

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: Harshana Perianayaki B

Department: IT

INTRODUCTION

Cloud-based monitoring is essential for tracking the performance, health, and availability of cloud resources. In Microsoft Azure, **Azure Monitor** is a powerful service that enables real-time insights into virtual machines (VMs), applications, and infrastructure. By enabling monitoring, users can view key metrics such as CPU usage, disk I/O, and network activity, helping them maintain optimal system performance.

OBJECTIVES

The primary objectives of this setup include:

- Enabling **Azure Monitor** for real-time metric tracking.
- Viewing key performance indicators such as **CPU usage**, **disk I/O**, and **network traffic**.
- Setting up **alerts** to notify administrators of potential issues.
- Enhancing **visibility and troubleshooting** for Azure VMs.

OVERVIEW

Azure Monitor collects and analyzes telemetry data from various cloud resources, providing a centralized view of performance. This service includes **Azure Metrics**, **Azure Logs**, and **Alerts**, which enable proactive troubleshooting and automation. For

virtual machines, **Azure Monitor Insights** provides a deeper analysis of system health and resource utilization.

IMPORTANCE

Monitoring cloud resources is crucial for:

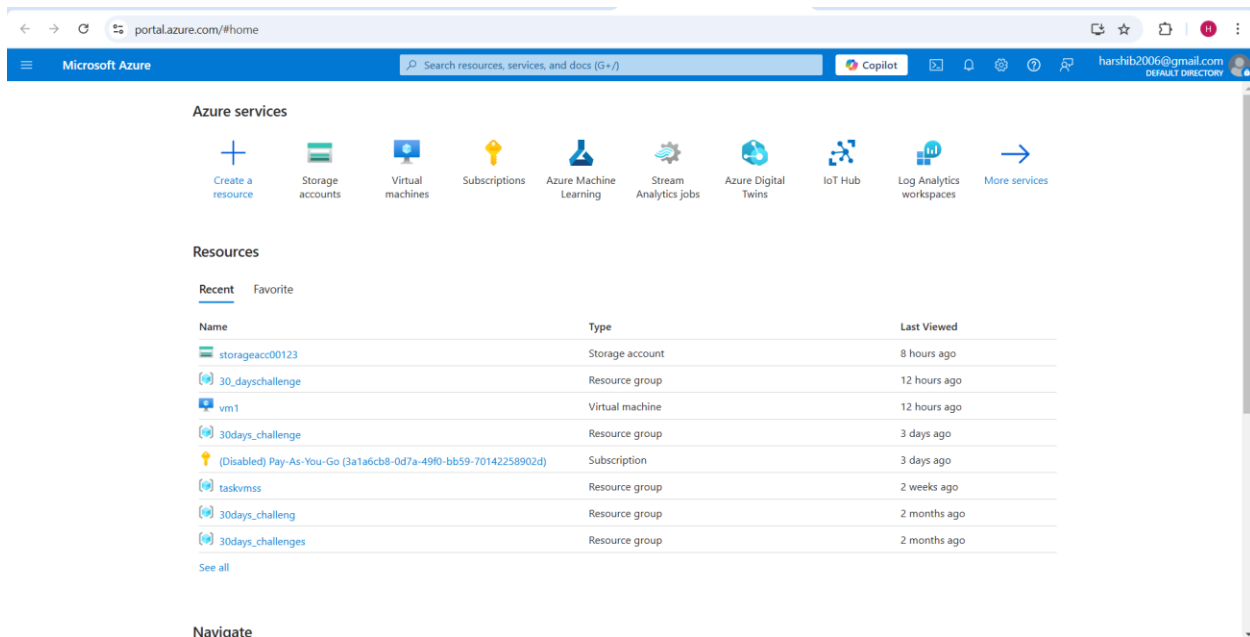
- **Performance Optimization:** Ensures that VMs run efficiently without excessive resource usage.
- **Cost Management:** Helps identify underutilized resources to reduce expenses.
- **Security & Compliance:** Detects unusual activity that may indicate security threats.
- **Proactive Issue Resolution:** Alerts enable quick responses before minor issues escalate.

STEP-BY-STEP OVERVIEW

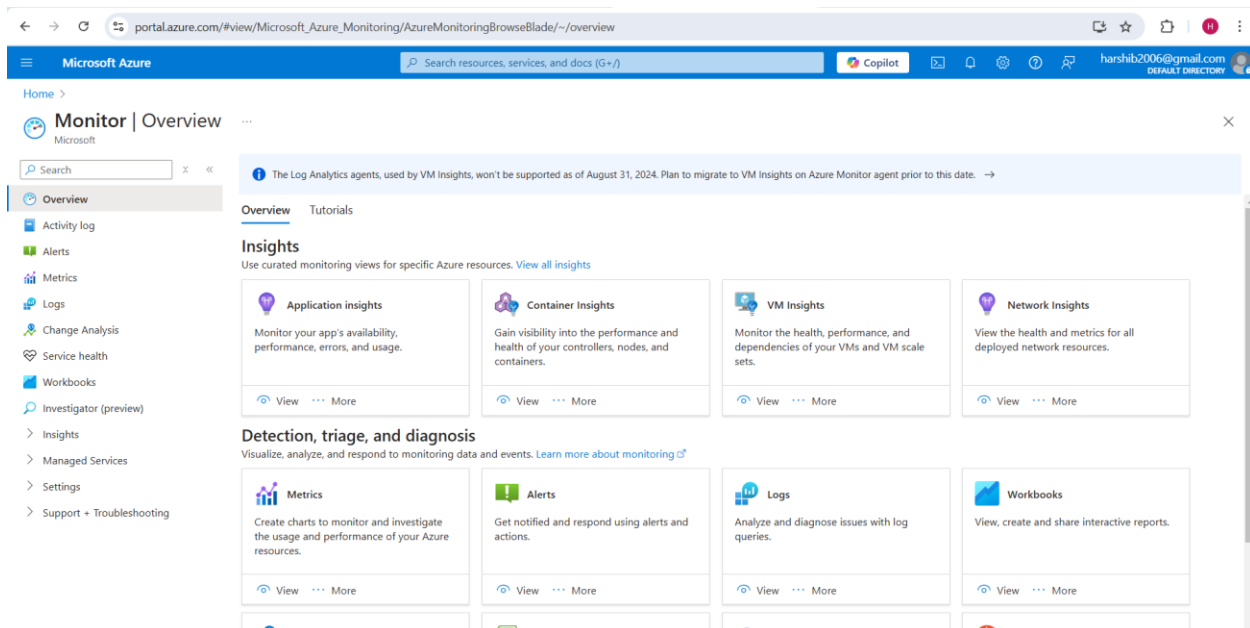
In Azure, you can set up a cloud-based monitoring service using **Azure Monitor** to track metrics like CPU usage and disk I/O for your cloud Virtual Machines (VMs). Here's how you can enable basic monitoring:

Step 1: Enable Monitoring in Azure Monitor

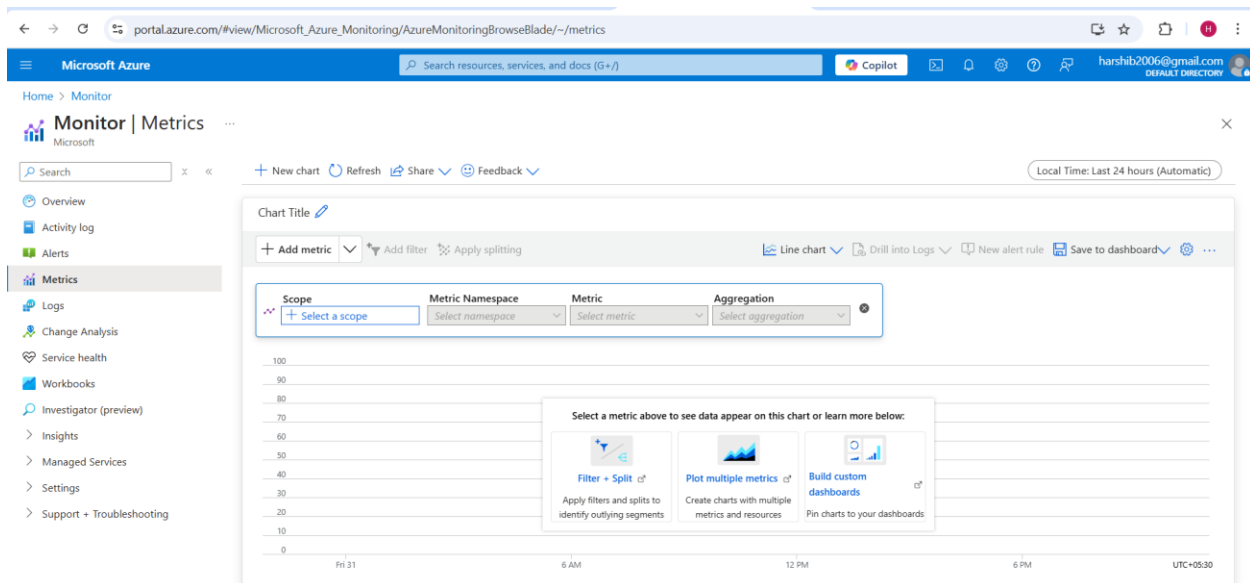
1. Go to Azure Portal



2. **Navigate to "Monitor"**: In the search bar, type "Monitor" and select it.



3. **Click on "Metrics"**: This allows you to view performance metrics for your VM.



Step 2: Enable Monitoring for Your VM

1. Go to **"Virtual Machines"** in the Azure portal.
2. Select the VM you want to monitor.

portal.azure.com/#@harshib2006gmail.onmicrosoft.com/resource/subscriptions/21b1c014-8356-4dca-ad53-ab5d71f790d7/resourceGroups/30_dayschallenge/providers/Microsoft.Compu...

Microsoft Azure

Home > vm1 Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

Advisor (1 of 1): Enable virtual machine replication to protect your applications from regional outage →

Help me copy this VM in any region

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Essentials

Resource group (move): 30_dayschallenge

Status: Running

Location: East US (Zone 1)

Subscription (move): Pay-As-You-Go

Subscription ID: 21b1c014-8356-4dca-ad53-ab5d71f790d7

Availability zone: 1

Tags (edit): Add tags

Operating system: Linux (ubuntu 24.04)

Size: Standard_B1s

Public IP address: -

Virtual network/subnet: -

DNS name: -

Health state: -

Time created: 1/31/2025, 1:17 AM UTC

JSON View

Properties Monitoring Capabilities (7) Recommendations (1) Tutorials

Virtual machine

Computer name: vm1

Operating system: Linux (ubuntu 24.04)

VM generation: V2

Networking

Public IP address: -

Public IP address (IPv6): -

Private IP address: -

3. In the left menu, click on "Monitoring" > "Insights".

portal.azure.com/#@harshib2006gmail.onmicrosoft.com/resource/subscriptions/21b1c014-8356-4dca-ad53-ab5d71f790d7/resourceGroups/30_dayschallenge/providers/Microsoft.Compu...

Microsoft Azure

Home > vm1

vm1 | Insights Virtual machine

Search

tags

Diagnose and solve problems

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Logs

Workbooks

Automation

Resource Group Monitoring Azure Monitor Diagnose and solve problems Refresh Monitoring configuration Provide Feedback

Get more visibility into the health and performance of your virtual machine

With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance and dependencies for your virtual machines.


You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the virtual machine and the monitoring data to appear.

The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please [click here](#).

Enable

https://aka.ms/vminights/ui/links/mapOverview

4. Click "Enable" to start collecting performance metrics.



Enable

Having difficulties enabling Azure Monitors for VM? [Troubleshoot](#)

Have more questions?
[Learn more about virtual machine monitoring](#)
[What is VM Insights?](#)
[Learn more about pricing](#)
[Support Matrix](#)
[FAQ](#)
[Update Azure Agent](#)

portal.azure.com/#@harshib2006gmail.onmicrosoft.com/resource/subscriptions/21b1c014-8356-4dca-ad53-ab5d71f790d7/resourceGroups/30_dayschallenge/providers/Microsoft.Compu...

Monitoring configuration

VM Insights now supports data collection using the Azure Monitor Agent and data collection rules.

Subscription * Pay-As-You-Go (21b1c014-8356-4dca-ad53-ab5d71f790d7)

Data collection rule (new) MSVMI-DefaultWorkspace-21b1c014-8356-4dca-ad53-ab5d71f790d7-EUS [Create New](#)

MSVMI-DefaultWorkspace-21b1c014-8356-4dca-ad53-ab5d71f790d7-EUS

Guest performance	Enabled
Processes and dependencies (Map)	Disabled
Log Analytics workspace	DefaultWorkspace-21b1c014-8356-4dca-ad53-ab5d71f790d7-EUS

Enable

Having difficulties enabling Azure Monitors for VM? [Troubleshoot](#)

Have more questions?
[Learn more about virtual machine monitoring](#)
[What is VM Insights?](#)
[Learn more about pricing](#)
[Support Matrix](#)
[FAQ](#)
[Update Azure Agent](#)

This will also enable System Assigned Managed Identity, in addition to existing User Assigned identities (if any).
Note: Unless specified in the request, the machine will default to using System Assigned Identity. [Learn More](#)
 Currently, only resources in certain regions are supported. [Learn More](#)

Configure **Cancel**

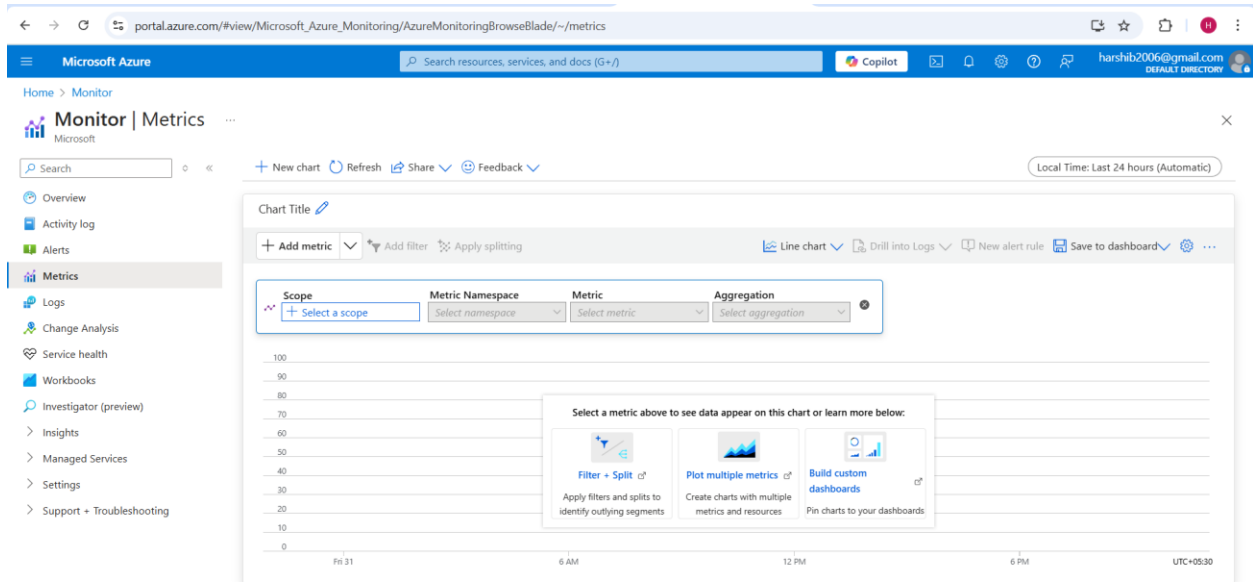
Step 3: View Basic Metrics

Once enabled, Azure Monitor will collect data such as:

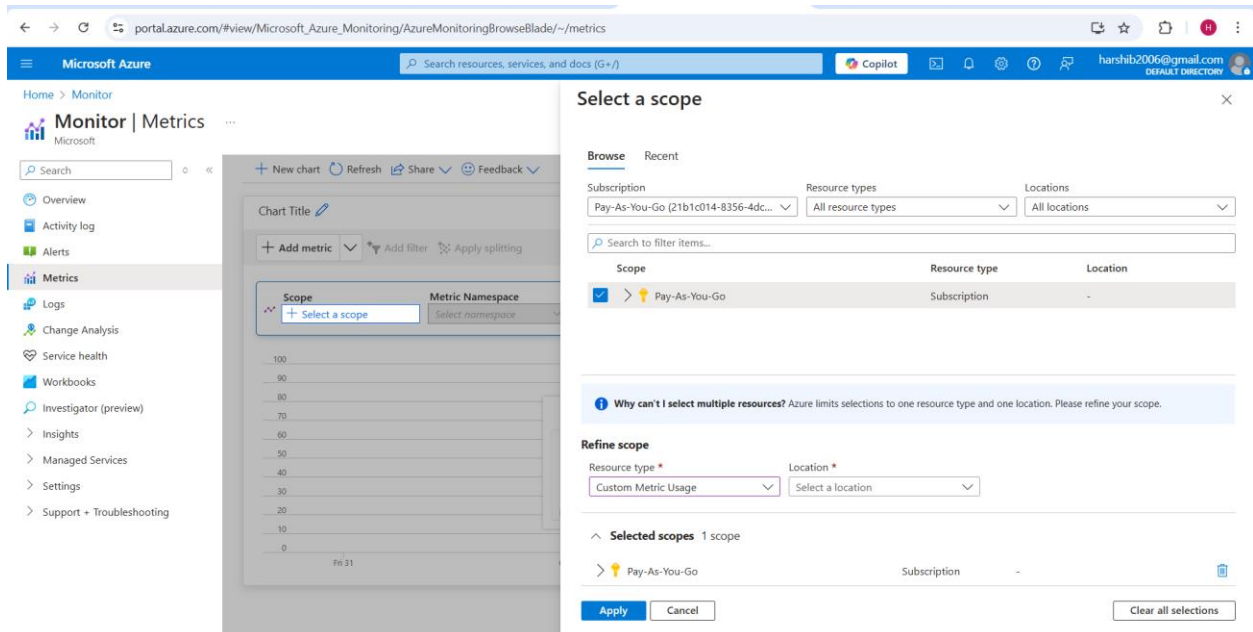
- **CPU Usage:** Measures the processor load of the VM.
- **Disk I/O:** Tracks read/write operations on the disk.
- **Network Traffic:** Monitors inbound and outbound traffic.

To view these metrics:

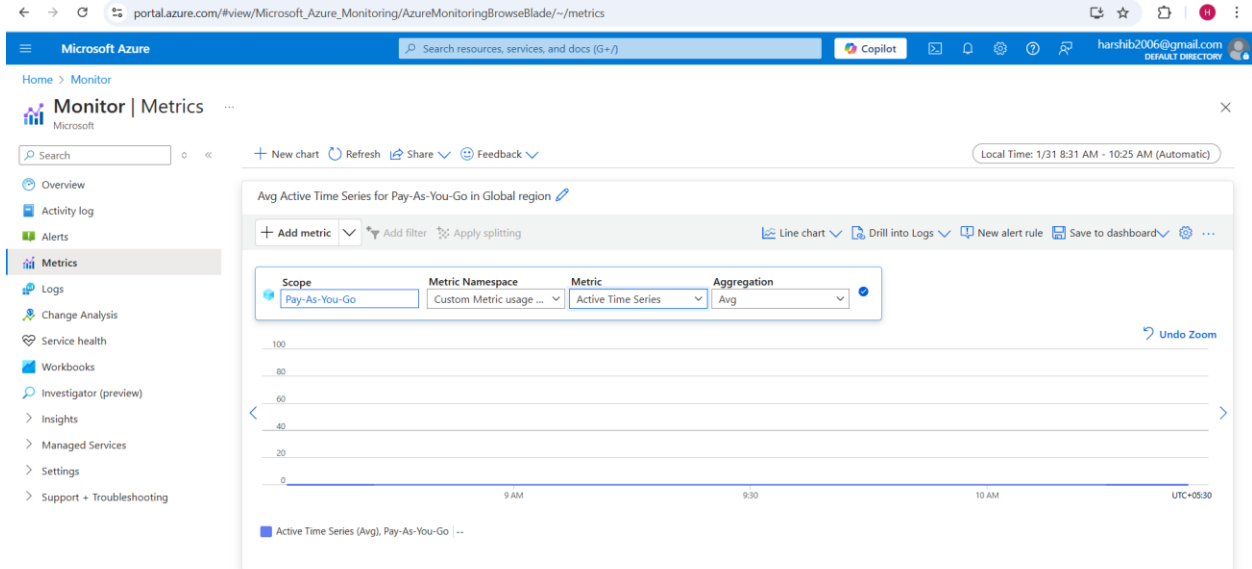
1. Go to Azure Monitor > Metrics.



2. Select the Scope (your VM).



3. Choose the **Metric Namespace**

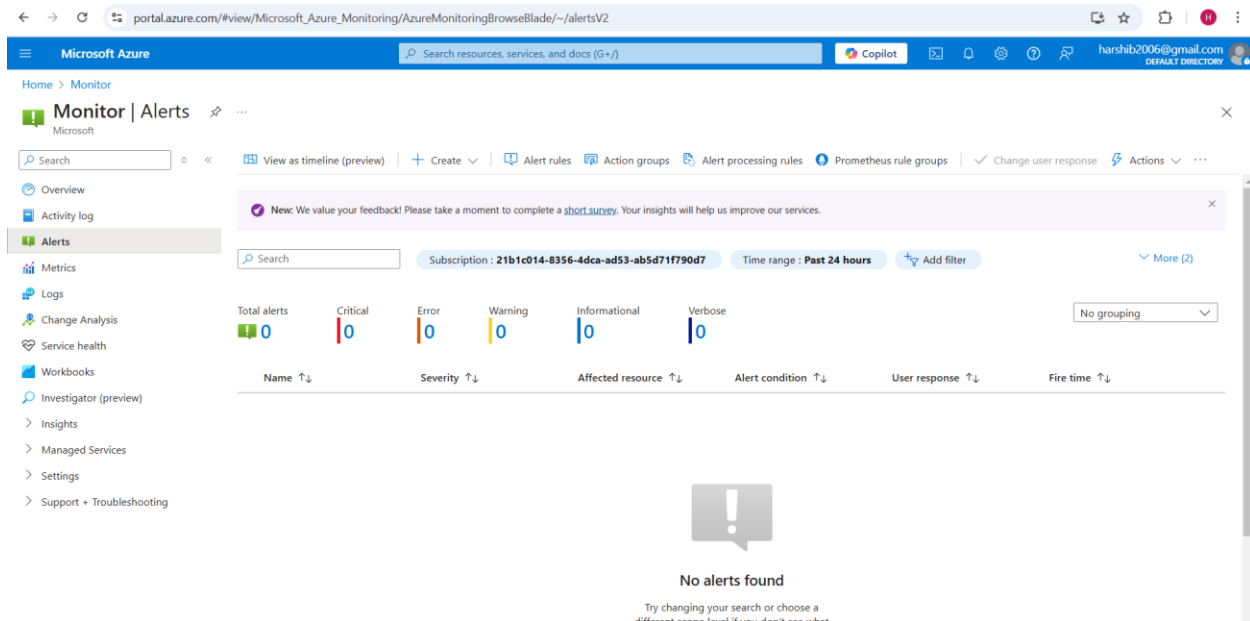


3. Select the **Metric** (e.g., CPU percentage, Disk I/O).

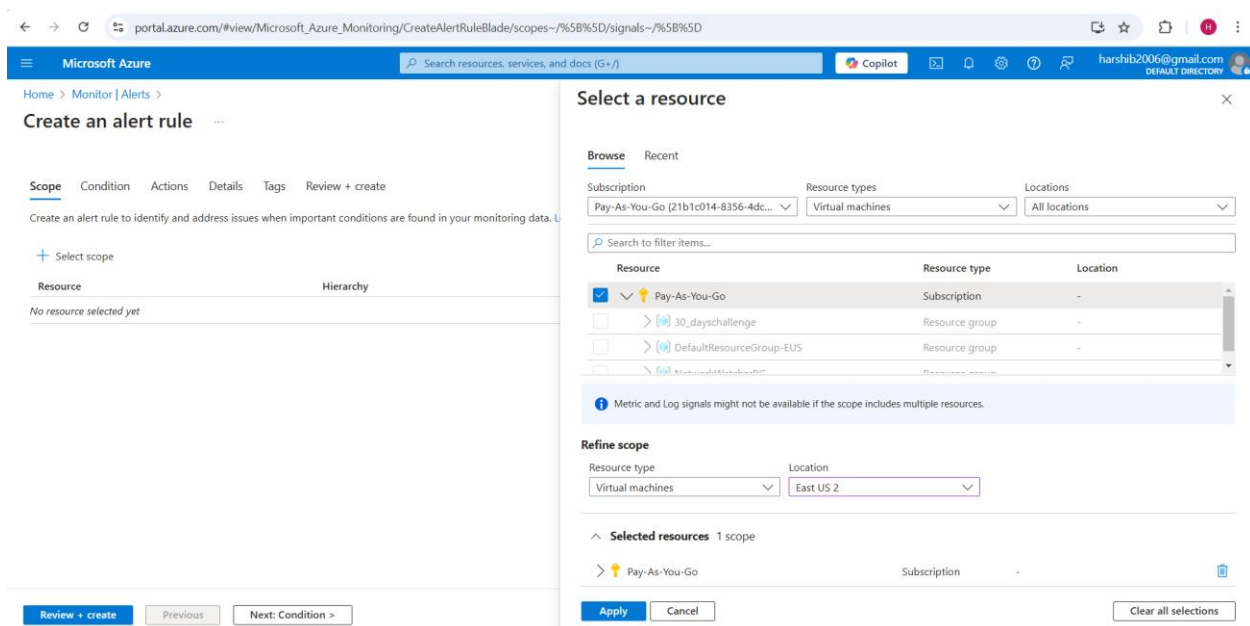
Step 4: Set Up Alerts (Optional)

You can set up alerts to notify you of high CPU usage or disk issues.

1. Go to Azure Monitor > Alerts.



2. Click "New alert rule".



3. Select your VM as the resource.

4. Choose a signal (e.g., CPU percentage > 80%).

portal.azure.com/#view/Microsoft_Azure_Monitoring/CreateAlertRuleBlade/scopes~/%5B%5D/signals~/%5B%5D

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Monitor | Alerts >

Create an alert rule

Scope Condition Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * [See all signals](#)

Alert logic

1 We have set the condition configuration automatically based on popular settings for this metric. Please review and make changes as needed.

Threshold type ☒ Static ☐ Dynamic

Aggregation type

Value is

Threshold * %

Split by dimensions

Use dimensions to monitor specific time series and provide context to the fired alert. [About monitoring multiple time](#)

Preview \$0.00 USD/month

Whenever the average Percentage CPU is greater than 80%

Preview time range : **Over the last 6 hours** Time series : None

100
90
80
70
60
50
40
30

[Review + create](#) [Previous](#) [Next: Actions >](#)

5. Set up an **Action Group** to receive email or SMS alerts.

portal.azure.com/#view/Microsoft_Azure_Monitoring_Alerts/CreateActionGroupBlade/subscriptionId/21b1c014-8356-4dca-ad53-ab5d71f790d7/subscriptionName//resourceGroupName//...

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Monitor | Alerts > Create an alert rule >

Create action group

Basics Notifications Actions Tags Review + create

This is a summary of your action group. Please review to ensure the information is correct and consider [Azure Monitoring Pricing](#) and the [Azure Privacy Statement](#).

Basics

Subscription	Pay-As-You-Go
Resource group	30_dayschallenge
Region	eastus
Action group name	action1
Display name	action1

Notifications

None

Actions

None

Tags

[Create](#) [Previous](#)

Create an alert rule ...

Scope Condition Actions Details Tags Review + create

An action group is a set of actions that can be applied to an alert rule. [Learn more](#)

+ Select action groups + Create action group

Action group name

Contains actions

action1



6. Click **Create**.

CONCLUSION:

Now our Azure VM is being monitored using **Azure Monitor**. We can view metrics and set alerts to track resource usage efficiently.

OUTCOME

By the end of this setup, We will be able to:

- Monitor Azure VM performance through the **Azure Monitor dashboard**.
- Track critical metrics for system health and efficiency.
- Detect performance bottlenecks and prevent downtime.
- Receive alerts for abnormal usage patterns, improving response time to issues.

