Lab Assignment 8

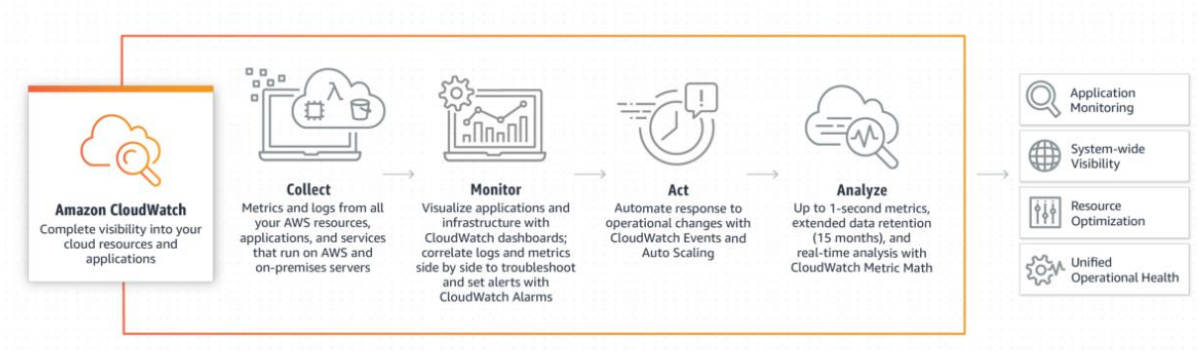
Lab Objective:

To study and implementation of AWS CloudWatch Service. In this lab assignment, the students will launch an EC2 Linux instance and create the CloudWatch Alarm to get a notification using AWS SNS (Simple Notification Service) when CPU utilization goes higher as per the decided threshold.

(*Students can do any custom change or can take any AWS resource for implementing CloudWatch Service but the testing will be the concern of themselves*)

AWS CloudWatch Introduction:

- Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers.
- CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.
- CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS and on-premises servers.
- You can use CloudWatch to detect anomalous behaviour in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.

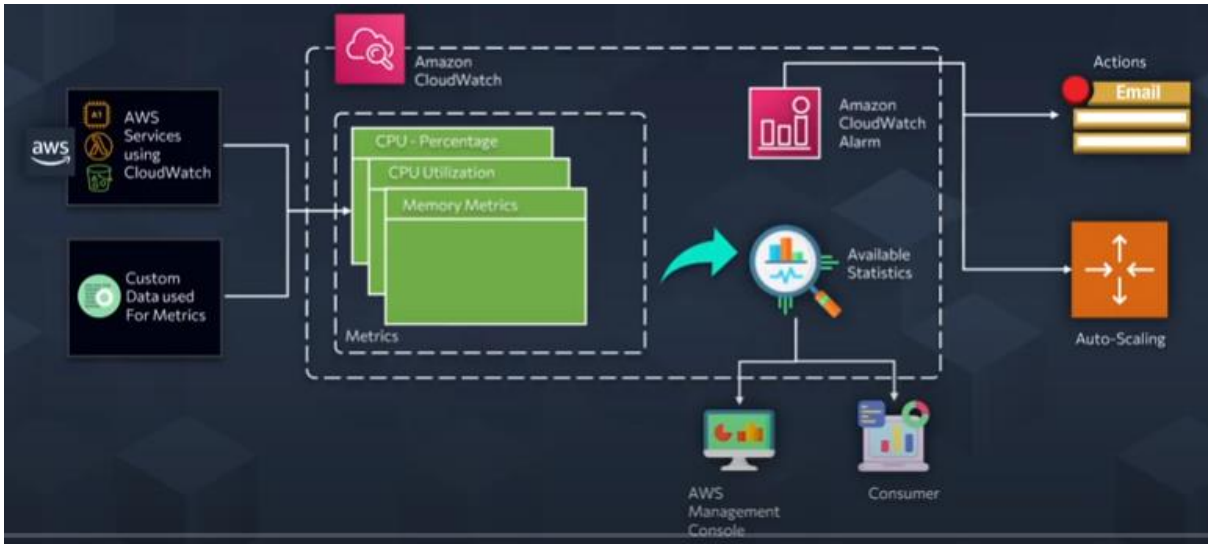


Working of CloudWatch

Detailed Explanation (Concepts and use cases) of CloudWatch is given in the below link:

https://www.youtube.com/watch?v=G4_ay2_h9GI&list=PLiH9_MU-6RjI9gdFqmvUfKRfw_zRxIb6o&index=92&ab_channel=Pythoholic

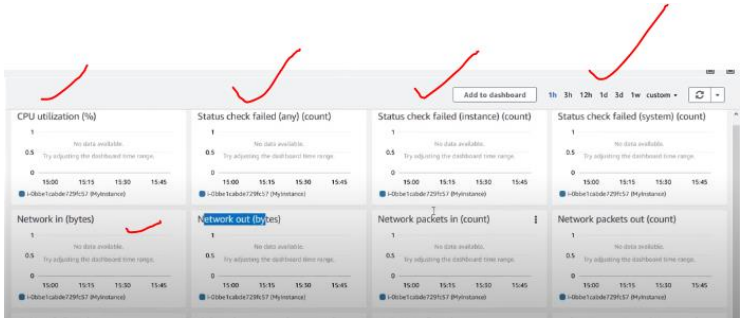
Lab Activities for Implementation of CloudWatch



The lab scenario

Task 0: Login to AWS account and go to AWS console.

Task 1: Launch an EC2 Linux instance and review its CPU utilization metrics once it gets running. Specially, review the Status check and Monitoring. When you will go in monitoring tab all CloudWatch metrics you will see.



A sample image for monitoring tab

Task 2: Go to CloudWatch Management Console and View CPU utilization metrics on dashboard. Moreover, you can find other metrics also here.

Task 3: Create the Alarm for EC2 instance by creating a static threshold CPU utilization. (Please remember minimum period should be 60 seconds and set the conditions properly so that Alarm can get triggered). This is the condition where no load on the CPU of EC2 instance.

Task 4: Configure the actions of CloudWatch by creating new Topic and give your email ID. Once you will create the SNS topic you will be received a confirmation E-Mail. Then click on the confirmation link and the services will be subscribed from your side.

Task 5: Now view your SNS console and review all the available metrics over here. Also check your status that subscription. It should be verified. (Your Email Id Should be the Endpoint there)

Task 6: The Main Agenda here is that when CPU utilization of the EC2 instance gets exceed the threshold then email notification should be reached to the given email address.

Task 7: Finally, Save the created Alarm by reviewing all the metrics.

Task 8: Check the proper working of created alarm. Also set the different combinations of CPU utilization, threshold, and time to validate the CloudWatch service and SNS service functionality/working.

Task 9: Install the Stress Testing Tool to increase the Load of CPU. Follow the steps given below to increase the CPU load of the EC2 instances using Command Line. So, connect your EC2 Linux instance and perform few steps on its terminal/command line interface.

```
$ sudo amazon-linux-extras install epel -y

$ sudo yum install stress

$clear

$ stress --help

$ stress --cpu 4 --timeout 180
```

Check your inbox where the CloudWatch Notification mail is received by you.

Check all the history using CloudWatch Alarm Dashboard.

Task 10: Take the snapshots of all performed tasks. Then create a doc/pdf of your enrolment number_lab08(Ex: E18CSE072_Lab08) and upload the file on LMS.

Please note that delete everything (EC2 Instances, AWS CloudWatch Alarm and SNS Topic) after performing Lab tasks.

YouTube Video for Lab Implementation:

https://www.youtube.com/watch?v=mcV1idfCXOo&list=PLiH9_MU-6RjI9gdFqmvUfKRfw_zRxIb6o&index=93&ab_channel=Pythoholic

AWS Web Documentation:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/US_AlarmAtThresholdEC2.html

Additional Task: (Glimpse of Next Lab)

CloudTrail:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

Youtube Video:

https://www.youtube.com/watch?v=0fSJv5AxC14&list=PLiH9_MU-6RjI9gdFqmvUfKRfw_zRxIb6o&index=94&ab_channel=Pythoholic

AWS Web Link:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html