Synctree Flosports | AWS WebHook

WebHook allows us to receive notifications on mail, slack, phone, etc.

This CDK package installs a Lambda function with an associated IAM role and subscribes the Lambda function to Control Tower aggregate security notifications. In the event of a Control Tower rule violation (e.g. publicly accessible S3 bucket), Lambda sends a notification to a webhook.

SNS topics and notifications you can receive

- The `aws-controltower-AllConfigNotifications` topic:

  It receives notifications from AWS Config regarding compliance, noncompliance, and change. It also receives notification from AWS CloudTrail on log file delivery.
- The `aws-controltower-SecurityNotifications` topic:

  One of these topics exists for each supported AWS Region. It receives compliance, noncompliance, and change notifications from AWS Config in that Region. It forwards all incoming notifications to `aws-controltower-AggregateSecurityNotifications`
- The `aws-controltower-AggregateSecurityNotifications` topic:

  This topic exists in each supported AWS Region. It receives compliance change notifications from the region-specific `aws-controltower-SecurityNotifications` topics. Additionally, in the home Region, it also receives drift notifications.

Prerequisites

- Admin access to the organization. This is used to assume the control tower role in the audit account
- AWS CDK installed
- Version 2 or above of the AWS CLI, Install CLI
- You should examine your system's dependencies if you encounter any errors during deployment using the CLI.

Let’s start deploying

To enable the notifications on a MAC or Linux, run the `install.sh` script as an administrative user. The script takes 3 parameters;

- The AWS audit account number
- The webhook URL notifications will be posted too (slack or can be other).
- Optional name of Guardrail configRuleName(s) you want notification for separate multiple rules with commas, Use ALL_RULES for notification of all Guardrails.

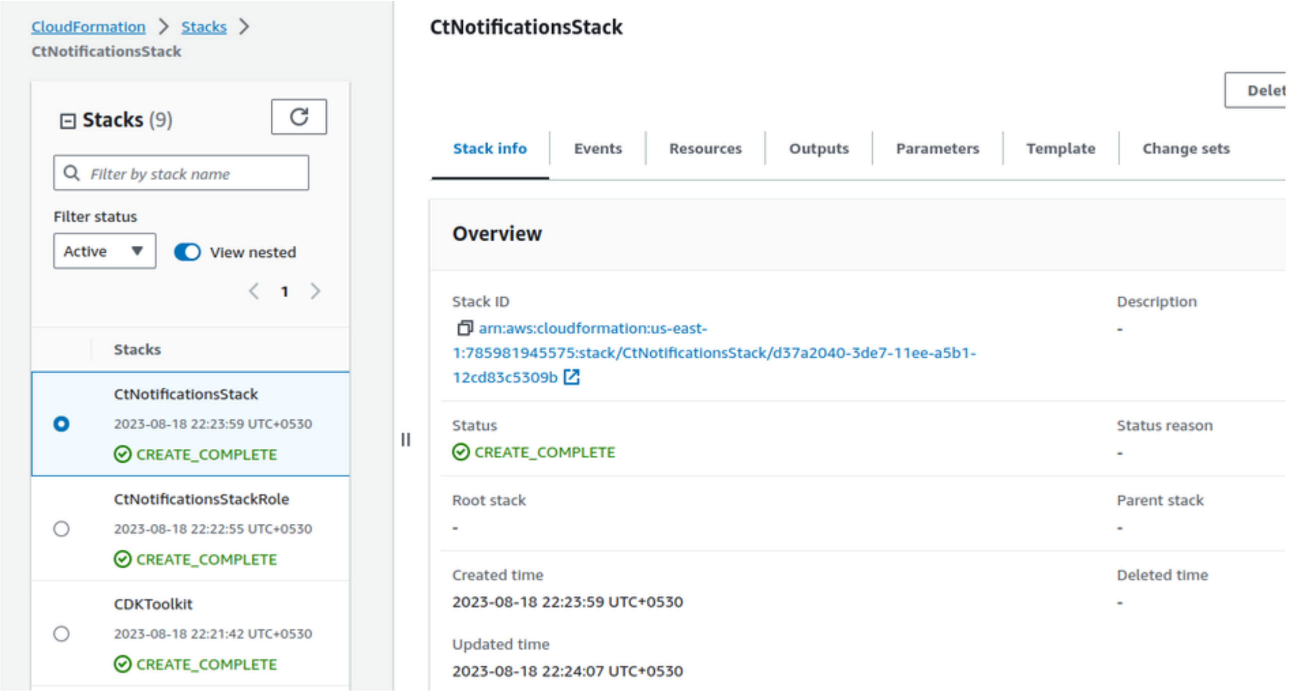
Follow steps to deploy:

- Clone repository of code.
- Run the following command:

```
bash install.sh 12345678902 https://mywebhookURL ALL_RULES
```

Add your Audit account number and your Webhook URL where you want notifications.

Finally created stacks in CloudFormation.



CloudFormation > Stacks > CtNotificationsStack

Stacks (9)

Filter by stack name

Filter status

Active ▼ View nested

Stacks
● CtNotificationsStack 2023-08-18 22:23:59 UTC+0530 CREATE_COMPLETE
○ CtNotificationsStackRole 2023-08-18 22:22:55 UTC+0530 CREATE_COMPLETE
○ CDKToolkit 2023-08-18 22:21:42 UTC+0530 CREATE_COMPLETE

CtNotificationsStack

Overview

Stack ID
arn:aws:cloudformation:us-east-1:785981945575:stack/CtNotificationsStack/d37a2040-3de7-11ee-a5b1-12cd83c5309b

Description
-

Status
CREATE_COMPLETE

Status reason
-

Root stack
-

Parent stack
-

Created time
2023-08-18 22:23:59 UTC+0530

Deleted time
-

Updated time
2023-08-18 22:24:07 UTC+0530

Reference Link:

Repository: aws-samples/aws-control-tower-webhook-notifications