**This artefact contains the following:**

* A CloudFormation stack per config rule which creates:
  + An AWS Lambda function
  + AWS IAM roles for the Lambda function
* A CloudFormation stack that creates:
  + Lambda Layer that is linked to the Lambda function (python + yaml)
  + AWS Config rule

## Config Rules Description

|  |  |  |
| --- | --- | --- |
| **AWS Config Rule Name** | **Description** | **Outside Access** |
| 1. **Core-s3-policy-outside-access-disabled** | Checks the given resource policy for the S3 Bucket and ensures S3 Bucket is owned by the same account. | Cross account access, will assume organizations role to query AWS accounts within the specified OU and detect if there are any buckets outside of the given OU |

## Prerequisites

1. **AWS Organisations account (Master and Member accounts) – Organisation Unit ID**
2. **The master account should have an IAM role that allows cross account access (Attached) This IAM access policy should have the Lambda role for the config rule attached as part of the “Trust relationship” (Included in stack).**

## Solution Deployment Walkthrough

**In the Master AWS Organisations account do the following:**

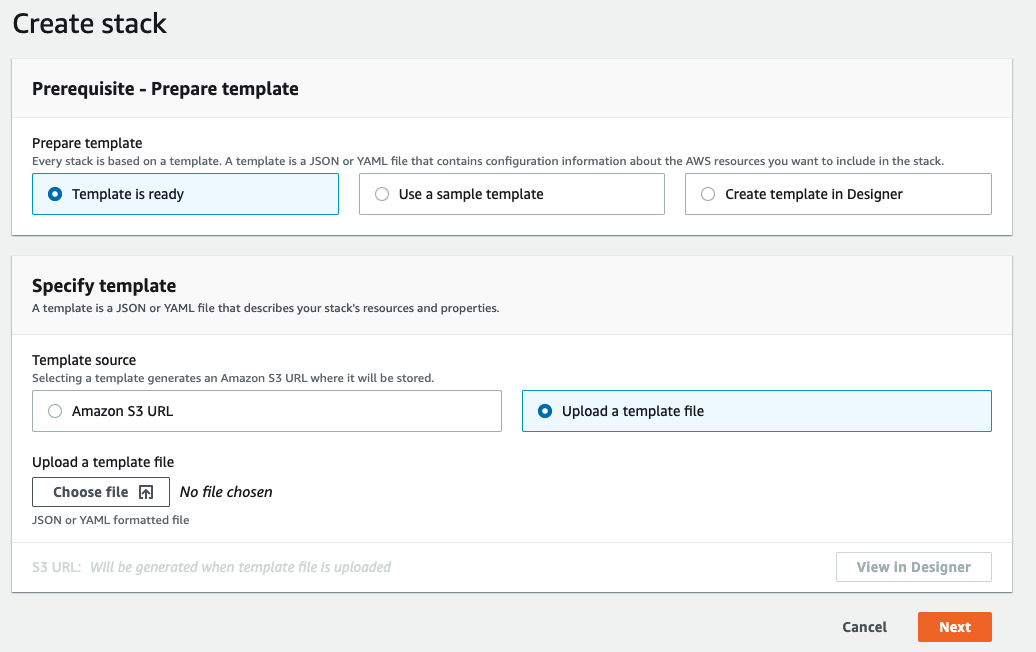
**Step 1)** Upload the cross-account-organisations IAM Role to your master AWS organisations account.

**In your member account do the following actions:**

**Step 1)** Upload the lambda layer python file to your Amazon S3 bucket and upload the yaml zip file to CloudFormation.

**Step 2**) Upload the lambda function of the config rule that you will deploy to your Amazon S3 bucket (python zip file).

**Step 3**) Go to the AWS CloudFormation Console, and select the region in which you will deploy the stack. Select on the “Create Stack” button and choose the .yaml file.

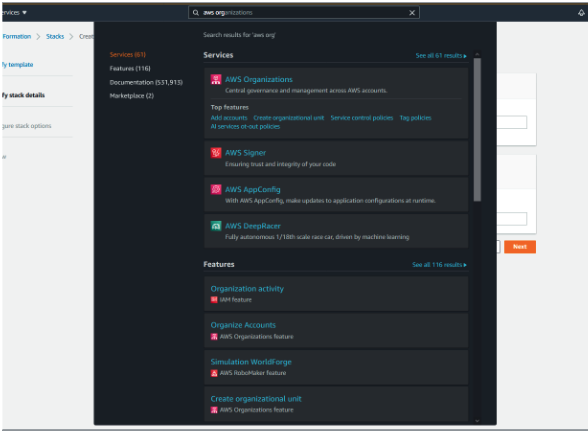
****

**Step 4**) Choose Next after selecting the file

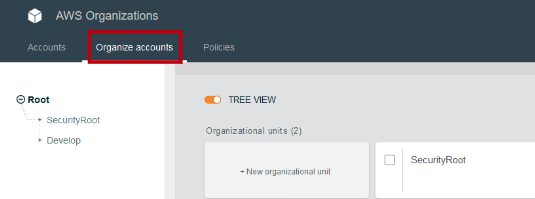
**Step 5**) Give a name to the stack and enter the appropriate parameters.

**To obtain the organisation ID, follow the next steps (Note: you can skip to step 4 if you already have the Organization OU ID):**

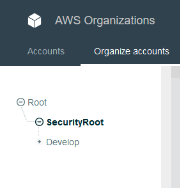
1. **Navigate to AWS Organizations**



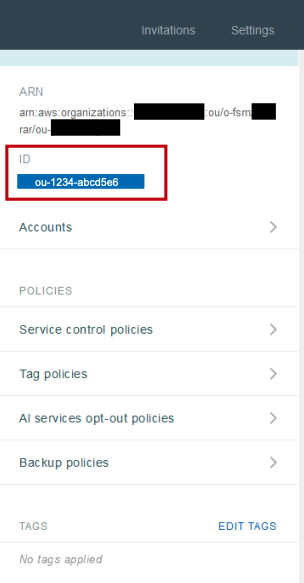
1. Navigate to organize accounts



1. From the left panel, select the organizational unit that you wish to deploy the config rule on.



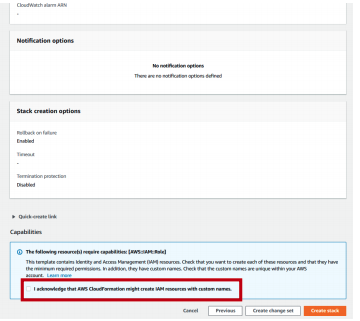
1. On the right side, a panel will display the Organization ID (The input required to for the environment variables in order for the stack to work).



**Step 7)** Input the organizational unit ID and press Next

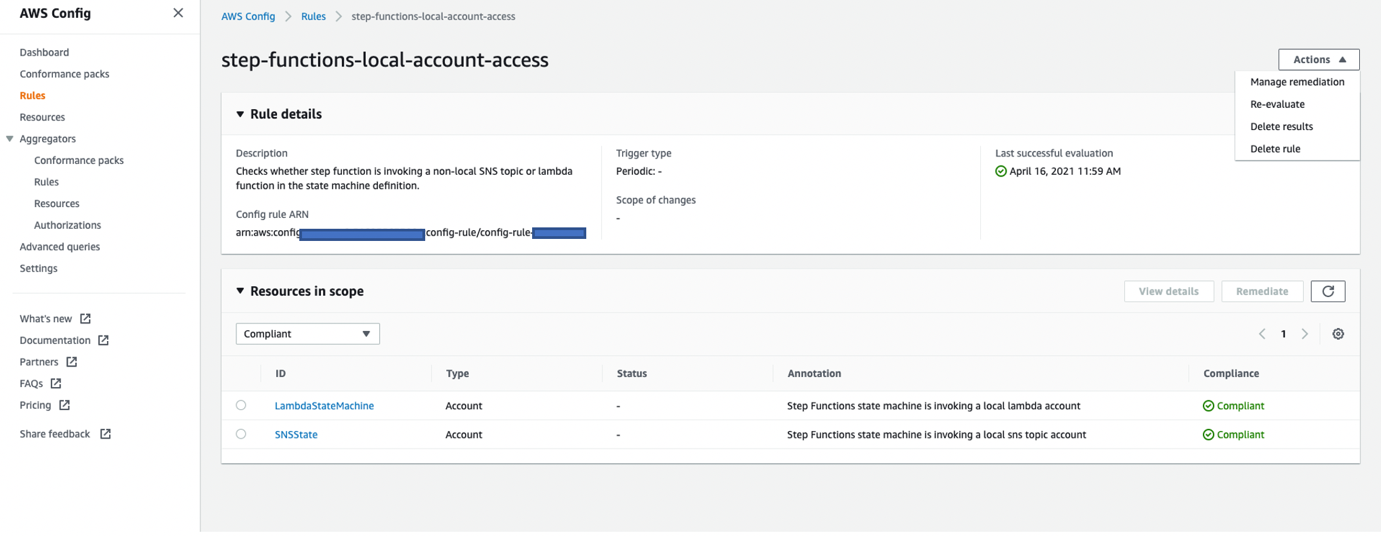
**Step 8**) If you require tagging, input the tagging information here and press Next, else proceed to Next first.

**Step 9)** Scroll down and accept the capabilities acknowledgement to allow AWS CloudFormation to create IAM resources with custom resources, and click “Create Stack”.



**Step 10)** After the stack is created, you will see the status: “CREATE\_COMPLETE” and this indicates that all the resources have been deployed correctly, with the Lambda function and Config rule automatically executed.

**Step 11**) Navigate to the CONFIG console, and you will see the latest evaluation of your resources (Unless empty). If not, then click the re-evaluate button to see the evaluation results.



**COMPLETE!**