# StackSets Overview

- Create, update, or delete stacks across **multiple accounts and regions** with a single operation/template
- Administrator account to create StackSets
- Target accounts to create, update, delete stack instances from StackSets
- When you update a stack set, *all* associated stack instances are updated throughout all accounts and regions
- Regional service
- Can be applied into all accounts of an AWS organizations
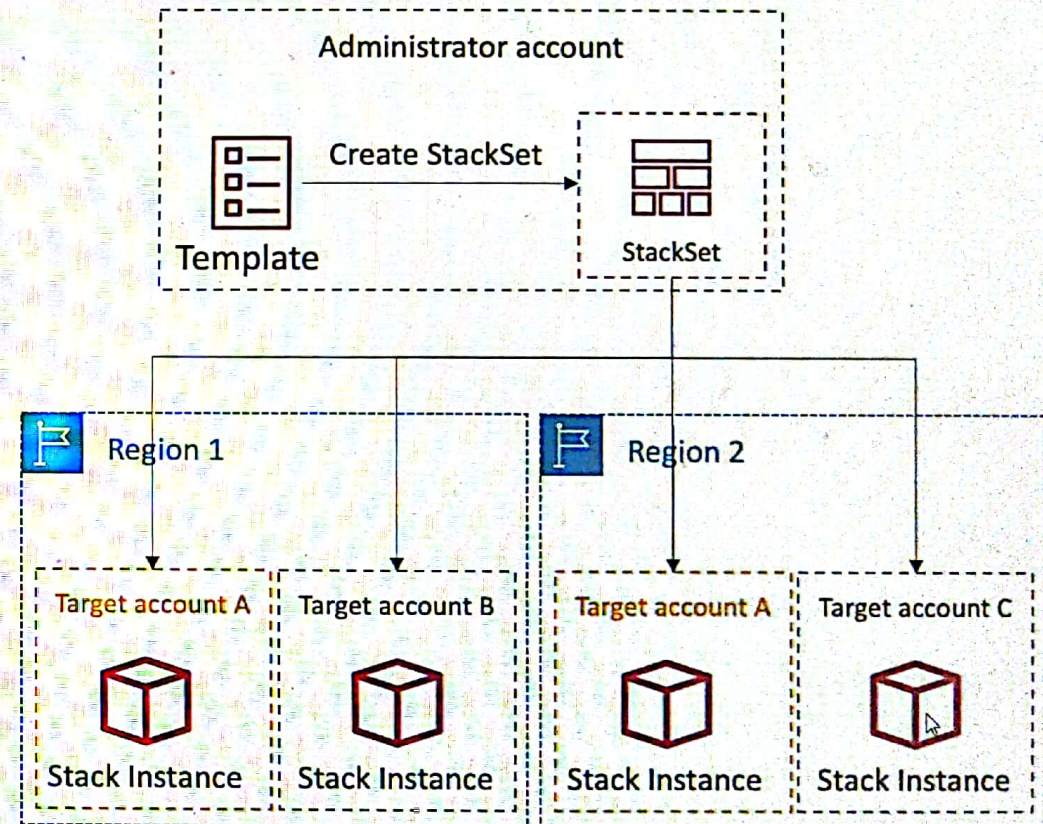
StackSet Operations

- Create StackSet
  - Provide template + target accounts/regions
- Update StackSet
  - Updates always affect all stacks (you can't selectively update some stacks in the StackSet but not others)
- Delete Stacks
  - Delete stack and its resources from target accounts/regions
  - Delete stack from your StackSet (the stack will continue to run independently)
  - Delete all stacks from your StackSet (prepare for StackSet deletion)
- Delete StackSet
  - Must delete all stack instances within StackSet to delete it

StackSet Deployment Options

- Deployment Order
  - Order of regions where stacks are deployed
  - Operations performed one region at a time
- Maximum Concurrent Accounts
  - Max. number/percentage of target accounts per region to which you can deploy stacks at one time
- Failure Tolerance
  - Max. number/percentage (target accounts per region) of stack operation failures that can occur before CloudFormation stops operation in all regions
- Region Concurrency
  - Whether StackSet deployed into regions Sequential (default) or Parallel
- Retain Stacks
  - Used when deleting StackSet to keep stacks and their resources running when removed from StackSet
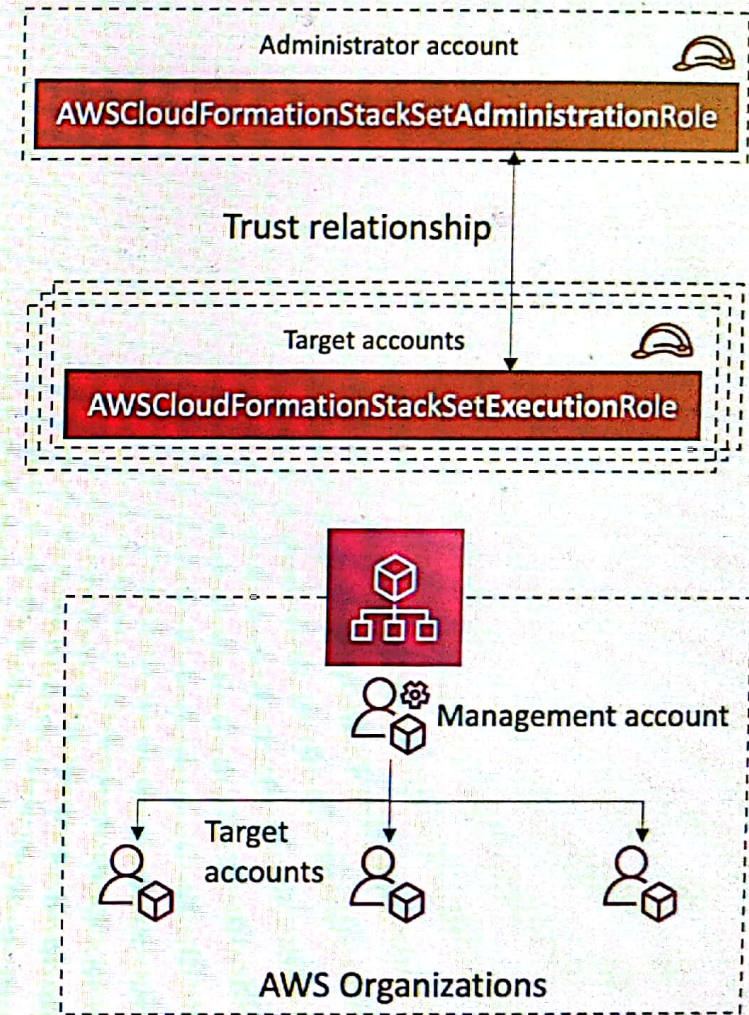
Permission Models for StackSet

- Self-managed Permissions
  - Create the IAM roles (with established trusted relationship) in both administrator and target accounts
 - Deploy to any target account in which you have permissions to create IAM role
- Service-managed Permissions
  - Deploy to accounts managed by AWS Organizations
  - StackSets create the IAM roles on your behalf (**enable trusted access** with AWS Organizations)
  - Must **enable all features** in AWS Organizations
  - Ability to deploy to accounts added to your organization in the future (Automatic Deployments)

Administrator account

AWSCloudFormationStackSetAdministrationRole

Trust relationship

Target accounts

AWSCloudFormationStackSetExecutionRole

Management account

Target accounts

AWS Organizations

Hands-On: StackSets

- We'll use StackSets to enable AWS Config across AWS regions with a single click

- Let's see how this works!
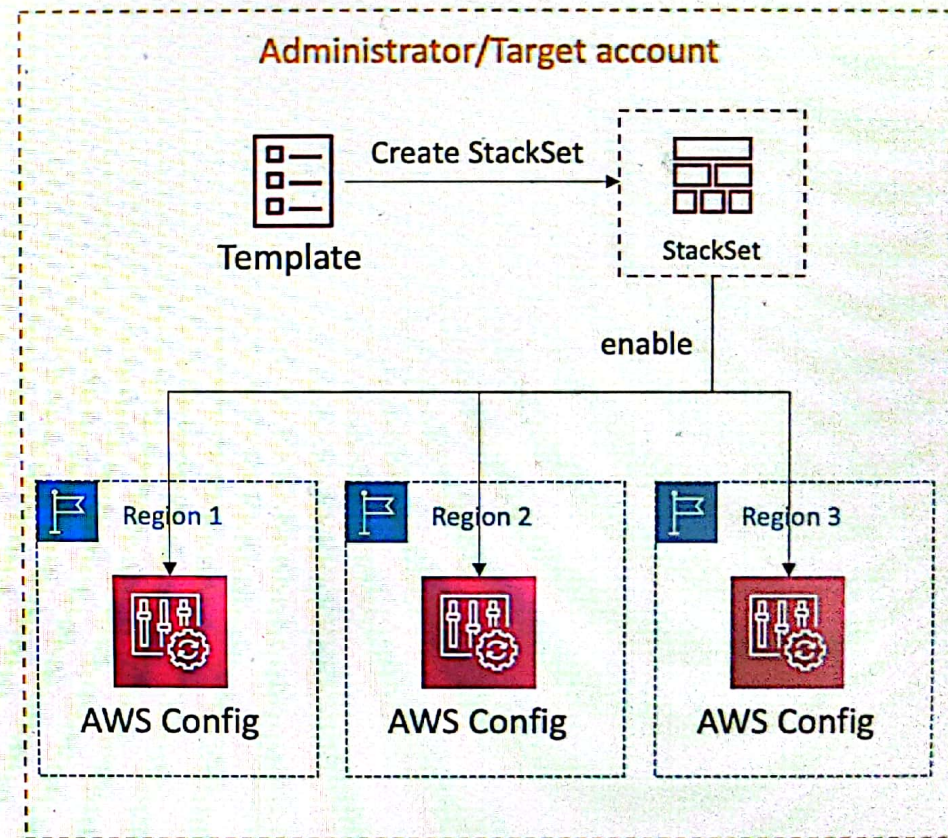
StackSet Drift Detection

- Performs drift detection on the stack associated with each stack instance in the StackSet
- If the current state of a resource in a stack varies from the expected state:
  - The stack considered drifted
  - And the stack instance that the stack associated with considered drifted
  - And the StackSet is considered drifted
- Drift detection identifies unmanaged changes (outside CloudFormation)
- Changes made through CloudFormation to a stack directly (not at the StackSet level), aren't considered drifted
- You can stop drift detection on a StackSet

Administrator account

StackSet ⚠️

Target account

Stack Instance ⚠️

Stack ⚠️

modify through EC2 console

EC2 instance ⚠️

User