AWS Security Checklist Report

AWS Security Checklist - Amazon MQ

Item	Description
Encrypt data in transit	Encrypting your MQ data in transit helps protect your data from unauthorized interception or disclosure during transmission.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your MQ resources is limited to authorized users and applications.
Implement monitoring and logging	Implementing monitoring and logging helps you identify potential security issues or anomalies in your MQ environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your MQ resources are secure and compliant with your security policies.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Secure your MQ VPC	Securing your MQ Virtual Private Cloud (VPC) helps protect your MQ resources from unauthorized access and network-based attacks.
Implement backup and recovery	Implementing backup and recovery helps ensure that you can recover your MQ resources and data in the event of a disaster or data loss.
Implement message-level encryption	Implementing message-level encryption helps protect your MQ messages from unauthorized access or disclosure.
Implement message filtering and validation	Implementing message filtering and validation helps protect your MQ resources from malicious or invalid messages.

This report has been generated by awscheck.fyi