects

This section gives information about service objects in WebSphere MQ for Windows.

In WebSphere MQ for Windows, services are now managed by service objects. The listener, command server, trigger monitor, and channel initiator services defined using the MMC plugin in earlier versions of WebSphere MQ will be migrated to queue manager objects as follows:

- The startup property of the command server (automatic or manual) is migrated to the SCMDSERV attribute of the queue manager.
- The startup property of the channel initiator (automatic or manual) is migrated to the SCHINIT attribute of the queue manager.
- For each listener defined in the WebSphere MQ Explorer, a queue manager LISTENER object is created.
- For each trigger monitor defined in the WebSphere MQ Explorer, a queue manager SERVICE object is created.

WebSphere MQ Explorer for Version 6.0 - error connecting to a migrated queue manager

If you cannot connect to a migrated queue manager and see an error like "SYSTEM.MQEXPLORER.REPLY.MODEL not defined", run:

```
strmqm -c
```

on that queue manager.

This command refreshes the default system objects, including creating the queue required by WebSphere MQ Explorer.

Considerations for migrating WebSphere MQ for z/OS

This section gives information on considerations for migrating WebSphere MQ for z/OS

Information relating to the migration of WebSphere MQ for z/OS to WebSphere MQ Version 6.0 can be found in the WebSphere MQ for z/OS System Setup Guide, Chapter 3, "Migrating from a previous version".

This covers information relating to:

- Migrating from a number of earlier versions of WebSphere MQ for z/OS
- Reverting to earlier versions of WebSphere MQ for z/OS
- Changing to full function WebSphere MQ for z/OS where the reduced function form of WebSphere MQ supplied with WebSphere Application Server has been installed
- Coexistence with earlier versions of WebSphere MQ for z/OS

Migrating from AMI

AMI is not supplied as part of WebSphere MQ Version 6.0. If you have previously used AMI in WebSphere MQ Version 5.3.1, you can continue to use it by including the Version 5.3.1 SCSQLOAD file in your STEPLIB concatenation, as shown below:

```
//STEPLIB DD DISP=SHR,DSN=PP.MQM.V600.SCSQANLE V6 Messages
//        DD DISP=SHR,DSN=PP.MQM.V600.SCSQAUTH V6 API MODULES
//        DD DISP=SHR,DSN=PP.MQM.V531.SCSQLOAD AMI CODE
```

If you have removed WebSphere MQ Version 5.3.1 but need AMI functionality, you can install the AMI SupportPac MA0F. This is available from the IBM Web site.

Appendix. Notices

This information was developed for products and services offered in the United States. 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, 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.

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.

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. 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 IBM's application programming interfaces.

Trademarks

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

AIX	CICS	IBM
iSeries	MQSeries	POWER
SupportPac	WebSphere	z/OS

Intel is a registered trademark of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds 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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Sending your comments to IBM

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM.

Feel free to comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this book.

Please limit your comments to the information in this book and the way in which the information is presented.

To make comments about the functions of IBM products or systems, talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

You can send your comments to IBM in any of the following ways:

- By mail, to this address:

  User Technologies Department (MP095)
  IBM United Kingdom Laboratories
  Hursley Park
  WINCHESTER,
  Hampshire
  SO21 2JN
  United Kingdom
- By fax:
  - From outside the U.K., after your international access code use 44–1962–816151
  - From within the U.K., use 01962–816151
- Electronically, use the appropriate network ID:
  - IBM Mail Exchange: GBIBM2Q9 at IBMMAIL
  - IBMLink™: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

Whichever method you use, ensure that you include:

- The publication title and order number
- The topic to which your comment applies
- Your name and address/telephone number/fax number/network ID.

SC34-6604-01

Spine information:

WebSphere MQ

Migration Information

Version 6.0