



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: Madhu Smitha

Department: CSE

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.

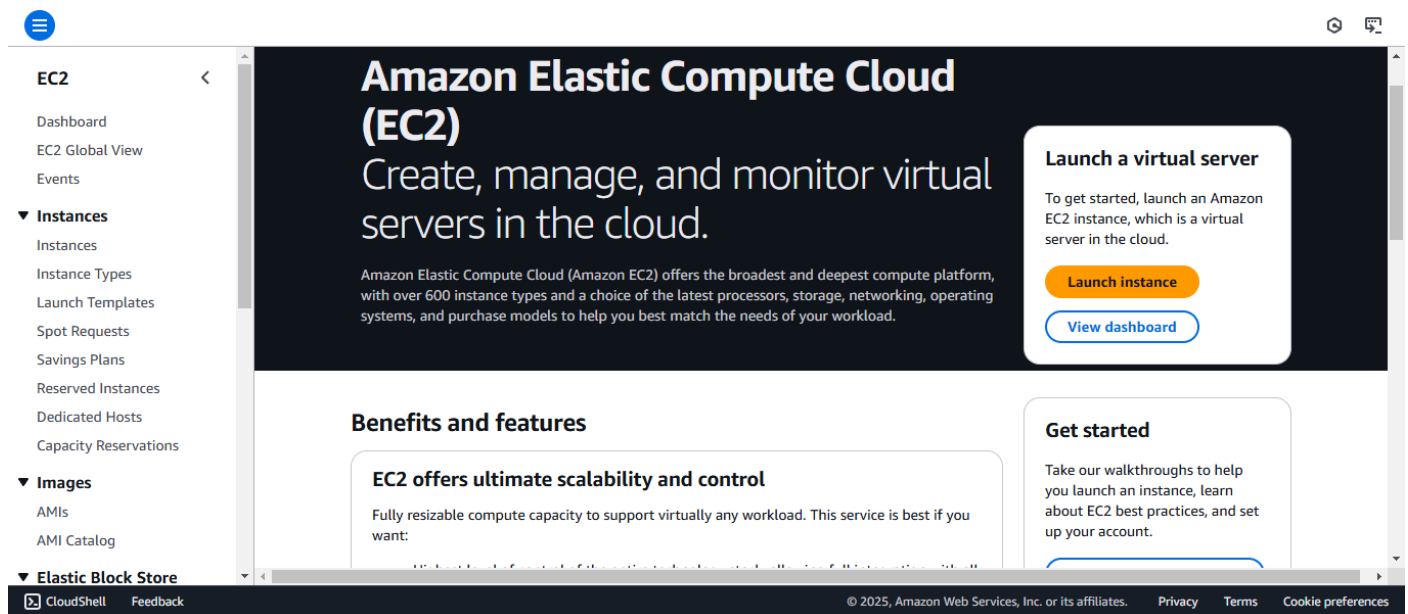
Proactive Resource Management: Enables you to monitor system performance in real-time, identify performance issues, and take corrective actions before they impact end users.

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)

aws

Search

[Alt+S]

Europe (Stockholm)

Madhu Smitha

EC2 > Instances > Launch an instance

Name and tags Info

Name

madhu_server

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Browse more AMIs

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...read more

ami-087fba4aa07ebd20f

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Cancel

Launch instance

Preview code

aws

Search

[Alt+S]

Europe (Stockholm)

Madhu Smitha

EC2 > Instances > Launch an instance

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-087fba4aa07ebd20f

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

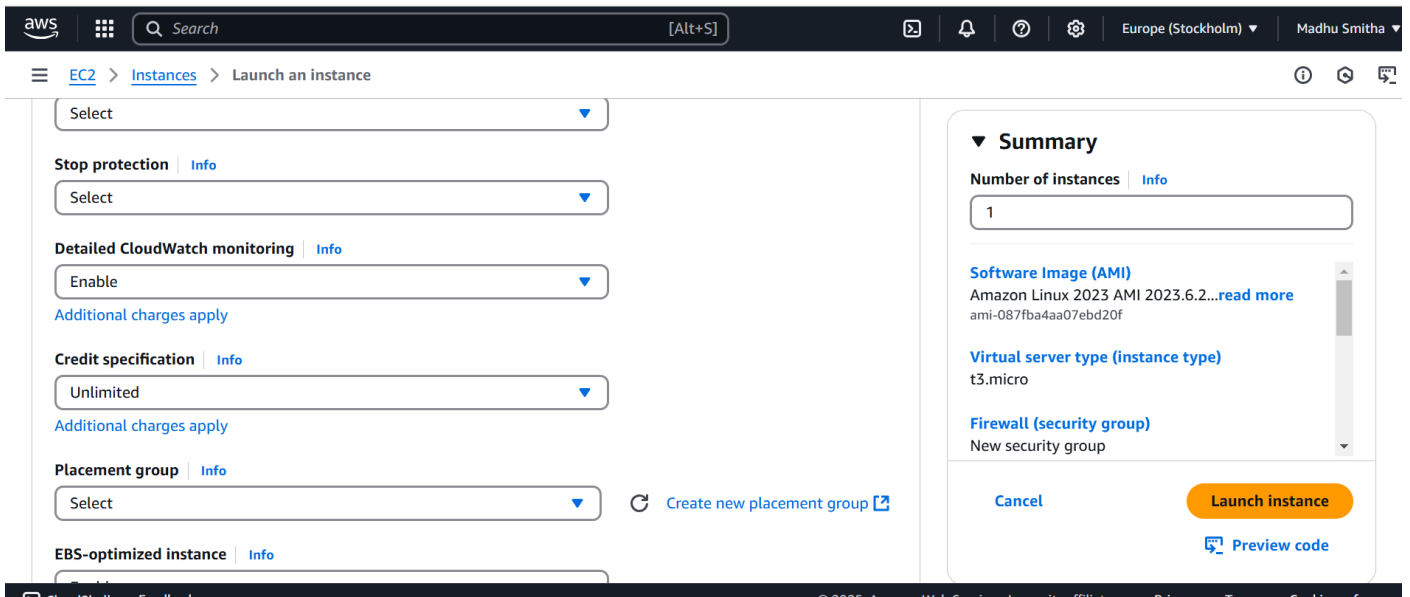
Cancel

Launch instance

Preview code

Step 3:

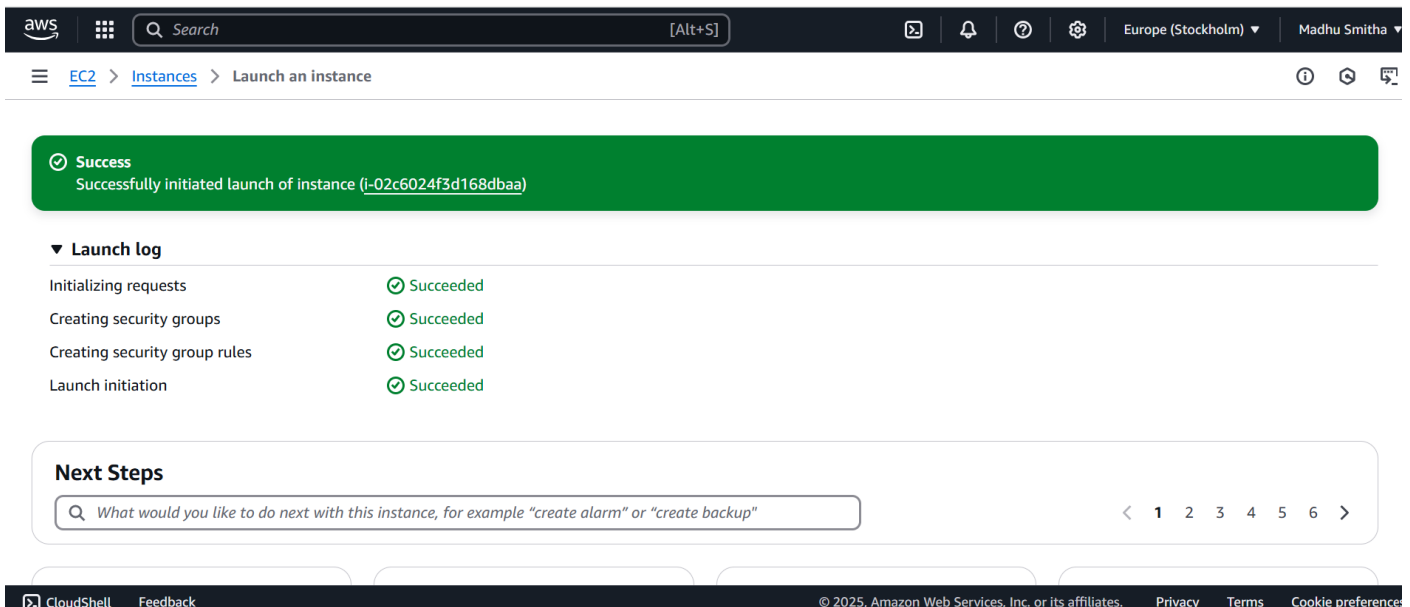
Configure the security group to allow necessary ports (e.g., SSH, HTTP, etc.).



Step 4:

Launch the instance, While launching the EC2 instance:

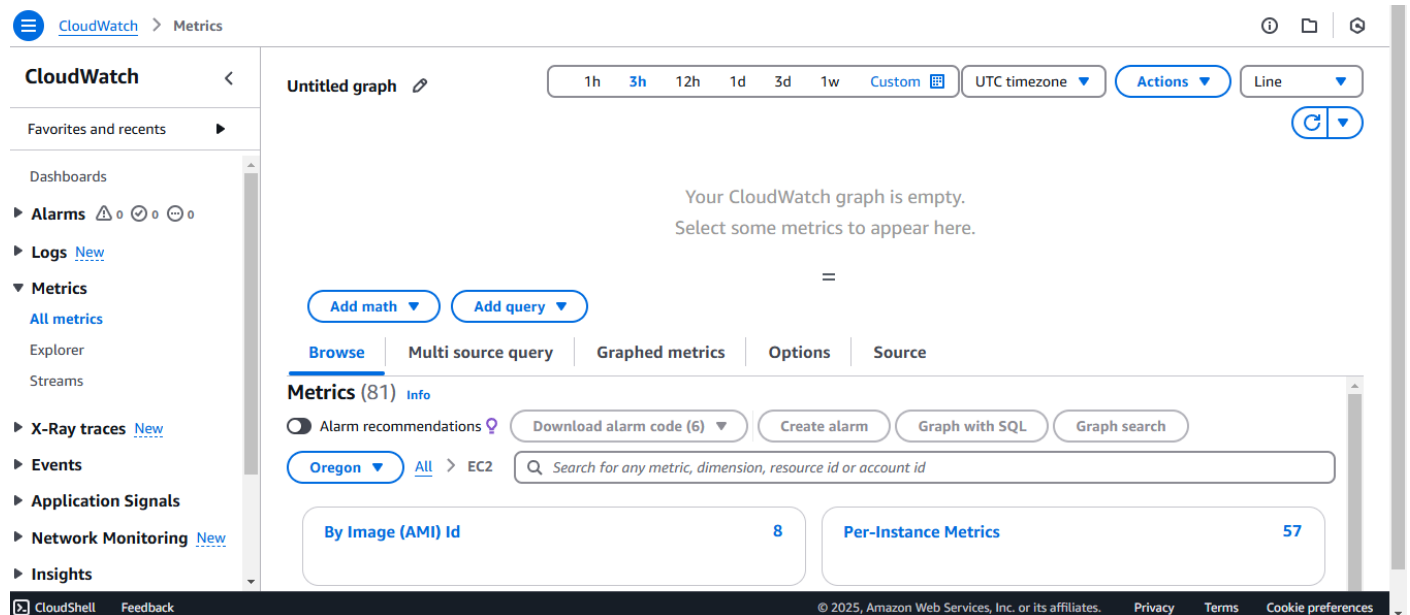
Under the "Advanced Details" section, ensure that the CloudWatch monitoring option is enabled.



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.



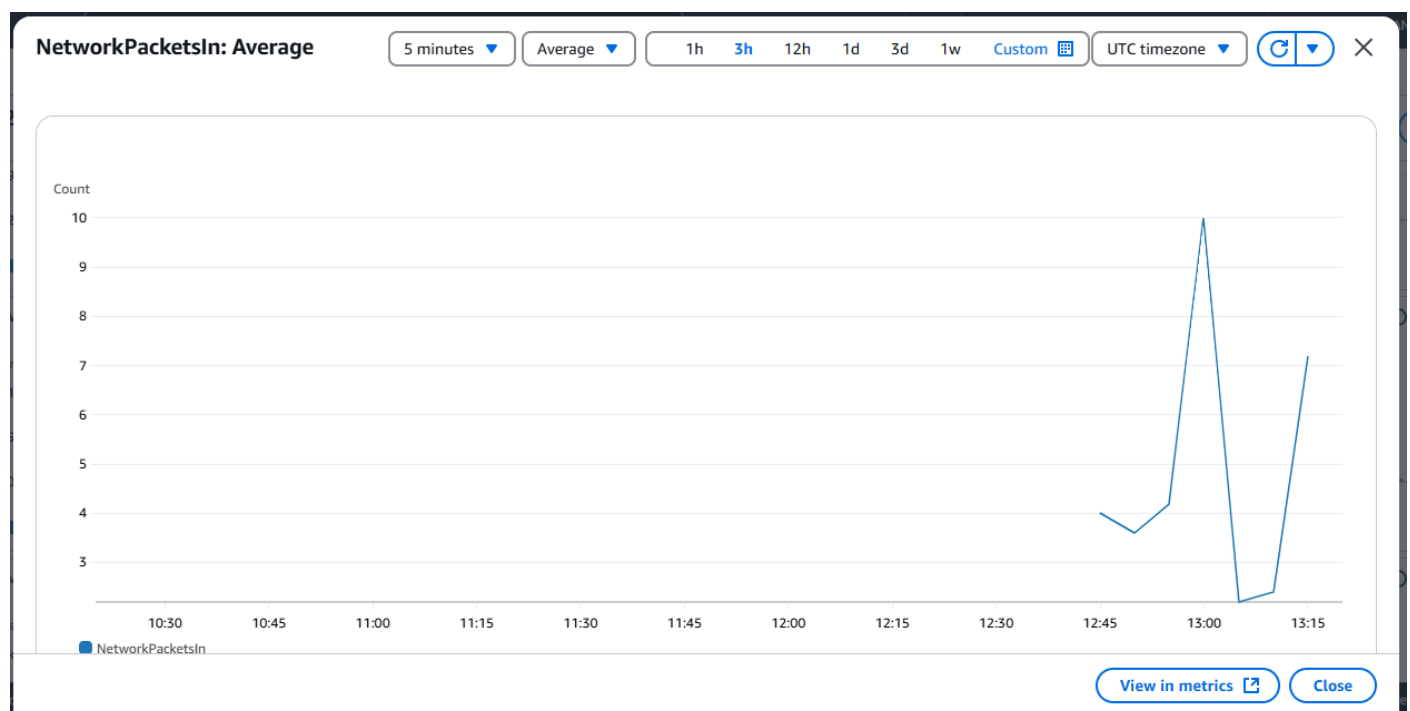
Step 6:

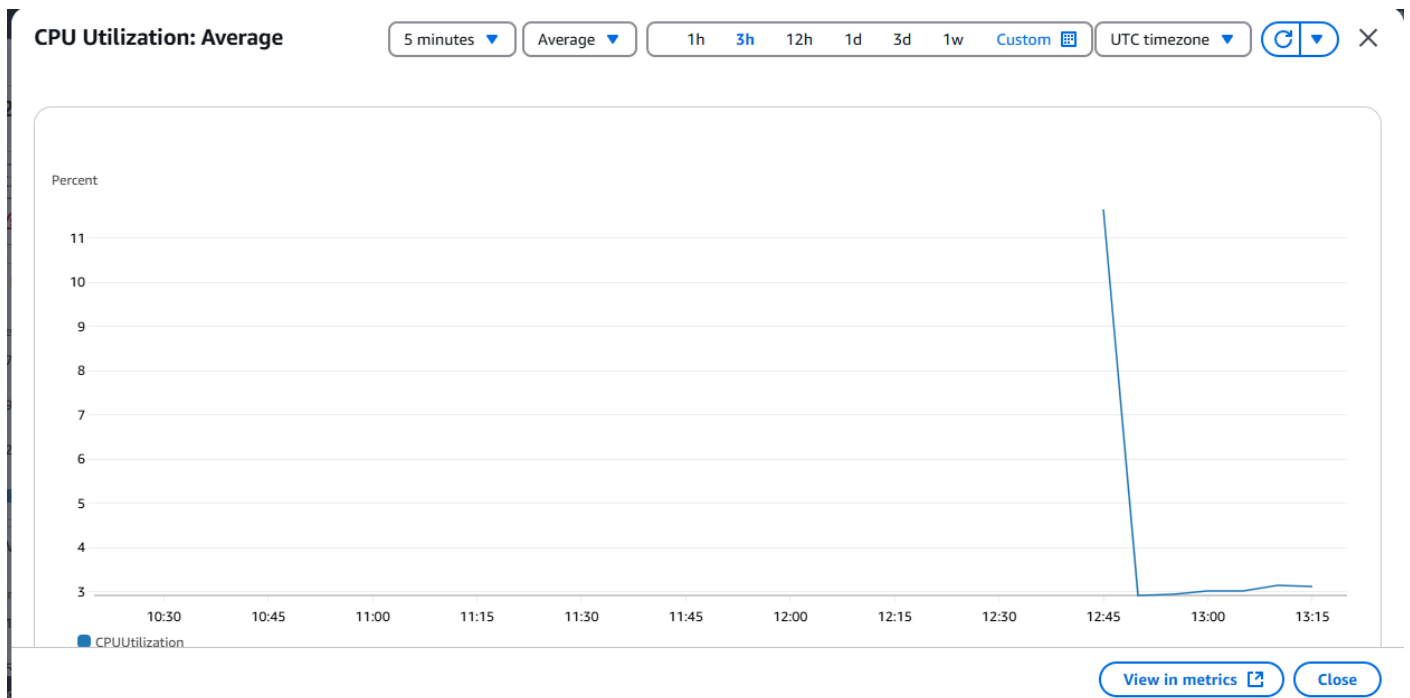
Select metrics like:

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.