Synctree Flosports | AWS Inspector

Introduction

Amazon Inspector is an automated vulnerability management service that continually scans Amazon EC2 and container workloads for software vulnerabilities and unintended network exposure.

Using Amazon Inspector you can manage multiple accounts that are associated with AWS Organizations by simply delegating an administrator account for Amazon Inspector. The delegated administrator manages Amazon Inspector for the organization and is granted special permission to perform tasks on behalf of your organization.

The Inspector Organization solution will automate enabling Amazon Inspector by delegating administration to an account (e.g. Audit or Security Tooling) and configuring Inspector for all the existing and future AWS Organization accounts.

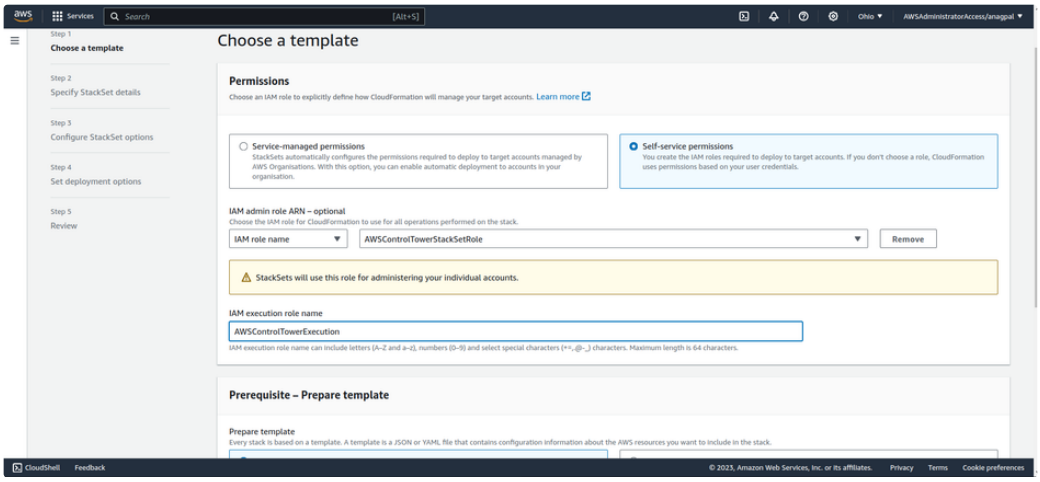
Important Features of Amazon Inspector:

- Enable or disable scans for member accounts
- View aggregated finding data from the entire organization
- Create and manage suppression rules

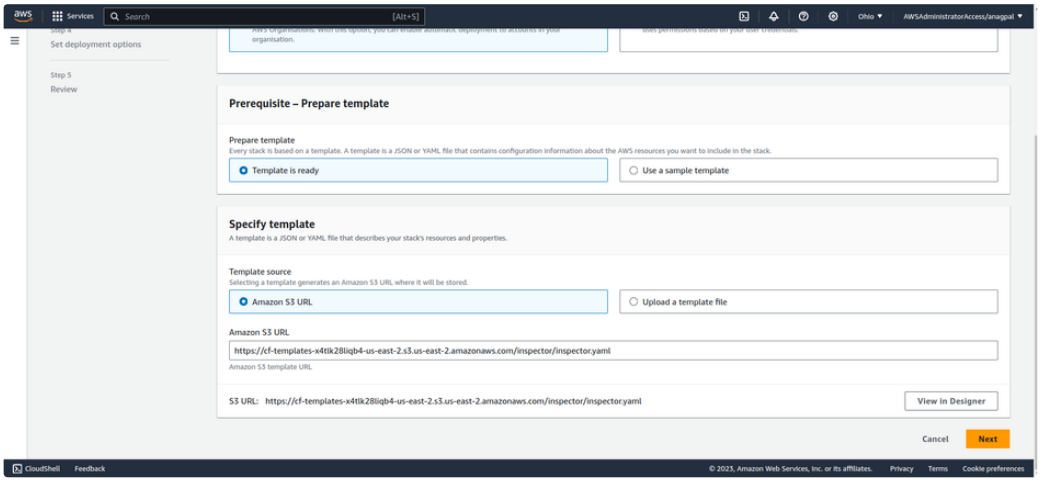
Start Creating CloudFormation StackSet :

Step 1: Go to AWS Cloudformation>StackSets and Select Create StackSet

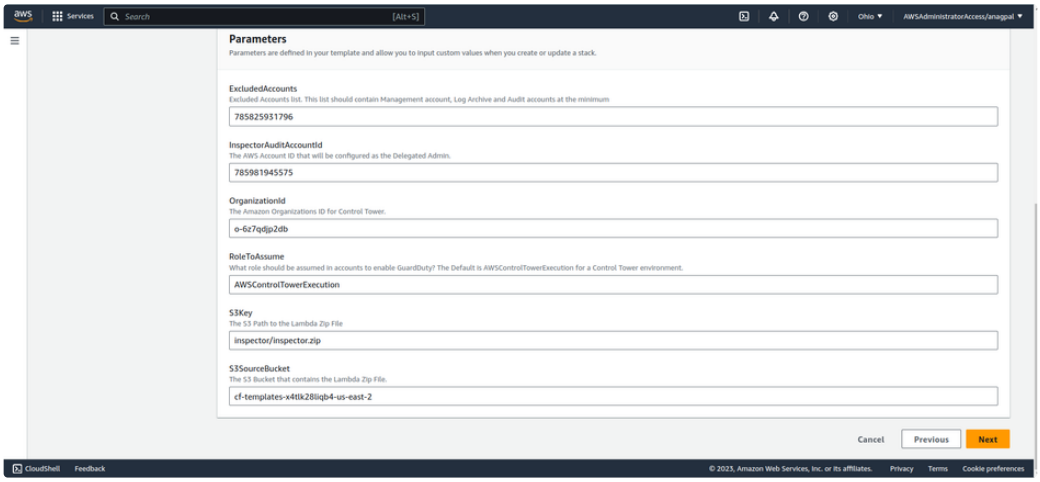
Step 2: Select Self-service permissions select IAM admin role ARN and give the IAM execution role name and select Next



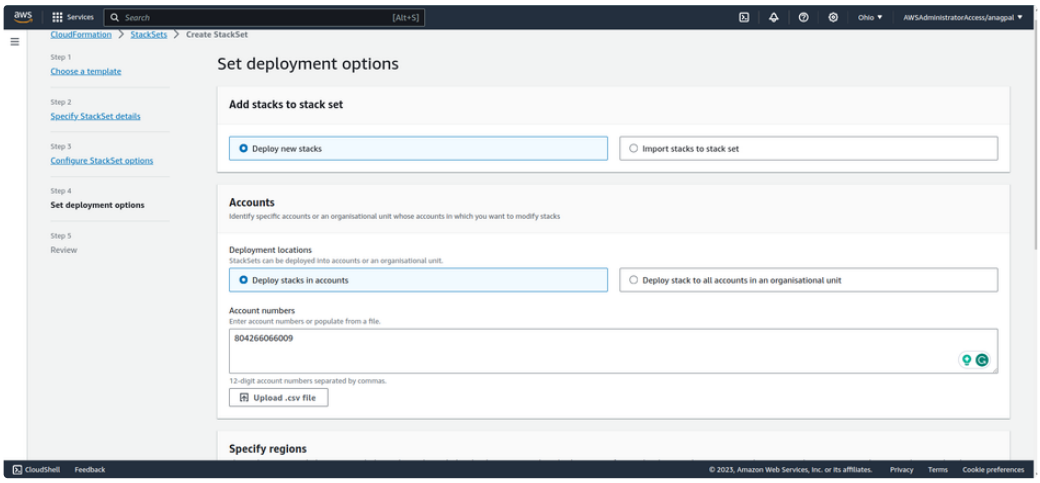
Step 3: Give the template file S3 URL.



Step 4: Fill all the required parameters and select Next



Step 5: Select Deploy stack in accounts, give management account Id, select control tower region and select Next.



Step 6: Review all the details and select Submit

References

Repository: aws-security-reference-architecture-examples Python ★813 200