Synctree Flosports | Inspection-Lambda

This sample gives you an example of Python 3.x based Lambda function code to inspect your Control Tower-based multi-account environment from your Control Tower Audit account. The function uses the existing Audit focused IAM roles in your Audit account to assume corresponding roles in the individual accounts being inspected.

The use case for inspection in this example looks for dangling Route53 DNS records for A records pointing to IP addresses that your accounts no longer own. Several other use cases for inspection and remediation can be developed using this mechanism.

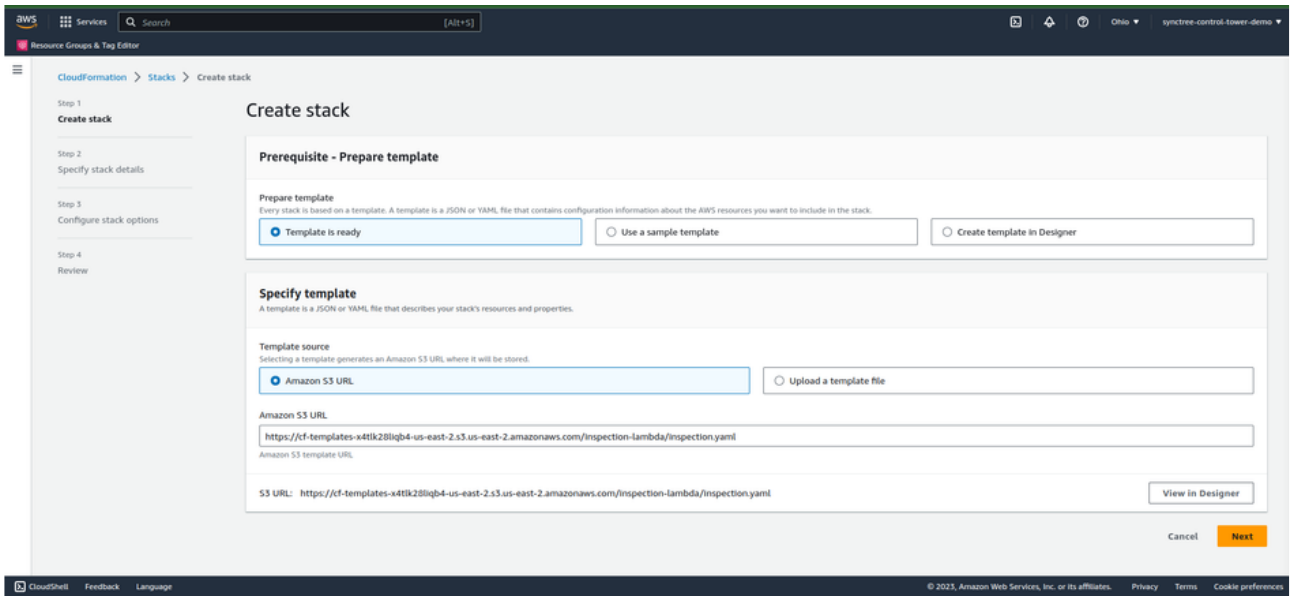
When you are building workloads on AWS, you are encouraged to follow a multi-account strategy to isolate workloads into multiple AWS accounts. You can separate your accounts based on different business units, stages of the software development lifecycle (SDLC), or another manner that suits your organization's needs. Whichever approach you decide to take, a multi-account strategy provides you with the right level of workload isolation and separation of concerns in your AWS environment. With decades of experience in architecting various workloads, we introduced AWS Control Tower as a service that provisions a managed landing zone. A landing zone refers to a well-architected multi-account AWS environment. Control Tower allows you to manage and govern your multi-account setup at scale. As your AWS environment grows, you often must inspect resources across your multiple AWS accounts for different needs.

In this post, we will show you how to inspect your multi-account AWS environment with the help of AWS Lambda.

Start Creating Stack of CloudFormation:

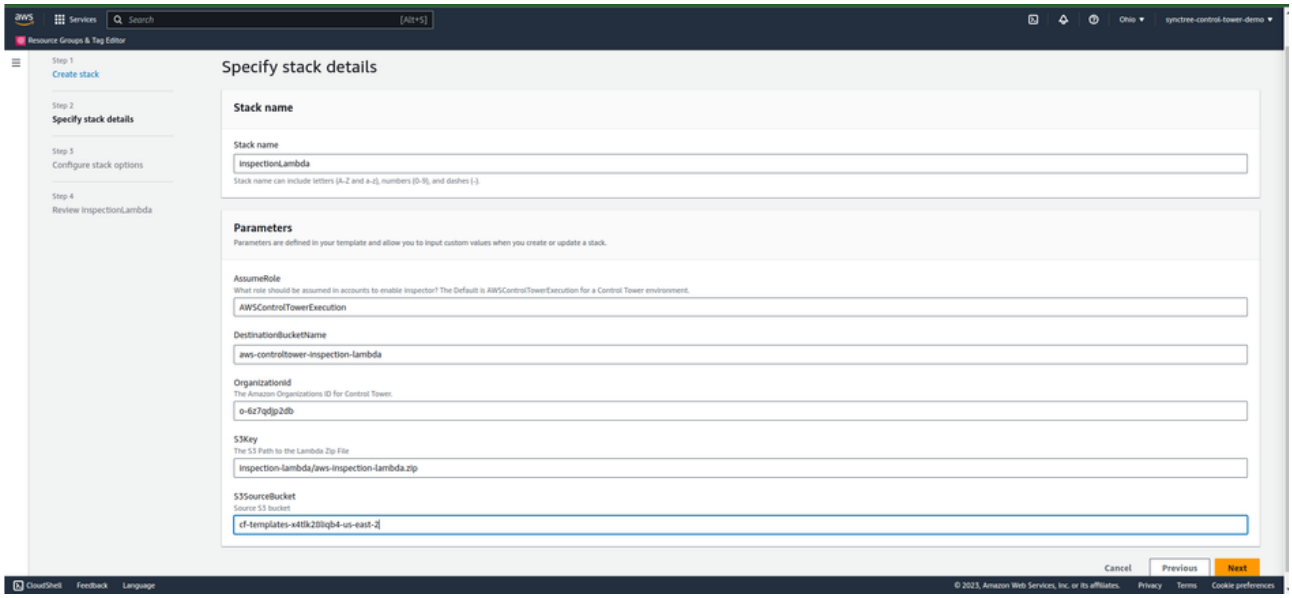
Step: 1

- Added Object URL of your S3 source Bucket in below



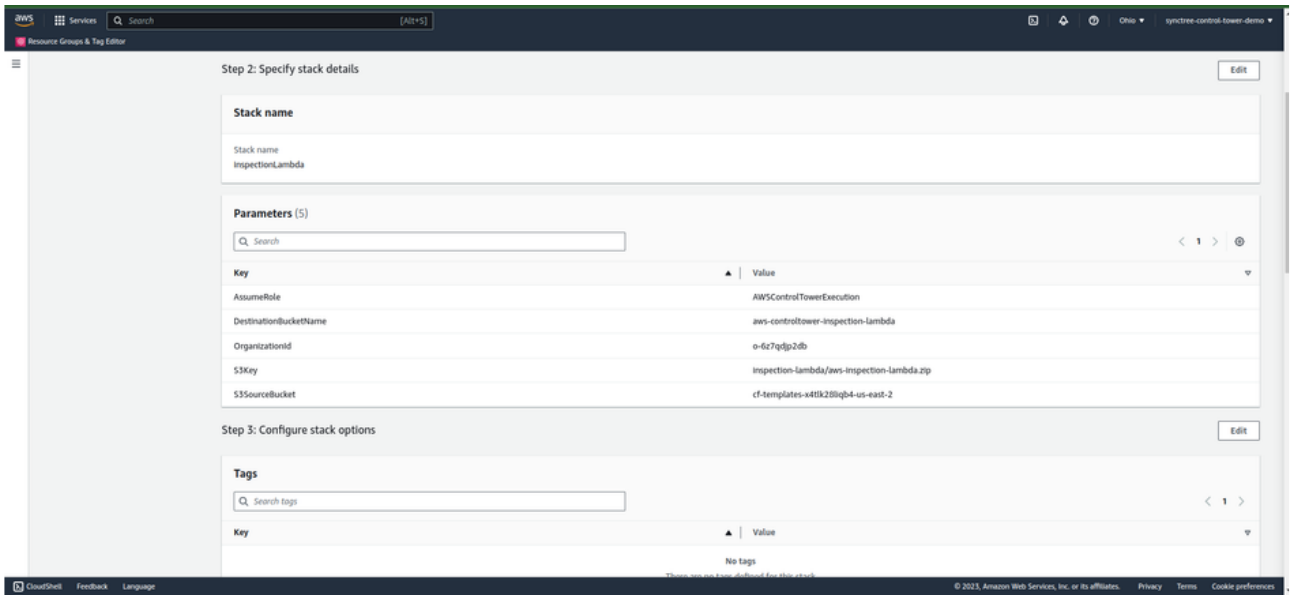
Step: 2

- Add parameters of CloudFormation Stack



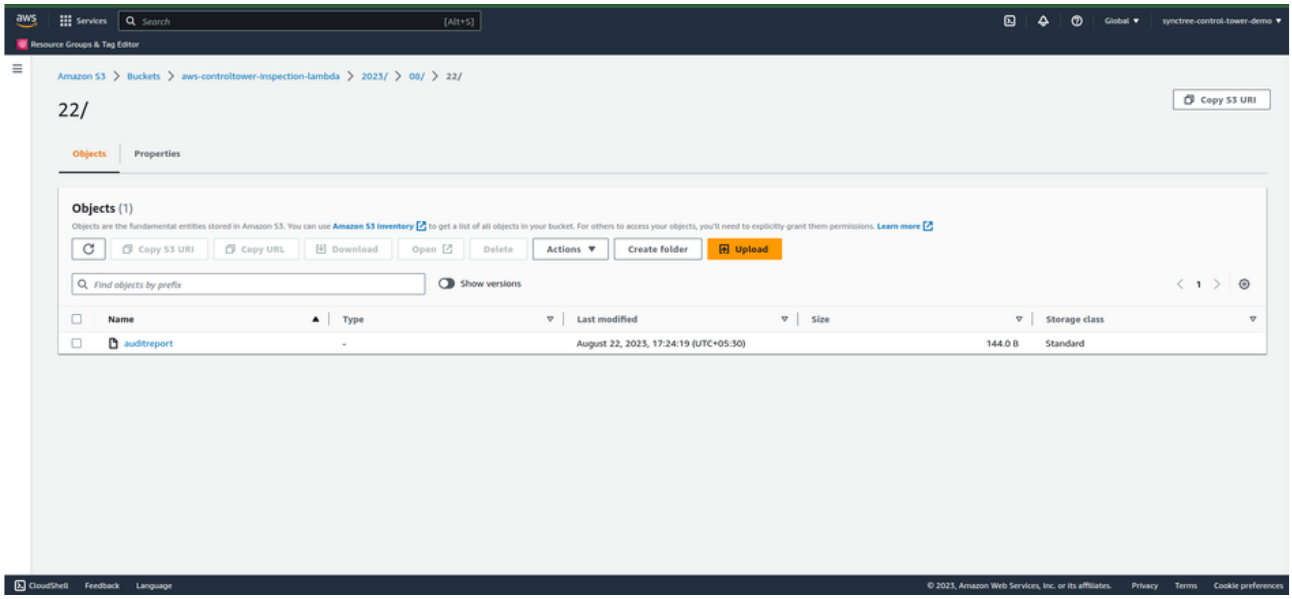
- **DestinatioBucketName :** Add the bucket name where we get generated report of DNS.

Step: 3



- Once reviewed parameters of stack & click on submit.

Step: 4


Services
Search
[Alt+S]
Global
synctree-control-tower-demo
Resource Groups & Tag Editor
Amazon S3 > Buckets > aws-controltower-inspection-lambda > 2023/ > 08/ > 22/
22/
Copy S3 URI
Objects
Properties
Objects (1)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
auditreport
-
August 22, 2023, 17:24:19 (UTC+05:30)
144.0 B
Standard
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- After successful deployment, we get a AuditReport in DestinationBucket where parameters of DNS are added like below format

```
Account#, Hosted Zone ID, Record Set Name, IP Address,
```

Reference Link:

Repository: aws-samples/aws-control-tower-multi-account-inspection-lambda