Module 7 – Monitoring and Analytics

Contents

Learning objectives

In this module, you will learn how to:

- Summarize approaches to monitoring your AWS environment.
- Describe the benefits of Amazon CloudWatch.
- Describe the benefits of AWS CloudTrail.
- Describe the benefits of AWS Trusted Advisor.

Introduction

Every business, including this coffee shop, can use metrics to measure how well systems and processes are running. This idea of observing systems, collecting metrics, evaluating those metrics over time, and then using them to make decisions or take actions, is what we call monitoring.

It's important to set up monitoring in the cloud. With the elastic nature of AWS services that dynamically scale up and down, you'll want to keep a close pulse on your AWS resources to ensure that your systems are running as expected.

For example, if an EC2 instance is being over-utilized, you can trigger a scaling event that automatically would launch another EC2 instance. Or if an application starts sending error responses at an unusually high rate, you can alert an employee to go take a look at what's going on.

In the next few videos, we will cover a variety of tools that help you monitor your AWS environment. This monitoring will help you measure how your systems are performing, alert you when things aren't right, and even help you debug and troubleshoot issues as they come along.

Amazon CloudWatch

Amazon CloudWatch is a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics.

CloudWatch uses **metrics** to represent the data points for your resources. AWS services send metrics to CloudWatch. CloudWatch then uses these metrics to create graphs automatically that show how performance has changed over time.

CloudWatch alarms

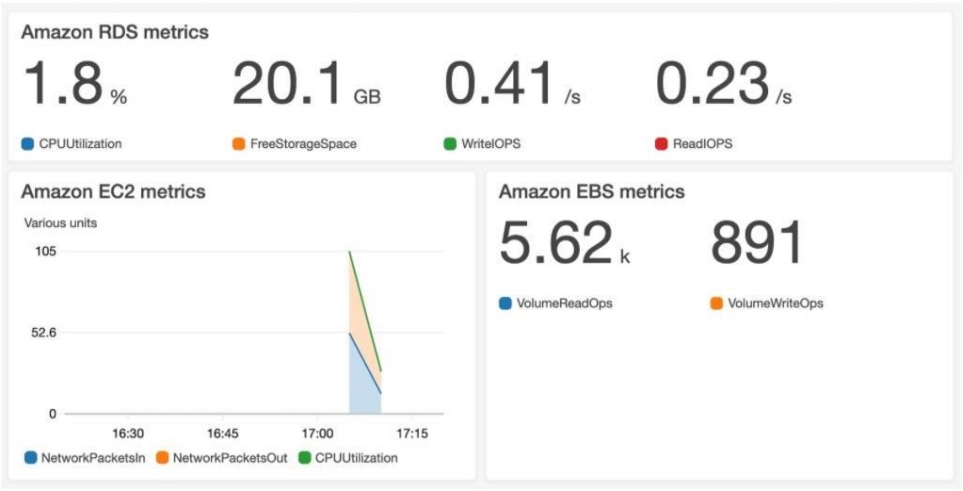
With CloudWatch, you can create **alarms** that automatically perform actions if the value of your metric has gone above or below a predefined threshold.

For example, suppose that your company's developers use Amazon EC2 instances for application development or testing purposes. If the developers occasionally forget to stop the instances, the instances will continue to run and incur charges.

In this scenario, you could create a CloudWatch alarm that **automatically stops an Amazon EC2 instance** when the CPU utilization percentage has remained below a certain threshold for a specified period. When configuring the alarm, you can specify to receive a notification whenever this alarm is triggered.

Even better, CloudWatch alarms are integrated with **SNS**.

CloudWatch dashboard



The CloudWatch **dashboard** feature enables you to access all the metrics for your resources from a single location. This enables you to collect metrics and logs from all your AWS resources applications, and services that run on AWS and on-premises servers, helping you break down silos so that you can easily gain system-wide visibility. For example, you can use a CloudWatch dashboard to **monitor the CPU utilization of an Amazon EC2 instance**, the **total number of requests made to an Amazon S3 bucket**, and more. You can even customize separate dashboards for different business purposes, applications, or resources.

You can get visibility across your applications, infrastructure, and services, which means you gain insights across your distributed stack so you can correlate and visualize metrics and logs to quickly pinpoint and resolve issues. This in turn means you can reduce **mean time to resolution, or MTTR**, and improve **total cost of ownership, or TCO**. So in our coffee shop, if the MTTR of cleaning hours for restaurant machines is shorter then we can save on TCO with them. This means freeing up important resources like developers to focus on adding business value.

Lastly, you can drive insights to optimize applications and operational resources. By, for example, aggregating usage across an entire fleet of EC2 instances to derive operational and utilization insights. And now our staff can focus on serving coffee versus constantly cleaning machines before they are due to be cleaned.

AWS CloudTrail

AWS CloudTrail is a comprehensive API auditing tool that records API calls for your account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more. You can think of CloudTrail as a “trail” of breadcrumbs (or a **log of actions**) that someone has left behind them.

Recall that you can use API calls to provision, manage, and configure your AWS resources. With CloudTrail, you can view a **complete history of user activity and API calls** for your applications and resources.

Events are typically updated in CloudTrail **within 15 minutes** after an API call. You can filter events by specifying the time and date that an API call occurred, the user who requested the action, the type of resource that was involved in the API call, and more.

CloudTrail can save those logs indefinitely in secure S3 buckets. In addition, with tamper-proof methods like Vault Lock, you then can show absolute provenance of all of these critical security audit logs.

Example: AWS CloudTrail event

Suppose that the coffee shop owner is browsing through the AWS Identity and Access Management (IAM) section of the AWS Management Console. They discover that a new IAM user named Mary was created, but they do not who, when, or which method created the user.

To answer these questions, the owner navigates to AWS CloudTrail.

In the CloudTrail Event History section, the owner applies a filter to display only the events for the “CreateUser” API action in IAM. The owner locates the event for the API call that created an IAM user for Mary. This event record provides complete details about what occurred:

On January 1, 2020 at 9:00 AM, IAM user John created a new IAM user (Mary) through the AWS Management Console.

CloudTrail Insights

Within CloudTrail, you can also enable **CloudTrail Insights**. This **optional** feature allows CloudTrail to automatically **detect unusual API activities** in your AWS account.

For example, CloudTrail Insights might detect that a higher number of Amazon EC2 instances than usual have recently launched in your account. You can then review the full event details to determine which actions you need to take next.

AWS Trusted Advisor

AWS Trusted Advisor is an automated web service that inspects your AWS environment and provides **real-time recommendations** in accordance with AWS best practices.

Trusted Advisor compares its findings to AWS best practices in **five** categories: **cost optimization, performance, security, fault tolerance, and service limits.** For the checks in each category, Trusted Advisor offers a list of recommended actions and additional resources to learn more about AWS best practices.

The guidance provided by AWS Trusted Advisor can benefit your company at all stages of deployment. For example, you can use AWS Trusted Advisor to assist you while you are creating new workflows and developing new applications. Or you can use it while you are making ongoing improvements to existing applications and resources.

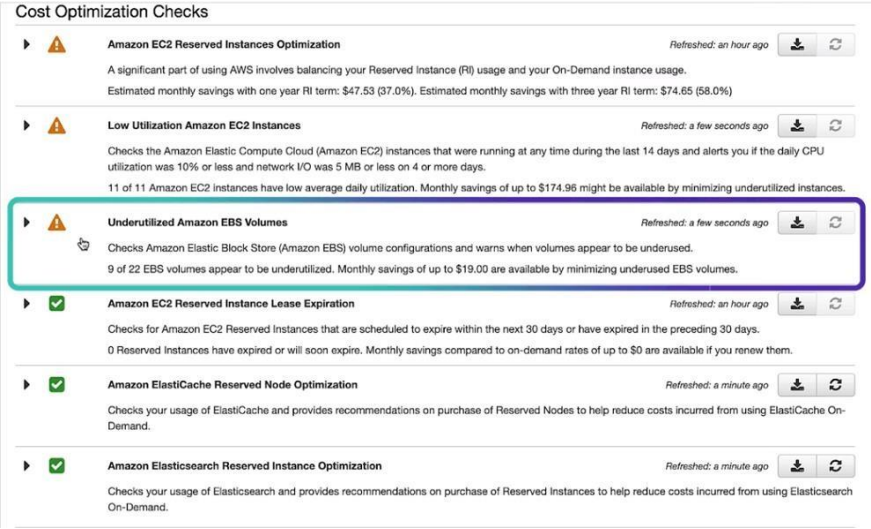
AWS Trusted Advisor dashboard

When you access the Trusted Advisor dashboard on the AWS Management Console, you can review completed checks for cost optimization, performance, security, fault tolerance, and service limits.

For each category:

- The green check indicates the number of items for which it detected **no problems**.
- The orange triangle represents the number of recommended **investigations**.
- The red circle represents the number of recommended **actions**.

Example:



Some checks are free and are included in your AWS account, and others are available depending on the level of your support plan. Some examples of checks are, if you don't have multi-factor authentication turned on for your root user, it's going to let you know. If you have **underutilized EC2 instances** that might be able to be turned off in order to save money, or if you have **EBS volumes that haven't been backed up** in a reasonable amount of time, it will let you know that, too.

Trusted Advisor can help point you in the right direction when it comes to the five pillars. You can set up email alerts that go out to billing, operations, and security contacts, as checks get run in your account. Make sure you have Trusted Advisor turned on so that you too can start taking action to optimize your AWS account.

Summary

Understanding what is happening in your environment is key to maintaining efficient, secure, and compliant applications. We discussed how **CloudWatch** can provide near real-time understanding of how your system is behaving, including being alerted to conditions that require your attention.

CloudWatch also gives you the ability to look at those metrics over time as you tune your system for maximum performance.

We discussed how **CloudTrail** can help you know exactly who did what, when, and from where. It answers all of your AWS **auditing** questions, except why they did it.

And finally, we looked at **Trusted Advisor** that compiles a **quick dashboard** of over 40 common concerns around cost, performance, security, and resilience in an actionable dashboard.

Quiz

Which actions can you perform using Amazon CloudWatch? (Select TWO.)

- Monitor your resources' utilization and performance
- Access metrics from a single dashboard

Which service enables you to review the security of your Amazon S3 buckets by checking for open access permissions?

- AWS Trusted Advisor

Which categories are included in the AWS Trusted Advisor dashboard? (Select TWO.)

- Performance
- Fault tolerance