AWS CloudFormation

AWS Security Best Practices

- Compliance standard is what your business requires from Infrastructure as Code (laC) service and is available in the region you need to operate in
- Amazon Organizations SCP - to restrict actions like creation, deletion, modification of production Cloudformation Templates/Resources - AWS CloudTrail is enabled & monitored to trigger alerts for malicious activities e.g changes to Production Environment
- AWS Audit Manager, IAM Access Analyzer

Application Security Best Practices

- Access Control - Roles or IAM Users for making changes in Amazon Cloudformation Template stacks or StackSets especially one for production.
- Security of the Cloudformation - Configuration access
- Security in the Cloudformation - Code Security Best Practices - SCA, SAST,
- Secret Scanner, DAST implemented in the CI/CD Pipeline
- Security of the CloudFormation entry points e.g - private access points using AWS Private Link - Only use Trusted Source Control for sending changes to Cloud
- Develop process for continuously verifying if there is a change compromise the known state of a CI/CD pipeline

Application Costs Best Practices

- Right-size resources to avoid overprovisioning and excessive costs.
- Use AWS Reserved Instances (RIs) or Savings Plans for long-term, predictable workloads.
- Implement lifecycle management to automate resource decommissioning during periods of low demand.
- Leverage CloudFormation StackSets for centralized and efficient resource provisioning.
- Regularly perform drift detection on CloudFormation stacks to identify configuration changes made outside of CloudFormation.
- Use AWS Cost Explorer and AWS Budgets to monitor and analyze your CloudFormation costs.