Configuring AWS CloudWatch Log Retention and Archiving

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

Learn how to store logs for long term retention

Discuss the importance of long term log retention

Demonstrate log archival

Archiving log data for long term retention

CloudWatch Log Retention

Never expire

This is the default; all log data will be kept indefinitely

Expire after

One day to 10 years

CloudWatch Logs

5GB of logs for free

After which a per GB fee for the collection, storage and analysis of logs

Log storage fee for CloudWatch in eu-west-2 is $0.0315 per GB

Glacier storage in eu-west-2 is $0.0045 per GB

CloudWatch Logs

Export log data to Amazon S3

Stream log data to Amazon Elasticsearch

Stream logs data to Amazon Kinesis

CloudWatch Logs and S3

S3 storage classes

Choose a storage class that provides the correct level service and cost

Integration

From S3 logged date can be used by EMR, Redshift, Athena and 3rd pary applications

Multi-region and account

Easier to gather logs from different regions and accounts into a single S3 bucket

Exporting Log Data to Amazon S3

Create an S3 bucket

Can not use buckets encrypted with a KMS key

Logs from multiple log groups can be exported to the same bucket

Log data can take 12 hours to become available for export

CloudWatch Log Integration

Near real-time

Consider using log insights or Kinesis integration

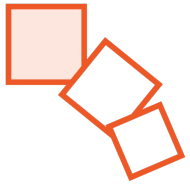
Automate your S3 export

Use a scheduled CloudWatch event to trigger a lambda function for a daily export to S3

S3 Lifecyle Rules

Logs exported to S3 become objects

We can manually set the S3 storage class for each object



Lifecyle rules allow us to automatically transition objects between storage classes and to expire objects

More S3 Features

Object lock

Once enabled on a bucket we can guarantee objects are not deleted or altered for a given period of time

Replication

Objects can be replicated across regions

Demo

Learn how to archived CloudWatch logs in Amazon S3

Working with

- AWS Console

To follow along you will need an AWS Account

Summary

Discussed the importance of log retention

Discussed different ways to archive logs

Shown how to archive logs to S3

In the next module

- Discuss event driven automation
- Learn how to use event rules to trigger Lambda functions
- Course review