Abstract

This guide describes how to configure AMQ Broker.
# Table of Contents

## CHAPTER 1. OVERVIEW

1.1. AMQ BROKER CONFIGURATION FILES AND LOCATIONS ................................. 8

1.2. UNDERSTANDING THE DEFAULT BROKER CONFIGURATION

   Default message persistence settings ............................................... 8

   Default acceptor settings ............................................................. 10

   Default security settings ............................................................. 11

   Default message address settings .................................................. 11

1.3. RELOADING CONFIGURATION UPDATES ................................................... 12

1.4. MODULARIZING THE BROKER CONFIGURATION FILE ............................... 13

1.5. DOCUMENT CONVENTIONS

   The sudo command ........................................................................... 14

   About the use of file paths in this document ..................................... 14

## CHAPTER 2. NETWORK CONNECTIONS: ACCEPTORS AND CONNECTORS

2.1. ABOUT ACCEPTORS

    Configuring an Acceptor .................................................................. 15

2.2. ABOUT CONNECTORS

    Configuring a Connector .................................................................. 16

2.3. CONFIGURING A TCP CONNECTION ....................................................... 16

2.4. CONFIGURING AN HTTP CONNECTION ................................................ 17

2.5. CONFIGURING AN SSL/TLS CONNECTION ............................................ 18

2.6. CONFIGURING AN IN-VM CONNECTION .............................................. 18

2.7. CONFIGURING A CONNECTION FROM THE CLIENT SIDE .................... 18

## CHAPTER 3. NETWORK CONNECTIONS: PROTOCOLS

3.1. CONFIGURING A NETWORK CONNECTION TO USE A PROTOCOL ................. 20

3.2. USING AMQP WITH A NETWORK CONNECTION ................................. 21

   3.2.1. Using an AMQP Link as a Topic ............................................... 22

   3.2.2. Configuring AMQP Security ..................................................... 22

3.3. USING MQTT WITH A NETWORK CONNECTION .................................... 22

3.4. USING OPENWIRE WITH A NETWORK CONNECTION .......................... 23

3.5. USING STOMP WITH A NETWORK CONNECTION .................................. 24

   3.5.1. Knowing the Limitations When Using STOMP .......................... 24

   3.5.2. Providing IDs for STOMP Messages ......................................... 24

   3.5.3. Setting a Connection’s Time to Live (TTL) ............................... 25

      Overriding the Broker’s Default Time to Live (TTL) ..................... 25

   3.5.4. Sending and Consuming STOMP Messages from JMS .............. 26

   3.5.5. Mapping STOMP Destinations to AMQ Broker Addresses and Queues 26

      Mapping STOMP Destinations to JMS Destinations ....................... 27

## CHAPTER 4. ADDRESSES, QUEUES, AND TOPICS

4.1. ADDRESS AND QUEUE NAMING REQUIREMENTS .................................. 28

4.2. CONFIGURING POINT-TO-POINT MESSAGING ................................. 29

4.3. CONFIGURING PUBLISH-SUBSCRIBE MESSAGING ............................. 29

4.4. CONFIGURING A POINT-TO-POINT USING TWO QUEUES ................. 30

4.5. USING POINT-TO-POINT AND PUBLISH-SUBSCRIBE TOGETHER .......... 31

4.6. CONFIGURING SUBSCRIPTION QUEUES ................................. 32

   Configuring a Durable Subscription Queue ..................................... 33

   Configuring a Non-Shared Durable Subscription ............................ 33

4.7. USING A FULLY QUALIFIED QUEUE NAME ........................................ 34

4.8. CONFIGURING SHARDED QUEUES .................................................... 35

4.9. CONFIGURING LAST VALUE QUEUES ................................................ 35
Enabling a Filter to Use Hyphens

CHAPTER 16. SETTING UP A BROKER CLUSTER ............................................... 123
16.1. UNDERSTANDING BROKER CLUSTERS ........................................... 123
  16.1.1. How broker clusters balance message load .............................. 123
  16.1.2. How broker clusters improve reliability ................................. 124
  16.1.3. Common broker cluster topologies
    Symmetric clusters .......................... 125
    Chain clusters ............................. 125
  16.1.4. Broker discovery methods
    Dynamic discovery .......................... 126
    Static discovery ............................ 126
  16.1.5. Cluster sizing considerations
    Messaging throughput ........................ 126
    Topology .................................... 127
    High availability ........................... 127
16.2. CREATING A BROKER CLUSTER .................................................... 127
  16.2.1. Creating a broker cluster with static discovery ...................... 127
  16.2.2. Creating a broker cluster with UDP-based dynamic discovery .... 129
  16.2.3. Creating a broker cluster with JGroups-based dynamic discovery 132
16.3. IMPLEMENTING HIGH AVAILABILITY ............................................ 135
  16.3.1. Understanding high availability.......................................... 136
    16.3.1.1. How live-backup groups provide high availability ............ 136
    16.3.1.2. High availability policies ........................................ 136
    16.3.1.3. Replication policy limitations ................................... 138
  16.3.2. Configuring high availability ............................................ 138
    16.3.2.1. Configuring shared store high availability ..................... 138
    16.3.2.2. Configuring replication high availability ...................... 141
    16.3.2.3. Configuring limited high availability with live-only .......... 143
    16.3.2.4. Configuring high availability with colocated backups ...... 145
  16.3.3. Configuring clients to fail over ....................................... 147
16.4. ENABLING MESSAGE REDISTRIBUTION ....................................... 148
16.5. CONFIGURING CLUSTERED MESSAGE GROUPING ................................. 149
16.6. CONNECTING CLIENTS TO A BROKER CLUSTER ................................ 151

CHAPTER 17. CONFIGURING A MULTI-SITE, FAULT-TOUCHER MESSAGING SYSTEM .......... 152
17.1. HOW RED HAT CEPH STORAGE CLUSTERS WORK ............................. 152
17.2. INSTALLING RED HAT CEPH STORAGE ......................................... 153
17.3. CONFIGURING A RED HAT CEPH STORAGE CLUSTER ......................... 154
17.4. MOUNTING THE CEPH FILE SYSTEM ON YOUR BROKER SERVERS ......... 159
17.5. CONFIGURING BROKERS IN A MULTI-SITE, FAULT-TOLERANT MESSAGING SYSTEM 160
  17.5.1. Adding backup brokers ............................................... 160
  17.5.2. Configuring brokers as Ceph clients ................................ 161
  17.5.3. Configuring shared store high availability .......................... 161
17.6. CONFIGURING CLIENTS IN A MULTI-SITE, FAULT-TOLERANT MESSAGING SYSTEM 162
  17.6.1. Configuring internal clients ....................................... 163
  17.6.2. Configuring external clients ..................................... 164
17.7. VERIFYING STORAGE CLUSTER HEALTH DURING A DATA CENTER OUTAGE 164
17.8. MAINTAINING MESSAGING CONTINUITY DURING A DATA CENTER OUTAGE 165
17.9. RESTARTING A PREVIOUSLY FAILED DATA CENTER .......................... 167
  17.9.1. Restarting storage cluster servers ................................ 167
  17.9.2. Restarting broker servers ......................................... 167
  17.9.3. Reestablishing client connections ................................ 168
CHAPTER 1. OVERVIEW

AMQ Broker configuration files define important settings for a broker instance. By editing a broker’s configuration files, you can control how the broker operates in your environment.

1.1. AMQ BROKER CONFIGURATION FILES AND LOCATIONS

All of a broker’s configuration files are stored in `<broker-instance-dir>/etc`. You can configure a broker by editing the settings in these configuration files.

Each broker instance uses the following configuration files:

- broker.xml
  The main configuration file. You use this file to configure most aspects of the broker, such as network connections, security settings, message addresses, and so on.

- bootstrap.xml
  The file that AMQ Broker uses to start a broker instance. You use it to change the location of broker.xml, configure the web server, and set some security settings.

- logging.properties
  You use this file to set logging properties for the broker instance.

- artemis.profile
  You use this file to set environment variables used while the broker instance is running.

- login.config, artemis-users.properties, artemis-roles.properties
  Security-related files. You use these files to set up authentication for user access to the broker instance.

1.2. UNDERSTANDING THE DEFAULT BROKER CONFIGURATION

You configure most of a broker’s functionality by editing the broker.xml configuration file. This file contains default settings, which are sufficient to start and operate a broker. However, you will likely need to change some of the default settings and add new settings to configure the broker for your environment.

By default, broker.xml contains default settings for the following functionality:

- Message persistence
- Acceptors
- Security
- Message addresses

Default message persistence settings
By default, AMQ Broker persistence uses an append-only file journal that consists of a set of files on disk. The journal saves messages, transactions, and other information.
<persistence-enabled>true</persistence-enabled>

<!-- this could be ASYNCIO, MAPPED, NIO
ASYNCIO: Linux Libaio
MAPPED: mmap files
NIO: Plain Java Files
-->

<journal-type>ASYNCIO</journal-type>

<paging-directory>data/paging</paging-directory>

<bindings-directory>data/bindings</bindings-directory>

<journal-directory>data/journal</journal-directory>

<large-messages-directory>data/large-messages</large-messages-directory>

<journal-datasync>true</journal-datasync>

<journal-min-files>2</journal-min-files>

<journal-pool-files>10</journal-pool-files>

<journal-file-size>10M</journal-file-size>

<!-- This value was determined through a calculation. Your system could perform 8.62 writes per millisecond on the current journal configuration. That translates as a sync write every 115999 nanoseconds.

Note: If you specify 0 the system will perform writes directly to the disk. We recommend this to be 0 if you are using journalType=MAPPED and journal-datasync=false.
-->

<journal-buffer-timeout>115999</journal-buffer-timeout>

<!-- When using ASYNCIO, this will determine the writing queue depth for libaio.
-->

<journal-max-io>4096</journal-max-io>

<!-- how often we are looking for how many bytes are being used on the disk in ms -->
<disk-scan-period>5000</disk-scan-period>

<!-- once the disk hits this limit the system will block, or close the connection in certain protocols that won't support flow control.
-->

<max-disk-usage>90</max-disk-usage>

<!-- should the broker detect dead locks and other issues -->
<critical-analyzer>true</critical-analyzer>

<critical-analyzer-timeout>120000</critical-analyzer-timeout>

<critical-analyzer-check-period>60000</critical-analyzer-check-period>
Default acceptor settings
Brokers listen for incoming client connections by using an acceptor configuration element to define the port and protocols a client can use to make connections. By default, AMQ Broker includes configuration for an acceptor for each supported messaging protocol.

<configuration ...>
    <core ...>
        ...
        ...
        <acceptors>
            <!-- Acceptor for every supported protocol -->
            <acceptor name="artemis">tcp://0.0.0.0:61616?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=CORE,AMQP,STOMP,HORNETQ,MQTT,OPENWIRE;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

            <!-- AMQP Acceptor. Listens on default AMQP port for AMQP traffic.-->
            <acceptor name="amqp">tcp://0.0.0.0:5672?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=AMQP;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

            <!-- STOMP Acceptor. -->
            <acceptor name="stomp">tcp://0.0.0.0:61613?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=STOMP;useEpoll=true</acceptor>

            <!-- HornetQ Compatibility Acceptor. Enables HornetQ Core and STOMP for legacy HornetQ clients. -->
            <acceptor name="hornetq">tcp://0.0.0.0:5445?
anycastPrefix=jms.queue.;multicastPrefix=jms.topic.;protocols=HORNETQ,STOMP;useEpoll=true</acceptor>

            <!-- MQTT Acceptor -->
            <acceptor name="mqtt">tcp://0.0.0.0:1883?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=MQTT;useEpoll=true</acceptor>
        </acceptors>
    </core>
</configuration>
Default security settings
AMQ Broker contains a flexible role-based security model for applying security to queues, based on their addresses. The default configuration uses wildcards to apply the amq role to all addresses (represented by the number sign, #).

```xml
<configuration ...>
  <core ...>
    ...
    <security-settings>
      <security-setting match="#">
        <permission type="createNonDurableQueue" roles="amq"/>
        <permission type="deleteNonDurableQueue" roles="amq"/>
        <permission type="createDurableQueue" roles="amq"/>
        <permission type="deleteDurableQueue" roles="amq"/>
        <permission type="createAddress" roles="amq"/>
        <permission type="deleteAddress" roles="amq"/>
        <permission type="consume" roles="amq"/>
        <permission type="browse" roles="amq"/>
        <permission type="send" roles="amq"/>
        <!--[-- we need this otherwise ./artemis data imp wouldn't work -->]
        <permission type="manage" roles="amq"/>
      </security-setting>
    </security-settings>
    ...
  </core>
</configuration>
```

Default message address settings
AMQ Broker includes a default address that establishes a default set of configuration settings to be applied to any created queue or topic.

Additionally, the default configuration defines two queues: DLQ (Dead Letter Queue) handles messages that arrive with no known destination, and Expiry Queue holds messages that have lived past their expiration and therefore should not be routed to their original destination.

```xml
<configuration ...>
  <core ...>
    ...
    <address-settings>
      <![--default for catch all-->]
      <address-setting match="#">
        <dead-letter-address>DLQ</dead-letter-address>
        <expiry-address>ExpiryQueue</expiry-address>
        <redelivery-delay>0</redelivery-delay>
        <!--[-- with -1 only the global-max-size is in use for limiting -->]
    </address-settings>
  </core>
</configuration>
```
1.3. RELOADING CONFIGURATION UPDATES

By default, a broker checks for changes in the configuration files every 5000 milliseconds. If any are found, the configuration is reloaded to activate the changes. You can change the interval at which the broker checks for configuration changes.

If the configuration is changed, the broker reloads the following modules:

- **Address settings and queues**
  When the configuration file is reloaded, the address settings determine how to handle addresses and queues that have been deleted from the configuration file. You can set this with the `config-delete-addresses` and `config-delete-queues` properties. For more information, see Appendix B, Address Setting Configuration Elements.

- **Security settings**
  SSL/TLS keystores and truststores on an existing acceptor can be reloaded to establish new certificates without any impact to existing clients. Connected clients, even those with older or differing certificates, can continue to send and receive messages.

**Procedure**

1. Open the `<broker-instance-dir>/etc/broker.xml` configuration file.

2. Within the `<core>` element, add the `<configuration-file-refresh-period>` element and set the refresh period (in milliseconds).
   This example sets the configuration refresh period to be 60000 milliseconds:

   ```xml
   <configuration>
   ...
   </configuration>
1.4. MODULARIZING THE BROKER CONFIGURATION FILE

If you have multiple brokers that share common configuration settings, you can define the common configuration in separate files, and then include these files in each broker’s `broker.xml` configuration file.

The most common configuration settings that you might share between brokers include:

- Addresses
- Address settings
- Security settings

Procedure

1. Create a separate XML file for each `broker.xml` section that you want to share. Each XML file can only include a single section from `broker.xml` (for example, either addresses or address settings, but not both). The top-level element must also define the element namespace (`xmlns="urn:activemq:core"`).

   This example shows a security settings configuration defined in `my-security-settings.xml`:

   ```xml
   <security-settings xmlns="urn:activemq:core">
     <security-setting match="a1">
       <permission type="createNonDurableQueue" roles="a1.1"/>
     </security-setting>
     <security-setting match="a2">
       <permission type="deleteNonDurableQueue" roles="a2.1"/>
     </security-setting>
   </security-settings>
   ```

2. Open the `<broker-instance-dir>/etc/broker.xml` configuration file for each broker that should use the common configuration settings.

3. For each `broker.xml` file that you opened, do the following:

   a. In the `<configuration>` element at the beginning of `broker.xml`, verify that the following line appears:

      ```xml
      xmlns:xi="http://www.w3.org/2001/XInclude"
      ```

   b. Add an XML inclusion for each XML file that contains shared configuration settings. This example includes the `my-security-settings.xml` file.

      ```xml
      <core>
        ...
        <configuration-file-refresh-period>60000</configuration-file-refresh-period>
        ...
      </core>
      </configuration>
      ```
If desired, validate `broker.xml` to verify that the XML is valid against the schema. You can use any XML validator program. This example uses `xmllint` to validate `broker.xml` against the `artemis-server.xsl` schema.

```
$ xmllint --noout --xinclude --schema /opt/redhat/amq-broker/amq-broker-7.2.0/schema/artemis-server.xsd /var/opt/amq-broker/mybroker/etc/broker.xml /var/opt/amq-broker/mybroker/etc/broker.xml validates
```

Additional resources

- For more information about XML Inclusions (XIncludes), see [https://www.w3.org/TR/xinclude/](https://www.w3.org/TR/xinclude/).

### 1.5. DOCUMENT CONVENTIONS

This document uses the following conventions for the `sudo` command and file paths.

**The `sudo` command**
In this document, `sudo` is used for any command that requires root privileges. You should always exercise caution when using `sudo`, as any changes can affect the entire system.

For more information about using `sudo`, see The `sudo` Command.

**About the use of file paths in this document**
In this document, all file paths are valid for Linux, UNIX, and similar operating systems (for example, `/home/...`). If you are using Microsoft Windows, you should use the equivalent Microsoft Windows paths (for example, `C:\Users\...`).
CHAPTER 2. NETWORK CONNECTIONS: ACCEPTORS AND CONNECTORS

There are two types of connections used in AMQ Broker: network and In-VM. Network connections are used when the two parties are located in different virtual machines, whether on the same server or physically remote. An In-VM connection is used when the client, whether an application or a server, resides within the same virtual machine as the broker.

Network connections rely on Netty. Netty is a high-performance, low-level network library that allows network connections to be configured in several different ways: using Java IO or NIO, TCP sockets, SSL/TLS, even tunneling over HTTP or HTTPS. Netty also allows for a single port to be used for all messaging protocols. A broker will automatically detect which protocol is being used and direct the incoming message to the appropriate handler for further processing.

The URI within a network connection’s configuration determines its type. For example, using `vm` in the URI will create an In-VM connection. In the example below, note that the URI of the acceptor starts with `vm`.

<acceptor name="in-vm-example">vm://0</acceptor>

Using `tcp` in the URI, alternatively, will create a network connection.

<acceptor name="network-example">tcp://localhost:61617</acceptor>

This chapter will first discuss the two configuration elements specific to network connections, Acceptors and Connectors. Next, configuration steps for TCP, HTTP, and SSL/TLS network connections, as well as In-VM connections, are explained.

2.1. ABOUT ACCEPTORS

One of the most important concepts when discussing network connections in AMQ Broker is the acceptor. Acceptors define the way connections are made to the broker. Below is a typical configuration for an acceptor that might be in found inside the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`.

<acceptors>
    <acceptor name="example-acceptor">tcp://localhost:61617</acceptor>
</acceptors>

Note that each acceptor is grouped inside an acceptors element. There is no upper limit to the number of acceptors you can list per server.

Configuring an Acceptor

You configure an acceptor by appending key-value pairs to the query string of the URI defined for the acceptor. Use a semicolon (`;`) to separate multiple key-value pairs, as shown in the following example. It configures an acceptor for SSL/TLS by adding multiple key-value pairs at the end of the URI, starting with `sslEnabled=true`.

<acceptor name="example-acceptor">tcp://localhost:61617?sslEnabled=true;key-store-path=/path</acceptor>

For details on connector configuration parameters, see Acceptor and Connector Configuration Parameters.
2.2. ABOUT CONNECTORS

Whereas acceptors define how a server accepts connections, a connector is used by clients to define how they can connect to a server.

Below is a typical connector as defined in the `BROKER_INSTANCE_DIR/etc/broker.xml` configuration file:

```xml
< connectors >
  < connector name="example-connector">tcp://localhost:61617</ connector >
</ connectors >
```

Note that connectors are defined inside a connectors element. There is no upper limit to the number of connectors per server.

Although connectors are used by clients, they are configured on the server just like acceptors. There are a couple of important reasons why:

- A server itself can act as a client and therefore needs to know how to connect to other servers. For example, when one server is bridged to another or when a server takes part in a cluster.

- A server is often used by JMS clients to look up connection factory instances. In these cases, JNDI needs to know details of the connection factories used to create client connections. The information is provided to the client when a JNDI lookup is performed. See Configuring a Connection on the Client Side for more information.

Configuring a Connector

Like acceptors, connectors have their configuration attached to the query string of their URI. Below is an example of a connector that has the tcpNoDelay parameter set to false, which turns off Nagle’s algorithm for this connection.

```xml
< connector name="example-connector">tcp://localhost:61616?tcpNoDelay=false</ connector >
```

For details on connector configuration parameters, see Acceptor and Connector Configuration Parameters.

2.3. CONFIGURING A TCP CONNECTION

AMQ Broker uses Netty to provide basic, unencrypted, TCP-based connectivity that can be configured to use blocking Java IO or the newer, non-blocking Java NIO. Java NIO is preferred for better scalability with many concurrent connections. However, using the old IO can sometimes give you better latency than NIO when you are less worried about supporting many thousands of concurrent connections.

If you are running connections across an untrusted network, remember that a TCP network connection is unencrypted. You may want to consider using an SSL or HTTPS configuration to encrypt messages sent over this connection if encryption is a priority. Refer to Configuring Transport Layer Security for details.

When using a TCP connection, all connections are initiated from the client side. In other words, the server does not initiate any connections to the client, which works well with firewall policies that force connections to be initiated from one direction.

For TCP connections, the host and the port of the connector’s URI defines the address used for the connection.

Procedure
1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Add or modify the connection and include a URI that uses `tcp` as the protocol. Be sure to include both an IP or hostname as well as a port.

In the example below, an acceptor is configured as a TCP connection. A broker configured with this acceptor will accept clients making TCP connections to the IP `10.10.10.1` and port `61617`.

```xml
<acceptors>
  <acceptor name="tcp-acceptor">tcp://10.10.10.1:61617</acceptor>
  ...
</acceptors>
```

You configure a connector to use TCP in much the same way.

```xml
<connectors>
  <connector name="tcp-connector">tcp://10.10.10.2:61617</connector>
  ...
</connectors>
```

The connector above would be referenced by a client, or even the broker itself, when making a TCP connection to the specified IP and port, `10.10.10.2:61617`.

For details on available configuration parameters for TCP connections, see Acceptor and Connector Configuration Parameters. Most parameters can be used either with acceptors or connectors, but some only work with acceptors.

### 2.4. CONFIGURING AN HTTP CONNECTION

HTTP connections tunnel packets over the HTTP protocol and are useful in scenarios where firewalls allow only HTTP traffic. With single port support, AMQ Broker will automatically detect if HTTP is being used, so configuring a network connection for HTTP is the same as configuring a connection for TCP. For a full working example showing how to use HTTP, see the `http-transport` example, located under `INSTALL_DIR/examples/features/standard/`.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Add or modify the connection and include a URI that uses `tcp` as the protocol. Be sure to include both an IP or hostname as well as a port

In the example below, the broker will accept HTTP communications from clients connecting to port `80` at the IP address `10.10.10.1`. Furthermore, the broker will automatically detect that the HTTP protocol is in use and will communicate with the client accordingly.

```xml
<acceptors>
  <acceptor name="http-acceptor">tcp://10.10.10.1:80</acceptor>
  ...
</acceptors>
```

Configuring a connector for HTTP is again the same as for TCP.

```xml
<connectors>
  ...
</connectors>
```
Using the configuration in the example above, a broker will create an outbound HTTP connection to port 80 at the IP address 10.10.10.2.

An HTTP connection uses the same configuration parameters as TCP, but it also has some of its own. For details on HTTP-related and other configuration parameters, see Acceptor and Connector Configuration Parameters.

2.5. CONFIGURING AN SSL/TLS CONNECTION

You can also configure connections to use SSL/TLS. Refer to Configuring Transport Layer Security for details.

2.6. CONFIGURING AN IN-VM CONNECTION

An In-VM connection can be used when multiple brokers are co-located in the same virtual machine, as part of a high availability solution for example. In-VM connections can also be used by local clients running in the same JVM as the server. For an in-VM connection, the authority part of the URI defines a unique server ID. In fact, no other part of the URI is needed.

Procedure

1. Open the configuration file BROKER_INSTANCE_DIR/etc/broker.xml
2. Add or modify the connection and include a URI that uses vm as the protocol.

The example acceptor above tells the broker to accept connections from the server with an ID of 0. The other server must be running in the same virtual machine as the broker.

Configuring a connector as an in-vm connection follows the same syntax.

The acceptor in the example above defines how clients establish an in-VM connection to the server with an ID of 0 that resides in the same virtual machine. The client can be an application or broker.

2.7. CONFIGURING A CONNECTION FROM THE CLIENT SIDE

Connectors are also used indirectly in client applications. You can configure the JMS connection factory directly on the client side without having to define a connector on the server side:

```java
Map<String, Object> connectionParams = new HashMap<String, Object>();
```
connectionParams.put(org.apache.activemq.artemis.core.remoting.impl.netty.TransportConstants.PORT_PROP_NAME, 61617);

TransportConfiguration transportConfiguration =
    new TransportConfiguration(
    "org.apache.activemq.artemis.core.remoting.impl.netty.NettyConnectorFactory",
    connectionParams);

ConnectionFactory connectionFactory =
ActiveMQJMSClient.createConnectionFactoryWithoutHA(JMSFactoryType.CF, transportConfiguration);

Connection jmsConnection = connectionFactory.createConnection();
CHAPTER 3. NETWORK CONNECTIONS: PROTOCOLS

AMQ Broker has a pluggable protocol architecture, so that you can easily enable one or more protocols for a network connection.

The broker supports the following protocols:

- AMQP
- MQTT
- OpenWire
- STOMP

**NOTE**

In addition to the protocols above, the broker also supports its own native protocol known as "Core". Past versions of this protocol were known as "HornetQ" and used by Red Hat JBoss Enterprise Application Platform.

3.1. CONFIGURING A NETWORK CONNECTION TO USE A PROTOCOL

You must associate a protocol with a network connection before you can use it. (See Network Connections: Acceptors and Connectors for more information about how to create and configure network connections.) The default configuration, located in the file `BROKER_INSTANCE_DIR/etc/broker.xml`, includes several connections already defined. For convenience, AMQ Broker includes an acceptor for each supported protocol, plus a default acceptor that supports all protocols.

Default acceptors in broker.xml

```xml
<configuration>
  <core>
    ...
    <acceptors>
      <!-- Default ActiveMQ Artemis Acceptor. Multi-protocol adapter. Currently supports ActiveMQ Artemis Core, OpenWire, STOMP, AMQP, MQTT, and HornetQ Core. -->
      <acceptor name="artemis">tcp://0.0.0.0:61616?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576</acceptor>

      <!-- AMQP Acceptor. Listens on default AMQP port for AMQP traffic.-->
      <acceptor name="amqp">tcp://0.0.0.0:5672?protocols=AMQP</acceptor>

      <!-- STOMP Acceptor. -->
      <acceptor name="stomp">tcp://0.0.0.0:61613?protocols=STOMP</acceptor>

      <!-- HornetQ Compatibility Acceptor. Enables HornetQ Core and STOMP for legacy HornetQ clients. -->
      <acceptor name="hornetq">tcp://0.0.0.0:5445?protocols=HORNETQ,STOMP</acceptor>

      <!-- MQTT Acceptor -->
      <acceptor name="mqtt">tcp://0.0.0.0:1883?protocols=MQTT</acceptor>
    </acceptors>
  </core>
</configuration>
```
NOTE

The only requirement to enable a protocol is to add the protocols parameter to the URI query string. The value of the parameter must be a comma separated list of protocol names. If the protocol parameter is omitted from the URI all protocols are enabled.

For example, to create an acceptor for receiving messages on port 3232 using the AMQP protocol, follow these steps:

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`
2. Add the following line to the `<acceptors>` stanza:

```xml
<acceptor name="ampq">tcp://0.0.0.0:3232?protocols=AMQP</acceptor>
```

### 3.2. USING AMQP WITH A NETWORK CONNECTION

The broker supports the AMQP 1.0 specification. An AMQP link is a uni-directional protocol for messages between a source and a target, that is, a client and the broker.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`
2. Add or configure an acceptor to receive AMQP clients by including the protocols parameter with a value of AMQP as part of the URI, as shown in the following example:

```xml
<acceptors>
  <acceptor name="amqp-acceptor">tcp://localhost:5672?protocols=AMQP</acceptor>
  ...
</acceptors>
```

In the preceding example, the broker accepts AMQP 1.0 clients on port 5672, which is the default AMQP port.

An AMQP link has two endpoints, a sender and a receiver. When senders transmit a message, the broker converts it into an internal format, so it can be forwarded to its destination on the broker. Receivers connect to the destination at the broker and convert the messages back into AMQP before they are delivered.

If an AMQP link is dynamic, a temporary queue is created and either the remote source or the remote target address is set to the name of the temporary queue. If the link is not dynamic, the address of the remote target or source is used for the queue. If the remote target or source does not exist, an exception is sent.

A link target can also be a Coordinator, which is used to handle the underlying session as a transaction, either rolling it back or committing it.
AMQP allows the use of multiple transactions per session, `amqp:multi-txns-per-ssn`, however the current version of AMQ Broker will support only single transactions per session.

The details of distributed transactions (XA) within AMQP are not provided in the 1.0 version of the specification. If your environment requires support for distributed transactions, it is recommended that you use the AMQ Core Protocol JMS.

See the AMQP 1.0 specification for more information about the protocol and its features.

### 3.2.1. Using an AMQP Link as a Topic

Unlike JMS, the AMQP protocol does not include topics. However, it is still possible to treat AMQP consumers or receivers as subscriptions rather than just consumers on a queue. By default, any receiving link that attaches to an address with the prefix `jms.topic`, is treated as a subscription, and a subscription queue is created. The subscription queue is made durable or volatile, depending on how the Terminus Durability is configured, as captured in the following table:

<table>
<thead>
<tr>
<th>To create this kind of subscription for a multicast-only queue...</th>
<th>Set Terminus Durability to this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Durable</td>
<td>UNSETTLED_STATE or CONFIGURATION</td>
</tr>
<tr>
<td>Non-durable</td>
<td>NONE</td>
</tr>
</tbody>
</table>

The name of a durable queue is composed of the container ID and the link name, for example `my-container-id:my-link-name`.

AMQ Broker also supports the qpid-jms client and will respect its use of topics regardless of the prefix used for the address.

### 3.2.2. Configuring AMQP Security

The broker supports AMQP SASL Authentication. See Security for more information about how to configure SASL-based authentication on the broker.

### 3.3. USING MQTT WITH A NETWORK CONNECTION

The broker supports MQTT v3.1.1 (and also the older v3.1 code message format). MQTT is a lightweight, client to server, publish/subscribe messaging protocol. MQTT reduces messaging overhead and network traffic, as well as a client’s code footprint. For these reasons, MQTT is ideally suited to constrained devices such as sensors and actuators and is quickly becoming the de facto standard communication protocol for Internet of Things(IoT).
1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`.

2. Add an acceptor with the MQTT protocol enabled. For example:

   ```xml
   <acceptors>
   <acceptor name="mqtt">tcp://localhost:1883?protocols=MQTT</acceptor>
   ...
   </acceptors>
   ```

   MQTT comes with a number of useful features including:

   **Quality of Service**
   
   Each message can define a quality of service that is associated with it. The broker will attempt to deliver messages to subscribers at the highest quality of service level defined.

   **Retained Messages**
   
   Messages can be retained for a particular address. New subscribers to that address receive the last-sent retained message before any other messages, even if the retained message was sent before the client connected.

   **Wild card subscriptions**
   
   MQTT addresses are hierarchical, similar to the hierarchy of a file system. Clients are able to subscribe to specific topics or to whole branches of a hierarchy.

   **Will Messages**
   
   Clients are able to set a "will message" as part of their connect packet. If the client abnormally disconnects, the broker will publish the will message to the specified address. Other subscribers receive the will message and can react accordingly.

   The best source of information about the MQTT protocol is in the specification. The MQTT v3.1.1 specification can be downloaded from the [OASIS website](http://oasis.openorganization.org/).

3.4. USING OPENWIRE WITH A NETWORK CONNECTION

The broker supports the OpenWire protocol, which allows a JMS client to talk directly to a broker. Use this protocol to communicate with older versions of AMQ Broker.

Currently AMQ Broker supports OpenWire clients that use standard JMS APIs only.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`.

2. Add or modify an acceptor so that it includes `OPENWIRE` as part of the `protocol` parameter, as shown in the following example:

   ```xml
   <acceptors>
   <acceptor name="openwire-acceptor">tcp://localhost:61616?protocols=OPENWIRE</acceptor>
   ...
   </acceptors>
   ```

   In the preceding example, the broker will listen on port 61616 for incoming OpenWire commands.

   For more details, see the examples located under `INSTALL_DIR/examples/protocols/openwire`. 
3.5. USING STOMP WITH A NETWORK CONNECTION

**STOMP** is a text-orientated wire protocol that allows STOMP clients to communicate with STOMP Brokers. The broker supports STOMP 1.0, 1.1 and 1.2. STOMP clients are available for several languages and platforms making it a good choice for interoperability.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Configure an existing `acceptor` or create a new one and include a `protocols` parameter with a value of `STOMP`, as below.

   ```xml
   <acceptors>
   <acceptor name="stomp-acceptor">tcp://localhost:61613?protocols=STOMP</acceptor>
   ...
   </acceptors>
   ```

In the preceding example, the broker accepts STOMP connections on the port **61613**, which is the default.

See the `stomp` example located under `INSTALL_DIR/examples/protocols` for an example of how to configure a broker with STOMP.

### 3.5.1. Knowing the Limitations When Using STOMP

When using STOMP, the following limitations apply:

1. The broker currently does not support virtual hosting, which means the `host` header in `CONNECT` frames are ignored.

2. Message acknowledgements are not transactional. The `ACK` frame cannot be part of a transaction, and it is ignored if its `transaction` header is set).

### 3.5.2. Providing IDs for STOMP Messages

When receiving STOMP messages through a JMS consumer or a QueueBrowser, the messages do not contain any JMS properties, for example `JMSMessageID`, by default. However, you can set a message ID on each incoming STOMP message by using a broker parameter.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Set the `stompEnableMessageId` parameter to `true` for the `acceptor` used for STOMP connections, as shown in the following example:

   ```xml
   <acceptors>
   <acceptor name="stomp-acceptor">tcp://localhost:61613?protocols=STOMP;stompEnableMessageId=true</acceptor>
   ...
   </acceptors>
   ```
By using the `stompEnableMessageId` parameter, each stomp message sent using this acceptor has an extra property added. The property key is `amq-message-id` and the value is a String representation of an internal message id prefixed with “STOMP”, as shown in the following example:

```
amq-message-id : STOMP12345
```

If `stompEnableMessageId` is not specified in the configuration, the default value is `false`.

### 3.5.3. Setting a Connection’s Time to Live (TTL)

STOMP clients must send a `DISCONNECT` frame before closing their connections. This allows the broker to close any server-side resources, such as sessions and consumers. However, if STOMP clients exit without sending a DISCONNECT frame, or if they fail, the broker will have no way of knowing immediately whether the client is still alive. STOMP connections therefore are configured to have a “Time to Live” (TTL) of 1 minute. The means that the broker stops the connection to the STOMP client if it has been idle for more than one minute.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Add the `connectionTtl` parameter to URI of the `acceptor` used for STOMP connections, as shown in the following example:

```
<acceptors>
  <acceptor name="stomp-acceptor">tcp://localhost:61613?
    protocols=STOMP;connectionTtl=20000</acceptor>
  ...
</acceptors>
```

In the preceding example, any stomp connection that using the `stomp-acceptor` will have its TTL set to 20 seconds.

**NOTE**

Version 1.0 of the STOMP protocol does not contain any heartbeat frame. It is therefore the user’s responsibility to make sure data is sent within connection-ttl or the broker will assume the client is dead and clean up server-side resources. With version 1.1, you can use heart-beats to maintain the life cycle of stomp connections.

**Overriding the Broker’s Default Time to Live (TTL)**

As noted, the default TTL for a STOMP connection is one minute. You can override this value by adding the `connection-ttl-override` attribute to the broker configuration.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Add the `connection-ttl-override` attribute and provide a value in milliseconds for the new default. It belongs inside the `<core>` stanza, as below.

```
<configuration ...>
  ...
  <core ...
```


In the preceding example, the default Time to Live (TTL) for a STOMP connection is set to 30 seconds, 30000 milliseconds.

### 3.5.4. Sending and Consuming STOMP Messages from JMS

STOMP is mainly a text-orientated protocol. To make it simpler to interoperate with JMS, the STOMP implementation checks for presence of the `content-length` header to decide how to map a STOMP message to JMS.

<table>
<thead>
<tr>
<th>If you want a STOMP message to map to a ...</th>
<th>The message should....</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMS TextMessage</td>
<td>Not include a <code>content-length</code> header.</td>
</tr>
<tr>
<td>JMS BytesMessage</td>
<td>Include a <code>content-length</code> header.</td>
</tr>
</tbody>
</table>

The same logic applies when mapping a JMS message to STOMP. A STOMP client can confirm the presence of the `content-length` header to determine the type of the message body (string or bytes).

See the STOMP specification for more information about message headers.

### 3.5.5. Mapping STOMP Destinations to AMQ Broker Addresses and Queues

When sending messages and subscribing, STOMP clients typically include a `destination` header. Destination names are string values, which are mapped to a destination on the broker. In AMQ Broker, these destinations are mapped to addresses and queues. See the STOMP specification for more information about the destination frame.

Take for example a STOMP client that sends the following message (headers and body included):

```
SEND
destination:/my/stomp/queue
hello queue a
^@
```

In this case, the broker will forward the message to any queues associated with the address /my/stomp/queue.

For example, when a STOMP client sends a message (by using a SEND frame), the specified destination is mapped to an address.

It works the same way when the client sends a `SUBSCRIBE` or `UNSUBSCRIBE` frame, but in this case AMQ Broker maps the `destination` to a queue.

```
SUBSCRIBE
destination: /other/stomp/queue
```
In the preceding example, the broker will map the destination to the queue /other/stomp/queue.

**Mapping STOMP Destinations to JMS Destinations**

JMS destinations are also mapped to broker addresses and queues. If you want to use STOMP to send messages to JMS destinations, the STOMP destinations must follow the same convention:

- Send or subscribe to a JMS Queue by prepending the queue name by `jms.queue`. For example, to send a message to the *orders* JMS Queue, the STOMP client must send the frame:

  ```
  SEND
  destination:jms.queue.orders
  hello queue orders
  ```

- Send or subscribe to a JMS Topic by prepending the topic name by `jms.topic`. For example, to subscribe to the *stocks* JMS Topic, the STOMP client must send a frame similar to the following:

  ```
  SUBSCRIBE
  destination:jms.topic.stocks
  ```
CHAPTER 4. ADDRESSES, QUEUES, AND TOPICS

AMQ Broker has a unique addressing model that is both powerful and flexible and that offers great performance. The addressing model comprises three main concepts: addresses, queues and routing types.

An **address** represents a messaging endpoint. Within the configuration, a typical address is given a unique name, 0 or more queues, and a routing type.

A **queue** is associated with an address. There can be multiple queues per address. Once an incoming message is matched to an address, the message is sent on to one or more of its queues, depending on the routing type configured. Queues can be configured to be automatically created and deleted.

A **routing type** determines how messages are sent to the queues associated with an address. A AMQ Broker address can be configured with two different routing types.

<table>
<thead>
<tr>
<th>If you want your messages routed to...</th>
<th>Use this routing type ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single queue within the matching address, in a point-to-point manner.</td>
<td><strong>anycast</strong></td>
</tr>
<tr>
<td>Every queue within the matching address, in a publish-subscribe manner.</td>
<td><strong>multicast</strong></td>
</tr>
</tbody>
</table>

**NOTE**

An address must have at least one routing type.

It is possible to define more than one routing type per address, but this typically results in an anti-pattern and is therefore not recommended.

If an address does use both routing types, however, and the client does not show a preference for either one, the broker typically defaults to the **anycast** routing type. The one exception is when the client uses the MQTT protocol. In that case, the default routing type is **multicast**.

4.1. ADDRESS AND QUEUE NAMING REQUIREMENTS

You should be aware of the following requirements when you configure addresses and queues:

- To ensure that a client can connect to a queue regardless of which wire protocol it uses, your address and queue names should not include any of the following characters:
  & :: , ? >
- The # and * characters are reserved for wildcard expressions. For more information, see the section called “AMQ Broker Wildcard Syntax”.
- Address and queue names should not include any spaces.
- To separate words in an address or queue name, use the configured delimiter character (the default is the . character). For more information, see the section called "AMQ Broker Wildcard Syntax".
4.2. CONFIGURING POINT-TO-POINT MESSAGING

Point-to-point messaging is a common scenario in which a message sent by a producer has only one consumer. AMQP and JMS message producers and consumers can make use of point-to-point messaging queues, for example. Define an anycast routing type for an address so that its queues receive messages in a point-to-point manner.

When a message is received on an address using anycast, AMQ Broker locates the queue associated with the address and routes the message to it. When consumers request to consume from the address, the broker locates the relevant queue and associates this queue with the appropriate consumers. If multiple consumers are connected to the same queue, messages are distributed amongst each consumer equally, providing the consumers are equally able to handle them.

Figure 4.1. Point-to-Point

Procedure

1. Open the file BROKER_INSTANCE_DIR/etc/broker.xml for editing.
2. Wrap an anycast configuration element around the chosen queue element of an address. Ensure the value of address name and queue name elements are same.

```
<configuration ...
<core ...
... 
 <address name="durable">
 <anycast>
 <queue name="durable"/>
 </anycast>
 </address>
</core>
</configuration>
```

4.3. CONFIGURING PUBLISH-SUBSCRIBE MESSAGING

In a publish-subscribe scenario, messages are sent to every consumer subscribed to an address. JMS topics and MQTT subscriptions are two examples of publish-subscribe messaging. When a message is received on an address with a multicast routing type, AMQ Broker routes a copy of the message to each queue. To reduce the overhead of copying, each queue is sent only a reference to the message and not a full copy.
Procedure

1. Open the file `BROKER_INSTANCE_DIR/etc/broker.xml` for editing.

2. Add an empty `multicast` configuration element to the chosen address.

   ```xml
   <configuration ...>
   <core ...>
   ...
   <address name="topic.foo">
   <multicast/>
   </address>
   </core>
   </configuration>
   ```

3. (Optional) Add one more `queue` elements to the address and wrap the `multicast` element around them. This step is typically not needed since the broker automatically creates a queue for each subscription requested by a client.

   ```xml
   <configuration ...>
   <core ...>
   ...
   <address name="topic.foo">
   <multicast>
   <queue name="client123.topic.foo"/>
   <queue name="client456.topic.foo"/>
   </multicast>
   </address>
   </core>
   </configuration>
   ```

4.4. CONFIGURING A POINT-TO-POINT USING TWO QUEUES

You can define more than one queue on an address by using an `anycast` routing type. Messages sent to an `anycast` address are distributed evenly across all associated queues. By using Fully Qualified Queue Names, which are described later, you can have clients connect to a specific queue. If more than one
consumer connects to the same queue, AMQ Broker distributes messages between them.

**Figure 4.3. Point-to-Point with Two Queues**

NOTE
This is how AMQ Broker handles load balancing of queues across multiple nodes in a cluster.

**Procedure**

1. Open the file `BROKER_INSTANCE_DIR/etc/broker.xml` for editing.

2. Wrap an `anycast` configuration element around the `queue` elements in the `address`.

```xml
<configuration ...
  <core ...
    ...
      <address name="address.foo"> ...
        <anycast>
          <queue name="q1"/>
          <queue name="q2"/>
        </anycast>
      </address>
    </core>
  </configuration>
```

4.5. USING POINT-TO-POINT AND PUBLISH-SUBSCRIBE TOGETHER

It is possible to define an address with both point-to-point and publish-subscribe semantics enabled. While not typically recommended, this can be useful when you want, for example, a JMS Queue named `orders` and a JMS topic named `orders`. The different routing types make the addresses appear to be distinct.

Using an example of JMS clients, the messages sent by a JMS queue producer are routed using the `anycast` routing type. Messages sent by a JMS topic producer uses the `multicast` routing type. In addition, when a JMS topic consumer attaches, it is attached to its own subscription queue. The JMS queue consumer, however, is attached to the `anycast` queue.
NOTE

The behavior in this scenario is dependent on the protocol being used. For JMS there is a clear distinction between topic and queue producers and consumers, which makes the logic straightforward. Other protocols like AMQP do not make this distinction. A message being sent via AMQP is routed by both anycast and multicast and consumers default to anycast. For more information, check the behavior of each protocol in the sections on protocols.

The XML excerpt below is an example of what the configuration for an address using both anycast and multicast routing types would look like in BROKER_INSTANCE_DIR/etc/broker.xml. Note that subscription queues are typically created on demand, so there is no need to list specific queue elements inside the multicast routing type.

```xml
<configuration ...>
  <core ...>...
    <address name="foo.orders"> 
      <anycast>
        <queue name="orders"/>
      </anycast>
      <multicast/>
    </address>
  </core>
</configuration>
```

4.6. CONFIGURING SUBSCRIPTION QUEUES

In most cases it is not necessary to pre-create subscription queues because protocol managers create...
subscription queues automatically when clients first request to subscribe to an address. See Protocol Managers and Addresses for more information. For durable subscriptions, the generated queue name is usually a concatenation of the client id and the address.

Configuring a Durable Subscription Queue
When an queue is configured as a durable subscription, the broker saves messages for any inactive subscribers and delivers them to the subscribers when they reconnect. Clients are therefore guaranteed to receive each message delivered to the queue after subscribing to it.

Procedure
1. Open the file `BROKER_INSTANCE_DIR/etc/broker.xml` for editing.
2. Add the `durable` configuration element to the chosen `queue` and assign it a value of `true`.

```xml
<configuration ...>
  <core ...>
    ...
    <address name="durable.foo">
      <multicast>
        <queue name="q1">
          <durable>true</durable>
        </queue>
        <queue name="orders1">
          <durable>true</durable>
        </queue>
        <queue name="orders2">
          <durable>true</durable>
        </queue>
      </multicast>
    </address>
  </core>
</configuration>
```

Configuring a Non-Shared Durable Subscription
The broker can be configured to prevent more than one consumer from connecting to a queue at any one time. The subscriptions to queues configured this way are therefore “non-shared”.

Procedure
1. Open the file `BROKER_INSTANCE_DIR/etc/broker.xml` for editing.
2. Add the `durable` configuration element to each chosen queue.

```xml
<configuration ...>
  <core ...>
    ...
    <address name="non.shared.durable.foo">
      <multicast>
        <queue name="orders1">
          <durable>true</durable>
        </queue>
        <queue name="orders2">
          <durable>true</durable>
        </queue>
      </multicast>
    </address>
  </core>
</configuration>
```
3. Add the `max-consumers` attribute to each chosen `queue` element and assign it a value of `1`. 
4.7. USING A FULLY QUALIFIED QUEUE NAME

Internally the broker maps a client’s request for an address to specific queues. The broker decides on behalf of the client which queues to send messages, or from which queue to receive messages. However, more advanced use cases might require that the client specify a queue directly. In these situations the client can use a Fully Qualified Queue Name (FQQN), by specifying both the address name and the queue name, separated by a ::.

Prerequisites

- An address is configured with two or more queues. In the example below the address foo has two queues, q1 and q2.

```
<configuration ...>
  <core ...
    ...
      <address name="non.shared.durable.foo">
        <multicast>
          <queue name="orders1" max-consumers="1">
            <durable>true</durable>
          </queue>
          <queue name="orders2" max-consumers="1">
            <durable>true</durable>
          </queue>
        </multicast>
      </address>
    ...
  </core>
</configuration>
```

Procedure

- In the client code, use both the address name and the queue name when requesting a connection from the broker. Remember to use two colons, ::, to separate the names, as in the example Java code below.

```java
String FQQN = "foo::q1";
Queue q1 = session.createQueue(FQQN);
MessageConsumer consumer = session.createConsumer(q1);
```
4.8. CONFIGURING SHARDED QUEUES

A common pattern for processing of messages across a queue where only partial ordering is required is to use queue sharding. In AMQ Broker this can be achieved by creating an anycast address that acts as a single logical queue, but which is backed by many underlying physical queues.

Procedure

1. Open `BROKER_INSTANCE_DIR/etc/broker.xml` and add an address with the desired name. In the example below the address named `sharded` is added to the configuration.

   ```xml
   <configuration ...>
   <core ...>
   ...  
   <addresses>
   <address name="sharded"></address>
   </addresses>
   </core>
   </configuration>
   
   2. Add the anycast routing type and include the desired number of sharded queues. In the example below, the queues `q1`, `q2`, and `q3` are added as anycast destinations.

   ```xml
   <configuration ...>
   <core ...>
   ...  
   <addresses>
   <address name="sharded">
   <anycast>
   <queue name="q1" />
   <queue name="q2" />
   <queue name="q3" />
   </anycast>
   </address>
   </addresses>
   </core>
   </configuration>
   ``

Using the configuration above, messages sent to `sharded` are distributed equally across `q1`, `q2` and `q3`. Clients are able to connect directly to a specific physical queue when using a fully qualified queue name and receive messages sent to that specific queue only.

To tie particular messages to a particular queue, clients can specify a message group for each message. The broker routes grouped messages to the same queue, and one consumer processes them all. See the chapter on Message Grouping for more information.

4.9. CONFIGURING LAST VALUE QUEUES

A last value queue is a type of queue that discards messages in the queue when a newer message with the same last value property name is placed in the queue. Through this behavior, last value queues retain only the last values for messages of the same property.

A simple use case for a last value queue is for monitoring stock prices, where only the latest value for a particular stock is of interest.
The broker delivers messages that are sent to a last value queue without a configured last value property as normal messages. Such messages are not purged from the queue when a new message with a configured last value property arrives.

You can configure last value queues using:

- The `broker.xml` configuration file
- The JMS client
- The Core API
- Address wildcards

For each of the above methods, apart from the Core API, you can specify a custom value for the last value key (also called the last value property), or leave this value unset, meaning that the key is set to the default value instead. The default value for the last value key is `_AMQ_LVQ_NAME_`.

For the Core API, you create last value queues using the constant last value key `Message.HDR_LAST_VALUE_NAME` to identify last value messages.

### 4.9.1. Configuring Last Value Queues Using broker.xml

To specify a custom value for the last value key, include lines in your `broker.xml` configuration file that look like the following:

```xml
<address name="my.address">
  <multicast>
    <queue name="prices1" last-value-key="stock_ticker"/>
  </multicast>
</address>
```

Alternatively, you can configure a last value queue that uses the default last value key name of `_AMQ_LVQ_NAME_`. To do this, set the last-value configuration parameter to true in your `broker.xml` configuration file, without specifying a value for the last value key. An example of this configuration is shown below.

```xml
<address name="my.address">
  <multicast>
    <queue name="prices1" last-value="true"/>
  </multicast>
</address>
```

### 4.9.2. Configuring Last Value Queues Using the JMS Client

When using the JMS Client to auto-create destinations used by a consumer, you can specify a last value key as part of the address settings. In this case, the auto-created queues are last value queues. An example of this configuration is shown below.

```java
Queue queue = session.createQueue("my.destination.name?last-value-key=stock_ticker");
Topic topic = session.createTopic("my.destination.name?last-value-key=stock_ticker");
```
Alternatively, configure a last value queue that uses the default last value key name of 
_AMQ_LVQ_NAME. To do this, set the last-value configuration parameter to true, without specifying a 
value for the last value key. An example of this configuration is shown below.

```java
Queue queue = session.createQueue("my.destination.name?last-value=true");
Topic topic = session.createTopic("my.destination.name?last-value=true");
```

4.9.3. Configuring Last Value Queues Using the Core API

To create a last value queue using the Core API, set the lastvalue parameter to true when creating a 
queue. To do this, use the createQueue method of the ClientSession interface. The syntax for 
creating a last value queue using this method is shown below.

```java
void createQueue(  
    SimpleString address,  
    RoutingType routingType,  
    SimpleString queueName,  
    SimpleString filter,  
    Boolean durable,  
    Boolean autoCreated,  
    int maxConsumers,  
    Boolean purgeOnNoConsumers,  
    Boolean exclusive,  
    Boolean lastValue  
)
```

In this case, the API uses the constant Message.HDR_LAST_VALUE_NAME to identify last value 
messages delivered to the queue.

Additional Resources

- For more information about using the createQueue method of the Core API to create a last 
  value queue, see createQueue.

4.9.4. Configuring Last Value Queues Using Address Wildcards

You can use address wildcards in the broker.xml configuration file to configure last value queues for a 
set of addresses. An example of this configuration is shown below.

```xml
<address-setting match="lastValueQueue">  
    <default-last-value-key>stock_ticker</default-last-value-key>  
</address-setting>
```

By default, the value of default-last-value-key is null.

When using address wildcards, you can also use the default last value key name. To do this, set the 
default-last-value-queue parameter to true, without specifying a value for the last value key.

4.9.5. Example of Last Value Queue Behavior

This example shows the configuration and behavior of a last value queue.

In your broker.xml configuration file, suppose that you have added configuration that looks like the 
following:
The configuration shown above creates a last value queue called *prices1*, with a last value key of *stock_ticker*.

Now, suppose that a client sends two messages with the same last value property name to the *prices1* queue, as shown below:

```
TextMessage message = session.createTextMessage("First message with last value property set");
message.setStringProperty("stock_ticker", "36.83");
producer.send(message);

TextMessage message = session.createTextMessage("Second message with last value property set");
message.setStringProperty("stock_ticker", "37.02");
producer.send(message);
```

When two messages with the same last value property name arrive to the last value queue *prices1*, only the latest message remains in the queue, with the first message being purged. At the command line, you can enter the following lines to validate this behavior:

```
TextMessage messageReceived = (TextMessage)messageConsumer.receive(5000);
System.out.format("Received message: %s\n", messageReceived.getText());
```

In this example, the output you see is the second message, since both messages use the last value property and the second message was received in the queue after the first.

### 4.9.6. Creating Non-Destructive Consumers

When a consumer attaches to a queue, the normal behavior is that messages sent to that consumer are acquired exclusively by the consumer. When the consumer acknowledges receipt of the messages, the broker removes the messages from the queue.

An alternative way to configure a consumer is to configure it as a queue *browser*. In this case, the queue still sends all messages to the consumer. However the browser does not prevent other consumers from receiving the messages. In addition, the messages remain in the queue once the browser has consumed the messages. A consumer configured as a browser is an instance of a non-destructive consumer.

In the case of a last value queue, configuring all consumers as non-destructive consumers ensures that the queue always retains the most up-to-date value for every last value key. The examples in the following sub-sections show how to configure a last value queue to ensure that all consumers are non-destructive.

#### 4.9.6.1. Configuring Non-destructive Consumers Using broker.xml

In the *broker.xml* configuration file, to create a last value queue, set the *non-destructive* parameter to *true*. An example of this configuration is shown below.

```
<address name="my.address">
  <multicast>
    <queue name="prices1" last-value-key="stock_ticker"/>
  </multicast>
</address>
```
4.9.6.2. Creating Non-destructive Consumers Using the JMS Client

When using the JMS Client to auto-create destinations used by a consumer, you configure last value queue behavior and non-destructive consumers as part of the address settings. An example of this configuration is shown below.

```
Queue queue = session.createQueue("my.destination.name?last-value-key=stock_ticker&non-destructive=true");
Topic topic = session.createTopic("my.destination.name?last-value-key=stock_ticker&non-destructive=true");
```

4.9.6.3. Configuring Non-destructive Consumers Using Address Wildcards

You can use address wildcards in the broker.xml configuration file to configure last value queues for a set of addresses. As part of this configuration, you can also specify that consumers are non-destructive, by setting `default-non-destructive` to `true`. An example of this configuration is shown below.

```
<address-setting match="lastValueQueue">
    <default-last-value-key>stock_ticker</default-last-value-key>
    <default-non-destructive>true</default-non-destructive>
</address-setting>
```

By default, the value of `default-non-destructive` is `false`.

4.9.6.4. Configuring Message Expiry Delay

For a queue other than a last value queue, if you have only non-destructive consumers, the broker never deletes messages from the queue, causing the queue size to increase over time. To prevent this unconstrained growth in queue size, use the `expiry-delay` parameter to specify when messages expire.

Specify a message expiry delay in the `address-setting` element of your broker.xml configuration file, as shown in the following example:

```
<address-setting match="exampleQueue">
    <expiry-delay>10</expiry-delay>
</address-setting>
```

When you add the preceding lines to your broker.xml configuration file, the broker sends expired messages in `exampleQueue` to the expiry address `expiryQueue`.

`expiry-delay` defines the expiration time, in milliseconds, that will be applied to messages that are using the default expiration time. By default, messages have an expiration time of `0`, meaning that they don’t expire. For messages with an expiration time greater than the default, `expiry-delay` has no effect.

For example, suppose you set `expiry-delay` on a queue to `10`. If a message with the default expiration time of `0` arrives in the queue, then the broker changes the expiration time of the message from `0` to `10`. However, if another message that is using an expiration time of `20` arrives in the queue, then its expiration time remains unchanged. If you set `expiry-delay` to `-1`, this feature is disabled. By default, `expiry-delay` is set to `-1`. 

4.10. LIMITING THE NUMBER OF CONSUMERS CONNECTED TO A QUEUE

Limit the number of consumers connected to a particular queue by using the `max-consumers` attribute. Create an exclusive consumer by setting `max-consumers` flag to 1. The default value is -1, which is sets an unlimited number of consumers.

Procedure

1. Open `BROKER_INSTANCE_DIR/etc/broker.xml` and add the `max-consumers` attribute to the desired queue. In the example below, only 20 consumers can connect to the queue `q3` at the same time.

   ```xml
   <configuration ...>
   <core ...>
   ...<addresses>
   <address name="foo">
   <anycast>
   <queue name="q3" max-consumers="20"/>
   </anycast>
   </address>
   </addresses>
   </core>
   </configuration>
   ``

2. (Optional) Create an exclusive consumer by setting `max-consumers` to 1, as in the example below.

   ```xml
   <configuration ...>
   <core ...>
   ...<addresses>
   <address name="foo">
   <anycast>
   <queue name="q3" max-consumers="1"/>
   </anycast>
   </address>
   </addresses>
   </core>
   </configuration>
   ``

3. (Optional) Have an unlimited number of consumers by setting `max-consumers` to -1, as in the example below.

   ```xml
   <configuration ...>
   <core ...>
   ...<addresses>
   <address name="foo">
   <anycast>
   <queue name="q3" max-consumers="-1"/>
   </anycast>
   </address>
   </addresses>
   </core>
   </configuration>
   ```
4.11. EXCLUSIVE QUEUES

Exclusive queues are special queues that route all messages to only one consumer at a time. This is useful when you want all messages to be processed serially by the same consumer. If there are multiple consumers on a queue only one consumer will receive messages. If this consumer disconnects then another consumer is chosen.

4.11.1. Configuring Exclusive Queues

You configure exclusive queues in the `broker.xml` configuration file something like this.

```
<configuration ...>
  <core ...>
    ...
    <address name="foo.bar">
      <multicast>
        <queue name="orders1" exclusive="true"/>
      </multicast>
    </address>
  </core>
</configuration>
```

Or on auto-create when using the JMS Client by using address parameters when creating the destination used by the consumer.

```java
Queue queue = session.createQueue("my.destination.name?exclusive=true");
Topic topic = session.createTopic("my.destination.name?exclusive=true");
```

4.11.2. Setting the Exclusive Queue Default

```
<address-setting match="myQueue">
  <default-exclusive-queue>true</default-exclusive-queue>
</address-setting>
```

The default value for `default-exclusive-queue` is `false`.

4.12. CONFIGURING A PREFIX TO CONNECT TO A SPECIFIC ROUTING TYPE

Normally, if a message is received by an address that uses both `anycast` and `multicast`, one of the `anycast` queues receive the message and all of the `multicast` queues. However, clients can specify a special prefix when connecting to an address to specify whether to connect using `anycast` or `multicast`. The prefixes are custom values that are designated using the `anycastPrefix` and `multicastPrefix` parameters within the URL of an `acceptor`.

Configuring an Anycast Prefix

- In `BROKER_INSTANCE_DIR/etc/broker.xml`, add the `anycastPrefix` to the URL of the desired `acceptor`. In the example below, the `acceptor` is configured to use `anycast://` for the `anycastPrefix`. Client code can specify `anycast://foo/` if the client needs to send a message to only one of the anycast queues.
Configuring a Multicast Prefix

- In `BROKER_INSTANCE_DIR/etc/broker.xml`, add the `anycastPrefix` to the URL of the desired acceptor. In the example below, the acceptor is configured to use `multicast://` for the `multicastPrefix`. Client code can specify `multicast://foo/` if the client needs the message sent to only the multicast queues of the address.

```
<configuration ...>
  <core ...>
    ...
    <acceptors>
      <!-- Acceptor for every supported protocol -->
      <acceptor name="artemis">tcp://0.0.0.0:61616?
        protocols=AMQP;anycastPrefix=anycast://</acceptor>
      </acceptors>
    ...
  </core>
</configuration>
```

4.13. PROTOCOL MANAGERS AND ADDRESSES

A protocol manager maps protocol-specific concepts down to the AMQ Broker address model concepts: queues and routing types. For example, when a client sends a MQTT subscription packet with the addresses `/house/room1/lights` and `/house/room2/lights`, the MQTT protocol manager understands that the two addresses require `multicast` semantics. The protocol manager therefore first looks to ensure that `multicast` is enabled for both addresses. If not, it attempts to dynamically create them. If successful, the protocol manager then creates special subscription queues for each subscription requested by the client.

Each protocol behaves slightly differently. The table below describes what typically happens when subscribe frames to various types of queue are requested.

Table 4.2. Protocol Manager Actions

<table>
<thead>
<tr>
<th>If the queue is of this type...</th>
<th>The typical action for a protocol manager is to...</th>
</tr>
</thead>
</table>

42
<table>
<thead>
<tr>
<th>If the queue is of this type...</th>
<th>The typical action for a protocol manager is to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Durable Subscription Queue</td>
<td>Look for the appropriate address and ensures that <strong>multicast</strong> semantics is enabled. It then creates a special subscription queue with the client ID and the address as its name and <strong>multicast</strong> as its routing type. The special name allows the protocol manager to quickly identify the required client subscription queues should the client disconnect and reconnect at a later date. When the client unsubscribes the queue is deleted.</td>
</tr>
<tr>
<td>Temporary Subscription Queue</td>
<td>Look for the appropriate address and ensures that <strong>multicast</strong> semantics is enabled. It then creates a queue with a random (read UUID) name under this address with <strong>multicast</strong> routing type. When the client disconnects the queue is deleted.</td>
</tr>
<tr>
<td>Point-to-Point Queue</td>
<td>Look for the appropriate address and ensures that <strong>anycast</strong> routing type is enabled. If it is, it aims to locate a queue with the same name as the address. If it does not exist, it looks for the first queue available. It this does not exist then it automatically creates the queue (providing auto create is enabled). The queue consumer is bound to this queue. If the queue is auto created, it is automatically deleted once there are no consumers and no messages in it.</td>
</tr>
</tbody>
</table>

### 4.14. DISABLING ADVISORY MESSAGES

By default, AMQ creates advisory messages about addresses and queues when an OpenWire client is connected to the broker. **Advisory** messages are sent to internally managed addresses created by the broker. These addresses appear on the AMQ Console within the same display as user-deployed addresses and queues. Although they provide useful information, advisory messages can cause unwanted consequences when the broker manages a large number of destinations. For example, the messages might increase memory usage or strain connection resources. Also, the AMQ Console might become cluttered when attempting to display all of the addresses created to send advisory messages.

To avoid these situations, use the `supportAdvisory` and `suppressInternalManagementObjects` parameters to manage the advisory messages behavior on the broker side.

- **supportAdvisory**: Set this option to `true` to enable creation of advisory messages or `false` to disable them. The default value is `true`.

- **suppressInternalManagementObjects**: Set this option to `true` to expose the advisory messages to the management service such as JMX registry and AMQ Console, or `false` to not expose them. The default value is `true`.

Use these parameters by editing the `BROKER_INSTANCE_DIR/etc/broker.xml` configuration file and configure the parameters on openwire acceptors by using URLs. For example:
4.15. CONFIGURING ADDRESS SETTINGS

AMQ Broker has several configurable options that control aspects of how and when a message is delivered, how many attempts should be made, and when the message expires. These configuration options all exist within the `<address-setting>` configuration element. You can have AMQ Broker apply a single `<address-setting>` to multiple destinations by using a wildcard syntax.

**AMQ Broker Wildcard Syntax**

AMQ Broker uses a specific syntax for representing wildcards in security settings, address settings, and when creating consumers.

- A wildcard expression contains words delimited by the character `.`.
- The special characters `#` and `*` also have special meaning and can take the place of a word.
- The character `#` means 'match any sequence of zero or more words'. Use this at the end of your expression.
- The character `*` means 'match a single word'. Use this anywhere within your expression.

Matching is not done character by character, but at each delimiter boundary. For example, an `<address-setting>` looking to match queues using `my` in their name would not match with a queue named `myqueue`.

When more than one `<address-setting>` matches a queue, the broker will overlay configurations, using the configuration of the least specific match as the baseline. Literal expressions are more specific than wildcards, and `*` is more specific than `#`. For example, both `my.queue` and `my.*` match the queue `my.queue`. In this case, the broker first applies the configuration found under `my.*`, since a wildcard expression is less specific than a literal. Next, the broker overlays the configuration of the `my.queue` `<address-setting>`, which will overwrite any configuration shared with `my.*`. Given the configuration below, the queue `my.queue` would have `max-delivery-attempts` set to `3` and `last-value-queue` set to `false`.

```
<acceptor name="artemis">tcp://127.0.0.1:61616?
protocols=CORE,AMQP,OPENWIRE;supportAdvisory=false;suppressInternalManagementObjects=false</acceptor>

<address-setting match="my.*">
  <max-delivery-attempts>3</max-delivery-attempts>
  <last-value-queue>true</last-value-queue>
</address-setting>

<address-setting match="my.queue">
  <last-value-queue>false</last-value-queue>
</address-setting>
```

The examples in the table below illustrate how wildcards are used to match a set of addresses.

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>The default <code>&lt;address-setting&gt;</code> used in <code>broker.xml</code>. Matches every address.</td>
</tr>
<tr>
<td></td>
<td>You can continue to apply this catch-all, or you can add a new <code>&lt;address-setting&gt;</code> for each address or group of addresses as the need arises.</td>
</tr>
</tbody>
</table>
### Configuring Wildcard Syntax

You can customize the syntax used for wildcard addresses by adding configuration to `broker.xml`.

**Procedure**

1. Edit `broker.xml` by adding a `<wildcard-addresses>` section to the configuration, as in the example below.

```xml
<configuration>
  <core>...
  </core>
  <wildcard-addresses>
    <enabled>true</enabled>
    <delimiter>,</delimiter>
    <any-words>@</any-words>
    <single-word>$</single-word>
  </wildcard-addresses>
  ...
</configuration>
```

1. Add `wildcard-addresses` beneath the `core` configuration element.
2. Set `enabled` to `true` to tell the broker to use your custom settings.
3. Provide a custom character to use as the `delimiter` instead of the default, which is `,`.
4. The character provided as the value for `any-words` is used to mean 'match any sequence of zero or more words' and will replace the default `#`. Use this character at the end of your expression.
5. The character provided as the value for `single-word` is used to mean 'match a single word' and will replace the default `*`. Use this character anywhere within your expression.

### 4.16. Creating and Deleting Queues and Addresses Automatically

You can configure AMQ Broker to automatically create addresses and queues, and to delete them after they are no longer in use. This saves you from having to pre-configure each address before a client can connect to it.
Automatic creation and deletion of queues and addresses is configured on a per address-setting basis. The configuration is applied to any address or queue that is a match for the address-setting. For more information about how to use wildcard syntax to match addresses and queues to an address-setting see Configuring Address Settings.

**IMPORTANT**

Disabling the automatic creation of queues and addresses can cause problems and is not recommended. AMQ Broker must be able to auto-create addresses and queues by using the activemq.# pattern. For an example see the example address setting.

The following table lists the configuration elements available when configuring an address-setting to automatically create and delete its queues and addresses.

<table>
<thead>
<tr>
<th>If you want the address-setting to...</th>
<th>Add this configuration...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create addresses when a client sends a message to or attempts to consume a message from a queue mapped to an address that does not exist.</td>
<td>auto-create-addresses</td>
</tr>
<tr>
<td>Create a queue when a client sends a message to or attempts to consume a message from a queue.</td>
<td>auto-create-queues</td>
</tr>
<tr>
<td>Delete an automatically created address when it no longer has any queues.</td>
<td>auto-delete-addresses</td>
</tr>
<tr>
<td>Delete an automatically created queue when the queue has 0 consumers and 0 messages.</td>
<td>auto-delete-queues</td>
</tr>
<tr>
<td>Use a specific routing type if the client does not specify one.</td>
<td>default-address-routing-type</td>
</tr>
</tbody>
</table>

**Procedure**

Edit the `BROKER_INSTANCE_DIR/etc/broker.xml` file and configure an address-setting for automatic creation and deletion. The following example uses all of the configuration elements mentioned in the previous table.

```xml
<configuration ...>
  <core ...>
    ...
    <address-settings>
      <address-setting match="activemq.#"> 1
        <auto-create-addresses>true</auto-create-addresses> 2
        <auto-delete-addresses>true</auto-delete-addresses> 3
        <auto-create-queues>true</auto-create-queues> 4
        <auto-delete-queues>true</auto-delete-queues> 5
        <default-address-routing-type>ANYCAST</default-address-routing-type> 6
      </address-setting>
    </address-settings>
    ...
  </core>
</configuration>
```
The configuration included in this address-setting is applied to any address or queue that matches the wildcard activemq.#. For more information on using wildcard syntax see AMQ Broker Wildcard Syntax.

The broker creates an address that does not exist when a client requests it.

An automatically created address is deleted when it no longer has any queues associated with it.

The broker creates a queue that does not exist when a client requests it.

An automatically created queue is deleted when it no longer has any consumers or messages.

If the client does not specify a routing type when connecting, the broker uses ANYCAST when delivering messages to an address. The default value is MULTICAST. See the introduction of this chapter for more information about routing types.
CHAPTER 5. USERS AND ROLES

The broker supports a flexible role-based security model for applying security to queues based on their respective addresses. It is important to understand that queues are bound to addresses either one-to-one (for point-to-point style messaging) or many-to-one (for publish-subscribe style messaging). When a message is sent to an address the server looks up the set of queues that are bound to that address and routes the message to that set of queues.

In the default configuration (using PropertiesLoginModule), users and their assigned roles are defined in three configuration files:

- login.config
- artemis-users.properties
- artemis-roles.properties

Each of these files is discussed in more detail in the following sections.

The command-line interface allows users and roles to be added to these files via an interactive process.

NOTE

The artemis-users.properties file can contain hashed passwords for security.

5.1. ENABLING GUEST ACCESS

A user who does not have login credentials, or whose credentials fail validation, can be granted limited access to the broker using a guest account.

A broker instance can be created with guest access enabled using the command-line switch; --allow-anonymous (the converse of which is --require-login).

The guest account is configured in the login.config file.

Procedure

1. In the login.config file, define a name and role for the guest account as follows:

```activemq {
   org.apache.activemq.artemis.spi.core.security.jaas.GuestLoginModule required
   org.apache.activemq.jaas.guest.user="guest" 1
   org.apache.activemq.jaas.guest.role="guest"; 2
};
```

1. Define the username assigned to anonymous users.
2. Define the role assigned to anonymous users.

The guest login module allows users without credentials (and, depending on how it is configured, possibly also users with invalid credentials) to access the broker. It is implemented by org.apache.activemq.artemis.spi.core.security.jaas.GuestLoginModule.
It is common for the guest login module to be used in conjunction with another login module, such as a properties login module. Read more about that use-case in the Section 6.2.5, "Using Multiple Login Modules" section.

### 5.2. ADDING USERS

When basic username and password validation is required, use the Properties login module to define it. This login module checks the user’s credentials against a set of local property files.

Users and their corresponding passwords are listed in the `BROKER_INSTANCE_DIR/etc/artemis-users.properties` file. The available roles and the users who are assigned those roles are defined in the `BROKER_INSTANCE_DIR/etc/artemis-roles.properties` file.

Both of these files are referenced in the `BROKER_INSTANCE_DIR/etc/login.config` file.

See the documentation from your Java vendor for more information on JAAS. For example, Oracle has a tutorial on configuring `login.config`.

#### Example 5.1. `login.config`

```java
activemq {
    org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule required
        org.apache.activemq.jaas.properties.user="artemis-users.properties";
        org.apache.activemq.jaas.properties.role="artemis-roles.properties";
};
```

1. An alias for a configuration. In this section the alias used is `activemq`. Substitute another in your environment.

2. The implementation class

3. A flag which indicates whether the success of the `LoginModule` is `required`, `requisite`, `sufficient`, or `optional`.

4. A list of configuration options specific to the login module implementation.

Below is an explanation for each of the success states listed in the previous example:

**Required**

The LoginModule is required to succeed and authentication continues to proceed down the LoginModule list regardless of success or failure.

**Requisite**

The LoginModule is required to succeed. A failure immediately returns control to the application and authentication does not proceed down the LoginModule list.

**Sufficient**

The LoginModule is not required to succeed. If it is successful, control returns to the application and authentication does not proceed further. If it fails, the authentication attempt proceeds down the LoginModule list.

**Optional**
The LoginModule is not required to succeed. Authentication continues down the **LoginModules** list regardless of success or failure.

More information on these flags and the authentication process is available in the Oracle documentation.

**Example 5.2. artemis-users.properties**

```
user1=secret
user2=swordfish
user3=myPassword
```

1. *User1* has a password of *secret*.
2. *User2* has a password of *swordfish*.
3. *User3* has a password of *myPassword*.

**Example 5.3. artemis-roles.properties**

```
admin=user1,user2
developer=user3
```

1. *User1* and *user2* belong to the *admin* role.
2. *User3* belongs to the *developer* role.

**NOTE**

If necessary, add your security domain alias (in this instance, *activemq*) to the **bootstrap.xml** file as shown below:

```
<jaas-security domain="activemq"/>
```

### 5.3. SETTING PERMISSIONS

Permissions are defined against the queues based on their address via the `<security-setting>` element in **broker.xml**. Multiple instances of `<security-setting>` can be defined in `<security-settings>`. An exact match on the address can be used or a wildcard match can be used using the wildcard characters `#` and `*`.

Different permissions can be given to the set of queues which match the address. Those permissions are:

**Table 5.1. Permissions**

<table>
<thead>
<tr>
<th>To allow users to...</th>
<th>Use this parameter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create addresses</td>
<td><code>createAddress</code></td>
</tr>
<tr>
<td>To allow users to...</td>
<td>Use this parameter...</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Delete addresses</td>
<td>deleteAddress</td>
</tr>
<tr>
<td>Create a durable queue under matching addresses</td>
<td>createDurableQueue</td>
</tr>
<tr>
<td>Delete a durable queue under matching addresses</td>
<td>deleteDurableQueue</td>
</tr>
<tr>
<td>Create a non-durable queue under matching addresses</td>
<td>createNonDurableQueue</td>
</tr>
<tr>
<td>Delete a non-durable queue under matching addresses</td>
<td>deleteNonDurableQueue</td>
</tr>
<tr>
<td>Send a message to matching addresses</td>
<td>send</td>
</tr>
<tr>
<td>Consume a message from a queue bound to matching addresses</td>
<td>consume</td>
</tr>
<tr>
<td>Invoke management operations by sending management messages to the management address</td>
<td>manage</td>
</tr>
<tr>
<td>Browse a queue bound to the matching address</td>
<td>browse</td>
</tr>
</tbody>
</table>

For each permission, a list of roles who are granted that permission is specified. If the user has any of those roles, they are granted that permission for that set of addresses.

5.3.1. Configuring Message Production for a Single Address

To define sending permissions for a single address, a configuration similar to the example shown below is used:

```xml
<security-settings>
  <security-setting match="queue1">
    <permission type="send" roles="producer"/>
  </security-setting>
</security-settings>
```

1. Messages sent to this queue get the nominated permissions.
2. The permissions applied to messages in the specified queue.

In the above example, members of the producer role have send permissions on queue1.

5.3.2. Configuring Message Consumption for a Single Address

To define consuming permissions for a single address, a configuration similar to the example shown below is used:
5.3.3. Configuring Complete Access on All Addresses

To allow complete access to addresses and queues, a configuration similar to the example shown below is used.

```
<security-settings>
  <security-setting match="#">
    <permission type="createDurableQueue" roles="guest"/>
    <permission type="deleteDurableQueue" roles="guest"/>
    <permission type="createNonDurableQueue" roles="guest"/>
    <permission type="deleteNonDurableQueue" roles="guest"/>
    <permission type="createAddress" roles="guest"/>
    <permission type="deleteAddress" roles="guest"/>
    <permission type="send" roles="guest"/>
    <permission type="browse" roles="guest"/>
    <permission type="consume" roles="guest"/>
    <permission type="manage" roles="guest"/>
  </security-setting>
</security-settings>
```

1. A wildcard setting to apply to all queues.

In the above configuration, all permissions are granted to members of the guest role on all queues. This can be useful in a development scenario where anonymous authentication was configured to assign the guest role to every user.

For information about more complex use cases see Configuring Multiple Permissions for Addresses.

5.3.4. Configuring a Queue with a User

The queue is assigned the username of the connecting client when it is auto-created. This is exposed as metadata on the queue. It is exposed by JMX and in the console.

You can configure a user on a pre-defined queue in `broker.xml`.

To define a user for a queue, use a configuration similar to the example shown below:

```
<address name="ExempleQueue">
  <anycast>
```

1. Messages sent to this queue get the nominated permissions.

2. The permissions applied to messages in the specified queue.
NOTE
Configuring a user on a queue does not change any of the security semantics for that queue, it is only used for metadata on that queue.

5.4. SETTING ROLE BASED ACCESS CONTROL

Role-based access control (RBAC) is used to restrict access to the attributes and methods of MBeans. RBAC enables administrators to grant the correct level of access to all users like web console, management interface, core messages, and so on based on their role. RBAC is configured using the authorization element in the `BROKER_INSTANCE_DIR/etc/management.xml` configuration file. Within the authorization element, you can configure `Whitelist`, `default-access`, and `role-access` sub-elements.

Prerequisites
You must first set up roles and add users to configure RBAC.

5.4.1. Configuring Whitelist Element for Bypassing the Authentication

A whitelist is a set of pre-approved domains or MBeans that do not require user authentication. You can provide a whitelist of domains or list of MBeans or both that must bypass the authentication. For example, you can use `whitelist` element for any MBeans that are needed by the AMQ Console to run.

Procedure

1. Open the broker `BROKER_INSTANCE_DIR/etc/management.xml` configuration file.

2. Search for the `whitelist` element and edit the configuration:

   ```xml
   <whitelist>
     <entry domain="hawtio"/>
   </whitelist>
   ```

   **1** MBean of this domain will bypass the authentication.

   In this example, any MBean with the domain `hawtio` will be allowed access without authentication. You can also use wildcard entries like `<entry domain="hawtio" key="type=*"/>` for the MBean properties to match.

3. Start or restart the broker by entering the following command:

   - On Linux: `BROKER_INSTANCE_DIR/bin/artemis run`
   - On Windows: `BROKER_INSTANCE_DIR/bin/artemis-service.exe start`

5.4.2. Configuring Authentication Based on Roles

The `role-access` method defines how roles are mapped to particular MBeans and their attributes and methods.
Procedure

1. Open the `BROKER_INSTANCE_DIR/etc/management.xml` configuration file.

2. Search for the `role-access` element and edit the configuration:

```xml
<role-access>
  <match domain="org.apache.activemq.artemis">
    <access method="list*" roles="view,update,amq"/>
    <access method="get*" roles="view,update,amq"/>
    <access method="is*" roles="view,update,amq"/>
    <access method="set*" roles="update,amq"/>
    <access method="*" roles="amq"/>
  </match>
</role-access>
```

1. A match will be applied to any MBean attribute that has the domain name `org.apache.activemq.apache`.

2. Specified roles can invoke the listed methods.

**IMPORTANT**

```plaintext
=== You must ensure that the order of the individual lines in the configuration is as per the template. Any change in the line indentation leads to changes in the semantics of the assigned privileges. For example, if you move the line `<access method="*" roles="amq,guest"/>` inside the `<role-access>` tag from last position to the first, it changes the semantics of applied privileges. If used as the first line, it means grant access to everything to these roles with the exception of following specific cases. If used as the last line, it means grant access to everything to these roles (default). ===
```

Here, the specific tasks like `list*`, `get*`, `set*`, `is*` and `*` are specified using the access method. The invoked method is matched against the methods listed in the configuration. The user is assigned the roles given for the best matching method. For example, if you try the invoke a method called `listMessages` on an MBean with the `org.apache.activemq.artemis` domain, then it would match the access with the method of `list`. You can also explicitly configure this by using the full method name like the following:

```xml
<access method="listMessages" roles="view,update,amq"/>
```

3. Start or restart the broker by entering the following command:

- On Linux: `BROKER_INSTANCE_DIR/bin/artemis run`
- On Windows: `BROKER_INSTANCE_DIR/bin/artemis-service.exe start`

You can also match specific MBeans within a domain by adding a `key` attribute that matches an MBean property. For example,

```xml
<match domain="org.apache.activemq.artemis" key="subcomponent=queues">
  <access method="list*" roles="view,update,amq"/>
  <access method="get*" roles="view,update,amq"/>
  <access method="is*" roles="view,update,amq"/>
</match>
```
Access to MBean attributes are converted to method calls, so these are controlled using the `list*`, `set*`, `get*`, and `is*` syntax. The * (wildcard) syntax is used as a catch-all for every other method that is not listed in the configuration.

**NOTE**

The `default-access` element is mainly the catch-all for every method call that is not handled using the `role-access` configuration. The `default-access` and `role-access` have the same `match` element semantics.
CHAPTER 6. SECURITY

This chapter covers the various security options available to administrators, and how they are configured. Administrators can use the information provided in this chapter to tailor the functions of the AMQ Broker security subsystems to their needs.

6.1. ACCESSING THE AMQ CONSOLE

Starting with AMQ Broker 7.1.0, you can access the AMQ Console only from the local host by default. You must modify the configuration in BROKER_INSTANCE_DIR/etc/jolokia-access.xml to enable remote access. For more information, see Securing AMQ Console and AMQ Broker Connections.

6.2. SECURING NETWORK CONNECTIONS

There are two basic use cases for transport layer security (TLS):

- Server-side (or one-way); where only the server presents a certificate. This is the most common use case.
- Client-side (or two-way); where both the server and the client present certificates. This is sometimes called mutual authentication.

6.2.1. Configuring Server-Side Certificates

One-way TLS is configured in the URL of the relevant acceptor in broker.xml. Here is a very basic acceptor configuration which does not use TLS:

```xml
<acceptor name="artemis">tcp://0.0.0.0:61616</acceptor>
```

Here is that same acceptor configured to use one-way TLS:

```xml
<acceptor name="artemis">tcp://0.0.0.0:61616?sslEnabled=true;keyStorePath=../etc/broker.keystore;keyStorePassword=1234!</acceptor>
```

This acceptor uses three additional parameters - sslEnabled, keyStorePath, and keyStorePassword. These, at least, are required to enable one-way TLS.

6.2.2. Configuring Client-Side Certificates

Two-way TLS uses the same sslEnabled, keyStorePath, and keyStorePassword properties as one-way TLS, but it adds needClientAuth to tell the client it should present a certificate of its own. For example:

```xml
<acceptor name="artemis">tcp://0.0.0.0:61616?sslEnabled=true;keyStorePath=../etc/broker.keystore;keyStorePassword=1234!;needClientAuth=true</acceptor>
```

This configuration assumes that the client’s certificate is signed by a trusted provider. If the client’s certificate is not signed by a trusted provider (it is self-signed, for example) then the server needs to import the client’s certificate into a trust-store and configure the acceptor with trustStorePath and trustStorePassword. For example:
NOTE

Client-side Considerations

AMQ Broker supports multiple protocols, and each protocol and platform has different ways to specify TLS parameters. However, in the case of a client using the Core protocol (a bridge) the TLS parameters are configured on the connector URL much like on the broker’s acceptor.

TLS Configuration Details
Below are configuration details to be aware of:

<table>
<thead>
<tr>
<th>Option</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslEnabled</td>
<td>Must be <strong>true</strong> to enable TLS. Default is <strong>false</strong>.</td>
</tr>
</tbody>
</table>
| keyStorePath     | **When used on an acceptor:** This is the path to the TLS key store on the server which holds the server’s certificates (whether self-signed or signed by an authority).  

**When used on a connector:** This is the path to the client-side TLS key store which holds the client certificates. This is only relevant for a connector if you are using two-way TLS (that is, mutual authentication). Although this value is configured on the server, it is downloaded and used by the client. If the client needs to use a different path from that set on the server then it can override the server-side setting by either using the customary `javax.net.ssl.keyStore` system property or the AMQ-specific `org.apache.activemq.ssl.keyStore` system property. The AMQ-specific system property is useful if another component on client is already making use of the standard, Java system property. |

```xml
<acceptor name="artemis">tcp://0.0.0.0:61616?
sslEnabled=true;keyStorePath=../etc/broker.keystore;keyStorePassword=1234!;needClientAuth=true;trustStorePath=../etc/client.truststore;trustStorePassword=5678!)</acceptor>
```
<table>
<thead>
<tr>
<th>Option</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyStorePassword</td>
<td><strong>When used on an acceptor:</strong> This is the password for the server-side KeyStore. <strong>When used on a connector:</strong> This is the password for the client-side KeyStore. This is only relevant for a connector if you are using two-way TLS (that is, mutual authentication). Although this value can be configured on the server, it is downloaded and used by the client. If the client needs to use a different password from that set on the server then it can override the server-side setting by either using the customary <code>javax.net.ssl.keyStorePassword</code> system property or the AMQ-specific <code>org.apache.activemq.ssl.keyStorePassword</code> system property. The AMQ-specific system property is useful if another component on client is already making use of the standard, Java system property.</td>
</tr>
<tr>
<td>trustStorePath</td>
<td><strong>When used on an acceptor:</strong> This is the path to the server-side TLS key store that holds the keys of all the clients that the server trusts. This is only relevant for an acceptor if you are using two-way TLS (mutual authentication). <strong>When used on a connector:</strong> This is the path to the client-side TLS key store which holds the public keys of all the servers that the client trusts. Although this value can be configured on the server, it is downloaded and used by the client. If the client needs to use a different path from that set on the server then it can override the server-side setting by either using the customary <code>javax.net.ssl.trustStore</code> system property or the AMQ-specific <code>org.apache.activemq.ssl.trustStore</code> system property. The AMQ-specific system property is useful if another component on client is already making use of the standard, Java system property.</td>
</tr>
</tbody>
</table>
### Option | Note
--- | ---
**trustStorePassword**<br>When used on an **acceptor**: This is the password for the server-side trust store. This is only relevant for an **acceptor** if you are using two-way TLS (that is, mutual authentication).<br><br>**When used on a connector**: This is the password for the client-side TrustStore. Although this value can be configured on the server, it is downloaded and used by the client. If the client needs to use a different password from that set on the server then it can override the server-side setting by either using the customary **javax.net.ssl.trustStorePassword** system property or the AMQ-specific **org.apache.activemq.ssl.trustStorePassword** system property. The AMQ-specific system property is useful if another component on client is already making use of the standard, Java system property.<br><br>**enabledCipherSuites**<br>Whether used on an **acceptor** or **connector** this is a comma-separated list of cipher suites used for TLS communication. The default value is **null** which means the JVM's default is used.<br><br>**enabledProtocols**<br>Whether used on an **acceptor** or **connector** this is a comma-separated list of protocols used for TLS communication. The default value is **null** which means the JVM's default is used.<br><br>**needClientAuth**<br>This property is only for an **acceptor**. It indicates to a client connecting to this acceptor that two-way TLS is required. Valid values are **true** or **false**. Default is **false**.

### 6.2.3. Adding Certificate-based Authentication

The JAAS certificate authentication login module requires TLS to be in use and clients must be configured with their own certificates. In this scenario, authentication is actually performed during the TLS handshake, not directly by the JAAS certificate authentication plug-in.

The role of the plug-in is as follows:

- To further constrain the set of acceptable users, because only the user Distinguished Names (DNs) explicitly listed in the relevant properties file are eligible to be authenticated.
- To associate a list of groups with the received user identity, facilitating integration with authorization.
- To require the presence of an incoming certificate (by default, the TLS layer is configured to treat the presence of a client certificate as optional).
The JAAS certificate login module stores a collection of certificate DNs in a pair of flat files. The files associate a username and a list of group IDs with each Distinguished Name.

The certificate login module is implemented by the


Prerequisites

- A valid artemis-users.properties file.
- A valid artemis-roles.properties file.
- The Subject DNs from the user certificate(s)

Procedure

1. Obtain the Subject DNs from user certificates
   a. Export the certificate from the KeyStore file into a temporary file. Substitute your required values into the following command:

   ```
   keytool -export -file __FILENAME__ -alias broker-localhost -keystore broker.ks -storepass __PASSWORD__
   ```

   b. Print the contents of the exported certificate:

   ```
   keytool -printcert -file __FILENAME__
   ```

   The output is similar to that shown below:

   Owner: CN=localhost, OU=broker, O=Unknown, L=Unknown, ST=Unknown, C=Unknown

   Issuer: CN=localhost, OU=broker, O=Unknown, L=Unknown, ST=Unknown, C=Unknown

   Serial number: 4537c82e


   Certificate fingerprints:


   The subject DN. The format used to enter the subject DN depends on your platform.

   The string above could also be represented as:

   ```
   Owner: 'CN=localhost, OU=broker, O=Unknown, L=Unknown, ST=Unknown, C=Unknown'
   ```

2. Configuring certificate-based authentication
   a. Open the login.config file and reference the user and roles properties files.

   b. Open the files declared in the previous step and supply the required information:
Users and their corresponding DNs should be listed in the `artemis-users.properties` file. The available roles and the users who hold those roles are defined in the `artemis-roles.properties` file.

Examples of the syntax of these files is shown below.

c. Ensure your security domain alias (in this instance, `activemq`) is referenced in `bootstrap.xml` as shown below:

```xml
<jaas-security domain="activemq"/>
```

**Example Configuration**

The following example shows how to configure certificate login module in the `login.config` file:

**Example 6.1. login.config**

```plaintext
activemq {
    org.apache.activemq.artemis.spi.core.security.jaas.TextFileCertificateLoginModule 1
    debug=true 2
    org.apache.activemq.jaas.textfiledn.user="artemis-users.properties" 3
    org.apache.activemq.jaas.textfiledn.role="artemis-roles.properties"; 4
};
```

1. Configure the JAAS realm. This example uses a single
   `org.apache.activemq.artemis.spi.core.security.jaas.TextFileCertificateLoginModule`
2. Toggle debugging on (`true`) or off (`false`). Default is `false`.
3. Define the file used to store user data (relative to the directory containing the `login.config` file).
4. Define the file used to store role data (relative to the directory containing the `login.config` file).

The `artemis-users.properties` file consists of a list of properties with the `user=StringifiedSubjectDN` (where the string encoding is specified by RFC 2253):

**Example 6.2. artemis-users.properties**

```plaintext
system=CN=system,O=Progress,C=US 1
user=CN=humble user,O=Progress,C=US
guest=CN=anon,O=Progress,C=DE
```

1. The user named `system` is mapped to the `CN=system,O=Progress,C=US` subject DN.

The `artemis-roles.properties` file follows the pattern of `role=user` where `user` can be either a single user or a comma-separated list of users:

**Example 6.3. artemis-roles.properties**
6.2.4. Adding Certificate-based Authentication for AMQP Clients

Use the SASL EXTERNAL mechanism configuration parameter to configure your AMQP client for certificate-based authentication when connecting to a broker.

The broker authenticates the TSL/SSL certificate of your AMQP client in the same way that it authenticates any certificate:

- The broker reads the TSL/SSL certificate of the client to obtain an identity from the certificate’s subject.
- The certificate subject is mapped to a broker identity by the certificate login module. The broker then authorizes the mapped user based on their roles.

**Prerequisites**

Before you can configure your AMQP clients to use certificate-based authentication, you must complete the following tasks:

- Configure a server-side SSL/TLS certificate.
- Configure a client-side SSL/TLS certificate.
- Configure the broker to use certificate-based authentication.

**Procedure**

To enable your AMQP client to use certificate-based authentication, add configuration parameters to the URI that the client uses to connect to a broker.

1. Open the resource containing the URI for editing:

   ```
   amqps://localhost:5500
   ```

2. Add the parameter `sslEnabled=true` to enable TSL/SSL for the connection:

   ```
   amqps://localhost:5500?sslEnabled=true
   ```

3. Add parameters related to the TrustStore and KeyStore of the client to enable the exchange of TSL/SSL certificates with the broker:

   ```
   amqps://localhost:5500?
   sslEnabled=true&trustStorePath=TRUST_STORE_PATH&trustStorePassword=TRUST_STORE_PASSWORD&keyStorePath=KEY_STORE_PATH&keyStorePassword=KEY_STORE_PASSWORD
   ```

4. Add the parameter `saslMechanisms=EXTERNAL` to request that the broker authenticate the client by using the identity found in its TSL/SSL certificate:

   ```
   -
   ```
amqps://localhost:5500?
sslEnabled=true&trustStorePath=TRUST_STORE_PATH&trustStorePassword=TRUST_STORE_PASSWORD&keyStorePath=KEY_STORE_PATH&keyStorePassword=KEY_STORE_PASSWORD&saslMechanisms=EXTERNAL

Additional Resources

- For more information about certificate-based authentication in AMQ Broker, see Section 6.2.3, “Adding Certificate-based Authentication”.

- For more information about configuring your AMQP client, go to the Red Hat Customer Portal for product documentation specific to your client.

### 6.2.5. Using Multiple Login Modules

It is possible to combine login modules to accommodate more complex use cases. The most common reason to combine login modules is to support authentication for both anonymous users and users who submit credentials.

#### Prerequisites

The prerequisites for different authentication combinations differ based on the methods being implemented. Prerequisites for the most common multiple login scenario are:

- A valid `artemis-users.properties` file
- A valid `artemis-roles.properties` file
- A `login.config` file configured for anonymous access

#### Procedure

1. Edit the `login.config` file to add entries for the desired authentication modules.

2. Set the parameters in each module entry as required for your environment.

3. Ensure your security domain alias (in this instance, `activemq`) is referenced in `bootstrap.xml` as shown below:

   **Example 6.4. bootstrap.xml**

   ```xml
   <jaas-security domain="activemq"/>
   ```

#### Example Configuration

The following examples illustrate the cascading nature of multiple login configurations:

**Example 6.5. login.config**

```java
activemq {
    org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule sufficient 1
    debug=true
    org.apache.activemq.jaas.properties.user="artemis-users.properties"
    org.apache.activemq.jaas.properties.role="artemis-roles.properties";
```
Password authentications module is activated if the user supplies credentials

Guest authentication module is activated if the user supplies no credentials or the credentials supplied are incorrect.

The following example shows how to configure a JAAS login entry for the use case where only those users with no credentials are logged in as guests. Note that the order of the login modules is reversed and the flag attached to the properties login module is changed to requisite.

**Example 6.6. login.config**

```xml
activemq {
    org.apache.activemq.artemis.spi.core.security.jaas.GuestLoginModule sufficient debug=true credentialsInvalidate=true org.apache.activemq.jaas.guest.user="guest" org.apache.activemq.jaas.guest.role="guests";

    org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule requisite debug=true org.apache.activemq.jaas.properties.user="artemis-users.properties" org.apache.activemq.jaas.properties.role="artemis-roles.properties";
}
```

1. The guest authentication module is activated if no login credentials are supplied.
2. The credentialsInvalidate option must be set to true in the configuration of the guest login module.
3. The password login module is activated if credentials are supplied and the credentials must be valid.

### 6.2.6. Configure Multiple Security Settings for Address Groups and Sub-groups

Below is an example security block from a broker.xml file. The various configuration options based on this example are explained in this section.

```xml
<security-setting match="globalqueues.europe.#">
    <permission type="createDurableQueue" roles="admin"/>
    <permission type="deleteDurableQueue" roles="admin"/>
    <permission type="createNonDurableQueue" roles="admin, guest, europe-users"/>
    <permission type="deleteNonDurableQueue" roles="admin, guest, europe-users"/>
</security-setting>
```

1. The guest authentication module is activated if no login credentials are supplied.
2. The credentialsInvalidate option must be set to true in the configuration of the guest login module.
3. The password login module is activated if credentials are supplied and the credentials must be valid.
The '#' character signifies "any sequence of words". Words are delimited by the '.' character. For a full description of the wildcard syntax, see AMQ Broker Wildcard Syntax. The above security block applies to any address that starts with the string `globalqueues.europe`.

Only users who have the **admin** role can create or delete durable queues bound to an address that starts with the string `globalqueues.europe`.

Any users with the roles **admin**, **guest**, or **europe-users** can create or delete temporary queues bound to an address that starts with the string `globalqueues.europe`.

Any users with the roles **admin** or **europe-users** can send messages to these addresses or consume messages from queues bound to an address that starts with the string `globalqueues.europe`.

The mapping between a user and what roles they have is handled by the security manager. AMQ Broker ships with a user manager that reads user credentials from a file on disk, and can also plug into JAAS or JBoss Application Server security.

There can be multiple `security-setting` elements in each XML file, or none, depending on requirements. When the **broker.xml** file contains multiple security-setting elements that can apply to a set of addresses, the most specific match takes precedence.

Let us look at an example of that, here's another `security-setting` block:

```xml
<security-setting match="globalqueues.europe.orders.#">
  <permission type="send" roles="europe-users"/>
  <permission type="consume" roles="europe-users"/>
</security-setting>
```

In this `security-setting` block the match `globalqueues.europe.orders.#` is more specific than the previous match 'globalqueues.europe.\#'. So any addresses which match 'globalqueues.europe.orders.\#' will take their security settings only from the latter security-setting block.

Note that settings are not inherited from the former block. All the settings will be taken from the more specific matching block, so for the address `globalqueues.europe.orders.plastics` the only permissions that exist are **send** and **consume** for the role **europe-users**. The permissions `createDurableQueue`, `deleteDurableQueue`, `createNonDurableQueue`, `deleteNonDurableQueue` are not inherited from the other security-setting block.

By not inheriting permissions, you can effectively deny permissions in more specific security-setting blocks by simply not specifying them. Otherwise it would not be possible to deny permissions in sub-groups of addresses.

### 6.2.7. Setting Resource Limits

Sometimes it is helpful to set particular limits on what certain users can do beyond the normal security settings related to authorization and authentication. For example, one can limit how many connections a user can create or how many queues a user can create.
6.2.7.1. Configuring Connection and Queue Limits

Here is an example of the XML used to set resource limits:

```xml
<resource-limit-settings>
  <resource-limit-setting match="myUser">
    <max-connections>5</max-connections>
    <max-queues>3</max-queues>
  </resource-limit-setting>
</resource-limit-settings>
```

Unlike the `match` from `address-setting`, this `match` does not use any wildcard syntax. It is a simple 1:1 mapping of the limits to a user.

- **max-connections**: Defines how many connections the matched user can make to the broker. The default is `-1`, which means there is no limit.
- **max-queues**: Defines how many queues the matched user can create. The default is `-1`, which means there is no limit.

6.3. INTEGRATING WITH LDAP

6.3.1. Using LDAP for Authentication

The LDAP login module enables authentication and authorization by checking the incoming credentials against user data stored in a central X.500 directory server. It is implemented by `org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule`.

Procedure

1. Open the `BROKER_INSTANCE_DIR/etc/broker.xml` file and add the following lines:

   ```xml
   <security-settings>
     <security-setting match="#">
       <permission type="createDurableQueue" roles="user"/>
       <permission type="deleteDurableQueue" roles="user"/>
       <permission type="createNonDurableQueue" roles="user"/>
       <permission type="deleteNonDurableQueue" roles="user"/>
       <permission type="send" roles="user"/>
       <permission type="consume" roles="user"/>
     </security-setting>
   </security-settings>
   ```

2. Open the `BROKER_INSTANCE_DIR/etc/login.config` file.

3. Locate and edit the appropriate alias block with the appropriate parameters (see the examples included below).

4. Start or restart the broker (service or process).
NOTE

Apache DS uses the **OID** portion of DN path; however, Microsoft AD does not, and instead uses the **CN** portion.

For example; The DN path `oid=testuser,dc=example,dc=com` would be used in Apache DS, while `cn=testuser,dc=example,dc=com` would be used in Microsoft AD.

Example 6.7. Example Apache DS `login.config` configuration

```java
activemq {
    org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule required
debug=true
    initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
    connectionURL="ldap://localhost:10389"
    connectionUsername="uid=admin,ou=system"
    connectionPassword=secret
    connectionProtocol=s
    authentication=simple
    userBase="dc=example,dc=com"
    userSearchMatching="(uid={0})"
    userSearchSubtree=true
    userRoleName=
    roleBase="dc=example,dc=com"
    roleName=cn
    roleSearchMatching="(member={0})"
    roleSearchSubtree=true
};
```

Example 6.8. Example Microsoft Active Directory `login.config` Configuration

```java
activemq {
    org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule required
debug=true
    initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
    connectionURL="LDAP://localhost:389"
    connectionUsername="CN=Administrator,CN=Users,DC=example,DC=com"
    connectionPassword=redhat.123
    connectionProtocol=s
    authentication=simple
    userBase="dc=example,dc=com"
    userSearchMatching="(CN={0})"
    userSearchSubtree=true
    userRoleName=
    roleBase="dc=example,dc=com"
    roleName=cn
    roleSearchMatching="(member={0})"
    roleSearchSubtree=true
};
```
1. Toggle debugging on (true) or off (false). Default is false.

2. The initialContextFactory parameter must always be set to com.sun.jndi.ldap.LdapCtxFactory

3. Specify the location of the directory server using an ldap URL, ldap://Host:Port. One can optionally qualify this URL, by adding a forward slash, /, followed by the DN of a particular node in the directory tree. The default port of Apache DS is 10389 while for Microsoft AD the default is 389.

4. The DN of the user that opens the connection to the directory server. For example, uid=admin,ou=system. Directory servers generally require clients to present username/password credentials in order to open a connection.

5. The password that matches the DN from connectionUsername. In the directory server, in the DIT, the password is normally stored as a userPassword attribute in the corresponding directory entry.

6. Any value is supported but is effectively unused. This option must be set explicitly because it has no default value.

7. Specify the authentication method used when binding to the LDAP server. This parameter can be set to either simple (which requires a username and password) or none (which allows anonymous access).

8. Select a particular subtree of the DIT to search for user entries. The subtree is specified by a DN, which specifies the base node of the subtree. For example, by setting this option to ou=User,ou=ActiveMQ,ou=system, the search for user entries is restricted to the subtree beneath the ou=User,ou=ActiveMQ,ou=system node.

9. Specify an LDAP search filter, which is applied to the subtree selected by userBase. See the Search Matching section below for more information.

10. Specify the search depth for user entries, relative to the node specified by userBase. This option is a boolean. A setting of false indicates it tries to match one of the child entries of the userBase node (maps to javax.naming.directory.SearchControls.ONELEVEL_SCOPE), while true indicates it tries to match any entry belonging to the subtree of the userBase node (maps to javax.naming.directory.SearchControls.SUBTREE_SCOPE).

11. Specify the name of the multi-valued attribute of the user entry that contains a list of role names for the user (where the role names are interpreted as group names by the broker’s authorization plug-in). If this option is omitted, no role names are extracted from the user entry.

12. If role data is stored directly in the directory server, one can use a combination of role options (roleBase, roleSearchMatching, roleSearchSubtree, and roleName) as an alternative to (or in addition to) specifying the userRoleName option. This option selects a particular subtree of the DIT to search for role/group entries. The subtree is specified by a DN, which specifies the base node of the subtree. For example, by setting this option to ou=Group,ou=ActiveMQ,ou=system, the search for role/group entries is restricted to the subtree beneath the ou=Group,ou=ActiveMQ,ou=system node.

13. Specify the attribute type of the role entry that contains the name of the role/group (such as C, O, OU, etc.). If this option is omitted the role search feature is effectively disabled.

14. Specify an LDAP search filter, which is applied to the subtree selected by roleBase. See the Search Matching section below for more information.

15. Specify the search depth for role entries, relative to the node specified by roleBase. If set to false (which is the default) the search tries to match one of the child entries of the roleBase node (maps to javax.naming.directory.SearchControls.ONELEVEL_SCOPE). If true it tries to match any
entry belonging to the subtree of the roleBase node (maps to javax.naming.directory.SearchControls.SUBTREE_SCOPE).

Search Matching

userSearchMatching

Before passing to the LDAP search operation, the string value provided in this configuration parameter is subjected to string substitution, as implemented by the java.text.MessageFormat class.

This means that the special string, {0}, is substituted by the username, as extracted from the incoming client credentials. After substitution, the string is interpreted as an LDAP search filter (the syntax is defined by the IETF standard RFC 2254).

For example, if this option is set to (uid={0}) and the received username is jdoe, the search filter becomes (uid=jdoe) after string substitution.

If the resulting search filter is applied to the subtree selected by the user base, ou=User,ou=ActiveMQ,ou=system, it would match the entry, uid=jdoe,ou=User,ou=ActiveMQ,ou=system.

A short introduction to the search filter syntax is available from Oracle’s JNDI tutorial.

roleSearchMatching

This works in a similar manner to the userSearchMatching option, except that it supports two substitution strings.

The substitution string {0} substitutes the full DN of the matched user entry (that is, the result of the user search). For example, for the user, jdoe, the substituted string could be uid=jdoe,ou=User,ou=ActiveMQ,ou=system.

The substitution string {1} substitutes the received username. For example, jdoe.

If this option is set to (member=uid={1}) and the received username is jdoe, the search filter becomes (member=uid=jdoe) after string substitution (assuming ApacheDS search filter syntax).

If the resulting search filter is applied to the subtree selected by the role base, ou=Group,ou=ActiveMQ,ou=system, it matches all role entries that have a member attribute equal to uid=jdoe (the value of a member attribute is a DN).

This option must always be set, even if role searching is disabled, because it has no default value. If OpenLDAP is used, the syntax of the search filter is (member:=uid=jdoe).

6.3.2. Configure LDAP Authorization

The LegacyLDAPSecuritySettingPlugin security-setting-plugin will read the security information that was previously handled by LDAPAuthorizationMap and the cachedLDAPAuthorizationMap in Apache A-MQ 6 and turn it into corresponding security settings where possible.

The security implementations of the two brokers do not match perfectly so some translation must occur to achieve near equivalent functionality.

Here is an example of the plugin’s configuration:

```
<security-setting-plugin class-
name="org.apache.activemq.artemis.core.server.impl.LegacyLDAPSecuritySettingPlugin">  
<setting name="initialContextFactory" value="com.sun.jndi.ldap.LdapCtxFactory"/>
<setting name="connectionURL" value="ldap://localhost:1024"/>
<setting name="connectionUsername" value="uid=admin,ou=system"/>
<setting name="connectionPassword" value="secret"/>
<setting name="connectionProtocol" value="s"/>
<setting name="authentication" value="simple"/>
</security-setting-plugin>

class-name. The implementation is

initialContextFactory. The initial context factory used to connect to LDAP. It must always be set
to com.sun.jndi.ldap.LdapCtxFactory (that is, the default value).

connectionURL. Specifies the location of the directory server using an LDAP URL,
ldap://Host:Port. You can optionally qualify this URL, by adding a forward slash, /, followed by the
DN of a particular node in the directory tree. For example, ldap://ldapservr:10389/ou=system.
The default is ldap://localhost:1024.

connectionUsername. The DN of the user that opens the connection to the directory server. For
example, uid=admin,ou=system. Directory servers generally require clients to present
username/password credentials in order to open a connection.

connectionPassword. The password that matches the DN from connectionUsername. In the
directory server, in the DIT, the password is normally stored as a userPassword attribute in the
corresponding directory entry.

connectionProtocol - any value is supported but is effectively unused. In the future, this option
may allow one to select the Secure Socket Layer (SSL) for the connection to the directory server.
This option must be set explicitly because it has no default value.

authentication. Specifies the authentication method used when binding to the LDAP server. Can
take either of the values, simple (username and password, the default value) or none
(anonymous). Note: Simple Authentication and Security Layer (SASL) authentication is currently
not supported.

Other possible settings not shown in the example above are:

destinationBase

Specifies the DN of the node whose children provide the permissions for all destinations. In this case
the DN is a literal value (that is, no string substitution is performed on the property value). For
example, a typical value of this property is ou=destinations,o=ActiveMQ,ou=system (that is, the
default value).

filter

Specifies an LDAP search filter, which is used when looking up the permissions for any kind of
destination. The search filter attempts to match one of the children or descendants of the queue or
topic node. The default value is (cn=*).

roleAttribute

Specifies an attribute of the node matched by filter whose value is the DN of a role. Default value is
uniqueMember.

adminPermissionValue
Specifies a value that matches the admin permission. The default value is admin.

readPermissionValue
Specifies a value that matches the read permission. The default value is read.

writePermissionValue
Specifies a value that matches the write permission. The default value is write.

enableListener
Whether or not to enable a listener that will automatically receive updates made in the LDAP server and update the broker’s authorization configuration in real-time. The default value is true.

The name of the queue or topic defined in LDAP will serve as the "match" for the security-setting, the permission value will be mapped from the A-MQ 6 type to the AMQ 7 type, and the role will be mapped as-is. Since the name of the queue or topic coming from LDAP will serve as the "match" for the security-setting the security-setting may not be applied as expected to JMS destinations since AMQ 7 always prefixes JMS destinations with "jms.queue." or "jms.topic." as necessary.

A-MQ 6 only has three permission types - read, write, and admin. These permission types are described on the ActiveMQ website; http://activemq.apache.org/security.html.

However, as described previously, AMQ 7 has 10 permission types:

- createAddress
- deleteAddress
- createDurableQueue
- deleteDurableQueue
- createNonDurableQueue
- deleteNonDurableQueue
- send
- consume
- manage
- browse

The list below shows how the old types are mapped to the new types:

- read - consume, browse
- write - send
- admin - createDurableQueue, deleteDurableQueue, createNonDurableQueue, deleteNonDurableQueue, createAddress, deleteAddress

As mentioned, there are a few places where a translation was performed to achieve some equivalence:

- This mapping does not include the AMQ 7 manage permission type since there is no type analogous for that in A-MQ 6.
- The admin permission in A-MQ 6 relates to whether or not the broker will auto-create a
destination if it does not exist and the user sends a message to it. AMQ 7 automatically allows
the automatic creation of a destination if the user has permission to send message to it.
Therefore, the plugin will map the admin permission to the four aforementioned permissions in
AMQ 7.

6.3.3. Encrypting the Password in the login.config File

Because organizations frequently securely store data with LDAP, the login.config file can contain the
configuration required for the broker to communicate with the organization’s LDAP server. This
configuration file usually includes a password to log in to the LDAP server, so this password needs to be
masked.

Prerequisites

- Ensure that you have modified the login-config file to add the required properties as described
  in Section 6.3.2, “Configure LDAP Authorization”.

Procedure

The following procedure explains how to mask the value of the connectionPassword found in the
BROKER_INSTANCE_DIR/etc/login.config file.

1. From a command prompt, use the mask utility to encrypt the password:

   $ BROKER_INSTANCE_DIR/bin/artemis mask PASSWORD

   The encrypted password is displayed on the screen:

   result: 3a34fd21b82bf2a822fa49a8d8fa115d

2. Open the BROKER_INSTANCE_DIR/etc/login.config file and locate the
   connectionPassword:

   connectionPassword = PASSWORD

3. Replace the plain text password with the encrypted value that you created in Step 1:

   connectionPassword = 3a34fd21b82bf2a822fa49a8d8fa115d

4. Wrap the encrypted value with the identifier "ENC()":

   connectionPassword = "ENC(3a34fd21b82bf2a822fa49a8d8fa115d)"

The login.config file now contains a masked password. Because the password is wrapped with the
"ENC()" identifier, AMQ Broker decrypts it before it is used.

Additional Resources

For more information about the configuration files included with AMQ Broker, see AMQ Broker
configuration files and locations.

6.4. INTEGRATING WITH KERBEROS

When sending and receiving messages with the AMQP protocol, clients can send Kerberos security
credentials that AMQ Broker authenticates by using the GSSAPI mechanism from the Simple Authentication and Security Layer (SASL) framework. Kerberos credentials can also be used for authorization by mapping an authenticated user to an assigned role configured in an LDAP directory or text-based properties file.

You can use SASL in tandem with Transport Layer Sockets (TLS) to secure your messaging applications. SASL provides user authentication, and TLS provides data integrity.

You must deploy and configure a Kerberos infrastructure before AMQ Broker can authenticate and authorize Kerberos credentials. See your operating system documentation for more information about deploying Kerberos. If your operating system is RHEL 7, for example, see the chapter Using Kerberos. A Kerberos Authentication Overview is available for Windows as well.

NOTE
You must deploy and configure a Kerberos infrastructure before AMQ Broker can authenticate and authorize Kerberos credentials.

NOTE
Users of an Oracle or IBM JDK should install the Java Cryptography Extension (JCE). See the documentation from the Oracle version of the JCE or the IBM version of the JCE for more information.

6.4.1. Enabling Network Connections to Use Kerberos

AMQ Broker integrates with Kerberos security credentials by using the GSSAPI mechanism from the Simple Authentication and Security Layer (SASL) framework. To use Kerberos in AMQ Broker, each acceptor authenticating or authorizing clients that use a Kerberos credential must be configured to used the GSSAPI mechanism.

**Prerequisites**
You must deploy and configure a Kerberos infrastructure before AMQ Broker can authenticate and authorize Kerberos credentials.

**Procedure**

1. Stop the broker.
   a. If the broker is running on Linux:
      ```
      BROKER_INSTANCE_DIR/bin/artemis stop
      ```
   b. If the broker is running on Windows as a service:
      ```
      BROKER_INSTANCE_DIR/bin\artemis-service.exe stop
      ```

2. Open the `broker.xml` configuration file located under `BROKER_INSTANCE_DIR/etc`

3. Add the name-value pair `saslMechanisms=GSSAPI` to the query string of the URL for the acceptor, as shown in the following example:

   ```
   <acceptor name="amqp">
     tcp://0.0.0.0:5672?protocols=AMQP;saslMechanisms=GSSAPI
   </acceptor>
   ```
The result is an acceptor that uses the GSSAPI mechanism when authenticating Kerberos credentials.

4. (Optional) The **PLAIN** and **ANONYMOUS** SASL mechanisms are also supported. If you want to use these other mechanisms in addition to **GSSAPI**, add them to the list of **saslMechanisms**. Be sure to separate each value with a comma. In the following example, the name-value pair `saslMechanisms=GSSAPI` is modified to add the value **PLAIN**.

```xml
<acceptor name="amqp">
  tcp://0.0.0.0:5672?protocols=AMQP;saslMechanisms=GSSAPI,PLAIN
</acceptor>
```

The result is an acceptor that uses both the **GSSAPI** and **PLAIN** SASL mechanisms.

5. Start the broker.
   a. If the broker is running on Linux:
      ```
      BROKER_INSTANCE_DIR/bin/artemis run
      ```
   b. If the broker is running on Windows as a service:
      ```
      BROKER_INSTANCE_DIR/bin/artemis-service.exe start
      ```

Related Information
See [About Acceptors](#) for more information about acceptors.

### 6.4.2. Authenticating Clients with Kerberos Credentials

AMQ Broker supports Kerberos authentication of AMQP connections that use the GSSAPI mechanism from the Simple Authentication and Security Layer (SASL) framework.

A broker acquires its Kerberos acceptor credentials by using the Java Authentication and Authorization Service (JAAS). The JAAS library included with your Java installation is packaged with a login module, **Krb5LoginModule**, that authenticates Kerberos credentials. See the documentation from your Java vendor for more information about their **Krb5LoginModule**. For example, Oracle provides information about their **Krb5LoginModule** login module as part of their [Java 8 documentation](#).

**Prerequisites**
You must enable the GSSAPI mechanism of an acceptor before it can authenticate AMQP connections using Kerberos security credentials.

**Procedure**

1. Stop the broker.
   a. If the broker is running on Linux:
      ```
      BROKER_INSTANCE_DIR/bin/artemis stop
      ```
   b. If the broker is running on Windows as a service:
      ```
      BROKER_INSTANCE_DIR/bin/artemis-service.exe stop
      ```

2. Open the **login.config** configuration file located under **BROKER_INSTANCE_DIR/etc**.
3. Add a configuration scope named `amqp-sasl-gssapi` to `login.config`. The following example shows configuration for the `Krb5LoginModule` found in Oracle and OpenJDK versions of the JDK.

```
NOTE
Verify the fully qualified class name of the `Krb5LoginModule` and its available options by referring to the documentation from your Java vendor.

```amqp-sasl-gssapi {
com.sun.security.auth.module.Krb5LoginModule required
isInitiator=false
storeKey=true
useKeyTab=true
principal="amqp/my_broker_host@example.com"
debug=true;
}
```

By default, the GSSAPI mechanism implementation on the broker uses a JAAS configuration scope named `amqp-sasl-gssapi` to obtain its Kerberos acceptor credentials.

This version of the `Krb5LoginModule` is provided by the Oracle and OpenJDK versions of the JDK. Verify the fully qualified class name of the `Krb5LoginModule` and its available options by referring to the documentation from your Java vendor.

The `Krb5LoginModule` is configured to use a Kerberos keytab when authenticating a principal. Keytabs are generated using tooling from your Kerberos environment. See the documentation from your vendor for details about generating Kerberos keytabs.

The Principal is set to `amqp/my_broker_host@example.com`. This value must correspond to the service principal created in your Kerberos environment. See the documentation from your vendor for details about creating service principals.

4. Start the broker.
   a. If the broker is running on Linux:
      ```
      BROKER_INSTANCE_DIR/bin/artemis run
      ```
   b. If the broker is running on Windows as a service:
      ```
      BROKER_INSTANCE_DIR/bin\artemis-service.exe start
      ```

Related Information
See Network Connections and Kerberos, for more information about enabling the GSSAPI mechanism in AMQ Broker.

6.4.2.1. Using an Alternative Configuration Scope

You can specify an alternative configuration scope by adding the parameter `saslLoginConfigScope` to the URL of an AMQP acceptor. In the following configuration example, the parameter `saslLoginConfigScope` is given the value `alternative-sasl-gssapi`. The result is an acceptor that uses
the alternative scope named `alternative-sasl-gssapi`, which was declared in the `BROKER_INSTANCE_DIR/etc/login.config` configuration file.

```xml
<acceptor name="amqp">
tcp://0.0.0.0:5672?
protocols=AMQP;saslMechanisms=GSSAPI,PLAIN;saslLoginConfigScope=alternative-sasl-gssapi`
</acceptor>
```

### 6.4.3. Authorizing Clients with Kerberos Credentials

AMQ Broker is packaged with an implementation of the JAAS `Krb5LoginModule` for use by other security modules when mapping roles. The module adds a Kerberos-authenticated Peer Principal to the Subject’s principal set as an AMQ Broker UserPrincipal. The credentials can then be passed to a `PropertiesLoginModule` or `LDAPLoginModule`, which maps the Kerberos-authenticated Peer Principal to an AMQ Broker role.

**NOTE**

The Kerberos Peer Principal does not exist as a broker user, only as a role member.

### Prerequisites

You must enable the GSSAPI mechanism of an acceptor before it can authorize AMQP connections using Kerberos security credentials.

### Procedure

1. Stop the broker.
   
   a. If the broker is running on Linux:

   ```bash
   BROKER_INSTANCE_DIR/bin/artemis stop
   ```

   b. If the broker is running on Windows as a service:

   ```bash
   BROKER_INSTANCE_DIR/bin/artemis-service.exe stop
   ```

2. Open the `login.config` configuration file located under `BROKER_INSTANCE_DIR/etc`.

3. Add configuration for the AMQ Broker `Krb5LoginModule` and the `LDAPLoginModule`.

   **NOTE**

   Verify the configuration options by referring to the documentation from your LDAP provider.

   ```properties
   org.apache.activemq.artemis.spi.core.security.jaas.Krb5LoginModule required
   org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule optional
   initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
   connectionURL="ldap://localhost:1024"
   authentication=GSSAPI
   saslLoginConfigScope=broker-sasl-gssapi
   connectionProtocol=s
   ```
userBase="ou=users,dc=example,dc=com"
userSearchMatching="(krb5PrincipalName={0})"
userSearchSubtree=true
authenticateUser=false
roleBase="ou=system"
roleName=cn
roleSearchMatching="(member={0})"
roleSearchSubtree=false
;

This version of the Krb5LoginModule is distributed with AMQ Broker and transforms the Kerberos identity into a broker identity that can be used by other AMQ modules for role mapping.

4. Start the broker.
   a. If the broker is running on Linux:
      
      ```
      BROKER_INSTANCE_DIR/bin/artemis run
      ```
   b. If the broker is running on Windows as a service:
      
      ```
      BROKER_INSTANCE_DIR/bin/artemis-service.exe start
      ```

Related Information
See Network Connections and Kerberos for more information about enabling the GSSAPI mechanism in AMQ Broker.

See Users and Roles for more information about the PropertiesLoginModule.

See Integrating with LDAP for more information about the LDAPLoginModule.

6.5. ENCRYPTING PASSWORDS IN CONFIGURATION FILES

By default, AMQ Broker stores all passwords in configuration files as plain text. Be sure to secure all configuration files with the correct permissions to prevent unauthorized access. You can also encrypt, or mask, the plain text passwords to prevent unwanted viewers from reading them.

A masked password is the encrypted version of a plain text password. The encrypted version is generated by the mask command-line utility provided by AMQ Broker. For more information about the mask utility, see the command-line help documentation:

```
$ BROKER_INSTANCE_DIR/bin/artemis help mask
```

To mask a password, replace its plain text value with the encrypted one. The masked password must be wrapped by the identifier ENC() so that it is decrypted when the actual value is needed.

In the following example, the configuration file BROKER_INSTANCE_DIR/etc/bootstrap.xml contains masked passwords for the attributes keyStorePassword and trustStorePassword.

Example with bootstrap.xml

```
<web bind="https://localhost:8443" path="web"
```
supported configuration files.

Supported Configuration Files

- broker.xml
- bootstrap.xml
- management.xml
- artemis-users.properties
- login.config (for use with the LDAPLoginModule)

Configuration files are found at `BROKER_INSTANCE_DIR/etc`.

NOTE

artemis-users.properties supports only masked passwords that have been hashed. When a user is created upon broker creation, artemis-users.properties contains hashed passwords by default. The default PropertiesLoginModule will not decode the passwords in artemis-users.properties file but will instead hash the input and compare the two hashed values for password verification. Changing the hashed password to a masked password does not allow access to the AMQ Console.

broker.xml, bootstrap.xml, management.xml, and login.config support passwords that are masked but not hashed.

Procedure

As an example, the following procedure explains how to mask the value of the cluster-password configuration element found in the file `BROKER_INSTANCE_DIR/etc/broker.xml`.

1. From a command prompt, use the mask utility to encrypt a password:

   ```
   $ BROKER_INSTANCE_DIR/bin/artemis mask PASSWORD
   
   result: 3a34fd21b82bf2a822fa49a8d8fa115d
   ```

2. Open the configuration file containing the plain text password you want to mask:

   ```
   <cluster-password>
   PASSWORD
   </cluster-password>
   ```

3. Replace the plain text password with the encrypted value that you created in Step 1:
4. Wrap the encrypted value with the identifier ENC():

```
<cluster-password>
ENC(3a34fd21b82bf2a822fa49a8d8fa115d)
</cluster-password>
```

The configuration file now contains a masked password. Because the password is wrapped with the ENC() identifier, AMQ Broker decrypts it before it is used.

Additional Resources

For more information about the configuration files included with AMQ Broker, see AMQ Broker configuration files and locations.

6.6. TRACKING MESSAGES FROM VALIDATED USERS

To enable tracking and logging the origins of messages (for example, for security-auditing purposes), you can use the _AMQ_VALIDATED_USER message key.

In the broker.xml configuration file, if the populate-validated-user option is set to true, then the broker adds the name of the validated user to the message using the _AMQ_VALIDATED_USER key. For JMS and STOMP clients, this message key maps to the JMSXUserID key.

**NOTE**

The broker cannot add the validated user name to a message produced by an AMQP JMS client. Modifying the properties of an AMQP message after it has been sent by a client is a violation of the AMQP protocol.

For a user authenticated based on his/her SSL certificate, the validated user name populated by the broker is the name to which the certificate’s Distinguished Name (DN) maps.

In the broker.xml configuration file, if security-enabled is false and populate-validated-user is true, then the broker populates whatever user name, if any, that the client provides. The populate-validated-user option is false by default.

You can configure the broker to reject a message that doesn’t have a user name (that is, the JMSXUserID key) already populated by the client when it sends the message. You might find this option useful for AMQP clients, because the broker cannot populate the validated user name itself for messages sent by these clients.

To configure the broker to reject messages without JMSXUserID set by the client, add the following configuration to the broker.xml configuration file:

```
<reject-empty-validated-user>true</reject-empty-validated-user>
```

By default, reject-empty-validated-user is set to false.

6.7. DISABLING SECURITY
Security is enabled by default. Broker security can be enabled or disabled by setting the `<security-enabled>` parameter in the `<core>` element of the `broker.xml` configuration file.

**Procedure**

1. Open the `broker.xml` file.

2. Locate the `<security-enabled>` parameter.

3. Edit the entry as needed:
   - Set the parameter to `false` to disable security:

     ```xml
     <security-enabled>false</security-enabled>
     ```

4. If necessary, change the `security-invalidation-interval` entry (which periodically invalidates secure logins) to a different value (in ms). The default is 10000.
CHAPTER 7. PERSISTING MESSAGES

This chapter describes how persistence works with AMQ Broker and how to configure it.

The broker ships with two persistence options:

1. **Journal-based**
   The default. A highly performant option that writes messages to journals on the file system.

2. **JDBC-based**
   Uses the broker’s JDBC Store to persist messages to a database of your choice.

Alternatively, you can also configure the broker for zero persistence.

The broker uses a different solution for persisting large messages outside the message journal. See Working with Large Messages for more information. The broker can also be configured to page messages to disk in low memory situations. See Paging Messages for more information.

**NOTE**

For current information regarding which databases and network file systems are supported see Red Hat AMQ Supported Configurations on the Red Hat Customer Portal.

7.1. ABOUT JOURNAL-BASED PERSISTENCE

A broker’s journal is a set of **append only** files on disk. Each file is pre-created to a fixed size and initially filled with padding. As messaging operations are performed on the broker, records are appended to end of the journal. Appending records allows the broker to minimize disk head movement and random access operations, which are typically the slowest operation on a disk. When one journal file is full, the broker uses a new one.

The journal file size is configurable, minimizing the number of disk cylinders used by each file. Modern disk topologies are complex, however, and the broker cannot control which cylinder(s) the file is mapped to. Journal file sizing therefore is not an exact science.

Other persistence-related features include:

- A sophisticated file garbage collection algorithm that determines whether a particular journal file is still in use. If not, the file can be reclaimed and re-used.

- A compaction algorithm that removes dead space from the journal and that compresses the data. This results in the journal using fewer files on disk.

- Support for local transactions.

- Support for XA transactions when using AMQ JMS clients.

The majority of the journal is written in Java. However, the interaction with the actual file system is abstracted, so you can use different, pluggable implementations. AMQ Broker ships with two implementations:

- **Java NIO.**
  Uses the standard Java NIO to interface with the file system. This provides extremely good performance and runs on any platform with a Java 6 or later runtime.

- **Linux Asynchronous IO**
Uses a thin native wrapper to talk to the Linux asynchronous IO library (AIO). With AIO, the broker is called back after the data has made it to disk, avoiding explicit syncs altogether. By default the broker tries to use an AIO journal, and falls back to using NIO if AIO is not available.

Using AIO typically provides even better performance than using Java NIO. For instructions on how to install libaio see Using an AIO journal.

NOTE

For current information regarding which network file systems are supported see Red Hat AMQ Supported Configurations on the Red Hat Customer Portal.

7.1.1. Using AIO

The Java NIO journal is highly performant, but if you are running the broker using Linux Kernel 2.6 or later, Red Hat recommends using the AIO journal for better persistence performance. It is not possible to use the AIO journal with other operating systems or earlier versions of the Linux kernel.

To use the AIO journal you must install the libaio if it is not already installed.

Procedure

- Use the yum command to install libaio, as in the example below:

  ```
  yum install libaio
  ```

7.2. CONFIGURING JOURNAL-BASED PERSISTENCE

Persistence configuration is maintained in the file `BROKER_INSTANCE_DIR/etc/broker.xml`. The broker’s default configuration uses journal based persistence and includes the elements shown below.

```xml
<configuration>
  <core>
    ...
    <persistence-enabled>true</persistence-enabled> 1
    <journal-type>ASYNCIO</journal-type> 2
    <bindings-directory>/data/bindings</bindings-directory> 3
    <journal-directory>/data/journal</journal-directory> 4
    <journal-datasync>true</journal-datasync> 5
    <journal-min-files>2</journal-min-files> 6
    <journal-pool-files>-1</journal-pool-files> 7
    ...
  </core>
</configuration>
```

1. Set to `true` to use the file based journal for persistence.
2. The type of journal to use. If set to ASYNCIO, the broker first attempts to use AIO and falls back to NIO if ASYNCIO is not found.
3. The file system location of the bindings journal. The default setting is relative to `BROKER_INSTANCE_DIR`. 

Red Hat AMQ 7.5 Configuring AMQ Broker
The file system location of the messaging journal. The default setting is relative to `BROKER_INSTANCE_DIR`.

Set to `true` to use `fdatasync` to confirm writes to the disk.

The number of journal files to pre-create when the broker starts.

The number of files to keep after reclaiming un-used files. The default value, `-1`, means that no files are deleted during clean up.

### 7.2.1. The Message Journal

The message journal stores all message-related data, including the messages themselves and duplicate ID caches. The files on this journal are prefixed as `activemq-data`. Each file has a `amq` extension and a default size of `10485760` bytes. The location of the message journal is set using the `journal-directory` configuration element. The default value is `BROKER_INSTANCE_DIR/data/journal`. The default configuration includes other elements related to the messaging journal:

- **journal-min-files**
  The number of journal files to pre-create when the broker starts. The default is `2`.

- **journal-pool-files**
  The number of files to keep after reclaiming un-used files. The default value, `-1`, means that no files are deleted once created by the broker. However, the system cannot grow infinitely, so you are required to use paging for destinations that are unbounded in this way. See the chapter on [Paging Messages](#) for more information.

There are several other configuration elements available for the messaging journal. See the [appendix](#) for a full list.

### 7.2.2. The Bindings Journal

The bindings journal is used to store bindings-related data, such as the set of queues deployed on the server and their attributes. It also stores data such as ID sequence counters.

The bindings journal always uses NIO because it is typically low throughput when compared to the message journal. Files on this journal are prefixed with `activemq-bindings`. Each file has a `bindings` extension and a default size of `1048576` bytes.

Use the following configuration elements in `BROKER_INSTANCE_DIR/etc/broker.xml` to configure the bindings journal.

- **bindings-directory**
  This is the directory in which the bindings journal lives. The default value is `BROKER_INSTANCE_DIR/data/bindings`.

- **create-bindings-dir**
  If this is set to `true` then the bindings directory is automatically created at the location specified in `bindings-directory` if it does not already exist. The default value is `true`.

### 7.2.3. The JMS Journal

The JMS journal stores all JMS-related data, including JMS Queues, Topics, and Connection Factories, as well as any JNDI bindings for these resources. Also, any JMS Resources created via the management API is persisted to this journal, but any resources configured via configuration files are not. The JMS
Journal is only created if JMS is being used.

The files on this journal are prefixed as `activemq-jms`. Each file has a `jms` extension and a default size of 1048576 bytes.

The JMS journal shares its configuration with the bindings journal.

### 7.2.4. Compacting Journal Files

AMQ Broker includes a compaction algorithm that removes dead space from the journal and compresses its data so that it takes up less space on disk. There are two criteria used to determine when to start compaction. After both criteria are met, the compaction process parses the journal and removes all dead records. Consequently, the journal comprises fewer files. The criteria are:

- The number of files created for the journal.
- The percentage of live data in the journal’s files.

You configure both criteria in `BROKER_INSTANCE_DIR/etc/broker.xml`.

**Procedure**

- To configure the criteria for the compaction process, add the following two elements, as in the example below.

  ```xml
  <configuration>
    <core>
      ...
      <journal-compact-min-files>15</journal-compact-min-files> 1
      <journal-compact-percentage>25</journal-compact-percentage> 2
      ...
    </core>
  </configuration>
  ```

  1. The minimum number of files created before compaction begins. That is, the compacting algorithm does not start until you have at least `journal-compact-min-files`. The default value is 10. Setting this to 0 disables compaction, which is dangerous because the journal could grow indefinitely.

  2. The percentage of live data in the journal’s files. When less than this percentage is considered live data, compacting begins. Remember that compacting does not begin until you also have at least `journal-compact-min-files` data files on the journal. The default value is 30.

**Compacting Journals Using the CLI**

You can also use the command-line interface (CLI) to compact journals.

**Procedure**

1. As the owner of the `BROKER_INSTANCE_DIR`, stop the broker. In the example below, the user `amq-broker` was created during the installation of AMQ Broker.
su - amq-broker

cd __BROKER_INSTANCE_DIR__/bin
$ ./artemis stop

2. (Optional) Run the following CLI command to get a full list of parameters for the data tool. Note that by default, the tool uses settings found in $BROKER_INSTANCE_DIR/etc/broker.xml.

$ ./artemis help data compact.

3. Run the following CLI command to compact the data.

$ ./artemis data compact.

4. After the tool has successfully compacted the data, restart the broker.

$ ./artemis run

Related Information

AMQ Broker includes a number of CLI commands for managing your journal files. See command-line Tools in the Appendix for more information.

7.2.5. Disabling Disk Write Cache

Most disks contain hardware write caches. A write cache can increase the apparent performance of the disk because writes are lazily written to the disk later. By default many systems ship with disk write cache enabled. This means that even after syncing from the operating system there is no guarantee the data has actually made it to disk, so if a failure occurs, critical data can be lost.

Some more expensive disks have non-volatile or battery-backed write caches that do not necessarily lose data in event of failure, but you should test them. If your disk does not have such features, you should ensure that write cache is disabled. Be aware that disabling disk write cache can negatively affect performance.

Procedure

- On Linux, manage your disk’s write cache settings using the tools `hdparm` (for IDE disks) or `sdparm` or `sginfo` (for SDSI/SATA disks).

- On Windows, manage the cache setting by right-clicking the disk and clicking Properties.

7.3. CONFIGURING JDBC PERSISTENCE

The JDBC persistence store uses a JDBC connection to store messages and bindings data in database tables. The data in the tables is encoded using AMQ Broker journal encoding.

NOTE

For current information regarding which databases are supported see Red Hat AMQ Supported Configurations on the Red Hat Customer Portal.
1. Add the appropriate JDBC client libraries to the broker runtime. You can do this by adding the relevant jars to the \texttt{BROKER\_INSTANCE\_DIR/lib} directory.

2. Create a \texttt{store} element in your \texttt{BROKER\_INSTANCE\_DIR/etc/broker.xml} configuration file under the \texttt{core} element, as in the example below.

\begin{verbatim}
<configuration>
  <core>
    <store>
      <database-store>
        <jdbc-connection-url>jdbc:derby:database-store;create=true</jdbc-connection-url>
        <jdbc-user>ENC(5493dd76567ee5ec269d11823973462f)</jdbc-user>
        <jdbc-password>ENC(56a0db3b71043054269d11823973462f)</jdbc-password>
        <bindings-table-name>BINDINGS_TABLE</bindings-table-name>
        <message-table-name>MESSAGE_TABLE</message-table-name>
        <large-message-table-name>LARGE\_MESSAGES\_TABLE</large-message-table-name>
        <page-store-table-name>PAGE\_STORE\_TABLE</page-store-table-name>
        <jdbc-driver-class-name>org.apache.derby.jdbc.EmbeddedDriver</jdbc-driver-class-name>
      </database-store>
    </store>
  </core>
</configuration>
\end{verbatim}

1. \texttt{jdbc-connection-url} is the full JDBC connection URL for your database server. The connection url should include all configuration parameters and the database name.

2. \texttt{jdbc-user} is the encrypted user name for your database server. For more information about encrypting user names and passwords for use in configuration files, see Encrypting Passwords in Configuration Files.

3. \texttt{jdbc-password} is the encrypted password for your database server. For more information about encrypting user names and passwords for use in configuration files, see Encrypting Passwords in Configuration Files.

4. \texttt{bindings-table-name} is the name of the table in which the bindings data is stored. Specifying this table name allows you to share a single database between multiple servers, without interference.

5. \texttt{message-table-name} is the name of the table in which the bindings data is stored.

6. \texttt{large-message-table-name} is the name of the table in which messages and related data are persisted.

7. \texttt{page-store-table-name} is the name of the table in which paged store directory information is stored.

8. \texttt{jdbc-driver-class-name} is the fully-qualified class name of the desired database driver.

### 7.4. CONFIGURING ZERO PERSISTENCE
In some situations, zero persistence is sometimes required for a messaging system. Configuring the broker to perform zero persistence is straightforward. Set the parameter `persistence-enabled` in `/etc/broker.xml` to `false`.

Note that if you set this parameter to false, then zero persistence occurs. That means no bindings data, message data, large message data, duplicate ID caches or paging data is persisted.
CHAPTER 8. PAGING MESSAGES

AMQ Broker transparently supports huge queues containing millions of messages while the server is running with limited memory.

In such a situation it’s not possible to store all of the queues in memory at any one time, so AMQ Broker transparently pages messages into and out of memory as they are needed, thus allowing massive queues with a low memory footprint.

Paging is done individually per address. AMQ Broker will start paging messages to disk when the size of all messages in memory for an address exceeds a configured maximum size. For more information about addresses, see Addresses, Queues, and Topics.

By default, AMQ Broker does not page messages. You must explicitly configure paging to enable it.

See the paging example located under INSTALL_DIR/examples/standard/ for a working example showing how to use paging with AMQ Broker.

8.1. ABOUT PAGE FILES

Messages are stored per address on the file system. Each address has an individual folder where messages are stored in multiple files (page files). Each file will contain messages up to a max configured size (page-size-bytes). The system will navigate on the files as needed, and it will remove the page file as soon as all the messages are acknowledged up to that point.

Browsers will read through the page-cursor system.

Consumers with selectors will also navigate through the page-files and ignore messages that don’t match the criteria.

NOTE

When you have a queue, and consumers filtering the queue with a very restrictive selector you may get into a situation where you won’t be able to read more data from paging until you consume messages from the queue.

Example: in one consumer you make a selector as 'color="red"' but you only have one color red one million messages after blue, you won’t be able to consume red until you consume blue ones. This is different to browsing as we will "browse" the entire queue looking for messages and while we "depage" messages while feeding the queue.

8.2. CONFIGURING THE PAGING DIRECTORY LOCATION

To configure the location of the paging directory, add the paging-directory configuration element to the broker’s main configuration file BROKER_INSTANCE_DIR/etc/broker.xml, as in the example below.

```xml
<configuration ...>
  ...
  <core ...>
    <paging-directory>/somewhere/paging-directory</paging-directory>
  ...
</core>
</configuration>
```
AMQ Broker will create one directory for each address being paged under the configured location.

### 8.3. CONFIGURING AN ADDRESS FOR PAGING

Configuration for paging is done at the address level by adding elements to a specific `address-settings`, as in the example below.

```xml
<address-settings>
    <address-setting match="jms.paged.queue">
        <max-size-bytes>104857600</max-size-bytes>
        <page-size-bytes>10485760</page-size-bytes>
        <address-full-policy>PAGE</address-full-policy>
    </address-setting>
</address-settings>
```

In the example above, when messages sent to the address `jms.paged.queue` exceed 104857600 bytes in memory, the broker will begin paging.

**NOTE**

Paging is done individually per address. If you specify `max-size-bytes` for an address, each matching address does not exceed the maximum size that you specified. It DOES NOT mean that the total overall size of all matching addresses is limited to `max-size-bytes`.

This is the list of available parameters on the address settings.

#### Table 8.1. Paging Configuration Elements

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-size-bytes</td>
<td>The maximum size in memory allowed for the address before the broker enters page mode.</td>
<td>-1 (disabled).</td>
</tr>
<tr>
<td>page-size-bytes</td>
<td>The size of each page file used on the paging system.</td>
<td>10MiB (10 * 1024 * 1024 bytes)</td>
</tr>
</tbody>
</table>
Valid values are PAGE, DROP, BLOCK, and FAIL. If the value is PAGE then further messages will be paged to disk. If the value is DROP then further messages will be silently dropped. If the value is FAIL then the messages will be dropped and the client message producers will receive an exception. If the value is BLOCK then client message producers will block when they try and send further messages.

The system will keep up to this number of page files in memory to optimize IO during paging navigation.

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-full-policy</td>
<td>Valid values are PAGE, DROP, BLOCK, and FAIL. If the value is PAGE then further messages will be paged to disk. If the value is DROP then further messages will be silently dropped. If the value is FAIL then the messages will be dropped and the client message producers will receive an exception. If the value is BLOCK then client message producers will block when they try and send further messages.</td>
<td>PAGE</td>
</tr>
<tr>
<td>page-max-cache-size</td>
<td>The system will keep up to this number of page files in memory to optimize IO during paging navigation.</td>
<td>5</td>
</tr>
</tbody>
</table>

8.4. CONFIGURING A GLOBAL PAGING SIZE

Sometimes configuring a memory limit per address is not practical, such as when a broker manages many addresses that have different usage patterns. In these situations, use the `global-max-size` parameter to set a global limit to the amount of memory the broker can use before it enters into the page mode configured for the address associated with the incoming message.

The default value for `global-max-size` is half of the maximum memory available to the Java virtual machine (JVM). You can specify your own value for this parameter by configuring it in the `broker.xml` configuration file. The value for `global-max-size` is in bytes, but you can use byte notation ("K", "Mb", "GB", for example) for convenience.

The following procedure shows how to configure the `global-max-size` parameter in the `broker.xml` configuration file.

Configuring the `global-max-size` parameter

**Procedure**

1. Stop the broker.
   a. If the broker is running on Linux, run the following command:

   ```
   BROKER_INSTANCE_DIR/bin/artemis stop
   ```

   b. If the broker is running on Windows as a service, run the following command:

   ```
   BROKER_INSTANCE_DIR\bin\artemis-service.exe stop
   ```

2. Open the `broker.xml` configuration file located under `BROKER_INSTANCE_DIR/etc`.

3. Add the `global-max-size` parameter to `broker.xml` to limit the amount of memory, in bytes, the broker can use. Note that you can also use byte notation (K, Mb, GB) for the value of `global-max-size`, as shown in the following example.

   ```
   <configuration>
   <core>
   ...
   <global-max-size>1GB</global-max-size>
   ```
In the preceding example, the broker is configured to use a maximum of one gigabyte, \(1 \text{GB}\), of available memory when processing messages. If the configured limit is exceeded, the broker enters the page mode configured for the address associated with the incoming message.

4. Start the broker.
   a. If the broker is running on Linux, run the following command:
      
      ```bash
      BROKER_INSTANCE_DIR/bin/artemis run
      ```
   b. If the broker is running on Windows as a service, run the following command:
      
      ```cmd
      BROKER_INSTANCE_DIR/bin/artemis-service.exe start
      ```

Related Information
See Section 8.3, “Configuring an Address for Paging” for information about setting the paging mode for an address.

8.5. LIMITING DISK USAGE WHEN PAGING

You can limit the amount of physical disk the broker uses before it blocks incoming messages rather than pages them. Add the `max-disk-usage` to the `broker.xml` configuration file and provide a value for the percentage of disk space the broker is allowed to use when paging messages. The default value for `max-disk-usage` is 90, which means the limit is set at 90 percent of disk space.

Configuring the `max-disk-usage`

Procedure

1. Stop the broker.
   a. If the broker is running on Linux, run the following command:
      
      ```bash
      BROKER_INSTANCE_DIR/bin/artemis stop
      ```
   b. If the broker is running on Windows as a service, run the following command:
      
      ```cmd
      BROKER_INSTANCE_DIR/bin/artemis-service.exe stop
      ```

2. Open the `broker.xml` configuration file located under `BROKER_INSTANCE_DIR/etc`.

3. Add the `max-disk-usage` configuration element and set a limit to the amount disk space to use when paging messages.

```xml
<configuration>
  <core>
    ...
  </core>
  <max-disk-usage>50</max-disk-usage>
</configuration>
```
In the preceding example, the broker is limited to using 50 percent of disk space when paging messages. Messages are blocked and no longer paged after 50 percent of the disk is used.

4. Start the broker.
   a. If the broker is running on Linux, run the following command:

      ```bash
      BROKER_INSTANCE_DIR/bin/artemis run
      ```
   b. If the broker is running on Windows as a service, run the following command:

      ```cmd
      BROKER_INSTANCE_DIR\bin\artemis-service.exe start
      ```

8.6. HOW TO DROP MESSAGES

Instead of paging messages when the max size is reached, an address can also be configured to just drop messages when the address is full.

To do this just set the `address-full-policy` to `DROP` in the address settings.

8.6.1. Dropping Messages and Throwing an Exception to Producers

Instead of paging messages when the max size is reached, an address can also be configured to drop messages and also throw an exception on the client-side when the address is full.

To do this just set the `address-full-policy` to `FAIL` in the address settings.

8.7. HOW TO BLOCK PRODUCERS

Instead of paging messages when the max size is reached, an address can also be configured to block producers from sending further messages when the address is full, thus preventing the memory from being exhausted on the server.

**NOTE**

Blocking works only if the protocol being used supports it. For example, an AMQP producer will understand a Block packet when it is sent by the broker, but a STOMP producer will not.

When memory is freed up on the server, producers will automatically unblock and be able to continue sending.

To do this just set the `address-full-policy` to `BLOCK` in the address settings.

In the default configuration, all addresses are configured to block producers after 10 MiB of data are in the address.

8.8. CAUTION WITH ADDRESSES WITH MULTICAST QUEUES
When a message is routed to an address that has multicast queues bound to it, for example, a JMS subscription in a Topic, there is only one copy of the message in memory. Each queue handles only a reference to it. Because of this the memory is only freed up after all queues referencing the message have delivered it.

If you have a single lazy subscription, the entire address will suffer IO performance hit as all the queues will have messages being sent through an extra storage on the paging system.

For example:

- An address has 10 queues
- One of the queues does not deliver its messages (maybe because of a slow consumer).
- Messages continually arrive at the address and paging is started.
- The other 9 queues are empty even though messages have been sent.

In this example, all the other 9 queues will be consuming messages from the page system. This may cause performance issues if this is an undesirable state.
CHAPTER 9. WORKING WITH LARGE MESSAGES

You can configure AMQ Broker to store large messages on a physical disk or in a database table. Handling large messages in this way avoids the memory overhead that occurs when storing several large messages in memory.

AMQ Broker can persist large messages even if the client and broker are running with limited memory. The maximum size of a large message depends only on the amount of space available for your physical disk or database table.

NOTE

Large message support is available for the AMQP, Core, and OpenWire protocols. Additionally, the STOMP protocol provides its own method for handling large messages. See "Handling Large Messages with STOMP" for more information.

NOTE

If you persist large messages on a disk, it is recommended that the large messages directory be located on a different volume than the one used to persist the message journal or the paging directory.

9.1. PREPARING BROKERS TO STORE LARGE MESSAGES

Large messages are stored on physical disk or database table. You must configure the broker to specify where large messages are stored.

Procedure

- Add configuration to `BROKER_INSTANCE_DIR/etc/broker.xml` that references the storage location for large messages.
  - If you are storing large messages on disk, add the `large-messages-directory` configuration element and provide the file system location, as shown in the following example:

    ```
    <configuration>
    <core>
      ...
      <large-messages-directory>/path/to/large-messages</large-messages-directory> 1
      ...
    </core>
    </configuration>
    ```

    1 The default value for the `large-messages-directory` configuration element is `BROKER_INSTANCE_DIR/data/largemessages`

- If you are storing large messages in a database table, add the name of the table to your `database-store`, as shown in the following example:

    ```
    <store>
    <database-store>
      ...
    </database-store>
    ```
The default value for the large-message-table configuration element is LARGE_MESSAGE_TABLE.

Additional Resources

See the large-message example found under BROKER_INSTANCE_DIR/examples/standard/ for a working example showing how to work with large messages.

For more information about configuring a data-store see Configuring JDBC Persistence.

9.2. PREPARING AMQ CORE PROTOCOL JMS CLIENTS TO SEND LARGE MESSAGES

You prepare client connections to handle large messages by setting a value for the property minLargeMessageSize. The value can be provided as a parameter in the connection URL, or it can be set by using a supported client API. Any message larger than minLargeMessageSize is considered a large message.

NOTE

AMQ Broker messages are encoded using two bytes per character. Therefore, if the message data is filled with ASCII characters (which are one byte in size), the size of the resulting message would roughly double. When setting the value of minLargeMessageSize, remember that encoding can increase message size. The default value for minLargeMessageSize is 100KiB.

Procedure

- Set the minimum size for large messages.
  - If you are using JNDI to instantiate your connection factory, set the size in a jndi.properties file by using the parameter minLargeMessageSize.
    ```java
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    connectionFactory.myConnectionFactory=tcp://localhost:61616?
    minLargeMessageSize=250000
    ```
  - If you are not using JNDI, set the size using the method ActiveMQConnectionFactory.setMinLargeMessageSize().
9.3. PREPARING OPENWIRE CLIENTS TO SEND LARGE MESSAGES

NOTE
Configuration options added to the connection URI used by an AMQ OpenWire JMS client must include the prefix wireFormat. to take effect. Options missing this prefix are ignored.

Procedure
- Set the minimum size for large messages.
  - If you are using JNDI to instantiate your connection factory, set the size in a jndi.properties file by using the parameter minLargeMessageSize. You must add the prefix wireFormat. to the parameter for it to take effect.
    ```
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    connectionFactory.myConnectionFactory=tcp://localhost:61616?
    wireFormat.minLargeMessageSize=250000
    ```
  - If you are not using JNDI, set the size using the method ActiveMQConnectionFactory.setMinLargeMessageSize().
    ```
    ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
    cf.setMinLargeMessageSize(250000);
    ```

9.4. SENDING LARGE MESSAGES
AMQ Broker supports Java-based InputStreams for sending large messages. The most common use case is to send files stored on your disk, but you could also send the data as JDBC Blobs or JSON objects recovered from HTTPRequests.

NOTE
When using JMS, streaming large messages is supported only when using StreamMessage and BytesMessage.

Procedure
- To send a large message, set the JMS_AMQ_InputStream property to mark the message as streamed:
  ```
  BytesMessage message = session.createBytesMessage();
  FileInputStream fileInputStream = new FileInputStream(fileInput);
  BufferedInputStream bufferedInput = new BufferedInputStream(fileInputStream);
  message.setObjectProperty("JMS_AMQ_InputStream", bufferedInput);
  ```
9.5. RECEIVING LARGE MESSAGES

The AMQ Broker Core JMS API has a method for synchronously receiving a streamed message. The methods block further processing until the input stream is completely received.

**Procedure**

- To receive a large message, set the `JMS_AMQ_SaveStream` on the message object:

```java
BytesMessage messageReceived = (BytesMessage)messageConsumer.receive(120000);
File output_file = new File("large_message_received.dat");
FileStream fileOutputStream = new FileInputStream(output_file);
BufferedOutputStream bufferedOutputStream = new BufferedOutputStream(fileOutputStream);

// This will block until the entire content is saved on disk
messageReceived.setObjectProperty("JMS_AMQ_SaveStream", bufferedOutputStream);
```

Receiving a Large Message Asynchronously

The Core JMS API also has a method for asynchronously receiving a streamed message. The method does not block processing by a consumer while it receives the input stream.

**Procedure**

- To receive a large message asynchronously, set the `JMS_AMQ_OutputStream` parameter on the message object:

```java
BytesMessage messageReceived = (BytesMessage)messageConsumer.receive(120000);
File output_file = new File("large_message_received.dat");
FileStream fileOutputStream = new FileInputStream(output_file);
BufferedOutputStream bufferedOutputStream = new BufferedOutputStream(fileOutputStream);

// This will not block until the entire content is saved on disk
messageReceived.setObjectProperty("JMS_AMQ_OutputStream", bufferedOutputStream);
```

9.6. LARGE MESSAGES AND JAVA CLIENTS

There are two recommended options available to Java developers who are writing clients that use large messages.

One option is to use an instance of `InputStream` and `OutputStream`. For example, a `FileInputStream` could be used to send a message taken from a large file on a physical disk. A `FileOutputStream` could then be used by the receiver to stream the message to a location on its local file system.

Another option is to stream a JMS `BytesMessage` or `StreamMessage` directly:

```java
BytesMessage rm = (BytesMessage)cons.receive(10000);
byte data[] = new byte[1024];
for (int i = 0; i < rm.getBodyLength(); i += 1024)
{
    int numberOfBytes = rm.readBytes(data);
    // Do whatever you want with the data
}
```

9.7. COMPRESSION LARGE MESSAGES
You can enable clients to compress large messages before sending them. The ZIP algorithm is used to compress the message body as the message is sent to the broker.

**NOTE**

If the compressed size of a large message is less than the value of `minLargeMessageSize`, the message is sent as a regular message. Therefore, it is not written to the broker’s large-message data directory.

- If you use a Core JMS client and JNDI, use the JNDI context environment to enable message compression:

```java
java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
connectionFactory.myConnectionFactory=tcp://localhost:61616?
compressLargeMessages=true
```

- Add the `minLargeMessageSize` parameter to the connection factory URL to set the minimum size requirement for messages to be compressed. In the following example, messages are compressed only when they exceed 250 kilobytes in size.

```java
connectionFactory.myConnectionFactory=tcp://localhost:61616?
compressLargeMessages=true&minLargeMessageSize=250kb
```

### 9.8. HANDLING LARGE MESSAGES WITH STOMP

STOMP clients might send large bodies of frames, which can exceed the size of the broker’s internal buffer, causing unexpected errors.

To prevent this situation from occurring, set the acceptor’s `stompMinLargeMessageSize` parameter to the desired size. Proper sizing is affected by system resources such as the amount of disk space available, as well as the size of the messages. It is recommended that you run performance tests using several values for `stompMinLargeMessageSize` to determine an appropriate size.

The broker checks the size of the body of each STOMP frame coming from connections established with this acceptor. If the size of the body is equal to or greater than the value of `stompMinLargeMessageSize`, the message is persisted as a large message.

**Procedure**

1. Open the configuration file `BROKER_INSTANCE_DIR/etc/broker.xml`

2. Add the `stompMinLargeMessageSize` parameter and its desired value to an existing or new acceptor, as shown in the following example:

```xml
<acceptors>
  <acceptor name="stomp-acceptor">tcp://localhost:61613?
  protocols=STOMP;stompMinLargeMessageSize=10240</acceptor>
  ...
</acceptors>
```

In the preceding example, the broker is configured to accept STOMP messages on port 61613. If the acceptor receives a STOMP frame with a body larger than or equal to 10240 bytes the broker will persist it as a large message.
When a large message is delivered to a STOMP consumer, the broker automatically converts it from a large message to a normal message before sending it to the client. If a large message is compressed, the broker decompresses it before sending it to STOMP clients.

The default value of `stompMinLargeMessageSize` is 102400 bytes.
CHAPTER 10. DETECTING DEAD CONNECTIONS

Sometimes clients stop unexpectedly and do not have a chance to clean up their resources. If this occurs, it can leave resources in a faulty state and result in the broker running out of memory or other system resources. The broker detects that a client’s connection was not properly shut down at garbage collection time. The connection is then closed and a message similar to the one below is written to the log. The log captures the exact line of code where the client session was instantiated. This enables you to identify the error and correct it.

```
[Finalizer] 20:14:43,244 WARNING [org.apache.activemq.artemis.core.client.impl.DelegatingSession] I'm closing a JMS Connection you left open. Please make sure you close all connections explicitly before letting them go out of scope!
[Finalizer] 20:14:43,244 WARNING [org.apache.activemq.artemis.core.client.impl.DelegatingSession] The session you didn't close was created here:
  java.lang.Exception
   at org.apache.activemq.artemis.core.client.impl.DelegatingSession.<init>(DelegatingSession.java:83)
   at org.acme.yourproject.YourClass (YourClass.java:666)
```

The line in the client code where the connection was instantiated.

Detecting Dead Connections from the Client Side

As long as it is receiving data from the broker, the client considers a connection to be alive. Configure the client to check its connection for failure by providing a value for the `client-failure-check-period` property. The default check period for a network connection is 30000 milliseconds (30 seconds), while the default value for an In-VM connection, is -1, which means the client never fails the connection from its side if no data is received.

Typically, you set the check period to be much lower than the value used for the broker’s connection time-to-live, which ensures that clients can reconnect in case of a temporary failure.

The examples below show how to set the check period to 10000 milliseconds (10 seconds) using Core JMS clients.

Procedure

- Set the check period for detecting dead connections.
  - If you are using JNDI with your Core JMS client, set the check period within the JNDI context environment, `jndi.properties`, for example, as below.
    ```
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    connectionFactory.myConnectionFactory=tcp://localhost:61616?
    clientFailureCheckPeriod=10000
    ```
  - If you are not using JNDI set the check period directly by passing a value to `ActiveMQConnectionFactory.setClientFailureCheckPeriod()`.
    ```
    ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
    cf.setClientFailureCheckPeriod(10000);
    ```
10.1. CONNECTION TIME-TO-LIVE

Because the network connection between the client and the server can fail and then come back online, allowing a client to reconnect, AMQ Broker waits to clean up inactive server-side resources. This wait period is called a time-to-live (TTL). The default TTL for a network-based connection is 60000 milliseconds (1 minute). The default TTL on an In-VM connection is -1, which means the broker never times out the connection on the broker side.

Configuring Time-To-Live on the Broker

If you do not want clients to specify their own connection TTL, you can set a global value on the broker side. This can be done by specifying the connection-ttl-override element in the broker configuration.

The logic to check connections for TTL violations runs periodically on the broker, as determined by the connection-ttl-check-interval element.

Procedure

- Edit BROKER_INSTANCE_DIR/etc/broker.xml by adding the connection-ttl-override configuration element and providing a value for the time-to-live, as in the example below.

```
<configuration>
  <core>
    ...
    <connection-ttl-override>30000</connection-ttl-override> 1
    <connection-ttl-check-interval>1000</connection-ttl-check-interval> 2
    ...
  </core>
</configuration>
```

1 The global TTL for all connections is set to 30000 milliseconds (30 seconds). The default value is -1, which allows clients to set their own TTL.

2 The interval between checks for dead connections is set to 1000 milliseconds (1 second). By default, the checks are done every 2000 milliseconds (2 seconds).

Configuring Time-To-Live on the Client

By default clients can set a TTL for their own connections. The examples below show you how to set the Time-To-Live using Core JMS clients.

Procedure

- Set the Time-To-Live for a Client Connection.
  - If you are using JNDI to instantiate your connection factory, you can specify it in the xml config, using the parameter connectionTtl.
    ```java
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    connectionFactory.myConnectionFactory=tcp://localhost:61616?connectionTtl=30000
    ```
  - If you are not using JNDI, the connection TTL is defined by the ConnectionTTL attribute on a ActiveMQConnectionFactory instance.
ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
cf.setConnectionTTL(30000);

10.2. DISABLING ASYNCHRONOUS CONNECTION EXECUTION

Most packets received on the broker side are executed on the **remoting** thread. These packets represent short-running operations and are always executed on the **remoting** thread for performance reasons. However, some packet types are executed using a thread pool instead of the **remoting** thread, which adds a little network latency.

The packet types that use the thread pool are implemented within the Java classes listed below. The classes are all found in the package

**org.apache.activemq.artemis.core.protocol.core.impl.wireformat**

- RollbackMessage
- SessionCloseMessage
- SessionCommitMessage
- SessionXACloseMessage
- SessionXACloseMessage
- SessionXAPrepareMessage
- SessionXARollbackMessage

**Procedure**

- To disable asynchronous connection execution, add the **async-connection-execution-enabled** configuration element to **BROKER_INSTANCE_DIR/etc/broker.xml** and set it to **false**, as in the example below. The default value is **true**.

```xml
<configuration>
  <core>
    ...
    <async-connection-execution-enabled>false</async-connection-execution-enabled>
    ...
  </core>
</configuration>
```

10.3. CLOSING CONNECTIONS FROM THE CLIENT SIDE

A client application must close its resources in a controlled manner before it exits to prevent dead connections from occurring. In Java, it is recommended to close connections inside a **finally** block:

```java
Connection jmsConnection = null;
try {
  ConnectionFactory jmsConnectionFactory =
  ActiveMQJMSClient.createConnectionFactoryWithoutHA(...);
  jmsConnection = jmsConnectionFactory.createConnection();
  ...use the connection...
} finally {
  if (jmsConnection != null) {
```
jmsConnection.close();
} }
CHAPTER 11. FLOW CONTROL

Flow control prevents producers and consumers from becoming overburdened by limiting the flow of data between them. Using AMQ Broker allows you to configure flow control for both consumers and producers.

11.1. CONSUMER FLOW CONTROL

Consumer flow control regulates the flow of data between the broker and the client as the client consumes messages from the broker. AMQ Broker clients buffer messages by default before delivering them to consumers. Without a buffer, the client would first need to request each message from the broker before consuming it. This type of “round-trip” communication is costly. Regulating the flow of data on the client side is important because out of memory issues can result when a consumer cannot process messages quickly enough and the buffer begins to overflow with incoming messages.

11.1.1. Setting the Consumer Window Size

The maximum size of messages held in the client-side buffer is determined by its window size. The default size of the window for AMQ Broker clients is 1 MiB, or 1024 * 1024 bytes. The default is fine for most use cases. For other cases, finding the optimal value for the window size might require benchmarking your system. AMQ Broker allows you to set the buffer window size if you need to change the default.

Setting the Window Size

The following examples demonstrate how to set the consumer window size parameter when using a Core JMS client. Each example sets a consumer’s window size to 300000 bytes.

Procedure

- Set the consumer window size.
  - If the Core JMS Client uses JNDI to instantiate its connection factory, include the consumerWindowSize parameter as part of the connection string URL. Store the URL within a JNDI context environment. The example below uses a jndi.properties file to store the URL.

```java
java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
ConnectionFactory.myConnectionFactory=tcp://localhost:61616?
consumerWindowSize=300000
```

- If the Core JMS client does not use JNDI to instantiate its connection factory, pass a value to `ActiveMQConnectionFactory.setConsumerWindowSize()`.

```java
ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
cf.setConsumerWindowSize(300000);
```

11.1.2. Handling Fast Consumers

Fast consumers can process messages as fast as they consume them. If you are confident that the consumers in your messaging system are that fast, consider setting the window size to -1. This setting allows for unbounded message buffering on the client side. Use this setting with caution, however. It can overflow client-side memory if the consumer is not able to process messages as fast as it receives them.
Setting the Window Size for Fast Consumers

Procedure

The examples below show how to set the window size to \(-1\) when using a Core JMS client that is a fast consumer of messages.

- Set the consumer window size to \(-1\).
  - If the Core JMS Client uses JNDI to instantiate its connection factory, include the `consumerWindowSize` parameter as part of the connection string URL. Store the URL within a JNDI context environment. The example below uses a `jndi.properties` file to store the URL.

```java
java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
connectionFactory.myConnectionFactory=tcp://localhost:61616?consumerWindowSize=-1
```

- If the Core JMS client does not use JNDI to instantiate its connection factory, pass a value to `ActiveMQConnectionFactory.setConsumerWindowSize()`.

```java
ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
cf.setConsumerWindowSize(-1);
```

11.1.3. Handling Slow Consumers

Slow consumers take significant time to process each message. In these cases, it is recommended to not buffer messages on the client side. Messages remain on the broker side ready to be consumed by other consumers instead. One benefit of turning off the buffer is that it provides deterministic distribution between multiple consumers on a queue. To handle slow consumers by disabling the client-side buffer, set the window size to \(0\).

Setting the Window Size for Slow Consumers

Procedure

The examples below show you how to set the window size to \(0\) when using the Core JMS client that is a slow consumer of messages.

- Set the consumer window size to \(0\).
  - If the Core JMS Client uses JNDI to instantiate its connection factory, include the `consumerWindowSize` parameter as part of the connection string URL. Store the URL within a JNDI context environment. The example below uses a `jndi.properties` file to store the URL.

```java
java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
connectionFactory.myConnectionFactory=tcp://localhost:61616?consumerWindowSize=0
```

- If the Core JMS client does not use JNDI to instantiate its connection factory, pass a value to `ActiveMQConnectionFactory.setConsumerWindowSize()`.
11.1.4. Setting the Rate of Consuming Messages

You can regulate the rate at which a consumer can consume messages. Also known as "throttling", regulating the rate of consumption ensures that a consumer never consumes messages at a rate faster than configuration allows.

**NOTE**

Rate-limited flow control can be used in conjunction with window-based flow control. Rate-limited flow control affects only how many messages a client can consume in a second and not how many messages are in its buffer. With a slow rate limit and a high window-based limit, the internal buffer of the client fills up with messages quickly.

The rate must be a positive integer to enable this functionality and is the maximum desired message consumption rate specified in units of messages per second. Setting the rate to -1 disables rate-limited flow control. The default value is -1.

Setting the Rate of Consuming Messages

Procedure

The examples below use a Core JMS client that limits the rate of consuming messages to 10 messages per second.

- Set the consumer rate.
  - If the Core JMS Client uses JNDI to instantiate its connection factory, include the consumerMaxRate parameter as part of the connection string URL. Store the URL within a JNDI context environment. The example below uses a jndi.properties file to store the URL.

```java
java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
java.naming.provider.url=tcp://localhost:61616?consumerMaxRate=10
```

- If the Core JMS client does not use JNDI to instantiate its connection factory, pass the value to `ActiveMQConnectionFactory.setConsumerMaxRate()`.

```java
ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
cf.setConsumerWindowSize(0);
```

```java
ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
cf.setConsumerMaxRate(10);
```

Related information

See the consumer-rate-limit example in `INSTALL_DIR/examples/standard` for a working example of how to limit the consumer rate.

11.2. PRODUCER FLOW CONTROL
In a similar way to consumer window-based flow control, AMQ Broker can limit the amount of data sent from a producer to a broker to prevent the broker from being overburdened with too much data. In the case of a producer, the window size determines the amount of bytes that can be in-flight at any one time.

11.2.1. Setting the Producer Window Size

The window size is negotiated between the broker and producer on the basis of credits, one credit for each byte in the window. As messages are sent and credits are used, the producer must request, and be granted, credits from the broker before it can send more messages. The exchange of credits between producer and broker regulates the flow of data between them.

Setting the Window Size
The following examples demonstrate how to set the producer window size to 1024 bytes when using Core JMS clients.

Procedure

- Set the producer window size.
  - If the Core JMS Client uses JNDI to instantiate its connection factory, include the producerWindowSize parameter as part of the connection string URL. Store the URL within a JNDI context environment. The example below uses a jndi.properties file to store the URL.

    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    java.naming.provider.url=tcp://localhost:61616?producerWindowSize=1024

  - If the Core JMS client does not use JNDI to instantiate its connection factory, pass the value to ActiveMQConnectionFactory.setProducerWindowSize().

    ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
    cf.setProducerWindowSize(1024);

11.2.2. Blocking Messages

Because more than one producer can be associated with the same address, it is possible for the broker to allocate more credits across all producers than what is actually available. However, you can set a maximum size on any address that prevents the broker from sending more credits than are available.

In the default configuration, a global maximum size of 100Mb is used for each address. When the address is full, the broker writes further messages to the paging journal instead of routing them to the queue. Instead of paging, you can block the sending of more messages on the client side until older messages are consumed. Blocking producer flow control in this way prevents the broker from running out of memory due to producers sending more messages than can be handled at any one time.

In the configuration, blocking producer flow control is managed on a per address-setting basis. The configuration applies to all queues registered to an address. In other words, the total memory for all queues bound to that address is capped by the value given for max-size-bytes.
NOTE

Blocking is protocol dependent. In AMQ Broker the AMQP, OpenWire, and Core protocols feature producer flow control. The AMQP protocol handles flow control differently, however. See Blocking Flow Control Using AMQP for more information.

Configuring the Maximum Size for an Address

To configure the broker to block messages if they are larger than the set maximum number of bytes, add a new `address-setting` configuration element to `BROKER_INSTANCE_DIR/etc/broker.xml`.

Procedure

- In the example configuration below, an `address-setting` is set to BLOCK producers from sending messages after reaching its maximum size of 300000 bytes.

```xml
<configuration>
  <core>
    ...
    <address-settings>
      <address-setting match="my.blocking.queue">
        <max-size-bytes>300000</max-size-bytes>
        <address-full-policy>BLOCK</address-full-policy>
      </address-setting>
    </address-settings>
  </core>
</configuration>
```

1. The above configuration applies to any queue referenced by the `my.blocking.queue` address.
2. Sets the maximum size to 300000 bytes. The broker will block producers from sending to the address if the message exceeds `max-size-bytes`. Note that this element supports byte notation such as "K", "Mb", and "GB".
3. Sets the `address-full-policy` to BLOCK to enable blocking producer flow control.

11.2.3. Blocking AMQP Messages

As explained earlier in this chapter the Core protocol uses a producer window-size flow control system. In this system, credits represent bytes and are allocated to producers. If a producer wants to send a message, it must wait until it has sufficient credits to accommodate the size of a message before sending it.

AMQP flow control credits are not representative of bytes, however, but instead represent the number of messages a producer is permitted to send, regardless of the message size. It is therefore possible in some scenarios for an AMQP client to significantly exceed the `max-size-bytes` of an address.

To manage this situation, add the element `max-size-bytes-reject-threshold` to the `address-setting` to specify an upper bound on an address size in bytes. Once this upper bound is reached, the broker rejects AMQP messages. By default, `max-size-bytes-reject-threshold` is set to -1, or no limit.

Configuring the Broker to Block AMQP Messages

To configure the broker to block AMQP messages if they are larger than the set maximum number of bytes, add a new `address-setting` configuration element to `BROKER_INSTANCE_DIR/etc/broker.xml`. 
Procedure

- The example configuration below applies a maximum size of 300000 bytes to any AMQP message routed to the my.amqp.blocking.queue address.

```
<configuration>
  <core>
    ...
    <address-settings>
      ...
      <address-setting match="my.amqp.blocking.queue">
        <max-size-bytes-reject-threshold>300000</max-size-bytes-reject-threshold>
      </address-setting>
    </address-settings>
  </core>
</configuration>
```

1. The above configuration applies to any queue referenced by the my.amqp.blocking.queue address.

2. The broker is configured to reject AMQP messages sent to queues matching this address if they are larger than the max-size-bytes-reject-threshold of 300000 bytes. Note that this element does not support byte notation such as K, Mb, and GB.

11.2.4. Setting the Rate of Sending Messages

AMQ Broker can also limit the rate a producer can emit messages. The producer rate is specified in units of messages per second. Setting it to -1, the default, disables rate-limited flow control.

Setting the Rate of Sending Messages

The examples below demonstrate how to set the rate of sending messages when the producer is using a Core JMS client. Each example sets the maximum rate of sending messages to 10 per second.

Procedure

- Set the rate that a producer can send messages.

  - If the Core JMS Client uses JNDI to instantiate its connection factory, include the producerMaxRate parameter as part of the connection string URL. Store the URL within a JNDI context environment. The example below uses a jndi.properties file to store the URL.

    ```java
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    java.naming.provider.url=tcp://localhost:61616?producerMaxRate=10
    ```

  - If the Core JMS client does not use JNDI to instantiate its connection factory, pass the value to ActiveMQConnectionFactory.setProducerMaxRate().

    ```java
    ConnectionFactory cf = ActiveMQJMSClient.createConnectionFactory(...)
    cf.setProducerMaxRate(10);
    ```

Related Information
See the `producer-rate-limit` example in `INSTALL_DIR/examples/standard` for a working example of how to limit the rate of sending messages.
CHAPTER 12. MESSAGE GROUPING

Message groups are sets of messages that have the following characteristics:

- Messages in a message group share the same group ID, that is, they have the same group identifier property. For JMS messages, the property is `JMSXGroupID`.
- Messages in a message group are always consumed by the same consumer, even if there are many consumers on a queue. Another consumer is chosen to receive a message group if the original consumer closes.

Message groups are useful when you want all messages for a certain value of the property to be processed serially by the same consumer. For example, you may want orders for any particular stock purchase to be processed serially by the same consumer. To do this, you could create a pool of consumers, then set the stock name as the value of the message property. This ensures that all messages for a particular stock are always processed by the same consumer.

**NOTE**

Grouped messages might impact the concurrent processing of non-grouped messages due to the underlying FIFO semantics of a queue. For example, if there is a chunk of 100 grouped messages at the head of a queue followed by 1,000 non-grouped messages, all the grouped messages are sent to the appropriate client before any of the non-grouped messages are consumed. The functional impact in this scenario is a temporary suspension of concurrent message processing while all the grouped messages are processed. Keep this potential performance bottleneck in mind when determining the size of your message groups. Consider whether to isolate your grouped messages from your non-grouped messages.

12.1. CLIENT-SIDE MESSAGE GROUPING

The examples below show how to use message grouping using Core JMS clients.

**Procedure**

- Set the group ID.
  - If you are using JNDI to establish a JMS connection factory for your JMS client, add the `groupID` parameter and supply a value. All messages sent using this connection factory have the property `JMSXGroupID` set to the specified value.

    ```java
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    connectionFactory.myConnectionFactory=tcp://localhost:61616?groupID=MyGroup
    ```
  - If you are not using JNDI, set the `JMSXGroupID` property using the `setStringProperty()` method.

    ```java
    Message message = new TextMessage();
    message.setStringProperty("JMSXGroupID", "MyGroup");
    producer.send(message);
    ```

**Related Information**
See `message-group` and `message-group2` under `INSTALL_DIR/examples/features/standard` for working examples of how message groups are configured and used.

### 12.2. AUTOMATIC MESSAGE GROUPING

Instead of supplying a group ID yourself, you can have the ID automatically generated for you. Messages grouped in this way are still processed serially by a single consumer.

**Procedure**

The examples below show how to enable message grouping using Core JMS clients.

- Enable automatic generation of the group ID.
  - If you are using a JNDI context environment to instantiate your JMS connection factory, add the `autogroup=true` name-value pair to the query string of the connection URL.
    
    ```java
    java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
    connectionFactory.myConnectionFactory=tcp://localhost:61616?autoGroup=true
    ```
  - If you are not using JNDI, set `autogroup` to `true` on the `ActiveMQConnectionFactory`.
    
    ```java
    ActiveMQConnectionFactory cf = ActiveMQJMSClient.createConnectionFactoryWithoutHA(...);
    cf.setAutoGroup(true);
    ```
CHAPTER 13. DUPLICATE MESSAGE DETECTION

AMQ Broker includes automatic duplicate message detection, which filters out any duplicate messages it receives so you do not have to code your own duplicate detection logic.

Without duplicate detection, a client cannot determine whether a message it sent was successful whenever the target broker or the connection to it fails. For example, if the broker or connection fails before the message was received and processed by the broker, the message never arrives at its address, and the client does not receive a response from the broker due to the failure. On the other hand, if the broker or connection failed after a message was received and processed by the broker, the message is routed correctly, but the client still does not receive a response.

Moreover, using a transaction to determine success does not help in these cases. If the broker or connection fails while the transaction commit is being processed, for example, the client is still unable to determine whether it successfully sent the message.

If the client resends the last message in an effort to correct the assumed failure, the result could be a duplicate message being sent to the address, which could negatively impact your system. Sending a duplicate message could mean that a purchase order is fulfilled twice, for example. Fortunately, [AMQ Broker] provides automatic duplicate messages detection as a way to prevent these kind of issues from happening.

13.1. USING THE DUPLICATE ID MESSAGE PROPERTY

To enable duplicate message detection provide a unique value for the message property _AMQ_DUPL_ID. When a broker receives a message, it checks if _AMQ_DUPL_ID has a value. If it does, the broker then checks in its memory cache to see if it has already received a message with that value. If a message with the same value is found, the incoming message is ignored.

Procedure

The examples below illustrate how to set the duplicate detection property using a Core JMS Client. Note that for convenience, the clients use the value of the constant org.apache.activemq.artemis.api.core.Message.HDR_DUPLICATE_DETECTION_ID for the name of the duplicate ID property, _AMQ_DUPL_ID.

- Set the value for _AMQ_DUPL_ID to a unique String.

```java
Message jmsMessage = session.createMessage();
String myUniqueID = "This is my unique id";
message.setStringProperty(HDR_DUPLICATE_DETECTION_ID.toString(), myUniqueID);
```

13.2. CONFIGURING THE DUPLICATE ID CACHE

The broker maintains caches of received values of the _AMQ_DUPL_ID property. Each address has its own distinct cache. The cache is circular and fixed. New entries replace the oldest ones as cache space demands.

NOTE

Be sure to size the cache appropriately. If a previous message arrived more than id-cache-size messages before the arrival of a new message with the same _AMQ_DUPL_ID, the broker cannot detect the duplicate. This results in both messages being processed by the broker.
Procedure

The example configuration below illustrates how to configure the ID cache by adding elements to

```
BROKER_INSTANCE_DIR/etc/broker.xml
```

The maximum size of the cache is configured by the parameter `id-cache-size`. The default value is

```
20000
```

entries. In the example above, the cache size is set to

```
5000
```

entries.

Set `persist-id-cache` to `true` to have each ID persisted to disk as they are received. The default

value is `true`. In the example above, persistence is disabled by setting the value to `false`.

---

### 13.3. DUPLICATE DETECTION AND TRANSACTIONS

Using duplicate detection to move messages between brokers can give you the same once and only once delivery guarantees as using an XA transaction to consume messages, but with less overhead and much easier configuration than using XA.

If you are sending messages in a transaction, you do not have to set `_AMQ_DUPL_ID` for every message in the transaction, but only in one of them. If the broker detects a duplicate message for any message in the transaction, it ignores the entire transaction.

### 13.4. DUPLICATE DETECTION AND CLUSTER CONNECTIONS

You can configure cluster connections to insert a duplicate ID for each message they move across the cluster.

Procedure

- Add the element `use-duplicate-detection` to the configuration of the desired cluster connection found in `BROKER_INSTANCE_DIR/etc/broker.xml`. Note that the default value for this parameter is `true`. In the example below, the element is added to the configuration for the cluster connection `my-cluster`.

```
<configuration>
  <core>
    ...
    <cluster-connection>
      <cluster-connection name="my-cluster"> 2
        <use-duplicate-detection>true</use-duplicate-detection>
      </cluster-connection>
    ...
  </cluster-connections>
</configuration>
```
Related Information

For more information about broker clusters, see Section 16.2, “Creating a broker cluster”.

CHAPTER 14. INTERCEPTING MESSAGES

With AMQ Broker you can intercept packets entering or exiting the broker, allowing you to audit packets or filter messages. Interceptors can change the packets they intercept, which makes them powerful, but also potentially dangerous.

You can develop interceptors to meet your business requirements. Interceptors are protocol specific and must implement the appropriate interface.

Interceptors must implement the `intercept()` method, which returns a boolean value. If the value is `true`, the message packet continues onward. If `false`, the process is aborted, no other interceptors are called, and the message packet is not processed further.

14.1. CREATING INTERCEPTORS

You can create your own incoming and outgoing interceptors. All interceptors are protocol specific and are called for any packet entering or exiting the server respectively. This allows you to create interceptors to meet business requirements such as auditing packets. Interceptors can change the packets they intercept. This makes them powerful as well as potentially dangerous, so be sure to use them with caution.

Interceptors and their dependencies must be placed in the Java classpath of the broker. You can use the `BROKER_INSTANCE_DIR/lib` directory since it is part of the classpath by default.

Procedure

The following examples demonstrate how to create an interceptor that checks the size of each packet passed to it. Note that the examples implement a specific interface for each protocol.

- Implement the appropriate interface and override its `intercept()` method.

  - If you are using the AMQP protocol, implement the `org.apache.activemq.artemis.protocol.amqp.broker.AmqpInterceptor` interface.

    ```java
    package com.example;

    import org.apache.activemq.artemis.protocol.amqp.broker.AMQPMessage;
    import org.apache.activemq.artemis.protocol.amqp.broker.AmqpInterceptor;
    import org.apache.activemq.artemis.spi.core.protocol.RemotingConnection;

    public class MyInterceptor implements AmqpInterceptor {
        private final int ACCEPTABLE_SIZE = 1024;

        @Override
        public boolean intercept(final AMQPMessage message, RemotingConnection connection) {
            int size = message.getEncodeSize();
            if (size <= ACCEPTABLE_SIZE) {
                System.out.println("This AMQPMessage has an acceptable size.");
                return true;
            }
            return false;
        }
    }
    ```
If you are using the Core protocol, your interceptor must implement the
org.apache.activemq.activemq.api.core.Interceptor interface.

package com.example;
import org.apache.activemq.activemq.api.core.Interceptor;
import org.apache.activemq.activemq.core.protocol.core.Packet;
import org.apache.activemq.activemq.activemq.core.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements Interceptor
{
    private final int ACCEPTABLE_SIZE = 1024;

    @Override
    boolean intercept(Packet packet, RemotingConnection connection)
        throws ActiveMQException
    {
        int size = packet.getPacketSize();
        if (size <= ACCEPTABLE_SIZE) {
            System.out.println("This Packet has an acceptable size.");
            return true;
        }
        return false;
    }
}

If you are using the MQTT protocol, implement the
org.apache.activemq.activemq.core.protocol.mqtt.MQTTInterceptor interface.

package com.example;
import org.apache.activemq.activemq.core.protocol.mqtt.MQTTInterceptor;
import io.netty.handler.codec.mqtt.MqttMessage;
import org.apache.activemq.activemq.activemq.core.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements Interceptor
{
    private final int ACCEPTABLE_SIZE = 1024;

    @Override
    boolean intercept(MqttMessage mqttMessage, RemotingConnection connection)
        throws ActiveMQException
    {
        byte[] msg = (mqttMessage.toString()).getBytes();
        int size = msg.length;
        if (size <= ACCEPTABLE_SIZE) {
            System.out.println("This MqttMessage has an acceptable size.");
            return true;
        }
        return false;
    }
}

If you are using the Stomp protocol, implement the
14.2. CONFIGURING THE BROKER TO USE INTERCEPTORS

Once you have created an interceptor, you must configure the broker to use it.

Prerequisites

You must create an interceptor class and add it (and its dependencies) to the Java classpath of the broker before you can configure it for use by the broker. You can use the `BROKER_INSTANCE_DIR/lib` directory since it is part of the classpath by default.

Procedure

- Configure the broker to use an interceptor by adding configuration to `BROKER_INSTANCE_DIR/etc/broker.xml`
  
  - If your interceptor is intended for incoming messages, add its `class-name` to the list of `remoting-incoming-interceptors`
  
    ```xml
    <configuration>
    <core>
        ...
        <remoting-incoming-interceptors>
            <class-name>org.example.MyIncomingInterceptor</class-name>
        </remoting-incoming-interceptors>
    ...
    </core>
    </configuration>
    
    - If your interceptor is intended for outgoing messages, add its `class-name` to the list of `remoting-outgoing-interceptors`.
      
      ```xml
      ...<configuration>
      ```

```java
package com.example;

import org.apache.activemq.artemis.core.protocol.stomp.StompFrameInterceptor;
import org.apache.activemq.artemis.core.protocol.stomp.StompFrame;
import org.apache.activemq.artemis.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements Interceptor {
    private final int ACCEPTABLE_SIZE = 1024;

    @Override
    boolean intercept(StompFrame stompFrame, RemotingConnection connection) throws ActiveMQException {
        int size = stompFrame.getEncodedSize();
        if (size <= ACCEPTABLE_SIZE) {
            System.out.println("This StompFrame has an acceptable size.");
            return true;
        }
        return false;
    }
}
```
14.3. INTERCEPTORS ON THE CLIENT SIDE

Clients can use interceptors to intercept packets either sent by the client to the server or by the server to the client. As in the case of a broker-side interceptor, if it returns false, no other interceptors are called and the client does not process the packet further. This process happens transparently to the client except when an outgoing packet is sent in a blocking fashion. In those cases, an ActiveMQException is thrown to the caller because blocking sends provides reliability. The ActiveMQException thrown contains the name of the interceptor that returned false.

As on the server, the client interceptor classes and their dependencies must be added to the Java classpath of the client to be properly instantiated and invoked.

```xml
<core>
  ...
  <remoting-outgoing-interceptors>
    <class-name>org.example.MyOutgoingInterceptor</class-name>
  </remoting-outgoing-interceptors>
</core>
</configuration>
```
CHAPTER 15. FILTERING MESSAGES

AMQ Broker provides a powerful filter language based on a subset of the SQL 92 expression syntax. The filter language uses the same syntax as used for JMS selectors, but the predefined identifiers are different. The table below lists the identifiers that apply to a AMQ Broker message.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMQPriority</td>
<td>The priority of a message. Message priorities are integers with valid values from 0 through 9. 0 is the lowest priority and 9 is the highest.</td>
</tr>
<tr>
<td>AMQExpiration</td>
<td>The expiration time of a message. The value is a long integer.</td>
</tr>
<tr>
<td>AMQDurable</td>
<td>Whether a message is durable or not. The value is a string. Valid values are DURABLE or NON_DURABLE.</td>
</tr>
<tr>
<td>AMQTimestamp</td>
<td>The timestamp of when the message was created. The value is a long integer.</td>
</tr>
<tr>
<td>AMQSize</td>
<td>The value of the encodeSize property of the message. The value of encodeSize is the space, in bytes, that the message takes up in the journal.</td>
</tr>
<tr>
<td></td>
<td>Because the broker uses a double-byte character set to encode messages, the actual size of the message is half the value of encodeSize.</td>
</tr>
</tbody>
</table>

Any other identifiers used in core filter expressions are assumed to be properties of the message. For documentation on selector syntax for JMS Messages, see the Java EE API.

15.1. CONFIGURING A QUEUE TO USE A FILTER

You can add a filter to the queues you configure in `BROKER_INSTANCE_DIR/etc/broker.xml`. Only messages that match the filter expression enter the queue.

Procedure

- Add the `filter` element to the desired `queue` and include the filter you want to apply as the value of the element. In the example below, the filter `NEWS='technology'` is added to the queue `technologyQueue`.

```xml
<configuration>
  <core>
    ...
    <addresses>
      <address name="myQueue">
        <anycast>
          <queue name="myQueue">
            <filter string="NEWS='technology'"/>
          </queue>
        </anycast>
      </address>
    </addresses>
  </core>
</configuration>
```
15.2. FILTERING JMS MESSAGE PROPERTIES

The JMS specification states that a String property must not be converted to a numeric type when used in a selector. For example, if a message has the age property set to the String value 21, the selector age > 18 must not match it. This restriction limits STOMP clients because they can send only messages with String properties.

The JMS specification also states that hyphens cannot be used as property identifiers, making them unavailable for use in filters. However, this constraint can be overcome by using the hyphenated_props: prefix.

Configuring a Filter to Convert a String to a Number
To convert String properties to a numeric type, add the prefix convert_string_expressions: to the value of the filter.

Procedure

- Edit BROKER_INSTANCE_DIR/etc/broker.xml by applying the prefix convert_string_expressions: to the desired filter. The example below edits the filter value from age > 18 to convert_string_expressions:age > 18.

<configuration>
  <core>
    ...
    <addresses>
      <address name="myQueue">
        <anycast>
          <queue name="myQueue">
            <filter string="convert_string_expressions='age > 18'"/>
          </queue>
        </anycast>
      </address>
    </addresses>
  </core>
</configuration>

Enabling a Filter to Use Hyphens
To enable the use of hyphens when filtering JMS properties, add the prefix hyphenated_props: to the value of the filter.

Procedure

- Edit BROKER_INSTANCE_DIR/etc/broker.xml by applying the prefix hyphenated_props: to the desired filter. In the example below, a filter is edited so that it can select for the hyphenated property foo-bar.

<configuration>
  <core>
    ...
    <addresses>
<address name="myQueue">
  <anycast>
    <queue name="myQueue">
      <filter string="hyphenated_props='foo-bar = 0'"/>
    </queue>
  </anycast>
</address>
</addresses>
</core>
</configuration>
CHAPTER 16. SETTING UP A BROKER CLUSTER

A cluster consists of multiple broker instances that have been grouped together. Broker clusters enhance performance by distributing the message processing load across multiple brokers. In addition, broker clusters can minimize downtime through high availability.

You can connect brokers together in many different cluster topologies. Within the cluster, each active broker manages its own messages and handles its own connections.

You can also balance client connections across the cluster and redistribute messages to avoid broker starvation.

16.1. UNDERSTANDING BROKER CLUSTERS

Before creating a broker cluster, you should understand some important clustering concepts.

16.1.1. How broker clusters balance message load

When brokers are connected to form a cluster, AMQ Broker automatically balances the message load between the brokers. This ensures that the cluster can maintain high message throughput.

Consider a symmetric cluster of four brokers. Each broker is configured with a queue named \textbf{OrderQueue}. The \textbf{OrderProducer} client connects to \textbf{Broker1} and sends messages to \textbf{OrderQueue}. \textbf{Broker1} forwards the messages to the other brokers in round-robin fashion. The \textbf{OrderConsumer} clients connected to each broker consume the messages. The exact order depends on the order in which the brokers started.
Without message load balancing, the messages sent to Broker1 would stay on Broker1 and only OrderConsumer1 would be able to consume them.

While AMQ Broker automatically load balances messages by default, you can configure the cluster to only load balance messages to brokers that have a matching consumer. You can also configure message redistribution to automatically redistribute messages from queues that do not have any consumers to queues that do have consumers.

Additional resources

- The message load balancing policy is configured with the `message-load-balancing` property in each broker’s cluster connection. For more information, see Appendix C, Cluster Connection Configuration Elements.

- For more information about message redistribution, see Section 16.4, “Enabling message redistribution”.

16.1.2. How broker clusters improve reliability

Broker clusters make high availability and failover possible, which makes them more reliable than standalone brokers. By configuring high availability, you can ensure that client applications can continue to send and receive messages even if a broker encounters a failure event.

With high availability, the brokers in the cluster are grouped into live-backup groups. A live-backup group consists of a live broker that serves client requests, and one or more backup brokers that wait...
passively to replace the live broker if it fails. If a failure occurs, the backup brokers replaces the live broker in its live-backup group, and the clients reconnect and continue their work.

16.1.3. Common broker cluster topologies

You can connect brokers to form either a symmetric or chain cluster topology. The topology you implement depends on your environment and messaging requirements.

Symmetric clusters
In a symmetric cluster, every broker is connected to every other broker. This means that every broker is no more than one hop away from every other broker.

Figure 16.2. Symmetric cluster

Each broker in a symmetric cluster is aware of all of the queues that exist on every other broker in the cluster and the consumers that are listening on those queues. Therefore, symmetric clusters are able to load balance and redistribute messages more optimally than a chain cluster.

Symmetric clusters are easier to set up than chain clusters, but they can be difficult to use in environments in which network restrictions prevent brokers from being directly connected.

Chain clusters
In a chain cluster, each broker in the cluster is not connected to every broker in the cluster directly. Instead, the brokers form a chain with a broker on each end of the chain and all other brokers just connecting to the previous and next brokers in the chain.
Chain clusters are more difficult to set up than symmetric clusters, but can be useful when brokers are on separate networks and cannot be directly connected. By using a chain cluster, an intermediary broker can indirectly connect two brokers to enable messages to flow between them even though the two brokers are not directly connected.

16.1.4. Broker discovery methods

Discovery is the mechanism by which brokers in a cluster propagate their connection details to each other. AMQ Broker supports both dynamic discovery and static discovery.

Dynamic discovery
Each broker in the cluster broadcasts its connection settings to the other members through either UDP multicast or JGroups. In this method, each broker uses:

- A broadcast group to push information about its cluster connection to other potential members of the cluster.
- A discovery group to receive and store cluster connection information about the other brokers in the cluster.

Static discovery
If you are not able to use UDP or JGroups in your network, or if you want to manually specify each member of the cluster, you can use static discovery. In this method, a broker "joins" the cluster by connecting to a second broker and sending its connection details. The second broker then propagates those details to the other brokers in the cluster.

16.1.5. Cluster sizing considerations

Before creating a broker cluster, consider your messaging throughput, topology, and high availability requirements. These factors affect the number of brokers to include in the cluster.
NOTE
After creating the cluster, you can adjust the size by adding and removing brokers. You can add and remove brokers without losing any messages.

Messaging throughput
The cluster should contain enough brokers to provide the messaging throughput that you require. The more brokers in the cluster, the greater the throughput. However, large clusters can be complex to manage.

Topology
You can create either symmetric clusters or chain clusters. The type of topology you choose affects the number of brokers you may need.

For more information, see Section 16.1.3, “Common broker cluster topologies”.

High availability
If you require high availability (HA), consider choosing an HA policy before creating the cluster. The HA policy affects the size of the cluster, because each master broker should have at least one slave broker.

For more information, see Section 16.3, “Implementing high availability”.

16.2. CREATING A BROKER CLUSTER

You create a broker cluster by configuring a cluster connection on each broker that should participate in the cluster. The cluster connection defines how the broker should connect to the other brokers.

You can create a broker cluster that uses static discovery or dynamic discovery (either UDP multicast or JGroups).

Prerequisites

- You should have determined the size of the broker cluster.
  For more information, see Section 16.1.5, “Cluster sizing considerations”.

16.2.1. Creating a broker cluster with static discovery

You can create a broker cluster by specifying a static list of brokers. Use this static discovery method if you are unable to use UDP multicast or JGroups on your network.

Procedure

1. Open the `<broker-instance-dir>/etc/broker.xml` configuration file.

2. Within the `<core>` element, add the following connectors:

   - A connector that defines how other brokers can connect to this one
   - One or more connectors that define how this broker can connect to other brokers in the cluster


```xml
<configuration>
  <core>
    ...
  <connectors>
```
This connector defines connection information that other brokers can use to connect to this one. This information will be sent to other brokers in the cluster during discovery.

The broker2 and broker3 connectors define how this broker can connect to two other brokers in the cluster, one of which will always be available. If there are other brokers in the cluster, they will be discovered by one of these connectors when the initial connection is made.

For more information about connectors, see Section 2.2, “About Connectors”.

3. Add a cluster connection and configure it to use static discovery.
   By default, the cluster connection will load balance messages for all addresses in a symmetric topology.

```
<configuration>
  <core>
    ...
    <cluster-connections>
      <cluster-connection name="my-cluster">
        <connector-ref>netty-connector</connector-ref>
        <static-connectors>
          <connector-ref>broker2-connector</connector-ref>
          <connector-ref>broker3-connector</connector-ref>
        </static-connectors>
      </cluster-connection>
      ...
    </cluster-connections>
  ...
  </core>
</configuration>
```

**cluster-connection**

Use the **name** attribute to specify the name of the cluster connection.

**connector-ref**

The connector that defines how other brokers can connect to this one.

**static-connectors**

One or more connectors that this broker can use to make an initial connection to another broker in the cluster. After making this initial connection, the broker will discover the other brokers in the cluster. You only need to configure this property if the cluster uses static discovery.

4. Configure any additional properties for the cluster connection.
   These additional cluster connection properties have default values that are suitable for most common use cases. Therefore, you only need to configure these properties if you do not want the default behavior. For more information, see Appendix C, Cluster Connection Configuration Elements.
5. Create the cluster user and password.
 AMQ Broker ships with default cluster credentials, but you should change them to prevent unauthorized remote clients from using these default credentials to connect to the broker.

**IMPORTANT**

The cluster password must be the same on every broker in the cluster.

```xml
<configuration>
  <core>
    ...
    <cluster-user>cluster_user</cluster-user>
    <cluster-password>cluster_user_password</cluster-password>
    ...
  </core>
</configuration>
```

6. Repeat this procedure on each additional broker.
 You can copy the cluster configuration to each additional broker. However, do not copy any of the other AMQ Broker data files (such as the bindings, journal, and large messages directories). These files must be unique among the nodes in the cluster or the cluster will not form properly.

Additional resources

- For an example of a broker cluster that uses static discovery, see the [clustered-static-discovery AMQ Broker example program](#).

### 16.2.2. Creating a broker cluster with UDP-based dynamic discovery

You can create a broker cluster in which the brokers discover each other dynamically through UDP multicast.

**Procedure**

1. Open the `<broker-instance-dir>/etc/broker.xml` configuration file.

2. Within the `<core>` element, add a connector.
 This connector defines connection information that other brokers can use to connect to this one. This information will be sent to other brokers in the cluster during discovery.

```xml
<configuration>
  <core>
    ...
    <connectors>
      <connector name="netty-connector">tcp://localhost:61617</connector>
    </connectors>
    ...
  </core>
</configuration>
```

3. Add a UDP broadcast group.
The broadcast group enables the broker to push information about its cluster connection to the other brokers in the cluster. This broadcast group uses UDP to broadcast the connection settings:

```xml
<configuration>
  <core>
    ...
    <broadcast-groups>
      <broadcast-group name="my-broadcast-group">
        <local-bind-address>172.16.9.3</local-bind-address>
        <local-bind-port>-1</local-bind-port>
        <group-address>231.7.7.7</group-address>
        <group-port>9876</group-port>
        <broadcast-period>2000</broadcast-period>
        <connector-ref>netty-connector</connector-ref>
      </broadcast-group>
    </broadcast-groups>
    ...
  </core>
</configuration>
```

The following parameters are required unless otherwise noted:

**broadcast-group**

Use the `name` attribute to specify a unique name for the broadcast group.

**local-bind-address**

The address to which the UDP socket is bound. If you have multiple network interfaces on your broker, you should specify which one you want to use for broadcasts. If this property is not specified, the socket will be bound to an IP address chosen by the operating system. This is a UDP-specific attribute.

**local-bind-port**

The port to which the datagram socket is bound. In most cases, use the default value of `-1`, which specifies an anonymous port. This parameter is used in connection with `local-bind-address`. This is a UDP-specific attribute.

**group-address**

The multicast address to which the data will be broadcast. It is a class D IP address in the range `224.0.0.0` - `239.255.255.255` inclusive. The address `224.0.0.0` is reserved and is not available for use. This is a UDP-specific attribute.

**group-port**

The UDP port number used for broadcasting. This is a UDP-specific attribute.

**broadcast-period (optional)**

The interval in milliseconds between consecutive broadcasts. The default value is 2000 milliseconds (2 seconds).

**connector-ref**

The previously configured cluster connector that should be broadcasted.

4. Add a UDP discovery group.

The discovery group defines how this broker receives connector information from other brokers. The broker maintains a list of connectors (one entry for each broker). As it receives broadcasts from a broker, it updates its entry. If it does not receive a broadcast from a broker for a length of time, it removes the entry.
This discovery group uses UDP to discover the brokers in the cluster:

```xml
<configuration>
  <core>
    ...<discovery-groups>
      <discovery-group name="my-discovery-group">
        <local-bind-address>172.16.9.7</local-bind-address>
        <group-address>231.7.7.7</group-address>
        <group-port>9876</group-port>
        <refresh-timeout>10000</refresh-timeout>
      </discovery-group>
      <discovery-groups>
    ...<core>
  </configuration>

The following parameters are required unless otherwise noted:

**discovery-group**

Use the `name` attribute to specify a unique name for the discovery group.

**local-bind-address (optional)**

If the machine on which the broker is running uses multiple network interfaces, you can specify the network interface to which the discovery group should listen. This is a UDP-specific attribute.

**group-address**

The multicast address of the group on which to listen. It should match the `group-address` in the broadcast group that you want to listen from. This is a UDP-specific attribute.

**group-port**

The UDP port number of the multicast group. It should match the `group-port` in the broadcast group that you want to listen from. This is a UDP-specific attribute.

**refresh-timeout (optional)**

The amount of time in milliseconds that the discovery group waits after receiving the last broadcast from a particular broker before removing that broker’s connector pair entry from its list. The default is 10000 milliseconds (10 seconds). Set this to a much higher value than the `broadcast-period` on the broadcast group. Otherwise, brokers might periodically disappear from the list even though they are still broadcasting (due to slight differences in timing).

5. Create a cluster connection and configure it to use dynamic discovery.
By default, the cluster connection will load balance messages for all addresses in a symmetric topology.

```xml
<configuration>
  <core>
    ...<cluster-connections>
      <cluster-connection name="my-cluster">
        <connector-ref>netty-connector</connector-ref>
        <discovery-group-ref discovery-group-name="my-discovery-group"/>
      </cluster-connection>
    </cluster-connections>
  </core>
</configuration>
6. Configure any additional properties for the cluster connection. These additional cluster connection properties have default values that are suitable for most common use cases. Therefore, you only need to configure these properties if you do not want the default behavior. For more information, see Appendix C, Cluster Connection Configuration Elements.

7. Create the cluster user and password. AMQ Broker ships with default cluster credentials, but you should change them to prevent unauthorized remote clients from using these default credentials to connect to the broker.

   IMPORTANT

   The cluster password must be the same on every broker in the cluster.

8. Repeat this procedure on each additional broker. You can copy the cluster configuration to each additional broker. However, do not copy any of the other AMQ Broker data files (such as the bindings, journal, and large messages directories). These files must be unique among the nodes in the cluster or the cluster will not form properly.

Additional resources

- For an example of a broker cluster configuration that uses dynamic discovery with UDP, see the clustered-queue AMQ Broker example program.

16.2.3. Creating a broker cluster with JGroups-based dynamic discovery

If you are already using JGroups in your environment, you can use it to create a broker cluster in which the brokers discover each other dynamically.

Prerequisites
JGroups must be installed and configured. For an example of a JGroups configuration file, see the `clustered-jgroups` AMQ Broker example program.

**Procedure**

1. Open the `<broker-instance-dir>/etc/broker.xml` configuration file.

2. Within the `<core>` element, add a connector.
   This connector defines connection information that other brokers can use to connect to this one. This information will be sent to other brokers in the cluster during discovery.

   ```xml
   <configuration>
   <core>
     ...
     <connectors>
       <connector name="netty-connector">tcp://localhost:61617</connector>
     </connectors>
     ...
   </core>
   </configuration>
   ``

3. Within the `<core>` element, add a JGroups broadcast group.
   The broadcast group enables the broker to push information about its cluster connection to the other brokers in the cluster. This broadcast group uses JGroups to broadcast the connection settings:

   ```xml
   <configuration>
   <core>
     ...
     <broadcast-groups>
       <broadcast-group name="my-broadcast-group">
         <jgroups-file>test-jgroups-file_ping.xml</jgroups-file>
         <jgroups-channel>activemq_broadcast_channel</jgroups-channel>
         <broadcast-period>2000</broadcast-period>
         <connector-ref>netty-connector</connector-ref>
       </broadcast-group>
     </broadcast-groups>
     ...
   </core>
   </configuration>
   ``

The following parameters are required unless otherwise noted:

**broadcast-group**

   Use the `name` attribute to specify a unique name for the broadcast group.

**jgroups-file**

   The name of JGroups configuration file to initialize JGroups channels. The file must be in the Java resource path so that the broker can load it.

**jgroups-channel**

   The name of the JGroups channel to connect to for broadcasting.

**broadcast-period (optional)**
The interval in milliseconds between consecutive broadcasts. The default value is 2000 milliseconds (2 seconds).

**connector-ref**

The previously configured cluster connector that should be broadcasted.

4. Add a JGroups discovery group.

The discovery group defines how connector information is received. The broker maintains a list of connectors (one entry for each broker). As it receives broadcasts from a broker, it updates its entry. If it does not receive a broadcast from a broker for a length of time, it removes the entry.

This discovery group uses JGroups to discover the brokers in the cluster:

```xml
<configuration>
  <core>
    ...
    <discovery-groups>
      <discovery-group name="my-discovery-group">
        <jgroups-file>test-jgroups-file_ping.xml</jgroups-file>
        <jgroups-channel>activemq_broadcast_channel</jgroups-channel>
        <refresh-timeout>10000</refresh-timeout>
      </discovery-group>
      ...
    </discovery-groups>
  ...
</configuration>
```

The following parameters are required unless otherwise noted:

**discovery-group**

Use the *name* attribute to specify a unique name for the discovery group.

**jgroups-file**

The name of JGroups configuration file to initialize JGroups channels. The file must be in the Java resource path so that the broker can load it.

**jgroups-channel**

The name of the JGroups channel to connect to for receiving broadcasts.

**refresh-timeout (optional)**

The amount of time in milliseconds that the discovery group waits after receiving the last broadcast from a particular broker before removing that broker’s connector pair entry from its list. The default is 10000 milliseconds (10 seconds).

Set this to a much higher value than the *broadcast-period* on the broadcast group. Otherwise, brokers might periodically disappear from the list even though they are still broadcasting (due to slight differences in timing).

5. Create a cluster connection and configure it to use dynamic discovery.

By default, the cluster connection will load balance messages for all addresses in a symmetric topology.

```xml
<configuration>
  <core>
    ...
    <cluster-connections>
```
Use the `name` attribute to specify the name of the cluster connection.

The connector that defines how other brokers can connect to this one.

The discovery group that this broker should use to locate other members of the cluster. You only need to configure this property if the cluster uses dynamic discovery.

6. Configure any additional properties for the cluster connection. These additional cluster connection properties have default values that are suitable for most common use cases. Therefore, you only need to configure these properties if you do not want the default behavior. For more information, see Appendix C, Cluster Connection Configuration Elements.

7. Create the cluster user and password. AMQ Broker ships with default cluster credentials, but you should change them to prevent unauthorized remote clients from using these default credentials to connect to the broker.

   IMPORTANT

   The cluster password must be the same on every broker in the cluster.

8. Repeat this procedure on each additional broker. You can copy the cluster configuration to each additional broker. However, do not copy any of the other AMQ Broker data files (such as the bindings, journal, and large messages directories). These files must be unique among the nodes in the cluster or the cluster will not form properly.

Additional resources

- For an example of a broker cluster that uses dynamic discovery with JGroups, see the clustered-jgroups AMQ Broker example program.

16.3. IMPLEMENTING HIGH AVAILABILITY
After creating a broker cluster, you can improve its reliability by implementing high availability (HA). With HA, the broker cluster can continue to function even if one or more brokers go offline.

Implementing HA involves several steps:

1. **Understand how HA works in AMQ Broker**. You should understand what live-backup groups are, and choose an HA policy that best meets your requirements.

2. **Configure the HA policy on each broker in the cluster**.

3. **Configure your client applications to use failover**.

### 16.3.1. Understanding high availability

In AMQ Broker, you implement high availability (HA) by grouping the brokers in the cluster into *live-backup groups*. In a live-backup group, a live broker is linked to a backup broker, which can take over for the live broker if it fails. AMQ Broker also provides several different strategies for failover (called *HA policies*) within a live-backup group.

#### 16.3.1.1. How live-backup groups provide high availability

In AMQ Broker, you implement high availability (HA) by linking together the brokers in your cluster to form *live-backup groups*. Live-backup groups provide *failover*, which means that if one broker fails, another broker can take over its message processing.

A live-backup group consists of one live broker (sometimes called the *master broker*) linked to one or more backup brokers (sometimes called *slave brokers*). The live broker serves client requests, while the backup brokers wait in passive mode. If the live broker fails, a backup broker replaces the live broker, enabling the clients to reconnect and continue their work.

#### 16.3.1.2. High availability policies

A high availability (HA) policy defines how failover happens in a live-backup group. AMQ Broker provides several different HA policies:

**Shared store (recommended)**

The live and backup brokers store their messaging data in a single directory on a shared file system (typically a storage area network, or SAN). If the live broker fails, the backup broker loads the messaging data from the shared file system and takes over for the failed live broker.

In most cases, you should use shared store instead of replication. Because shared store does not replicate data over the network, it typically provides better performance than replication. Shared store also avoids network isolation (also called "split brain") issues in which a live broker and its backup become live at the same time.
Replication

The live and backup brokers continuously synchronize their messaging data over the network. If the live broker fails, the backup broker loads the synchronized data and takes over for the failed live broker.

Data synchronization between the live and backup brokers ensures that no messaging data is lost if the live broker fails. When the live and backup brokers initially join together, the live broker replicates all of its existing data to the backup broker over the network. Once this initial phase is complete, the live broker replicates persistent data to the backup broker as the live broker receives it. This means that if the live broker drops off the network, the backup broker has all of the persistent data that the live broker has received up to that point.

Because replication synchronizes data over the network, network failures can result in network isolation in which a live broker and its backup become live at the same time.

Live-only (limited HA)

When a live broker is stopped gracefully, it copies its messages and transaction state to another live broker and then shuts down. Clients can then reconnect to the other broker to continue sending and receiving messages.

Additional resources

- For more information about the persistent message data that is shared between brokers in a live-backup group, see Section 7.1, “About Journal-based Persistence”.
16.3.1.3. Replication policy limitations

Network isolation (sometimes called “split brain”) is a limitation of the replication high availability (HA) policy. You should understand how it occurs, and how to avoid it.

Network isolation can happen if a live broker and its backup lose their connection. In this situation, both a live broker and its backup can become active at the same time. Specifically, if the backup broker can still connect to more than half of the live brokers in the cluster, it also becomes active. Because there is no message replication between the brokers in this situation, they each serve clients and process messages without the other knowing it. In this case, each broker has a completely different journal. Recovering from this situation can be very difficult and in some cases, not possible.

To avoid network isolation, consider the following:

- To eliminate any possibility of network isolation, use the shared store HA policy.
- If you do use the replication HA policy, you can reduce (but not eliminate) the chance of encountering network isolation by using at least three live-backup pairs.

16.3.2. Configuring high availability

After choosing a high availability (HA) policy, configure the policy on each broker in the cluster.

You can configure HA in any of the following ways:

- Shared store HA
- Replication HA
- Limited HA with live-only
- Colocated backups (using either shared store or replication as the HA policy)

Prerequisites

- You must have chosen the HA policy that best fits your requirements. For more information, see Section 16.3.1.2, “High availability policies”.

16.3.2.1. Configuring shared store high availability

You can use the shared store high availability (HA) policy to implement HA in a broker cluster. With shared store, both live and backup brokers access a single directory on a shared file system. If a live broker fails, the backup broker loads the message data from the shared store and takes over for the failed live broker.

In most cases, you should use shared store instead of replication. Because shared store does not replicate data over the network, it typically provides better performance than replication. Shared store also avoids network isolation (also called “split brain”) issues in which a live broker and its backup become live at the same time.

NOTE

When using shared store, the startup time for the backup broker depends on the size of the message journal. When the backup broker takes over for a failed live broker, it loads the journal from the shared store. This process can be time consuming if the journal contains a lot of data.
Prerequisites

- A shared file system must be accessible to the live and backup brokers.
  Typically, you should use a Storage Area Network (SAN) to provide the shared store. For more information about supported network file systems, see Red Hat AMQ Supported Configurations.

Procedure

1. Group the brokers in your cluster into live-backup groups.
   In most cases, a live-backup group should consist of two brokers: a live broker and a backup broker. If you have six brokers in your cluster, you would need three live-backup groups.

2. Create the first live-backup group consisting of one live broker and one backup broker.
   a. Open the live broker’s `<broker-instance-dir>/etc/broker.xml` configuration file.
      b. Verify that the live broker’s paging, bindings, journal, and large messages directories point to a shared location that the backup broker can also access.
      c. Configure the live broker to use shared store for its HA policy.

      ```xml
      <configuration>
      <core>
        ...
        <paging-directory>../sharedstore/data/paging</paging-directory>
        <bindings-directory>../sharedstore/data/bindings</bindings-directory>
        <journal-directory>../sharedstore/data/journal</journal-directory>
        <large-messages-directory>../sharedstore/data/large-messages</large-messages-directory>
        ...
      </core>
      </configuration>
      
      <configuration>
      <core>
        ...
        <ha-policy>
          <shared-store>
            <master>
              <failover-on-shutdown>true</failover-on-shutdown>
            </master>
            <shared-store>
          </ha-policy>
          ...
        </configuration>
      
      failover-on-shutdown
      If this broker is stopped normally, this property controls whether the backup broker should become live and take over.

      d. Open the backup broker’s `<broker-instance-dir>/etc/broker.xml` configuration file.
Verify that the backup broker’s paging, bindings, journal, and large messages directories point to the same shared location as the live broker.

```xml
<configuration>
  <core>
    ...
    <paging-directory>./sharedstore/data/paging</paging-directory>
    <bindings-directory>./sharedstore/data/bindings</bindings-directory>
    <journal-directory>./sharedstore/data/journal</journal-directory>
    <large-messages-directory>./sharedstore/data/large-messages</large-messages-directory>
    ...
  </core>
</configuration>
```

Configure the backup broker to use shared store for its HA policy.

```xml
<configuration>
  <core>
    ...
    <ha-policy>
      <shared-store>
        <slave>
          <failover-on-shutdown>true</failover-on-shutdown>
          <allow-failback>true</allow-failback>
        </slave>
        <shared-store>
          ...
        </shared-store>
      </shared-store>
    </ha-policy>
    ...
  </core>
</configuration>
```

**failover-on-shutdown**

If this broker has become live and then is stopped normally, this property controls whether the backup broker (the original live broker) should become live and take over.

**allow-failback**

If failover has occurred and the backup broker has taken over for the live broker, this property controls whether the backup broker should fail back to the original live broker when it restarts and reconnects to the cluster.

**NOTE**

Failback is intended for a live-backup pair (one live broker paired with a single backup broker). If the live broker is configured with multiple backups, then failback will not occur. Instead, if a failover event occurs, the backup broker will become live, and the next backup will become its backup. When the original live broker comes back online, it will not be able to initiate failback, because the broker that is now live already has a backup.

3. Repeat Step 2 for each remaining live-backup group in the cluster.
16.3.2.2. Configuring replication high availability

You can use the replication high availability (HA) policy to implement HA in a broker cluster. With replication, persistent data is synchronized between the live and backup brokers. If a live broker encounters a failure, message data is synchronized to the backup broker and it takes over for the failed live broker.

You should use replication as an alternative to shared store, if you do not have a shared file system. However, replication can result in network isolation in which a live broker and its backup become live at the same time.

NOTE
Because the live and backup brokers must synchronize their messaging data over the network, replication adds a performance overhead. This synchronization process blocks journal operations, but it does not block clients.

You can configure the maximum amount of time that journal operations can be blocked for data synchronization.

The following procedure describes how to configure HA for a six-broker cluster. In this topology, the six brokers are grouped into three live-backup pairs: each of the three live brokers is paired with a dedicated backup broker.

Replication requires at least three live-backup pairs to lessen (but not eliminate) the risk of network isolation.

Prerequisites

- You must have a broker cluster with at least six brokers.
  The six brokers will be configured into three live-backup pairs. For more information about adding brokers to a cluster, see Chapter 16, Setting up a broker cluster.

Procedure

1. Group the brokers in your cluster into live-backup groups.
   In most cases, a live-backup group should consist of two brokers: a live broker and a backup broker. If you have six brokers in your cluster, you would need three live-backup groups.

2. Create the first live-backup group consisting of one live broker and one backup broker.
   a. Open the live broker’s `<broker-instance-dir>/etc/broker.xml` configuration file.
   b. Configure the live broker to use replication for its HA policy.

```xml
<configuration>
  <core>...
    <ha-policy>
      <replication>
        <master>
          <check-for-live-server>true</check-for-live-server>
          <group-name>my-group-1</group-name>
        </master>
      </replication>
    </ha-policy>
  </core>
</configuration>
```
check-for-live-server

If the live broker fails, this property controls whether clients should fail back to it when it restarts.
If you set this to true, when the broker restarts, it searches for another broker in the cluster with the same cluster node ID. If it finds one, it synchronizes its data with it and then requests that the other broker shut down. The live broker then resumes its active role, and clients reconnect to it.

WARNING
If you restart a live broker after failover has occurred, then the value for check-for-live-server must be set to true. Otherwise, the live broker restarts and processes the same messages that its backup broker has already handled, causing duplicates.

group-name

A name for this live-backup group. To form a live-backup group, the live and backup brokers must be configured with the same group name.

c. Configure any additional HA properties for the live broker.
These additional HA properties have default values that are suitable for most common use cases. Therefore, you only need to configure these properties if you do not want the default behavior. For more information, see Appendix F, Replication High Availability Configuration Elements.

d. Open the backup broker’s <broker-instance-dir>/etc/broker.xml configuration file.

e. Configure the backup broker to use replication for its HA policy.

```xml
<configuration>
  <core>
    ...
    <ha-policy>
      <replication>
        <slave>
          <allow-failback>true</allow-failback>
          <group-name>my-group-1</group-name>
          ...
        </slave>
      </replication>
    </ha-policy>
    ...
  </core>
</configuration>
```
allow-failback

If failover has occurred and the backup broker has taken over for the live broker, this property controls whether the backup broker should fail back to the original live broker when it restarts and reconnects to the cluster.

NOTE

Failback is intended for a live-backup pair (one live broker paired with a single backup broker). If the live broker is configured with multiple backups, then failback will not occur. Instead, if a failover event occurs, the backup broker will become live, and the next backup will become its backup. When the original live broker comes back online, it will not be able to initiate failback, because the broker that is now live already has a backup.

group-name

The group name of the live broker to which this backup should connect. A backup broker connects only to a live broker that shares the same group name.

1. Configure any additional HA properties for the backup broker.
   These additional HA properties have default values that are suitable for most common use cases. Therefore, you only need to configure these properties if you do not want the default behavior. For more information, see Appendix F, Replication High Availability Configuration Elements.

3. Repeat Step 2 for each additional live-backup group in the cluster.
   If there are six brokers in the cluster, you would repeat this procedure two more times: once for each remaining live-backup group.

Additional resources
   - For examples of broker clusters that use replication for HA, see the HA example programs.

16.3.2.3. Configuring limited high availability with live-only

The live-only HA policy enables you to shut down a broker in a cluster without losing any messages. With live-only, when a live broker is stopped gracefully, it copies its messages and transaction state to another live broker and then shuts down. Clients can then reconnect to the other broker to continue sending and receiving messages.

The live-only HA policy only handles cases when the broker is stopped gracefully. It does not handle unexpected broker failures.

While live-only HA prevents message loss, it may not preserve message order. If a broker configured with live-only HA is stopped, its messages will be appended to the ends of the queues of another broker.
NOTE

When a broker is preparing to scale down, it sends a message to its clients before they are disconnected informing them which new broker is ready to process their messages. However, clients should reconnect to the new broker only after their initial broker has finished scaling down. This ensures that any state, such as queues or transactions, is available on the other broker when the client reconnects. The normal reconnect settings apply when the client is reconnecting, so you should set these high enough to deal with the time needed to scale down.

This procedure describes how to configure each broker in the cluster to scale down. After completing this procedure, whenever a broker is stopped gracefully, it will copy its messages and transaction state to another broker in the cluster.

Procedure

1. Open the first broker’s `<broker-instance-dir>/etc/broker.xml` configuration file.

2. Configure the broker to use the live-only HA policy.

   ```xml
   <configuration>
     <core>
       ...
       <ha-policy>
         <live-only/>
       </live-only>
       <ha-policy>
       ...
     </core>
   </configuration>
   ```

3. Configure a method for scaling down the broker cluster. Specify the broker or group of brokers to which this broker should scale down.

<table>
<thead>
<tr>
<th>To scale down to...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A specific broker in the cluster</td>
<td>Specify the connector of the broker to which you want to scale down.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;live-only&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;scale-down&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;connectors&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;connector-ref&gt;</code>broker1-connector&lt;/connector-ref&gt;`</td>
</tr>
<tr>
<td></td>
<td><code>&lt;connectors&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;scale-down&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;live-only&gt;</code></td>
</tr>
</tbody>
</table>
To scale down to... | Do this...
--- | ---
Any broker in the cluster | Specify the broker cluster’s discovery group.

```xml
<live-only>
  <scale-down>
    <discovery-group-ref discovery-group-name="my-discovery-group"/>
  </scale-down>
</live-only>

```

A broker in a particular broker group | Specify a broker group.

```xml
<live-only>
  <scale-down>
    <group-name>my-group-name</group-name>
  </scale-down>
</live-only>
```

4. Repeat this procedure for each remaining broker in the cluster.

Additional resources

- For an example of a broker cluster that uses live-only to scale down the cluster, see the `scale-down` example programs.

16.3.2.4. Configuring high availability with colocated backups

Rather than configure live-backup groups, you can colocate backup brokers in the same JVM as another live broker. In this configuration, each live broker is configured to request another live broker to create and start a backup broker in its JVM.

Figure 16.4. Colocated live and backup brokers
You can use colocation with either shared store or replication as the high availability (HA) policy. The new backup broker inherits its configuration from the live broker that creates it. The name of the backup is set to `colocated_backup_n` where `n` is the number of backups the live broker has created.

In addition, the backup broker inherits the configuration for its connectors and acceptors from the live broker that creates it. By default, port offset of 100 is applied to each. For example, if the live broker has an acceptor for port 61616, the first backup broker created will use port 61716, the second backup will use 61816, and so on.

Directories for the journal, large messages, and paging are set according to the HA policy you choose. If you choose shared store, the requesting broker notifies the target broker which directories to use. If replication is chosen, directories are inherited from the creating broker and have the new backup’s name appended to them.

This procedure configures each broker in the cluster to use shared store HA, and to request a backup to be created and colocated with another broker in the cluster.

**Procedure**

1. Open the first broker’s `<broker-instance-dir>/etc/broker.xml` configuration file.

2. Configure the broker to use an HA policy and colocation.
   In this example, the broker is configured with shared store HA and colocation.

```
<configuration>
  <core>...
  <ha-policy>
    <shared-store>
      <colocated>
        <request-backup>true</request-backup>
        <max-backups>1</max-backups>
        <backup-request-retries>1</backup-request-retries>
        <backup-request-retry-interval-5000</backup-request-retry-interval>
        <backup-port-offset>150</backup-port-offset>
        <excludes>
          <connector-ref>remote-connector</connector-ref>
        </excludes>
        <master>
          <failover-on-shutdown>true</failover-on-shutdown>
        </master>
        <slave>
          <failover-on-shutdown>true</failover-on-shutdown>
          <allow-failback>true</allow-failback>
        </slave>
      </colocated>
    </shared-store>
  </ha-policy>
  ...
</core>
</configuration>
```

**request-backup**

By setting this property to `true`, this broker will request a backup broker to be created by another live broker in the cluster.
max-backups
The number of backup brokers that this broker can create. If you set this property to 0, this broker will not accept backup requests from other brokers in the cluster.

backup-request-retries
The number of times this broker should try to request a backup broker to be created. The default is 0, which means unlimited tries.

backup-request-retry-interval
The amount of time in milliseconds that the broker should wait before retrying a request to create a backup broker. The default is 5000, or 5 seconds.

backup-port-offset
The port offset to use for the acceptors and connectors for a new backup broker. If this broker receives a request to create a backup for another broker in the cluster, it will create the backup broker with the ports offset by this amount. The default is 100.

excludes (optional)
Excludes connectors from the backup port offset. If you have configured any connectors for external brokers that should be excluded from the backup port offset, add a <connector-ref> for each of the connectors.

master
The shared store or replication failover configuration for this broker.

slave
The shared store or replication failover configuration for this broker’s backup.

3. Repeat this procedure for each remaining broker in the cluster.

Additional resources
- For examples of broker clusters that use colocated backups, see the HA example programs.

16.3.3. Configuring clients to fail over
After configuring high availability in a broker cluster, you configure your clients to fail over. Client failover ensures that if a broker fails, the clients connected to it can reconnect to another broker in the cluster with minimal downtime.

NOTE
In the event of transient network problems, AMQ Broker automatically reattaches connections to the same broker. This is similar to failover, except that the client reconnects to the same broker.

You can configure two different types of client failover:

Automatic client failover
The client receives information about the broker cluster when it first connects. If the broker to which it is connected fails, the client automatically reconnects to the broker’s backup, and the backup broker re-creates any sessions and consumers that existed on each connection before failover.

Application-level client failover
As an alternative to automatic client failover, you can instead code your client applications with your own custom reconnection logic in a failure handler.
Procedure

- Use AMQ Core Protocol JMS to configure your client application with automatic or application-level failover.
  For more information, see Using the AMQ Core Protocol JMS Client.

16.4. ENABLING MESSAGE REDISTRIBUTION

If your broker cluster uses on-demand message load balancing, you should enable message redistribution to prevent messages from being “stuck” in a queue that does not have a consumer to consume them.

Broker clusters use load balancing to distribute the message load across the cluster. When configuring load balancing in the cluster connection, if you set message-load-balancing to ON_DEMAND, the broker will only forward messages to other brokers that have matching consumers. This ensures that messages are not moved to queues that do not have any consumers to consume them. However, if the consumers attached to a queue close after the messages are forwarded to the broker, those messages will be “stuck” in the queue and not consumed. This issue is sometimes called starvation.

Message redistribution prevents starvation by automatically redistributing the messages from queues that have no consumers to brokers in the cluster that do have matching consumers.

Procedure

1. Open the `<broker-instance-dir>/etc/broker.xml` configuration file.

2. In the `<cluster-connection>` element, verify that `<message-load-balancing>` is set to `<ON_DEMAND>`.

   ```xml
   <configuration>
   <core>
     ...
     <cluster-connections>
       <cluster-connection name="my-cluster">
         ...
         <message-load-balancing>ON_DEMAND</message-load-balancing>
       </cluster-connection>
     </cluster-connections>
   </core>
   </configuration>
   
   <configuration>
   <core>
     ...
     <address-settings>
       <address-setting match="my.queue">
         <redistribution-delay>5000</redistribution-delay>
       </address-setting>
     </address-settings>
   </configuration>
   
   3. Within the `<address-settings>` element, set the redistribution delay for a queue or set of queues.
   In this example, messages load balanced to my.queue will be redistributed 5000 milliseconds (5 seconds) after the last consumer closes.
address-setting
Set the match attribute to be the name of the queue for which you want messages to be redistributed. You can use the broker wildcard syntax to specify a range of queues. For more information, see the section called “AMQ Broker Wildcard Syntax”.

redistribution-delay
The amount of time (in milliseconds) that the broker should wait after this queue’s final consumer closes before redistributing messages to other brokers in the cluster. If you set this to 0, messages will be redistributed immediately. However, you should typically set a delay before redistributing - it is common for a consumer to close but another one to be quickly created on the same queue.

4. Repeat this procedure on each additional broker.

Additional resources
- For an example of a broker cluster configuration that redistributes messages, see the queue-message-redistribution AMQ Broker example program.

16.5. CONFIGURING CLUSTERED MESSAGE GROUPING
Message grouping enables clients to send groups of messages of a particular type to be processed serially by the same consumer. By adding a grouping handler to each broker in the cluster, you ensure that clients can send grouped messages to any broker in the cluster and still have those messages consumed in the correct order by the same consumer.

There are two types of grouping handlers: local handlers and remote handlers. They enable the broker cluster to route all of the messages in a particular group to the appropriate queue so that the intended consumer can consume them in the correct order.

Prerequisites
- There should be at least one consumer on each broker in the cluster.
  When a message is pinned to a consumer on a queue, all messages with the same group ID will be routed to that queue. If the consumer is removed, the queue will continue to receive the messages even if there are no consumers.

Procedure
1. Configure a local handler on one broker in the cluster.
  If you are using high availability, this should be a master broker.
  a. Open the broker’s <broker-instance-dir>/etc/broker.xml configuration file.
  b. Within the <core> element, add a local handler:
     The local handler serves as an arbiter for the remote handlers. It stores route information and communicates it to the other brokers.

     <configuration>
     <core>
     ...
Use the **name** attribute to specify a unique name for the grouping handler.

**type**

Set this to **LOCAL**.

**timeout**

The amount of time to wait (in milliseconds) for a decision to be made about where to route the message. The default is 5000 milliseconds (5 seconds). If the timeout is reached before a routing decision is made, an exception is thrown, which ensures strict message ordering.

When the broker receives a message with a group ID, it proposes a route to a queue to which the consumer is attached. If the route is accepted by the grouping handlers on the other brokers in the cluster, then the route is established: all brokers in the cluster will forward messages with this group ID to that queue. If the broker’s route proposal is rejected, then it proposes an alternate route, repeating the process until a route is accepted.

2. If you are using high availability, copy the local handler configuration to the master broker’s slave broker.

   Copying the local handler configuration to the slave broker prevents a single point of failure for the local handler.

3. On each remaining broker in the cluster, configure a remote handler.

   a. Open the broker’s `<broker-instance-dir>/etc/broker.xml` configuration file.

   b. Within the `<core>` element, add a remote handler:

   ```xml
   <configuration>
   <core>
   ...
   <grouping-handler name="my-grouping-handler">
   <type>REMOTE</type>
   <timeout>5000</timeout>
   </grouping-handler>
   ...
   </core>
   </configuration>
   ```

   **grouping-handler**

   Use the **name** attribute to specify a unique name for the grouping handler.

   **type**

   Set this to **REMOTE**.

   **timeout**
The amount of time to wait (in milliseconds) for a decision to be made about where to route the message. The default is 5000 milliseconds (5 seconds). Set this value to at least half of the value of the local handler.

Additional resources

- For an example of a broker cluster configured for message grouping, see the clustered-grouping AMQ Broker example program.

16.6. CONNECTING CLIENTS TO A BROKER CLUSTER

You can use the AMQ JMS clients to connect to the cluster. By using JMS, you can configure your messaging clients to discover the list of brokers dynamically or statically. You can also configure client-side load balancing to distribute the client sessions created from the connection across the cluster.

Procedure

- Use AMQ Core Protocol JMS to configure your client application to connect to the broker cluster.
  For more information, see Using the AMQ Core Protocol JMS Client.
CHAPTER 17. CONFIGURING A MULTI-SITE, FAULT-TOLERANT MESSAGING SYSTEM

Large-scale enterprise messaging systems commonly have discrete broker clusters located in geographically distributed data centers. In the event of a data center outage, system administrators might need to preserve existing messaging data and ensure that client applications can continue to produce and consume messages. You can use specific broker topologies and the Red Hat Ceph Storage software-defined storage platform to ensure continuity of your messaging system during a data center outage. This type of solution is called a multi-site, fault-tolerant architecture.

The following sections explain how to protect your messaging system from data center outages. These sections provide information about:

- How Red Hat Ceph Storage clusters work
- Installing and configuring a Red Hat Ceph Storage cluster
- Adding backup brokers to take over from live brokers in the event of a data center outage
- Configuring your broker servers with the Ceph client role
- Configuring each broker to use the shared store high-availability (HA) policy, specifying where in the Ceph File System each broker stores its messaging data
- Configuring client applications to connect to new brokers in the event of a data center outage
- Restarting a data center after an outage

**NOTE**

Multi-site fault tolerance is not a replacement for high-availability (HA) broker redundancy within data centers. Broker redundancy based on live-backup groups provides automatic protection against single broker failures within single clusters. By contrast, multi-site fault tolerance protects against large-scale data center outages.

**NOTE**

To use Red Hat Ceph Storage to ensure continuity of your messaging system, you must configure your brokers to use the shared store high-availability (HA) policy. You cannot configure your brokers to use the replication HA policy. For more information about these policies, see Implementing High Availability.

17.1. HOW RED HAT CEPH STORAGE CLUSTERS WORK

Red Hat Ceph Storage is a clustered object storage system. Red Hat Ceph Storage uses data sharding of objects and policy-based replication to guarantee data integrity and system availability.

Red Hat Ceph Storage uses an algorithm called CRUSH (Controlled Replication Under Scalable Hashing) to determine how to store and retrieve data by automatically computing data storage locations. You configure Ceph items called CRUSH maps, which detail cluster topography and specify how data is replicated across storage clusters.

CRUSH maps contain lists of Object Storage Devices (OSDs), a list of ‘buckets’ for aggregating the devices into a failure domain hierarchy, and rules that tell CRUSH how it should replicate data in a Ceph cluster’s pools.
By reflecting the underlying physical organization of the installation, CRUSH maps can model — and thereby address — potential sources of correlated device failures, such as physical proximity, shared power sources, and shared networks. By encoding this information into the cluster map, CRUSH can separate object replicas across different failure domains (for example, data centers) while still maintaining a pseudo-random distribution of data across the storage cluster. This helps to prevent data loss and enables the cluster to operate in a degraded state.

Red Hat Ceph Storage clusters require a number of nodes (physical or virtual) to operate. Clusters must include the following types of nodes:

**Monitor nodes**

Each Monitor (MON) node runs the monitor daemon (ceph-mon), which maintains a master copy of the cluster map. The cluster map includes the cluster topology. A client connecting to the Ceph cluster retrieves the current copy of the cluster map from the Monitor, which enables the client to read from and write data to the cluster.

**IMPORTANT**

A Red Hat Ceph Storage cluster can run with one Monitor node; however, to ensure high availability in a production cluster, Red Hat supports only deployments with at least three Monitor nodes. A minimum of three Monitor nodes means that in the event of the failure or unavailability of one Monitor, a quorum exists for the remaining Monitor nodes in the cluster to elect a new leader.

**Manager nodes**

Each Manager (MGR) node runs the Ceph Manager daemon (ceph-mgr), which is responsible for keeping track of runtime metrics and the current state of the Ceph cluster, including storage utilization, current performance metrics, and system load. Usually, Manager nodes are colocated (that is, on the same host machine) with Monitor nodes.

**Object Storage Device nodes**

Each Object Storage Device (OSD) node runs the Ceph OSD daemon (ceph-osd), which interacts with logical disks attached to the node. Ceph stores data on OSD nodes. Ceph can run with very few OSD nodes (the default is three), but production clusters realize better performance at modest scales, for example, with 50 OSDs in a storage cluster. Having multiple OSDs in a storage cluster enables system administrators to define isolated failure domains within a CRUSH map.

**Metadata Server nodes**

Each Metadata Server (MDS) node runs the MDS daemon (ceph-mds), which manages metadata related to files stored on the Ceph File System (CephFS). The MDS daemon also coordinates access to the shared cluster.

**Additional resources**

For more information about Red Hat Ceph Storage, see [What is Red Hat Ceph Storage?](#)

### 17.2. INSTALLING RED HAT CEPH STORAGE

AMQ Broker multi-site, fault-tolerant architectures use Red Hat Ceph Storage 3. By replicating data across data centers, a Red Hat Ceph Storage cluster effectively creates a shared store available to brokers in separate data centers. You configure your brokers to use the shared store high-availability (HA) policy and store messaging data in the Red Hat Ceph Storage cluster.
Red Hat Ceph Storage clusters intended for production use should have a minimum of:

- Three Monitor (MON) nodes
- Three Manager (MGR) nodes
- Three Object Storage Device (OSD) nodes containing multiple OSD daemons
- Three Metadata Server (MDS) nodes

**IMPORTANT**

You can run the OSD, MON, MGR, and MDS nodes on either the same or separate physical or virtual machines. However, to ensure fault tolerance within your Red Hat Ceph Storage cluster, it is good practice to distribute each of these types of nodes across distinct data centers. In particular, you must ensure that in the event of a single data center outage, your storage cluster still has a minimum of two available MON nodes. Therefore, if you have three MON nodes in your cluster, each of these nodes must run on separate host machines in separate data centers. Do not run two MON nodes in a single data center, because failure of this data center will leave your storage cluster with only one remaining MON node. In this situation, the storage cluster can no longer operate.

The procedures linked-to from this section show you how to install a Red Hat Ceph Storage 3 cluster that includes MON, MGR, OSD, and MDS nodes.

**Prerequisites**

- For information about preparing a Red Hat Ceph Storage installation, see:
  - Prerequisites
  - Requirements Checklist for Installing Red Hat Ceph Storage

**Procedure**

- For procedures that show how to install a Red Hat Ceph 3 storage cluster that includes MON, MGR, OSD, and MDS nodes, see:
  - Installing a Red Hat Ceph Storage Cluster
  - Installing Metadata Servers

### 17.3. CONFIGURING A RED HAT CEPH STORAGE CLUSTER

This example procedure shows how to configure your Red Hat Ceph storage cluster for fault tolerance. You create CRUSH buckets to aggregate your Object Storage Device (OSD) nodes into data centers that reflect your real-life, physical installation. In addition, you create a rule that tells CRUSH how to replicate data in your storage pools. These steps update the default CRUSH map that was created by your Ceph installation.

**Prerequisites**

- You have already installed a Red Hat Ceph Storage cluster. For more information, see Installing Red Hat Ceph Storage.
You should understand how Red Hat Ceph Storage uses Placement Groups (PGs) to organize large numbers of data objects in a pool, and how to calculate the number of PGs to use in your pool. For more information, see Placement Groups (PGs).

You should understand how to set the number of object replicas in a pool. For more information, Set the Number of Object Replicas.

Procedure

1. Create CRUSH buckets to organize your OSD nodes. Buckets are lists of OSDs, based on physical locations such as data centers. In Ceph, these physical locations are known as failure domains.

   ceph osd crush add-bucket dc1 datacenter
   ceph osd crush add-bucket dc2 datacenter

2. Move the host machines for your OSD nodes to the data center CRUSH buckets that you created. Replace host names host1-host4 with the names of your host machines.

   ceph osd crush move host1 datacenter=dc1
   ceph osd crush move host2 datacenter=dc1
   ceph osd crush move host3 datacenter=dc2
   ceph osd crush move host4 datacenter=dc2

3. Ensure that the CRUSH buckets you created are part of the default CRUSH tree.

   ceph osd crush move dc1 root=default
   ceph osd crush move dc2 root=default

4. Create a rule to map storage object replicas across your data centers. This helps to prevent data loss and enables your cluster to stay running in the event of a single data center outage. The command to create a rule uses the following syntax: ceph osd crush rule create-replicated <rule-name> <root> <failure-domain> <class>. An example is shown below.

   ceph osd crush rule create-replicated multi-dc default datacenter hdd

   NOTE
   
   In the preceding command, if your storage cluster uses solid-state drives (SSD), specify ssd instead of hdd (hard disk drives).

5. Configure your Ceph data and metadata pools to use the rule that you created. Initially, this might cause data to be backfilled to the storage destinations determined by the CRUSH algorithm.

   ceph osd pool set cephfs_data crush_rule multi-dc
   ceph osd pool set cephfs_metadata crush_rule multi-dc

6. Specify the numbers of Placement Groups (PGs) and Placement Groups for Placement (PGPs) for your metadata and data pools. The PGP value should be equal to the PG value.

   ceph osd pool set cephfs_metadata pg_num 128
   ceph osd pool set cephfs_metadata pgp_num 128
7. Specify the numbers of replicas to be used by your data and metadata pools.

```bash
ceph osd pool set cephfs_data pg_num 128
ceph osd pool set cephfs_data pgp_num 128

ceph osd pool set cephfs_data min_size 1
ceph osd pool set cephfs_metadata min_size 1

ceph osd pool set cephfs_data size 2
ceph osd pool set cephfs_metadata size 2
```

The following figure shows the Red Hat Ceph Storage cluster created by the preceding example procedure. The storage cluster has OSDs organized into CRUSH buckets corresponding to data centers.

The following figure shows a possible layout of the first data center, including your broker servers. Specifically, the data center hosts:

- The servers for two live-backup broker pairs
- The OSD nodes that you assigned to the first data center in the preceding procedure
- Single Metadata Server, Monitor and Manager nodes. The Monitor and Manager nodes are usually co-located on the same machine.
IMPORTANT

You can run the OSD, MON, MGR, and MDS nodes on either the same or separate physical or virtual machines. However, to ensure fault tolerance within your Red Hat Ceph Storage cluster, it is good practice to distribute each of these types of nodes across distinct data centers. In particular, you must ensure that in the event of a single data center outage, your storage cluster still has a minimum of two available MON nodes. Therefore, if you have three MON nodes in your cluster, each of these nodes must run on separate host machines in separate data centers.

The following figure shows a complete example topology. To ensure fault tolerance in your storage cluster, the MON, MGR, and MDS nodes are distributed across three separate data centers.
NOTE

Locating the host machines for certain OSD nodes in the same data center as your broker servers does not mean that you store messaging data on those specific OSD nodes. You configure the brokers to store messaging data in a specified directory in the Ceph File System. The Metadata Server nodes in your cluster then determine how to distribute the stored data across all available OSDs in your data centers and handle replication of this data across data centers. The sections that follow show how to configure brokers to store messaging data on the Ceph File System.

The figure below illustrates replication of data between the two data centers that have broker servers.
Additional resources

For more information about:

- Administrating CRUSH for your Red Hat Ceph Storage cluster, see CRUSH Administration.
- The full set of attributes that you can set on a storage pool, see Pool Values.

17.4. MOUNTING THE CEPH FILE SYSTEM ON YOUR BROKER SERVERS

Before you can configure brokers in your messaging system to store messaging data in your Red Hat Ceph Storage cluster, you first need to mount a Ceph File System (CephFS).

The procedure linked-to from this section shows you how to mount the CephFS on your broker servers.

Prerequisites

- You have:
  - Installed and configured a Red Hat Ceph Storage cluster. For more information, see Installing Red Hat Ceph Storage and Configuring a Red Hat Ceph Storage cluster.
  - Installed and configured three or more Ceph Metadata Server daemons (ceph-mds). For more information, see Installing Metadata Servers and Configuring Metadata Server Daemons.
  - Created the Ceph File System from a Monitor node. For more information, see Creating the Ceph File System.
17.5. CONFIGURING BROKERS IN A MULTI-SITE, FAULT-TOLERANT MESSAGING SYSTEM

To configure your brokers as part of a multi-site, fault-tolerant messaging system, you need to:

- Add idle backup brokers to take over from live brokers in the event of a data center failure
- Configure all broker servers with the Ceph client role
- Configure each broker to use the shared store high-availability (HA) policy, specifying where in the Ceph File System the broker stores its messaging data

17.5.1. Adding backup brokers

Within each of your data centers, you need to add idle backup brokers that can take over from live master-slave broker groups that shut down in the event of a data center outage. You should replicate the configuration of live master brokers in your idle backup brokers. You also need to configure your backup brokers to accept client connections in the same way as your existing brokers.

In a later procedure, you see how to configure an idle backup broker to join an existing master-slave broker group. You must locate the idle backup broker in a separate data center to that of the live master-slave broker group. It is also recommended that you manually start the idle backup broker only in the event of a data center failure.

The following figure shows an example topology.

![Topology Diagram]

**Data Center 1**
- Master Broker
- Slave Broker

**Data Center 2**
- Backup Broker (Idle)

**Shared Store Directory**
- Ceph File System

Additional resources

- To learn how to create additional broker instances, see Creating a standalone broker.
17.5.2. Configuring brokers as Ceph clients

When you have added the backup brokers that you need for a fault-tolerant system, you must configure all of the broker servers with the Ceph client role. The client role enable brokers to store data in your Red Hat Ceph Storage cluster.

To learn how to configure Ceph clients, see Installing the Ceph Client Role.

17.5.3. Configuring shared store high availability

The Red Hat Ceph Storage cluster effectively creates a shared store that is available to brokers in different data centers. To ensure that messages remain available to broker clients in the event of a failure, you configure each broker in your live-backup group to use:

- The shared store high availability (HA) policy
- The same journal, paging, and large message directories in the Ceph File System

The following procedure shows how to configure the shared store HA policy on the master, slave, and idle backup brokers of your live-backup group.

Procedure

1. Edit the broker.xml configuration file of each broker in the live-backup group. Configure each broker to use the same paging, bindings, journal, and large message directories in the Ceph File System.

   # Master Broker - DC1
   <paging-directory>/mnt/cephfs/broker1/paging</paging-directory>
   <bindings-directory>/mnt/cephfs/data/broker1/bindings</bindings-directory>
   <journal-directory>/mnt/cephfs/data/broker1/journal</journal-directory>
   <large-messages-directory>/mnt/cephfs/data/broker1/large-messages</large-messages-directory>

   # Slave Broker - DC1
   <paging-directory>/mnt/cephfs/broker1/paging</paging-directory>
   <bindings-directory>/mnt/cephfs/data/broker1/bindings</bindings-directory>
   <journal-directory>/mnt/cephfs/data/broker1/journal</journal-directory>
   <large-messages-directory>/mnt/cephfs/data/broker1/large-messages</large-messages-directory>

   # Backup Broker (Idle) - DC2
   <paging-directory>/mnt/cephfs/broker1/paging</paging-directory>
   <bindings-directory>/mnt/cephfs/data/broker1/bindings</bindings-directory>
   <journal-directory>/mnt/cephfs/data/broker1/journal</journal-directory>
   <large-messages-directory>/mnt/cephfs/data/broker1/large-messages</large-messages-directory>

2. Configure the backup broker as a master within it’s HA policy, as shown below. This configuration setting ensures that the backup broker immediately becomes the master when you manually start it. Because the broker is an idle backup, the failover-on-shutdown parameter that you can specify for an active master broker does not apply in this case.
Additional resources

- For more information about configuring the shared store high availability policy for live-backup broker groups, see Configuring shared store high availability.

17.6. CONFIGURING CLIENTS IN A MULTI-SITE, FAULT-TOLERANT MESSAGING SYSTEM

An internal client application is one that is running on a machine located in the same data center as the broker server. The following figure shows this topology.

An external client application is one running on a machine located outside the broker data center. The following figure shows this topology.
The following sub-sections describe how examples of configuring your internal and external client applications to connect to a backup broker in another data center in the event of a data center outage.

### 17.6.1. Configuring internal clients

If you experience a data center outage, internal client applications will shut down along with your brokers. To mitigate this situation, you must have another instance of the client application available in a separate data center. In the event of a data center outage, you manually start your backup client to connect to a backup broker that you have also manually started.

To enable the backup client to connect to a backup broker, you need to configure the client connection similarly to that of the client in your primary data center.

**Example**

A basic connection configuration for an AMQ Core Protocol JMS client to a master-slave broker group is shown below. In this example, `host1` and `host2` are the host servers for the master and slave brokers.

```
<ConnectionFactory connectionFactory = new ActiveMQConnectionFactory("(tcp://host1:port,tcp://host2:port)?ha=true&retryInterval=100&retryIntervalMultiplier=1.0&reconnectAttempts=-1");
```

To configure a backup client to connect to a backup broker in the event of a data center outage, use a similar connection configuration, but specify only the host name of your backup broker server. In this example, the backup broker server is `host3`.

```
<ConnectionFactory connectionFactory = new ActiveMQConnectionFactory("(tcp://host3:port)?ha=true&retryInterval=100&retryIntervalMultiplier=1.0&reconnectAttempts=-1");
```

**Additional resources**

For more information about configuring broker and client network connections, see:

- [Network Connections: Acceptors and Connectors](#)
- [Configuring a Connection from the Client Side](#)
17.6.2. Configuring external clients

To enable an external broker client to continue producing or consuming messaging data in the event of a data center outage, you must configure the client to fail over to a broker in another data center. In the case of a multi-site, fault-tolerant system, you configure the client to fail over to the backup broker that you manually start in the event of an outage.

Examples

Shown below are examples of configuring the AMQ Core Protocol JMS and AMQP JMS clients to fail over to a backup broker in the event that the primary master-slave group is unavailable. In these examples, `host1` and `host2` are the host servers for the primary master and slave brokers, while `host3` is the host server for the backup broker that you manually start in the event of a data center outage.

- To configure an AMQ Core Protocol JMS client, include the backup broker on the ordered list of brokers that the client attempts to connect to.

```
<ConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory("(tcp://host1:port,tcp://host2:port,tcp://host3:port)?
        ha=true&retryInterval=100&retryIntervalMultiplier=1.0&reconnectAttempts=-1");
```

- To configure an AMQP JMS client, include the backup broker in the failover URI that you configure on the client.

```
failover:(amqp://host1:port,amqp://host2:port,amqp://host3:port)?
    jms.clientId=foo&failover.maxReconnectAttempts=20
```

Additional resources

For more information about configuring failover on:

- The AMQ Core Protocol JMS client, see Reconnect and failover.
- The AMQP JMS client, see Failover options.
- Other supported clients, consult the client-specific documentation in the AMQ Clients section of Product Documentation for Red Hat AMQ 7.5.

17.7. VERIFYING STORAGE CLUSTER HEALTH DURING A DATA CENTER OUTAGE

When you have configured your Red Hat Ceph Storage cluster for fault tolerance, the cluster continues to run in a degraded state without losing data, even when one of your data centers fails.

This procedure shows how to verify the status of your cluster while it runs in a degraded state.

Procedure

1. To verify the status of your Ceph storage cluster, use the `health` or `status` commands:

```
# ceph health
# ceph status
```

2. To watch the ongoing events of the cluster on the command line, open a new terminal. Then, enter:
# ceph -w

When you run any of the preceding commands, you see output indicating that the storage cluster is still running, but in a degraded state. Specifically, you should see a warning that resembles the following:

```
health: HEALTH_WARN
  2 osds down
  Degraded data redundancy: 42/84 objects degraded (50.0%), 16 pgs unclean, 16 pgs degraded
```

Additional resources

- For more information about monitoring the health of your Red Hat Ceph Storage cluster, see [Monitoring](#).

## 17.8. MAINTAINING MESSAGING CONTINUITY DURING A DATA CENTER OUTAGE

The following procedure shows you how to keep brokers and associated messaging data available to clients during a data center outage. Specifically, when a data center fails, you need to:

- Manually start any idle backup brokers that you created to take over from brokers in your failed data center.
- Connect internal or external clients to the new active brokers.

### Prerequisites

- You must have:
  - Installed and configured a Red Hat Ceph Storage cluster. For more information, see [Installing Red Hat Ceph Storage](#) and [Configuring a Red Hat Ceph Storage cluster](#).
  - Mounted the Ceph File System. For more information, see [Mounting the Ceph File System on your broker servers](#).
  - Added idle backup brokers to take over from live brokers in the event of a data center failure. For more information, see [Adding backup brokers](#).
  - Configured your broker servers with the Ceph client role. For more information, see [Configuring brokers as Ceph clients](#).
  - Configured each broker to use the shared store high availability (HA) policy, specifying where in the Ceph File System each broker stores its messaging data. For more information, see [Configuring shared store high availability](#).
  - Configured your clients to connect to backup brokers in the event of a data center outage. For more information, see [Configuring clients in a multi-site, fault-tolerant messaging system](#).

### Procedure

1. For each master-slave broker pair in the failed data center, manually start the idle backup broker that you added.
2. Reestablish client connections.

   a. If you were using an internal client in the failed data center, manually start the backup client that you created. As described in Configuring clients in a multi-site, fault-tolerant messaging system, you must configure the client to connect to the backup broker that you manually started. The following figure shows the new topology.

   b. If you have an external client, manually connect the external client to the new active broker or observe that the clients automatically fails over to the new active broker, based on its configuration. For more information, see Configuring external clients. The following figure shows the new topology.
17.9. RESTARTING A PREVIOUSLY FAILED DATA CENTER

When a previously failed data center is back online, follow these steps to restore the original state of your messaging system:

- Restart the servers that host the nodes of your Red Hat Ceph Storage cluster
- Restart the brokers in your messaging system
- Re-establish connections from your client applications to your restored brokers

The following sub-sections show to perform these steps.

17.9.1. Restarting storage cluster servers

When you restart Monitor, Metadata Server, Manager, and Object Storage Device (OSD) nodes in a previously failed data center, your Red Hat Ceph Storage cluster self-heals to restore full data redundancy. During this process, Red Hat Ceph Storage automatically backfills data to the restored OSD nodes, as needed.

To verify that your storage cluster is automatically self-healing and restoring full data redundancy, use the commands previously shown in Verifying storage cluster health during a data center outage. When you re-execute these commands, you see that the percentage degradation indicated by the previous HEALTH_WARN message starts to improve until it returns to 100%.

17.9.2. Restarting broker servers

The following procedure shows how to restart your broker servers when your storage cluster is no longer operating in a degraded state.

Procedure

1. Stop any client applications connected to backup brokers that you manually started when the data center outage occurred.

2. Stop the backup brokers that you manually started.
   a. On Linux:
On Windows:

3. In your previously failed data center, restart the original master and slave brokers.
   a. On Linux:

   BROKER_INSTANCE_DIR/bin/artemis run

   b. On Windows:

   BROKER_INSTANCE_DIR/bin/artemis-service.exe start

The original master broker automatically resumes its role as master when you restart it.

17.9.3. Reestablishing client connections

When you have restarted your broker servers, reconnect your client applications to those brokers. The following subsections describe how to reconnect both internal and external client applications.

17.9.3.1. Reconnecting internal clients

Internal clients are those running in the same, previously failed data center as the restored brokers. To reconnect internal clients, restart them. Each client application reconnects to the restored master broker that is specified in its connection configuration.

For more information about configuring broker and client network connections, see:

- Network Connections: Acceptors and Connectors
- Configuring a Connection from the Client Side

17.9.3.2. Reconnecting external clients

External clients are those running outside the data center that previously failed. Based on your client type, and the information in Configuring external broker clients, you either configured the client to automatically fail over to a backup broker, or you manually established this connection. When you restore your previously failed data center, you reestablish a connection from your client to the restored master broker in a similar way, as described below.

- If you configured your external client to automatically fail over to a backup broker, the client automatically fails back to the original master broker when you shut down the backup broker and restart the original master broker.

- If you manually connected the external client to a backup broker when a data center outage occurred, you must manually reconnect the client to the original master broker that you restart.
CHAPTER 18. LOGGING

AMQ Broker uses the JBoss Logging framework to do its logging and is configurable via the BROKER_INSTANCE_DIR/etc/logging.properties configuration file. This configuration file is a list of key value pairs.

There are six loggers available, which are configured by the `loggers` key.

```
```

Table 18.1. Loggers

<table>
<thead>
<tr>
<th>Logger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>org.jboss.logging</td>
<td>Logs any calls not handled by the Brokers loggers</td>
</tr>
<tr>
<td>org.apache.activemq.artemis.core.server</td>
<td>Logs the Broker core</td>
</tr>
<tr>
<td>org.apache.activemq.artemis.utils</td>
<td>Logs utility calls</td>
</tr>
<tr>
<td>org.apache.activemq.artemis.journal</td>
<td>Logs Journal calls</td>
</tr>
<tr>
<td>org.apache.activemq.artemis.jms</td>
<td>Logs JMS calls</td>
</tr>
<tr>
<td>org.apache.activemq.artemis.integration.bootstrap</td>
<td>Logs bootstrap calls</td>
</tr>
</tbody>
</table>

By default there are two loggers configured by default by the `logger.handlers` key.

```
logger.handlers=FILE,CONSOLE
```

As the names suggest these log to the console and to a file.

18.1. CHANGING THE LOGGING LEVEL

The default logging level for all loggers is `INFO` and is configured on the root logger.

```
logger.level=INFO
```

All other loggers specified can be configured individually via the logger name.

```
logger.org.apache.activemq.artemis.core.server.level=INFO
logger.org.apache.activemq.artemis.journal.level=INFO
logger.org.apache.activemq.artemis.utils.level=INFO
logger.org.apache.activemq.artemis.jms.level=INFO
logger.org.apache.activemq.artemis.integration.bootstrap.level=INFO
```
NOTE

The root logger configuration will always be the finest logging logged even if the other logs have a finer logging configuration.

Table 18.2. Available Logging Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FATAL</td>
<td>Use the FATAL level priority for events that indicate a critical service failure. If a service issues a FATAL error it is completely unable to service requests of any kind.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Use the ERROR level priority for events that indicate a disruption in a request or the ability to service a request. A service should have some capacity to continue to service requests in the presence of ERRORs.</td>
</tr>
<tr>
<td>WARN</td>
<td>Use the WARN level priority for events that may indicate a non-critical service error. Resumable errors, or minor breaches in request expectations fall into this category. The distinction between WARN and ERROR may be hard to discern and so it is up to the developer to judge. The simplest criterion is would this failure result in a user support call. If it would use ERROR. If it would not use WARN.</td>
</tr>
<tr>
<td>INFO</td>
<td>Use the INFO level priority for service life-cycle events and other crucial related information. Looking at the INFO messages for a given service category should tell you exactly what state the service is in.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Use the DEBUG level priority for log messages that convey extra information regarding life-cycle events. Developer or in depth information required for support is the basis for this priority. The important point is that when the DEBUG level priority is enabled, the JBoss server log should not grow proportionally with the number of server requests. Looking at the DEBUG and INFO messages for a given service category should tell you exactly what state the service is in, as well as what server resources it is using: ports, interfaces, log files, and so on.</td>
</tr>
</tbody>
</table>
Use TRACE the level priority for log messages that are directly associated with activity that corresponds requests. Further, such messages should not be submitted to a Logger unless the Logger category priority threshold indicates that the message will be rendered. Use the Logger.isTraceEnabled() method to determine if the category priority threshold is enabled. The point of the TRACE priority is to allow for deep probing of the JBoss server behavior when necessary. When the TRACE level priority is enabled, you can expect the number of messages in the JBoss server log to grow at least a x N, where N is the number of requests received by the server, a some constant. The server log may well grow as power of N depending on the request-handling layer being traced.

### 18.2. CONFIGURING CONSOLE LOGGING

Console Logging can be configured via the following keys.

```java
handler.CONSOLE=org.jboss.logmanager.handlers.ConsoleHandler
handler.CONSOLE.properties=autoFlush
handler.CONSOLE.level=DEBUG
handler.CONSOLE.autoFlush=true
handler.CONSOLE.formatter=PATTERN
```

**NOTE**

`handler.CONSOLE` refers to the name given in the `logger.handlers` key.

#### Table 18.3. Available Console Configuration

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The handler’s name.</td>
</tr>
<tr>
<td>encoding</td>
<td>The character encoding used by this Handler.</td>
</tr>
<tr>
<td>level</td>
<td>The log level specifying which message levels will be logged by this. Message levels lower than this value will be discarded.</td>
</tr>
<tr>
<td>formatter</td>
<td>Defines a formatter. See Section 18.4, “Configuring the Logging Format”.</td>
</tr>
<tr>
<td>autoflush</td>
<td>Automatically flush after each write.</td>
</tr>
</tbody>
</table>
### 18.3. CONFIGURING FILE LOGGING

File Logging can be configured via the following keys.

```java
handler.FILE=org.jboss.logmanager.handlers.PeriodicRotatingFileHandler
handler.FILE.level=DEBUG
handler.FILE.properties=suffix,append,autoFlush,fileName
handler.FILE.suffix=.yyyy-MM-dd
handler.FILE.append=true
handler.FILE.autoFlush=true
handler.FILE.fileName=${artemis.instance}/log/artemis.log
handler.FILE.formatter=PATTERN
```

**NOTE**

`handler.FILE` refers to the name given in the `logger.handlers` key.

### Table 18.4. Available Console Configuration

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The handler’s name.</td>
</tr>
<tr>
<td>encoding</td>
<td>The character encoding used by this Handler.</td>
</tr>
<tr>
<td>level</td>
<td>The log level specifying which message levels will be logged by this. Message levels lower than this value will be discarded.</td>
</tr>
<tr>
<td>formatter</td>
<td>Defines a formatter. See Section 18.4, “Configuring the Logging Format”.</td>
</tr>
<tr>
<td>autoflush</td>
<td>Automatically flush after each write.</td>
</tr>
<tr>
<td>append</td>
<td>Specify whether to append to the target file.</td>
</tr>
<tr>
<td>file</td>
<td>The file description consisting of the path and optional relative to path.</td>
</tr>
</tbody>
</table>

### 18.4. CONFIGURING THE LOGGING FORMAT

The formatter describes how log messages should be shown. The following is the default configuration.
formatter.PATTERN=org.jboss.logmanager.formatters.PatternFormatter
formatter.PATTERN.properties=pattern
formatter.PATTERN.pattern=%d{HH:mm:ss,SSS} %-5p [%c] %s%E%n

Where %s is the message and %E is the exception if one exists.

The format is the same as the Log4J format. A full description can be found here.

18.5. CLIENT OR EMBEDDED SERVER LOGGING

Firstly, if you want to enable logging on the client side you need to include the JBoss logging JARs in your client’s class path. If you are using Maven, add the following dependencies:

```xml
<dependency>
  <groupId>org.jboss.logmanager</groupId>
  <artifactId>jboss-logmanager</artifactId>
  <version>1.5.3.Final</version>
</dependency>
<dependency>
  <groupId>org.apache.activemq</groupId>
  <artifactId>artemis-core-client</artifactId>
  <version>1.0.0.Final</version>
</dependency>
```

There are two properties you need to set when starting your Java program. The first is to set the Log Manager to use the JBoss Log Manager. This is done by setting the `-Djava.util.logging.manager` property. For example:

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager
```

The second is to set the location of the `logging.properties` file to use. This is done by setting the `-Dlogging.configuration` property with a valid URL. For example:

```
-Dlogging.configuration=file:///home/user/projects/myProject/logging.properties
```

The following is a typical `logging.properties` file for a client:

```
# Root logger option

# Root logger level
logger.level=INFO

# ActiveMQ Artemis logger levels
logger.org.apache.activemq.artemis.core.server.level=INFO
logger.org.apache.activemq.artemis.util.level=INFO
logger.org.apache.activemq.artemis.jms.level=DEBUG

# Root logger handlers
logger.handlers=FILE,CONSOLE

# Console handler configuration
handler.CONSOLE=org.jboss.logmanager.handlers.ConsoleHandler
handler.CONSOLE.properties=autoFlush
```
18.6. AMQ BROKER PLUG-INS SUPPORT

AMQ supports custom plug-ins. You can use plug-ins to log information about many different types of events that would otherwise only be available through debug logs. Multiple plug-ins can be registered, tied, and executed together. The plug-ins will be executed based on the order of the registration, that is, the first plug-in registered is always executed first.

You can create custom plug-ins and implement them using the ActiveMQServerPlugin interface. This interface ensures that the plug-in is on the classpath, and is registered with the broker. As all the interface methods are implemented by default, you have to add only the required behavior that needs to be implemented.

18.6.1. Adding Plug-ins to the Classpath

Add the custom created broker plug-ins to the broker runtime by adding the relevant jars to the BROKER_INSTANCE_DIR/lib directory.

If you are using an embedded system then place the jar under the regular classpath of your embedded application.

18.6.2. Registering a Plug-in

You must register a plug-in by adding the broker-plugins element in the broker.xml file. You can specify the plug-in configuration value using the property child elements. These properties will be read and passed into the plug-in’s init (Map<String, String>) operation after the plug-in has been instantiated.

18.6.3. Registering a Plug-in Programmatically
To register a plug-in programmatically, use the `registerBrokerPlugin()` method and pass in a new instance of your plug-in. The example below shows the registration of the `UserPlugin` plugin:

```
Configuration config = new ConfigurationImpl();
config.registerBrokerPlugin(new UserPlugin());
```

18.6.4. Logging Specific Events

By default, AMQ broker provides the `LoggingActiveMQServerPlugin` plug-in to log specific broker events. The `LoggingActiveMQServerPlug-in` plug-in is commented out by default and does not log any information. The following table provides information about the plug-in properties and its description. Set the configuration property value to `true` to log events.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG_CONNECTION_EVENTS</td>
<td>Logs information when a connection is created or destroyed.</td>
</tr>
<tr>
<td>LOG_SESSION_EVENTS</td>
<td>Logs information when a session is created or closed.</td>
</tr>
<tr>
<td>LOG_CONSUMER_EVENTS</td>
<td>Logs information when a consumer is created or closed.</td>
</tr>
<tr>
<td>LOG_DELIVERING_EVENTS</td>
<td>Logs information when message is delivered to a consumer and when a message is acknowledged by a consumer.</td>
</tr>
<tr>
<td>LOG_SENDING_EVENTS</td>
<td>Logs information when a message has been sent to an address and when a message has been routed within the broker.</td>
</tr>
<tr>
<td>LOG_INTERNAL_EVENTS</td>
<td>Logs information when a queue created or destroyed, when a message is expired, when a bridge is deployed, and when a critical failure occurs.</td>
</tr>
<tr>
<td>LOG_ALL_EVENTS</td>
<td>Logs information for all the above events.</td>
</tr>
</tbody>
</table>

To configure the `LoggingActiveMQServerPlugin` plugin to log connection events, uncomment the `<broker-plugins>` section in the `broker.xml` file. The value of all the events is set to `true` in the commented default example.

```
<configuration ...>
  ...
  <!-- Uncomment the following if you want to use the Standard LoggingActiveMQServerPlugin plugin to log in events -->
  <broker-plugins>
    <broker-plugin class-name="org.apache.activemq.artemis.core.server.plugin.impl.LoggingActiveMQServerPlugin">
      <property key="LOG_ALL_EVENTS" value="true"/>
      <property key="LOG_CONNECTION_EVENTS" value="true"/>
    </broker-plugin>
  </broker-plugins>
</configuration>
```
After changing the configuration parameters inside the `<broker-plugins>` section of the `broker.xml` file, you must restart the broker to reload the configuration updates. These configuration changes will not be reloaded by the `configuration-file-refresh-period` setting.

When the log level is set to `INFO`, an entry is logged after the event has occurred. If the log level is set to `DEBUG`, log entries are generated for both before and after the event has occurred. For example, it logs `beforeCreateConsumer()` and `afterCreateConsumer()`. If the log Level is set to `DEBUG`, it logs more information for a notification when available.
APPENDIX A. ACCEPTOR AND CONNECTOR CONFIGURATION PARAMETERS

The tables below detail some of the available parameters used to configure Netty network connections. Parameters and their values are appended to the URI of the connection string. See Network Connections: Acceptors and Connectors for more information. Each table lists the parameters by name and notes whether they can be used with acceptors or connectors or with both. You can use some parameters, for example, only with acceptors.

NOTE

All Netty parameters are defined in the class org.apache.activemq.artemis.core.remoting.impl.netty.TransportConstants. Source code is available for download on the customer portal.

Table A.1. Netty TCP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use with…</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>batchDelay</td>
<td>Both</td>
<td>Before writing packets to the acceptor or connector, the broker can be configured to batch up writes for a maximum of \texttt{batchDelay} milliseconds. This can increase overall throughput for very small messages. It does so at the expense of an increase in average latency for message transfer. The default value is 0 ms.</td>
</tr>
<tr>
<td>connectionsAllowed</td>
<td>Acceptors</td>
<td>Limits the number of connections that the acceptor will allow. When this limit is reached, a DEBUG-level message is issued to the log and the connection is refused. The type of client in use determines what happens when the connection is refused.</td>
</tr>
<tr>
<td>directDeliver</td>
<td>Both</td>
<td>When a message arrives on the server and is delivered to waiting consumers, by default, the delivery is done on the same thread as that on which the message arrived. This gives good latency in environments with relatively small messages and a small number of consumers, but at the cost of overall throughput and scalability - especially on multi-core machines. If you want the lowest latency and a possible reduction in throughput then you can use the default value for \texttt{directDeliver}, which is \texttt{true}. If you are willing to take some small extra hit on latency but want the highest throughput set \texttt{directDeliver} to \texttt{false}.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Use with…</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>handshake-timeout</td>
<td>Acceptors</td>
<td>Prevents an unauthorized client to open a large number of connections and keep them open. Because each connection requires a file handle, it consumes resources that are then unavailable to other clients. This timeout limits the amount of time a connection can consume resources without having been authenticated. After the connection is authenticated, you can use resource limit settings to limit resource consumption. The default value is set to 10 seconds. You can set it to any other integer value. You can turn off this option by setting it to 0 or negative integer. After you edit the timeout value, you must restart the broker.</td>
</tr>
<tr>
<td>localAddress</td>
<td>Connectors</td>
<td>Specifies which local address the client will use when connecting to the remote address. This is typically used in the Application Server or when running Embedded to control which address is used for outbound connections. If the local-address is not set then the connector will use any local address available.</td>
</tr>
<tr>
<td>localPort</td>
<td>Connectors</td>
<td>Specifies which local port the client will use when connecting to the remote address. This is typically used in the Application Server or when running Embedded to control which port is used for outbound connections. If the default is used, which is 0, then the connector will let the system pick up an ephemeral port. Valid ports are 0 to 65535</td>
</tr>
<tr>
<td>nioRemotingThreads</td>
<td>Both</td>
<td>When configured to use NIO, the broker will by default use a number of threads equal to three times the number of cores (or hyper-threads) as reported by Runtime.getRuntime().availableProcessors() for processing incoming packets. If you want to override this value, you can set the number of threads by specifying this parameter. The default value for this parameter is -1, which means use the value derived from Runtime.getRuntime().availableProcessors() * 3.</td>
</tr>
<tr>
<td>tcpNoDelay</td>
<td>Both</td>
<td>If this is true then Nagle's algorithm will be disabled. This is a Java (client) socket option. The default value is true.</td>
</tr>
<tr>
<td>tcpReceiveBufferSize</td>
<td>Both</td>
<td>Determines the size of the TCP receive buffer in bytes. The default value is 32768.</td>
</tr>
</tbody>
</table>
TCP buffer sizes should be tuned according to the bandwidth and latency of your network.

In summary TCP send/receive buffer sizes should be calculated as:

\[
\text{buffer\_size} = \text{bandwidth} \times \text{RTT}.
\]

Where bandwidth is in bytes per second and network round trip time (RTT) is in seconds. RTT can be easily measured using the `ping` utility.

For fast networks you may want to increase the buffer sizes from the defaults.

---

### Table A.2. Netty HTTP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use with...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpClientIdleTime</td>
<td>Acceptors</td>
<td>How long a client can be idle before sending an empty HTTP request to keep the connection alive.</td>
</tr>
<tr>
<td>httpClientIdleScanPeriod</td>
<td>Acceptors</td>
<td>How often, in milliseconds, to scan for idle clients.</td>
</tr>
<tr>
<td>httpEnabled</td>
<td>Acceptors</td>
<td>No longer required. With single port support the broker will now automatically detect if HTTP is being used and configure itself.</td>
</tr>
<tr>
<td>httpRequiresSessionId</td>
<td>Both</td>
<td>If true the client will wait after the first call to receive a session id. Used when an HTTP connector is connecting to a servlet acceptor. This configuration is not recommended.</td>
</tr>
<tr>
<td>httpResponseTime</td>
<td>Acceptors</td>
<td>How long the server can wait before sending an empty HTTP response to keep the connection alive.</td>
</tr>
<tr>
<td>httpServerScanPeriod</td>
<td>Acceptors</td>
<td>How often, in milliseconds, to scan for clients needing responses.</td>
</tr>
</tbody>
</table>

### Table A.3. Netty TLS/SSL Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use with...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabledCipherSuites</td>
<td>Both</td>
<td>Comma separated list of cipher suites used for SSL communication. The default value is empty which means the JVM’s default will be used.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Use with…</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| enabledProtocols | Both        | Comma separated list of protocols used for SSL communication. The default value is empty which means the JVM’s default will be used.  
<p>| | | |
|                  |             |                                                                                                                                                                                                                                                                                                                                           |
| keyStorePassword | Both        | When used on an acceptor this is the password for the server-side keystore. When used on a connector this is the password for the client-side keystore. This is only relevant for a connector if you are using 2-way SSL (that is, mutual authentication). Although this value can be configured on the server, it is downloaded and used by the client. If the client needs to use a different password from that set on the server then it can override the server-side setting by either using the customary <strong>javax.net.ssl.keyStorePassword</strong> system property or the ActiveMQ-specific <strong>org.apache.activemq.ssl.keyStorePassword</strong> system property. The ActiveMQ-specific system property is useful if another component on client is already making use of the standard, Java system property. |
| keyStorePath     | Both        | When used on an acceptor this is the path to the SSL key store on the server which holds the server’s certificates (whether self-signed or signed by an authority). When used on a connector this is the path to the client-side SSL key store which holds the client certificates. This is only relevant for a connector if you are using 2-way SSL (that is, mutual authentication). Although this value is configured on the server, it is downloaded and used by the client. If the client needs to use a different path from that set on the server then it can override the server-side setting by either using the customary <strong>javax.net.ssl.keyStore</strong> system property or the ActiveMQ-specific <strong>org.apache.activemq.ssl.keyStore</strong> system property. The ActiveMQ-specific system property is useful if another component on client is already making use of the standard, Java system property. |
| needClientAuth   | Acceptors   | Tells a client connecting to this acceptor that 2-way SSL is required. Valid values are <strong>true</strong> or <strong>false</strong>. Default is <strong>false</strong>.                                                                                                                                                                                                         |
| sslEnabled       | Both        | Must be <strong>true</strong> to enable SSL. Default is <strong>false</strong>.                                                                                                                                                                                                                                                                                    |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use with...</th>
<th>Description</th>
</tr>
</thead>
</table>
| trustStorePassword     | Both        | When used on an acceptor this is the password for the server-side trust store. This is only relevant for an acceptor if you are using 2-way SSL (that is, mutual authentication).  
When used on a connector this is the password for the client-side truststore. Although this value can be configured on the server, it is downloaded and used by the client. If the client needs to use a different password from that set on the server then it can override the server-side setting by either using the customary `javax.net.ssl.trustStorePassword` system property or the ActiveMQ-specific `org.apache.activemq.ssl.trustStorePassword` system property. The ActiveMQ-specific system property is useful if another component on client is already making use of the standard, Java system property. |
| trustStorePath         | Both        | When used on an acceptor this is the path to the server-side SSL key store that holds the keys of all the clients that the server trusts. This is only relevant for an acceptor if you are using 2-way SSL (that is, mutual authentication).  
When used on a connector this is the path to the client-side SSL key store which holds the public keys of all the servers that the client trusts. Although this value can be configured on the server, it is downloaded and used by the client. If the client needs to use a different path from that set on the server then it can override the server-side setting by either using the customary `javax.net.ssl.trustStore` system property or the ActiveMQ-specific `org.apache.activemq.ssl.trustStore` system property. The ActiveMQ-specific system property is useful if another component on client is already making use of the standard, Java system property. |
| verifyHost             | Both        | When used on an acceptor the CN of the connecting client’s SSL certificate will be compared to its hostname to verify they match. This is useful only for 2-way SSL.  
When used on a connector the CN of the server’s SSL certificate will be compared to its hostname to verify they match. This is useful for both 1-way and 2-way SSL.  
Valid values are **true** or **false**. Default is **false**. |
APPENDIX B. ADDRESS SETTING CONFIGURATION ELEMENTS

The table below lists all of the configuration elements of an address-setting. Note that some elements are marked DEPRECATED. Use the suggested replacement to avoid potential issues.

Table B.1. Address Setting Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-full-policy</td>
<td>Determines what happens when an address configured with a max-size-bytes becomes full. The available policies are:</td>
</tr>
<tr>
<td></td>
<td><strong>PAGE</strong>: messages sent to a full address will be paged to disk.</td>
</tr>
<tr>
<td></td>
<td><strong>DROP</strong>: messages sent to a full address will be silently dropped.</td>
</tr>
<tr>
<td></td>
<td><strong>FAIL</strong>: messages sent to a full address will be dropped and the message producers will receive an exception.</td>
</tr>
<tr>
<td></td>
<td><strong>BLOCK</strong>: message producers will block when they try and send any further messages.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>The BLOCK policy works only for the AMQP, OpenWire, and Core protocols because they feature flow control.</td>
</tr>
<tr>
<td>auto-create-addresses</td>
<td>Whether to automatically create addresses when a client sends a message to or attempts to consume a message from a queue mapped to an address that does not exist a queue. The default value is <strong>true</strong>.</td>
</tr>
<tr>
<td>auto-create-jms-queues</td>
<td>DEPRECATED: Use <strong>auto-create-queues</strong> instead. Determines whether this broker should automatically create a JMS queue corresponding to the address settings match when a JMS producer or a consumer tries to use such a queue. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>auto-create-jms-topics</td>
<td>DEPRECATED: Use <strong>auto-create-queues</strong> instead. Determines whether this broker should automatically create a JMS topic corresponding to the address settings match when a JMS producer or a consumer tries to use such a queue. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>auto-create-queues</td>
<td>Whether to automatically create a queue when a client sends a message to or attempts to consume a message from a queue. The default value is <strong>true</strong>.</td>
</tr>
<tr>
<td>auto-delete-addresses</td>
<td>Whether to delete auto-created addresses when the broker no longer has any queues. The default value is <strong>true</strong>.</td>
</tr>
<tr>
<td>auto-delete-jms-queues</td>
<td>DEPRECATED: Use <strong>auto-delete-queues</strong> instead. Determines whether AMQ Broker should automatically delete auto-created JMS queues when they have no consumers and no messages. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auto-delete-jms-topics</td>
<td>DEPRECATED: Use auto-delete-queues instead. Determines whether AMQ Broker should automatically delete auto-created JMS topics when they have no consumers and no messages. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>auto-delete-queues</td>
<td>Whether to delete auto-created queues when the queue has no consumers and no messages. The default value is <strong>true</strong>.</td>
</tr>
<tr>
<td>config-delete-addresses</td>
<td>When the configuration file is reloaded, this setting specifies how to handle an address (and its queues) that has been deleted from the configuration file. You can specify the following values:</td>
</tr>
<tr>
<td></td>
<td><strong>OFF (default)</strong></td>
</tr>
<tr>
<td></td>
<td>The address is not deleted when the configuration file is reloaded.</td>
</tr>
<tr>
<td></td>
<td><strong>FORCE</strong></td>
</tr>
<tr>
<td></td>
<td>The address and its queues are deleted when the configuration file is reloaded. If there are any messages in the queues, they are removed also.</td>
</tr>
<tr>
<td>config-delete-queues</td>
<td>When the configuration file is reloaded, this setting specifies how to handle queues that have been deleted from the configuration file. You can specify the following values:</td>
</tr>
<tr>
<td></td>
<td><strong>OFF (default)</strong></td>
</tr>
<tr>
<td></td>
<td>The queue is not deleted when the configuration file is reloaded.</td>
</tr>
<tr>
<td></td>
<td><strong>FORCE</strong></td>
</tr>
<tr>
<td></td>
<td>The queue is deleted when the configuration file is reloaded. If there are any messages in the queue, they are removed also.</td>
</tr>
<tr>
<td>dead-letter-address</td>
<td>The address to which the broker sends dead messages.</td>
</tr>
<tr>
<td>default-address-routing-type</td>
<td>The routing-type used on auto-created addresses. The default value is <strong>MULTICAST</strong>.</td>
</tr>
<tr>
<td>default-max-consumers</td>
<td>The maximum number of consumers allowed on this queue at any one time. The default value is <strong>200</strong>.</td>
</tr>
<tr>
<td>default-purge-on-no-</td>
<td>Whether to purge the contents of the queue once there are no consumers. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>consumers</td>
<td></td>
</tr>
<tr>
<td>default-queue-routing-type</td>
<td>The routing-type used on auto-created queues. The default value is <strong>MULTICAST</strong>.</td>
</tr>
<tr>
<td>expiry-address</td>
<td>The address that will receive expired messages.</td>
</tr>
<tr>
<td>expiry-delay</td>
<td>Defines the expiration time in milliseconds that will be used for messages using the default expiration time. The default value is <strong>-1</strong>, which is means no expiration time.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>last-value-queue</td>
<td>Whether a queue uses only last values or not. The default value is <code>false</code>.</td>
</tr>
<tr>
<td>management-browse-page-size</td>
<td>How many messages a management resource can browse. The default value is <code>200</code>.</td>
</tr>
<tr>
<td>max-delivery-attempts</td>
<td>how many times to attempt to deliver a message before sending to dead letter address. The default is <code>10</code>.</td>
</tr>
<tr>
<td>max-redelivery-delay</td>
<td>Maximum value for the redelivery-delay, in milliseconds.</td>
</tr>
<tr>
<td>max-size-bytes</td>
<td>The maximum memory size for this address, specified in bytes. Used when the address-full-policy is <code>PAGING</code>, <code>BLOCK</code>, or <code>FAIL</code>, this value is specified in byte notation such as &quot;K&quot;, &quot;Mb&quot;, and &quot;GB&quot;. The default value is <code>-1</code>, which denotes infinite bytes. This parameter is used to protect broker memory by limiting the amount of memory consumed by a particular address space. This setting does not represent the total amount of bytes sent by the client that are currently stored in broker address space. It is an estimate of broker memory utilization. This value can vary depending on runtime conditions and certain workloads. It is recommended that you allocate the maximum amount of memory that can be afforded per address space. Under typical workloads, the broker requires approximately 150% to 200% of the payload size of the outstanding messages in memory.</td>
</tr>
<tr>
<td>max-size-bytes-reject-threshold</td>
<td>Used when the address-full-policy is <code>BLOCK</code>. The maximum size, in bytes, that an address can reach before the broker begins to reject messages. Works in combination with max-size-bytes for the AMQP protocol only. The default value is <code>-1</code>, which means no limit.</td>
</tr>
<tr>
<td>message-counter-history-day-limit</td>
<td>How many days to keep a message counter history for this address. The default value is <code>0</code>.</td>
</tr>
<tr>
<td>page-max-cache-size</td>
<td>The number of page files to keep in memory to optimize I/O during paging navigation. The default value is <code>5</code>.</td>
</tr>
<tr>
<td>page-size-bytes</td>
<td>The paging size in bytes. Also supports byte notation like <code>K</code>, <code>Mb</code>, and <code>GB</code>. The default value is <code>10485760</code> bytes, almost <code>10.5 MB</code>.</td>
</tr>
<tr>
<td>redelivery-delay</td>
<td>The time, in milliseconds, to wait before redelivering a cancelled message. The default value is <code>0</code>.</td>
</tr>
<tr>
<td>redelivery-delay-multiplier</td>
<td>Multiplier to apply to the redelivery-delay parameter. The default value is <code>1.0</code>.</td>
</tr>
<tr>
<td>redistribution-delay</td>
<td>Defines how long to wait in milliseconds after the last consumer is closed on a queue before redistributing any messages. The default value is <code>-1</code>.</td>
</tr>
</tbody>
</table>

Red Hat AMQ 7.5 Configuring AMQ Broker
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send-to-dla-on-no-route</td>
<td>When set to <strong>true</strong>, a message will be sent to the configured dead letter address if it cannot be routed to any queues. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>slow-consumer-check-period</td>
<td>How often to check, in seconds, for slow consumers. The default value is <strong>5</strong>.</td>
</tr>
<tr>
<td>slow-consumer-policy</td>
<td>Determines what happens when a slow consumer is identified. Valid options are <strong>KILL</strong> or <strong>NOTIFY</strong>. <strong>KILL</strong> kills the consumer’s connection, which impacts any client threads using that same connection. <strong>NOTIFY</strong> sends a <strong>CONSUMER_SLOW</strong> management notification to the client. The default value is <strong>NOTIFY</strong>.</td>
</tr>
<tr>
<td>slow-consumer-threshold</td>
<td>The minimum rate of message consumption allowed before a consumer is considered slow. Measured in messages-per-second. The default value is <strong>-1</strong>, which is unbounded.</td>
</tr>
</tbody>
</table>
## APPENDIX C. CLUSTER CONNECTION CONFIGURATION ELEMENTS

The table below lists all of the configuration elements of a **cluster-connection**.

### Table C.1. Cluster Connection Configuration Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| address                   | Each cluster connection applies only to addresses that match the value specified in the **address** field. If no address is specified, then all addresses will be load balanced.  
                           | The **address** field also supports comma separated lists of addresses. Use exclude syntax, ! to prevent an address from being matched. Below are some example addresses:  
<pre><code>                       | jms.eu                                                                                                                                  | Matches all addresses starting with jms.eu.                                                                                       |
</code></pre>
<p>|                           | !jms.eu                                                                                                                                         | Matches all addresses except for those starting with jms.eu                                                                       |
|                           | jms.eu.uk, jms.eu.de                                                                                                                              | Matches all addresses starting with either jms.eu.uk or jms.eu.de                                                               |
|                           | jms.eu, !jms.eu.uk                                                                                                                              | Matches all addresses starting with jms.eu, but not those starting with jms.eu.uk                                               |
|                           | <strong>NOTE</strong>                                                                                                                                                                                                    | You should not have multiple cluster connections with overlapping addresses (for example, &quot;europe&quot; and &quot;europe.news&quot;), because the same messages could be distributed between more than one cluster connection, possibly resulting in duplicate deliveries. |
| call-failover-timeout     | Use when a call is made during a failover attempt. The default is -1, or no timeout.                                                           |
| call-timeout              | When a packet is sent over a cluster connection, and it is a blocking call, <strong>call-timeout</strong> determines how long the broker will wait (in milliseconds) for the reply before throwing an exception. The default is 30000. |
| check-period              | The interval, in milliseconds, between checks to see if the cluster connection has failed to receive pings from another broker. The default is 30000.                                                        |
| confirmation-window-size  | The size, in bytes, of the window used for sending confirmations from the broker connected to. When the broker receives <strong>confirmation-window-size</strong> bytes, it notifies its client. The default is 1048576. A value of -1 means no window. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connector-ref</td>
<td>Identifies the <strong>connector</strong> that will be transmitted to other brokers in the cluster so that they have the correct cluster topology. This parameter is mandatory.</td>
</tr>
<tr>
<td>connection-ttl</td>
<td>Determines how long a cluster connection should stay alive if it stops receiving messages from a specific broker in the cluster. The default is <strong>60000</strong>.</td>
</tr>
<tr>
<td>discovery-group-ref</td>
<td>Points to a <strong>discovery-group</strong> to be used to communicate with other brokers in the cluster. This element must include the attribute <strong>discovery-group-name</strong>, which must match the <strong>name</strong> attribute of a previously configured <strong>discovery-group</strong>.</td>
</tr>
<tr>
<td>initial-connect-attempts</td>
<td>Sets the number of times the system will try to connect a broker in the cluster initially. If the max-retry is achieved, this broker will be considered permanently down, and the system will not route messages to this broker. The default is <strong>-1</strong>, which means infinite retries.</td>
</tr>
<tr>
<td>max-hops</td>
<td>Configures the broker to load balance messages to brokers which might be connected to it only indirectly with other brokers as intermediates in a chain. This allows for more complex topologies while still providing message load-balancing. The default value is <strong>1</strong>, which means messages are distributed only to other brokers directly connected to this broker. This parameter is optional.</td>
</tr>
<tr>
<td>max-retry-interval</td>
<td>The maximum delay for retries, in milliseconds. The default is <strong>2000</strong>.</td>
</tr>
<tr>
<td>message-load-balancing</td>
<td>Determines whether and how messages will be distributed between other brokers in the cluster. Include the <strong>message-load-balancing</strong> element to enable load balancing. The default value is <strong>ON_DEMAND</strong>. You can provide a value as well. Valid values are:</td>
</tr>
<tr>
<td></td>
<td><strong>OFF</strong></td>
</tr>
<tr>
<td></td>
<td>Disables load balancing.</td>
</tr>
<tr>
<td></td>
<td><strong>STRICT</strong></td>
</tr>
<tr>
<td></td>
<td>Forwards messages to all brokers that have a matching queue, whether or not the queue has an active consumer or a matching selector.</td>
</tr>
<tr>
<td></td>
<td><strong>ON_DEMAND</strong></td>
</tr>
<tr>
<td></td>
<td>Ensures that messages are forwarded only to brokers that have active consumers or a matching selector.</td>
</tr>
<tr>
<td>min-large-message-size</td>
<td>If a message size, in bytes, is larger than <strong>min-large-message-size</strong>, it will be split into multiple segments when sent over the network to other cluster members. The default is <strong>102400</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>notification-attempts</td>
<td>Sets how many times the cluster connection should broadcast itself when connecting to the cluster. The default is 2.</td>
</tr>
<tr>
<td>notification-interval</td>
<td>Sets how often, in milliseconds, the cluster connection should broadcast itself when attaching to the cluster. The default is 1000.</td>
</tr>
<tr>
<td>producer-window-size</td>
<td>The size, in bytes, for producer flow control over cluster connection. By default, it is disabled, but you may want to set a value if you are using really large messages in cluster. A value of -1 means no window.</td>
</tr>
<tr>
<td>reconnect-attempts</td>
<td>Sets the number of times the system will try to reconnect to a broker in the cluster. If the max-retry is achieved, this broker will be considered permanently down and the system will stop routing messages to this broker. The default is -1, which means infinite retries.</td>
</tr>
<tr>
<td>retry-interval</td>
<td>Determines the interval, in milliseconds, between retry attempts. If the cluster connection is created and the target broker has not been started or is booting, then the cluster connections from other brokers will retry connecting to the target until it comes back up. This parameter is optional. The default value is 500 milliseconds.</td>
</tr>
<tr>
<td>retry-interval-multiplier</td>
<td>The multiplier used to increase the retry-interval after each reconnect attempt. The default is 1.</td>
</tr>
<tr>
<td>use-duplicate-detection</td>
<td>Cluster connections use bridges to link the brokers, and bridges can be configured to add a duplicate ID property in each message that is forwarded. If the target broker of the bridge crashes and then recovers, messages might be resent from the source broker. By setting use-duplicate-detection to true, any duplicate messages will be filtered out and ignored on receipt at the target broker. The default is true.</td>
</tr>
</tbody>
</table>
APPENDIX D. COMMAND-LINE TOOLS

AMQ Broker includes a set of command-line interface (CLI) tools so you can manage your messaging journal. The table below lists the name for each tool and its description.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exp</td>
<td>Exports the message data using a special and independent XML format.</td>
</tr>
<tr>
<td>imp</td>
<td>Imports the journal to a running broker using the output provided by exp.</td>
</tr>
<tr>
<td>data</td>
<td>Prints reports about journal records and compacts their data.</td>
</tr>
<tr>
<td>encode</td>
<td>Shows an internal format of the journal encoded to String.</td>
</tr>
<tr>
<td>decode</td>
<td>Imports the internal journal format from encode.</td>
</tr>
</tbody>
</table>

For a full list of commands available for each tool, use the help parameter followed by the tool’s name. In the example below, the CLI output lists all the commands available to the data tool after the user entered the command ./artemis help data.

```
$ ./artemis help data

NAME
  artemis data - data tools group
  (print|imp|exp|encode|decode|compact) (example ./artemis data print)

SYNOPSIS
  artemis data
  artemis data compact [--broker <brokerConfig>] [--verbose]
    [--paging <paging>] [--journal <journal>]
    [--large-messages <largeMessages>] [--bindings <binding>]
  artemis data decode [--broker <brokerConfig>] [--suffix <suffix>]
    [--directory <directory>] --input <input> [--journal <journal>]
    [--large-messages <largeMessages>] [--bindings <binding>]
  artemis data encode [--directory <directory>] [--broker <brokerConfig>]
    [--suffix <suffix>] [--verbose] [--paging <paging>] [--prefix <prefix>]
    [--file-size <size>] [--journal <journal>]
    [--large-messages <largeMessages>] [--bindings <binding>]
  artemis data exp [--broker <brokerConfig>] [--verbose]
    [--paging <paging>] [--journal <journal>]
    [--large-messages <largeMessages>] [--bindings <binding>]
  artemis data imp [--host <host>] [--verbose] [--port <port>]
    [--password <password>] [--transaction] --input <input> [--user <user>]
  artemis data print [--broker <brokerConfig>] [--verbose]
    [--paging <paging>] [--journal <journal>]
    [--large-messages <largeMessages>] [--bindings <binding>]

COMMANDS
  With no arguments, Display help information
```
You can use the help at the tool for more information on how to execute each of the tool’s commands. For example, the CLI lists more information about the **data print** command after the user enters the `./artemis help data print`.

```
$ ./artemis help data print

NAME
   artemis data print - Print data records information (WARNING: don't use while a production server is running)

SYNOPSIS
   artemis data print [--bindings <binding>] [--journal <journal>] [--paging <paging>]

OPTIONS
   --bindings <binding>
      The folder used for bindings (default ../data/bindings)

   --journal <journal>
      The folder used for messages journal (default ../data/journal)

   --paging <paging>
      The folder used for paging (default ../data/paging)
```
## APPENDIX E. MESSAGING JOURNAL CONFIGURATION ELEMENTS

The table below lists all of the configuration elements related to the AMQ Broker messaging journal.

### Table E.1. Address Setting Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>journal-directory</td>
<td>The directory where the message journal is located. The default value is <code>BROKER_INSTANCE_DIR/data/journal</code>. For the best performance, the journal should be located on its own physical volume in order to minimize disk head movement. If the journal is on a volume that is shared with other processes that may be writing other files (for example, bindings journal, database, or transaction coordinator) then the disk head may well be moving rapidly between these files as it writes them, thus drastically reducing performance. When using a SAN, each journal instance should be given its own LUN (logical unit).</td>
</tr>
<tr>
<td>create-journal-dir</td>
<td>If set to <code>true</code>, the journal directory will be automatically created at the location specified in <code>journal-directory</code> if it does not already exist. The default value is <code>true</code>.</td>
</tr>
<tr>
<td>journal-type</td>
<td>Valid values are <code>NIO</code> or <code>ASYNCIO</code>. If set to <code>NIO</code>, the broker uses Java NIO interface to its journal. Set to <code>ASYNCIO</code>, and the broker will use the Linux asynchronous IO journal. If you choose <code>ASYNCIO</code> but are not running Linux or you do not have <code>libaio</code> installed then the broker will detect this and automatically fall back to using <code>NIO</code>.</td>
</tr>
<tr>
<td>journal-sync-transactional</td>
<td>If set to <code>true</code>, the broker flushes all transaction data to disk on transaction boundaries (that is, commit, prepare, and rollback). The default value is <code>true</code>.</td>
</tr>
<tr>
<td>journal-sync-non-transactional</td>
<td>If set to <code>true</code>, the broker flushes non-transactional message data (sends and acknowledgements) to disk each time. The default value is <code>true</code>.</td>
</tr>
<tr>
<td>journal-file-size</td>
<td>The size of each journal file in bytes. The default value is <code>10485760</code> bytes (10MiB).</td>
</tr>
<tr>
<td>journal-min-files</td>
<td>The minimum number of files the broker pre-creates when starting. Files are pre-created only if there is no existing message data. Depending on how much data you expect your queues to contain at steady state, you should tune this number of files to match the total amount of data expected.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>journal-pool-files</td>
<td>The system will create as many files as needed; however, when reclaiming files it will shrink back to <em>journal-pool-files</em>. The default value is <em>-1</em>, meaning it will never delete files on the journal once created. The system cannot grow infinitely, however, as you are still required to use paging for destinations that can grow indefinitely.</td>
</tr>
<tr>
<td>journal-max-io</td>
<td>Controls the maximum number of write requests that can be in the IO queue at any one time. If the queue becomes full then writes will block until space is freed up. When using NIO, this value should always be <em>1</em>. When using AIO, the default value is <em>500</em>. The total max AIO can’t be higher than the value set at the OS level (<em>/proc/sys/fs/aio-max-nr</em>), which is usually at 65536.</td>
</tr>
<tr>
<td>journal-buffer-timeout</td>
<td>Controls the timeout for when the buffer will be flushed. AIO can typically withstand with a higher flush rate than NIO, so the system maintains different default values for both NIO and AIO. The default value for NIO is <em>3333333</em> nanoseconds, or 300 times per second, and the default value for AIO is <em>50000</em> nanoseconds, or 2000 times per second. By increasing the timeout value, you might be able to increase system throughput at the expense of latency, since the default values are chosen to give a reasonable balance between throughput and latency.</td>
</tr>
<tr>
<td>journal-buffer-size</td>
<td>The size of the timed buffer on AIO. The default value is <em>490KiB</em>.</td>
</tr>
<tr>
<td>journal-compact-min-files</td>
<td>The minimal number of files necessary before the broker compacts the journal. The compacting algorithm will not start until you have at least <em>journal-compact-min-files</em>. The default value is <em>10</em>. Setting the value to <em>0</em> will disable compacting and could be dangerous because the journal could grow indefinitely.</td>
</tr>
<tr>
<td>journal-compact-percentage</td>
<td>The threshold to start compacting. Journal data will be compacted if less than <em>journal-compact-percentage</em> is determined to be live data. Note also that compacting will not start until you have at least <em>journal-compact-min-files</em> data files on the journal. The default value is <em>30</em>.</td>
</tr>
</tbody>
</table>
APPENDIX F. REPLICATION HIGH AVAILABILITY CONFIGURATION ELEMENTS

The following tables list the valid ha-policy configuration elements when using a replication HA policy.

Table F.1. Configuration Elements Available when Using Replication High Availability

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>check-for-live-server</td>
<td>Applies to master brokers only. Determines whether the master checks the cluster for another master server using its own server ID when starting up. Set to true if you want to fail back to the original master broker. The default is false.</td>
</tr>
<tr>
<td>cluster-name</td>
<td>Name of the cluster configuration to use for replication. This setting is only necessary if you configure multiple cluster connections. If configured, the cluster configuration with this name will be used when connecting to the cluster. If unset, the first cluster connection defined in the configuration is used.</td>
</tr>
<tr>
<td>group-name</td>
<td>If set, slave brokers will only pair with master brokers with the matching group-name.</td>
</tr>
<tr>
<td>initial-replication-sync-timeout</td>
<td>The amount of time the replicating broker will wait at the completion of the initial replication process for the replica to acknowledge it has received all the necessary data. The default is 30,000 milliseconds, or 30 seconds.</td>
</tr>
<tr>
<td>max.saved.replicated-journals-size</td>
<td>Applies to slave brokers only. Specifies how many times a slave broker can restart after moving its files on start. Once there are this number of slave journal files the broker will stop permanently after if fails back. The default is 2.</td>
</tr>
<tr>
<td>allow-failback</td>
<td>Applies to slave brokers only. Determines whether the slave broker will automatically restart and resume its original role when another broker places a request to take over its place. The default is true.</td>
</tr>
</tbody>
</table>

Revised on 2019-10-11 11:27:07 UTC