

AWS Security Checklist Report

AWS Security Checklist - ECR

Item	Description
Enable encryption	Enable encryption at rest for your ECR repositories to protect against unauthorized access to your data.
Use private repositories	Use private repositories to protect your container images from being accessed by unauthorized users.
Scan images for vulnerabilities	Use Amazon ECR image scanning to detect and remediate vulnerabilities in your container images.
Implement access control	Use IAM policies and resource-based permissions to control access to your ECR repositories and images.
Use VPC endpoints	Use VPC endpoints to securely access your ECR repositories without exposing them to the public internet.
Enable lifecycle policies	Use lifecycle policies to automatically clean up untagged or unused images, and to expire old images to reduce storage costs.
Audit trail	Enable AWS CloudTrail to log all API calls made to your ECR repositories for auditing and compliance purposes.