Contents

[AWS Organization Account Landing zone 2](#_Toc8821606)

[Overview 2](#_Toc8821607)

[Steps to implement 3](#_Toc8821608)

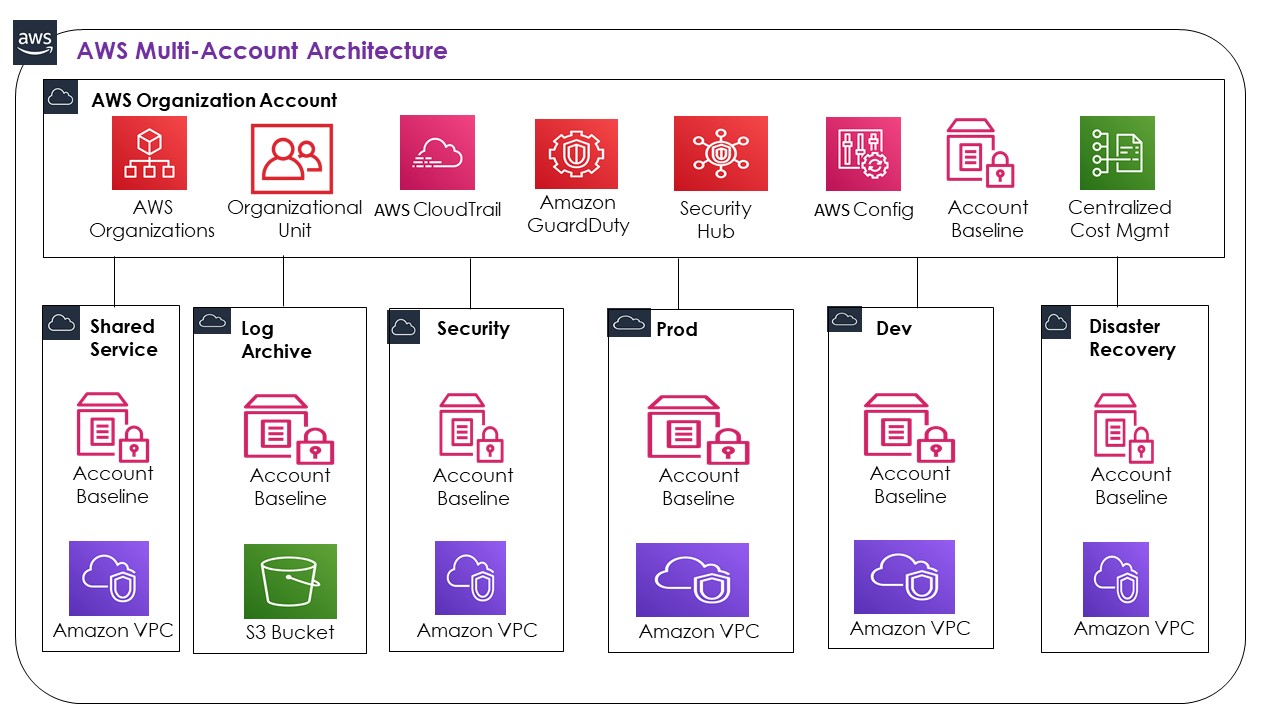
[Prerequisites: - 3](#_Toc8821609)

[Template Executions 5](#_Toc8821610)

# AWS Organization Account Landing zone

## Overview

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

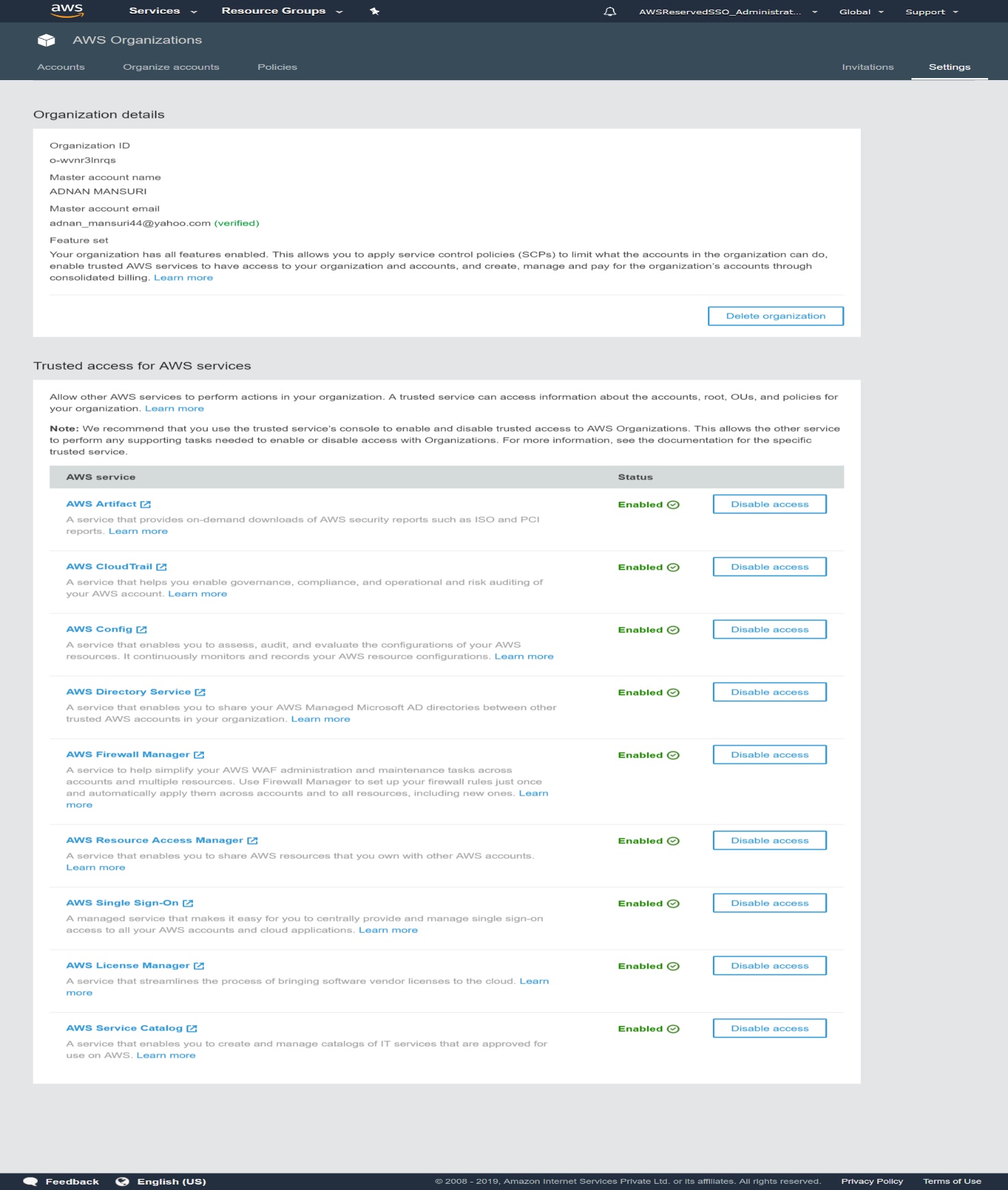


* 1-Prerequisite-IAM Roles-Master
* 2-Prerequisite-Buckets-KMS-Log
* 3-MasterCloudtrail-Master
* 4-SettingupAccount-All-Delete
* 5-Config-Cloudwatch-All-Home-Region
* 6-Config-Cloudwatch-All-Other-Regions
* 7-VPC-Individual Account only

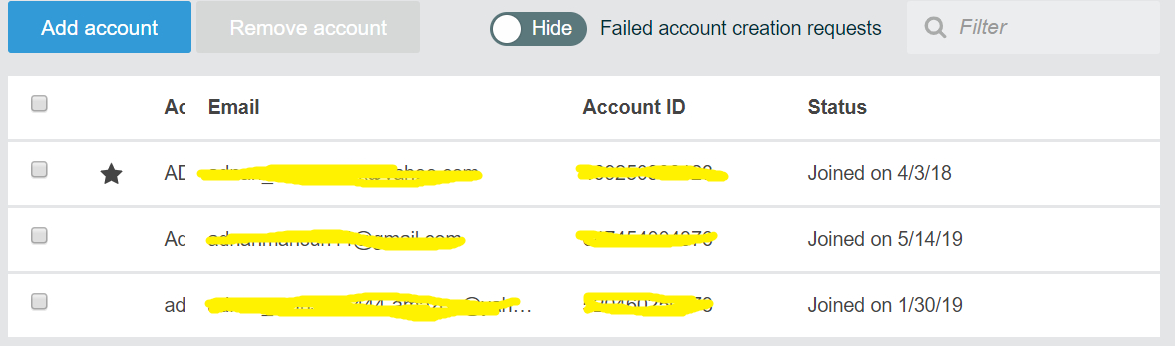
## Steps to implement

### Prerequisites: -

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



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



Note: - Star symbol shows it master.

1. 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

1. 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

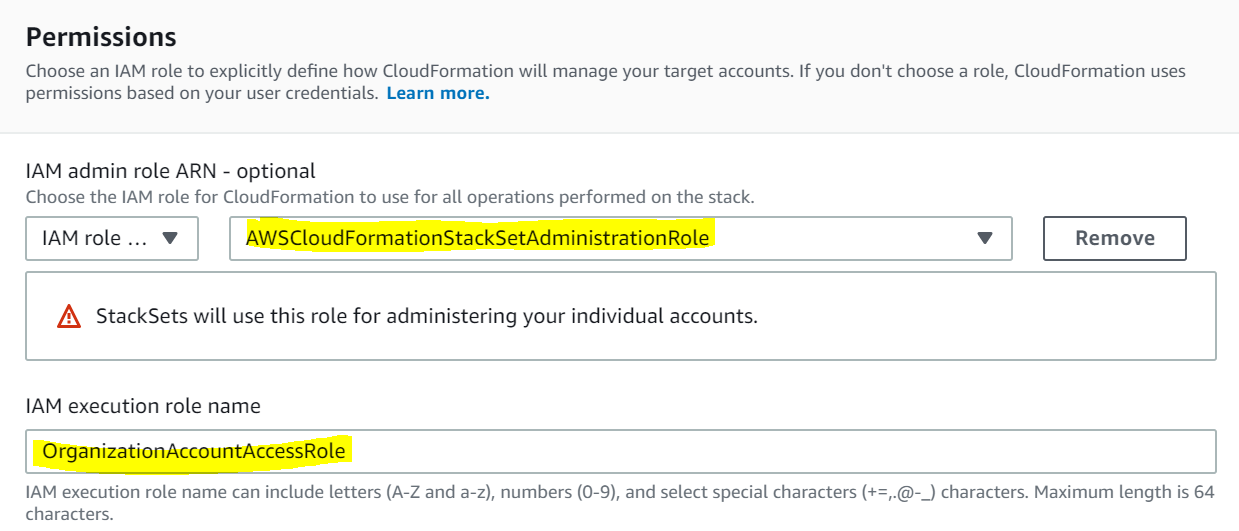
**By stack or stackset**: - stackset

**Output**: - Create S3 bucket, KMS in log account.

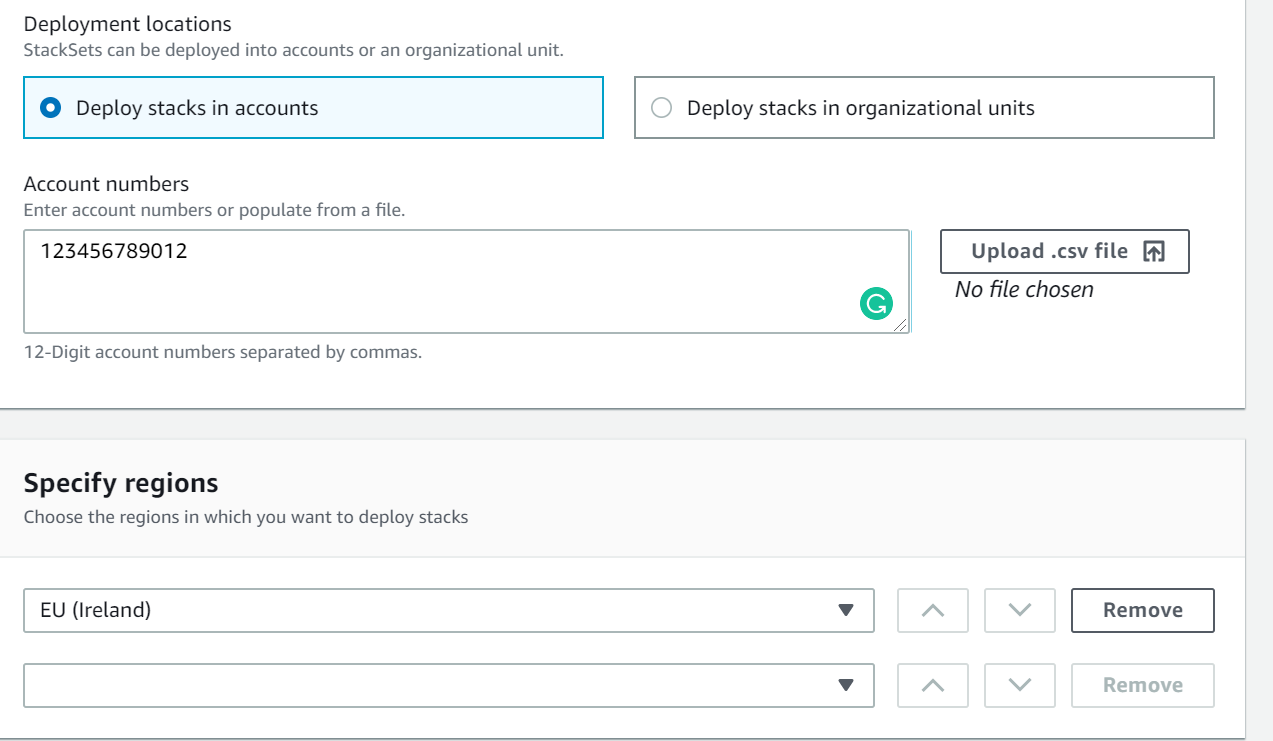
* Go to Cloudformation > Stackset > Create New Stackset
* Upload template file > Next
* Enter Stack Name and paste Master Account id in parameter > next
* Add Followings info and click next

Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole

Enter IAM Execution Role:- OrganizationAccountAccessRole



* Paste Log account id and Home Region > next



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

1. 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

1. 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

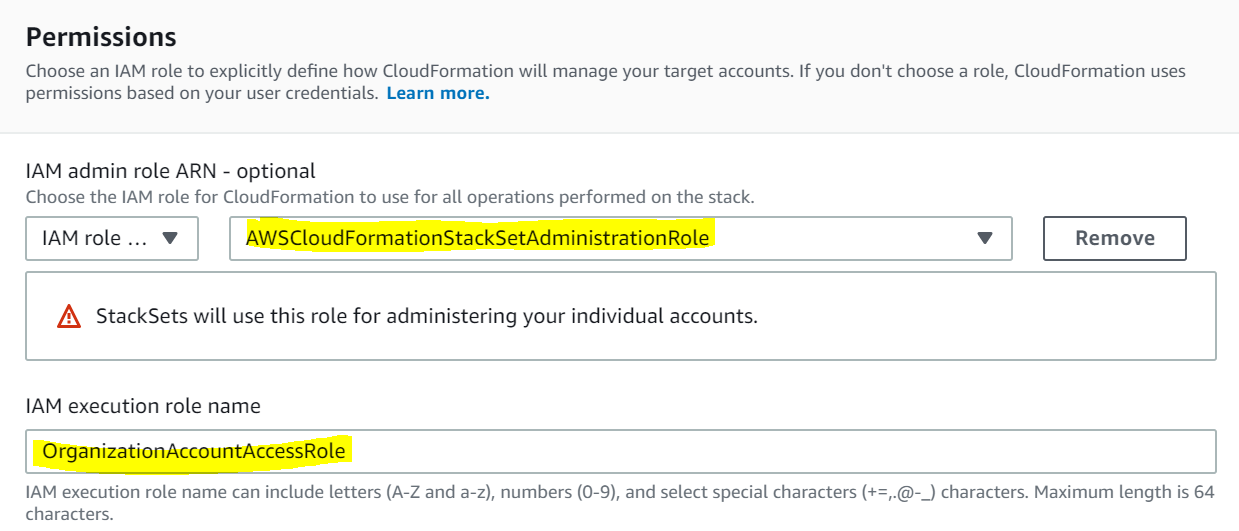
**Output: -** delete default VPC, Update CloudTrail to master, IAM password policy update, S3 Public access block, Security hub and GuardDuty as master

**Note:-** This stack needs to delete after 15 min of successful execution

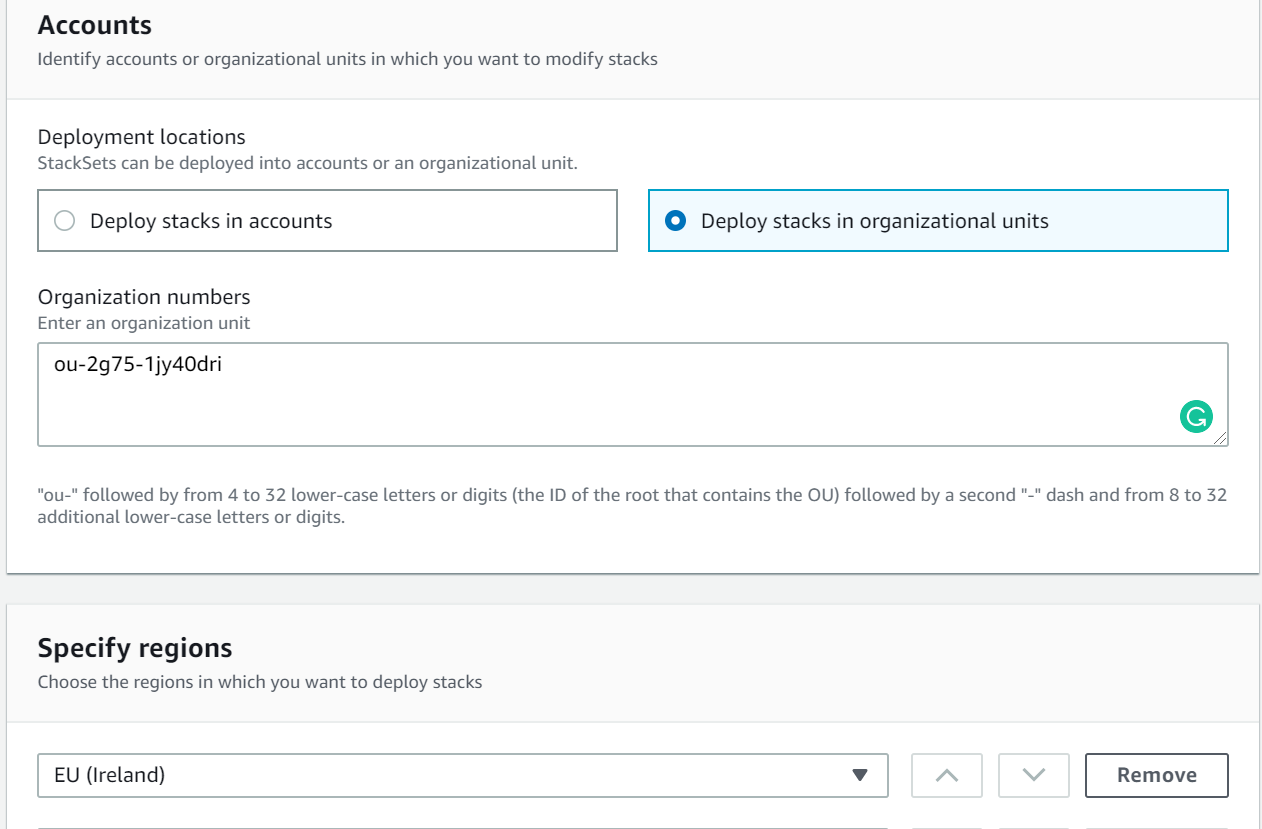
* Go to Cloudformation > Stackset > Create New Stackset
* Upload template file > Next
* Enter Stack Name and paste Master Account id in parameter > next
* Add Followings info and click next

Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole

Enter IAM Execution Role:- OrganizationAccountAccessRole



* Paste Organizational unit id and select Home Region > next



* 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

1. Next template will enable config and cloudwatch alerts in all account

**Template: -** 5-Config-Cloudwatch-All-Home-Region

**Execute: -** All Account with Organization id

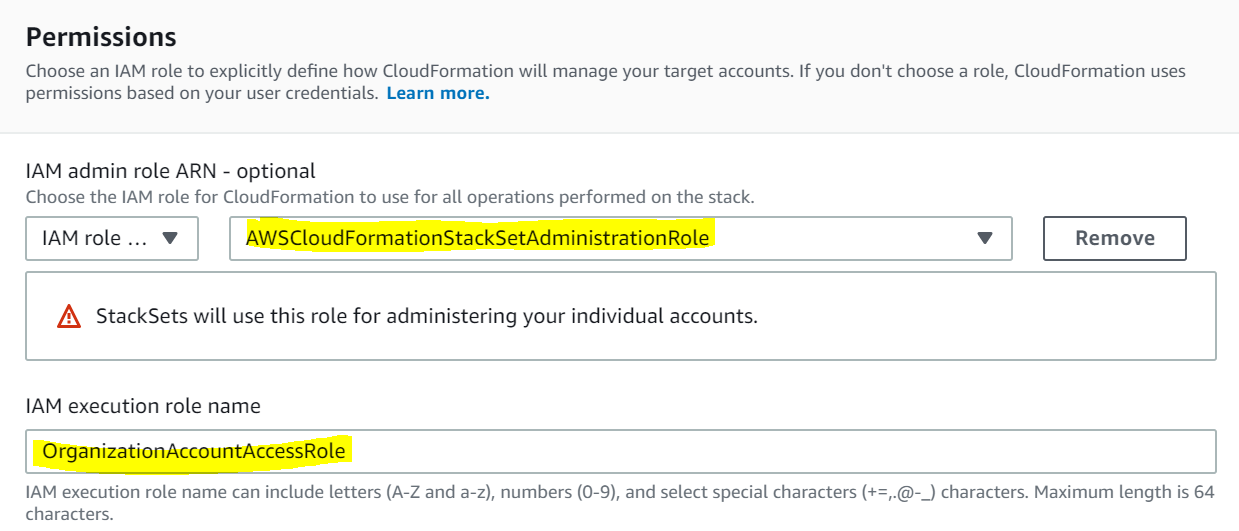
**By stack or stackset: -** stackset

**Output: -** enable config, alarm and events

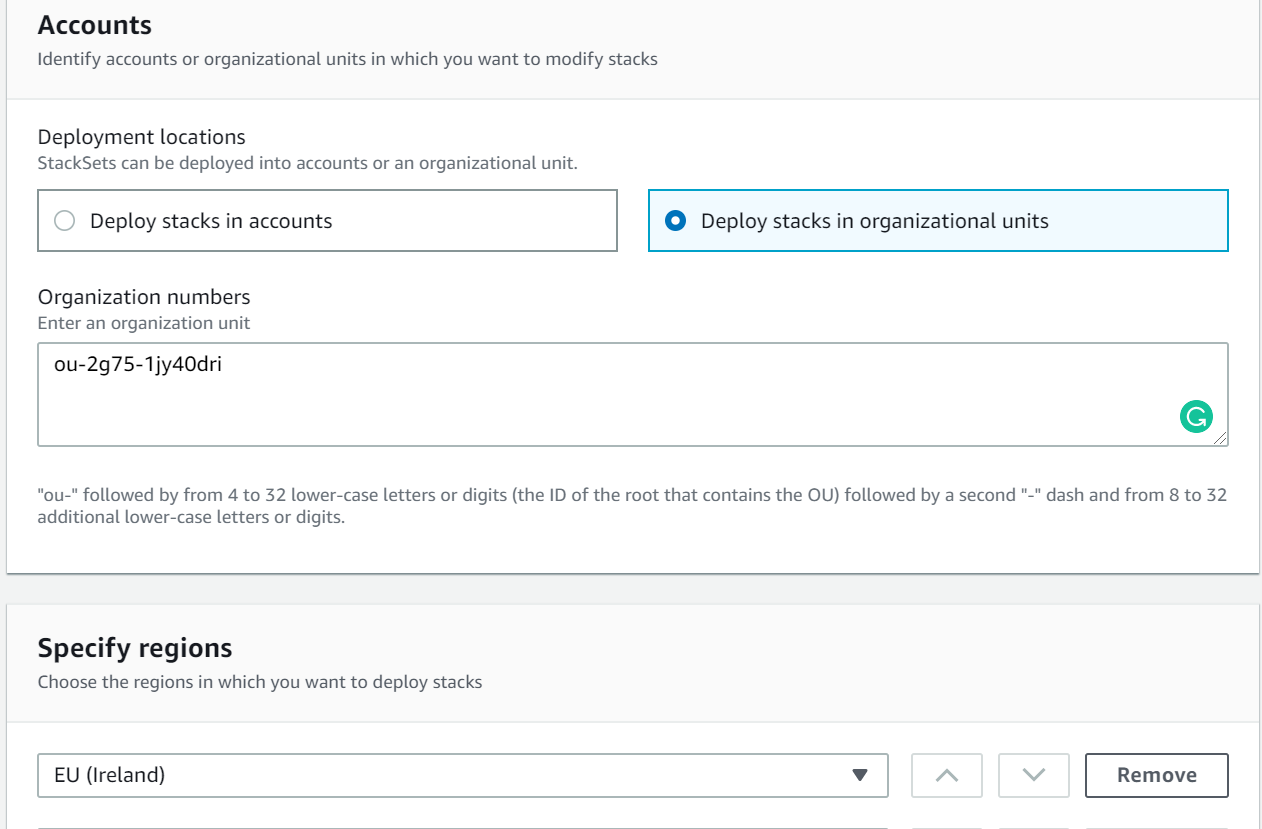
* Go to Cloudformation > Stackset > Create New Stackset
* Upload template file > Next
* Enter Stack Name and paste Master Account id, Email ids in parameter > next
* Add Followings info and click next

Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole

Enter IAM Execution Role:- OrganizationAccountAccessRole



* Paste Organizational unit id and select Home Region > next



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

1. 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

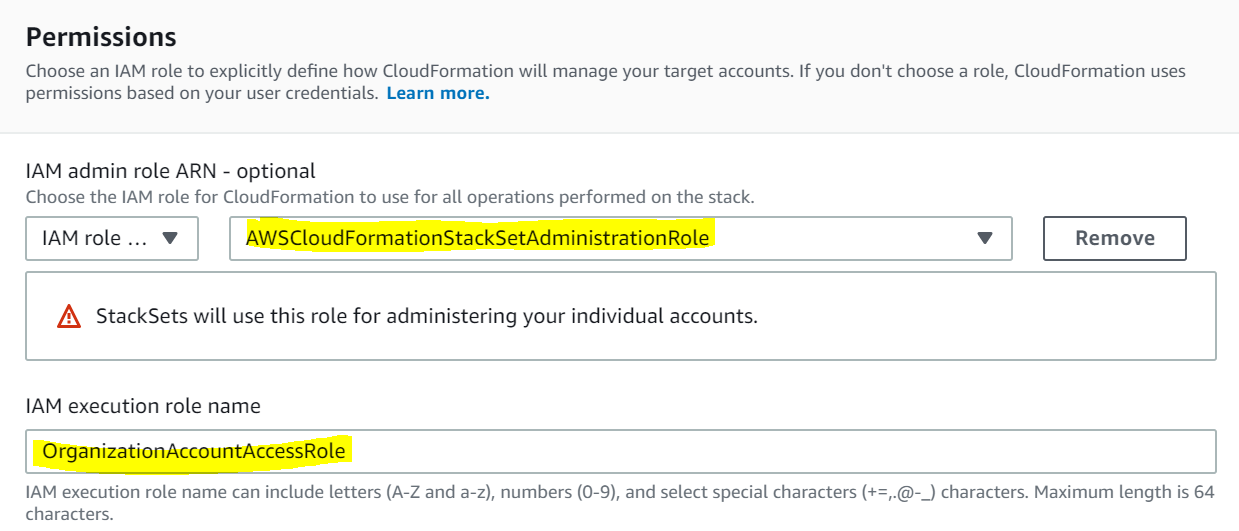
**By stack or stackset: -** stackset

**Output: -** enable config, alarm and events

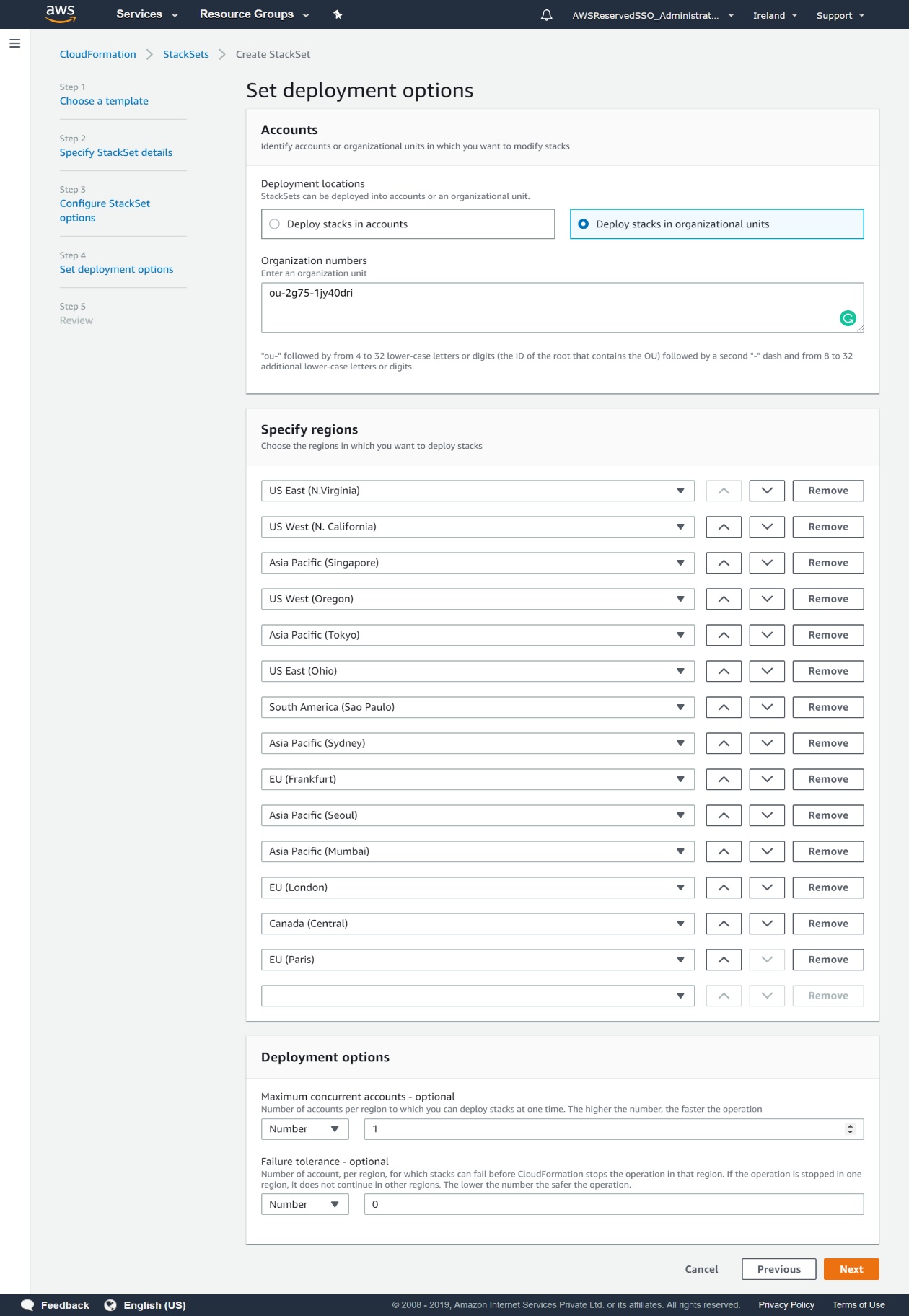
* Go to Cloudformation > Stackset > Create New Stackset
* Upload template file > Next
* Enter Stack Name and paste Master Account id, Email ids in parameter > next
* Add Followings info and click next

Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole

Enter IAM Execution Role:- OrganizationAccountAccessRole



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



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

1. 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

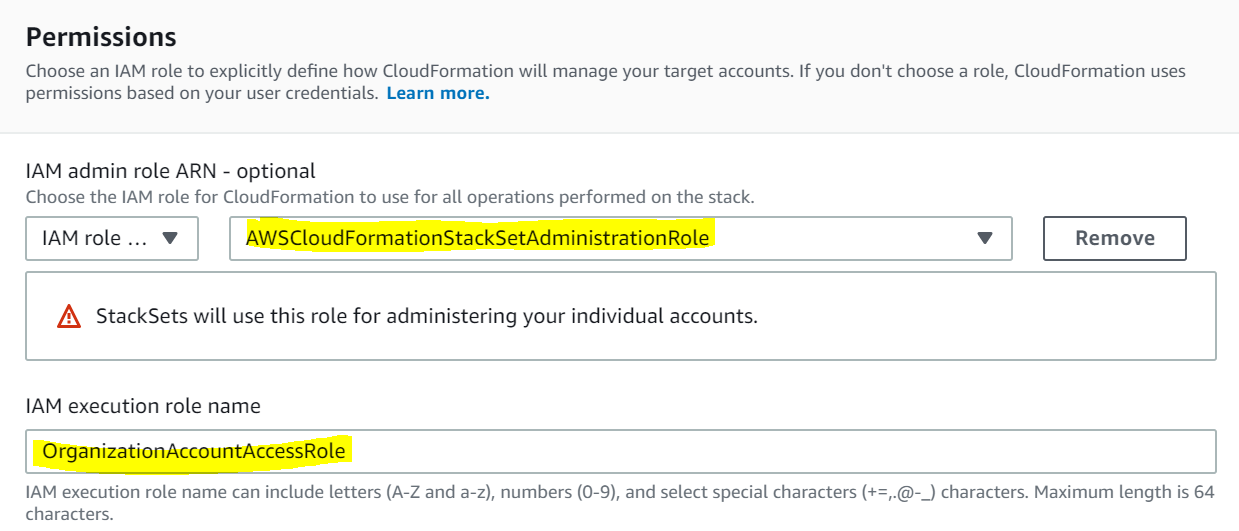
**By stack or stackset**: - stackset

**Output**: - Create VPC, Subnets, VPC Flowlogs.

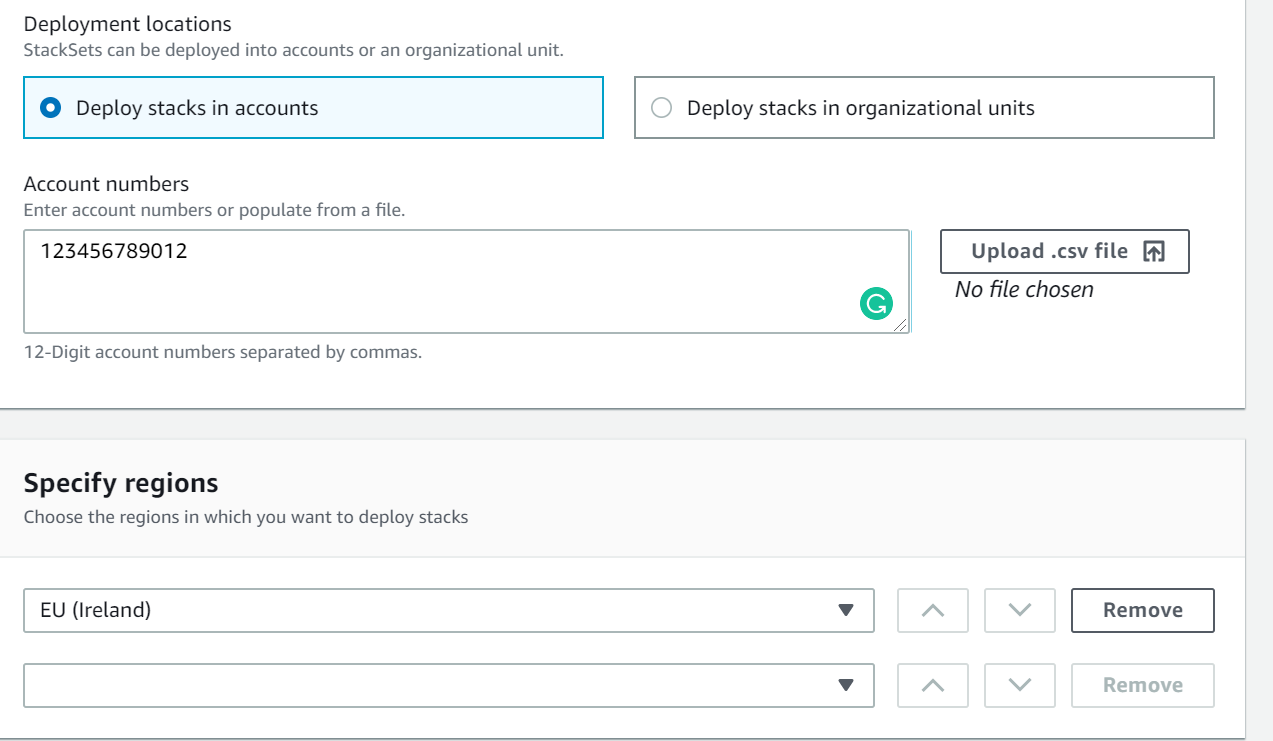
* Go to Cloudformation > Stackset > Create New Stackset
* Upload template file > Next
* Enter Stack Name and VPC CIDR and Name in parameter > next
* Add Followings info and click next

Select IAM Admin role: - AWSCloudFormationStackSetAdministrationRole

Enter IAM Execution Role:- OrganizationAccountAccessRole



* Paste respective account id and Home Region > next



* 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