Monitoring and Alerting on Azure VM Performance

PROJECT SUMMARY

In this project, I designed and implemented a complete monitoring and alerting solution for a virtual machine in Microsoft Azure. The goal was to simulate real-world performance issues and validate those alerts trigger correctly when predefined thresholds are exceeded. The project focused on CPU, memory, and disk monitoring using Azure Monitor, metric alerts, and an Action Group for email notifications.

Tebogo Matseding

Table of Contents

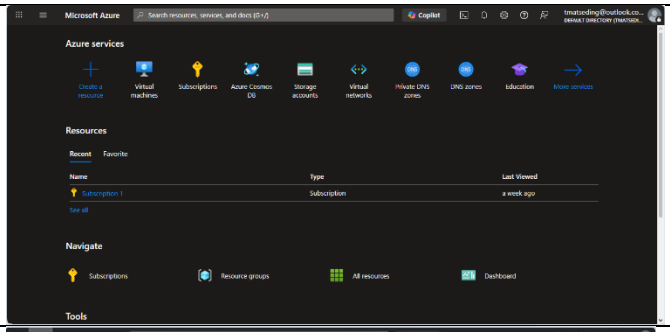
Introduction

This project focuses on implementing a cloud-based monitoring and alerting solution using Microsoft Azure. The goal was to deploy a virtual machine, configure Azure Monitor, define performance thresholds, and validate that alerts are triggered when system resources exceed acceptable limits.

Modern cloud environments rely heavily on monitoring to detect performance issues before they impact users. In this lab, I simulated a real-world scenario where CPU usage exceeds safe levels and ensured that the monitoring system successfully detected the issue and delivered an email notification.

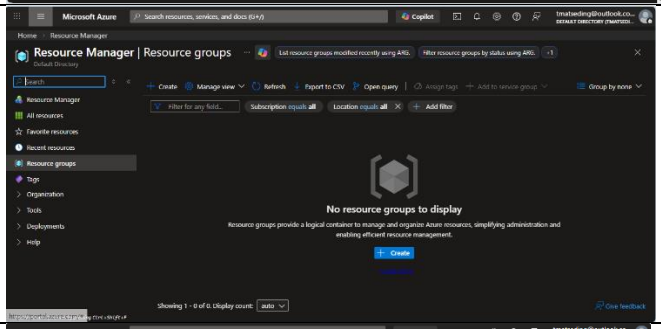
Azure Dashboard

The Azure Dashboard is the central location where all available Azure resources can be viewed and managed, depending on your subscription. This is where I began setting up and organizing the entire project.

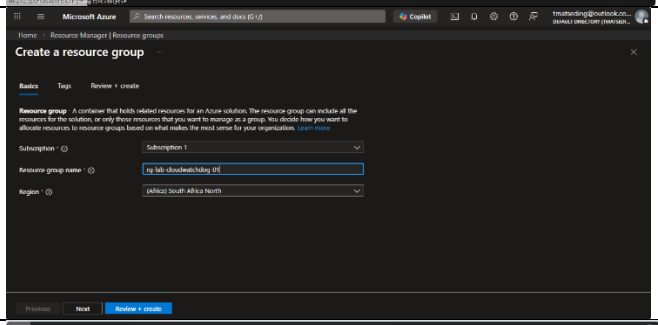


Resource Groups

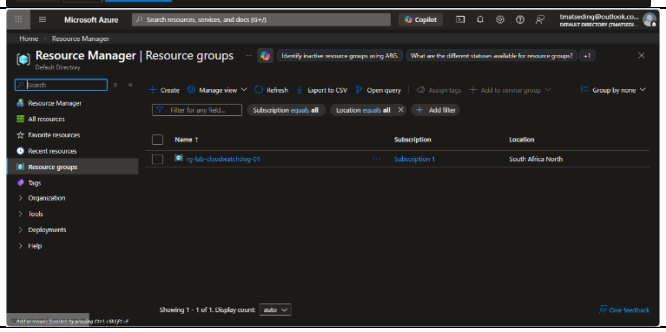
A Resource Group allows us to logically organize all related resources into one container. This makes management easier and ensures that everything related to the project can be controlled or deleted together.

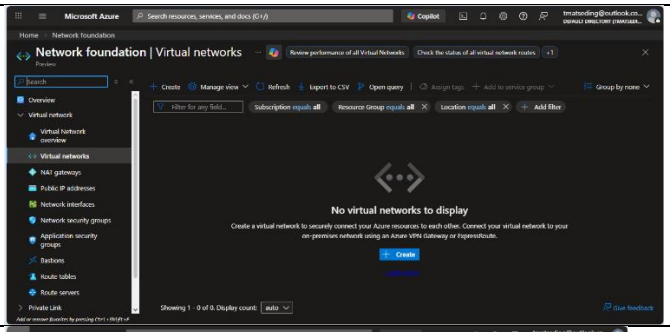
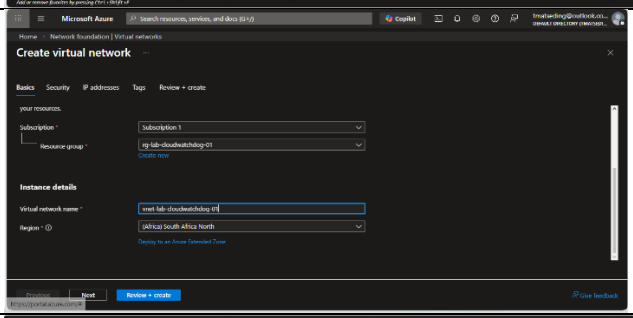
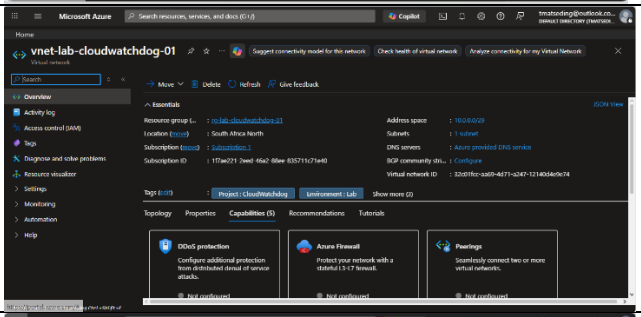
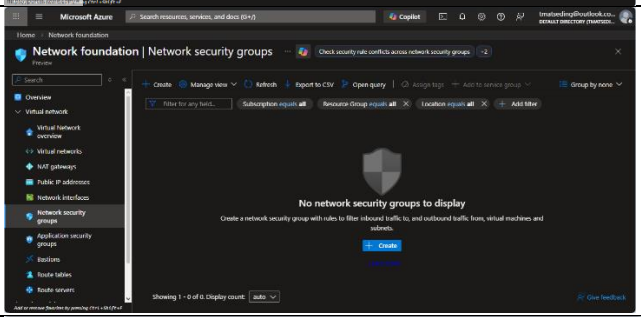
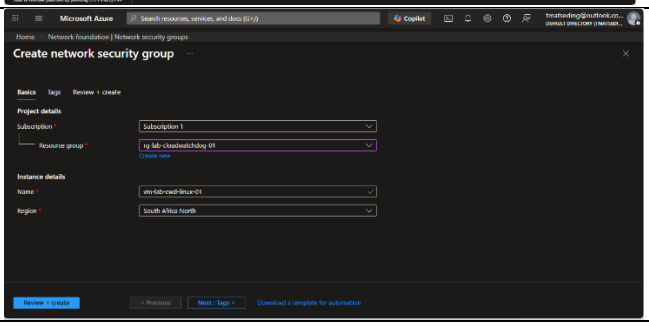


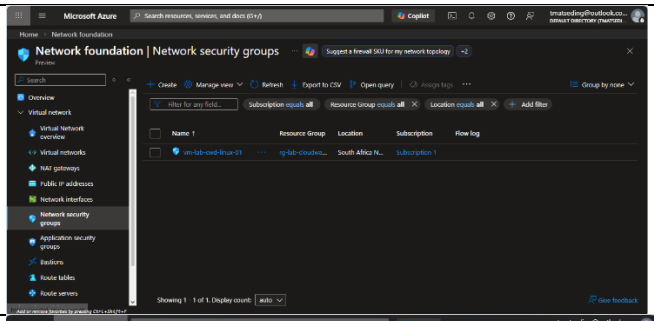
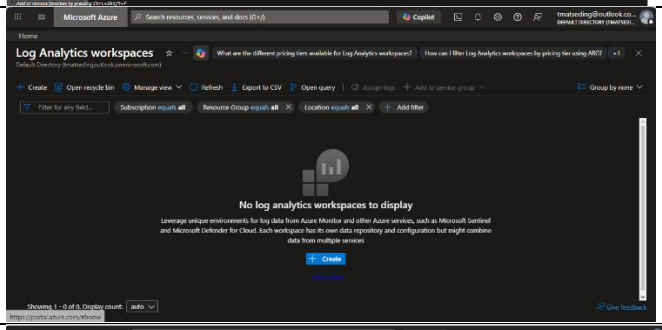
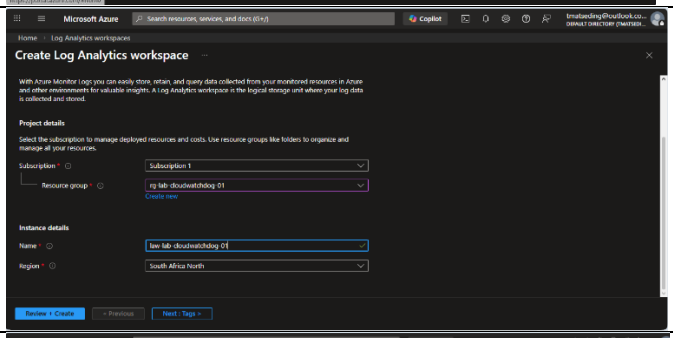
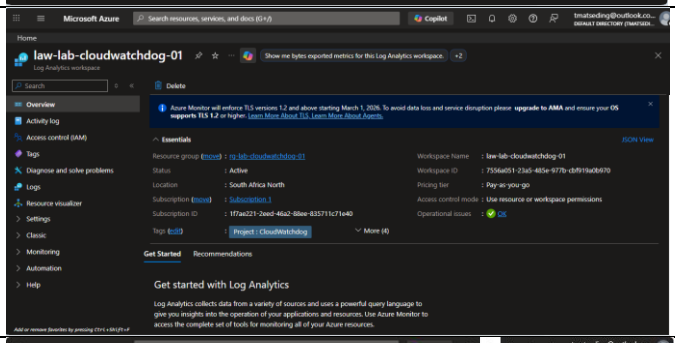
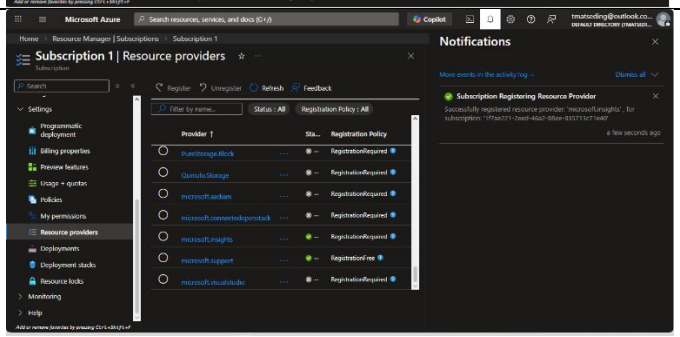
Name Resource Group

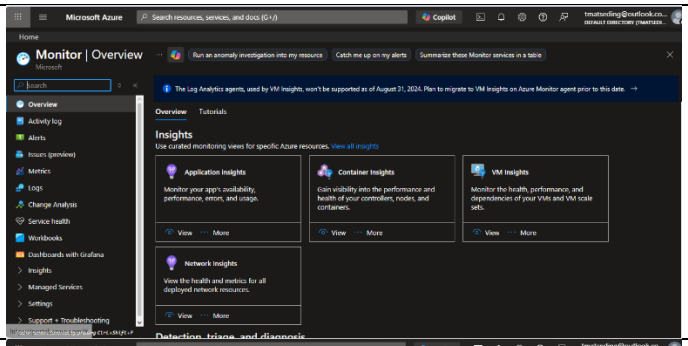
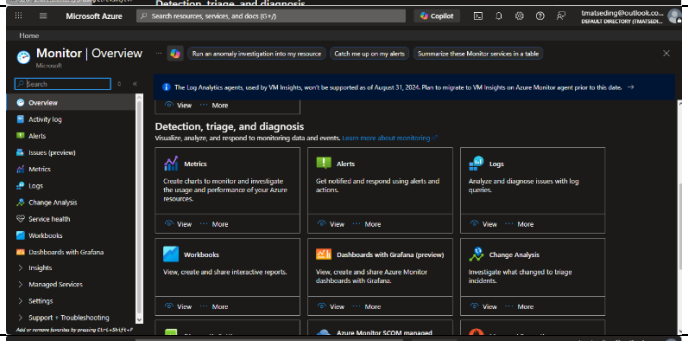
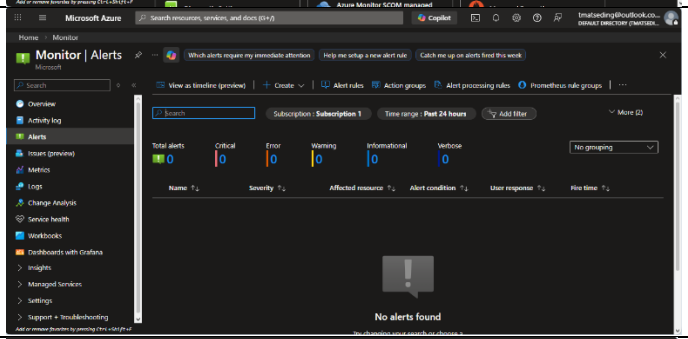
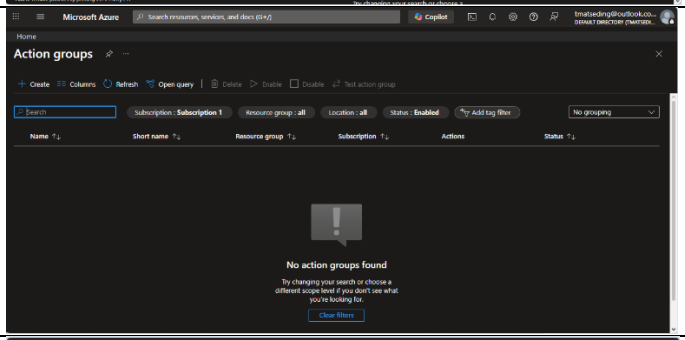
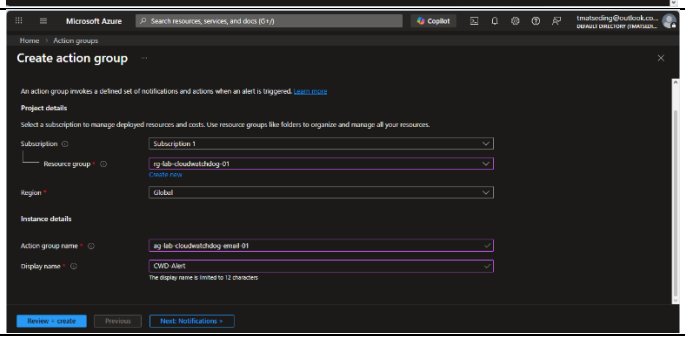


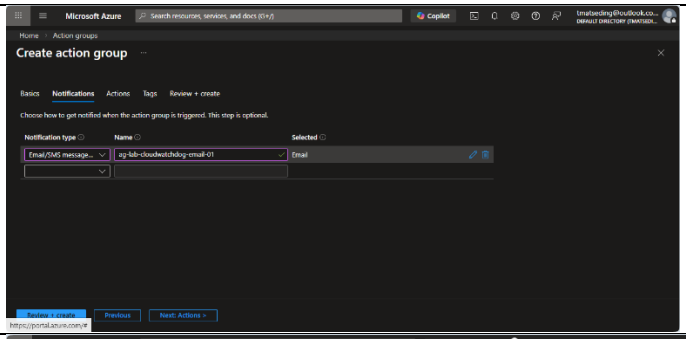
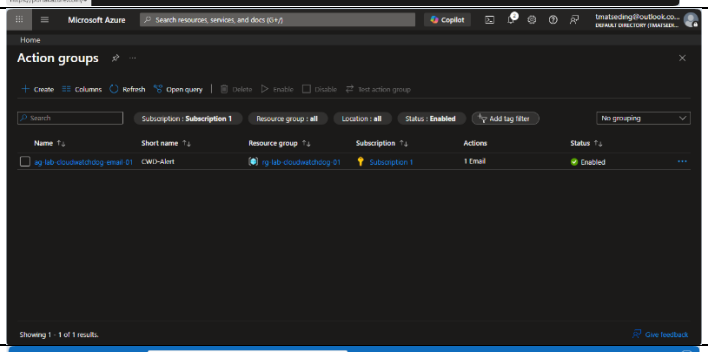
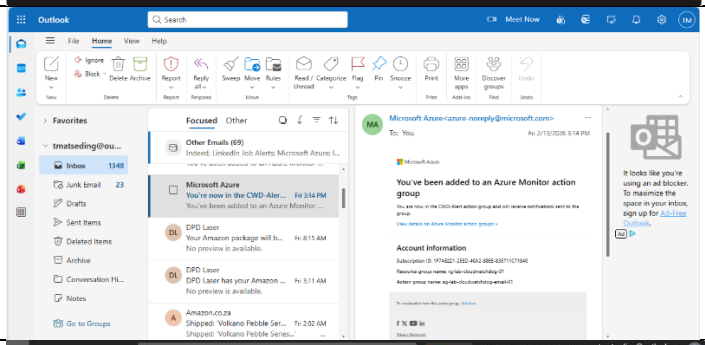
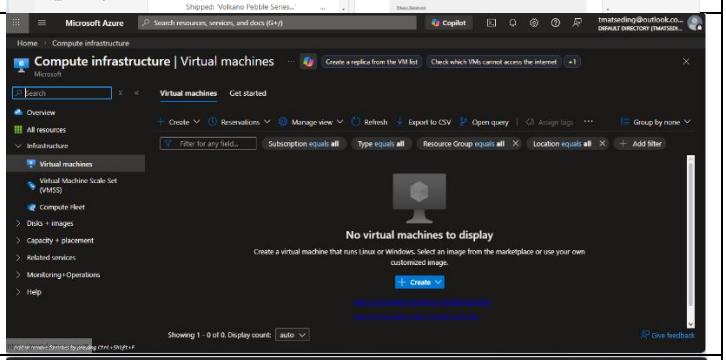
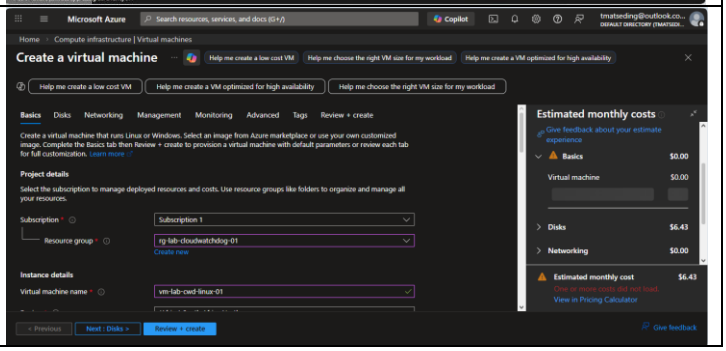
Resource Group Created

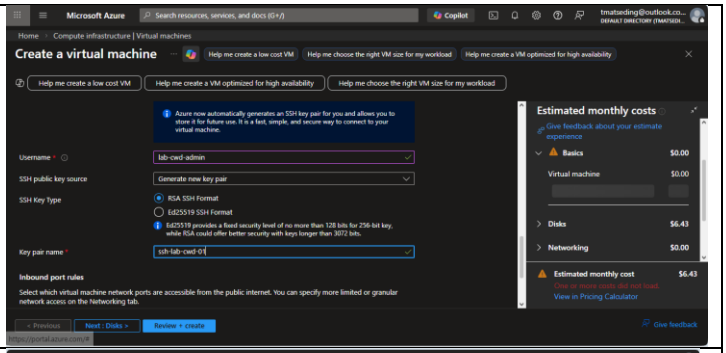
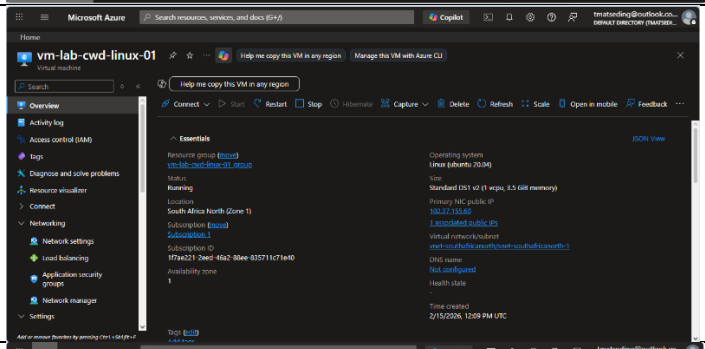
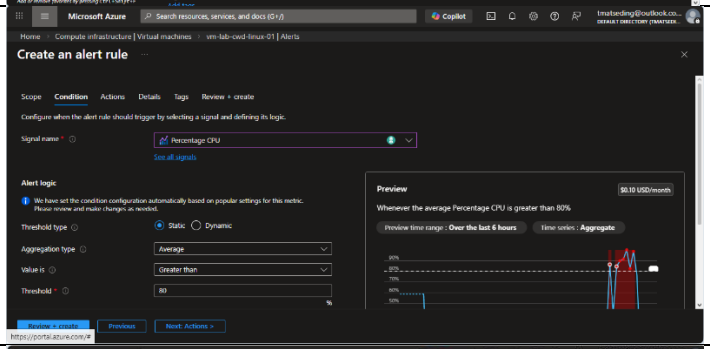
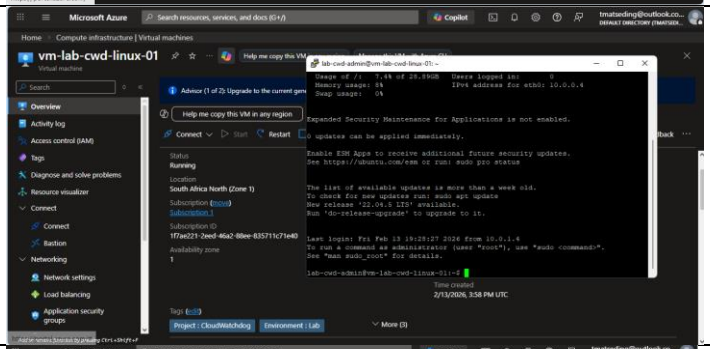
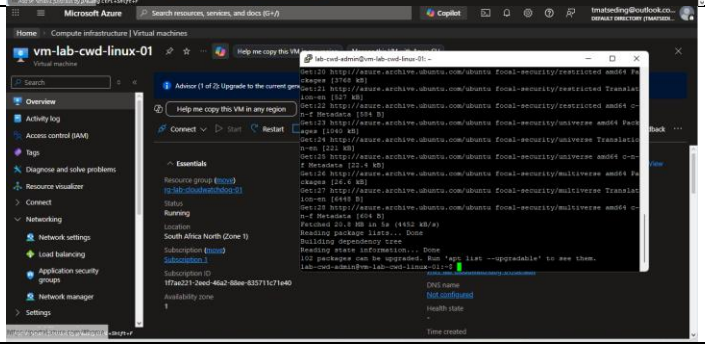


Virtual Network The Virtual Network (VNet) allows us to create a private network environment where the virtual machine will operate. This ensures proper network structure and isolation.	
Name Virtual Network	
Virtual Network Created	
Network Security Group The Network Security Group (NSG) allows us to control inbound and outbound traffic for the VM. This ensures that only required traffic, such as SSH access, is permitted.	
Name Network Security Group	

Network Security Group Created	
Log Analytics Log Analytics provides centralized visibility into performance metrics and logs for connected resources. This workspace is necessary for monitoring and alerting.	
Name Log Analytics	
Log Analytics Created	
Register Resource Provider Ensured that required resource providers, such as Microsoft.Insights, were registered in the subscription so that monitoring and alerting features would function correctly.	

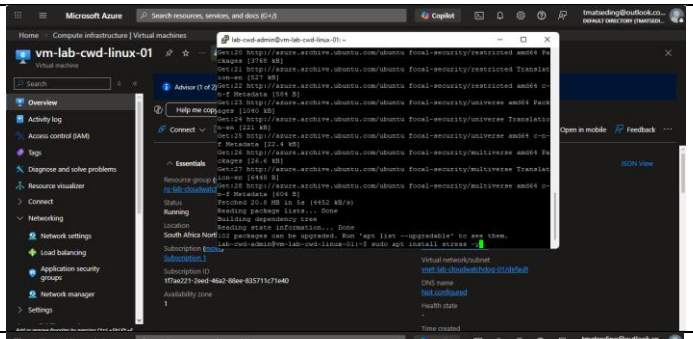
## Open Azure Monitor Accessed Azure Monitor to configure alerts, metrics, and monitoring rules.	
## Select Alerts Navigated to the Alerts section to create a new alert rule based on VM performance metrics.	
## Select Action Group Selected Action Groups to configure how notifications would be delivered when an alert is triggered.	
## Create Action Group	
## Name Action Group	

## Set up Email Alerts Configured email notification within the Action Group to receive alerts when performance thresholds are exceeded.	
## Action Group Created	
## Verify email is added to Action Group	
## Virtual Machine A Virtual Machine (VM) is a cloud-based computer that runs in Microsoft Azure instead of on physical hardware. In this project, the VM acted as the system being monitored. It was used to simulate high CPU usage so that Azure Monitor could detect the performance issue and trigger an alert.	
## Name Virtual Machine	

Create SSH Key	
Virtual Machine Created	
Create Alert Rule Created an alert rule in Azure Monitor configured to notify me when CPU usage exceeds 80%. The alert was linked to the previously created Action Group to ensure email notifications would be sent when the threshold was reached.	
Start VM using PuTTY Used PuTTY to securely connect to the virtual machine via SSH.	
Sudo Apt Update Updated the Linux package repository to ensure the system was ready for installing additional tools.	

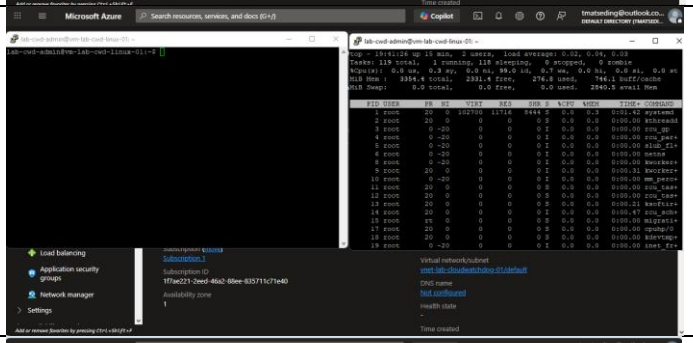
Install Stress

Installed the stress tool to simulate high CPU usage for alert testing.



Status of VM before running stress test

Monitored baseline CPU usage through Azure Monitor to record normal operating performance before simulation. (used the top command to monitor the status)

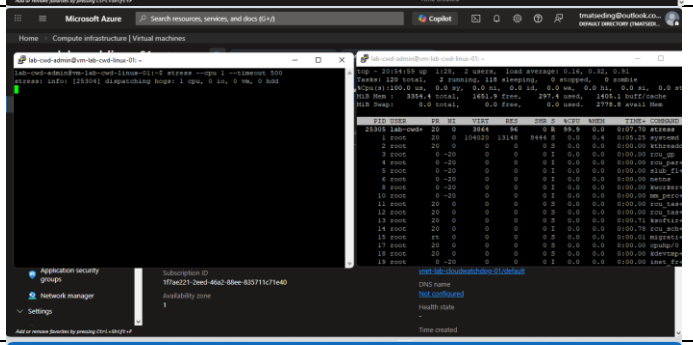


Run Stress Test

Executed:

stress --cpu 1 --timeout 500

This pushed CPU utilization above 80% for a sustained period to trigger the alert rule.



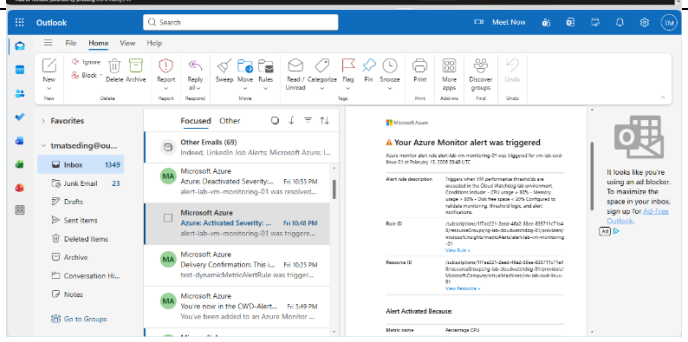
Receive Alert on Email

After sustained high CPU usage, the alert rule triggered successfully and I received an email notification from the configured Action Group.

This confirmed that:
Monitoring was properly configured

The threshold logic worked as expected

Notifications were successfully delivered



Delete Resources

Deleted the resource group to remove all deployed components and prevent unnecessary cloud costs.