

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

The screenshot shows the AWS CloudFormation console's 'Choose a template' page for creating a StackSet. The left sidebar shows a five-step process: Step 1 (Choose a template), Step 2 (Specify StackSet details), Step 3 (Configure StackSet options), Step 4 (Set deployment options), and Step 5 (Review). The main content area is titled 'Choose a template' and includes a 'Permissions' section with two options: 'Service-managed permissions' (unselected) and 'Self-service permissions' (selected). Below this, the 'IAM admin role ARN - optional' section shows a dropdown menu with 'AWSControlTowerStackSetRole' selected. A yellow warning box states: 'StackSets will use this role for administering your individual accounts.' The 'IAM execution role name' field is filled with 'AWSControlTowerExecution'. At the bottom, the 'Prerequisite - Prepare template' section is partially visible.

Step 3: Give the template file S3 URL.

Set deployment options

Step 4
Review

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready ☐ Use a sample template

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL, where it will be stored.

☒ Amazon S3 URL ☐ Upload a template file

Amazon S3 URL
`https://cf-templates-x4tk28liqb4-us-east-2.s3-us-east-2.amazonaws.com/inspector/inspector.yaml`

Amazon S3 template URL
S3 URL: `https://cf-templates-x4tk28liqb4-us-east-2.s3-us-east-2.amazonaws.com/inspector/inspector.yaml` [View in Designer](#)

Cancel [Next](#)

Step 4: Fill all the required parameters and select Next

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

ExcludedAccounts
Excluded Accounts list. This list should contain Management account, Log Archive and Audit accounts at the minimum.

`785825931796`

InspectorAuditAccountid
The AWS Account ID that will be configured as the Delegated Admin.

`785981945575`

OrganizationId
The Amazon Organizations ID for Control Tower.

`o-6c7qdp2db`

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

`AWSControlTowerExecution`

S3Key
The S3 Path to the Lambda Zip File

`inspector/inspector.zip`

S3SourceBucket
The S3 Bucket that contains the Lambda Zip File.

`cf-templates-x4tk28liqb4-us-east-2`

Cancel [Previous](#) [Next](#)

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

Set deployment options

Step 1
[Choose a template](#)

Step 2
[Specify StackSet details](#)

Step 3
[Configure StackSet options](#)

Step 4
Set deployment options

Step 5
Review

Add stacks to stack set

☒ Deploy new stacks ☐ Import stacks to stack set

Accounts
Identify specific accounts or an organisational unit whose accounts in which you want to modify stacks

Deployment locations
StackSets can be deployed into accounts or an organisational unit.

☒ Deploy stacks in accounts ☐ Deploy stack to all accounts in an organisational unit

Account numbers
Enter account numbers or populate from a file.

`80426606009`

12-digit account numbers separated by commas.

[Upload .csv file](#)

Specify regions

CloudShell Feedback

Step 6: Review all the details and select Submit

References

Repository: [aws-security-reference-architecture-examples](#) Python ★ 813 📄 200

