AWS Security Checklist Report

AWS Security Checklist - Amazon Aurora

Item	Description
Encrypt data at rest	Encrypting your Aurora database at rest helps protect your data from unauthorized access or disclosure in the event of theft or loss of your storage devices.
Encrypt data in transit	Encrypting your Aurora database connections 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 Aurora database is limited to authorized users and applications.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your Aurora database is available and functional during a security breach or other disaster.
Monitor Aurora database activity	Monitoring Aurora database activity helps you identify potential security issues or anomalies in your Aurora environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Aurora 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.