Working with CloudWatch Logs, Alarms and Metrics

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

- Work with CloudWatch metrics and alarms
- Discuss ways to gather logs from EC2 instances
- Discuss CloudTrail events
- Demonstrate ways to query logged data

Understanding CloudWatch Metrics and Alarms

CloudWatch Metrics

Metrics are data about the performance of our systems

Most AWS services provide free metrics to CloudWatch and some like EC2 offer detailed monitoring

We can search metrics, graph metrics and generate alarms based on metrics

Metric data is kept for 15 months

Viewing Metrics

Metrics are grouped first by namespace and then by dimension combinations

Only AWS services that you are using send metrics to CloudWatch

We can view metrics through the AW console or the AWS CLI

Publishing Custom Metrics

AWS CLI and APIs can be used to publish custom metrics to CloudWatch

Publish as standard resolution (1-minute) or high resolution (1-second)

Adding custom metrics

- From the AWS CLI use cloudwatch put-metric-data
- Use --dimensions to add detail to your custom metrics
- From the AWS CLI use cloudwatch get-metric-statistics

CloudWatch Alarms

We can create CloudWatch alarms to monitor for changes in metrics

Alarms can integrate with SNS, auto scale and EC2 actions

We can configure metric alarms and composite alarms

Alarms invoke actions only when the alarm state changes. The exception is auto scaling actions

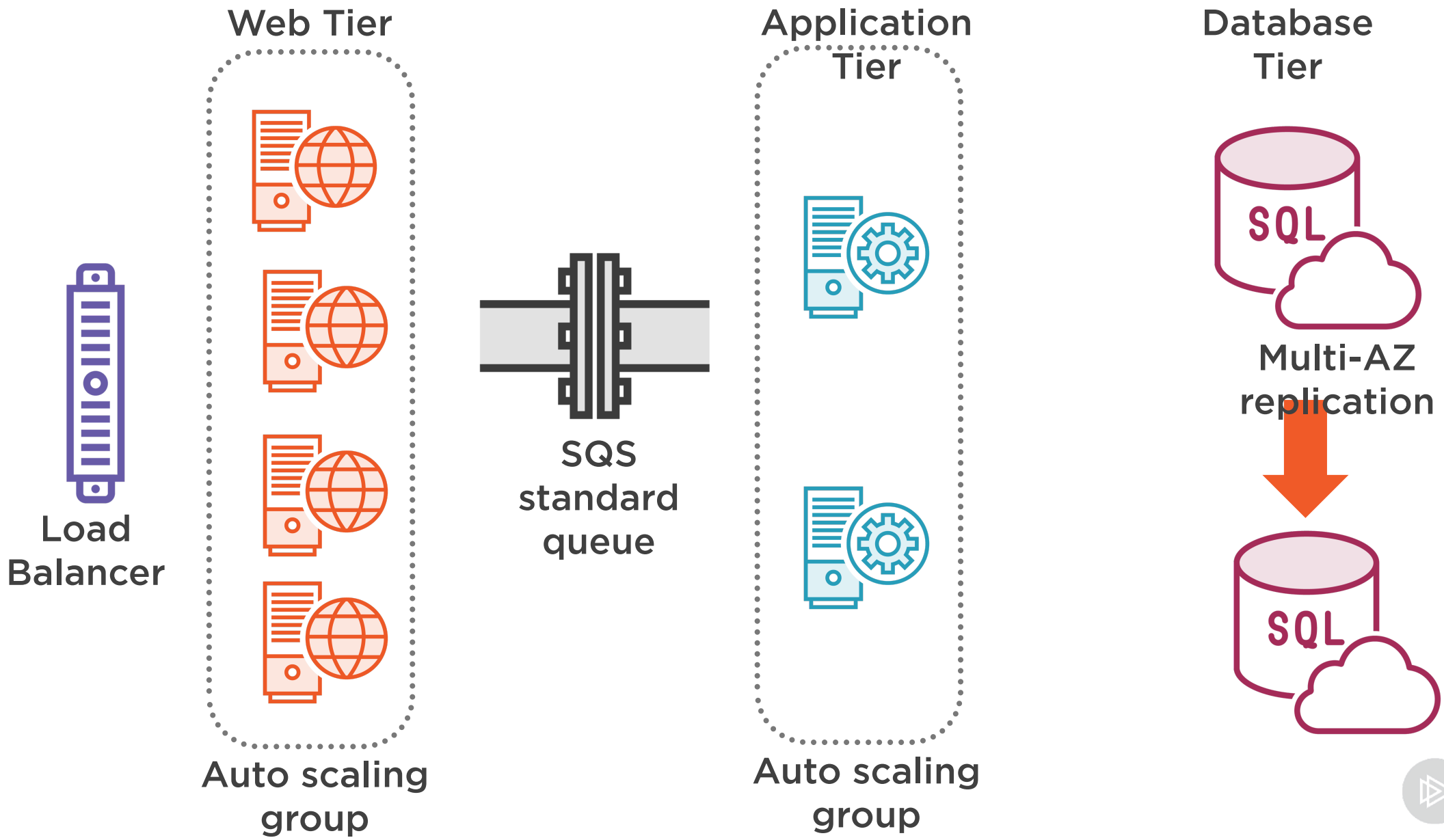
Metric Alarm States

OK – The metric or expression is within the defined threshold

ALARM – The metric or expression is outside of the defined threshold

INSUFFICIENT_DATA – The alarm has just started, the metric is not available, or not enough data is available

Globomantics' Application



What would you suggest Globomantics monitor so that their application can respond to changes in demand and react to availability issues?

Possible Monitoring Options

EC2 instance

CPU, disk metrics, SQS queue length all can be used with auto scale

AWS health

Events from the load balancer, AWS region or SQS queue

RDS database

RDS database metrics, RDS database events

The key to success is automation.

Gathering Logs from EC2 Instances

CloudWatch Agent

EC2 or on-premise

Collect metrics and logs from both EC2 and on-premise systems

Linux or Windows

Multiple Linux and Windows operating systems supported

CloudWatch Agent Installation

Create and attach an IAM role

Download the agent package

Modify the agent configuration file

Install and start the agent on your servers

CloudWatch Agent

For EC2 instances create a role that can write to CloudWatch

For and on-premise server create an IAM user and create a profile locally

CloudWatch agent can be deployed using Systems Manager, CloudFormation or manually

The CloudWatch configuration file can be create manually or by using a wizard

Consider storing your CloudWatch agent configuration file settings in Parameter Store.

With the CloudWatch Agent

Collect more system-level metrics from EC2 instances

Collect system-level metrics from on-premise servers

Collect custom metrics from your applications or services

Collect logs from both EC2 instances and on-premise servers

Sending log data to CloudWatch

- Centralized log file storage
- Quicker access to logs
- Indefinite log file retention
- Access logs regardless of the state of the instance
- Integrate with other CloudWatch features such as alarms

Demo

Work with CloudWatch metrics and alarms

Work with EC2 integration with CloudWatch

Working with

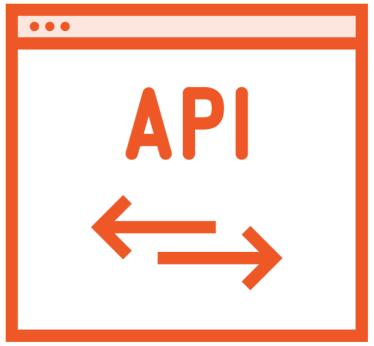
- AWS Console

To follow along you will need an AWS Account

Understanding AWS CloudTrail Events

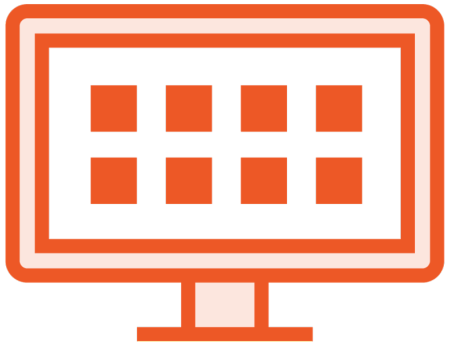
CloudTrail Events

Module 3 covered CloudTrail integration with CloudWatch, lets talk more about different event types.



API events

Events generated by calls to public APIs



AWS Console Sign-in

All attempts to sign into to the AWS console are recorded

Service events

Events created by an AWS service

CloudTrail Events

Each event has an event ID, some events will share and event ID

Each entry will have a userIdentity field that identifies the entity

Interact with events through the CloudTrail dashboard, CloudWatch and S3

Interacting with CloudTrail Events

CloudTrail dashboard

90 days of activity, search through and download events

CloudWatch

CloudWatch events, alarms, metrics, logs and log insights

S3

Long term archival at scale, S3 select, Athena and 3rd party tools

Globomantics

Alerted when the root user account is used

Alerted when their EC2 instances are running low on disk space

Alerted when KMS keys are created or deleted

Alerted when their deployed web application is generating 404 errors

Which of these can CloudTrail help with?

CloudTrail Events

Root user and KMS keys

Both would generate events in CloudTrail

Disk space and 404

Both can be seen if you integrate your EC2 operating system metrics and logging with CloudWatch

Demo

Querying logs in CloudWatch

Working with

- AWS Console

To follow along you will need an AWS Account

Summary

Discussed how CloudWatch alarms can be used to automate actions in response to changes in metrics

Discussed gathering logs for EC2 instances

Discussed CloudTrail events and how they can be used in CloudWatch

In the next module

- Discuss CloudWatch log retention
- Discuss CloudWatch log archiving