Cloud Custodian Setup Guide

# Overview

This document provides a step-by-step guide to set up Cloud Custodian to automatically delete CloudFormation stacks based on an 'end\_time' tag and a scheduled invocation every five minutes.

# Prerequisites

**•** Python 3.7+ and pip  
**•** AWS CLI configured with appropriate credentials  
**•** An S3 bucket to stage Custodian policy code  
**•** IAM permissions to create IAM roles, Lambda functions, EventBridge rules, and S3 access

# Step 1: Install Cloud Custodian

Install Cloud Custodian using pip:  
```bash  
pip3 install c7n  
```

# Step 2: Configure AWS Credentials

Ensure your AWS CLI has a default region and credentials:  
```bash  
aws configure  
```

# Step 3: Define the Custodian Policy

Create a policy file `delete-by-end-time.yml` with the following content:

```yaml  
policies:  
 - name: cfn-delete-by-end-time  
 resource: cfn  
 description: >  
 Delete CFN stacks whose 'end\_time' tag has passed.  
 mode:  
 type: periodic  
 schedule: "rate(5 minutes)"  
 role: arn:aws:iam::123456789012:role/CustodianLambdaRole  
 filters:  
 - type: value  
 key: "tag:end\_time"  
 value\_type: age  
 op: ge  
 value: 0  
 actions:  
 - type: set-protection  
 state: False  
 - type: delete  
```

# Step 4: Create the IAM Execution Role

Create a role `CustodianLambdaRole` with trust and permissions policies:  
1. Trust policy (trust-policy.json)  
2. Permissions policy (permissions-policy.json)  
3. AWS CLI commands:  
```bash  
aws iam create-role --role-name CustodianLambdaRole --assume-role-policy-document file://trust-policy.json  
aws iam attach-role-policy --role-name CustodianLambdaRole --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole  
aws iam put-role-policy --role-name CustodianLambdaRole --policy-name CustodianStackPolicy --policy-document file://permissions-policy.json  
```

# Step 5: Prepare the S3 Bucket

Ensure the S3 bucket exists or create it:  
```bash  
aws s3 ls s3://my-custodian-bucket || aws s3 mb s3://my-custodian-bucket  
```

# Step 6: Deploy the Policy

Deploy the policy as a scheduled Lambda:  
```bash  
custodian run --region us-east-1 -s s3://my-custodian-bucket policies/delete-by-end-time.yml  
```

# Step 7: Verify Deployment

• Check the Lambda function in the AWS Console (name: custodian-cfn-delete-by-end-time)  
• Confirm the EventBridge rule is scheduled for every 5 minutes  
• Monitor CloudWatch Logs under `/aws/lambda/custodian-cfn-delete-by-end-time`