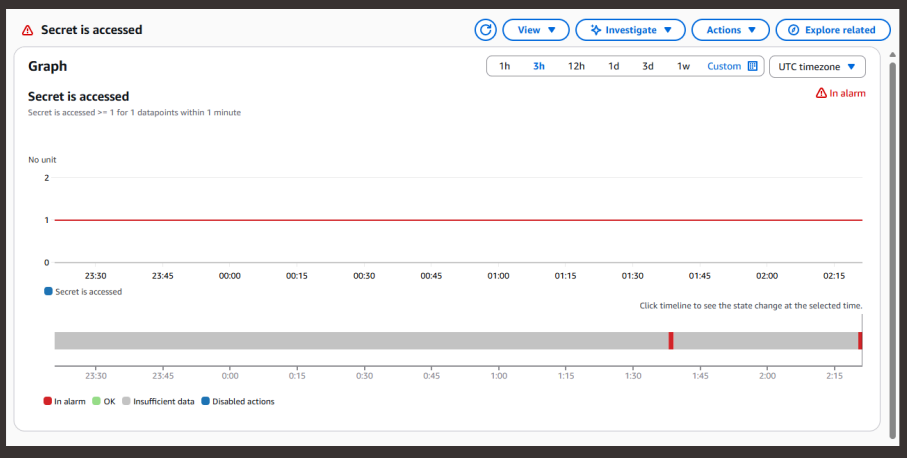
nextwork.org

Build a Security Monitoring System

ME Melvin J Bonner



ME
Melvin J Bonner
NextWork Student

Introducing Today's Project!

In this project, I will be building my own powerful monitoring system using AWS. I'm doing this project to learn how to use Secrets Manager and configure an alarm using CloudWatch. I will be using SNS to send me an email when my secret has been accessed.

Tools and concepts

The services I used were CloudTrail, S3, CloudWatch, Secrets Manager, and SNS. Key concepts I learned include, log delivery, metric filter, and alarm configuration.

Project reflection

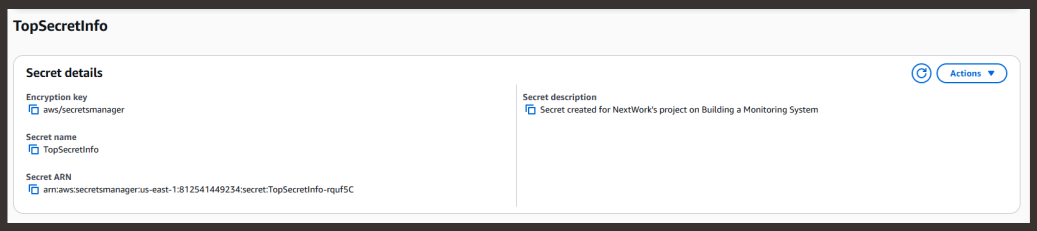
This project took me approximately 3 hours to complete.

ME
Melvin J Bonner
NextWork Student

Create a Secret

Secrets Manager helps you protect secrets, which are passwords, API keys, credentials and sensitive information. You could use Secrets Manager to keep database passwords, API keys, and other sensitive information

To set up for my project, I created a secret called TopSecretInfo that contains a key and a value.



ME
Melvin J Bonner
NextWork Student

Set Up CloudTrail

CloudTrail is monitoring service that records activity throughout my account.

CloudTrail events include types like management events, data events, insight events, and network activity events.

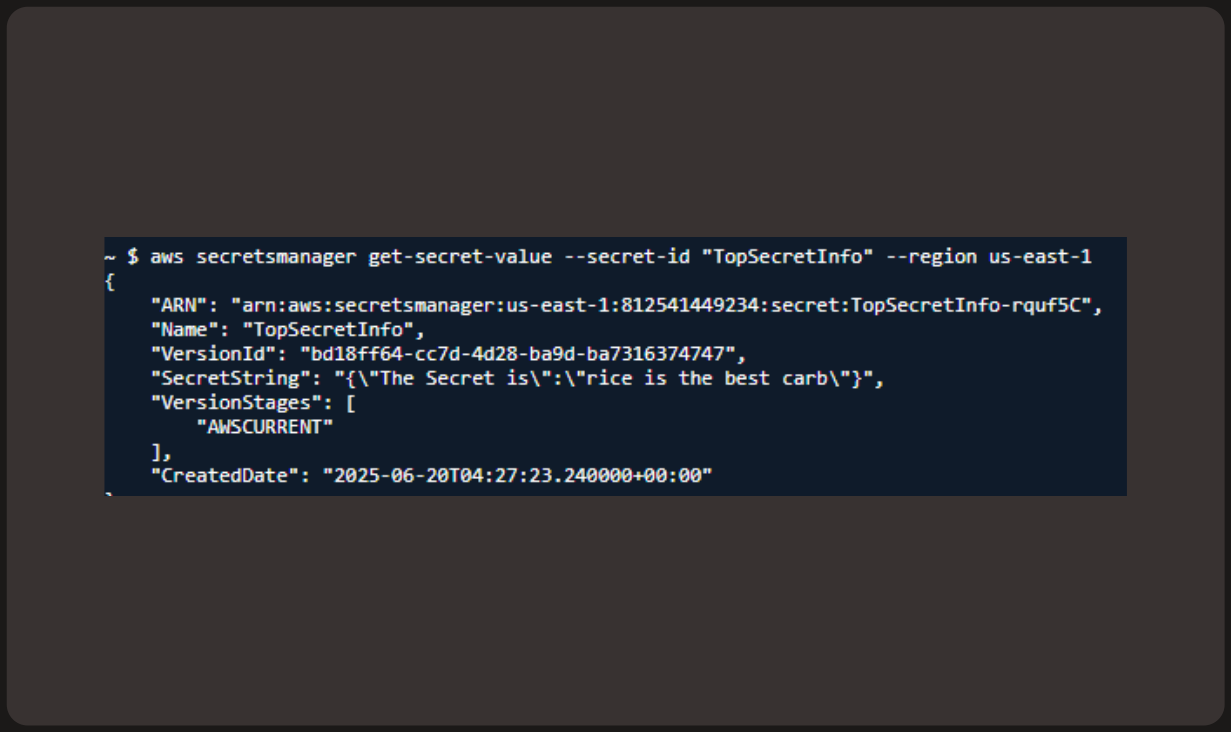
Read vs Write Activity

Read API activity involves when someone views but doesn't change anything. Write API activity involves when changes happen - creating, deleting, modifying resources, or even retrieving the value of a secret. For this project, we need both Read API and Write API.

Verifying CloudTrail

I retreived the secret in two ways: first through AWS console, and second using the AWS CLI.

To analyze my CloudTrail events, I visited event history. I found GetSecretValue. This tells me that my secret's value was retreived or used.



ME
Melvin J Bonner
NextWork Student

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 its a service that helps you bring together your logs from different AWS services, including CloudTrail, for visibility, troubleshooting, and analysis.

CloudTrail's Event History is useful for storing events for only 90 days; with CloudWatch Logs you are able to store events for as long as you like.

A CloudWatch metric is what gets recorded when our filter spots a match in the logs. When setting up a metric, the metric value represents the number of times someone acceses our secret. Default value is used when our filter doesn't find any matches during a given time period.

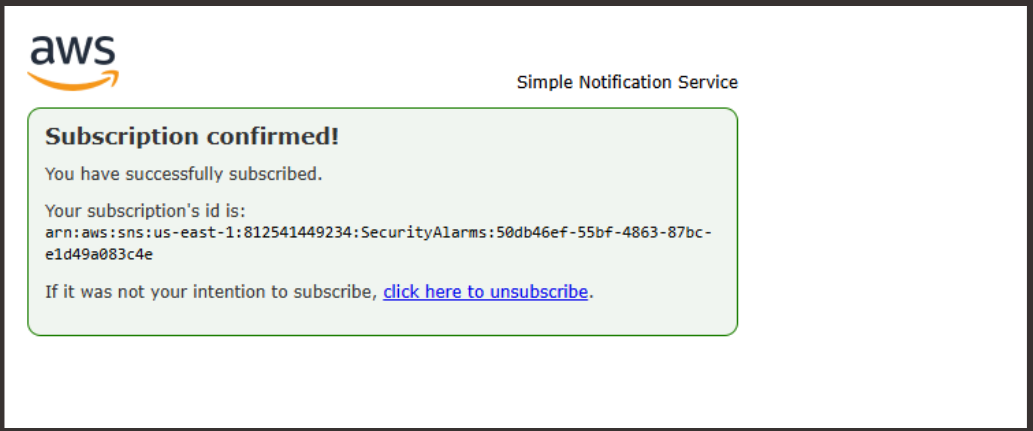

Assign metric
Filter name
GetSecretsValue
Metric name
Secret is accessed
Metric namespace
SecurityMetrics
Applied on transformed logs
-
Metric value
1
Default value
0
Unit
-

CloudWatch Alarm

A CloudWatch alarm is based on the SecretIsAccessed metric. I set my CoudWatch alarm threshold to greater than or equal to 1 in a 5-minute period, 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. My SNS topic is set up to email.

AWS requires email confirmation because they want to make sure it's really you asking for these alerts. This helps prevents sending unsolicited emails.



ME
Melvin J Bonner
NextWork Student

Troubleshooting Notification Errors

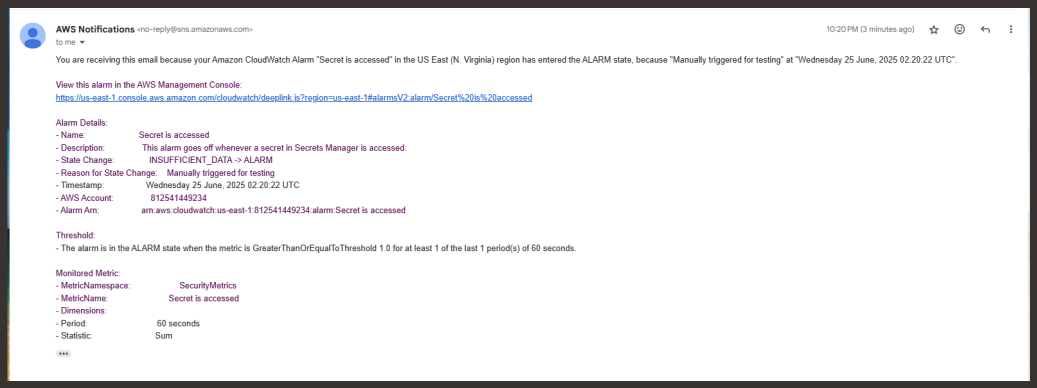
To test my monitoring system, I retrieved my secret value. The results were not what I expected. I didn't receive an email.

When troubleshooting the notification issues I exposed my secret value, checked my email, I checked CloudWatch and checked CloudTrail event history.

I initially didn't receive an email before because the CloudWatch alarm statistic was set to average. The solution was changing the CloudWatch alarm statistic to sum. Sum adds up all occurrences of secret access in the period (what I want).

Success!

To validate the alarm, I checked the alarm configuration using a CLI command for manually triggering the alarm.



AWS Notifications <no-reply@sns.amazonaws.com> 10:20 PM (3 minutes ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "Secret is accessed" in the US East (N. Virginia) region has entered the ALARM state, because "Manually triggered for testing" at "Wednesday 25 June, 2025 02:20:22 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Secret%20is%20accessed

Alarm Details:
- Name: Secret is accessed
- Description: This alarm goes off whenever a secret in Secrets Manager is accessed.
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Manually triggered for testing
- Timestamp: Wednesday 25 June, 2025 02:20:22 UTC
- AWS Account: 812541449234
- Alarm Arn: arn:aws:cloudwatch:us-east-1:812541449234:alarm:Secret is accessed

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:
- MetricNamespace: SecurityMetrics
- MetricName: Secret is accessed
- Dimensions:
- Period: 60 seconds
- Statistic: Sum

...

ME
Melvin J Bonner
NextWork Student

Comparing CloudWatch with CloudTrail Notifications

In a project extension, I enabled SNS notification delivery in CloudTrail, because it will send a notification to my SNS topic every time a new log file is delivered to my S3 bucket.

Aftrer enabling CloudTrail SNS notifications, my inbox was flooded with alerts. In terms of the usefulness of these emails, I thought they were unnecessary and useless notifications.

nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects