Working with Amazon CloudWatch and CloudTrail

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

CloudTrail and CloudWatch integration

Centralized CloudTrail logs

Introducing Amazon CloudTrail and CloudWatch Integration

What Is AWS CloudTrail?

Records and stores events

View user and resource activity

Integrates with CloudWatch events

Search through console or integrate with SDKs

AWS CloudTrail Features

Always on

Enabled by default on all AWS accounts

Event history

View, search and download events

Multi-region

Collect events from multiple regions in one place

Integrity

Validate the integrity of CloudTrail logs

Encryption

All logs encrypted by default

CloudTrail Events

Data events

Activities such as S3 object level APIs and AWS Lambda invoke APIs

Management events

Log all administrative actions from all admin tools

CloudTrail Insights Events

Capture unusual activity

Logged only when CloudTrail detects changes in your API activity

Insight events are disabled by default

Additional charges apply

CloudTrail Trails

Event history

90 days of events available to view and search

Trails

Deliver events to S3 or CloudWatch for long term use and analysis

Organization trail

Collect all events into a central AWS account

Think about your own audit requirements, would CloudTrail work for you?

CloudTrail Use Cases

- Helps maintain compliance
- Security analysis
- Monitor S3 object activity
- Operational troubleshooting
- Detecting unusual activity

Working with Amazon CloudTrail

Globomantics

Alerted when the AWS Root user account is used

Ability to view API activity for 2 years

Query, analyze and download API activity

Secure access to API activity

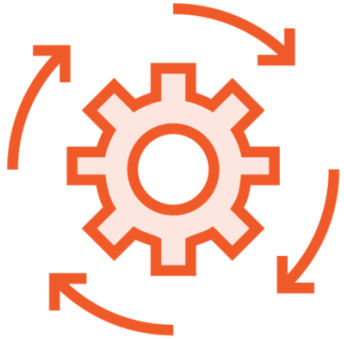
Alerted when the AWS Root user account is used

Integrate CloudTrail with CloudWatch

Integrating CloudTrail with CloudWatch solves Globomantics auditing requirements.

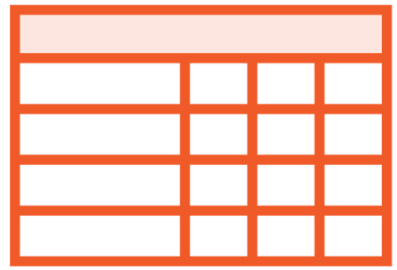
Retention

We can configure log retention for the 2-year period required



Log insights

We can use log insights to query and analyze logs and download the results



IAM integration

Using IAM policies we can control access to CloudTrail information

Working with CloudTrail

CloudTrail Console

Query up to 90 days of activity

Integration

Log activity to an S3 bucket and to CloudWatch

Working with CloudTrail

Single region

Capture events generated in a single region

Multi region

Capture events generated across al regions

Create a new trail

Select optional CloudWatch integration

Provide new log group name

Provide role name

Select events

Implement Integration

Demo

Implementing Amazon CloudTrail and CloudWatch integration

Working with

- AWS Console

To follow along you will need an AWS Account

Working with Centralized CloudTrail logs

AWS Accounts and Audit Logs

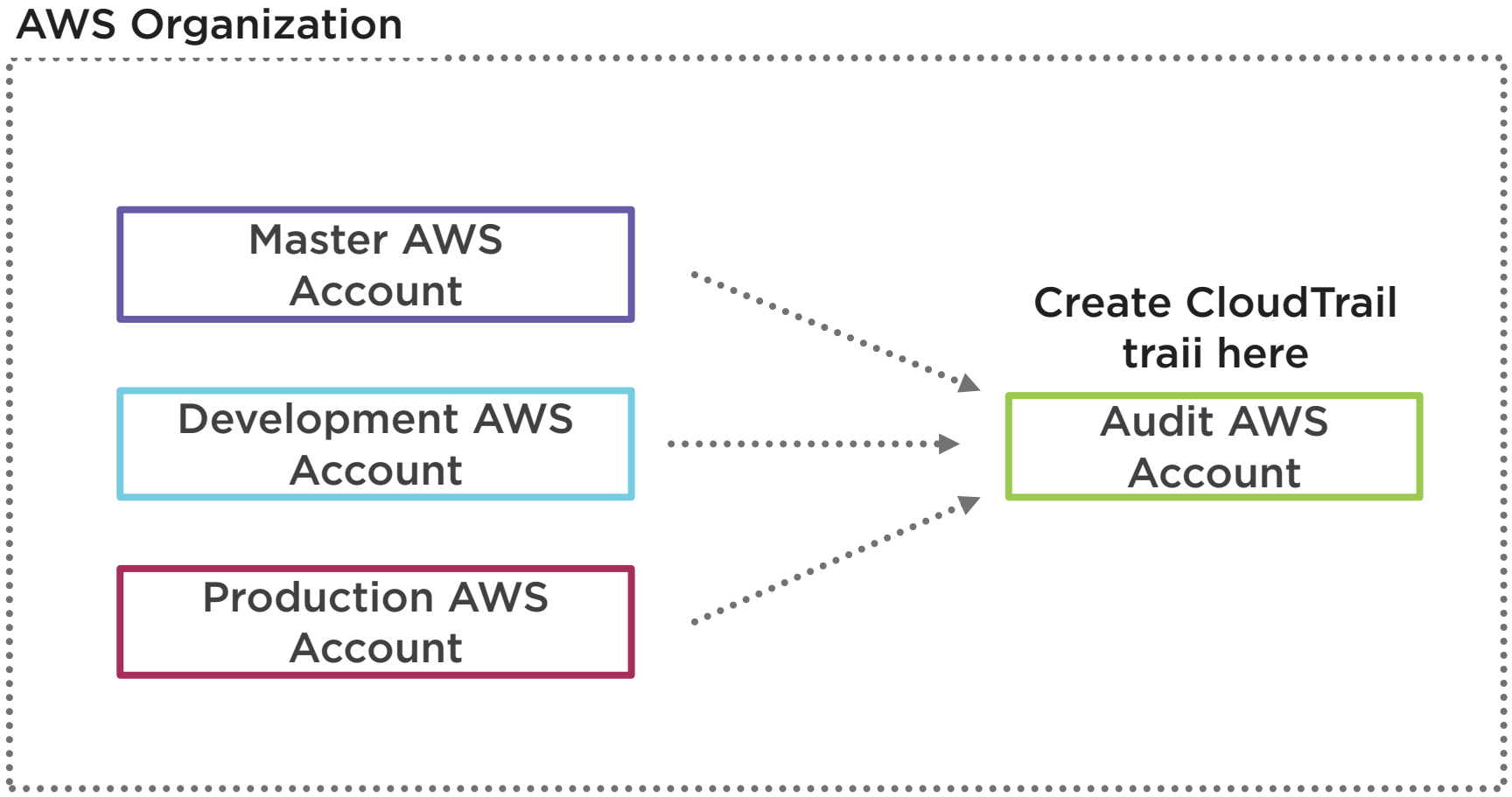
Most organizations using AWS, use multiple AWS accounts

Resources are deployed to induvial AWS accounts and each AWS accounts has its own IAM

Audit logs should be stored and secured centrally

We can secure access so that our audit team can work with the centralized logs

AWS Organization



Organizations are not a requirement

Use roles to grant access needed

Use AWS single sign on

Member accounts can not alter the trail

Centralized CloudTrail Logs

Summary

CloudTrail and CloudWatch integration

Worked with CloudTrail

Discussed centralized CloudTrail logs

In the next module

- Working with CloudWatch events