Managing Amazon MQ

Michael Heydt
FREELANCE CLOUD DEV, ARCHITECT AND TRAINER

@mikeheydt www.smac.io

Module Overview

- Concepts in Amazon MQ management
- Security concepts
- Broker architectures for high availability
- Performance monitoring
- Securing broker access using authorization maps
- Using CloudWatch to monitor performance
- Performing failover of active/standby brokers
- Best practices in using Amazon MQ

Overview of Amazon MQ Management

Amazon MQ Management Concepts

Security

High availability

Performance monitoring

Core Amazon MQ Security Concepts

Amazon MQ Security

AWS / IAM API authentication and authorization

Encryption in-transit and at-rest

Network level

Connections

Active MQ authorization

IAM

Amazon MQ administration is integrated with IAM

Control operations such as creating, deleting, and rebooting brokers

Does not integrate into the broker at the Active MQ level

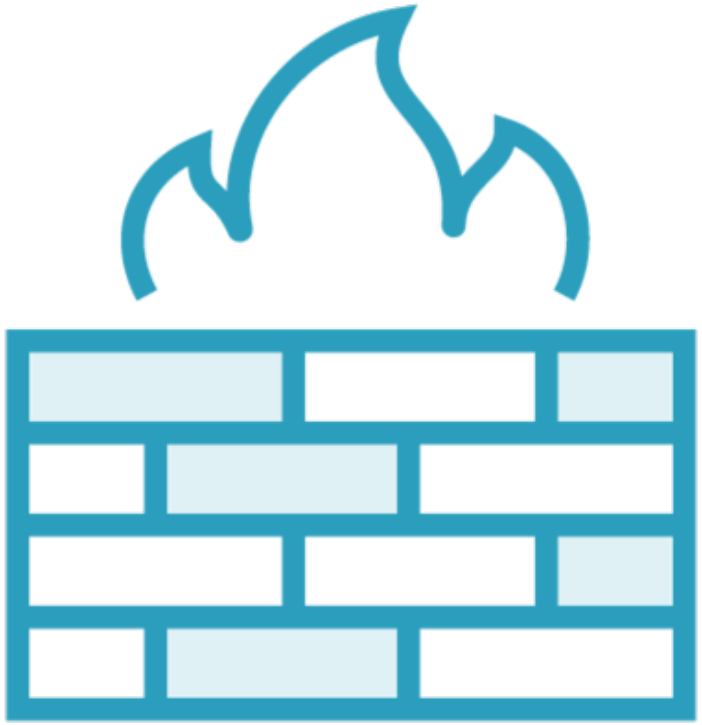
Encryption

All data stored by Amazon MQ is encrypted at-rest

You can use keys that are AWS owned CMK, AWS managed CMK, or customer managed

All communications uses TLS regardless of protocol

Network Level Security



Your broker is one or more EC2 instances that are located in one or more VPC's

Access to the broker is not enabled by default by the VPC's security group

Create network security group rules to allow access based on protocol and source

Connection Security

Username and password

Certificates

Between clients and broker

Inter-broker

Security Using Authorization Maps

Define the action that Active MQ users can take within the broker

Amazon MQ uses native ActiveMQ authentication

Authorization is specified in the brokers XML configuration

Three authorization levels: read, write, and admin

Demo

Securing queue access using authorization maps

Broker Architecture and High Availability

High Availability

Characteristic of a system which aims to ensure a specified level of operational performance, usually *uptime*. High availability in Amazon MQ is implemented using several different broker architectures.

Broker Architectures and High Availability

Single Instance

Active / Standby

Network / Mesh

Single Instance Broker

One broker in one AWS Availability Zone

The broker can utilize EFS or EBS

Active / Standby

Two brokers in two availability zones

If one broker malfunctions or is under maintenance, AWS will take that instance out of service

Utilizes EFS for storage

Two Web Console URL's are provided, and two endpoints for each wire-level protocol

Failover transport can be used to automatically connect to either endpoint

Network / Mesh

- Multiple single-instance or active/standby brokers
- Configured into various topologies such as concentrator, hub-and-spoke, tree or mesh
- Useful to increase aggregate throughput and increased connection capabilities
- Producers and consumer can reconnect to other nodes without delay
- Also useful for forwarding messages

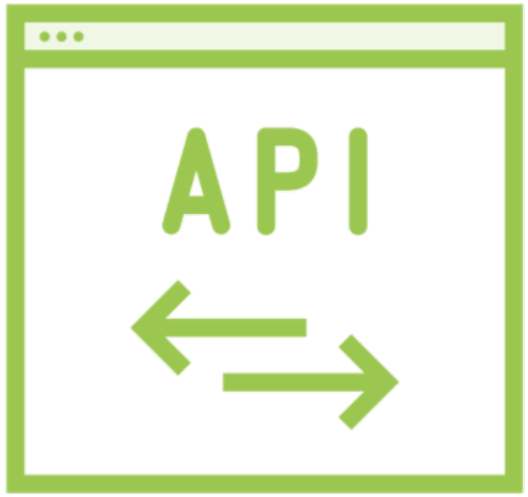
Demo

Examining active/standby broker failover

Operational Monitoring

Types of Operational Monitoring for Amazon MQ

Performance monitoring with CloudWatch



Administrative / API monitoring with CloudTrail

Monitoring Performance with CloudWatch

Amazon MQ is preconfigured for integration with CloudWatch

Metrics are polled every minute

Accessible via CloudWatch console, AWS CLI, or the CloudWatch CLI

Useful Amazon MQ Performance Metrics

- Message counts
- Message volume
- Connection counts
- Network
- CPU
- Producer vs consumer counts

Demo

Monitoring broker operations with CloudWatch

Best Practices

Security

Prefer brokers without public accessibility

Use client-side encryption as a complement to TLS

Always configure an authorization map

Block unnecessary protocols with VPC security groups

Connecting to Amazon MQ

Never modify or delete the Amazon MQ elastic network interface

Always use connection pooling

Always use the failover transport to connect to multiple broker endpoints

Avoid using message selectors

Prefer virtual destinations to durable subscriptions

Ensuring Effective Performance

Disable concurrent store and dispatch for queues with slow consumers

Choose the correct broker instance type for the best throughput

Choose the appropriate storage type for best throughput

Configure your network of brokers correctly

Summary

- Reviewed important concepts in managing Amazon MQ
- Examined security concepts in Amazon MQ
- Used authorization maps to control access to queues
- Reviewed broker architectures for high availability
- Saw failover of brokers in operation
- Monitored performance with CloudWatch
- Examined best practices to make the most of Amazon MQ