

# Syntree 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

The screenshot shows the AWS CloudFormation console's 'Create stack' wizard. The left sidebar indicates the current step is 'Step 1: Create stack'. The main content area is divided into two sections: 'Prerequisite - Prepare template' and 'Specify template'. In the 'Prerequisite' section, the 'Template is ready' radio button is selected. In the 'Specify template' section, the 'Amazon S3 URL' radio button is selected. The 'Amazon S3 URL' text field contains the URL 'https://cf-templates-x4tkl28lqib4-us-east-2.s3.us-east-2.amazonaws.com/inspection-lambda/inspection.yaml'. Below this, the 'S3 URL' field is automatically populated with the same URL. A 'View in Designer' button is located to the right of the S3 URL field. At the bottom right of the wizard, there are 'Cancel' and 'Next' buttons.

### Step: 2

- Add parameters of CloudFormation Stack

**Specify stack details**

**Stack name**

Stack name

InspectionLambda

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**AssumeRole**

What role should be assumed in accounts to enable Inspector? The Default is AWSControlTowerExecution for a Control Tower environment.

AWSControlTowerExecution

**DestinationBucketName**

aws-controltower-inspection-lambda

**OrganizationId**

The Amazon Organizations ID for Control Tower.

o-6c7gdp2db

**S3Key**

The S3 Path to the Lambda Zip File

inspection-lambda/aws-inspection-lambda.zip

**S3SourceBucket**

Source S3 bucket

cf-templates-x4tk28lqb4-us-east-2

Cancel Previous Next

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

### Step: 3

**Step 2: Specify stack details**

**Stack name**

InspectionLambda

**Parameters (5)**

Key	Value
AssumeRole	AWSControlTowerExecution
DestinationBucketName	aws-controltower-inspection-lambda
OrganizationId	o-6c7gdp2db
S3Key	inspection-lambda/aws-inspection-lambda.zip
S3SourceBucket	cf-templates-x4tk28lqb4-us-east-2

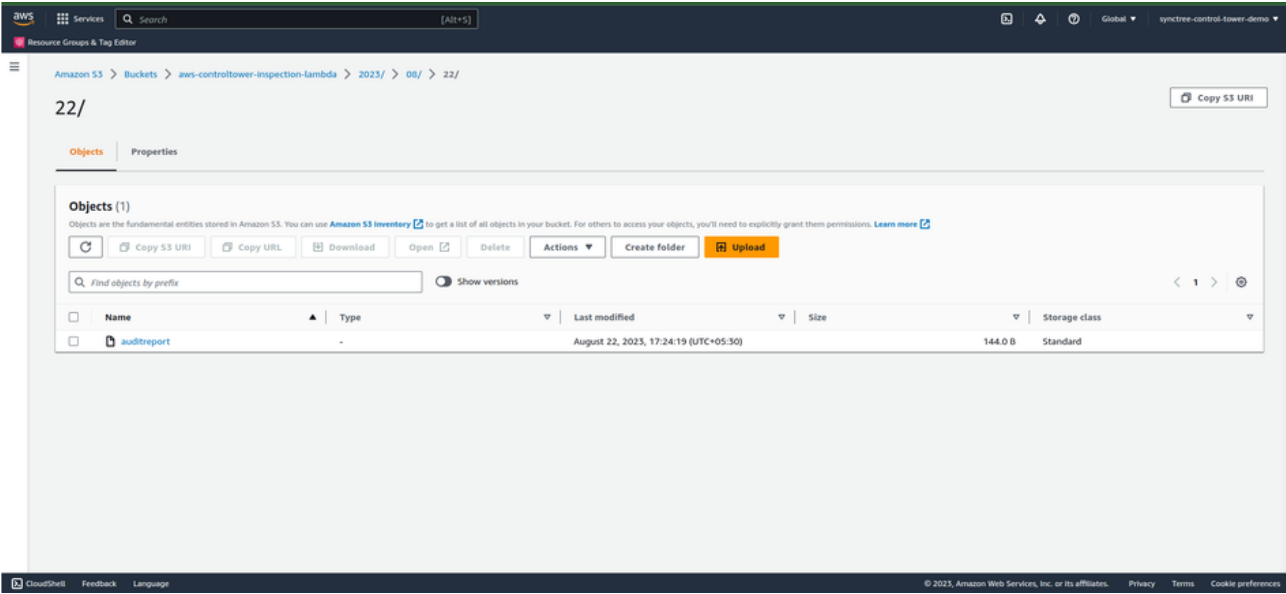
**Step 3: Configure stack options**

**Tags**

No tags

- Once reviewed parameters of stack & click on submit.

Step: 4



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

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

## Reference Link:

Repository: [aws-samples/aws-control-tower-multi-account-inspection-lambda](#)