AWS Security Checklist Report

AWS Security Checklist - Amazon EKS

Item	Description
Enable VPC Flow Logs	Enabling VPC Flow Logs allows you to capture information about the IP traffic going to and from your EKS cluster, which can be useful for troubleshooting and security analysis.
Use RBAC (Role-Based Access Control) to control access to the Kubernetes API	RBAC enables you to define granular access controls to the Kubernetes API, which helps prevent unauthorized access and privilege escalation.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Use network policies to control traffic flow	Network policies enable you to control the flow of traffic to and from your Kubernetes pods, which can help prevent unauthorized access and limit the impact of security breaches.
Regularly update your EKS cluster and its components	Regularly updating your EKS cluster and its components 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 EKS cluster.