AWS Security Checklist Report

AWS Security Checklist - DynamoDB

Item	Description
Enable VPC Endpoints	Enable VPC endpoints to ensure that all traffic to and from your DynamoDB tables is restricted within your VPC and does not traverse the public internet.
Use IAM roles	Use IAM roles to control access to your DynamoDB tables and limit access to only the necessary permissions.
Enable encryption	Enable server-side encryption for your DynamoDB tables to protect against unauthorized access to your data.
Monitor access patterns	Monitor access patterns to your DynamoDB tables to detect anomalous behavior and potential security threats.
Enable audit logging	Enable audit logging for your DynamoDB tables to track access and changes to your data.
Enable automatic backups	Enable automatic backups for your DynamoDB tables to ensure that you can restore your data in the event of a disaster or data loss.
Use fine-grained access control	Use fine-grained access control to limit access to specific items or attributes within your DynamoDB tables.
Monitor network traffic	Monitor network traffic to and from your DynamoDB tables to detect and prevent unauthorized access or data exfiltration.