AWS re:Invent

DOP325-R

Deploying AWS CloudFormation StackSets across accounts and Regions

Prabhu Nakkeeran
Software Development Manager
AWS CloudFormation
Amazon Web Services

Mahesh Gundelly
Software Development Manager
AWS CloudFormation
Amazon Web Services

AWS re:Invent

aws

Agenda

- Common cross-account, cross-Region use cases
- AWS CloudFormation StackSets overview
  - Prerequisites
  - Parameter overrides
  - Operation preferences
  - Limits
- Integration with AWS Organizations
- AWS CloudFormation StackSets drift detection
- Demo
- Q&A

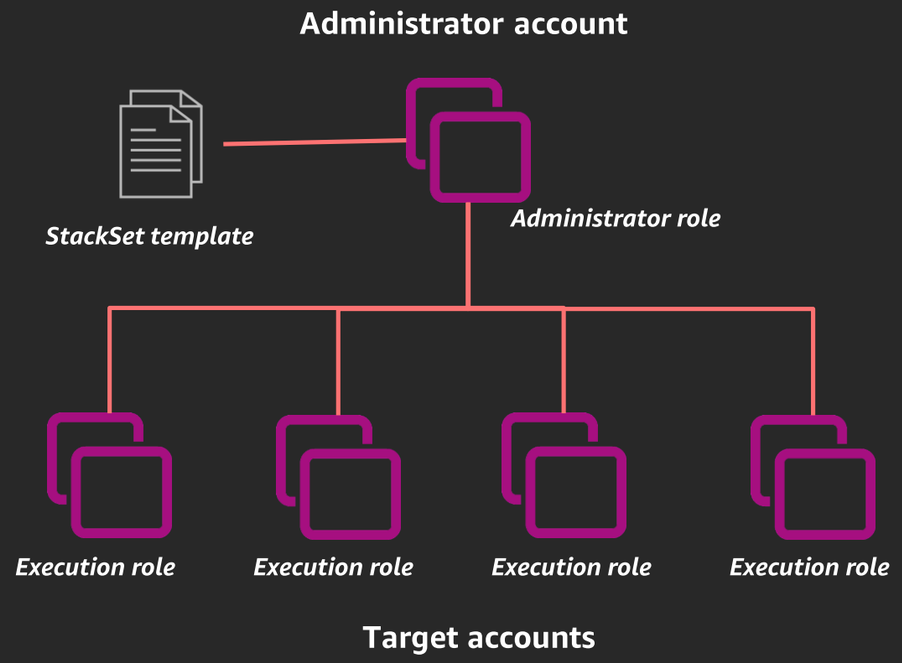
Common cross-account, cross-Region use cases

Seeding new accounts with critical prerequisite resources before the account is used	AWS CloudTrail, AWS Identity and Access Management (IAM), AWS Config, etc.
Separately setting up groups of accounts that have similar purposes consistently	Devs/QA/admins, etc.
Controlled rollout of resource changes across multiple accounts and Regions	Multi-Region production environments

AWS CloudFormation StackSets

AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across **multiple accounts and Regions** with a single operation

- **Administrator account:** The AWS account in which you create & manage stack sets
- **Target account:** The account in which you create, update, or delete one or more stacks in your stack set
- **Stack instance:** A reference to a stack in a target account within a Region; associated with only one stack set
- **Roles:** Default and custom administrator and execution roles



A stack set is a regional resource

If you create a stack set in one Region, you cannot see it or change it in other Regions

Prerequisites – administration and execution roles

- Administration role
  - Control which *users and groups* can perform stack set operations in which *target accounts*
  - Create a trust relationship between each target account and a specific administration role

- Execution role
  - Use execution roles to control which stack *resources* users and groups can include in their stack sets

Note: It is no longer required to name your administration role as AWSCloudFormationStackSetAdministrationRole and your execution role as AWSCloudFormationStackSetExecutionRole

Parameter overrides

A list of input parameters whose values you want to update for the specified stack instances

- **CreateStackInstances/UpdateStackInstances APIs**
  - Any overridden parameter values will be applied to all stack instances in the specified accounts and Regions. When specifying parameters and their values, be aware of how AWS CloudFormation sets parameter values during stack instance update operations

- **Update StackSet API**
  - To update the stack set template or add or delete a parameter use UpdateStackSet API
  - During stack set updates, any parameters overridden for a stack instance are not updated, but retain their overridden value
  - If you add a parameter to a template, before you can override the parameter value specified in the stack set you must first use UpdateStackSet to update all stack instances with the updated template and parameter value specified in the stack set

Operation preferences

- **FailureToleranceCount or FailureTolerancePercentage**
  - The number of accounts or the percentage of accounts, **per Region**, for which this operation can fail before AWS CloudFormation StackSets stops the operation in that Region
- **MaxConcurrentCount or MaxConcurrentPercentage**
  - The maximum number of accounts or the maximum percentage of accounts, **per Region**, in which to perform this operation at one time
- **RegionOrder.member.N**
  - The order of the Regions where you want to perform the stack operation

AWS CloudFormation StackSets: Limits

- Number of stack sets: (~~20~~) 100
- Number of stack instances per stack set: (~~500~~) 2,000
- Number of concurrent stack instances: 3,500

Integration with AWS Organizations: Overview

Enable AWS CloudFormation StackSets integration with AWS Organizations

- Auto deployment
- Simplified permissions management

Integration with AWS Organizations: Auto deployments

- Move an account into an organizational unit
  - Provision the stack instance in the account if the auto deployment is enabled
- Remove an account from an organizational unit
  - Remove the stack instance if the auto deployment is enabled
  - Retain stack in the member account if the retain stack flag is true; otherwise, delete the stack from the account

Integration with AWS Organizations: Permissions management (IAM policy)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:*"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/*/*",
                "arn:aws:cloudformation:*:*:stackset/*",
                "arn:aws:cloudformation:*::type/resource/AWS-S3-*",
                "arn:aws:cloudformation:us-west-2::type/resource/AWS-SES-ConfigurationSet",
                "arn:aws:cloudformation::204876809651:stackset-target/*/ou-enz4-9c1k01nl",
                "arn:aws:cloudformation::204876809651:stackset-target/*/104876809554"
            ],
            "Condition": {
                "ForAllValues:StringEqualsIgnoreCase": {
                    "cloudformation:TargetRegion": [
                        "us-east-1",
                        "us-west-2"
                    ]
                }
            }
        }
    ]
}
```

Detecting drift cross-account, cross-Region

- Ability to detect whether stack instances have drifted from their expected template configuration
- Single stack set operation to detect drift across all stack instances
- Drift status: drifted, in sync, not checked
- Review drift details at the stack set, operation and stack instance level
- Resource-level drift details can be reviewed by logging into the specific account

Demo

AWS CloudFormation StackSets: Best practices

- Leverage TaskCat to ensure the resources you're provisioning exist in all the Regions you want
- Separate stacks by function and frequency of changes needed
- Partially deploy your stack set updates to reduce blast radius
- Depending on your speed/safety needs, consider setting a higher concurrent account limit
- Use parameter overrides to define specific parameters in account/Region pairs
- Distribute stack set creation and management to multiple Regions

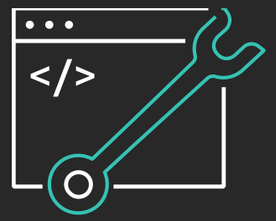
Q&A

Summary

- Leverage AWS CloudFormation StackSets for automation and repeatability when dealing with cross-account, cross-Region use cases
- Use IAM policies to control the permissions used to provision resources
- Leverage operation preferences
- Reduce blast radius for your deployments
- Recent and upcoming launches

Learn DevOps with AWS Training and Certification

Resources created by the experts at AWS to propel your organization and career forward



Take free digital training to learn best practices for developing, deploying, and maintaining applications

Classroom offerings, like DevOps Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified DevOps Engineer - Professional** or **AWS Certified Developer - Associate** exams

Visit aws.amazon.com/training/path-developing/

aws training and certification

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.