Security Monitoring System with AWS

Introducing the Project!

In this project, I will demonstrate how to set up a monitoring system in AWS using CloudTrail, CloudWatch and SNS! I'm doing this project to learn how security and monitoring services in AWS work, plus have a working system that actually send us emails too

Tools and concepts

Services I used were CloudTrail, CloudWatch and SNS. I also used Secrets Manager, IAM (roles) and S3 buckets. Key concepts I learnt include secret storing, CloudWatch vs CloudTrail, what are notifications and different kinds of endpoints, how to create a CloudWatch and alarm.

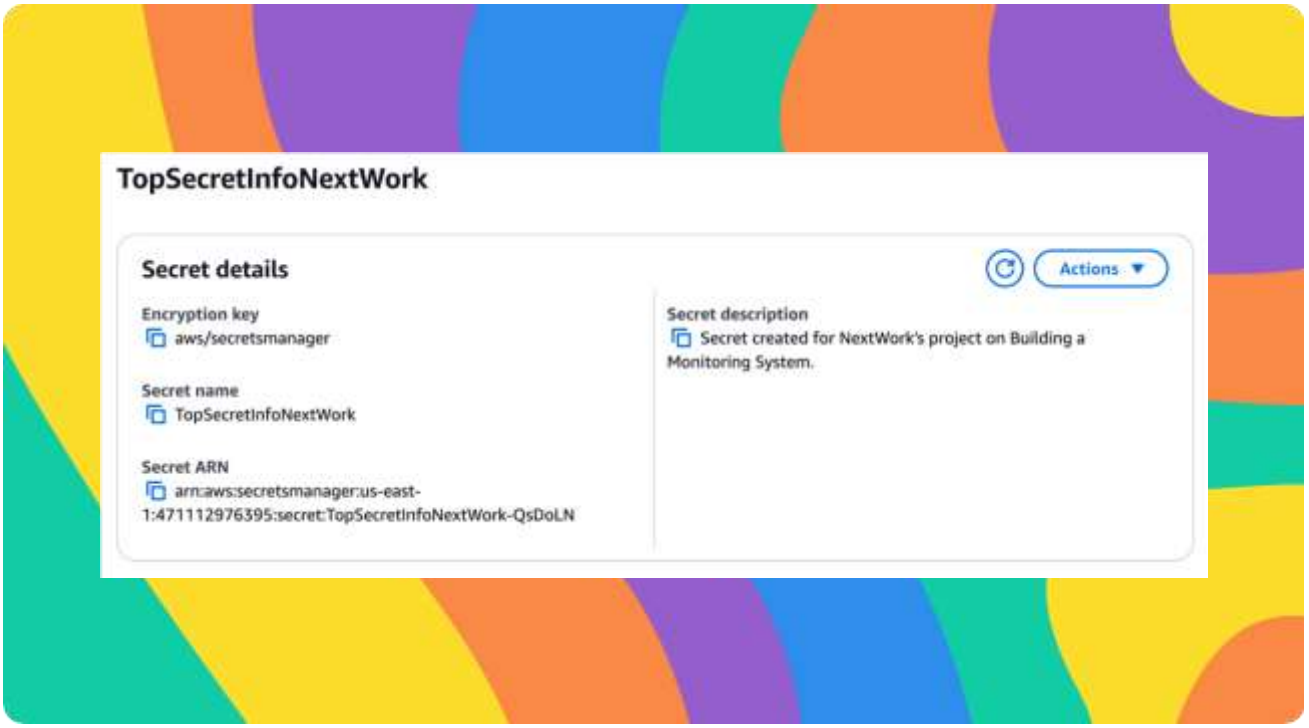
Project reflection

This project took me just under 5 hours. The most challenging part was to troubleshooting why the email wasn't delivering in our first test - it would be frustruating when an error is happening but there are no 'error logs' or error messages. It was most rewarding to compare CloudTrail SNS notifications - it really opened up my mind around WHY I had to use CloudWatch and alarms too.

Create a Secret

Secrets Manager is AWS' security service for storing secrets i.e. database credentials, account IDs, API keys... anything that is sensitive information that would cause damage/trouble if it got leaked and shouldn't be lying around in code.

To set up for my project, I created a secret called TopSecretInfo in SecretsManager. This secret is a string that contains a hot take from me... I mentioned that I need 3 coffees a day to function.



Set Up CloudTrail

CloudTrail is a monitoring service - it's used to track events and acitivities in my AWS account. These logs are very helpful for security (i.e. detecting suspicious activity), compliance (i.e. proving that you're following the rules for something), and troubleshooting (i.e. identifying what happened/changed if something breaks).

CloudTrail events include types like management, data, insights and network activity events. In this project, I set up my trail to track Management events because accessing a secert falls into that category. It is not a data event (which captures high volume actions performed on resources) because all management events are free to track (and AWS lets us track security operations like this for free)!

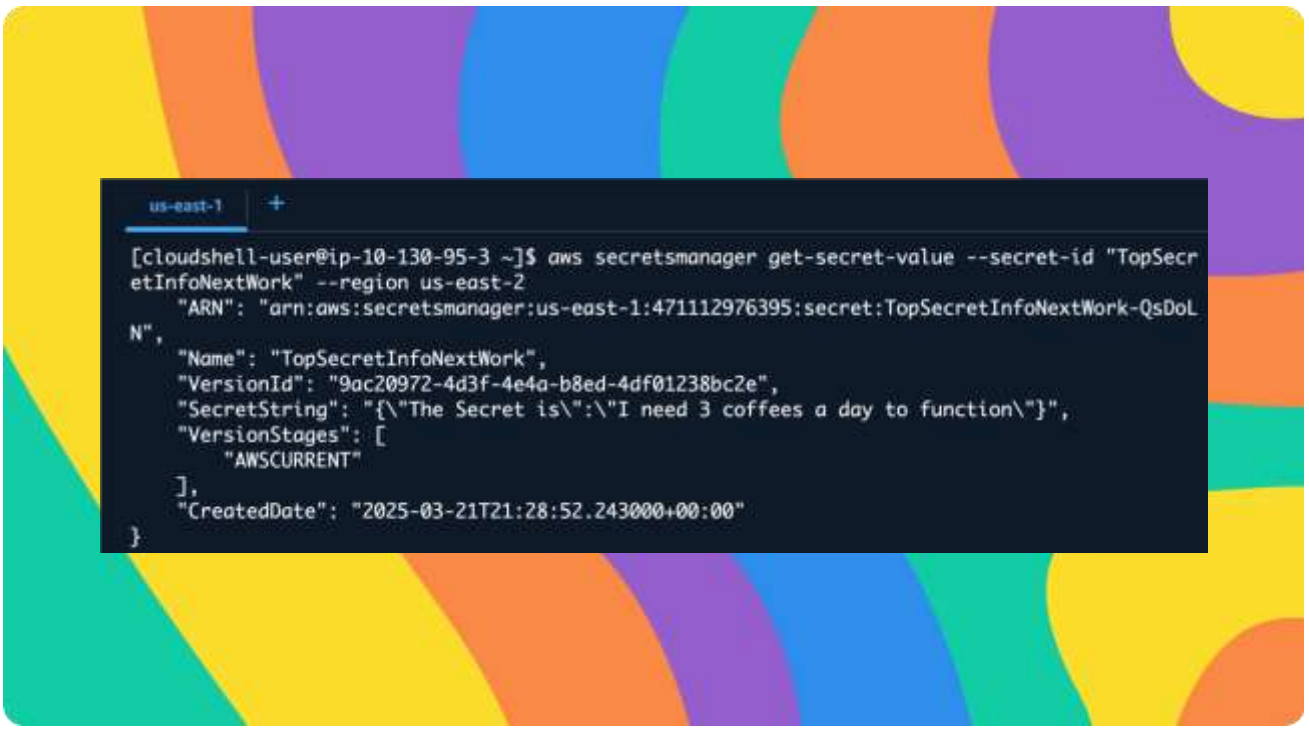
Read vs Write Activity

Read API activity involves accessing, reading, opening a resource. Write API activity involves creating, deleting, updating a resource. For this project, I ticked both to learn about both types of activities, but I really only need the Write acitivty (accessing a secret is considered a Write activity because of its importance)

Verifying CloudTrail

I retrieved my secret in two ways: First through the Secrets Manager console, where I could easily just select a "Retrieve secrets value" button. Second way was using the AWS CLI i.e. running a get-secret-value in CloudShell.

To analyze our CloudTrail events i.e. see the event where I got my secret's value, I visited the Event history in CloudTrail. I found that there was a GetSecretValue event tracked regardless of whether I did it over the CLI or over the console. This tells me that CloudTrail can definitely see and track when I open our Secrets Manager key.

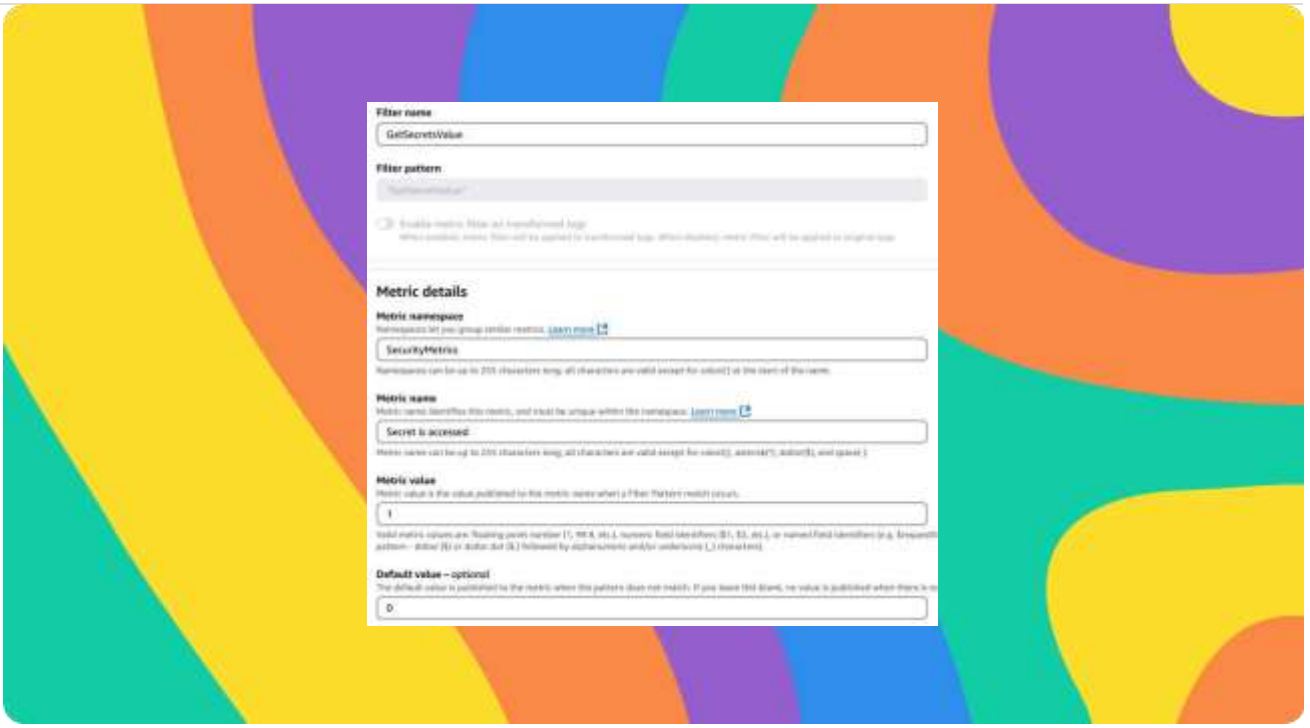


CloudWatch Metrics

CloudWatch Logs is a monitoring service that brings together logs from other AWS services (including CloudTrail) to help us analyze and create alarms for. It's important for monitoring because you get to create insights and get alerted based on events that happen in your account.

CloudTrail's Event History is useful for quickly reading (management) events that happened in the last 90 days, while CloudWatch Logs are better for combining and analysing logs from different sources, accessing logs for longer than 90 days, and advaced filtering.

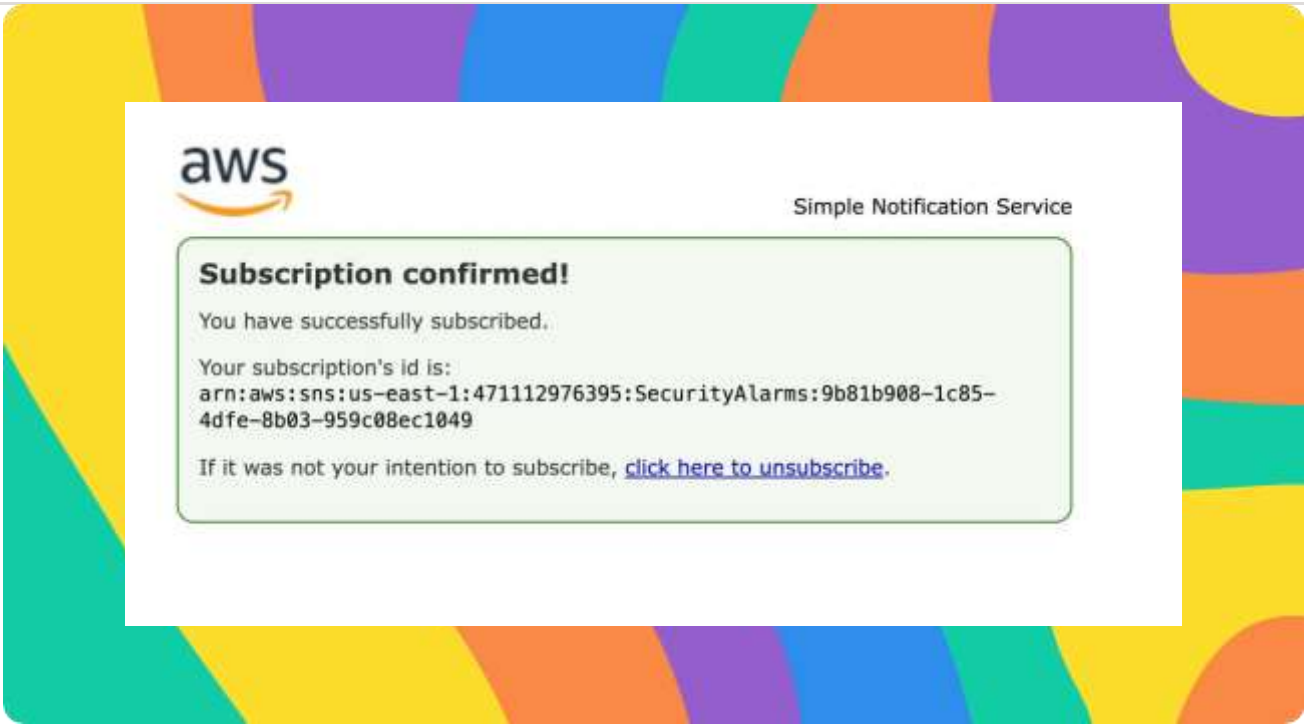
A CloudWatch metric is a specific way that I count or track events that are in a log group. When setting up a metric, the metric value represents how I increment or 'count' an event when it passes our filters (in our case, I want to increment our metric value by 1 whenever our secret is accessed). Default value is used when the event that we're tracking does not occur!



CloudWatch Alarm

A CloudWatch alarm is a feature and alert system in CloudWatch that's designed to "go off" i.e. indicate when certain conditions have been met in our log group. I set my CloudWatch alarm threshold to be about how many times the GetSecretValue event happens in a 5 minute period so the alarm will trigger when the average number of times is above 1.
I created an SNS topic along the way. An SNS topic is like a newsletter/broadcast channel that emails, phone numbers, functions, apps can subscribe to (so they get notified when SNS has a new update to share) Our SNS topic is set up to send us an email when our secret gets accessed.

AWS requires email confirmation because it would not automatically start emailing addresses that I subscribe to an SNS topic. This helps prevent any unwanted subscriptions for recipicients (i.e. people who are receiving those emails).



Troubleshooting Notification Errors

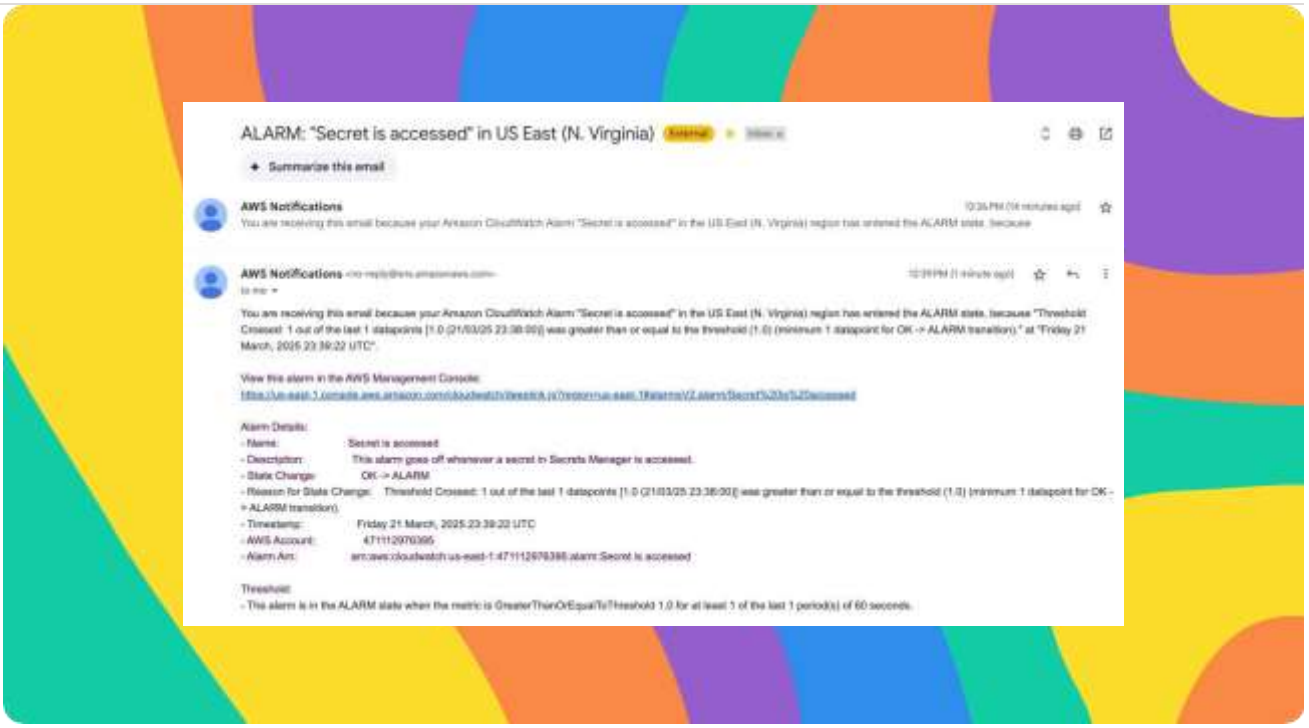
To test my monitoring system, I opened and accessed my secret again! The results weren't successful - I didn't get any emails/notifications about our secret getting accessed!

When troubleshooting the notification issues, I investigated every single part of my monitoring system - whether CloudTrail is picking up on events that are happening when I access our secret, whether CloudTrail is sending logs to CloudWatch, whether the filter is accidentally rejecting the correct events, whether the alarm gets triggered, whether the triggering the alarm sends an email.

I initially didn't receive an email because CloudWatch was configured to use the wrong threshold - instead of calculating the AVERAGE number of times a secret was accessed in a time period, it should've been the SUM!

Success!

To validate that my monitoring system can successfully detect and alert when my secret is accessed, I checked my secret's value one more time. I received an email within 1-2 minutes of the event! My alarm in CloudWatch is also in "In alarm" state.



Comparing CloudWatch with CloudTrail Notifications

In a project extension, I enabled SNS notification delivery in CloudTrail because this lets me evaluate CloudTrail vs CloudWatch for notifying us about events like our secert getting access.

After enabling CloudTrail SNS notifications, my inbox was very quickly filled with new emails from SNS (as it was notified by CloudTrail). In terms of the usefulness of these emails, I thought that we're receiving LOTS (it's a little overwhelming) and the logs themselves don't show what happened in terms of management events that ocurred. I only see that new logs have been stored in our bucket.

Contact Information

Name: Rakesh J

Email: rakeshj.woks@gmail.com

Phone: +91 7090466131

LinkedIn: https://www.linkedin.com/in/rakesh-jayanna-215a3728b/

GitHub: https://github.com/rakeshjayanna/Security-Monitoring-System