Contents

[Overview 1](#_Toc138794468)

[CMO Suggestions 1](#_Toc138794469)

[AWS – GuardDuty Heartbeat IAM Role 1](#_Toc138794470)

[Role Details 1](#_Toc138794471)

[CloudFormation Template 1](#_Toc138794472)

[Deploy Role and Permissions on Member Accounts using CloudFormation StackSet 1](#_Toc138794473)

[AWS – Prisma role permissions management 1](#_Toc138794474)

[CloudFormation Template 1](#_Toc138794475)

[Deploy IAM Policy on Member Accounts using CloudFormation StackSet 1](#_Toc138794476)

[Update new Prisma permissions on Member Accounts using StackSet 1](#_Toc138794477)

[Deploy IAM Policy/Update IAM Policy Management Account using CloudFormation Stack on 1](#_Toc138794478)

[AWS – Service Control Policies 1](#_Toc138794479)

# Overview

As part of security standards, CMO are using defined process on AWS Global Master Payer Account. We recommend clients with individual Organizations to follow the same process for enhanced security and better management of resources.

# CMO Suggestions

* AWS – GuardDuty Heartbeat IAM Role
* AWS – Prisma role permissions management
* AWS – Service Control Policies

## **AWS – GuardDuty Heartbeat IAM Role**

Currently InfoSec expects AWS GuardDuty configuration to be done in a certain way on each client account. If the configuration is not as per InfoSec standard, that AWS account will be flagged as non-complaint. But clients can configure GuardDuty the way they need to send findings to InfoSec's Splunk. Because of this reason, InfoSec has now decided to change the approach for GuardDuty Non-Complaint. Until account is sending GuardDuty findings to InfoSec, that account is Complaint.

To know if the GuardDuty configuration is correct to send findings to InfoSec's Splunk, a sample finding will be generated on each AWS account using an automation. This sample finding will be generated daily keep checking the GuardDuty configuration. InfoSec will have a system in place to find out if they do not receive a sample finding from any of the AWS account and will mark the account as non-Complaint accordingly.

### **Role Details**

Role Name: AWSGuardDutyExecutionRole

Permissions: "guardduty:ListDetectors", "guardduty:CreateSampleFindings", "ec2:DescribeRegions"

### **CloudFormation Template**

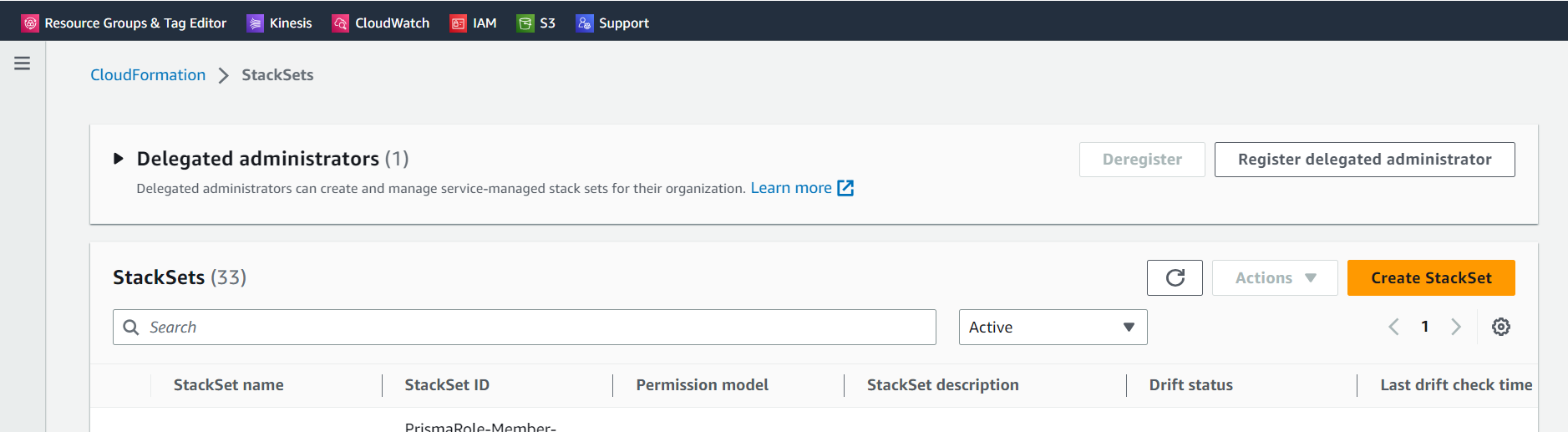
This CloudFormation template is used to create StackSet. You can double click on below icon to download the same.



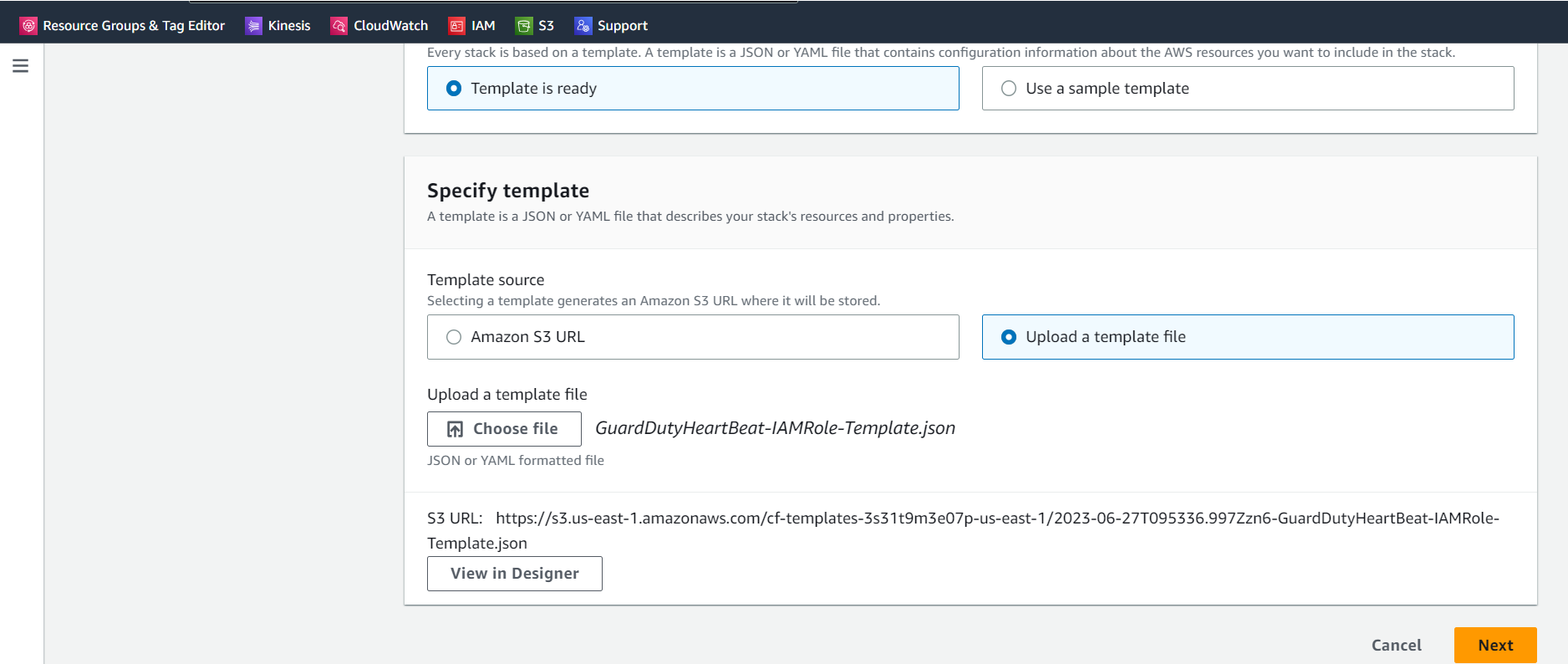
### **Deploy Role and Permissions on Member Accounts using CloudFormation StackSet**

Required IAM role can be created using any method on your account. CMO recommendation is to use CloudFormation StackSet for the same. Please follow below steps to create IAM role and required permissions using StackSet.

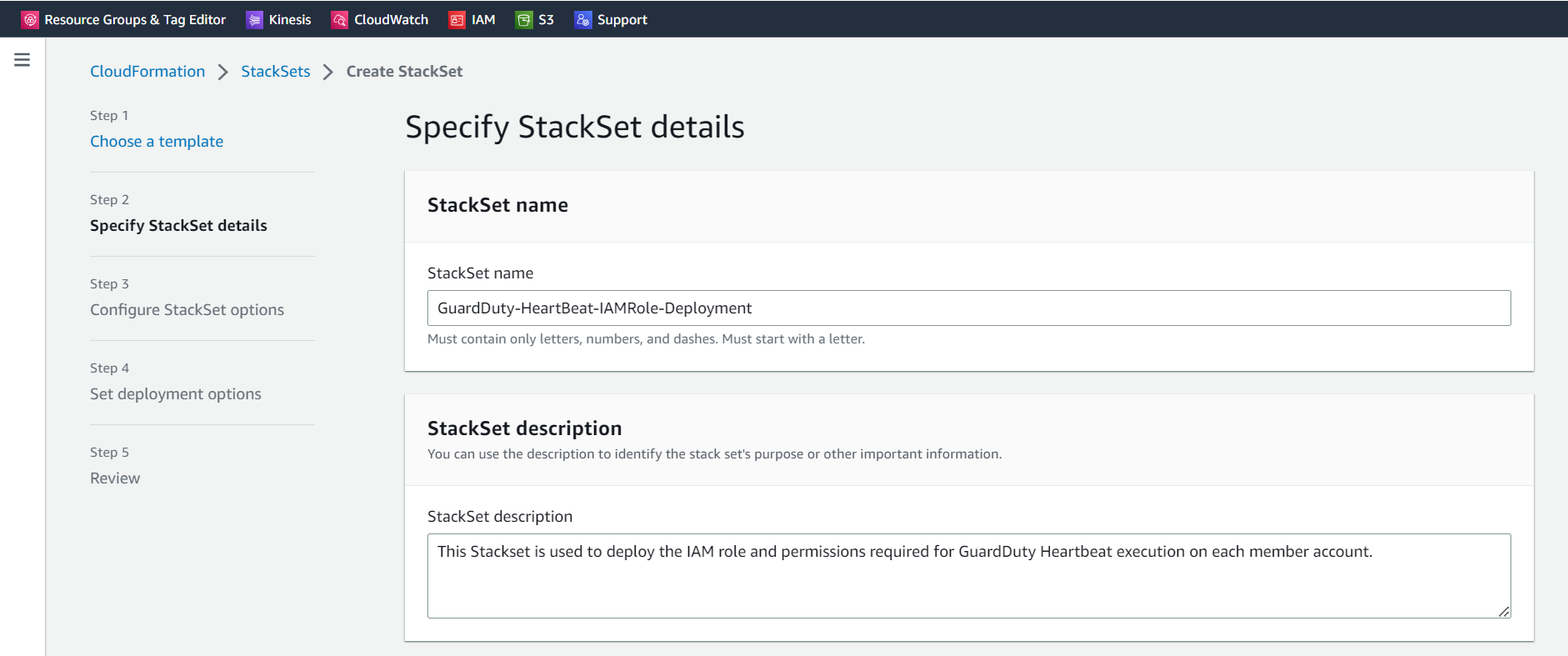
* Login to your MPA. Navigate to CloudFormation StackSets and click on “Create StackSet”



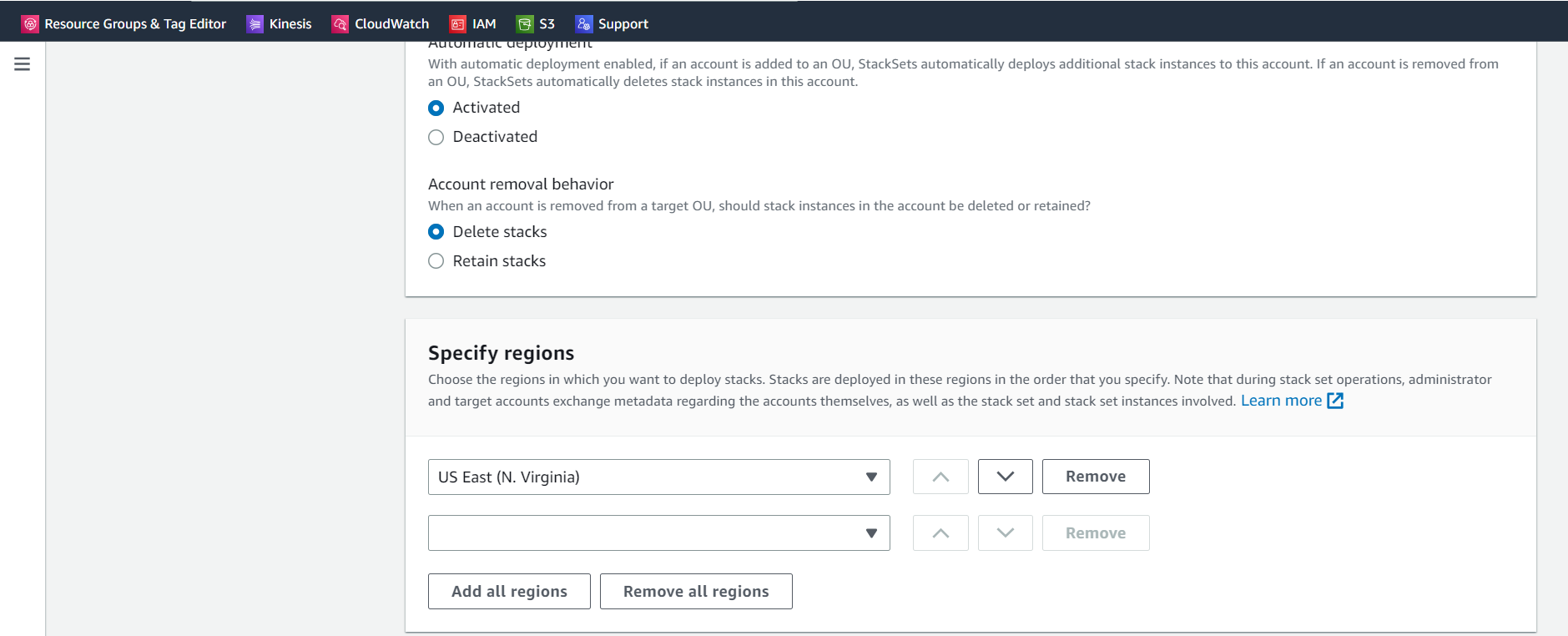
* Select values as per below screenshot and upload the template file. Once the template file is uploaded, click on "Next"



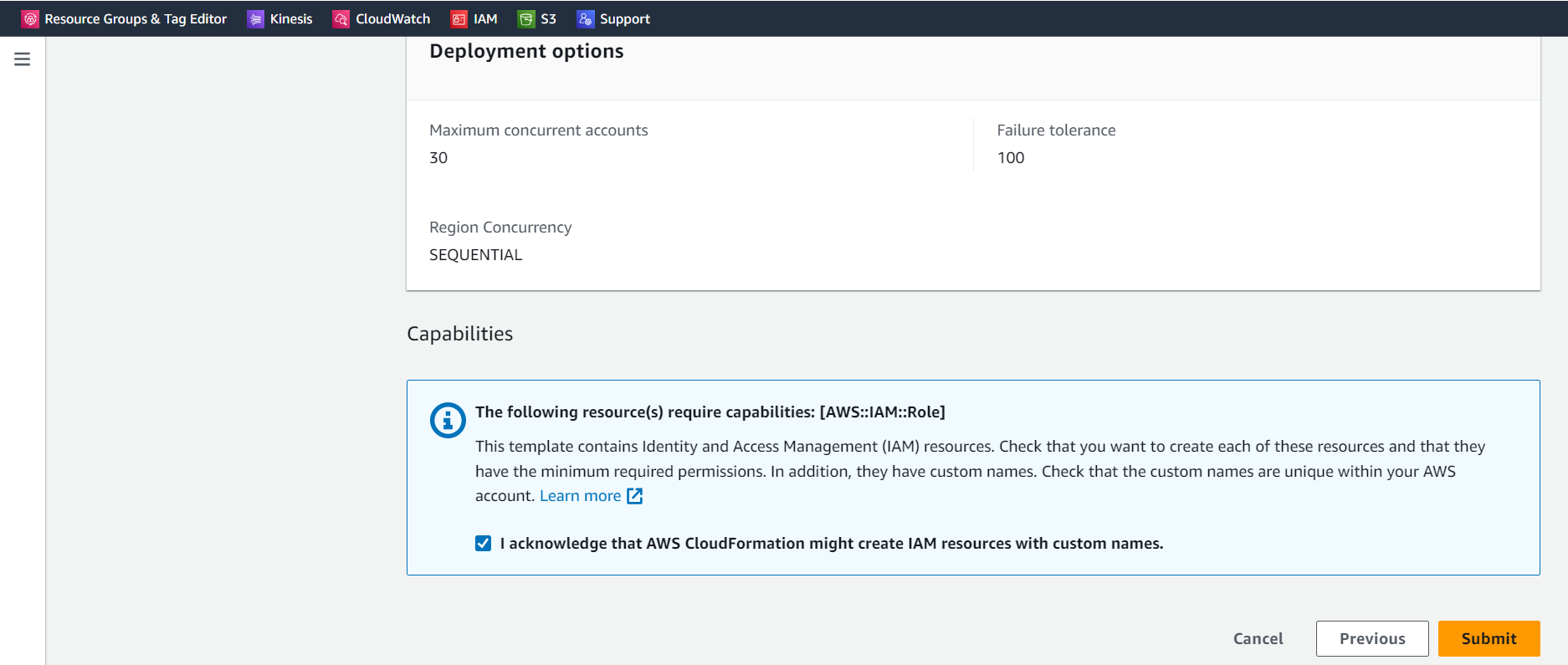
* On the next screen, give StackSet name and description and click on "Next"



* On the next screen, select one region. You can select "US East (N. Virginia)



* On the next screen, click on check box to acknowledge and click on "Submit"



## **AWS – Prisma role permissions management**

As part of continuous security improvements, Prisma release new permissions and same needs to be updated on PrismaReadOnly role on each AWS account. In CMO Global master payer, we have a new process to overcome this problem of updating permission on each account.

A new solution has been designed and implemented which involves using AWS Organization feature. Instead of using inline policy on IAM role, we are using customer managed policy. These managed policies have been deployed in each AWS account through MPA using AWS CloudFormation StackSet. There will be one-time manual activity to delete the existing inline policy from the IAM role and to attach the newly created managed policy to the IAM role.

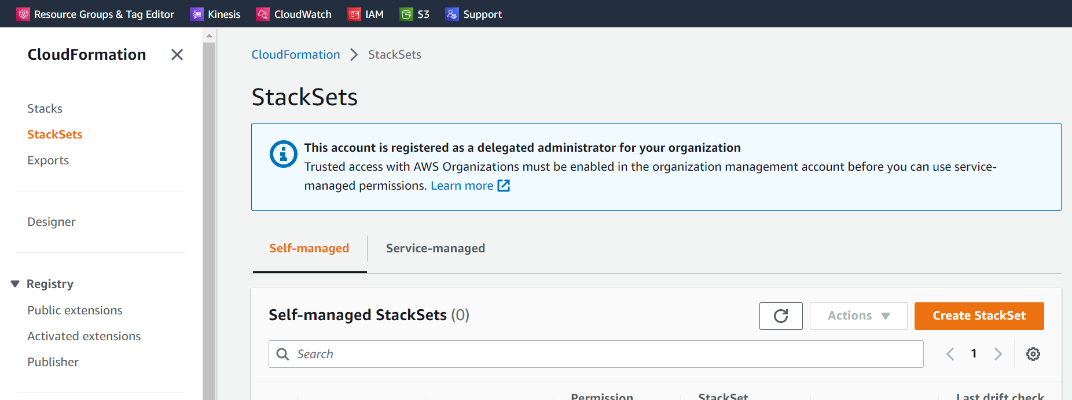
### **CloudFormation Template**

This CloudFormation template is used to create StackSet. You can double click on below icon to download the same.

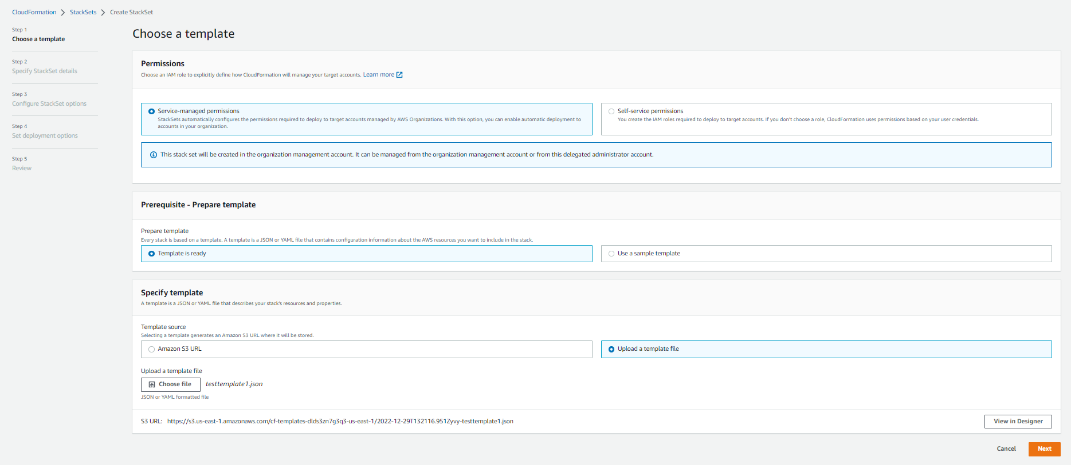


### **Deploy IAM Policy on Member Accounts using CloudFormation StackSet**

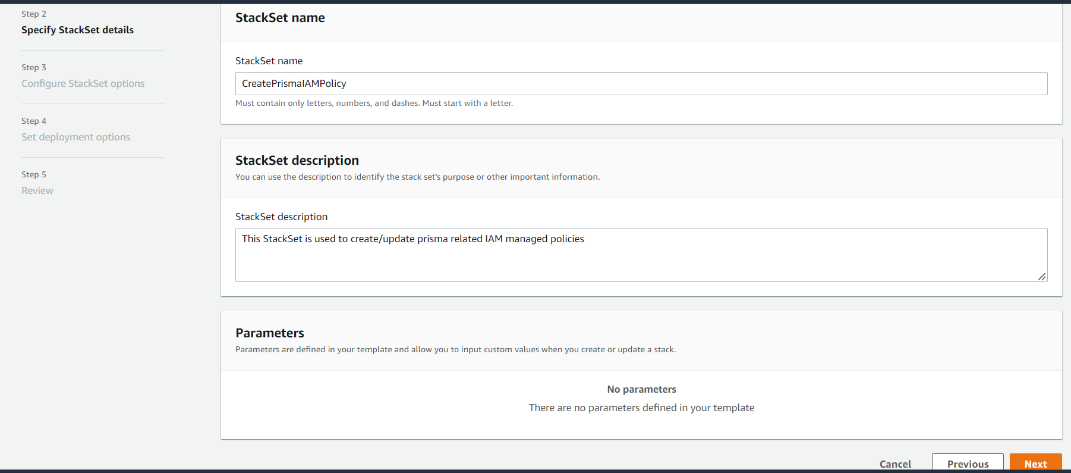
* Login to your MPA. Navigate to CloudFormation StackSets and click on Create StackSet



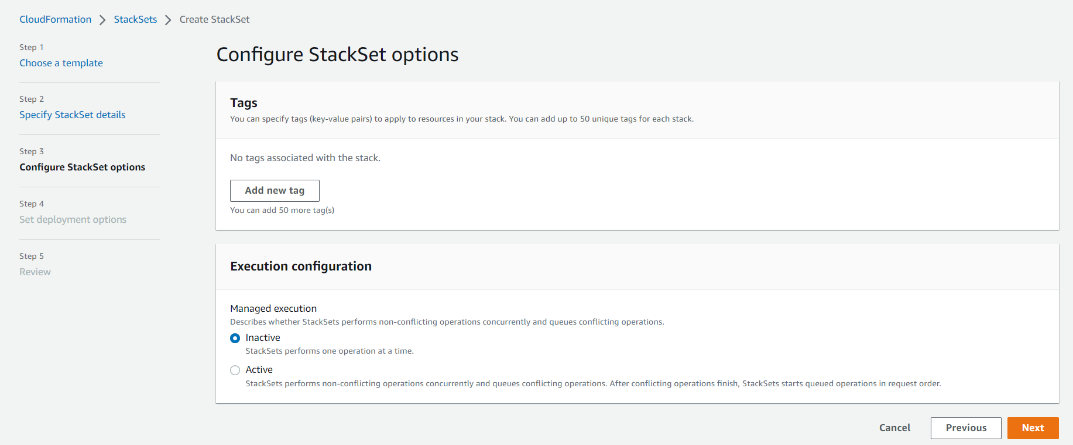
* Select values as per below screenshot and upload the template file. Once the template file is uploaded, click on "Next"



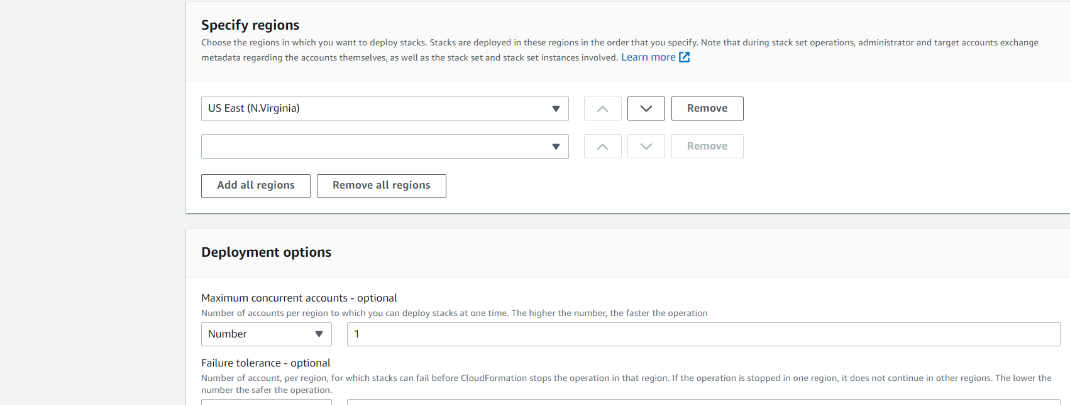
* On the next screen, give StackSet name and description and click on "Next"



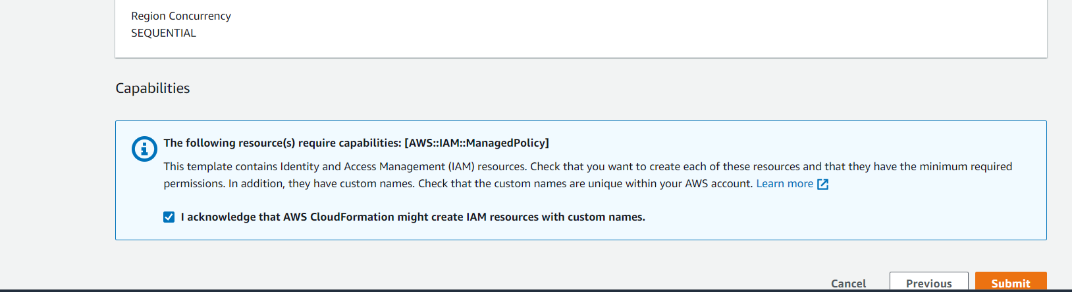
* On the next screen, do not make any change and click on "Next"



* On the next screen, select one region. You can select "US East (N. Virginia)

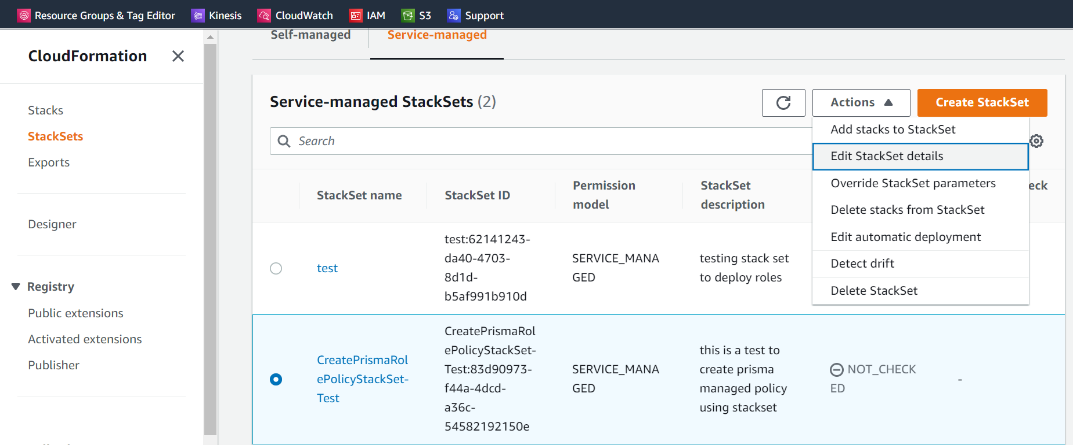


* On the next screen, click on check box to acknowledge and click on "Submit"

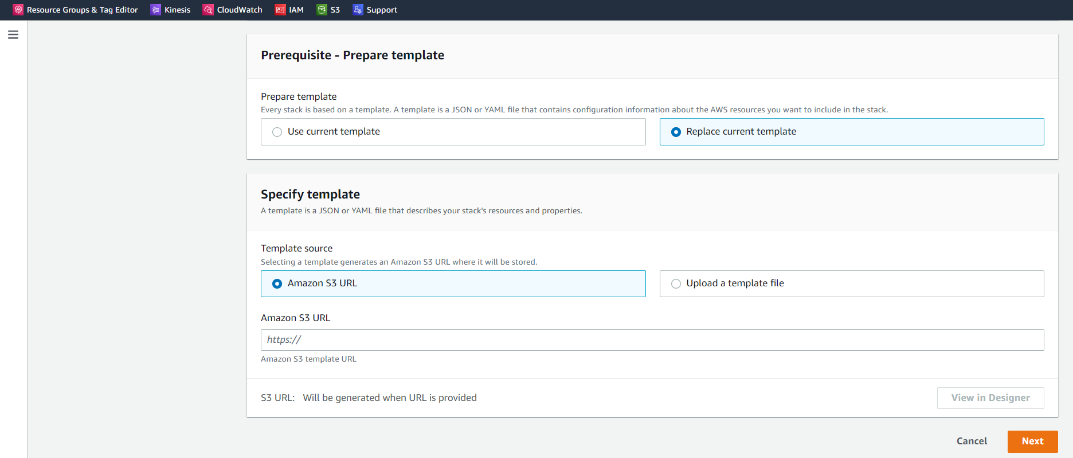


### **Update new Prisma permissions on Member Accounts using StackSet**

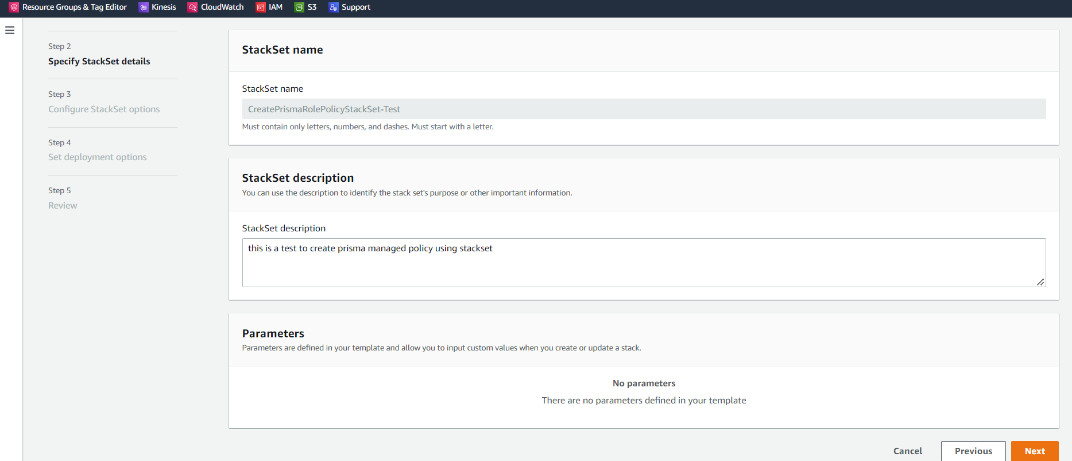
* Login to your AWS MPA. Navigate to CloudFormation StackSets. Select your StackSet and click on "Edit StackSet details" from Actions dropdown



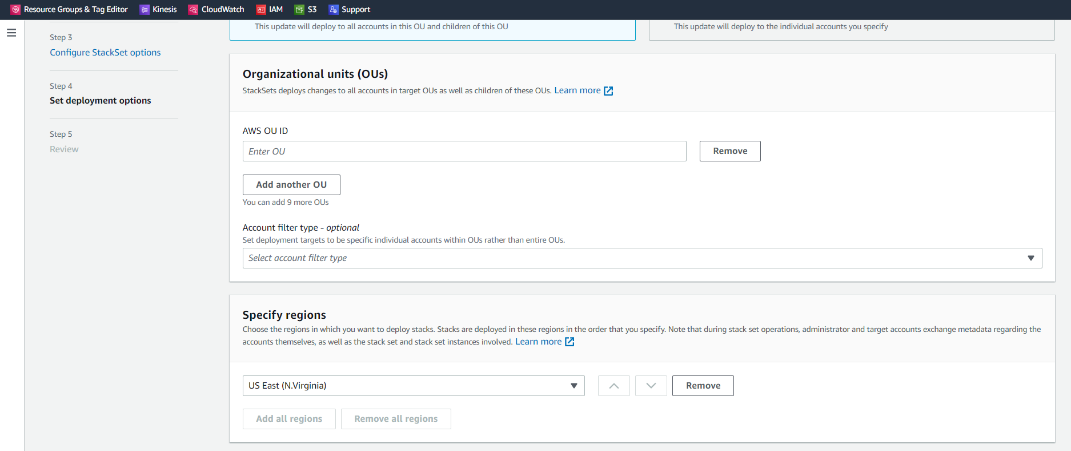
* On the next screen, click on Relace current template. Then click on Upload a template file and select your updated template file and upload it. Once the file is uploaded, click on "Next"



* On the next screen, make changes if required and click on "Next"



* On the next screen, do not make any change and click on "Next"
* On the next screen, specify your OU ID and region and click on "Next"

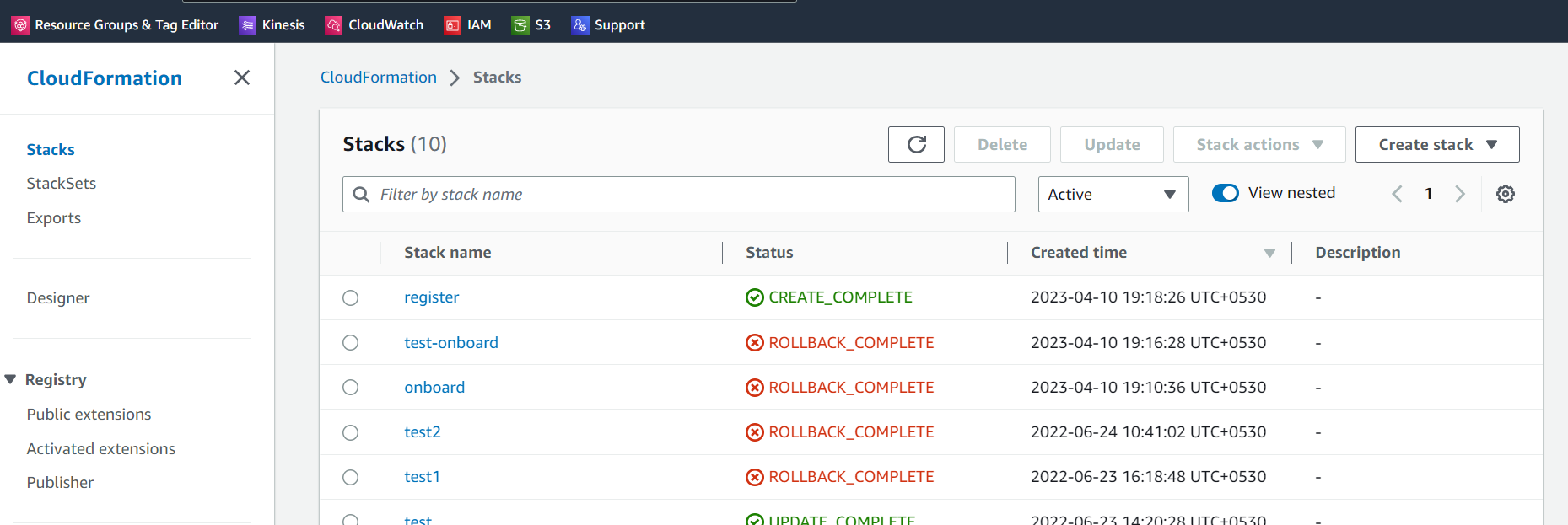


* On the next screen, review and click on "Submit"

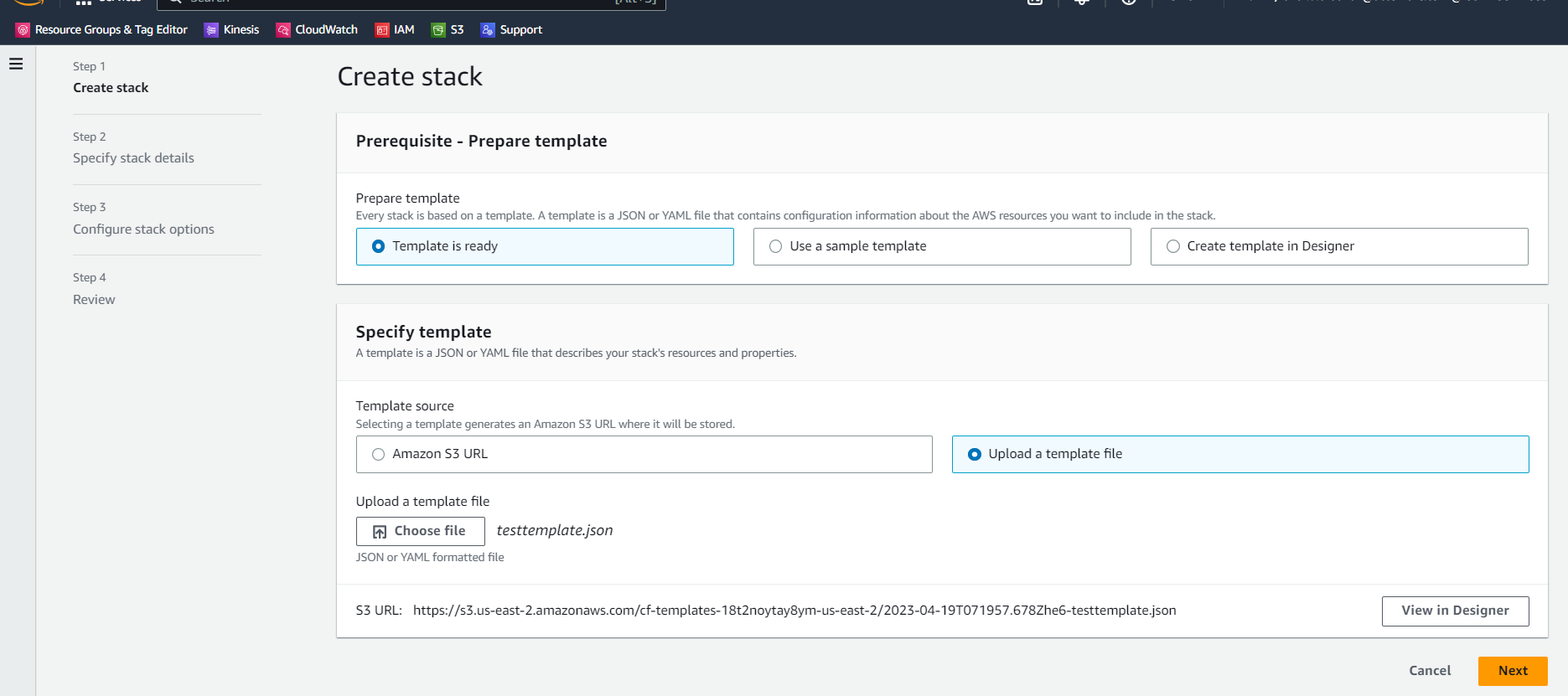
### **Deploy IAM Policy/Update IAM Policy Management Account using CloudFormation Stack on**

When the CloudFormation template is run using a StackSet on management account (MPA), it will create resources only on member accounts. But the MPA is also registered in Prisma and hence the permission needs to be updated on this account too. To do this, the same CloudFormation template can be run as a Stack to create managed policies on MPA. The same Stack can be used in future to update new permissions.

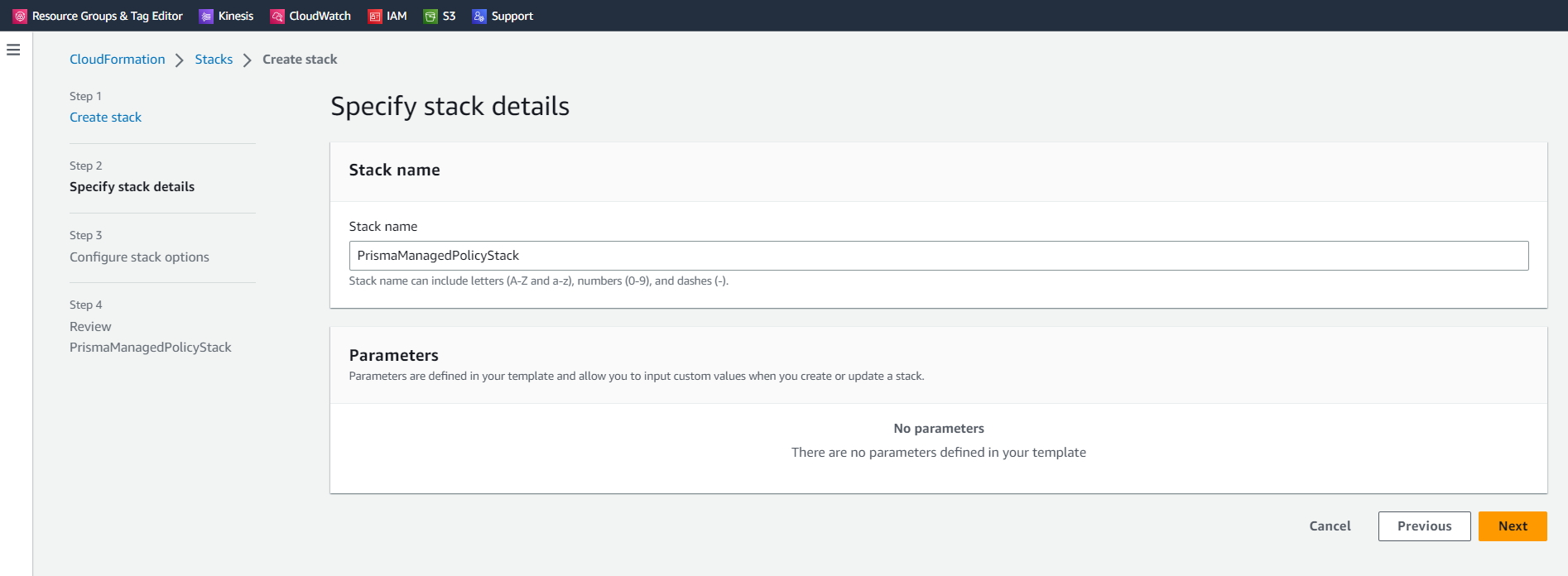
* Login to your AWS MPA. Navigate to CloudFormation Stack and click on "Create Stack with new Resources" from Actions dropdown



* Select values as per below screenshot and upload the template file. Once the template file is uploaded, click on "Next"



* On the next screen, give StackSet name and click on "Next"



* On the next screen, do not make any change and click on "Next"
* On the next screen, review and click on Submit
* Same steps can be followed to update permissions on the Stack

## **AWS – Service Control Policies**

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization’s access control guidelines. SCPs alone are not sufficient to granting permissions to the accounts in your organization. No permissions are granted by an SCP. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts. To know more on SCP [here](https://aws.amazon.com/blogs/security/get-more-out-of-service-control-policies-in-a-multi-account-environment/).

We (CMO) have applied [these](https://kxdocuments.accenture.com/contribution/9e618003-4354-4afd-8ec7-537d1d25632b) SCPs on our Global Master Payer. We suggest clients with dedicated Organization to apply same SCPs on their MPA.