Cloud Computing Architecture

Working with CloudFormation Templates

Image licensed under creative commons

SWINBURNE UNIVERSITY OF TECHNOLOGY

Working with CloudFormation Template

This presentation:

- Change Sets
- Drift Detection
- Organizing CloudFormation Templates

AWS CloudFormation template syntax

AWS CloudFormation templates

- Author in JavaScript Object Notation (JSON) or YAML Ain’t Markup Language (YAML)
- YAML advantages –
  - Less verbose (no {},"", characters)
  - Supports embedded comments
- JSON advantages –
  - More widely used by other computer systems (for example, APIs)
- Recommendation – Treat templates as source code
  - Store them in a code repository

```
{
 "AWSTemplateFormatVersion": "2010-09-09",
 "Resources" : {
 “awsexamplebucket1" : {
 "Type" : "AWS::S3::Bucket"
 }
 }
}
```

JSON example

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
 awsexamplebucket1:
 Type: AWS::S3::Bucket
```

YAML example

Templates can also be authored in the AWS CloudFormation Designer—a graphical design interface in the AWS Management Console.

Simple template: Create an EC2 instance

```
{
 "AWSTemplateFormatVersion": "2010-09-09",
 "Description": "Create EC2 instance",
 "Parameters": {
 "KeyPair": {
 "Description": "SSH Key Pair",
 "Type": "String"}},
 "Resources": {
 "Ec2Instance": {
 "Type": "AWS::EC2::Instance",
 "Properties": {
 "ImageId": "ami-9d23aeea",
 "InstanceType": "m3.medium",
 "KeyName": {"Ref": "KeyPair}

        }},
 "Outputs": {
 "InstanceId": {
 "Description": "InstanceId",
 "Value": {"Ref": "Ec2Instance"}
 }
 }
}
```

Parameters – Specify what values can be set at runtime when you create the stack

- Example uses: Region-specific settings, or production versus test environment settings

Resources – Define what needs to be created in the AWS account

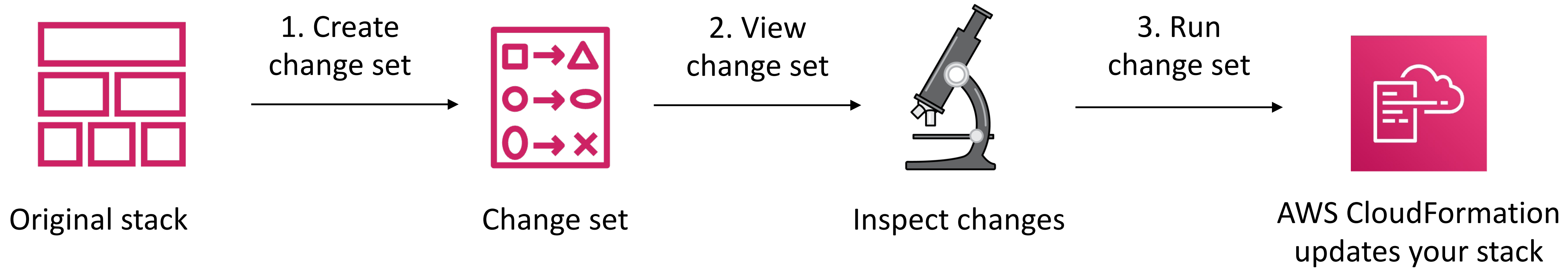
- Example: Create all components of a virtual private cloud (VPC) in a Region, and then create EC2 instances in the VPC
- Can reference parameters

Outputs – Specify values returned after the stack is created

- Example use: Return the instanceId or the public IP address of an EC2 instance

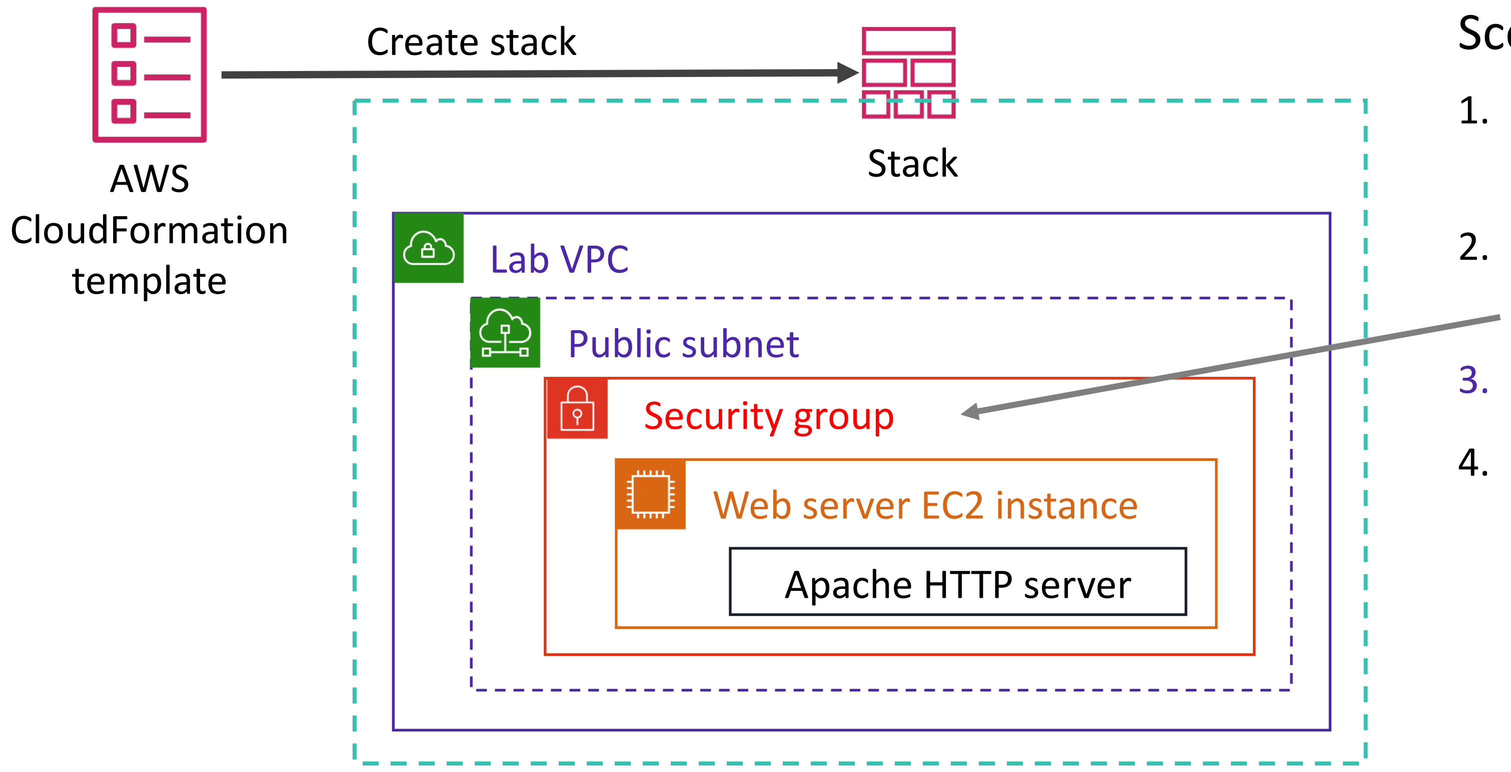
AWS CloudFormation change sets

Change sets enable you to preview changes before you implement them.



Use the DeletionPolicy attribute to preserve or backup a resource when its stack is deleted or updated.

Drift detection



Scenario:

1. An application environment is created by an AWS CloudFormation stack.
2. Later, someone ***manually modifies* the security group** and opens a new inbound TCP port.
3. Drift detection is run on the stack.
4. All resources except the security group show the result IN_SYNC, but the security group shows a status of MODIFIED, with details.

Question: In this scenario, what would be a better approach if the team wants to modify the security group setting?

Answer: Modify the AWS CloudFormation template security group settings. Then, run Update Stack. AWS CloudFormation will update the security group. Keeps the *model* deployment synchronized with the actual deployment.

Organizing Your AWS CloudFormation Templates

- Assign resources to CloudFormation templates based on **ownership and application lifecycles**.
- At a minimum: Separate network resources, security resources, and application resources into their own templates.
  - For example, a network resource template named “NetworkSharedTierVpcIgwNat.template” may include definitions for the following resources: VPCs, subnets, internet gateways, route tables, and network ACLs.

Scoping and organizing templates

Frontend services	Web interfaces, mobile access, analytics dashboard
Backend services	Search, payments, reviews, recommendations
Shared services	Customer relationship management (CRM) databases, common monitoring, alarms, subnets, security groups
Network	VPCs, internet gateways, virtual private networks (VPNs), Network Address Translation (NAT) devices
Security	AWS Identity and Access Management (IAM) policies, users, groups, and roles

Review

- Reviewed the drawbacks of manual; environment creation
- Explained the concept of infrastructure as code on AWS
- Discussed the use of templates for automating resource creation

Lecture References

SWINBURNE UNIVERSITY OF TECHNOLOGY

References

Recommend Viewing

Swinburne Lecture – High Level Overview

AWS Academy – Deeper dive

ACA Module 10