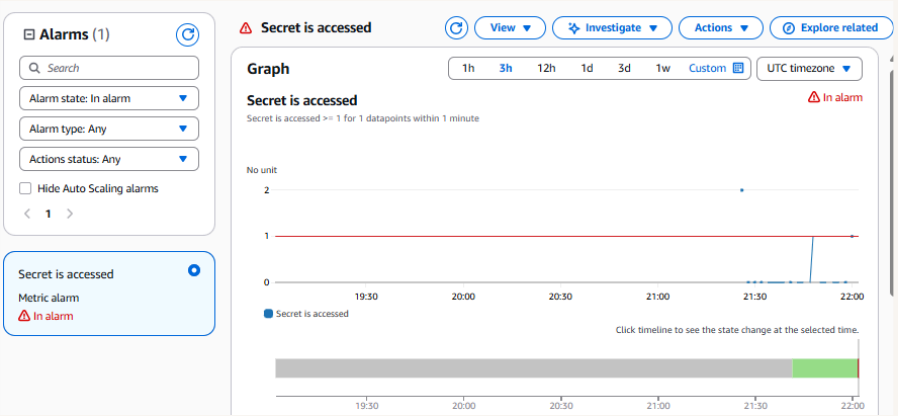
nextwork.org

Build a Security Monitoring System

R Russell Geisler



Russell Geisler
NextWork Student

Introducing Today's Project!

I will demonstrate my knowledge of Cloud Trail, Secrets Manager, Cloud Watch and SNS

Tools and concepts

In this project I learned CLoudWatch, CloudTrail, Secrets Manager and SNS

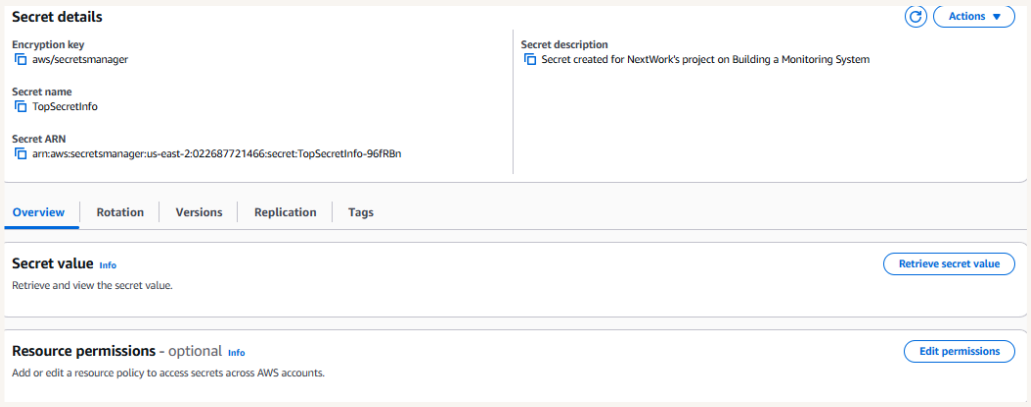
Project reflection

This project took about 2 hours

Create a Secret

Secrets Manager helps you protect secrets, which are passwords, API keys, credentials and sensitive information. Instead of storing them in code, you can store them in Secrets Manager

To set up my project, I created a secret called TopSecretInfo that contains sensitive information



Set Up CloudTrail

AWS CloudTrail is a monitoring service like 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. A trail tells AWS what activity to record and where to sve it.

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

Read vs Write Activity

Read API activity happens when someone views your resoures but no changes are made. Write API happens when someone edits or deletes resources.

Verifying CloudTrail

I retrieved he secret in two ways: first through SecretsManager and second through CloudShell

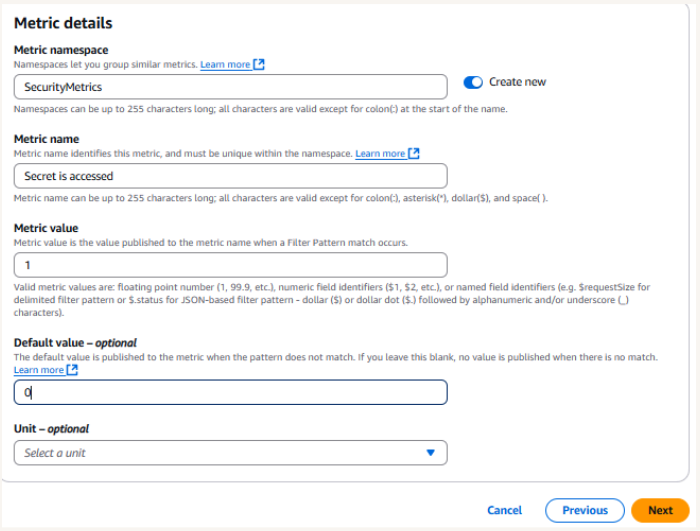
To analyze my cloud events, I visited CloudTrail which showed 2 GetSecretValue activity logs.

CloudWatch Metrics

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

CloudTrail is good for quickly seeing logs for up to 90 days. CloudWatch Logs is where we can set up alerts and automated responses when specific events happen.

Metric value is 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 what gets recorded 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.

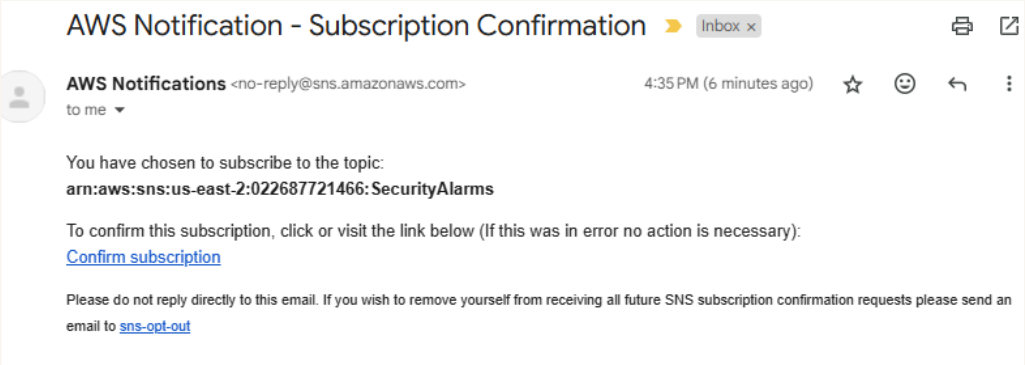

Metric details
Metric namespace
Namespaces let you group similar metrics. Learn more
SecurityMetrics
Create new
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.
Metric name
Metric name identifies this metric, and must be unique within the namespace. Learn more
Secret is accessed
Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar($), and space( ).
Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.
1
Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers ($1, $2, etc.), or named field identifiers (e.g. $requestSize for delimited filter pattern or $.status for JSON-based filter pattern - dollar ($) or dollar dot ($.) followed by alphanumeric and/or underscore (_) characters).
Default value – optional
The default value is published to the metric when the pattern does not match. If you leave this blank, no value is published when there is no match. Learn more
0
Unit – optional
Select a unit
Cancel
Previous
Next

CloudWatch Alarm

The alarm threshold is when the alarm should trigger. We're setting up a static threshold so that your alarm goes off when the SecretIsAccessed metric is greater than or equal to 1 in a 5-minute period. This is a very sensitive setting.

An SNS (Simple Notification Service) 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. SNS automatically delivers that message to all subscribers.

When you set up your email with SNS, AWS doesn't just start sending you emails right away! Instead, they want to make sure it's really you asking for these alerts. That's why they've sent a confirmation email to your inbox.


AWS Notification - Subscription Confirmation
Inbox ×
AWS Notifications <no-reply@sns.amazonaws.com>
4:35 PM (6 minutes ago)
to me
You have chosen to subscribe to the topic:
arn:aws:sns:us-east-2:022687721466:SecurityAlarms
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

Troubleshooting Notification Errors

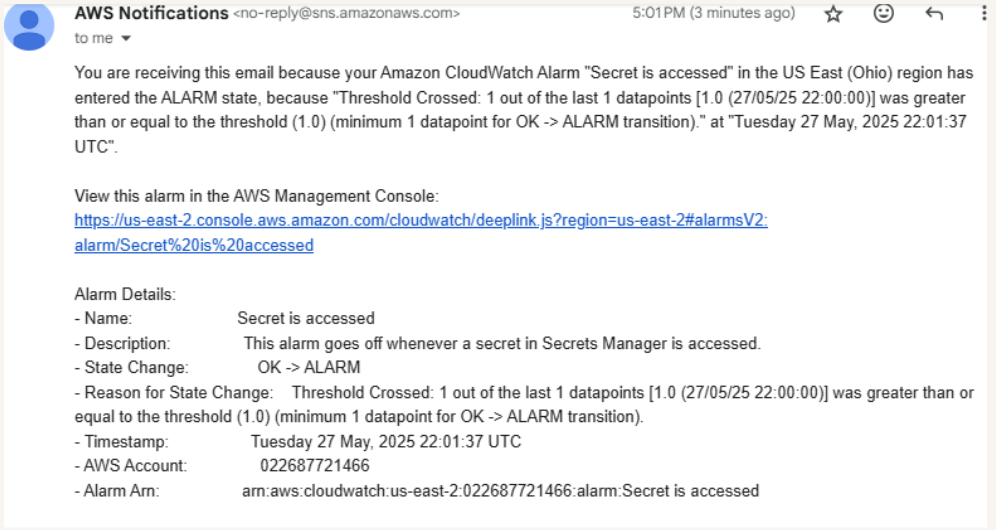
To test my montioring system, I accessed the SecretsManager value again.

Wen troubleshooting the notification issues, I checked the CloudTrail events, log delivery, metric filter, alarm config, and SNS subscription.

I didnt get an email because the alarm was configured to average of 1 instead of sum.

Success!

I validated the alarm worked by looking to CloudWatch alarms and checking my email



AWS Notifications <no-reply@sns.amazonaws.com> 5:01 PM (3 minutes ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "Secret is accessed" in the US East (Ohio) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (27/05/25 22:00:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 27 May, 2025 22:01:37 UTC".

View this alarm in the AWS Management Console:
https://us-east-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-2#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: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (27/05/25 22:00:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Tuesday 27 May, 2025 22:01:37 UTC
- AWS Account: 022687721466
- Alarm Arn: arn:aws:cloudwatch:us-east-2:022687721466:alarm:Secret is accessed

The place to learn & showcase your skills

Check out nextwork.org for more projects