AWS CloudFormation Remediation Workflows

Mike Brown

Senior Cloud Instructor

@mgbleeds

Globomantics Problem:

Changes have been made to deployed resources that have made the resources more open to attack and moved the resources away from a desired state.

Configuration Changes

Problems often occur when changes are made away from CloudFormation

Changes to existing stacks should be made through the change set process

You want to keep resource configurations consistent, secure, and free of vulnerabilities

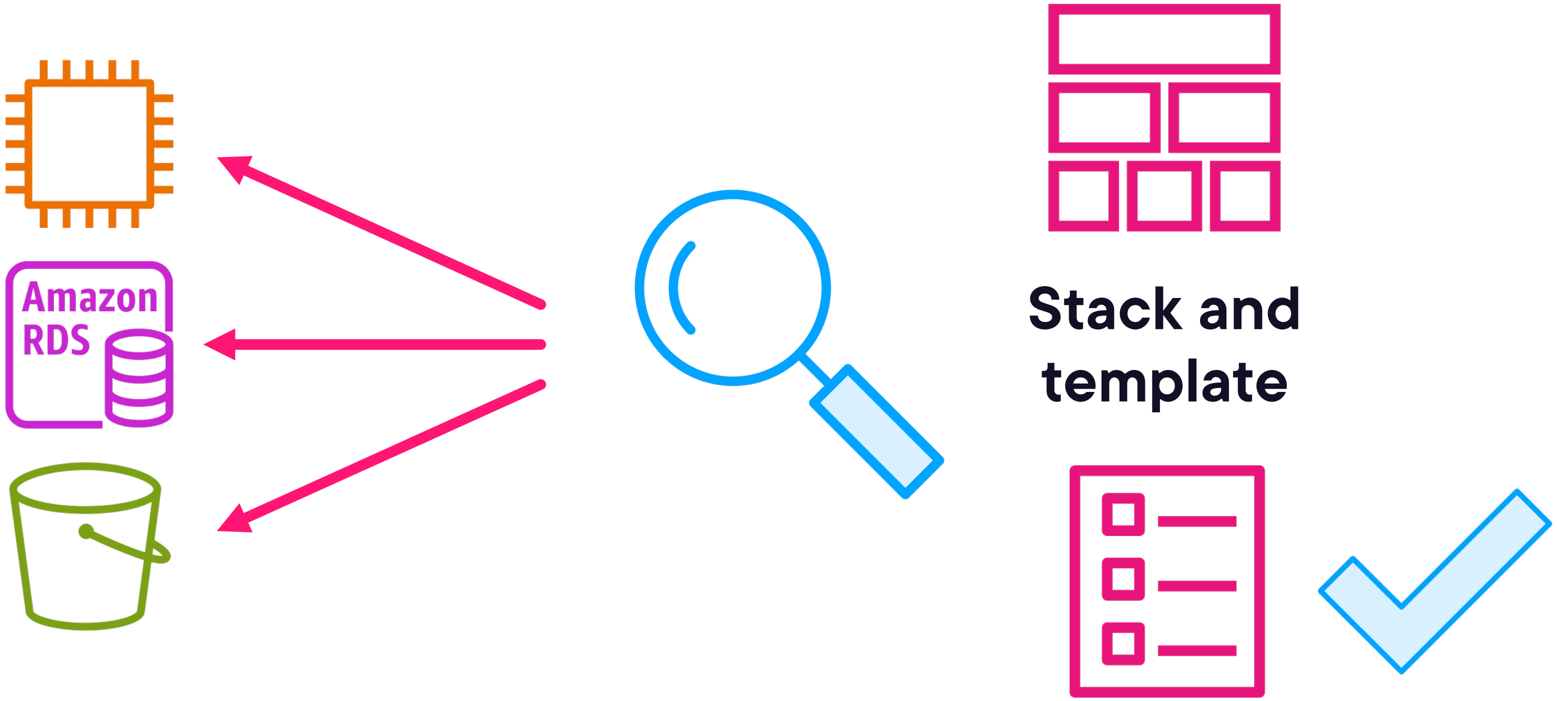
Drift Detection

Encouraged to check stacks for drifts

A configuration of deployed resources no longer matches the configuration in a stack template

CloudFormation includes a drift detection feature

Drift Detection



Stack and template

Drift Detection

IN_SYNC

MODIFIED

DELETED

NOT-CHECKED

If we detect drift, we can run a stack update to bring the stack back to our desired state.

Drift Detection

Globomantics team members can run drift detection manually, then run a stack update process

Much more powerful to automate the drift detection and remediation process

Drift Detection Automation and Remediation

Must implement a version control system (VCS)

Templates stored in a VCS act as single sources of truth

These templates are used to create new stacks, update stacks, and remediate drift

Drift Detection Automation and Remediation

Use AWS Config Rules to periodically run drift detection; a rule named cloudformation-stack-drift-detection-check **is provided for you**

An Amazon EventBridge rule can be used to detect the message sent when the AWS Config rule detects drift

Drift Detection Automation and Remediation

1. Integrate with the Simple Notification Service (SNS)

2. Add items to Systems Manager OpsCenter

3. Trigger an AWS Lambda function to run a stack update