Monitoring and Event Response on AWS for DevOps Engineers

INTRODUCING AMAZON CLOUDWATCH

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

Course overview

Why is this course important to you?

Module overview

Introduce CloudWatch

Course Overview

This Course Includes

CloudWatch

Overview of CloudWatch

Logs

Use CloudWatch to store and work with logs

Events

Use CloudWatch events for automation

Alarms

Create alarms to automate responses

Integration

Integrate CloudWatch with other AWS services

Why Is This Course Important to You?

Automation

CloudWatch sits at the heart of automation in AWS

Save time

Understanding event response and CloudWatch integration will save time and money

Security

Securing CloudWatch access, implement tagging and working with EC2 metadata

Who Should View This Course?

Anyone interested in using CloudWatch for event monitoring and response

Learners who are part of a DevOps team or who have monitoring as part of their job role

Before attending this course

- Understanding of AWS core services
- Understanding of AWS cloud concepts

Globomantics

Global health care organization

Been using AWS for some time

Most core services such as EC2, RDS, S3 etc.

We have been asked to

- Identify solutions that can be used for monitoring and event response
- How monitoring solutions integrate with other AWS services

Module Overview

Introducing Amazon CloudWatch

Introduce CloudWatch

List core features

Logs and log streams

Focus in on CloudWatch logs and log streams

Permission and encryption

Discuss securing access to and encrypting CloudWatch logs

Introducing Amazon CloudWatch

Why CloudWatch?

Collect metrics from AWS deployed resources and on-premises

Up to 1-second visibility of metrics and log data

Automate actions based on predefined thresholds, or on machine learning

Help reduce mean-time-to-detect and mean-time-to-resolution

CloudWatch Features

Collect

Collect and store logs and metrics

Monitor

Dashboards, application insights, log and metrics correlation

Act

Automate with alarms and events

Analyze

Log analytics, contributor insights and custom metric operations

Secure

Integrated with IAM and encryption

Amazon CloudWatch Logs

Centralize logs from all your systems

Logs can be stored indefinitely

Log features include

- Custom query language used to query log groups
- Search for specific error codes or patterns
- Visualize log data in dashboards

CloudWatch Log Features

Monitor applications and systems running on EC2

Monitor AWS CloudTrail logged events

Gain Route 53 insights by logging queries

Highly durable storage for log archiving

Amazon CloudWatch Logs Concepts

Log events

A record of activity with a timestamp and message

Log streams

A sequence of log events that share the same source

Log groups

A collection of log streams

Metric filters

Convert logged data into metric data points

Retention settings

Indefinite, one day - ten years

Globomantics

Respond to changes in demand for their customer facing stateless app hosted on EC2

Log information about customer access to their app

Search through AWS API activity

Can CloudWatch help?

CloudWatch Features for Globomantics

Alarms

Monitor a metric and use it to trigger auto scale

Logs

Deploy the CloudWatch agent to gather custom logs

CloudTrail

Integrate CloudTrail with CloudWatch

Demo

Working with Amazon CloudWatch logs

Working with

- AWS Console

To follow along you will need an AWS Account

Working with CloudWatch Log Encryption and User Permissions

CloudWatch Access

Authentication

Credentials are required to authenticate requests to CloudWatch

Authorization

Permissions are required to create and access CloudWatch resources

CloudWatch Authentication

AWS account root user

IAM user with appropriate permissions

IAM role with appropriate permissions

Authorization

Access granted using policies

Policies can be attached to users, groups or roles

Different types of policies

- AWS managed policies
- Customer managed policies

AWS Managed Policies

Full access

Granted with the CloudWatchLogsFullAccess policy

Read only access

Granted with the CloudWatchLogsReadOnlyAccess Policy

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
             "Action": [
    "logs:*" ],
            "Effect": "Allow",

            "Resource": "*"
        }
    ]
}
```

- API version
- Single statement
- List of actions
- Allow
- All resources

```
{
    "Version": "2012-10-17",
    "Statement": [
            {
        "Action": [
            "logs:Describe*",
            "logs:Get*",
    "logs:StartQuery",
        "logs:StopQuery",
            “logs:TestMetricFilter",
            "logs:FilterLogEvents"
],
        "Effect": "Allow",

        "Resource": "*"  }
     ]  }
```

- API version
- Single statement
- List of actions needed for read only access
- Allow
- All resources

What does the next policy do?

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Action": [
        "logs:CreateLogStream",
         "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:us-
west-2:123456789012:log-
group:GlobomanticsApp:*"
      } ] }
```

- API version
- Single statement
- List of actions
- Allow
- Specific resource, Globomantics APP log group

Globomantics

One set of users need to create, view and delete CloudWatch logs

One set of users need to read logs created by the Globomantics customer facing app hosted on EC2

One set of users need to read and edit a set of logs created by Lambda function

CloudWatch Log Encryption

Encryption at rest

All log groups are encrypted by default. You can control the keys.

Encryption in transit

Uses end-to-end encryption of data in transit. CloudWatch controls the keys.

Demo

Working with Amazon CloudWatch log authentication and access control

Working with

- AWS Console

To follow along you will need an AWS Account

Summary

We introduced Globomantics

You were introduced to Amazon CloudWatch

Worked with CloudWatch logs and log streams

Learned the importance of securing access to CloudWatch

In the next module

- Working with CloudWatch and CloudTrail