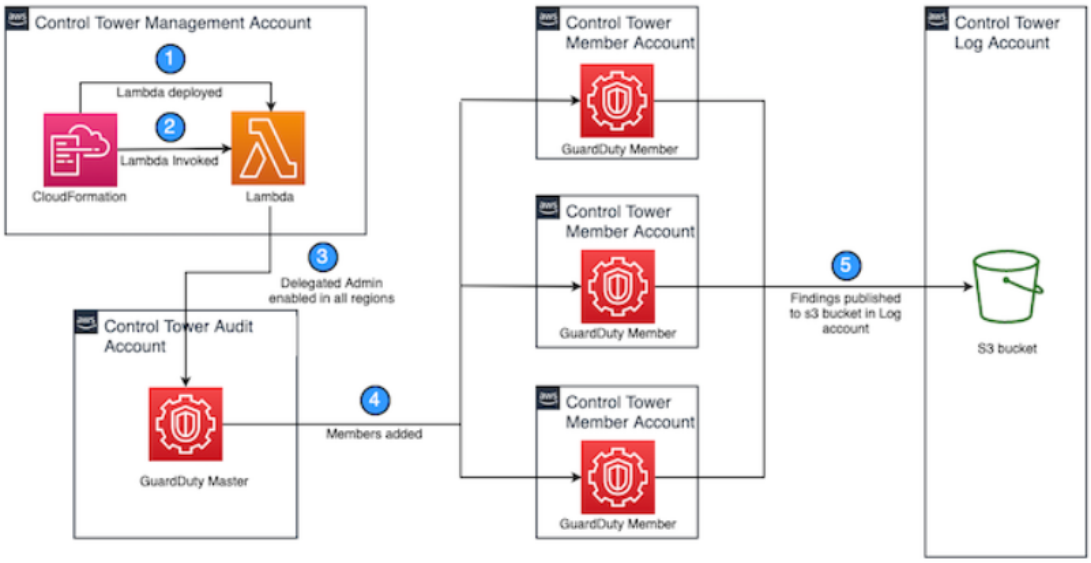
Synctree Flosports | GuardDuty

GuardDuty can be used to continuously monitor any AWS account or workload for malicious activity and unauthorized behavior. It uses machine learning and integrated threat intelligence to identify abnormal behavior and suspected attackers. This is done from billions of events recorded via AWS CloudTrail, Amazon Virtual Private Cloud (VPC) Flow logs, and Domain Name System (DNS) logs. In this example, we implement GuardDuty to protect accounts that have been created and are governed by AWS Control Tower.

We deploy GuardDuty using the GuardDuty delegated administrator feature. This feature allows you to manage multiple GuardDuty accounts in an AWS Organization, and is broadly applicable to any AWS Organization. Where AWS Control Tower is an ideal use case, it is not a prerequisite for using GuardDuty or the GuardDuty delegated administrator feature.

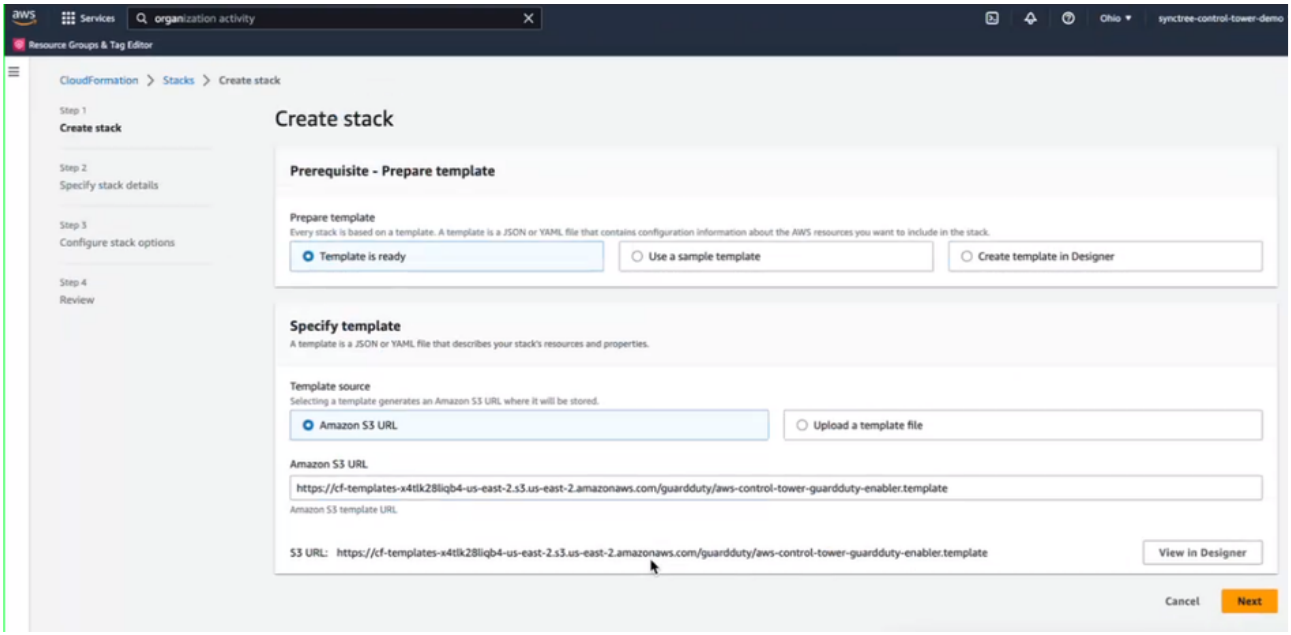


Let’s Do practically:

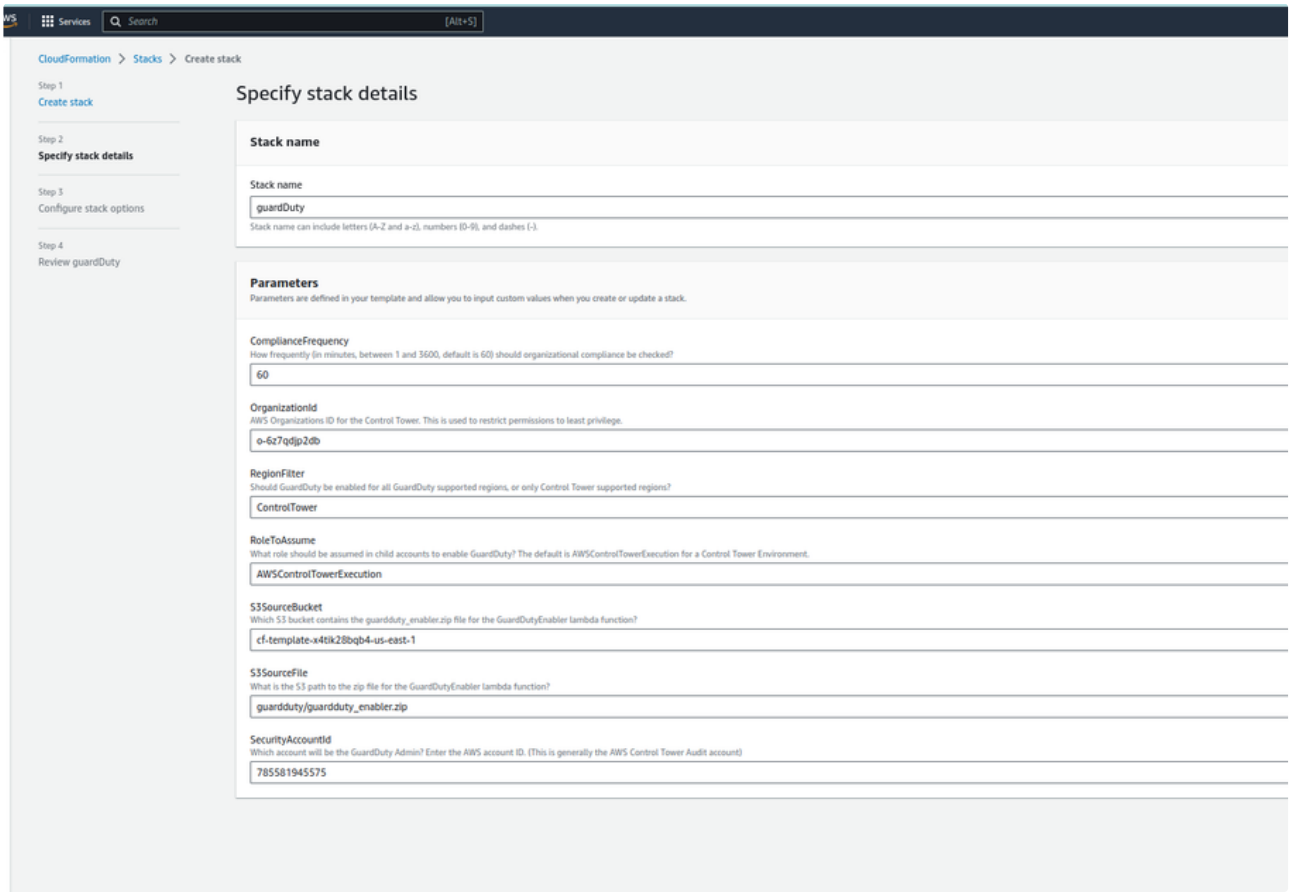
- **GDDelegatedAdminAccountId:** The Account ID of the account you would like to be your GuardDuty administrator. This is typically the AWS Control Tower audit account.
- **OrganizationId:** The ID of the organization (in a format such as o-xxxxxxxxxx), which can be found on the Settings tab of the AWS Organizations console.
- **RoleToAssume:** IAM role to be assumed in child accounts to enable GuardDuty. The default is `AWSControlTowerExecution` that is created by AWS Control Tower and has necessary permission.
- **S3Key:** The path to the function.zip file that contains the *EnableGDDelegatedAdminLambda* function. Path of S3-bucket where template file are added in S3 -
- **S3-SourceBucket:** The S3 bucket that hosts the function.zip file that contains the *EnableGDDelegatedAdminLambda* function. The function.zip file is hosted in the *aws-service-catalog-reference-architectures* S3 bucket. we added like this : `guardduty/guardduty_enabler.zip`

Start Creating Stack of Cloud-Formation:

Step-1 :



Step-2 :



Add your resource parameters as above in stack

- ComplianceFrequency set 60 by default & other parameters add your own.

- Click on **Next** and reviewed once all parameters

Step-3 :

Finally check guardDuty working in AWS Console.