



## **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:SAIRAM S

Department: IT

## 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.

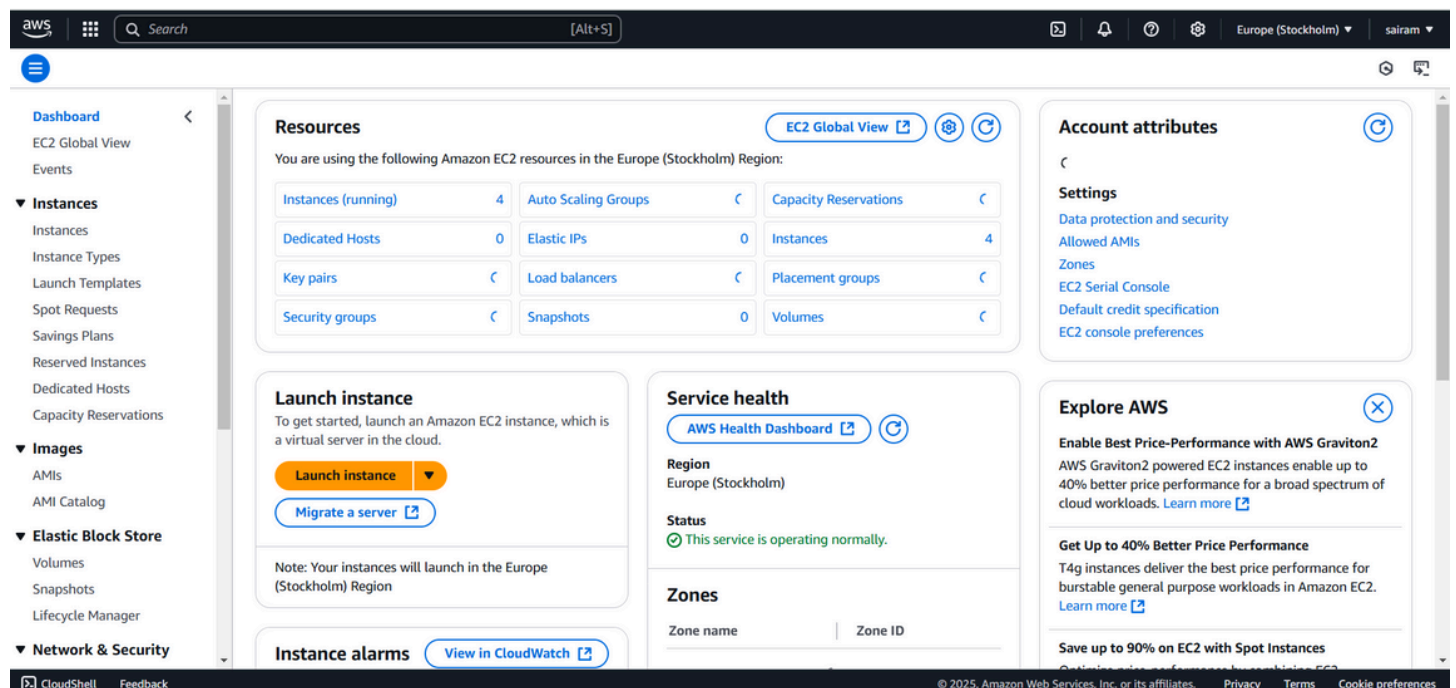
**Foundation for Automation:** Lays the groundwork for automating monitoring processes, such as setting up alerts and scaling actions, which are critical for

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) sairam

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

 [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  
aws

macOS  
Mac

Ubuntu  
ubuntu

Windows  
Microsoft

Red Hat  
Red Hat

SUSE Linux  
SUSE

Debian  
debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

### ▼ Summary

Number of instances [Info](#)

**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

**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 IP address usage.

Cancel [Launch instance](#) [Preview code](#)

### ▼ Network settings [Info](#)

**Network** [Info](#)

vpc-0b0a54fba2228213d

**Subnet** [Info](#)

No preference (Default subnet in any availability zone)

**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-6' with the following rules:

☒ Allow SSH traffic from  
Helps you connect to your instance

☐ 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

Anywhere  
0.0.0.0/0

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](#)

**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

**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 IP address usage.

Cancel [Launch instance](#) [Preview code](#)

## Step 3:

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

Shutdown behavior | Info

Stop

Stop - Hibernate behavior | Info

Select

Termination protection | Info

Select

Stop protection | Info

Select

Detailed CloudWatch monitoring | Info

Enable

Additional charges apply

Credit specification | Info

Standard

Placement group | Info

Select

Create new placement group

EBS-optimized instance | Info

Enable

Summary

Number of instances | Info

1

Software Image (AMI)  
Amazon Linux 2023.6.2...read more  
ami-087fb4aa07ebd20f

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

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 are month 750 hours of public IP.

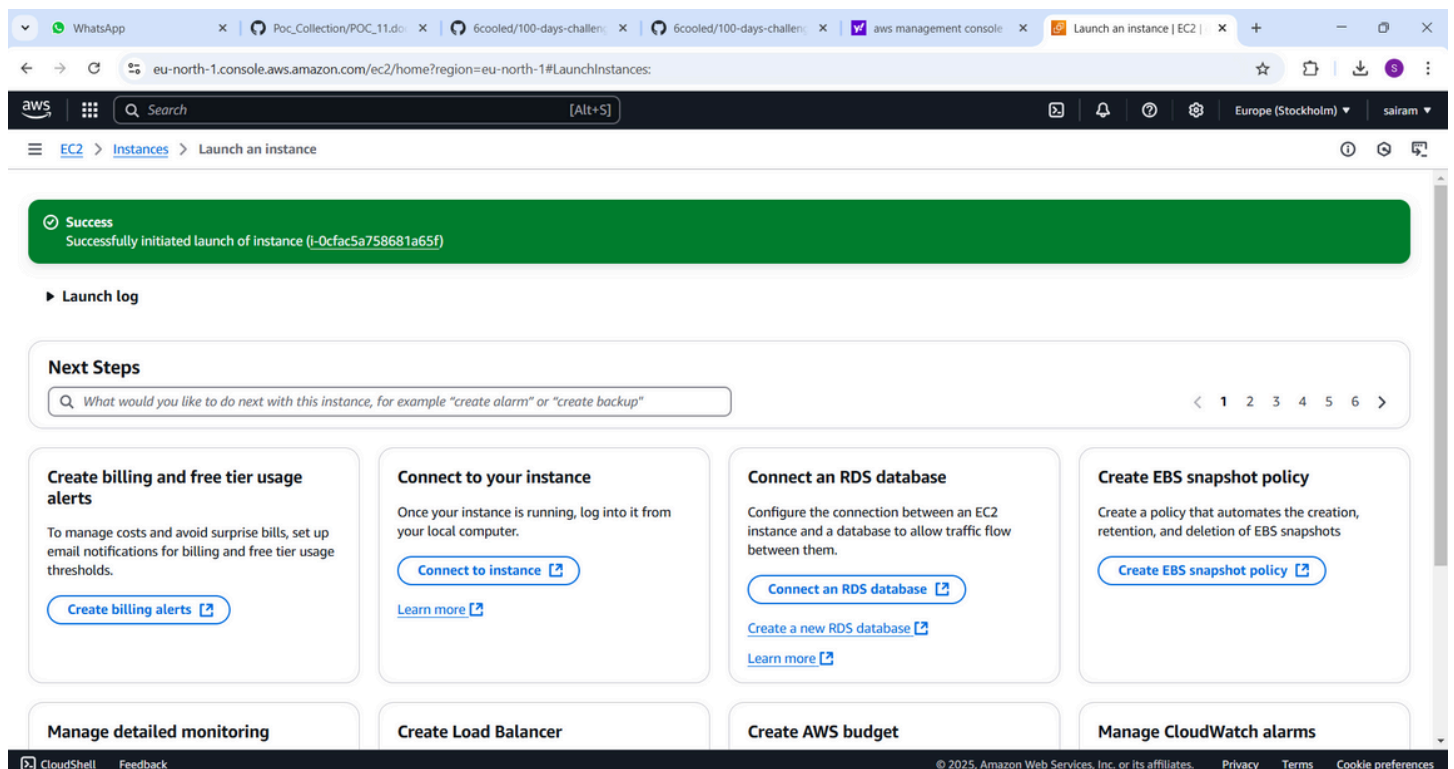
Cancel

Launch instance

Preview code

### Step 4:

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



The screenshot shows the AWS Management Console for the eu-north-1 region. The main content area displays the 'Instances (1/1)' page. A table lists the instance 'mycloudsample' with ID 'i-0cfac5a758681a65f', state 'Running', type 't3.micro', and availability zone 'eu-north-1b'. Below the table, the 'Monitoring' tab is active, showing a notification about CloudWatch agent metrics. The left-hand menu includes 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'.

## 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.

The screenshot shows the AWS CloudWatch Metrics page. The 'All metrics' view is selected, displaying a grid of metric cards for various services. The left-hand menu shows 'Metrics' and 'All metrics' selected. The main content area shows a grid of metric cards for services like AmplifyHosting, CodePipeline, EBS, EC2, Events, Kinesis, Logs, and S3. The bottom of the page shows the footer with copyright information and links to Privacy, Terms, and Cookie preferences.

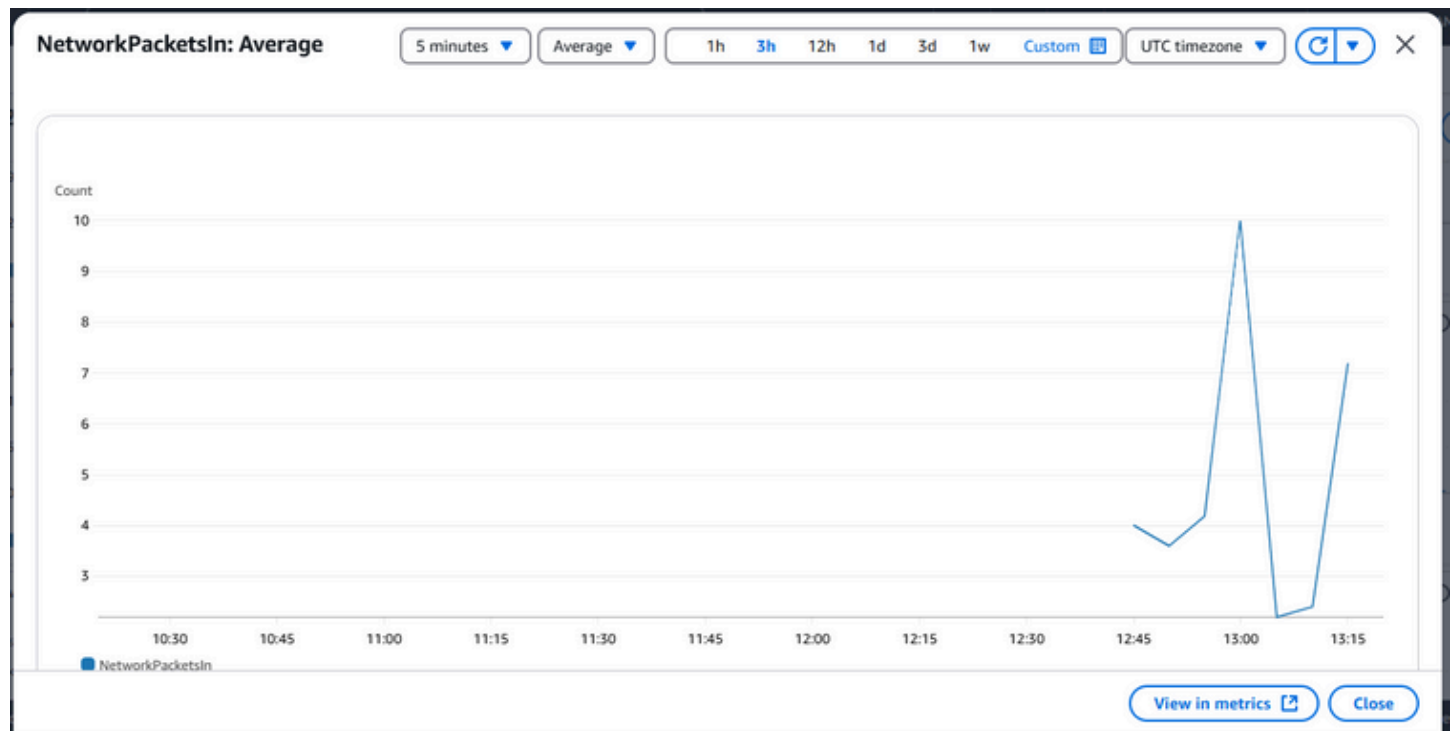
## Step 6:

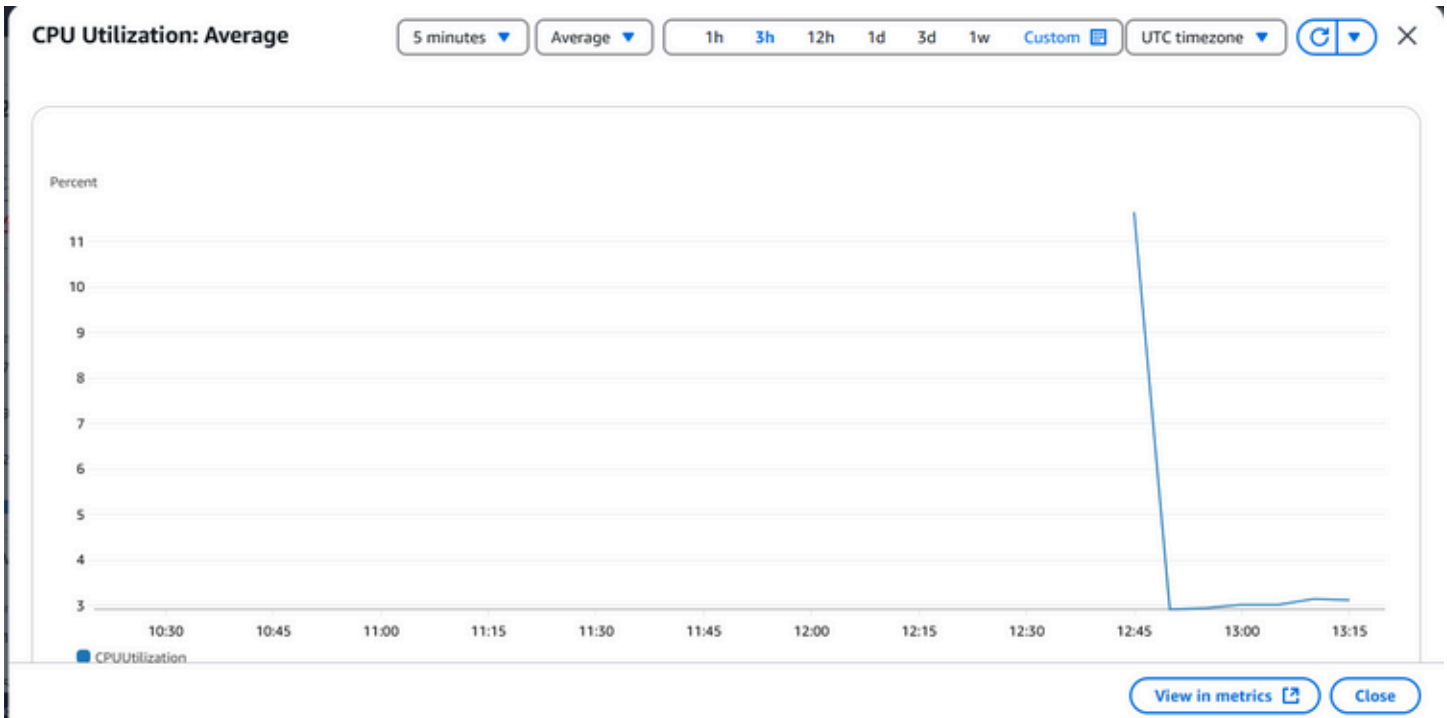
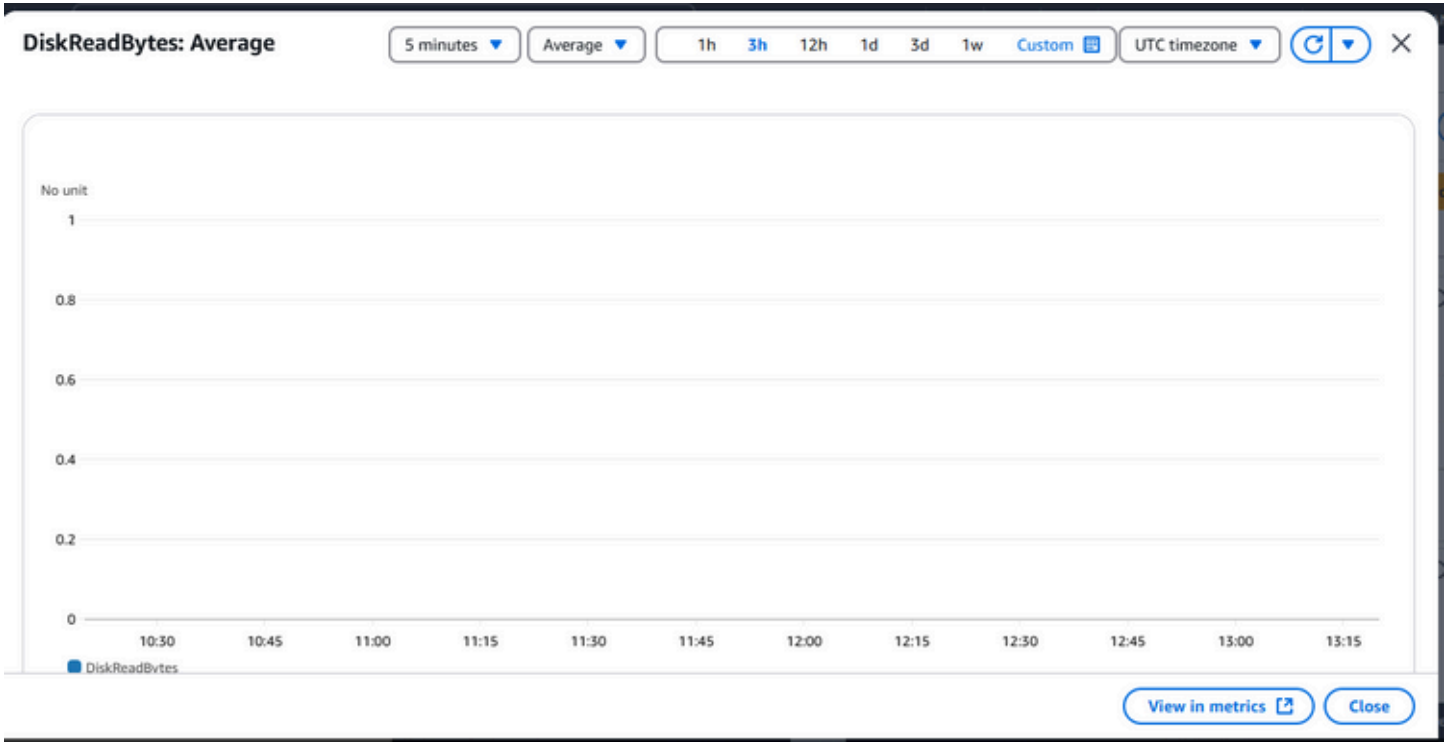
Select metrics like:

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.
1. Creation of a custom CloudWatch dashboard for real-time performance tracking.
1. Improved understanding of cloud monitoring and proactive resource management.