AWS Security Checklist Report

AWS Security Checklist - Fargate

Item	Description
Use task roles	Assign a task role to your Fargate tasks to ensure that they have only the necessary permissions to perform their specific functions.
Use VPC	Deploy Fargate tasks in a VPC to control network access and to restrict public access to your resources.
Use security groups	Define security groups to control inbound and outbound traffic for your Fargate tasks and to restrict access to only necessary ports.
Use IAM roles for service accounts (IRSA)	Use IAM roles for service accounts (IRSA) to enable your pods to communicate securely with other AWS services using IAM credentials.
Encrypt data at rest	Use encryption to protect sensitive data stored in volumes attached to Fargate tasks.
Encrypt data in transit	Use encryption to protect data in transit between Fargate tasks and other AWS services or external endpoints.
Monitor container images	Regularly scan and monitor container images for vulnerabilities and keep them up to date to reduce the risk of exploits.
Enable logging	Enable logging for your Fargate tasks to monitor and audit activity within your containers.
Use AWS Secrets Manager	Use AWS Secrets Manager to securely store and manage sensitive data such as passwords, API keys, and other credentials used by your Fargate tasks.