AWS Security Checklist Report

AWS Security Checklist - Amazon Redshift

Item	Description
Encrypt data at rest	Encrypting your Redshift data 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 Redshift cluster 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 Redshift cluster is limited to authorized users and applications.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your Redshift cluster is available and functional during a security breach or other disaster.
Monitor Redshift cluster activity	Monitoring Redshift cluster activity helps you identify potential security issues or anomalies in your Redshift environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Redshift 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 Redshift VPC	Securing your Redshift Virtual Private Cloud (VPC) helps protect your Redshift cluster from unauthorized access and network-based attacks.
Implement network security best practices	Implementing network security best practices helps ensure that your Redshift cluster is protected from network-based attacks and threats.