

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	Create Action Group
Azure Dashboard	Name Action Group
Resource Groups	Set up Email Alerts
Name Resource Group	Action Group Created
Resource Group Created	Verify email is added to Action Group
Virtual Network	Virtual Machine
Name Virtual Network	Name Virtual Machine
Virtual Network Created	Create SSH Key
Network Security Group	Virtual Machine Created
Name Network Security Group	Create Alert Rule
Network Security Group Created	Start VM using PuTTY
Log Analytics	Sudo Apt Update
Name Log Analytics	Install Stress
Log Analytics Created	Status of VM before running stress test
Register Resource Provider	Run Stress Test
Open Azure Monitor	Receive Alert on Email
Select Alerts	Delete Resources
Select Action Group	

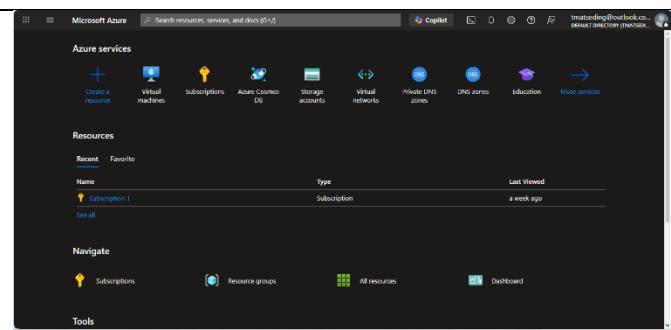
Introduction

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.

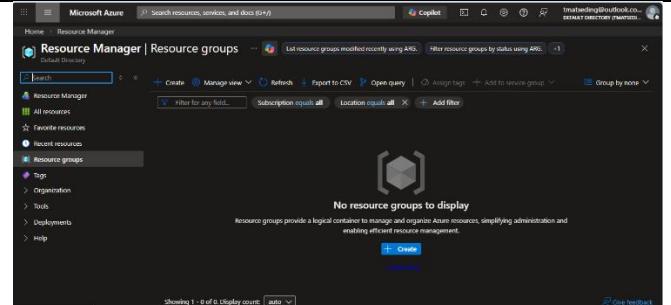
Azure Dashboard

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.

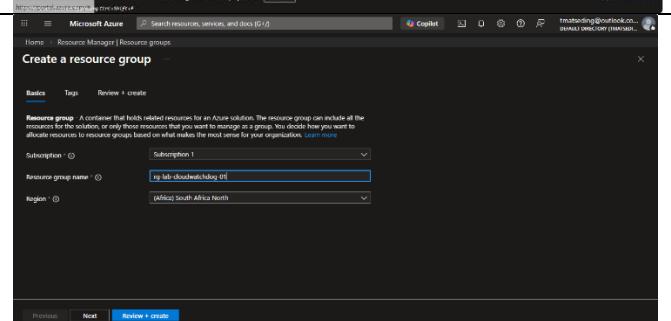


Resource Groups

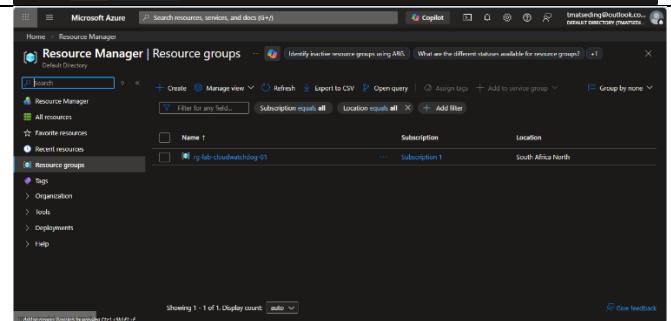
A Resource Group allows us to logically organize all related resources into one container. This makes management easier and ensures that everything related to the project can be controlled or deleted together.



Name Resource Group

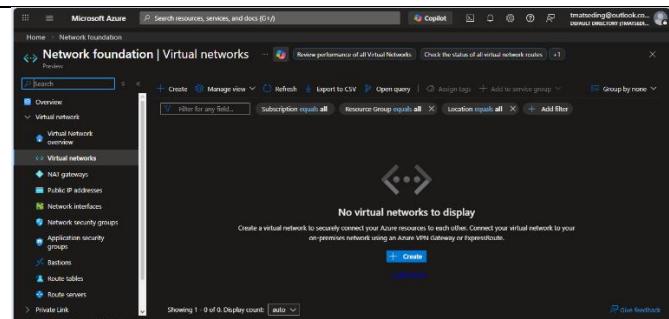


Resource Group Created



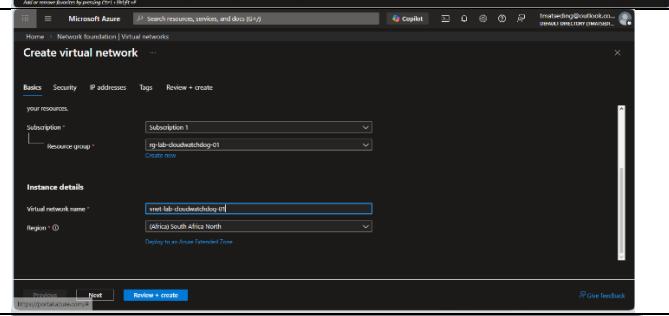
Virtual Network

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.



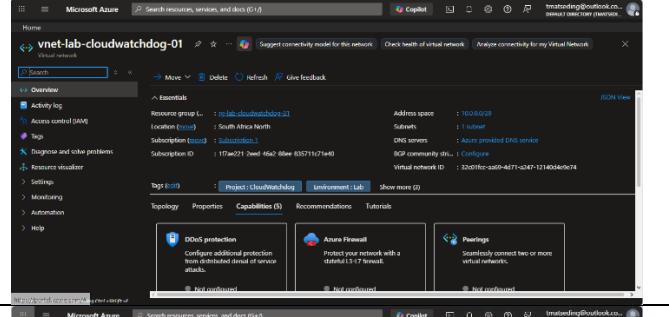
The screenshot shows the Microsoft Azure portal interface for the Network foundation | Virtual networks section. The main content area displays the message 'No virtual networks to display' with a sub-instruction: 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN gateway or ExpressRoute.' Below this message are two buttons: '+ Create' and 'Feedback'.

Name Virtual Network



The screenshot shows the 'Create virtual network' page in the Microsoft Azure portal. The 'Basics' tab is selected. Under 'Subscription', 'Subscription 1' is chosen. Under 'Resource group', 'vnet-lab-cloudwatchdog-01' is selected. The 'Virtual network name' field contains 'vnet-lab-cloudwatchdog-01'. The 'Region' dropdown shows 'South Africa North'. At the bottom, there are 'Review + create' and 'Give feedback' buttons.

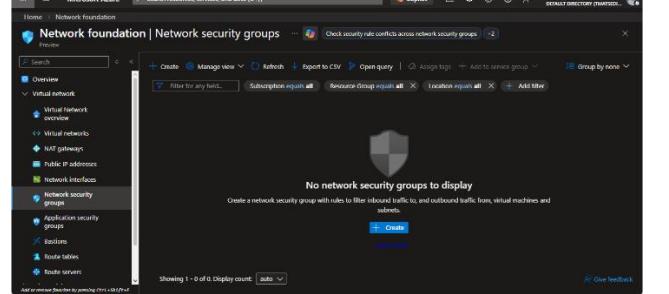
Virtual Network Created



The screenshot shows the details page for the virtual network 'vnet-lab-cloudwatchdog-01'. The 'Overview' tab is selected. Key details shown include: Resource group: 'vnet-lab-cloudwatchdog-01', Location: 'South Africa North', Subscription: 'Subscription 1', and Virtual network ID: '1177ae221-2edf-46a2-8f8e-83711671e4d0'. The page also features a 'Tags' section and a 'Topology' section with cards for 'DDoS protection', 'Azure Firewall', and 'Peering'.

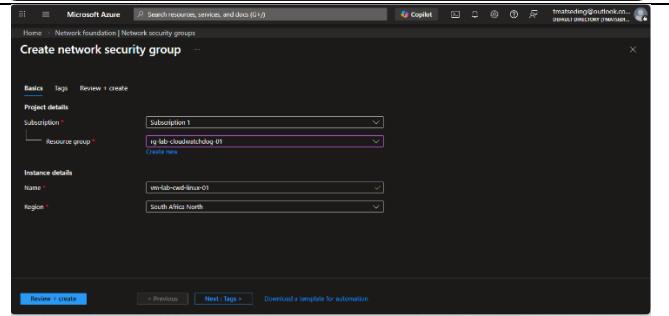
Network Security Group

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.



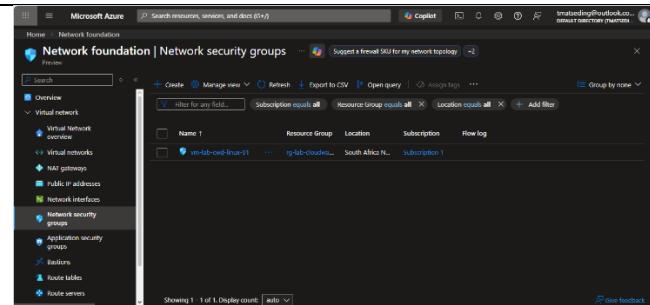
The screenshot shows the Microsoft Azure portal interface for the Network security groups section. The main content area displays the message 'No network security groups to display' with a sub-instruction: 'Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and services.' Below this message are two buttons: '+ Create' and 'Feedback'.

Name Network Security Group



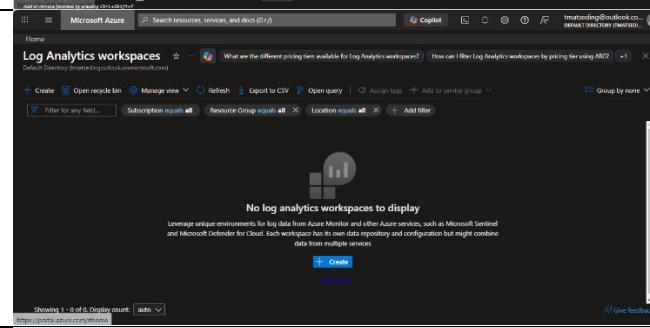
The screenshot shows the 'Create network security group' page in the Microsoft Azure portal. The 'Basics' tab is selected. Under 'Subscription', 'Subscription 1' is chosen. Under 'Resource group', 'vnet-lab-cloudwatchdog-01' is selected. The 'Name' field contains 'vnet-lab-ceil-linu-01'. The 'Region' dropdown shows 'South Africa North'. At the bottom, there are 'Review + create', 'Previous', 'Next + Tags', and 'Download a template for automation' buttons.

Network Security Group Created

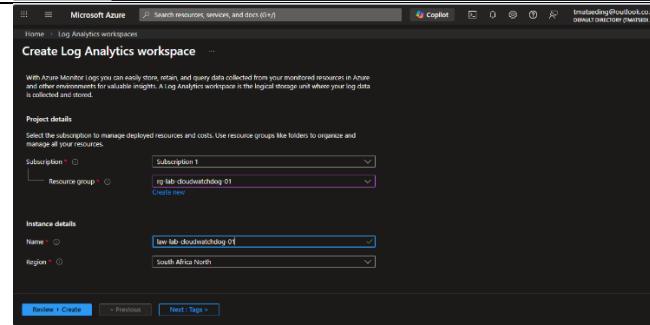


Log Analytics

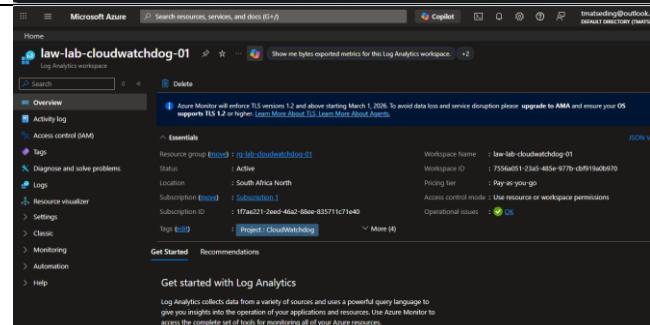
Log Analytics provides centralized visibility into performance metrics and logs for connected resources. This workspace is necessary for monitoring and alerting.



Name Log Analytics



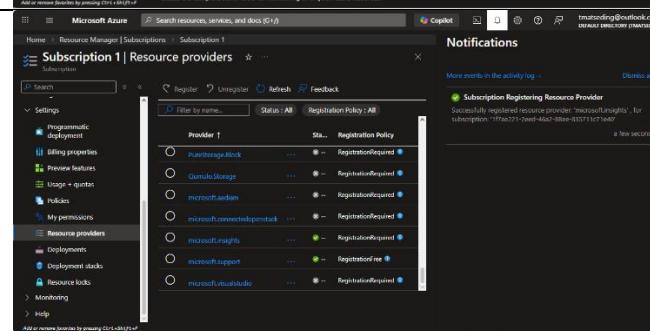
Log Analytics Created



Register Resource

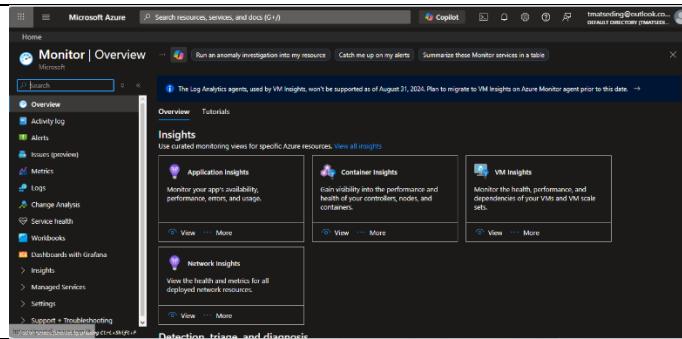
Provider

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

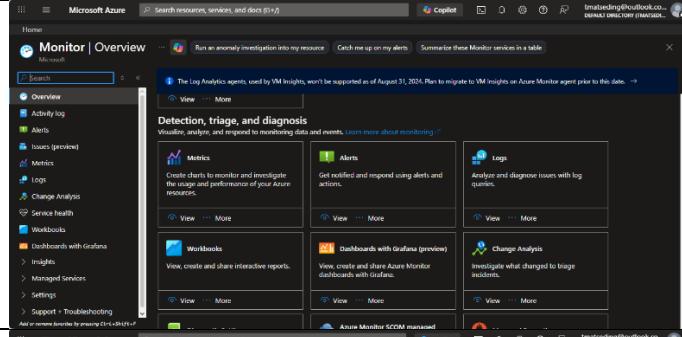
Accessed Azure Monitor to configure alerts, metrics, and monitoring rules.



The screenshot shows the Azure Monitor Overview page. The left sidebar includes options like Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, and Dashboards with Grafana. The main content area is divided into 'Insights' and 'Detection, triage, and diagnosis'. The 'Insights' section contains cards for Application Insights, Container Insights, and Network Insights. The 'Detection, triage, and diagnosis' section contains cards for Metrics, Alerts, Logs, Workbooks, Dashboards with Grafana, and Change Analysis.

Select Alerts

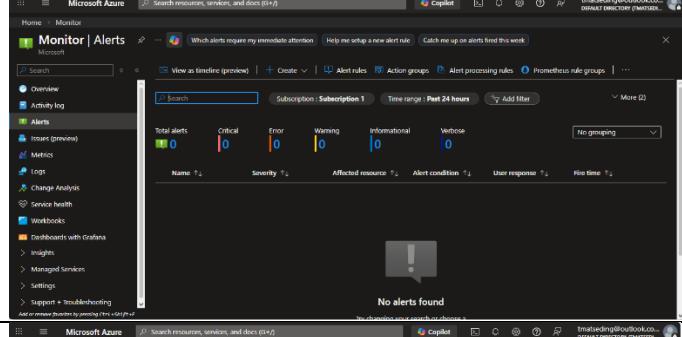
Navigated to the Alerts section to create a new alert rule based on VM performance metrics.



The screenshot shows the Azure Monitor Overview page with the 'Alerts' section selected in the sidebar. The main content area displays a grid of cards for Metrics, Alerts, Logs, Workbooks, Dashboards with Grafana, and Change Analysis, similar to the general overview but with a focus on alerts.

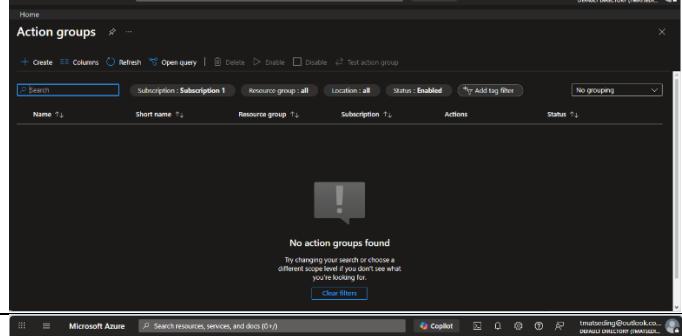
Select Action Group

Selected Action Groups to configure how notifications would be delivered when an alert is triggered.



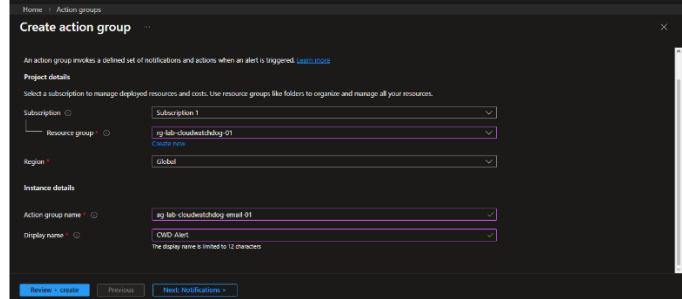
The screenshot shows the Azure Monitor Alerts page. The left sidebar shows 'Alerts' selected. The main content area displays a table of alerts with columns for Name, Severity, Affected resource, Alert condition, User response, and Hit time. A message at the bottom states 'No alerts found'.

Create Action Group



The screenshot shows the Azure Action groups page. The left sidebar shows 'Action groups' selected. The main content area displays a table with a single row showing 'No action groups found'. A message below the table says 'My changes might not be visible if they're in a different location or if you don't see what you're looking for.' with a 'Clear filters' button.

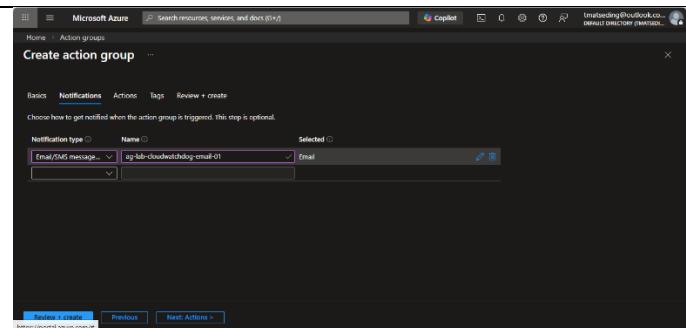
Name Action Group



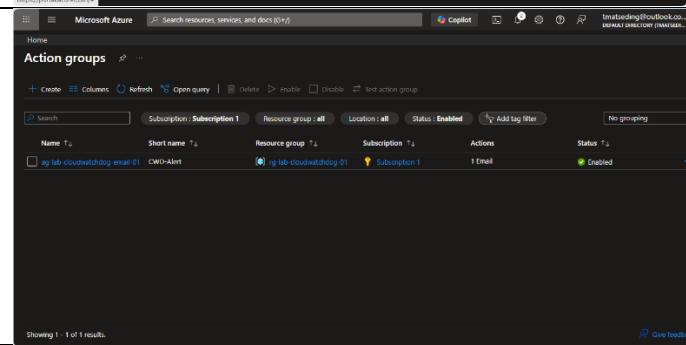
The screenshot shows the 'Create action group' wizard page. The 'Project details' section includes fields for Subscription (Subscription 1), Resource group (rg-lab-cloudwatchlog-01), and Region (Global). The 'Instance details' section includes fields for Action group name (ag-lab-cloudwatchlog-email-01) and Display name (CWD Alert). At the bottom are 'Review + Create' and 'Next: Notifications >' buttons.

Set up Email Alerts

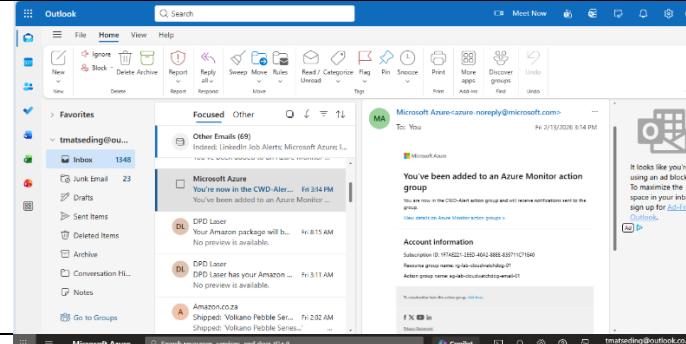
Configured email notification within the Action Group to receive alerts when performance thresholds are exceeded.



Action Group Created

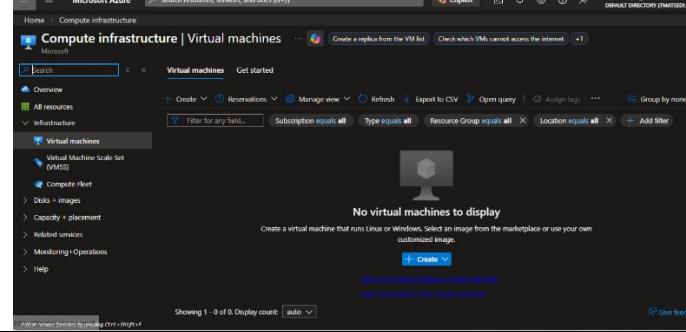


Verify email is added to Action Group

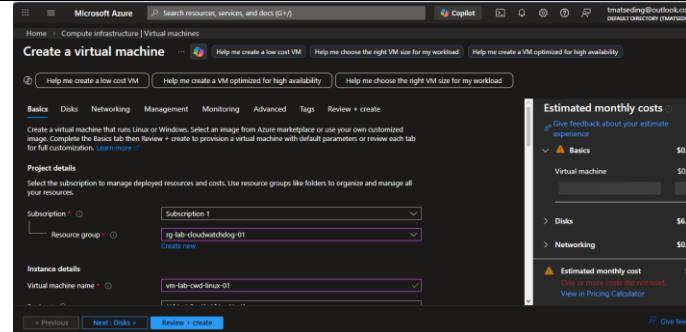


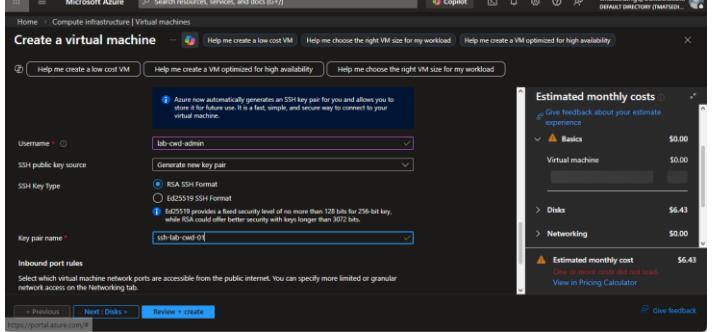
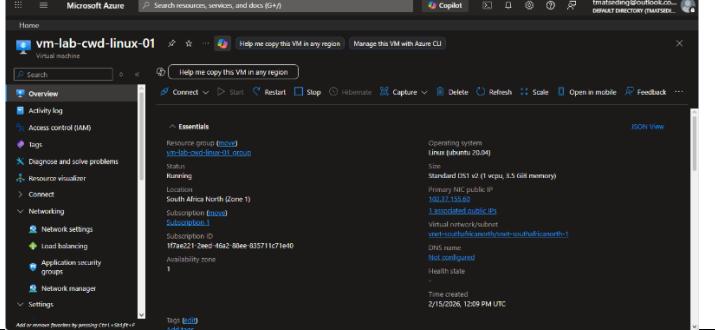
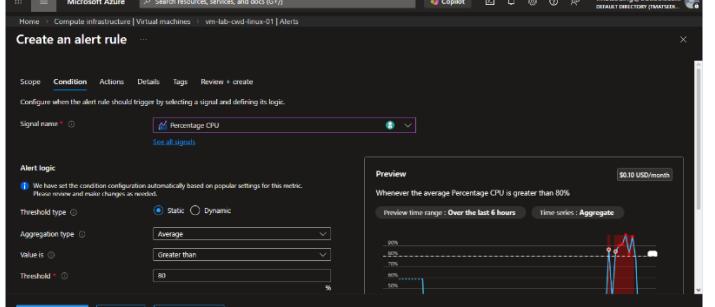
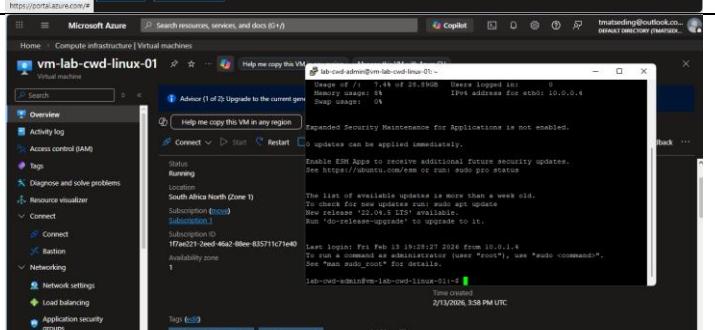
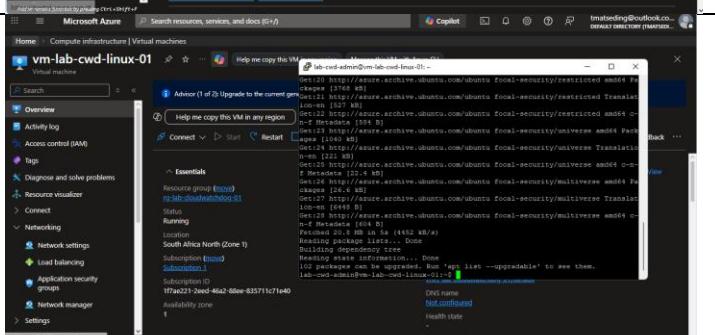
Virtual Machine

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.



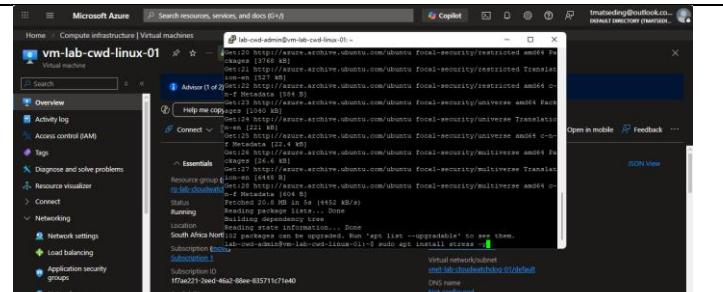
Name Virtual Machine



<h2>Create SSH Key</h2>	
<h2>Virtual Machine Created</h2>	
<h2>Create Alert Rule</h2> <p>Created an alert rule in Azure Monitor configured to notify me when CPU usage exceeds 80%.</p> <p>The alert was linked to the previously created Action Group to ensure email notifications would be sent when the threshold was reached.</p>	
<h2>Start VM using PuTTY</h2> <p>Used PuTTY to securely connect to the virtual machine via SSH.</p>	
<h2>Sudo Apt Update</h2> <p>Updated the Linux package repository to ensure the system was ready for installing additional tools.</p>	

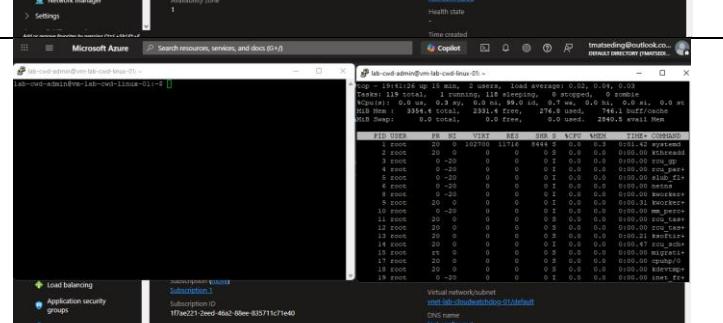
Install Stress

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)

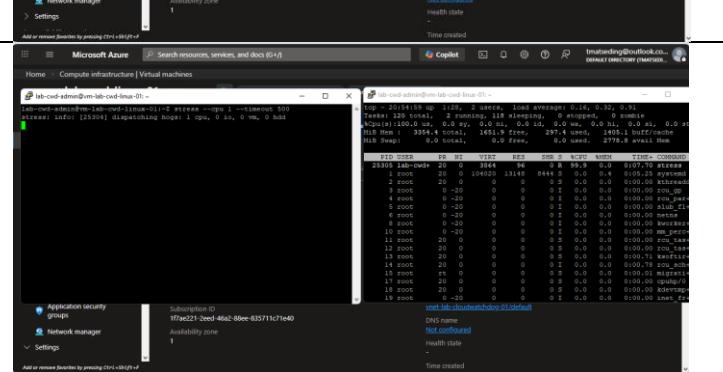


Run Stress Test

Executed:

```
stress --cpu 1 --timeout 500
```

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



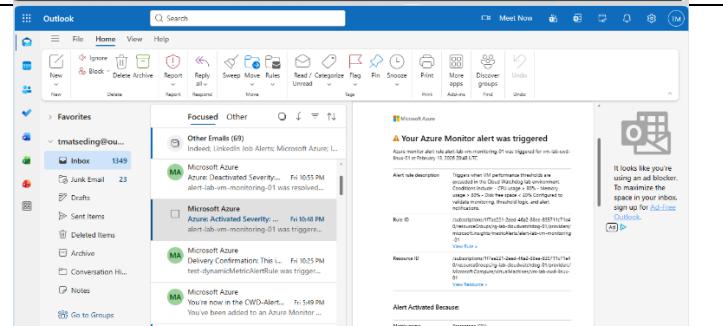
Receive Alert on Email

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.

