MINOR PROJECT 2 : Wazuh SIEM Implementation & Security Monitoring

Name: *Kaushal Jung Thapa*
Course: *CEH*
Sem: *5th Sem*
ERP: *6604309*
College: *Rungta College of Engineering & Technology, Bhilai*

1. Project Overview

Objective:

To plan, deploy, and configure a Wazuh-based SIEM solution in a Linux environment to enable centralized log collection, real-time threat detection, and security event analysis, while systematically documenting configurations, alerts, and security evidence.

Tools & Environment:

- Ubuntu Server (SIEM VM)
- Wazuh Manager
- Wazuh Agent (VMs)
- Wazuh Dashboard (OpenSearch)
- Web Browser (Chrome/Firefox)

2. Baseline Architecture Document

Component	Purpose
Wazuh Manager	Collects and analyzes logs from agents
Wazuh Agent	Sends system and security logs

	to manager
Wazuh Dashboard	Visualizes alerts, logs, and compliance

3. Implementation Steps

a) Virtual Machine Setup

Commands Used:

sudo apt update && sudo apt upgrade -y

b) Wazuh Manager Installation

Installed Wazuh manager using the official installation script.

Commands Used:

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

sudo bash wazuh-install.sh -a

Verification:

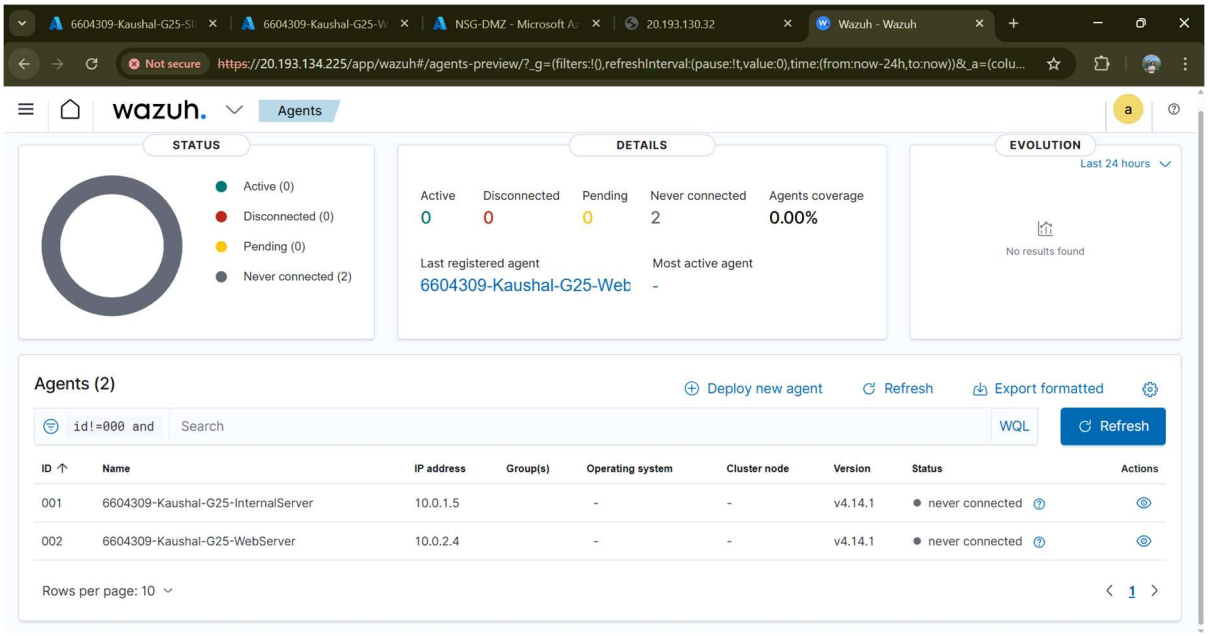
systemctl status wazuh-manager

c) Wazuh Dashboard Configuration

Configured OpenSearch dashboard to visualize logs and alerts.

Verification:

Accessed dashboard via browser on port 5601.



d) Agent Installation & Registration

Installed Wazuh agent and authenticated it with the manager.

Commands Used:

sudo apt install wazuh-agent -y

sudo /var/ossec/bin/agent-auth -m <Manager-IP>

Verification:

systemctl status wazuh-agent

e) Log Monitoring & Alert Generation

System activities were monitored and alerts were generated for security-related events.

4. Vulnerability Detection & Observations

Issue No	Observation	Impact	Status
1	Unauthorized login attempts detected	Brute-force risk	Alert Generated
2	File permission change detected	Integrity violation	Alert Generated
3	Service restart activity logged	Configuration monitoring	Logged

7. Remediation Checklist

Task	Status
Install Wazuh Manager	Completed
Configure Dashboard	Completed
Register Agent	Completed

Enable Log Monitoring	Completed
Generate Alerts	Completed
Maintain Evidence	Completed

8. Summary

Wazuh Manager: Installed and operational

Wazuh Agent: Successfully registered

Dashboard: Accessible and functional

Alerts: Generated and analyzed

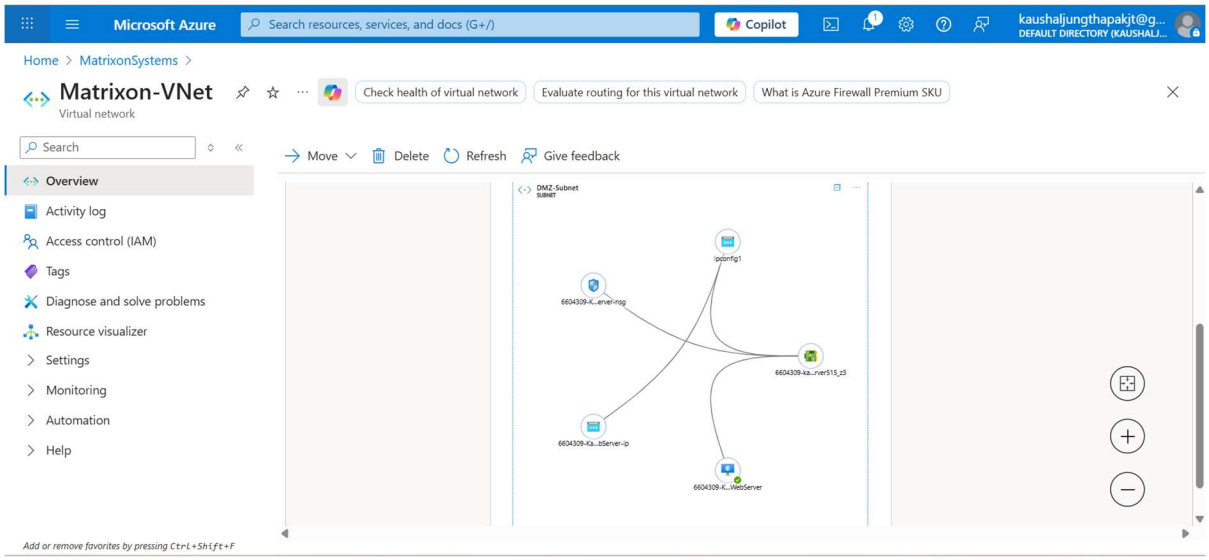
Monitoring: Active and real-time

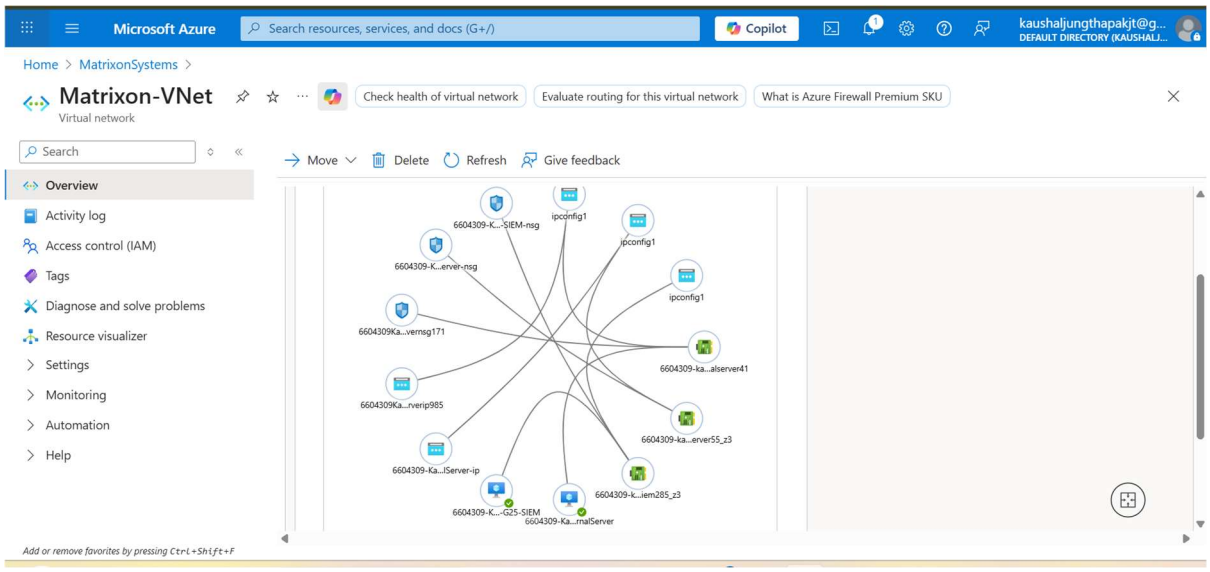
9. Conclusion

This minor project effectively demonstrated the real-world implementation of a SIEM solution based on Wazuh. Through practical exercises in log analysis, security monitoring, and alert management, the project enhanced applied knowledge of cybersecurity principles.

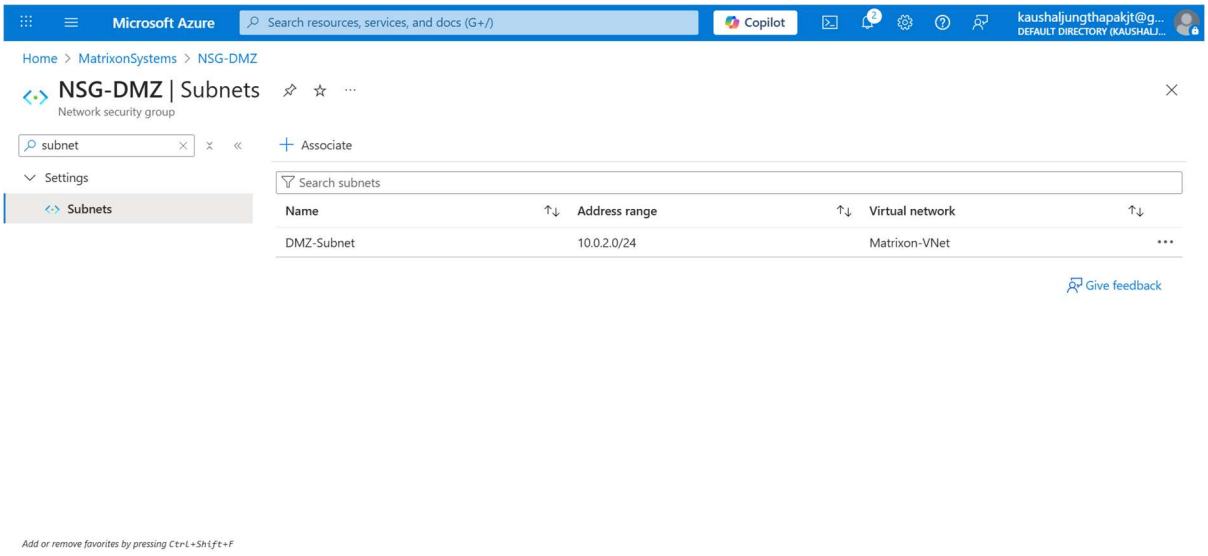
10. Supporting Screenshots

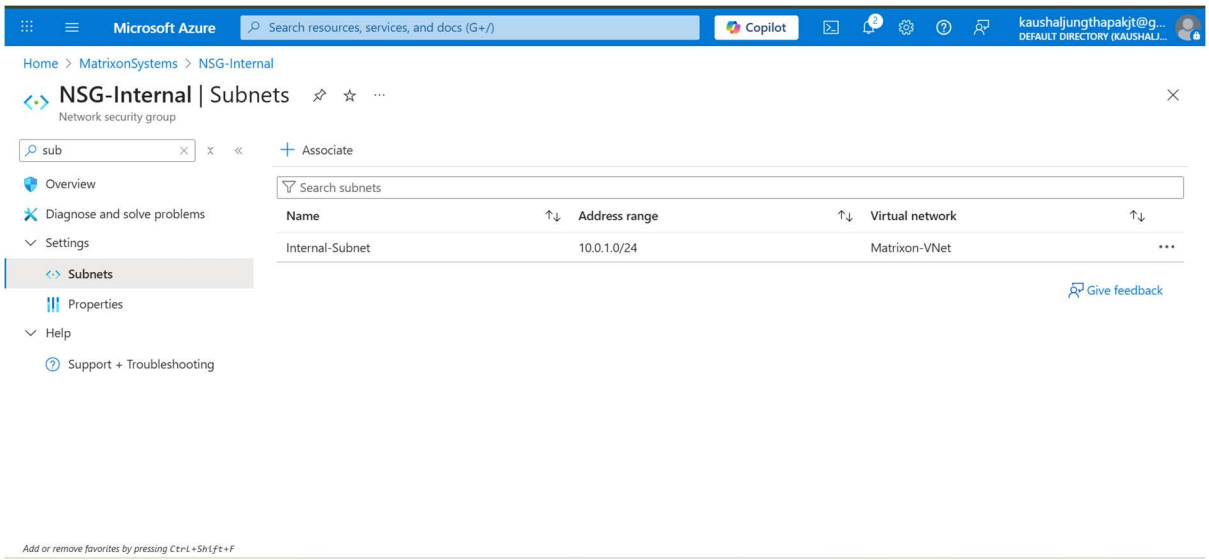
Subnets





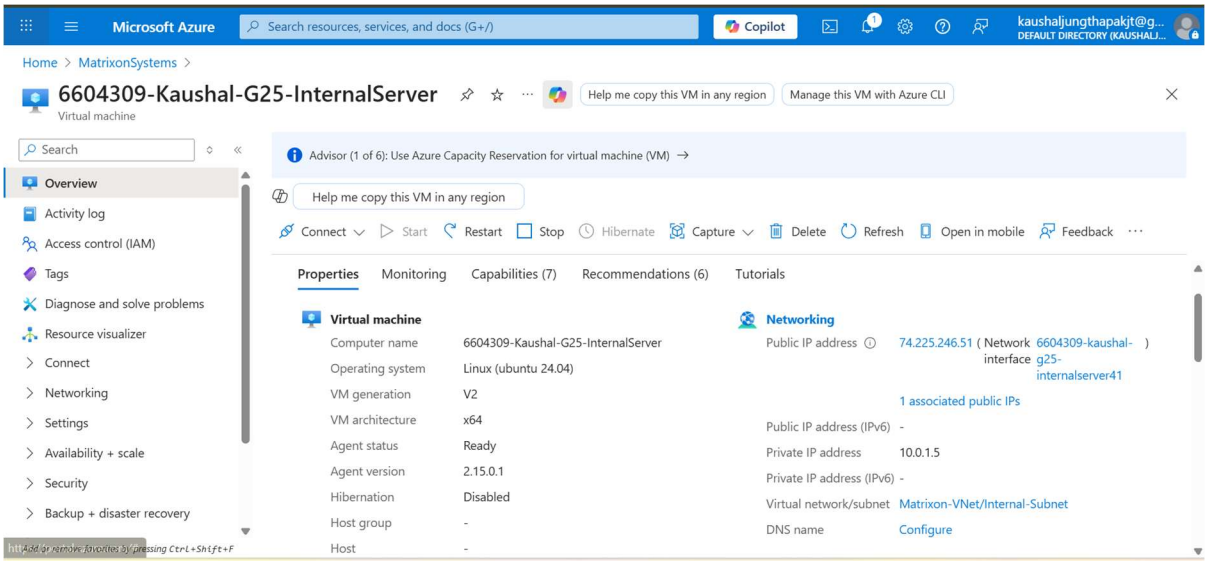
Network Security Groups (NSGs)



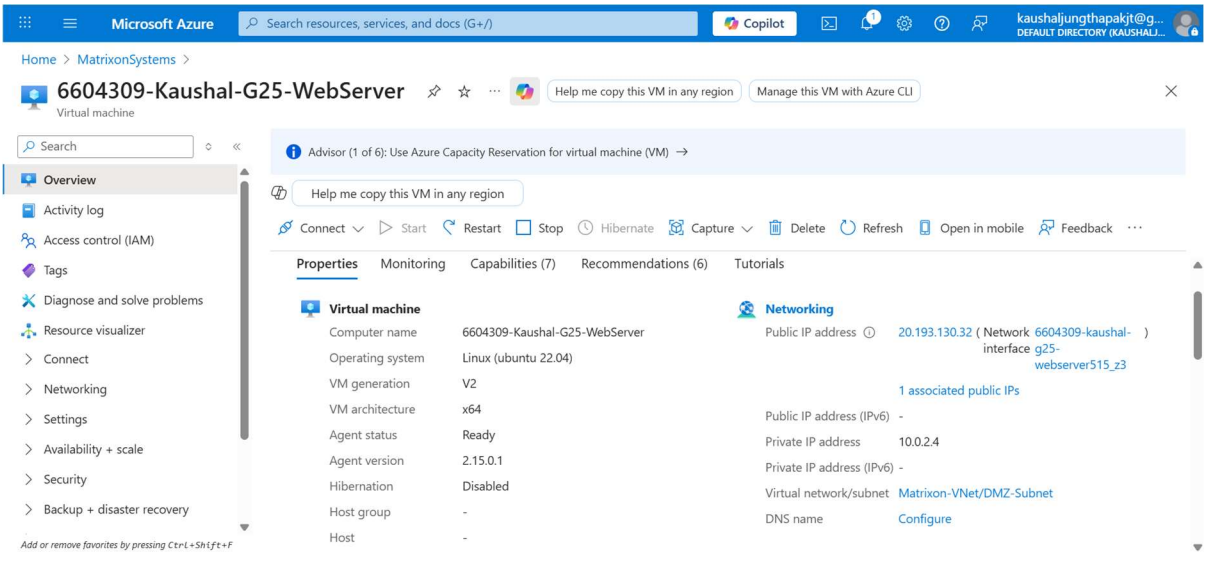


Three Virtual Machines

1) Internal Server



2) WebServer



3) SIEM (WAZUH Server)