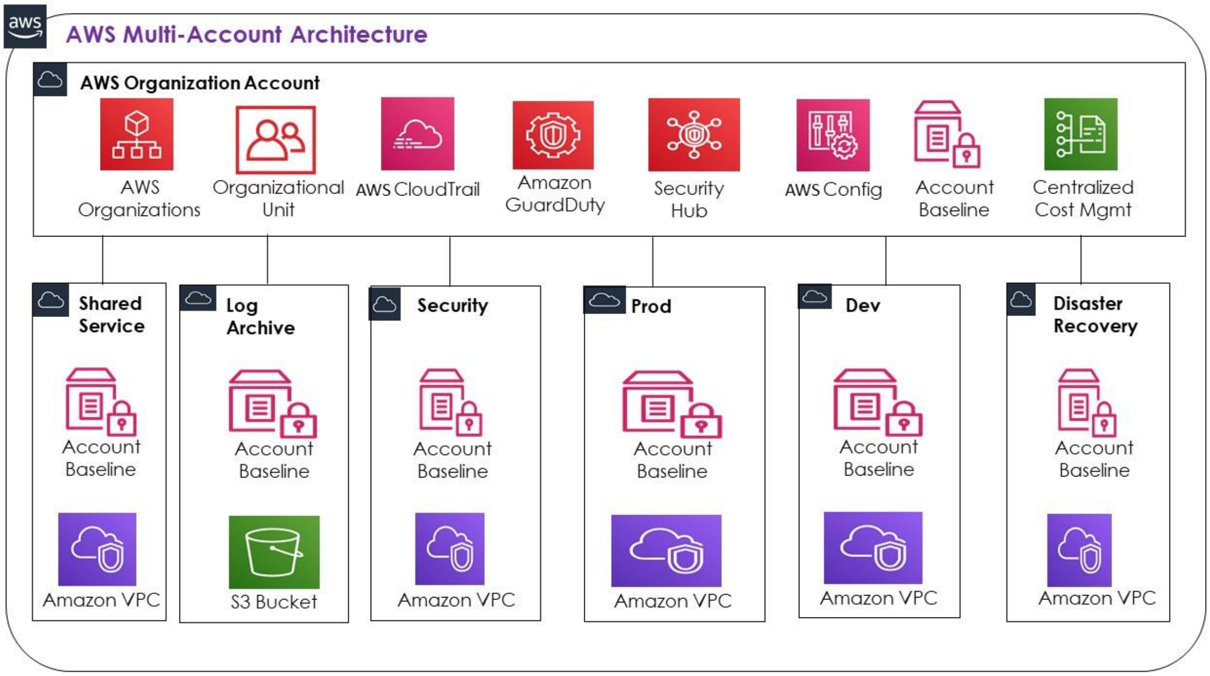
Contents

AWS Organization Account Landing zone

Overview

By using this 7 template we can achieve following services implement with CIS Compliance.

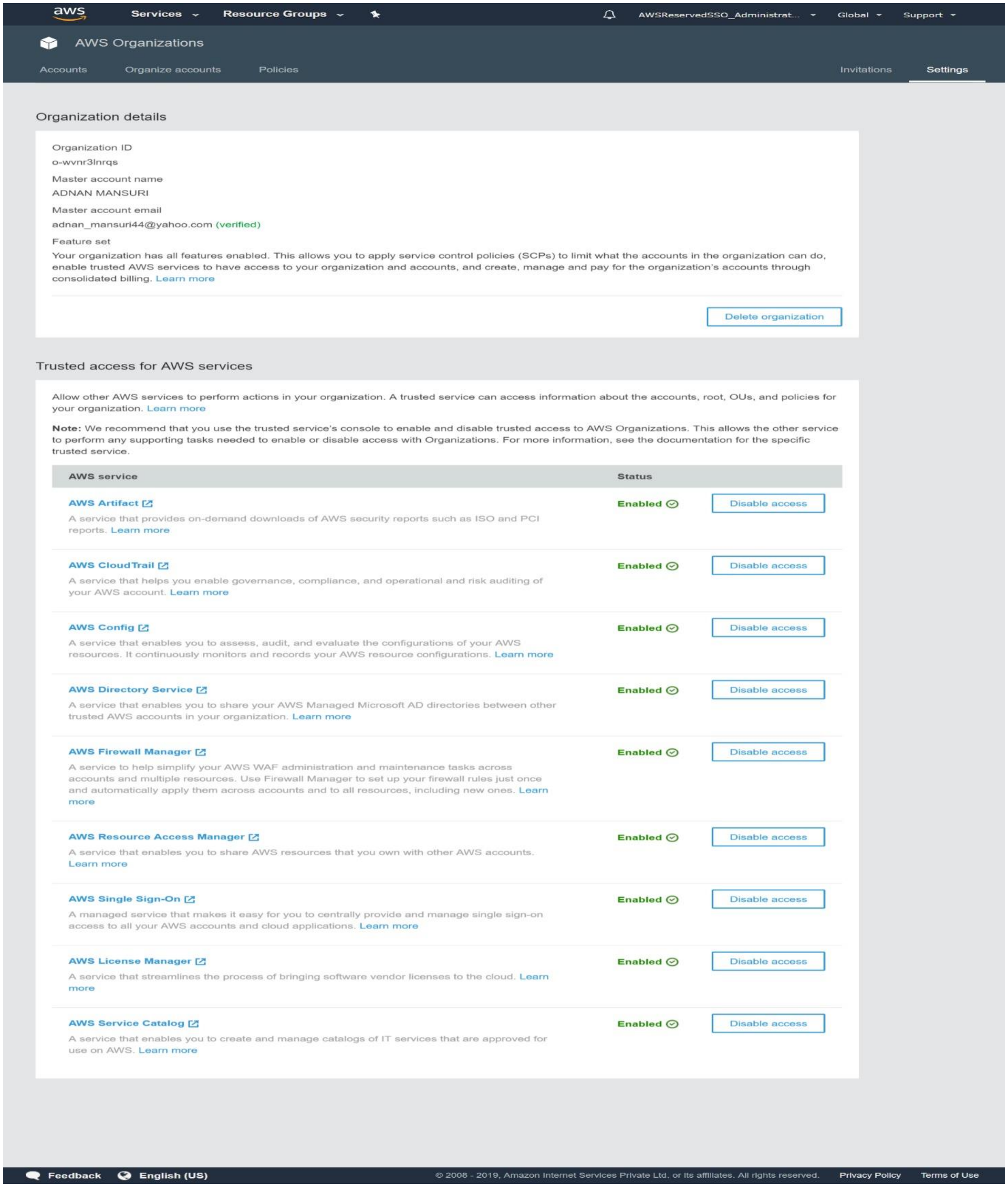


- 1-Prerequisite-IAM Roles-Master
- 2-Prerequisite-Buckets-KMS-Log
- 3-MasterCloudtrail-Master
- 4-SettingupAccount-All-Delete
- 5-Config-Cloudwatch-All-Home-Region
- 6-Config-Cloudwatch-All-Other-Regions
- 7-VPC-Individual Account only

Steps to implement

Prerequisites: -

1. Before executing any script please login into Master account and enable organization, Verify and manually enable all features like below.



Organization details

Organization ID
o-wvnr3lnrqs

Master account name
ADNAN MANSURI

Master account email
adnan_mansuri44@yahoo.com (verified)

Feature set
Your organization has all features enabled. This allows you to apply service control policies (SCPs) to limit what the accounts in the organization can do, enable trusted AWS services to have access to your organization and accounts, and create, manage and pay for the organization's accounts through consolidated billing. Learn more

Trusted access for AWS services

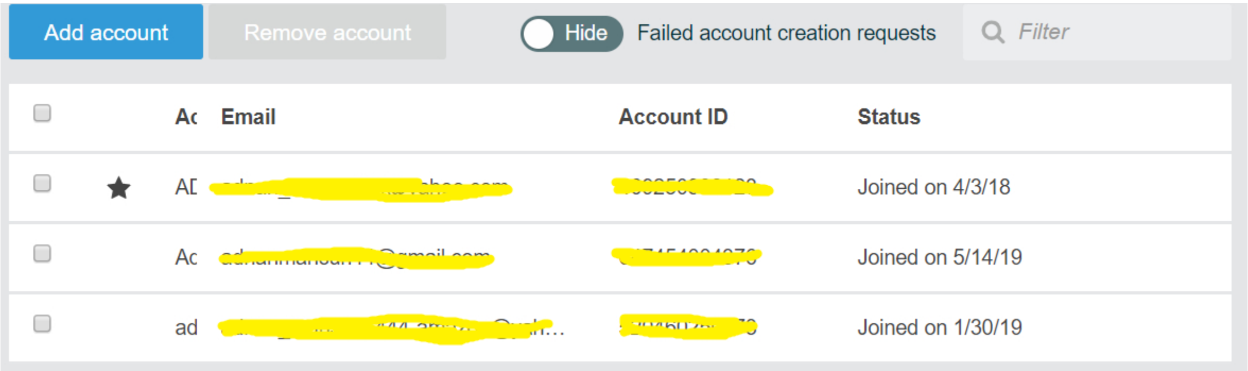
Allow other AWS services to perform actions in your organization. A trusted service can access information about the accounts, root, OUs, and policies for your organization. Learn more

Note: We recommend that you use the trusted service's console to enable and disable trusted access to AWS Organizations. This allows the other service to perform any supporting tasks needed to enable or disable access with Organizations. For more information, see the documentation for the specific trusted service.

AWS service	Status	
AWS Artifact A service that provides on-demand downloads of AWS security reports such as ISO and PCI reports. Learn more	Enabled ✓	Disable access
AWS CloudTrail A service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Learn more	Enabled ✓	Disable access
AWS Config A service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It continuously monitors and records your AWS resource configurations. Learn more	Enabled ✓	Disable access
AWS Directory Service A service that enables you to share your AWS Managed Microsoft AD directories between other trusted AWS accounts in your organization. Learn more	Enabled ✓	Disable access
AWS Firewall Manager A service to help simplify your AWS WAF administration and maintenance tasks across accounts and multiple resources. Use Firewall Manager to set up your firewall rules just once and automatically apply them across accounts and to all resources, including new ones. Learn more	Enabled ✓	Disable access
AWS Resource Access Manager A service that enables you to share AWS resources that you own with other AWS accounts. Learn more	Enabled ✓	Disable access
AWS Single Sign-On A managed service that makes it easy for you to centrally provide and manage single sign-on access to all your AWS accounts and cloud applications. Learn more	Enabled ✓	Disable access
AWS License Manager A service that streamlines the process of bringing software vendor licenses to the cloud. Learn more	Enabled ✓	Disable access
AWS Service Catalog A service that enables you to create and manage catalogs of IT services that are approved for use on AWS. Learn more	Enabled ✓	Disable access

Feedback
English (US)
© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

2. Create multiple account from aws organization. Log account is must.



□		Ac	Email	Account ID	Status
□	★	AI	[redacted]	[redacted]	Joined on 4/3/18
□		Ac	[redacted]	[redacted]	Joined on 5/14/19
□		ad	[redacted]	[redacted]	Joined on 1/30/19

Note: - Star symbol shows it master.

3. Create New Organizational unit and add all account. And copy organizational id at some safe place.

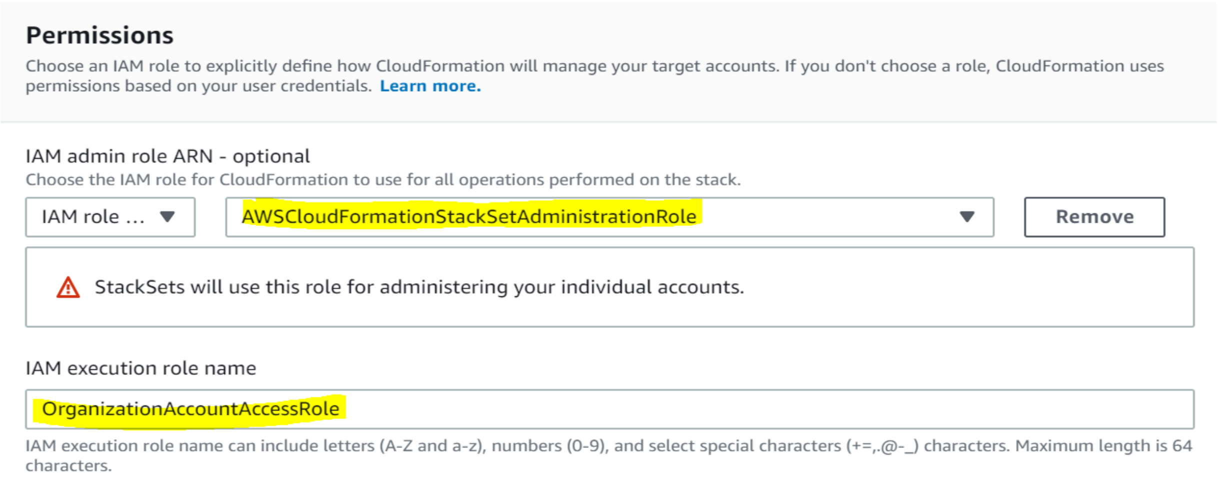
Template Executions

Note :- we have to execute everything from master account Cloudformation only. No need to login into any other account.

1. Execute following template into Cloudformation > Stack.
   Template: - 1-Prerequisite-IAM Roles-Master
   Execute: - only in master account
   By stack or stackset: - stack
   Output: - Create Stackset IAM resources in master account.
   - Cloudformation > Stack > New Stack > Upload Template > Next
   - Enter Stack name > Next > Review and submit

2. Now it's time to use stackset and execute 2nd stack into Log account.
   Template: - 2-Prerequisite-Buckets-KMS-Log
   Execute: - only in master account
   By stack or stackset: - stackset
   Output: - Create S3 bucket, KMS in log account.
   - Go to Cloudformation > Stackset > Create New Stackset
   - Upload template file > Next
   - Enter Stack Name and paste Master Account id in parameter > next
   - Add Followings info and click next

     Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole
     Enter IAM Execution Role:- OrganizationAccountAccessRole



Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more.

IAM admin role ARN - optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

AWSCloudFormationStackSetAdministrationRole

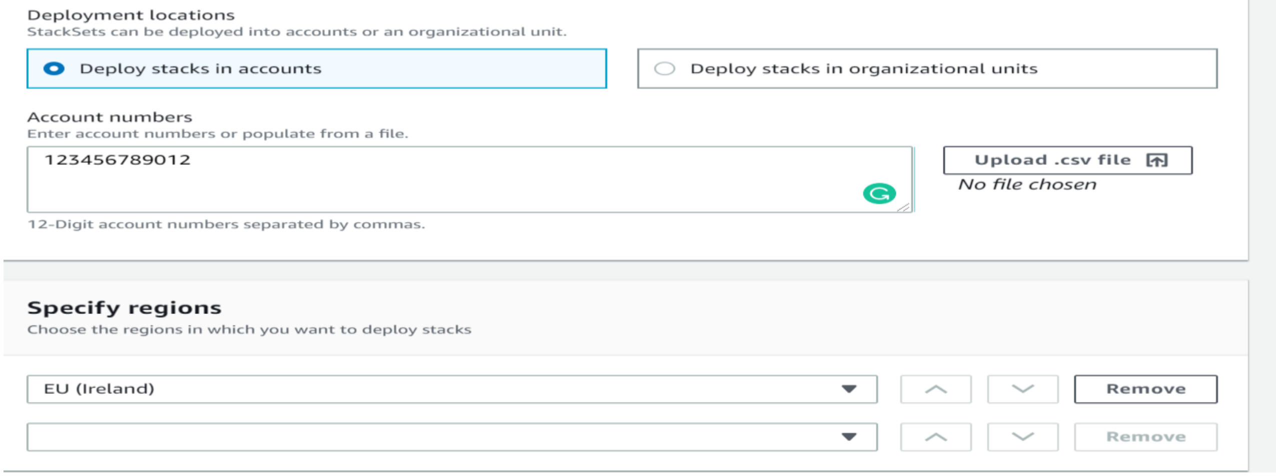
StackSets will use this role for administering your individual accounts.

IAM execution role name

OrganizationAccountAccessRole

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

- Paste Log account id and Home Region > next



Deployment locations

StackSets can be deployed into accounts or an organizational unit.

● Deploy stacks in accounts ○ Deploy stacks in organizational units

Account numbers

Enter account numbers or populate from a file.

123456789012

12-Digit account numbers separated by commas.

No file chosen

Specify regions

Choose the regions in which you want to deploy stacks

EU (Ireland)

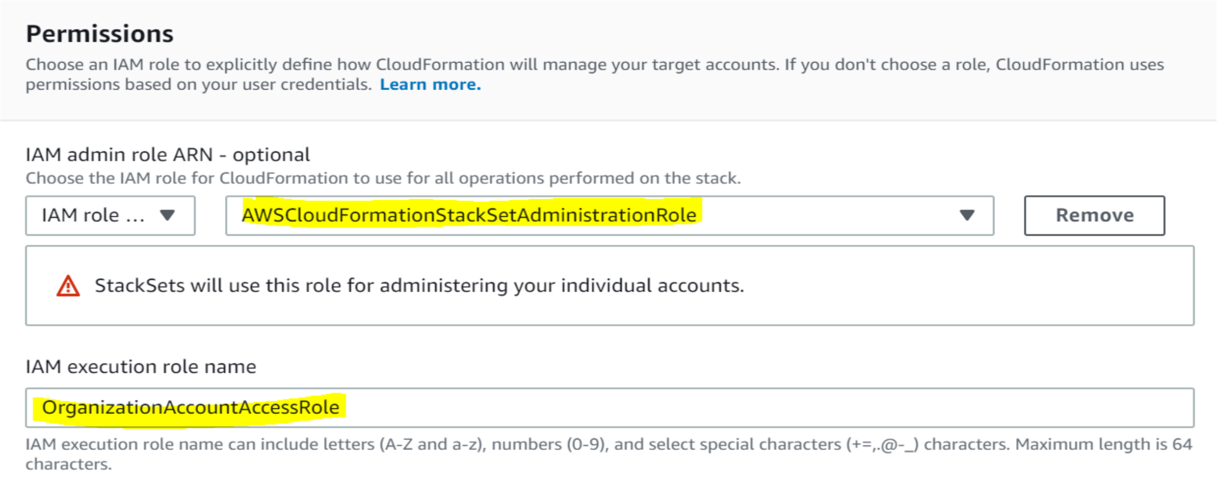
- Review and submit. This will execute stack in log account.

3. If above stack execute successfully than, please go with next stack which only needs to execute in master.
   Template: - 3-MasterCloudtrail-Master
   Execute: - only in master account
   By stack or stackset: - stack
   Output: - Create trail with required properties
   - Cloudformation > Stack > New Stack > Upload Template > Next
   - Enter Stack name and log account no > Next > Review > Submit

4. Next template will use CLI and Execute everything in userdata
   Template: - 4-SettingupAccount-All-Delete
   Execute: - All Account with Organization id
   By stack or stackset: - stackset
   Output: - delete default VPC, Update CloudTrail to master, IAM password policy update, S3 Public access block, Security hub and GuardDuty as master

   Note:- This stack needs to delete after 15 min of successful execution
   - Go to Cloudformation > Stackset > Create New Stackset
   - Upload template file > Next
   - Enter Stack Name and paste Master Account id in parameter > next
   - Add Followings info and click next

     Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole
     Enter IAM Execution Role:- OrganizationAccountAccessRole



Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more.

IAM admin role ARN - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role … ▼ | AWSCloudFormationStackSetAdministrationRole ▼ | Remove

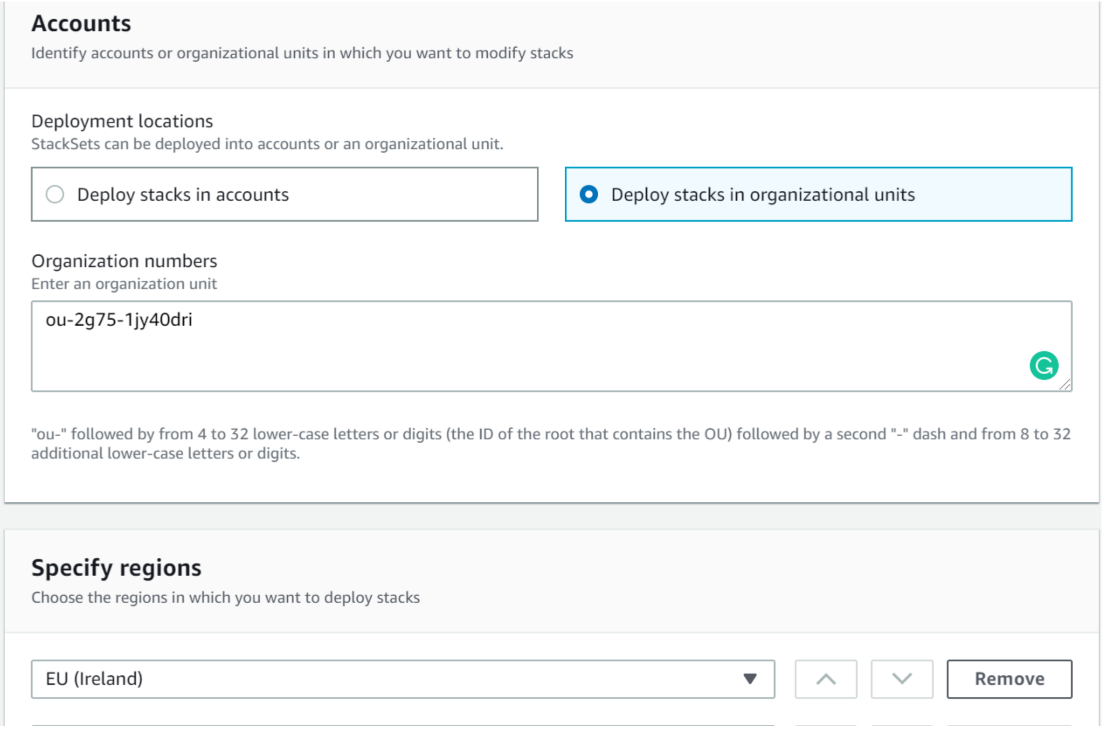
⚠ StackSets will use this role for administering your individual accounts.

IAM execution role name

OrganizationAccountAccessRole

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

- Paste Organizational unit id and select Home Region > next



Accounts

Identify accounts or organizational units in which you want to modify stacks

Deployment locations

StackSets can be deployed into accounts or an organizational unit.

○ Deploy stacks in accounts ● Deploy stacks in organizational units

Organization numbers

Enter an organization unit

ou-2g75-1jy40dri

"ou-" followed by from 4 to 32 lower-case letters or digits (the ID of the root that contains the OU) followed by a second "-" dash and from 8 to 32 additional lower-case letters or digits.

Specify regions

Choose the regions in which you want to deploy stacks

EU (Ireland) ▼ | ^ | ∨ | Remove

- Review and submit. This will execute in all Account.

Once execute delete it successfully. Follow below steps for delete.

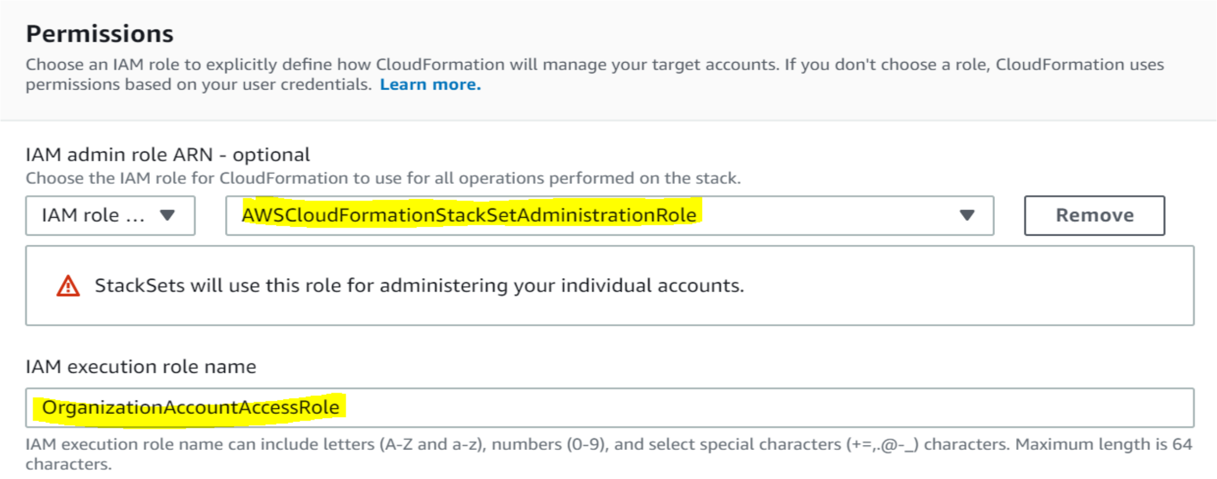
- Select Stackset checkbox and click on Delete stacks from Stackset
- Enter Organizational unit id and select Region > next and submit.
- Once done than delete stackset

5. Next template will enable config and cloudwatch alerts in all account
   Template: - 5-Config-Cloudwatch-All-Home-Region
   Execute: - All Account with Organization id
   By stack or stackset: - stackset
   Output: - enable config, alarm and events

   - ➢ Go to Cloudformation > Stackset > Create New Stackset
   - ➢ Upload template file > Next
   - ➢ Enter Stack Name and paste Master Account id, Email ids in parameter > next
   - ➢ Add Followings info and click next

     Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole

     Enter IAM Execution Role:- OrganizationAccountAccessRole



Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more.

IAM admin role ARN - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role … ▼ | AWSCloudFormationStackSetAdministrationRole ▼

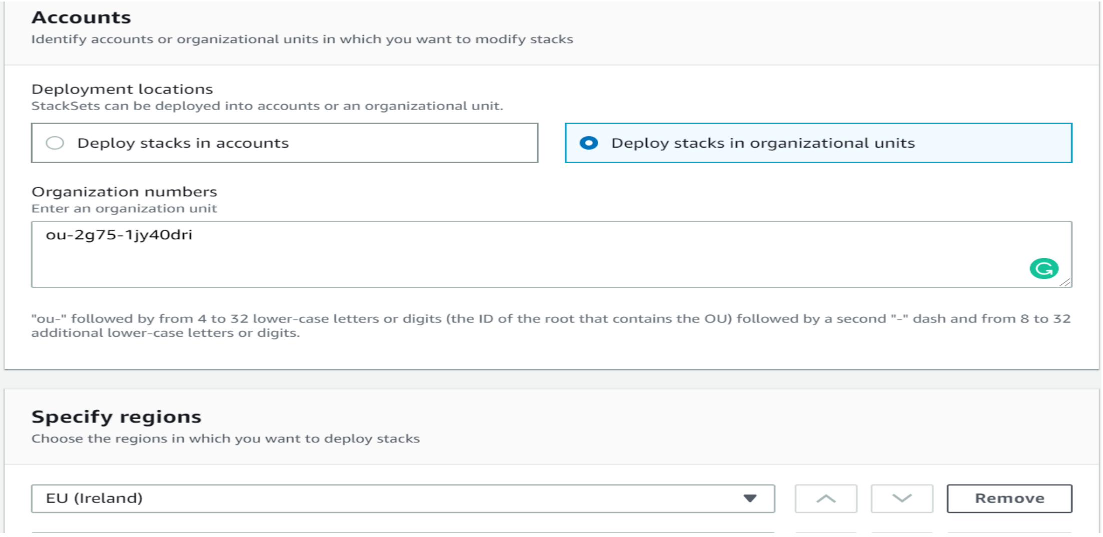
⚠ StackSets will use this role for administering your individual accounts.

IAM execution role name

OrganizationAccountAccessRole

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

- ➢ Paste Organizational unit id and select Home Region > next



Accounts

Identify accounts or organizational units in which you want to modify stacks

Deployment locations

StackSets can be deployed into accounts or an organizational unit.

○ Deploy stacks in accounts

● Deploy stacks in organizational units

Organization numbers

Enter an organization unit

ou-2g75-1jy40dri

"ou-" followed by from 4 to 32 lower-case letters or digits (the ID of the root that contains the OU) followed by a second "-" dash and from 8 to 32 additional lower-case letters or digits.

Specify regions

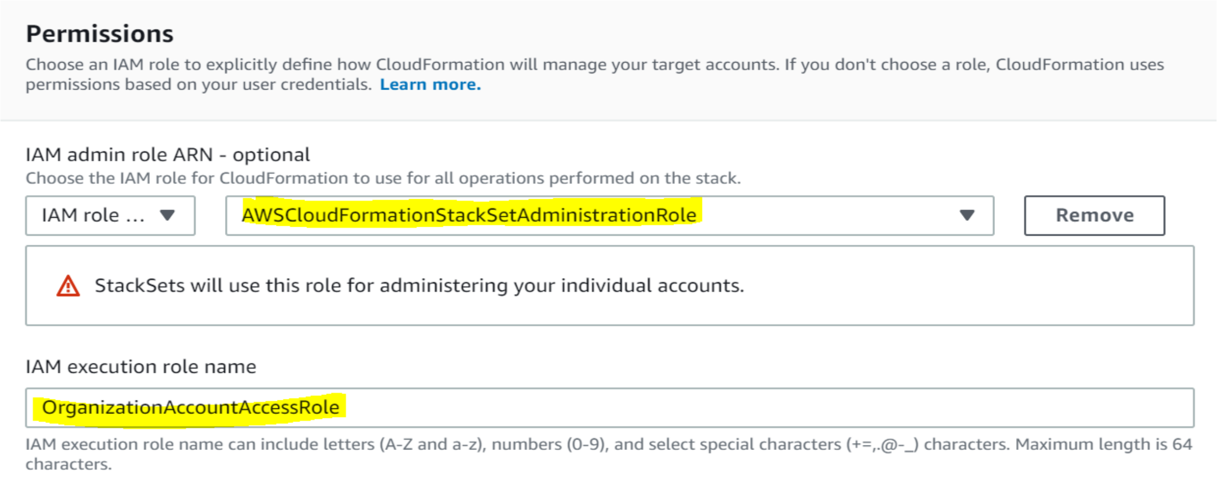
Choose the regions in which you want to deploy stacks

EU (Ireland) ▼

- ➢ Review and submit. This will execute in all Account.

6. Next template will enable config and cloudwatch alerts(optional) in all account for other region
   Template: - 6-Config-Cloudwatch-All-Other-Regions
   Execute: - All Account(other than home region) with Organization id
   By stack or stackset: - stackset
   Output: - enable config, alarm and events

   - Go to Cloudformation > Stackset > Create New Stackset
   - Upload template file > Next
   - Enter Stack Name and paste Master Account id, Email ids in parameter > next
   - Add Followings info and click next
     Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole
     Enter IAM Execution Role:- OrganizationAccountAccessRole



Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. **Learn more.**

IAM admin role ARN - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role … ▼ AWSCloudFormationStackSetAdministrationRole ▼

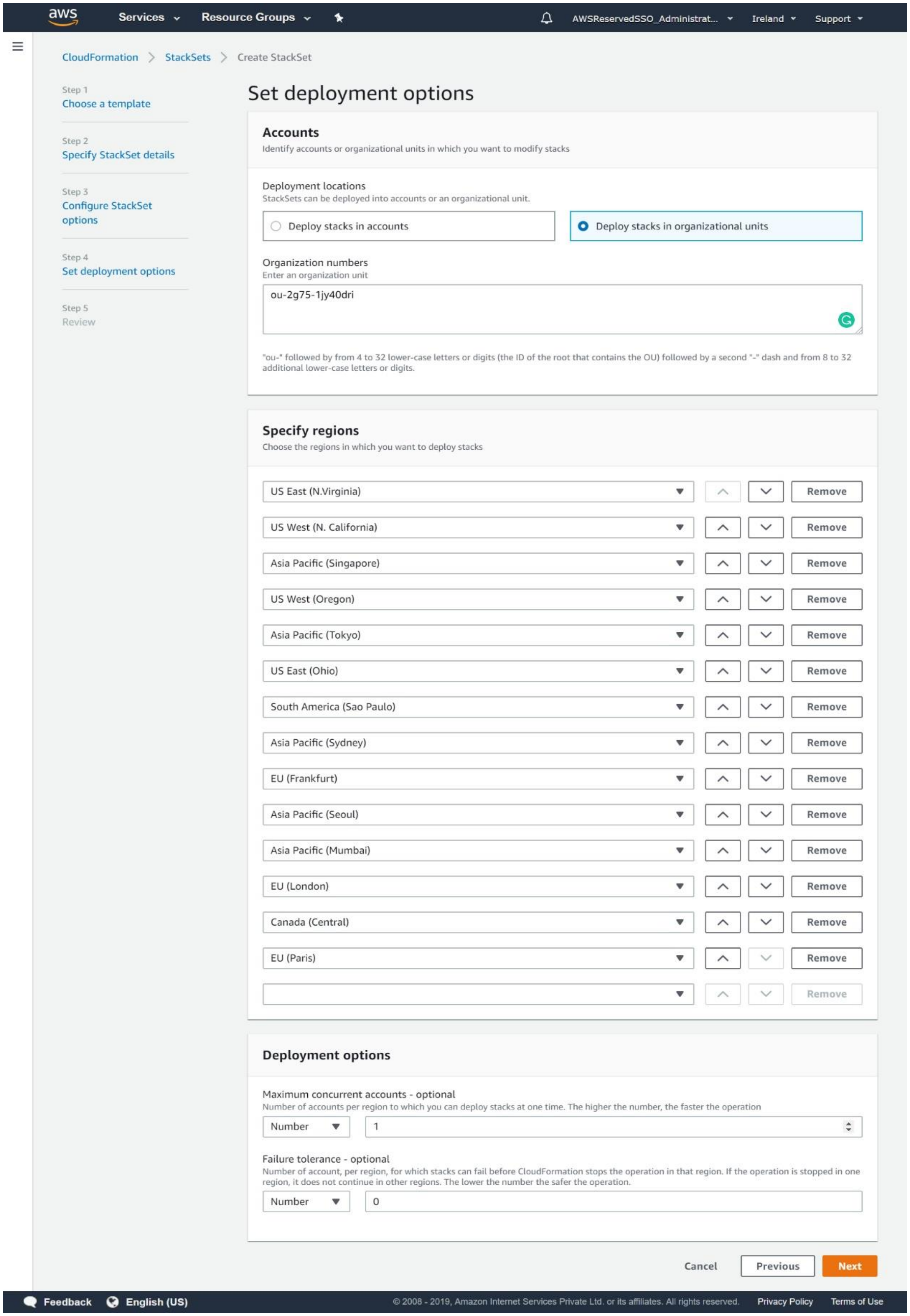
⚠ StackSets will use this role for administering your individual accounts.

IAM execution role name

OrganizationAccountAccessRole

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

- Paste Organizational unit id and select all other regions > next



Set deployment options

Accounts

Identify accounts or organizational units in which you want to modify stacks

Deployment locations
StackSets can be deployed into accounts or an organizational unit.

○ Deploy stacks in accounts ● Deploy stacks in organizational units

Organization numbers
Enter an organization unit

ou-2g75-1jy40dri

"ou-" followed by from 4 to 32 lower-case letters or digits (the ID of the root that contains the OU) followed by a second "-" dash and from 8 to 32 additional lower-case letters or digits.

Specify regions

Choose the regions in which you want to deploy stacks

- US East (N.Virginia)
- US West (N. California)
- Asia Pacific (Singapore)
- US West (Oregon)
- Asia Pacific (Tokyo)
- US East (Ohio)
- South America (Sao Paulo)
- Asia Pacific (Sydney)
- EU (Frankfurt)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- EU (London)
- Canada (Central)
- EU (Paris)

Deployment options

Maximum concurrent accounts - optional
Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation
Number 1

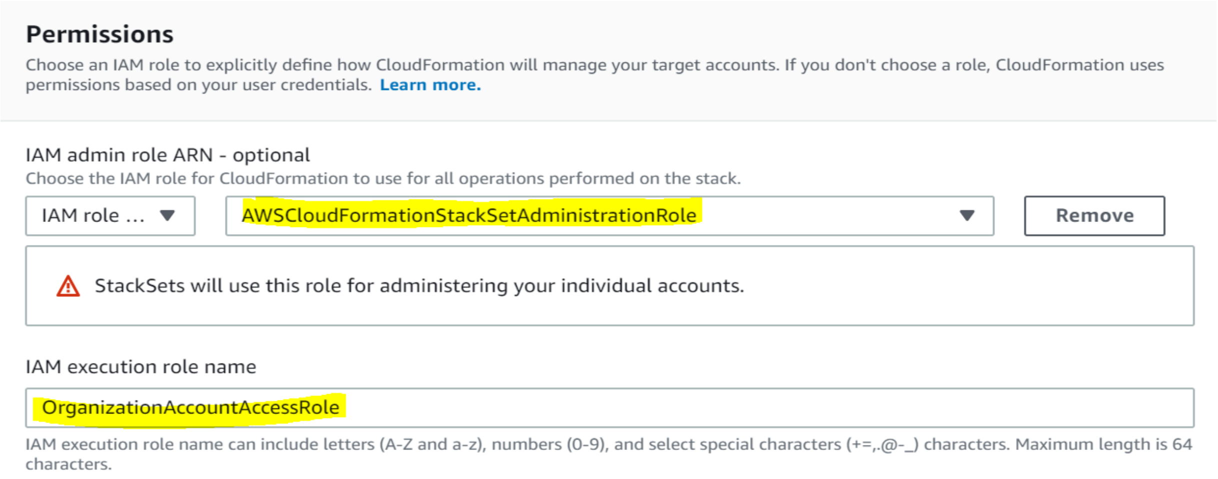
Failure tolerance - optional
Number of account, per region, for which stacks can fail before CloudFormation stops the operation in that region. If the operation is stopped in one region, it does not continue in other regions. The lower the number the safer the operation.
Number 0

Cancel
Previous
Next
Feedback
English (US)
© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

- Review and submit. This will execute in all Account.

7. This is last template will create VPC in required account
   Template: - 7-VPC-Individual Account only
   Execute: - Need to execute in each account 1 by 1 where VPC required
   By stack or stackset: - stackset
   Output: - Create VPC, Subnets, VPC Flowlogs.
   - ➢ Go to Cloudformation > Stackset > Create New Stackset
   - ➢ Upload template file > Next
   - ➢ Enter Stack Name and VPC CIDR and Name in parameter > next
   - ➢ Add Followings info and click next

     Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole
     Enter IAM Execution Role:- OrganizationAccountAccessRole



Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more.

IAM admin role ARN - optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role … ▼ | AWSCloudFormationStackSetAdministrationRole ▼

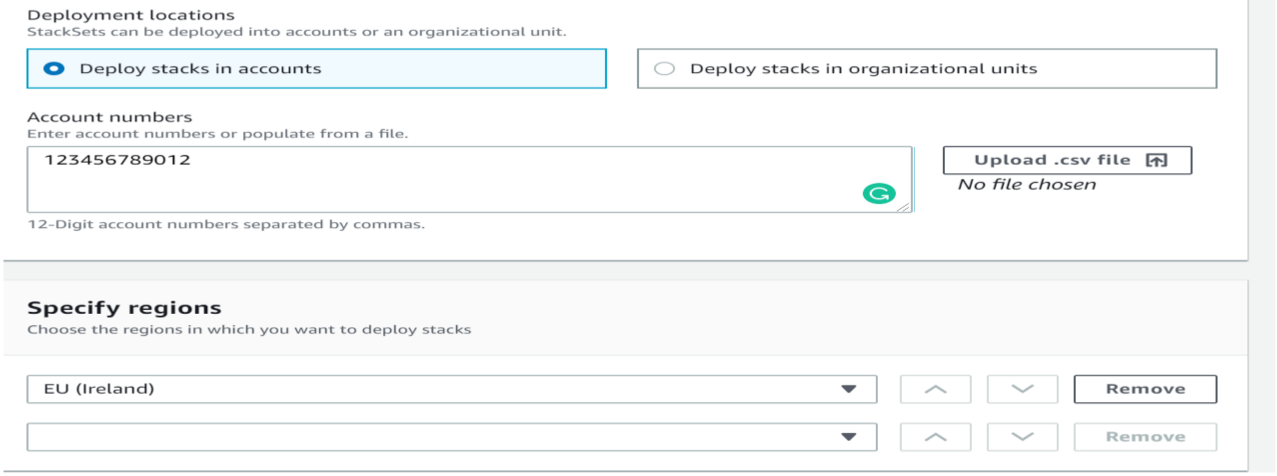
⚠ StackSets will use this role for administering your individual accounts.

IAM execution role name

OrganizationAccountAccessRole

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

- ➢ Paste respective account id and Home Region > next



Deployment locations
StackSets can be deployed into accounts or an organizational unit.

● Deploy stacks in accounts   ○ Deploy stacks in organizational units

Account numbers
Enter account numbers or populate from a file.

123456789012

12-Digit account numbers separated by commas.

Specify regions
Choose the regions in which you want to deploy stacks

EU (Ireland) ▼

- ➢ Review and submit. This will execute stack in log account.

Note: - This last template you need to execute for all account 1 by 1. Like 1 for Prod, 1 for Dev, 1 for Sec, etc