IBM MQ on the AWS Cloud

Quick Start Reference Deployment

August 2017

Arthur Barr, James McGuire, and Jon Tilt — IBM
Vinod Shukla and Scott Kellish — Amazon Web Services

Contents

Overview.................................................................................................................................2

Costs and Licenses................................................................................................................3
Architectures..........................................................................................................................4
Prerequisites ........................................................................................................................6
Specialized Knowledge ........................................................................................................5
Design Considerations ........................................................................................................6
IBM MQ Instances ..............................................................................................................6
Amazon EFS ........................................................................................................................7
Deployment Options ............................................................................................................7
Deployment Steps ...............................................................................................................7
Step 1. Prepare Your AWS Account ....................................................................................7
Step 2. Sign up for an IBM MQ License ............................................................................8
Step 3. Launch the Quick Start .........................................................................................8
Step 4. Test the Deployment Using the IBM MQ Console ...............................................14
Step 5. Connect to the IBM MQ Server .........................................................................19
Troubleshooting ................................................................................................................20
Security ..............................................................................................................................20
AWS Identity and Access Management (IAM) ...............................................................21
This Quick Start was created by IBM in partnership with Amazon Web Services (AWS).

Quick Starts are automated reference deployments that use AWS CloudFormation templates to launch, configure, and run the AWS compute, network, storage, and other services required to deploy a specific workload on AWS.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying a simple, highly available, production-ready IBM MQ server on the AWS Cloud.

IBM MQ is messaging middleware that simplifies and accelerates the integration of diverse applications and business data across multiple platforms. It uses message queues to facilitate the exchange of information, and offers a single messaging solution for cloud, mobile, the Internet of Things (IoT), and on-premises environments.

By connecting virtually everything, from a simple pair of applications to the most complex business environments, IBM MQ helps you improve business responsiveness, control costs, reduce risk, and gain real-time insight from mobile, IoT, and sensor data.

AWS offers flexible compute, storage, and database services that provide a scalable, secure cloud platform for running IBM MQ.

IBM MQ delivers:

- **Flexible, near-universal connectivity** to adapt systems to meet changing market demands and take advantage of emerging opportunities.
- **Secure message delivery** to preserve message integrity and mitigate risk of data loss.
- **Dynamic scaling** to improve business responsiveness and control costs.
- **Simplified management and control** to improve productivity.
• **A unified messaging solution** to simplify integration, lower cost of ownership, and accelerate application deployment.

For more information about IBM MQ features, see the [IBM MQ product page](#).

This Quick Start is for IT infrastructure decision makers and IBM MQ system administrators who require guidance on how to rapidly configure, deploy, and run an IBM MQ server on AWS. It deploys a reference architecture of a highly available, secure IBM MQ version 9 queue manager.

### Costs and Licenses

The Quick Start builds the IBM MQ environment by using a pre-built Amazon Machine Image (AMI) with IBM MQ installed on the Ubuntu operating system.

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using.

This Quick Start requires a license for IBM MQ. To use the Quick Start in your production environment, sign up for an IBM MQ program license at [IBM developerWorks](#). You’ll need to place the license key in an Amazon Simple Storage Service (Amazon S3) bucket and specify its location when you launch the Quick Start. (For details, see step 2 of the deployment instructions.)

If you don’t have a license file, the Quick Start will deploy an IBM MQ trial license, which allows 90 days of free usage in a non-production environment. After this time, the queue manager will expire. You can purchase support at an additional cost, or use the forums.

If the license file is in place at stack creation time, the IBM MQ server will automatically use the production license. To upgrade from a trial license to a production license after deployment, follow the instructions in the [IBM Knowledge Center](#).

The IBM MQ [software license agreement](#) contains more details about licensing terms. When you launch the Quick Start, you’ll be asked to read and agree to the terms of the agreement.
Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with default parameters builds the following IBM MQ environment in the AWS Cloud:

![Diagram of IBM MQ architecture on AWS]

The Quick Start sets up the following:

- A virtual private cloud (VPC) that spans two Availability Zones and includes two public and two private subnets, for security and high availability.*
- An Internet gateway to allow access to the Internet.*
- In a public subnet, a bastion host to provide secure Secure Shell (SSH) access to the IBM MQ server. The bastion host is in an Auto Scaling group of 1, ensuring there will always be one host available.*
- In a private subnet, an IBM MQ server in an Auto Scaling group of 1.

*Default parameters refer to the default settings used in the Quick Start deployment.
- Amazon Elastic File System (Amazon EFS) automatically mounted on the IBM MQ server instance for distributed storage, to ensure high availability of the queue manager service and the message data. If the IBM MQ server fails in one Availability Zone, a new server is created in the second Availability Zone and connected to the existing data so no persistent messages are lost. Failover typically takes 3-5 minutes, but can be longer if there are outstanding transactions.

- Elastic Load Balancing to automatically distribute connections to the active IBM MQ server.

- An IAM instance role with fine-grained permissions for access to AWS services necessary for the deployment process.

- Appropriate security groups for each instance or function to restrict access to only necessary protocols and ports. For example, access to HTTP server ports on Amazon EC2 servers is limited to Elastic Load Balancing.

* You can choose to create a new VPC for the IBM MQ deployment or use your existing VPC on AWS. The template that deploys the Quick Start into an existing VPC skips the components marked by asterisks.

Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see the Getting Started Resource Center.)

- **Amazon EC2** – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.

- **Amazon VPC** – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, subnet creation, and configuration of route tables and network gateways.

- **AWS CloudFormation** – AWS CloudFormation gives you an easy way to create and manage a collection of related AWS resources, and provision and update them in an orderly and predictable way. You use a template to describe all the AWS resources (e.g.,
EC2 instances) that you want. You don’t have to create and configure the resources or figure out dependencies; AWS CloudFormation handles all of that.

- **Auto Scaling** – Auto Scaling helps maintain high availability and manage capacity by automatically increasing or decreasing the EC2 instance fleet. You can use Auto Scaling to run your fleet at optimal utilization by increasing instance capacity during demand spikes and decreasing capacity during down times.

- **ELB** – Elastic Load Balancing automatically distributes incoming application traffic across multiple EC2 instances.

- **Amazon EFS** – Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with EC2 instances. This IBM MQ deployment uses Amazon EFS to ensure high availability of message data in case of server failure.

- **IAM** – AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. With IAM, you can manage users, security credentials such as access keys, and permissions that control which AWS resources users can access, from a central location.

**Design Considerations**

IBM MQ provides a messaging platform that can be deployed with a variety of options, depending on your needs. This Quick Start provides a great starting point for building your messaging solution rapidly with IBM MQ on the AWS Cloud. The following sections discuss design considerations for large-scale deployments and options for optimizing performance.

To enhance availability and reliability for production workloads, this Quick Start uses two Availability Zones. This provides an automated failover from the primary server to a server that runs in a different Availability Zone, with no loss of message or configuration data.

The IBM MQ service will support client messaging applications from within your VPC, from trusted addresses on the Internet, and via a VPN from your on-premises environment.

**IBM MQ Instances**

The deployment launches an EC2 instance running Ubuntu Linux x86-64. Elastic Load Balancing is used to automatically ensure that traffic is pointed to an active server.

The Quick Start supports a large selection of EC2 instance types for the IBM MQ server instances. We recommend that you benchmark the environment to make sure you achieve the level of performance you need before starting a production deployment.
Amazon EFS
Amazon EFS is a file storage service with a simple interface that enables you to create and configure file systems quickly and easily. Multiple EC2 instances can access an Amazon EFS file system at the same time, so this service provides a common data source for workloads and applications that are running on more than one EC2 instance.

In the architecture built by this Quick Start, only one EC2 instance will access the data at a specific time.

Deployment Options
This Quick Start provides two deployment options:

- **Deploy IBM MQ into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, security groups, bastion hosts, and other infrastructure components, and then deploys IBM MQ into this new VPC.

- **Deploy IBM MQ into an existing VPC**. This option provisions IBM MQ in your existing AWS infrastructure.

The Quick Start also lets you configure additional settings such as CIDR blocks, instance types, and IBM MQ settings, as discussed later in this guide.

Deployment Steps
**Step 1. Prepare Your AWS Account**

1. If you don’t already have an AWS account, create one at [https://aws.amazon.com](https://aws.amazon.com) by following the on-screen instructions.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy IBM MQ on AWS.

   **Important** This Quick Start uses Amazon EFS, which is supported only in the regions listed on the [AWS Regions and Endpoints](https://aws.amazon.com/regions) webpage.

3. Create a [key pair](https://aws.amazon.com/) in your preferred region.

4. If necessary, request a service limit increase for the Amazon EC2 instance types that you intend to deploy. To do this, in the AWS Support Center, choose **Create Case, Service Limit Increase, EC2 instances**, and then complete the fields in the limit increase form.
Step 2. Sign up for an IBM MQ License

To use the Quick Start in your production environment, you must have an IBM MQ program license. If you’d like to try out the software first, skip this step. The Quick Start will automatically sign you up for a 90-day trial period, and you can add a program license later.

To get a program license:

1. Sign up for an IBM MQ program license at IBM developerWorks.

2. Place the license key file for the software in an S3 bucket. You’ll be prompted for the bucket name and license file name in step 3.

Step 3. Launch the Quick Start

**Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.

   Option 1  
   Deploy IBM MQ into a new VPC on AWS
   ![Launch](Launch)

   Option 2  
   Deploy IBM MQ into an existing VPC on AWS
   ![Launch](Launch)

**Important** If you are deploying IBM MQ into an existing VPC, make sure that your VPC has two private subnets in different Availability Zones for the queue manager instances. You’ll also need the domain name option configured in the DHCP options as explained in the Amazon VPC documentation. You will be prompted for your VPC settings when you launch the Quick Start.

Your existing VPC should have at least one bastion host and associated security group so you can SSH into the IBM MQ server instance. (To set up bastion hosts, see the Linux bastion host Quick Start.)

Each deployment takes about 30 minutes to complete.
2. Check the region that is displayed in the upper-right corner of the navigation bar. This is where the network infrastructure for IBM MQ will be built. The template is launched in the US East (Ohio) Region by default. You can change the region.

**Important**  This Quick Start uses Amazon EFS, which is supported only in the regions listed on the [AWS Regions and Endpoints](https://aws.amazon.com/about-aws/global-infrastructure/regions-endpoints/) webpage.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

In the following tables, parameters are listed by category and described separately for the two deployment options:

- Parameters for deploying IBM MQ into a new VPC
- Parameters for deploying IBM MQ into an existing VPC

- **Option 1: Parameters for deploying IBM MQ into a new VPC**

  **View template**

  **Software License Agreement**:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Agreement</td>
<td>Requires input</td>
<td>To deploy this Quick Start, you must accept the terms of the IBM MQ license agreement. After you read the agreement, choose <strong>I agree</strong> to confirm your acceptance of the licensing terms.</td>
</tr>
</tbody>
</table>

  **VPC & Bastion Configuration**:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Zones</td>
<td>Requires input</td>
<td>The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.</td>
</tr>
<tr>
<td>Allowed Bastion External Access CIDR</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access the IBM MQ server through the bastion host. We recommend that you set this value to a trusted IP range. For example, you might</td>
</tr>
<tr>
<td>Parameter label (name)</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allowed Admin Web Console External Access CIDR</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access the IBM MQ Console through the ELB load balancer. We recommend that you set this value to a trusted IP range.</td>
</tr>
<tr>
<td>(AdminConsoleAccessCIDR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowed Client Application External Access CIDR</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access IBM MQ client applications. We recommend that you set this value to a trusted IP range.</td>
</tr>
<tr>
<td>(ClientAppAccessCIDR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Name</td>
<td>Requires input</td>
<td>Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.</td>
</tr>
<tr>
<td>(KeyPairName)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bastion AMI Operating System</td>
<td>Amazon-Linux-HVM</td>
<td>The Linux distribution for the AMI to be used for the bastion host instances. If you choose CentOS, make sure that you have a subscription to the <a href="https://aws.amazon.com/marketplace/pp/B00TJFJK20">CentOS AMI in AWS Marketplace</a>.</td>
</tr>
<tr>
<td>(BastionAMIOS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bastion Instance Type</td>
<td>t2.micro</td>
<td>EC2 instance type for the bastion host instances.</td>
</tr>
<tr>
<td>(BastionInstanceType)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IBM MQ Instance Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM MQ Instance Owner</td>
<td>ibm-mq</td>
<td>The owner tag for the IBM MQ server instance.</td>
</tr>
<tr>
<td>(MQOwner)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM MQ Instance Name</td>
<td>ibm-mq</td>
<td>Name for the IBM MQ server instance.</td>
</tr>
<tr>
<td>(MQInstanceName)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM MQ Instance Type</td>
<td>t2.micro</td>
<td>EC2 instance type for the IBM MQ server.</td>
</tr>
<tr>
<td>(MQInstanceType)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queue Manager Name</td>
<td>QM1</td>
<td>The name to use for the IBM MQ queue manager. This string can include a maximum of 48 characters, consisting of uppercase letters, numbers, periods (.), underscores (_), and percent signs (%). See the IBM Knowledge Center for naming rules.</td>
</tr>
<tr>
<td>(QueueManagerName)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM MQ Web Console Admin Username</td>
<td>mqconsoleadmin</td>
<td>Administrator user name for accessing the IBM MQ Console and REST API.</td>
</tr>
<tr>
<td>(MQConsoleUsername)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM MQ Web Console Admin Password</td>
<td>Requires input</td>
<td>Administrator password for accessing the IBM MQ Console and REST API. This is an 8-12 character string.</td>
</tr>
<tr>
<td>(MQConsolePassword)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mqadmin Password</td>
<td>Requires input</td>
<td>Password for predefined mqadmin user, which is used to administer IBM MQ. See the IBM Knowledge Center for information on authority to administer IBM MQ. This is an 8-12 character string.</td>
</tr>
<tr>
<td>(MQAdminPassword)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter label (name)</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>mqapp Password</strong></td>
<td>Requires input</td>
<td>Password for predefined <strong>mqapp</strong> user, which applications use to securely connect to IBM MQ. See the IBM Knowledge Center for details on authorization for applications to use IBM MQ. This is an 8-12 character string.</td>
</tr>
</tbody>
</table>

**IBM MQ License:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IBM MQ License Bucket Name</strong></td>
<td>Optional</td>
<td>The name of the S3 bucket that contains your IBM MQ license key file, from step 2. Leave this parameter blank to use the 90-day trial license.</td>
</tr>
<tr>
<td><strong>IBM MQ License S3 Key Prefix Name</strong></td>
<td>Optional</td>
<td>The S3 key name prefix for the directory in which your IBM MQ license key file is stored, from step 2. Leave this parameter blank to use the 90-day trial license.</td>
</tr>
</tbody>
</table>

**AWS Quick Start Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quick Start S3 Bucket Name</strong></td>
<td>aws-quickstart</td>
<td>S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you’ve created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.</td>
</tr>
<tr>
<td><strong>Quick Start S3 Key Prefix</strong></td>
<td>quickstart-ibm-mq/</td>
<td>The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.</td>
</tr>
</tbody>
</table>

- **Option 2: Parameters for deploying IBM MQ into an existing VPC**

  View template

**Software License Agreement:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>License Agreement</strong></td>
<td>Requires input</td>
<td>To deploy this Quick Start, you must accept the terms of the IBM MQ license agreement. After you read the agreement, choose I agree to confirm your acceptance of the licensing terms.</td>
</tr>
</tbody>
</table>
## Network Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC ID (VPCID)</td>
<td>Requires input</td>
<td>ID of your existing VPC (e.g., vpc-0343606e).</td>
</tr>
<tr>
<td>Private Subnet 1 ID (PrivateSubnet1ID)</td>
<td>Requires input</td>
<td>ID of the private subnet in Availability Zone 1 in your existing VPC (e.g., subnet-a0246dcd).</td>
</tr>
<tr>
<td>Private Subnet 2 ID (PrivateSubnet2ID)</td>
<td>Requires input</td>
<td>ID of the private subnet in Availability Zone 2 in your existing VPC.</td>
</tr>
<tr>
<td>Public Subnet 1 ID (PublicSubnet1ID)</td>
<td>Requires input</td>
<td>ID of the public (DMZ) subnet in Availability Zone 1 in your existing VPC (e.g., subnet-b58c3d67).</td>
</tr>
<tr>
<td>Public Subnet 2 ID (PublicSubnet2ID)</td>
<td>Requires input</td>
<td>ID of the public (DMZ) subnet in Availability Zone 2 in your existing VPC.</td>
</tr>
<tr>
<td>Allowed Admin Web Console External Access CIDR (AdminConsoleAccessCIDR)</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access the IBM MQ Console through the ELB load balancer. We recommend that you set this value to a trusted IP range.</td>
</tr>
<tr>
<td>Allowed Client Application External Access CIDR (ClientAppAccessCIDR)</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access IBM MQ client applications. We recommend that you set this value to a trusted IP range.</td>
</tr>
</tbody>
</table>

## Bastion Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Key Name (KeyPairName)</td>
<td>Requires input</td>
<td>Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region. All instances will launch with this key pair.</td>
</tr>
<tr>
<td>Bastion Security Group ID (BastionSecurityGroupID)</td>
<td>Requires input</td>
<td>ID of the bastion security group in your existing VPC (e.g., sg-7f16e910).</td>
</tr>
</tbody>
</table>

## IBM MQ Instance Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM MQ Instance Owner (MQOwner)</td>
<td>ibm-mq</td>
<td>The owner tag for the IBM MQ server instance.</td>
</tr>
<tr>
<td>IBM MQ Instance Name (MQInstanceName)</td>
<td>ibm-mq</td>
<td>Name for the IBM MQ server instance.</td>
</tr>
<tr>
<td>IBM MQ Instance Type (MQInstanceType)</td>
<td>t2.micro</td>
<td>EC2 instance type for the IBM MQ server.</td>
</tr>
<tr>
<td>Queue Manager Name (QueueManagerName)</td>
<td>QM1</td>
<td>The name to use for the IBM MQ queue manager. This string can include a maximum of 48 characters, consisting of</td>
</tr>
</tbody>
</table>
### Parameter label (name) | Default | Description
---|---|---
**IBM MQ Web Console Admin Username** *(MQConsoleUsername)* | mqconsoleadmin | Administrator user name for accessing the IBM MQ Console and REST API.

**IBM MQ Web Console Admin Password** *(MQConsolePassword)* | Requires input | Administrator password for accessing the IBM MQ Console and REST API. This is an 8-12 character string.

**mqadmin Password** *(MQAdminPassword)* | Requires input | Password for predefined mqadmin user, which is used to administer IBM MQ. See the IBM Knowledge Center for information on authority to administer IBM MQ. This is an 8-12 character string.

**mqapp Password** *(MQAppPassword)* | Requires input | Password for predefined mqapp user, which applications use to securely connect to IBM MQ. See the IBM Knowledge Center for details on authorization for applications to use IBM MQ. This is an 8-12 character string.

### IBM MQ License:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
**IBM MQ License Bucket Name** *(LicenseS3Bucket)* | Optional | The name of the S3 bucket that contains your IBM MQ license key file, from step 2. Leave this parameter blank to use the 90-day trial license. |

**IBM MQ License S3 Key Prefix Name** *(LicenseS3KeyPrefix)* | Optional | The S3 key name prefix for the directory in which your IBM MQ license key file is stored, from step 2. Leave this parameter blank to use the 90-day trial license. |

5. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you’re done, choose **Next**.

6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.

7. Choose **Create** to deploy the stack.

8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the IBM MQ environment is ready.

9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.
Note This Quick Start deployment is automated by nested AWS CloudFormation templates. The main template builds the network-related resources first, using the VPC template, and then launches separate stacks for the bastion host and IBM MQ. Deleting the main template deletes the entire stack.

Step 4. Test the Deployment Using the IBM MQ Console

When the AWS CloudFormation template has successfully created the stack, all server nodes will be running with the software installed in your AWS account.

In the following steps, you’ll connect to IBM MQ through a web console to verify the deployment, and then use the console to explore IBM MQ features.

To connect to IBM MQ through the web console:

1. Choose the URL of the Elastic Load Balancing endpoint for the IBM MQ console. This is the URL highlighted in Figure 2.

   ![Figure 2: URLs for connecting to MQ](image)

2. The Liberty server used by the MQ Console is initially configured to use a self-signed certificate, so your browser may display the warning shown in Figure 3. In the dialog box, choose Advanced, and then accept the security certificate to proceed.

   We recommend that you update the self-signed certificate to a certificate that’s signed by a trusted CA. For more information about setting up certificates, see the IBM MQ documentation.
Figure 3: Accepting the security certificate
3. In the IBM MQ Console login screen, enter the user name and password you created during deployment. (The default user name is `mqconsoleadmin`.)

![IBM MQ Console - Login](image)

**Figure 4:** IBM MQ Console login screen

The Console initially shows the default queue manager. If the status of the queue manager `QM1` (or the name you entered for the **Queue Manager Name** parameter in step 3) is **Running**, as shown in Figure 5, then you have successfully deployed your queue manager.

![Local Queue Managers](image)

**Figure 5:** Displaying the local queue manager
You can use the IBM MQ Console to perform administration tasks such as stopping and starting queue managers and creating objects such as queues and channels. In the following steps, you'll use the console to verify that the server is working correctly and add a message to a queue.

1. In the console window, choose **Add widget**.

![Add widget](image)

*Figure 6: Adding a widget*

2. In the **Add a new widget** dialog box, choose **Queues** to display the predefined queue, Q1.

![Add a new widget](image)

*Figure 7: Creating a queues widget*
3. On the toolbar, choose the envelope icon to put a test message on the queue.

4. On the Queues on QM1 window toolbar, you can now choose the folder icon to browse the messages on the queue.
Figure 11: Folder icon

Figure 12: Browsing messages on the queue

For more information about using the IBM MQ Console, see the IBM Knowledge Center.

Step 5. Connect to the IBM MQ Server

It is possible to administer IBM MQ locally from the server. For more information about this option, see Administering IBM MQ in the IBM Knowledge Center.

To connect to the IBM MQ server instance, use SSH to connect to the bastion host instance in your VPC. Use an SSH agent to forward your private key on connection. For more information about SSH agents, see the GitHub documentation.

**Important**  Do not copy your private key to the bastion host instance.
Troubleshooting

Q. I encountered a CREATE_FAILED error when I launched the Quick Start. What should I do?

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with Rollback on failure set to No. (This setting is under Advanced in the AWS CloudFormation console, Options page.) With this setting, the stack’s state will be retained and the instance will be left running, so you can troubleshoot the issue. (Look at the log files in %ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.)

```
Important  When you set Rollback on failure to No, you’ll continue to incur AWS charges for this stack. Please make sure to delete the stack when you’ve finished troubleshooting.
```

For additional information, see Troubleshooting AWS CloudFormation on the AWS website, or contact us on the AWS Quick Start Discussion Forum.

Q. I encountered a size limitation error when I deployed the AWS Cloudformation templates.

A. We recommend that you launch the Quick Start templates from the location we’ve provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Security

The AWS Cloud provides a scalable, highly reliable platform that helps customers deploy applications and data quickly and securely.

When you build systems on the AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, you assume responsibility and management of the guest operating system (including updates and security patches), other associated applications, as well as the configuration of the AWS-provided security group firewall. For more information about security on AWS, visit the AWS Security Center.
AWS Identity and Access Management (IAM)
This solution leverages an IAM role with least privileged access. It is not necessary or recommended to store SSH keys, secret keys, or access keys on the provisioned instances.

OS Security
The root user on cluster nodes can be accessed only by using the SSH key specified during the deployment process. AWS doesn't store these SSH keys, so if you lose your SSH key you can lose access to these instances.

Operating system patches are your responsibility and should be performed on a periodic basis.

Security Groups
A security group acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group.

The security groups created and assigned to the individual instances as part of this solution are restricted as much as possible while allowing access to the various functions needed by IBM MQ. We recommend reviewing security groups to further restrict access as needed once the cluster is up and running.

Additional Resources
AWS services
- Amazon EC2
- AWS CloudFormation
  [https://aws.amazon.com/documentation/cloudformation/](https://aws.amazon.com/documentation/cloudformation/)
- Amazon VPC
  [https://aws.amazon.com/documentation/vpc/](https://aws.amazon.com/documentation/vpc/)

IBM MQ
- IBM blog
  [http://ibm.biz/mqawsquickstartblog](http://ibm.biz/mqawsquickstartblog)
MQ on Cloud resources
https://developer.ibm.com/messaging/mq-on-cloud/

IBM MQ downloads

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Send Us Feedback
You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2017</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>
© 2017, Amazon Web Services, Inc. or its affiliates, and IBM. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.