AWS Security Checklist Report

AWS Security Checklist - Amazon Lightsail

Item	Description
Use strong passwords and multi-factor authentication (MFA)	Using strong passwords and MFA helps prevent unauthorized access to your Lightsail resources and data.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit network access to Lightsail resources	Limiting network access helps prevent unauthorized access and limits the impact of security breaches.
Enable backups and snapshots	Backups and snapshots enable you to recover your data and restore your instances to a previous state in case of data loss or security incidents.
Regularly update your Lightsail instances and their software	Regularly updating your Lightsail instances and their software helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your Lightsail instances.