

Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up a Cloud-Based Monitoring Service Enable basic cloud monitoring (e.g., CloudWatch on AWS) View metrics like CPU usage and disk I/O for your cloud VM.

Name: Swathika K

Department: AML

Introduction and Overview

Cloud-based monitoring plays a vital role in modern infrastructure management by providing real-time insights into the performance and health of cloud resources. In this Proof of Concept (PoC), we will configure **Amazon CloudWatch** to monitor essential metrics for an **EC2 instance**, including **CPU utilization, disk I/O, and network traffic**. This implementation will help track system performance, detect potential bottlenecks, and set up alerts for proactive issue resolution, ensuring optimal resource utilization and uptime.

Objective

The goal of this project is to:

1. Understanding the basics of AWS CloudWatch and its monitoring capabilities.
2. Configuring CloudWatch to monitor essential EC2 metrics.
3. Gaining hands-on experience in proactive cloud resource management

Importance of Cloud-Based Monitoring

Hands-On Learning: Provides practical exposure to cloud-based monitoring tools like AWS CloudWatch, helping you gain essential skills for real-world cloud infrastructure management.

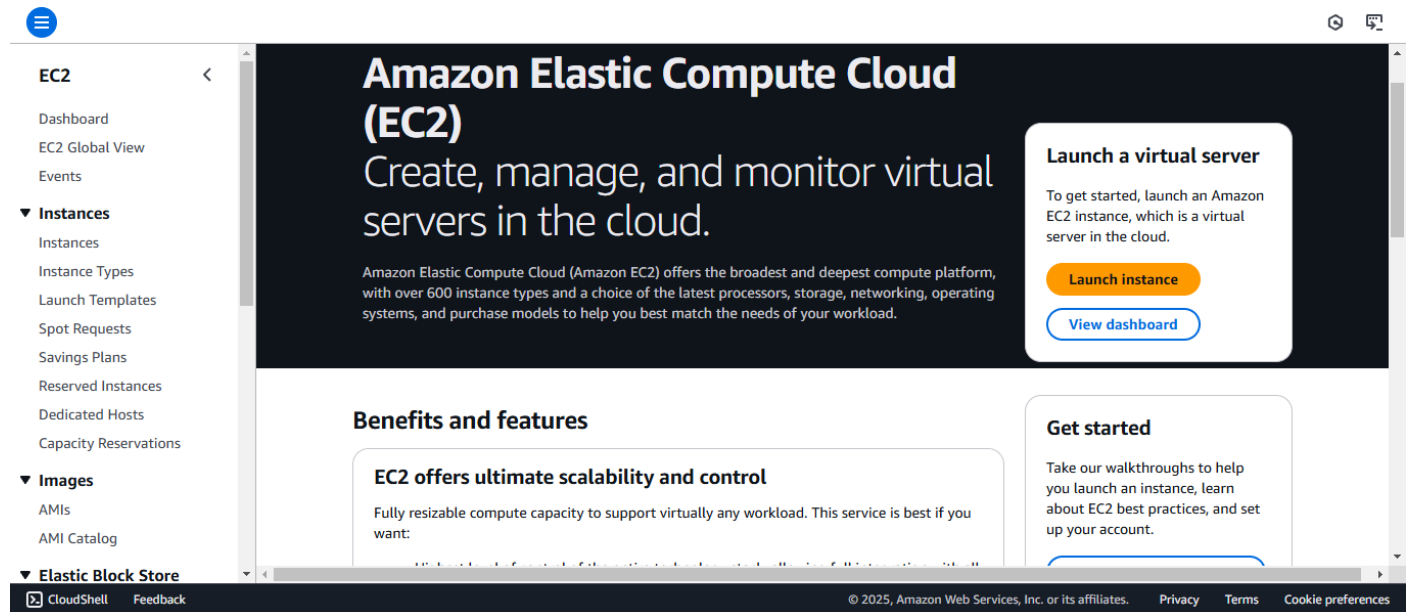
Proactive Resource Management: Enables you to monitor system performance in real-time, identify performance issues, and take corrective actions before they impact end users.

Foundation for Automation: Lays the groundwork for automating monitoring processes, such as setting up alerts and scaling actions, which are critical for efficient cloud operations and DevOps practices.

Step-by-Step Overview

Step1:

Open the AWS Management Console. Navigate to the EC2 Dashboard.

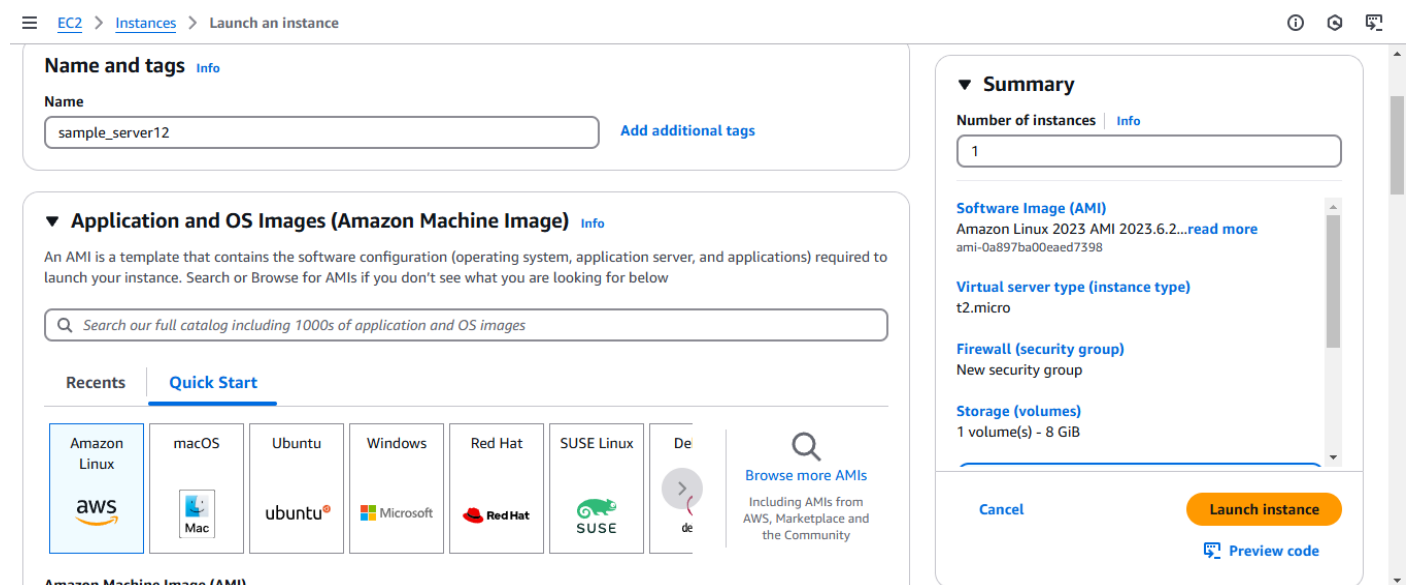


Step 2 :

Click Launch Instance, Configure the instance as needed:

Select an Amazon Machine Image (e.g., Amazon Linux or Ubuntu).

Choose an instance type (e.g., t2.Micro for free-tier eligibility)



EC2 > Instances > Launch an instance

Auto-assign public IP | Info
Enable
Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

We'll create a new security group called 'launch-wizard-3' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances | Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0a897ba00eae7398

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel Launch instance Preview code

Step 3:

Configure the security group to allow necessary ports (e.g., SSH, HTTP, etc.).

EC2 > Instances > Launch an instance

Stop - Hibernate behavior | Info
Select

Termination protection | Info
Select

Stop protection | Info
Select

Detailed CloudWatch monitoring | Info
Enable
Additional charges apply

Elastic GPU | Info
Select

Credit specification | Info
Standard

Placement group | Info

Summary

Number of instances | Info
1

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Preview code

Step 4:

Launch the instance, While launching the EC2 instance:

Under the "Advanced Details" section, ensure that the CloudWatch monitoring option is enabled.

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0a5db4d125ee8f92f)

► Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
[Create billing alerts](#)

Connect to your instance
Once your instance is running, log into it from your local computer.
[Connect to instance](#)
[Learn more](#)

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
[Connect an RDS database](#)
[Create a new RDS database](#)
[Learn more](#)

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots.
[Create EBS snapshot policy](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EC2 > Instances > i-0a5db4d125ee8f92f

EC2

- Dashboard
- EC2 Global View
- Events
- ▼ **Instances**
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
- ▼ **Images**
 - AMI

Auto-assigned IP address 34.222.36.53 [Public IP]	VPC ID vpc-0f2a0b0d66361319f	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
IAM Role -	Subnet ID subnet-0b95e8f72cb2ad94b	Auto Scaling Group name -
IMDSv2 Required	Instance ARN arn:aws:ec2:us-west-2:423623830296:instance/i-0a5db4d125ee8f92f	Managed false
Operator -		

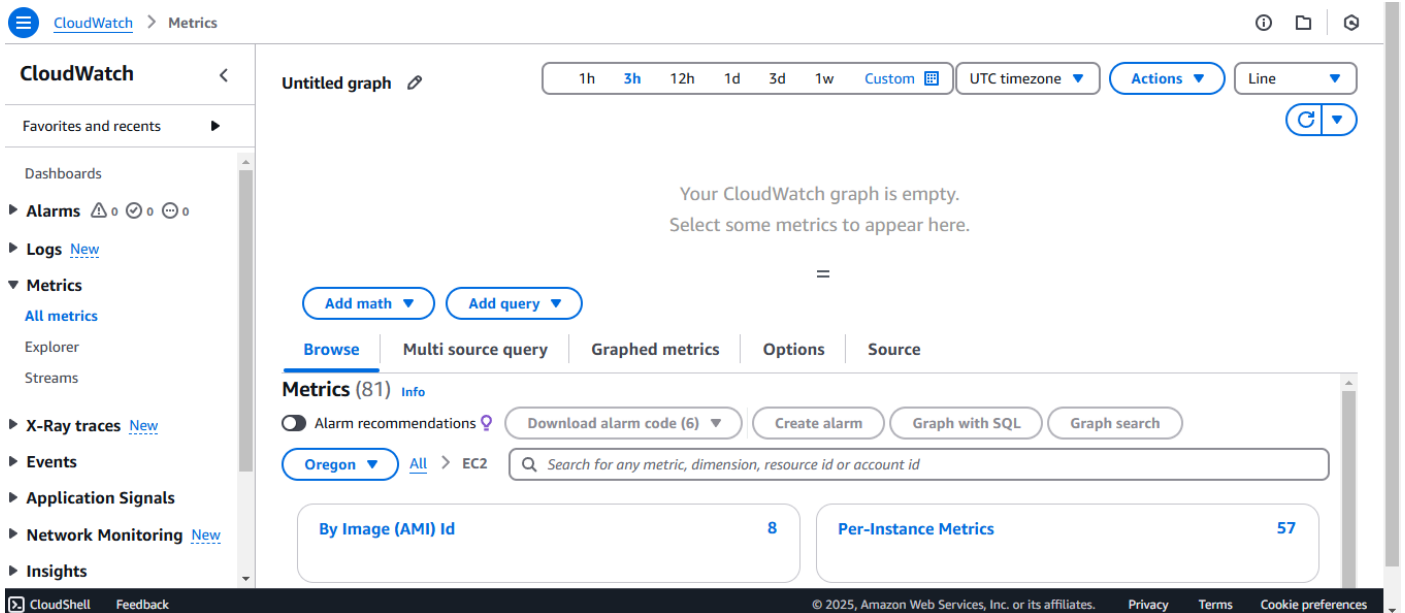
Details Status and alarms **Monitoring** Security Networking Storage Tags

CloudWatch agent metrics
The monitoring tab will now include metrics related to a single instance in the CWAgent namespace. If you want metrics that are emitted from the CloudWatch agent to be displayed, include them in the CWAgent namespace.

Step 5:

Open the CloudWatch Dashboard, On the CloudWatch Dashboard, navigate to Metrics on the left-hand menu.

Click All Metrics and choose the EC2 namespace.



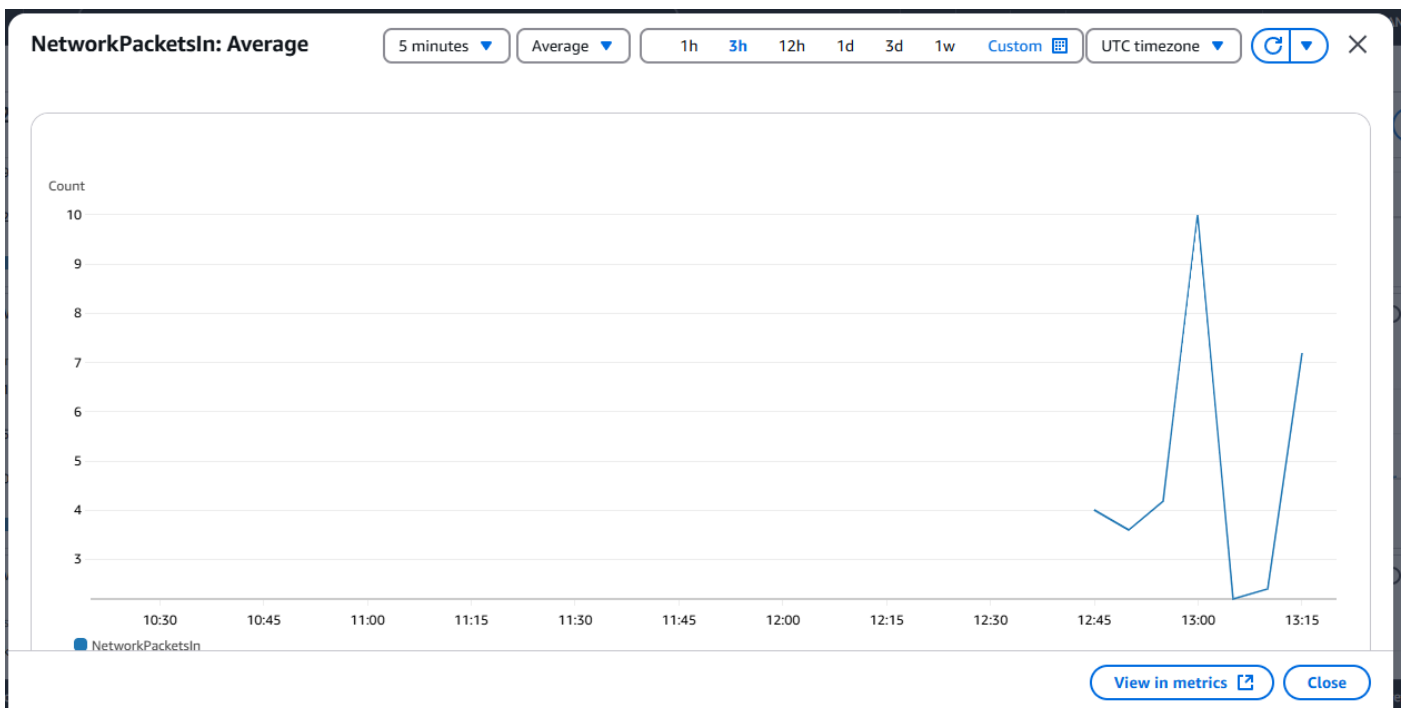
Step 6:

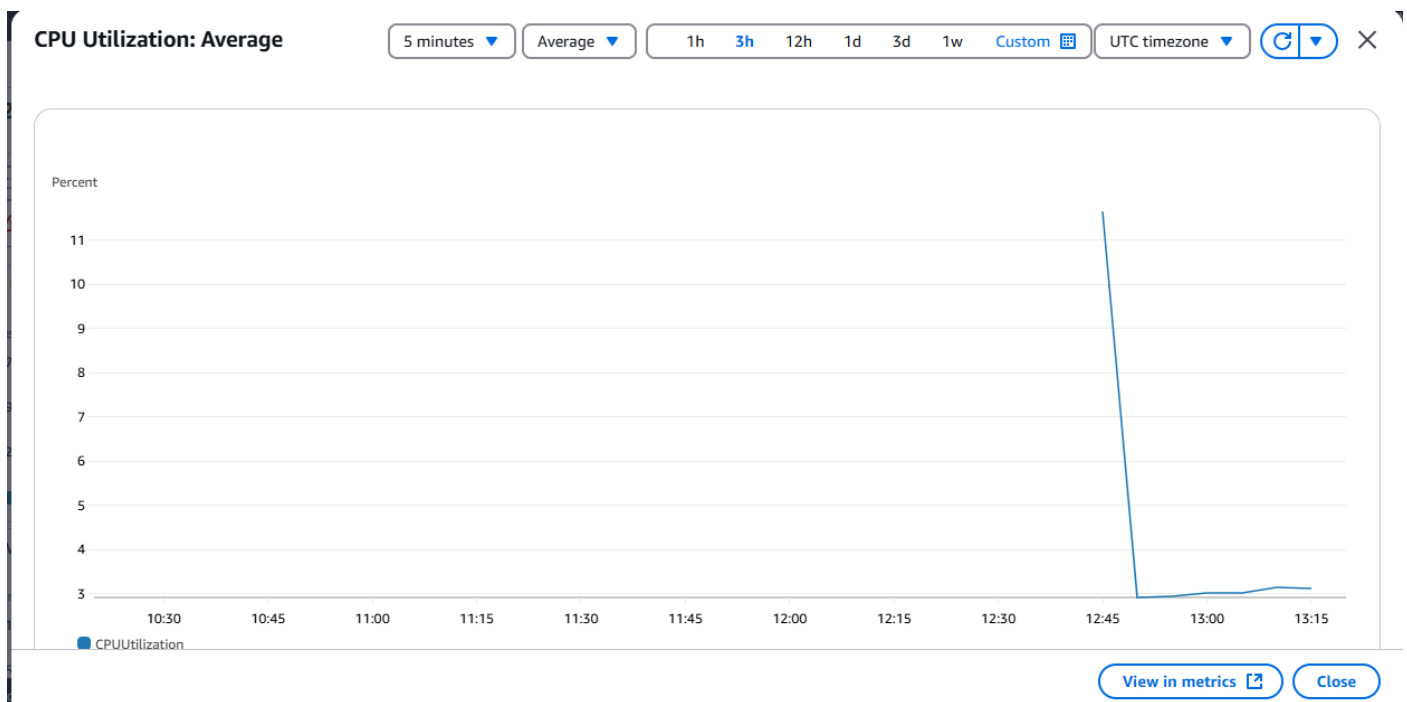
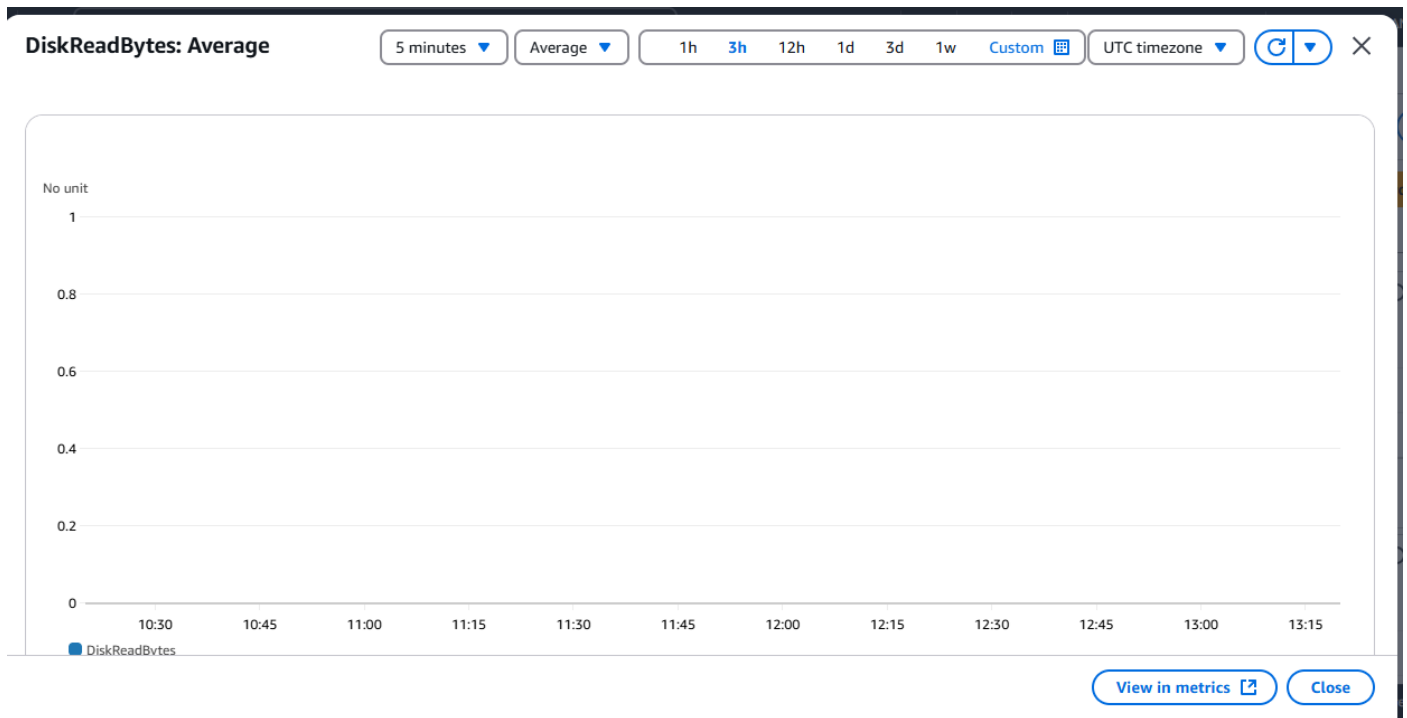
Select metrics like:

CPUUtilization (CPU usage in percentage).

DiskReadBytes and DiskWriteBytes (disk I/O activity).

Network In and Network Out (network data transfer).





Expected Outcome

By completing this POC, you will:

1. Successful setup of AWS CloudWatch to monitor key metrics like CPU usage, disk I/O, and network traffic for an EC2 instance.
2. Creation of a custom CloudWatch dashboard for real-time performance tracking.
3. Improved understanding of cloud monitoring and proactive resource management.