



# **Red Hat JBoss Middleware for OpenShift 3 Red Hat JBoss A-MQ for OpenShift**

---

Learn to install and develop with Red Hat JBoss A-MQ for OpenShift

Red Hat JBoss Middleware for OpenShift Documentation  
Team



Red Hat JBoss Middleware for OpenShift 3 Red Hat JBoss A-MQ for OpenShift

---

Learn to install and develop with Red Hat JBoss A-MQ for OpenShift

## Legal Notice

Copyright © 2016 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

Guide to using the Red Hat JBoss A-MQ for OpenShift

---

## Table of Contents

<b>CHAPTER 1. INTRODUCTION</b>	<b>3</b>
1.1. WHAT IS RED HAT JBOSS A-MQ?	3
<b>CHAPTER 2. BEFORE YOU BEGIN</b>	<b>4</b>
2.1. COMPARISON: RED HAT JBOSS A-MQ FOR OPENSIFT AND A-MQ FOR OPENSIFT IMAGE	4
<b>CHAPTER 3. USING THE A-MQ FOR OPENSIFT IMAGE STREAMS AND APPLICATION TEMPLATES</b>	<b>5</b>
3.1. VERSION COMPATIBILITY AND SUPPORT	5
3.2. INITIAL SETUP	5
<b>CHAPTER 4. GET STARTED</b>	<b>6</b>
4.1. USING THE A-MQ FOR OPENSIFT IMAGE STREAMS AND APPLICATION TEMPLATES	6
4.2. DEPLOYMENT CONSIDERATIONS FOR THE A-MQ FOR OPENSIFT IMAGE	6
4.3. UPGRADING THE IMAGE REPOSITORY	8
<b>CHAPTER 5. TUTORIALS</b>	<b>10</b>
5.1. EXAMPLE DEPLOYMENT WORKFLOW	10
<b>CHAPTER 6. REFERENCE</b>	<b>13</b>
6.1. APPLICATION TEMPLATE PARAMETERS FOR PERSISTENT CONFIGURATION	13
6.2. SECURITY	14
6.3. LOGGING	15



# CHAPTER 1. INTRODUCTION

## 1.1. WHAT IS RED HAT JBOSS A-MQ?

Red Hat JBoss A-MQ (A-MQ) is available as a containerized image that is designed for use with OpenShift. It allows developers to quickly deploy an A-MQ message broker in a hybrid cloud environment.

A-MQ, based on Apache ActiveMQ, is a JMS 1.1-compliant messaging system. It consists of a broker and client-side libraries that enable remote communication among distributed client applications. A-MQ provides numerous connectivity options and can communicate with a wide variety of non-JMS clients through its support of the OpenWire and STOMP wire protocols.

## CHAPTER 2. BEFORE YOU BEGIN

### 2.1. COMPARISON: RED HAT JBOSS A-MQ FOR OPENSIFT AND A-MQ FOR OPENSIFT IMAGE

This topic details the differences between the regular release of JBoss A-MQ and the A-MQ for OpenShift image, and provides instructions specific to running and configuring the A-MQ for OpenShift image. Documentation for other JBoss A-MQ functionality not specific to the A-MQ for OpenShift image can be found in the [Red Hat JBoss A-MQ documentation on the Red Hat Customer Portal](#).

Differences between the regular release of JBoss A-MQ and the A-MQ for OpenShift image:

- ✎ The Karaf shell is not available.
- ✎ The Fuse Management Console (Hawtio) is not available.
- ✎ To connect to the A-MQ web console, click the **Connect** button in the A-MQ pod of the OpenShift web console, or the **Open Java Console** button in OpenShift 3.2.
- ✎ Configuration of the broker can be performed:
  - using parameters specified in the A-MQ application template, as described in Application Template Parameters section.
  - using the S2I (Source-to-image) tool, as described in Configuration Using S2I section.
- ✎ Clients for the A-MQ xPaaS image need to specify the OpenShift API port (443) when setting the broker URL for SSL connections. Otherwise, A-MQ will attempt to use the default SSL port (61617).

## CHAPTER 3. USING THE A-MQ FOR OPENSIFT IMAGE STREAMS AND APPLICATION TEMPLATES

Red Hat JBoss Middleware for OpenShift images were automatically created during the installation of OpenShift along with the other default image streams and templates.

### 3.1. VERSION COMPATIBILITY AND SUPPORT

See the xPaaS part of the [OpenShift and Atomic Platform Tested Integrations page](#) for details about OpenShift image version compatibility.

### 3.2. INITIAL SETUP

The Tutorials in this guide follow on from and assume an OpenShift instance similar to that created in the [OpenShift Primer](#).

## CHAPTER 4. GET STARTED

### 4.1. USING THE A-MQ FOR OPENSIFT IMAGE STREAMS AND APPLICATION TEMPLATES

{prodctname} images were [automatically created during the installation](#) of OpenShift along with the other default image streams and templates.

### 4.2. DEPLOYMENT CONSIDERATIONS FOR THE A-MQ FOR OPENSIFT IMAGE

#### 4.2.1. Creating the Service Account

The A-MQ for OpenShift image requires a service account for deployments. For multiple node deployments, the service account must have the **view** role enabled so that it can manage the various pods in the cluster. In addition, you will need to configure SSL to enable connections to A-MQ from outside of the OpenShift instance.

1. Create the service account:

```
$ echo '{"kind": "ServiceAccount", "apiVersion": "v1",
"metadata": {"name": "<service-account-name>"}}' | oc create -f -
```

OpenShift 3.2 users can use the following command to create the service account:

```
$ oc create serviceaccount <service-account-name>
```

2. Add the **view** role to the service account:

```
$ oc policy add-role-to-user view system:serviceaccount:<project-
name>:<service-account-name>
```

#### 4.2.2. Configuring SSL

For a minimal SSL configuration to allow for connections outside of OpenShift, A-MQ requires a broker keyStore, a client keyStore, and a client trustStore that includes the broker keyStore. The broker keyStore is also used to create a secret for the A-MQ for OpenShift image, which is added to the service account.

The following example commands use **keytool**, a package included with the Java Development Kit, to generate the necessary certificates and stores:

1. Generate a self-signed certificate for the broker keyStore:

```
$ keytool -genkey -alias broker -keyalg RSA -keystore broker.ks
```

2. Export the certificate so that it can be shared with clients:

```
$ keytool -export -alias broker -keystore broker.ks -file
broker_cert
```

3. Generate a self-signed certificate for the client keyStore:

```
$ keytool -genkey -alias client -keyalg RSA -keystore client.ks
```

4. Create a client trustStore that imports the broker certificate:

```
$ keytool -import -alias broker -keystore client.ts -file  
broker_cert
```

### 4.2.3. Generating the A-MQ Secret

The broker keyStore can then be used to generate a secret for the namespace, which is also added to the service account so that the applications can be authorized:

```
$ oc secrets new <secret-name> <broker-keystore> <broker-truststore>
```

```
$ oc secrets add sa/<service-account-name> secret/<secret-name>
```

### 4.2.4. Creating a Route

After the A-MQ for OpenShift image has been deployed, an SSL route needs to be created for the A-MQ transport protocol port to allow connections to A-MQ outside of OpenShift.

In addition, selecting **Passthrough** for **TLS Termination** relays all communication to the A-MQ broker without the OpenShift router decrypting and resending it. Only SSL routes can be exposed because the OpenShift router requires SNI to send traffic to the correct service. See [Secured Routes](#) for more information.

The default ports for the various A-MQ transport protocols are:

**61616/TCP** (OpenWire)

**61617/TCP** (OpenWire+SSL)

**5672/TCP** (AMQP)

**5671/TCP** (AMQP+SSL)

**1883/TCP** (MQTT)

**8883/TCP** (MQTT+SSL)

**61613/TCP** (STOMP)

**61612/TCP** (STOMP+SSL)

### 4.2.5. Scaling Up and Persistent Storage Partitioning

There are two methods for deploying A-MQ with persistent storage: single-node and multi-node partitioning. Single-node partitioning stores the A-MQ logs and the kahadb store directory, with the message queue data, in the storage volume. Multi-node partitioning creates additional, independent **split-*n*** directories to store the messaging queue data for each broker, where *n* is an incremental integer. This communication is not altered if a broker pod is updated, goes down unexpectedly, or is redeployed. When the broker pod is operational again, it reconnects to the associated split directory and continues as before. If a new broker pod is added, a corresponding **split-*n*** directory is created for that broker.

 **Important**

Due to the different storage methods of single-node and multi-node partitioning, changing a deployment from single-node to multi-node results in the application losing all previously stored messages. This is also true if changing a deployment from multi-node to single-node, as the storage paths will not match.

Similarly, if a [Rolling Strategy](#) is implemented, the **maxSurge** parameter must be set to **0%**, otherwise the new broker creates a new partition and be unable to connect to the stored messages.

In multi-node partitioning, OpenShift routes new connections to the broker pod with the least amount of connections. Once this connection has been made, messages from that client are sent to the same broker every time, even if the client is run multiple times. This is because the OpenShift router is set to route requests from a client with the same IP to the same pod.

You can see which broker pod is connected to which split directory by viewing the logs for the pod, or by connecting to the broker console. In the **ActiveMQ** tab of the console, the **PersistenceAdapter** shows the **KahaDBPersistenceAdapter**, which includes the split directory as part of its name.

#### 4.2.6. Customizing A-MQ Configuration Files for Deployment

If using a template from an alternate repository, A-MQ configuration files such as **user.properties** can be included. When the image is downloaded for deployment, these files are copied to the **<amq-home>/amq/conf/** directory on the broker, which are committed to the container and pushed to the registry.

 **Note**

If using this method, it is important that the placeholders in the configuration files (such as **##### AUTHENTICATION #####**) are not removed as these placeholders are necessary for building the A-MQ for OpenShift image.

#### 4.2.7. Configuring Client Connections

Clients for the A-MQ for OpenShift image must specify the OpenShift router port (443) when setting the broker URL for SSL connections. Otherwise, A-MQ attempts to use the default SSL port (61617). Including the failover protocol in the URL preserves the client connection in case the pod is restarted or upgraded, or there is a disruption on the router.

```
...
factory.setBrokerURL("failover://ssl://<route-to-broker-pod>:443");
...
```

### 4.3. UPGRADING THE IMAGE REPOSITORY

On your master host(s), ensure you are logged into the CLI as a cluster administrator or user that has project administrator access to the global "openshift" project. For example:

```
$ oc login -u system:admin
```

■

Then, run the following command to update the core A-MQ OpenShift image stream in the "openshift" project:

```
$ oc -n openshift import-image jboss-amq-62
```

Depending on the deployment configuration, OpenShift deletes one of the broker pods and start a new upgraded pod. The new pod connects to the same persistent storage so that no messages are lost in the process. Once the upgraded pod is running, the process is repeated for the next pod until all of the pods have been upgraded.

If a [Rolling Strategy](#) has been configured, OpenShift deletes and recreate pods based on the rolling update settings. Any new pod will only connect to the same persistent storage if the **maxSurge** parameter is set to **0%**, otherwise the new pod creates a new partition and will not be able to connect to the stored messages in the previous partition.

## CHAPTER 5. TUTORIALS

### 5.1. EXAMPLE DEPLOYMENT WORKFLOW

This tutorial prepares and deploys a multi-node A-MQ instance with persistent storage.

#### 5.1.1. Preparing A-MQ Deployment

1. Create a new project:

```
$ oc new-project amq-demo
```

2. Create a service account to be used for the A-MQ deployment:

```
$ echo '{"kind": "ServiceAccount", "apiVersion": "v1",  
  "metadata": {"name": "amq-service-account"}}' | oc create -f -
```

3. Add the view role to the service account. This enables the service account to view all the resources in the amq-demo namespace, which is necessary for managing the cluster when using the Kubernetes REST API agent for discovering the mesh endpoints.

```
$ oc policy add-role-to-user view system:serviceaccount:amq-  
demo:amq-service-account
```

4. A-MQ requires a broker keyStore, a client keyStore, and a client trustStore that includes the broker keyStore.

This example uses 'keytool', a package included with the Java Development Kit, to generate dummy credentials for use with the A-MQ installation.

- a. Generate a self-signed certificate for the broker keyStore:

```
$ keytool -genkey -alias broker -keyalg RSA -keystore  
broker.ks
```

- b. Export the certificate so that it can be shared with clients:

```
$ keytool -export -alias broker -keystore broker.ks -file  
broker_cert
```

- c. Generate a self-signed certificate for the client keyStore:

```
$ keytool -genkey -alias client -keyalg RSA -keystore  
client.ks
```

- d. Create a client trust store that imports the broker certificate:

```
$ keytool -import -alias broker -keystore client.ts -file  
broker_cert
```

5. Use the broker keyStore file to create the A-MQ secret:

```
$ oc secrets new amq-app-secret broker.ks
```

6. Add the secret to the service account created earlier:

```
$ oc secrets add sa/amq-service-account secret/amq-app-secret
```

### 5.1.2. Deployment

1. Log in to the OpenShift web console and select the amq-demo project space.
2. Click **Add to Project** to list all of the default image streams and templates.
3. Use the Filter by keyword search bar to limit the list to those that match amq. You may need to click **See all** to show the desired application template.
4. Select the template. This example uses the *amq62-persistent-ssl* template to allow for persistent storage.

#### *Example Template:*

##### **APPLICATION\_NAME**

broker

##### **MQ\_PROTOCOL**

openwire

##### **MQ\_USERNAME**

amq-demo-user

##### **MQ\_PASSWORD**

password

##### **VOLUME\_CAPACITY**

512Mi

##### **AMQ\_SECRET**

amq-app-secret

##### **AMQ\_TRUSTSTORE**

broker.ks

##### **AMQ\_TRUSTSTORE\_PASSWORD**

password

##### **AMQ\_KEYSTORE**

broker.ks

##### **AMQ\_KEYSTORE\_PASSWORD**

password

##### **AMQ\_MESH\_DISCOVERY\_TYPE**

kube

##### **AMQ\_MESH\_SERVICE\_NAME**

broker

##### **AMQ\_MESH\_SERVICE\_NAMESPACE**

amq-demo

##### **AMQ\_STORAGE\_USAGE\_LIMIT**

1 gb

##### **AMQ\_SPLIT**

true

##### **IMAGE\_STREAM\_NAMESPACE**

openshift

### 5.1.3. Post-Deployment

### Creating a route

Create a route for the broker so that clients outside of OpenShift can connect using SSL. By default, the OpenWire protocol uses the 61617/TCP port.

1. Click **Create a Route** and click **Show options for secured routes** to display all parameters.
2. Use the **Target Port** drop-down menu to select **61617/TCP**
3. Use the **TLS Termination** drop-down menu to select **Passthrough**. This will relay all communication to the A-MQ broker without the OpenShift router decrypting and resending it.
4. Clients can now connect to the broker by specifying the following in their configuration:

```
factory.setBrokerURL("failover://ssl://broker-amq-  
demo.example.com:443");
```

### Scaling up

Scale up by clicking the **Scale up** arrow in the *amq-demo* project **Overview** in the web console. Or, using the OpenShift command line:

```
$ oc scale dc amq-demo --replicas=3
```

### Connecting to the A-MQ Console

To connect to the A-MQ console from the OpenShift web console, navigate to the broker pod and click the **Connect** button located in the **Template** information.

For OpenShift 3.2, click the **Open Java Console** button.

## CHAPTER 6. REFERENCE

### 6.1. APPLICATION TEMPLATE PARAMETERS FOR PERSISTENT CONFIGURATION

Configuration of the A-MQ for OpenShift image is performed by specifying values of application template parameters. Different A-MQ images require different subsets of these parameters. The following parameters can be configured:

#### AMQ\_RELEASE

The A-MQ release version. This determines which A-MQ image will be used as a basis for the application. At the moment, only version 6.2 is available.

#### APPLICATION\_NAME

The name of the application used internally in OpenShift. It is used in names of services, pods, and other objects within the application.

#### MQ\_PROTOCOL

Comma-separated list of the messaging protocols used by the broker. Available options are `amqp`, `mqtt`, `openwire`, and `stomp`. If left empty, all available protocols will be available. Please note that for integration of the image with Red Hat JBoss Enterprise Application Platform, the OpenWire protocol must be specified, while other protocols can be optionally specified as well.

#### MQ\_QUEUES

Comma-separated list of queues available by default on the broker on its startup.

#### MQ\_TOPICS

Comma-separated list of topics available by default on the broker on its startup.

#### VOLUME\_CAPACITY

The size of the persistent storage for database volumes.

#### MQ\_USERNAME

The user name used for authentication to the broker. In a standard non-containerized JBoss A-MQ, you would specify the user name in the `<amq-home>/opt/user.properties` file. If no value is specified, a random user name is generated.

#### MQ\_PASSWORD

The password used for authentication to the broker. In a standard non-containerized JBoss A-MQ, you would specify the password in the `<amq-home>/opt/user.properties` file. If no value is specified, a random password is generated.

#### AMQ\_ADMIN\_USERNAME

The user name used as an admin authentication to the broker. If no value is specified, a random user name is generated.

#### AMQ\_ADMIN\_PASSWORD

The password used for authentication to the broker. If no value is specified, a random password is generated.

**AMQ\_SECRET**

The name of a secret containing SSL related files. If no value is specified, a random password is generated.

**AMQ\_TRUSTSTORE**

The SSL trustStore filename. If no value is specified, a random password is generated but SSL will not be configured.

**AMQ\_KEYSTORE**

The SSL keyStore filename. If no value is specified, a random password is generated but SSL will not be configured.

**AMQ\_TRUSTSTORE\_PASSWORD**

The password used to decrypt the SSL trustStore (optional).

**AMQ\_KEYSTORE\_PASSWORD**

The password used to decrypt the SSL keyStore (optional).

**AMQ\_MESH\_DISCOVERY\_TYPE**

The discovery agent type to use for discovering mesh endpoints. 'dns' will use the OpenShift DNS service to resolve endpoints. 'kube' will use Kubernetes REST API to resolve service endpoints. If using 'kube' the service account for the pod must have the 'view' role.

**AMQ\_MESH\_SERVICE\_NAME**

Name of service used for mesh creation.

**AMQ\_MESH\_SERVICE\_NAMESPACE**

The namespace in which the service resides. Must be specified if using **kube** discovery.

**AMQ\_STORAGE\_USAGE\_LIMIT**

The A-MQ storage usage limit.

**AMQ\_SPLIT**

Boolean. Setting to 'true' partitions the persistent volume, allowing for multiple A-MQ pods for scalability.

## 6.2. SECURITY

Only SSL connections can connect from outside of the OpenShift instance, regardless of the protocol specified in the **MQ\_PROTOCOL** property of the A-MQ application templates. The non-SSL version of the protocols can only be used inside the OpenShift instance.

For security reasons, using the default keyStore and trustStore generated by the system is discouraged. Generate your own keyStore and trustStore and supply them to the image using the OpenShift secrets mechanism or S2I.

## 6.3. LOGGING

In addition to viewing the OpenShift logs, you can troubleshoot a running A-MQ image by viewing the A-MQ logs that are outputted to the container's console:

```
$ oc logs -f <pod-name> <container-name>
```



### Note

By default, the A-MQ for OpenShift image does not have a file log handler configured. Logs are only sent to the console.