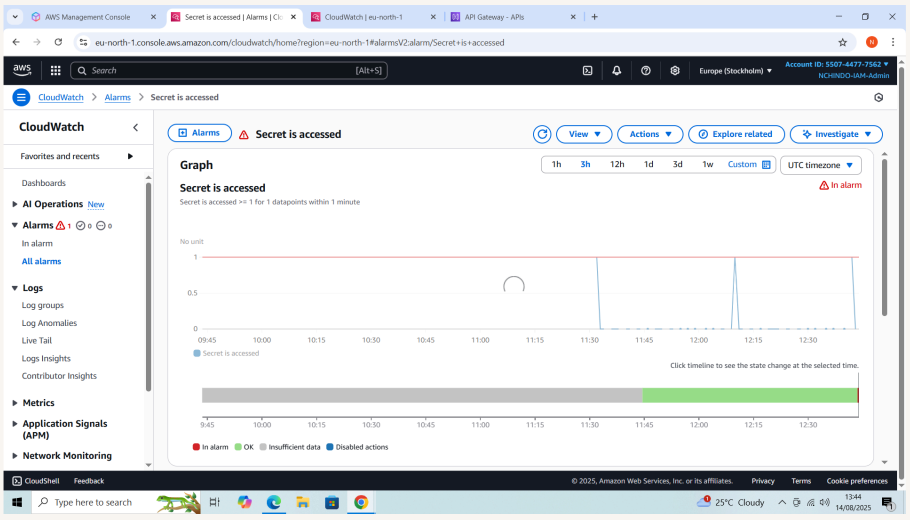
nextwork.org

Build a Security Monitoring System

Nchindo Boris



Introducing Today's Project!

In this project, I will; - Set up AWS CloudTrail to track secret access events. - Use AWS CloudWatch to log access attempts and trigger notifications. - Create SNS alerts to get notified when my secrets are accessed.

Tools and concepts

Services I used were; - AWS Secrets Manager - AWS CloudTrail - Amazon CloudWatch - Amazon SNS - Amazon S3 - AWS CLI Key concepts I learnt include; - Securely store and manage secrets using AWS Secrets Manager. - Monitor secret access by enabling AWS CloudTrail logging. - Investigate security events in CloudTrail Event History and S3 logs. - Create CloudWatch Metric Filters to track secret access events. - Set up CloudWatch Alarms and SNS notifications for real-time security alerts

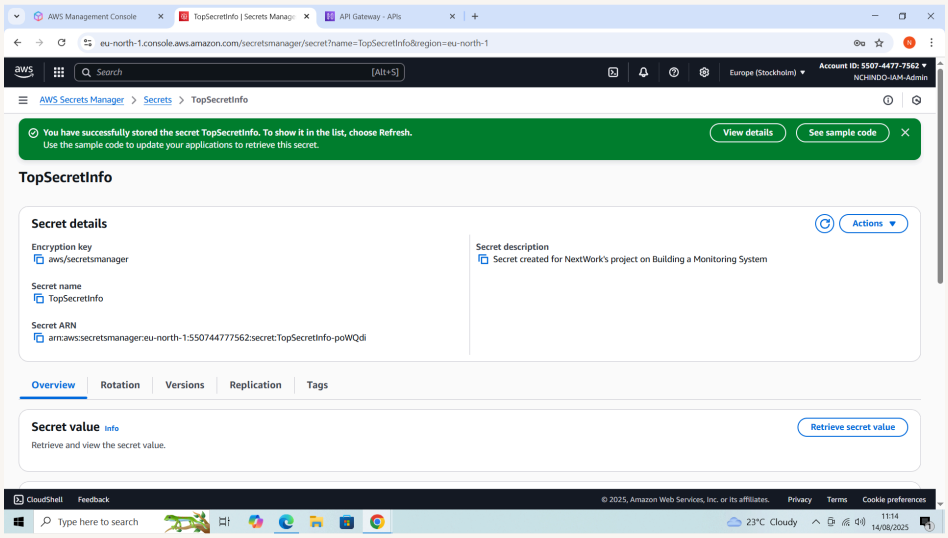
Project reflection

This project took me approximately 2 hours 45 minutes The most challenging part was troubleshooting after not receiving the email It was most rewarding to receive the email from AWS Notifications with the subject ALARM: "SecretIsAccessedAlarm"

Create a Secret

Secrets Manager is an AWS service which helps you protect secrets, which are passwords, API keys, credentials and sensitive information.

To set up for my project, I created a secret called TopSecretInfo that contains a key/value pair of my secret



Set Up CloudTrail

CloudTrail is a monitoring service - think of it as an activity recorder throughout your AWS account. It documents every action taken, like who did what, when they did it, and where they did it from. I set up a trail to tell CloudTrail exactly what activity to record and where to save those recordings.

CloudTrail events include types like; management events, data events, insight events and Network activity events

Read vs Write Activity

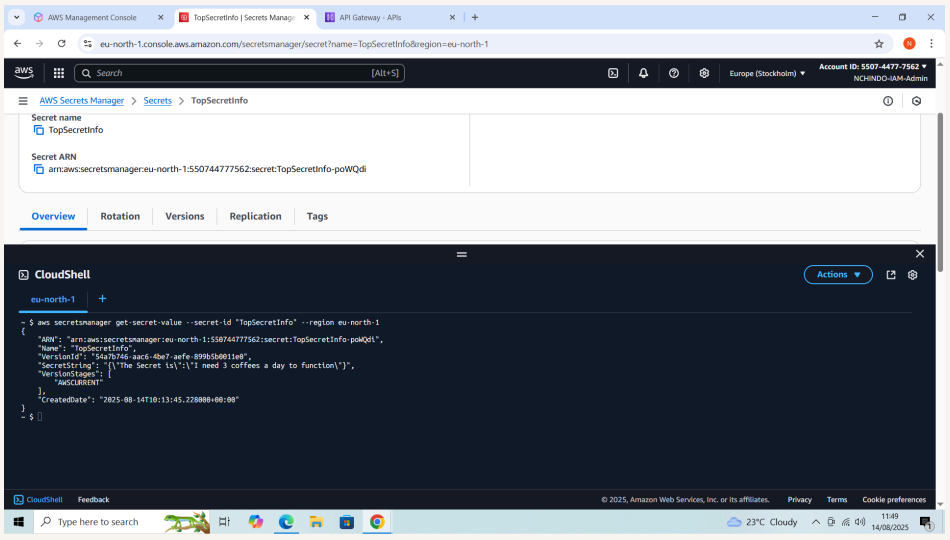
Read API activity happens when someone views but doesn't change anything. For example, listing your S3 buckets, describing your EC2 instances, or in our project, viewing (but not changing) metadata about a secret. Write API activity involves occurs when changes happen - creating, deleting, modifying resources, or even retrieving the value of a secret (which is what we want to monitor) so for this project, we need Write API

Nchindo Boris
NextWork Student

Verifying CloudTrail

I retrieved the secret in two ways: First through the console. Second using the command aws secretsmanager get-secret-value --secret-id "TopSecretInfo" --region eu-north-1 with AWS CLI

To analyze my CloudTrail events, I visited the events history page in cloudtrail, Under Lookup attributes, selected the dropdown and choose Event source. Next, In the search bar close to Event source, entered secretsmanager.amazonaws.com to check for an event called GetSecretValue I found the event - GetSecretValue; This tells me my secret's value was retrieved or used



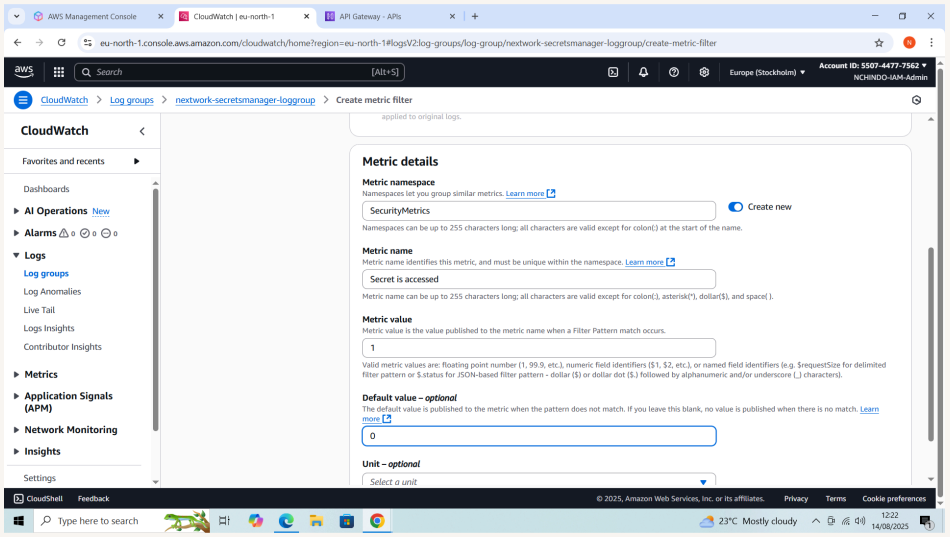
CloudWatch Metrics

CloudWatch Logs is a service that helps you bring together your logs from different AWS services, including CloudTrail, for visibility, troubleshooting, and analysis. It's important for monitoring because once your logs are in CloudWatch, you can create alerts based on specific patterns (such as someone accessing your secret), visualize trends, or trigger automated responses.

CloudTrail's Event History is useful for keeping events for 90 days, while CloudWatch Logs can store them for as long as you'd like. Also, CloudWatch Logs are better for setting up alerts and automated responses when specific events happen

A CloudWatch metric is a time-ordered set of data points that represent the performance or behavior of a system or application in AWS When setting up a metric, the metric value represents what gets recorded when our filter spots a match in the logs. We're setting it to 1 so that each time someone accesses our secret, the counter increases by exactly one. Default value is used when our filter doesn't find any matches during a given time period. We're setting it to 0 so that time periods with no secret access show up as zero on our charts, rather than not showing up at all. This gives us a complete picture - we can see both when access happened AND when it didn't.

Nchindo Boris
NextWork Student

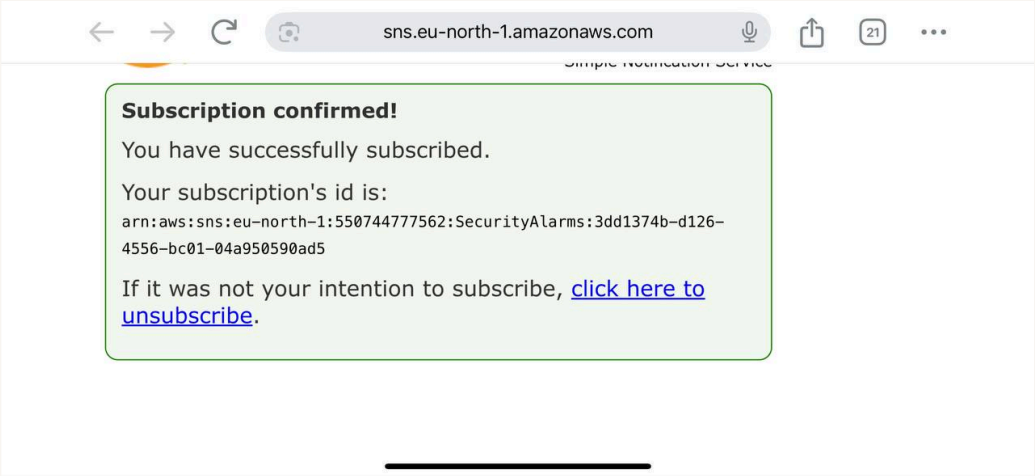


CloudWatch Alarm

A CloudWatch alarm is a feature in Amazon CloudWatch that monitors metrics and performs automated actions when certain thresholds are met. I set my CloudWatch alarm threshold to static threshold so the alarm will trigger when the SecretIsAccessed metric is greater than or equal to 1 in a 5-minute period.

I created an SNS topic along the way. An SNS topic is like a broadcast channel for your notifications. First, you create the channel (topic), then you invite subscribers (such as your email), and finally, you send messages to the topic. My SNS topic is set up to SecurityAlarms

AWS requires email confirmation because they want to make sure it's really you asking for these alerts.


sns.eu-north-1.amazonaws.com
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:eu-north-1:550744777562:SecurityAlarms:3dd1374b-d126-4556-bc01-04a950590ad5
If it was not your intention to subscribe, click here to unsubscribe.

Nchindo Boris
NextWork Student

Troubleshooting Notification Errors

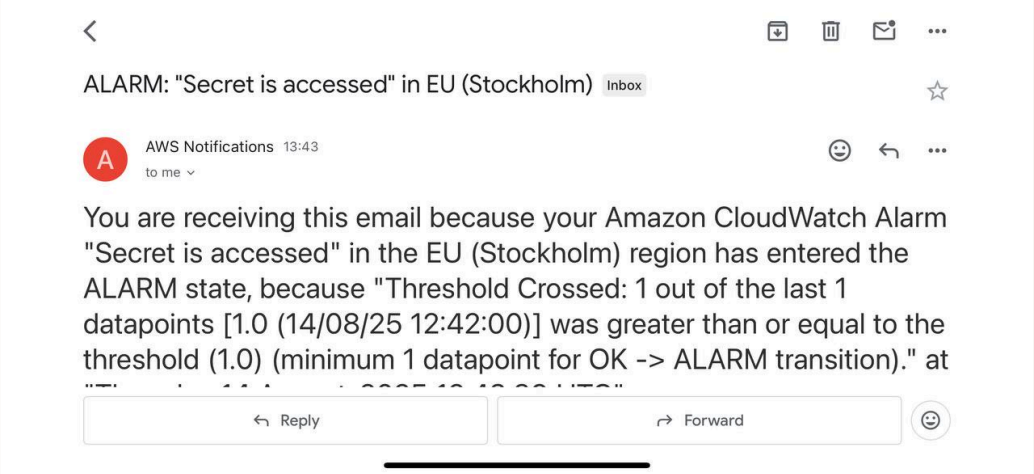
To test my monitoring system, I Selected Retrieve secret value from my secret in the Secrets Manager console. I did not receive any email notification for that

When troubleshooting the notification issues I checked if; - CloudTrail did capture the event! - CloudTrail isn't sending Logs to CloudWatch - Something went wrong with the CloudWatch metric filter - CloudWatch alarm isn't getting triggered properly - SNS is actually set up properly

I initially didn't receive an email before because CloudWatch alarm wasn't getting triggered properly. The key solution was to; Adjust my Alarm Settings as follows; - On the alarm details page, look at the Statistic field. - Statistic should be set to Sum, not Average or any other statistic! This is crucial because: Sum adds up all occurrences of secret access in the period (what we want). Average would calculate an average rate (i.e. the average number of times the secret was accessed per second over the 5 minute period), which might never cross the threshold. I also updated the Period from 5 minutes to 1 minute, so I can trigger the alarm even faster when I see the Secret's value.

Success!

To validate that your monitoring system works; - I accessed my Secret Again - I checked and refreshed my Secret is accessed alarm in the CloudWatch console to put it to be in the In alarm state! - I received email from AWS Notifications with the subject ALARM: "SecretIsAccessedAlarm".



The place to learn & showcase your skills

Check out nextwork.org for more projects