Emons,Joep J.G.J.

[Bedrijfsnaam]  [Bedrijfsadres]

SNO week 15

Inhoud

[Overview 2](#_Toc200573360)

[What I implemented 2](#_Toc200573361)

[1. CloudTrail Setup 2](#_Toc200573362)

[2. CloudWatch alarm 2](#_Toc200573363)

[3. Athena Analysis 4](#_Toc200573364)

[4. CloudWatch insights 4](#_Toc200573365)

[Key findings 5](#_Toc200573366)

[Security Events Captured 5](#_Toc200573367)

[System health 5](#_Toc200573368)

[Conclusion 6](#_Toc200573369)

# Overview

This document will show how I implemented CloudTrail in our case study project. I’m using CloudTrail to monitor our vector database system. This system uses multiple AWS tools. We use API gateway, Lambda, Step Functions, and ECS containers running different vector databases

# What I implemented

## CloudTrail Setup

I created a CloudTrail named vectordb-trail, which captures all the logs and puts them in an S3 bucket. I enabled the CloudWatch logs integration. All of this results in capturing all AWS API Calls

Afbeelding met tekst, schermopname, Lettertype, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.

## CloudWatch alarm

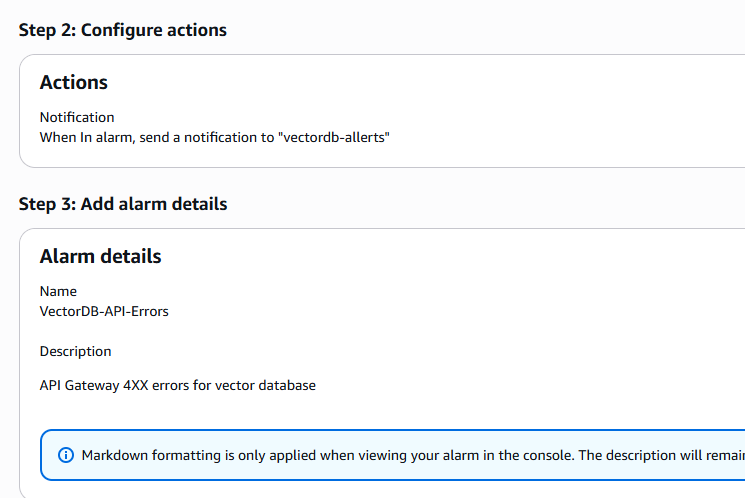
I set up 4 alarms, they are

1. **Api gateway errors**: this system monitors api failures with a threshold of greater than 5 in 5 minutes
2. **Lambda Errors:** this system monitors the ValidateVectorDBInputs function failures with a threshold of greater than 2 in 5 minutes
3. **Step Function Deploy Failures:** this system monitors deployment state-machine failures with a threshold of greater than 1 in 15 minutes
4. **Step function cleanup failures:** this system monitors cleanup state-machine failures with a threshold of greater than 1 in 15 minutes

Afbeelding met tekst, schermopname, Lettertype, lijn

Door AI gegenereerde inhoud is mogelijk onjuist.  
Here you can see all alarms, and also that only 1 is okay because the other 3 haven't had sufficient data yet to get an ok. This means not a lot of errors have happened, so this is a good thing

All of these alarms are connected to sns that I created for this.



## Athena Analysis

In Athena, I created a database (vectordb\_analysis). In this database, I created a table (cloudtrail\_logs) pointing to an S3 bucket with cloudtrail data. After running queries that you can find later in the document, I found 6-7 CloudTrail events showing real AWS activity. The services that I captured were: KMS, IAM, and STS operations.

The main query I used to see if it works was this.

Afbeelding met tekst, Lettertype, lijn, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.

Result

Afbeelding met tekst, Lettertype, schermopname

Door AI gegenereerde inhoud is mogelijk onjuist.

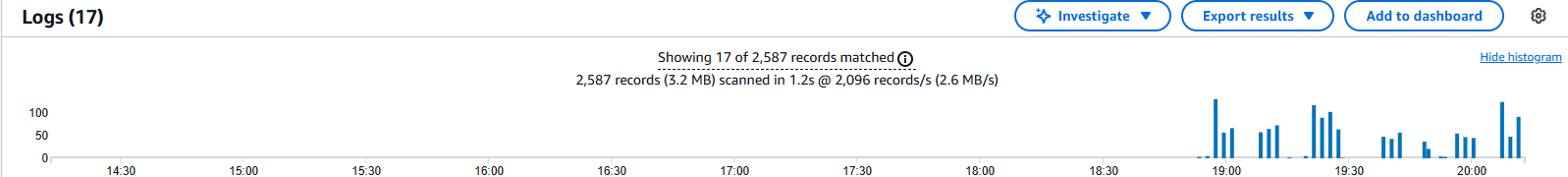
From this, we can gather that we are capturing information, and we can see IAM, KMS, and STS services being captured.

## CloudWatch insights

* Analyzed cloudtrail logs in real-time
* The total records that were processed were: 1285 events
* These were found over server hours of activity
* The peak activity was 238 events in 5 minutes

Queries used

Afbeelding met tekst, Lettertype, lijn, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.This query shows a timeline analysis that found 1285 records with activity.

Afbeelding met tekst, Lettertype, lijn, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.Afbeelding met tekst, schermopname, Lettertype, lijn

Door AI gegenereerde inhoud is mogelijk onjuist.  
shows 5 recent events  
Afbeelding met tekst, Lettertype, lijn, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.  
Afbeelding met tekst, Lettertype, lijn, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.  
shows IAM user activity

# Key findings

## Security Events Captured

* **IAM user activities:** multiple login events for my user, of course
* **Service activites:** ECS task definitions operating, and also STS role assumptions, so basically security tokens
* **AWS Service Calls:** KMS is being used, so the keys we created are being used or deleted

## System health

When checking for errors or unauthorized access attempts, or api gateway attacks, nothing was detected/found. I just found normal activities. This is a good thing; our systems are working and secure.

# Conclusion

The CloudTrail monitoring system is up and running. This system is providing us with a great way to monitor our vector database system. CloudTrail is showing us all api activity, alerting us of errors in the system, we can analyze with Athena and CloudWatch. Cloudtrail is successfully monitoring the entire system providing security oversight needed for a production system