Capturing and Analyzing Logs

Ben Piper
AWS CERTIFIED SOLUTIONS ARCHITECT

https://benpiper.com

Module Overview

Capturing events with CloudTrail

Viewing logs with CloudWatch Logs

Creating alerts with CloudWatch Alarms

Searching logs with Athena

Tracking changes with AWS Config

Understanding CloudTrail

Event Types

Management

Configuration changes to AWS services

Reading resources

Logging into the management console

Assuming a role

Data

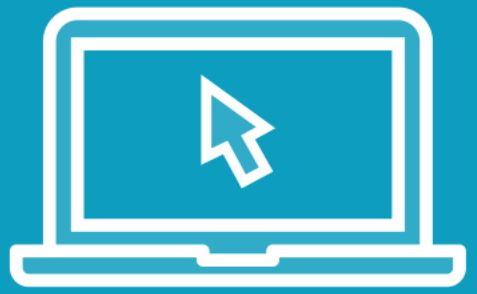
Access to S3 objects

Lambda function execution

CloudTrail logs are stored in S3

Limit what you log to control costs

Demo



Analyze event logs that CloudTrail stores by default

Configure CloudTrail to log all management write events

CloudTrail vs. CloudWatch Logs

CloudTrail vs. CloudWatch Logs

CloudTrail

Logs AWS actions

Stores logs in S3

CloudWatch Logs

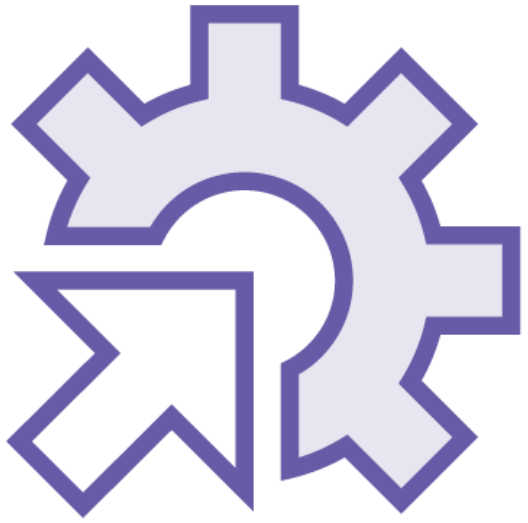
Aggregates logs from CloudTrail *and* non-AWS sources

Provides interface to view and search logs

Configuring CloudWatch Logs

Create a CloudWatch Logs log group to store CloudTrail logs

Configuring CloudWatch Logs



Create IAM service role

- Contains inline service policy that grants CloudTrail permissions to send logs to CloudWatch Logs
- Contains trust policy that allows CloudTrail to assume the role

Role is an IAM principal for CloudTrail to use to authenticate to CloudWatch Logs

Demo

Create a log group in CloudWatch Logs

Create an IAM role for CloudTrail to assume

Browse and search logs in CloudWatch Logs

Demo

Create CloudWatch alarm to trigger when CloudTrail logs a management event

Searching Logs with Athena

Why Athena?

You don't want to use CloudWatch Logs

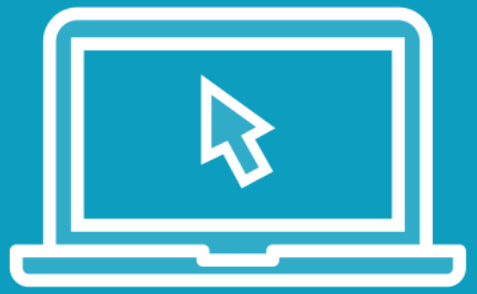
You want to search the contents of S3 objects

Athena uses SQL

You must provide the schema

AWS provides the schema for CloudTrail logs

Demo



Select the S3 bucket containing the objects to search

Create a table in Athena

Run queries against CloudTrail logs

Tracking Configuration Changes in AWS Config

Events and Configuration States

One month ago

Event: Alarm created
State: Alarm exists

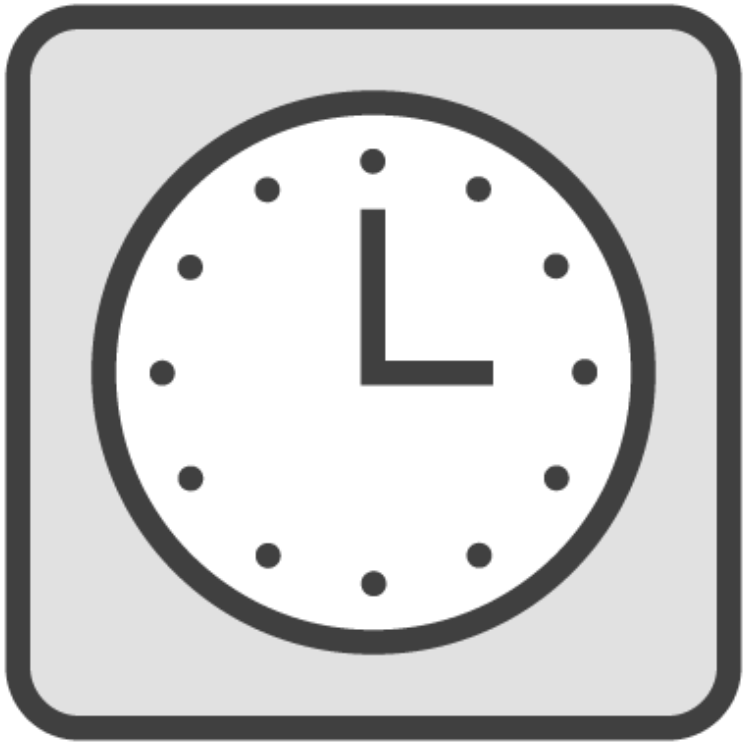
Two weeks ago

State: Alarm exists

Today

Event: Alarm deleted
State: Alarm doesn't exist

AWS Config



Tracks configuration changes over time

Records changes in S3

Notifies of changes

Demo

Configure AWS Config to monitor a CloudWatch alarm

Summary

CloudTrail tracks events

CloudWatch Logs aggregates logs from different sources

CloudWatch Alarms trigger based on specific log activity

Athena performs SQL queries against objects in S3

AWS Config tracks configuration states over time

Coming up Next

Protecting network and host-level boundaries