MINOR PROJECT REPORT

Infrastructure Deployment & Basic Logging on Microsoft Azure

Student Details

- **Name**: Aanchal dewangan
- **ERP** : 6700440
- **Group Number**: G6

---

1. Introduction

This Minor Project focuses on deploying a **small-scale enterprise cloud infrastructure** using **Microsoft Azure**.
The project simulates a real-world company environment where students act as the **Infrastructure Team**, responsible for deploying servers, networking, and logging mechanisms.

This phase intentionally avoids any form of **security hardening** so that vulnerabilities and misconfigurations can later be exploited and mitigated during the **Major Project phase**.

---

2. Project Objective

The objective of this project is to:

- Design and deploy a **functional mini-company infrastructure** on Microsoft Azure
- Deploy **three Linux-based virtual machines** with defined enterprise roles
- Configure **basic logging mechanisms** only
- Enable **centralized log collection using SIEM**
- Prepare an **intentionally unsecured environment** for cyber-attacks and SOC analysis

---

3. Resource Group Configuration

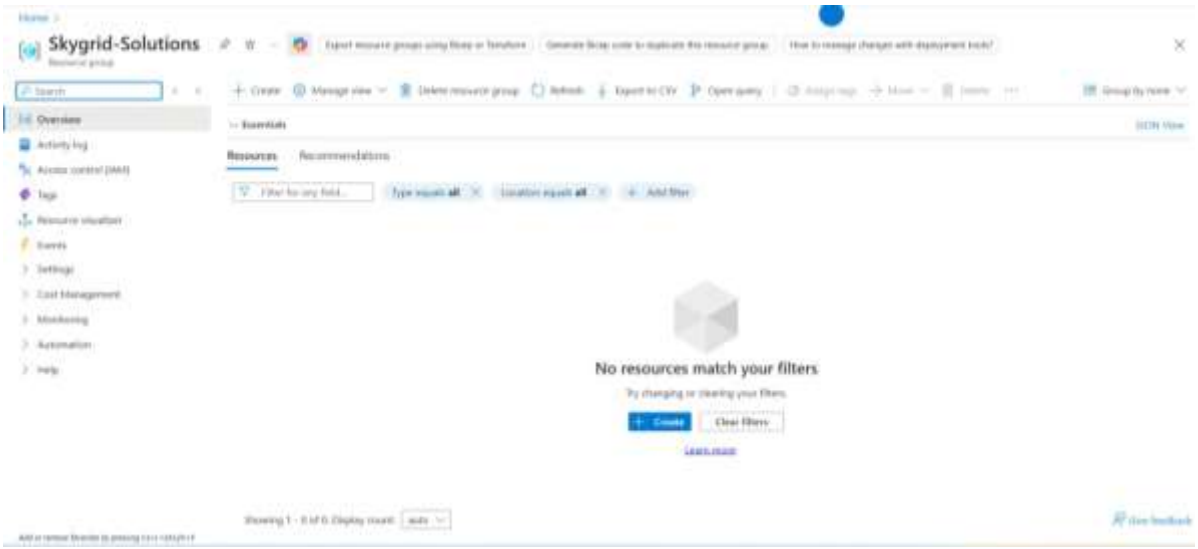
As per project compliance rules, **exactly one Azure Resource Group** was created.

- **Resource Group Name:** Skygrid-Solutions
- **Region:** Central India

All Azure resources including:

- Virtual Machines
- Virtual Network
- Subnets
- Network Security Groups
- Public IP addresses

were created **inside this Resource Group only.**



Azure Portal showing the Resource Group **Skygrid-Solutions** with student account name visible.

---

4. Network Architecture Design

4.1 Virtual Network Creation

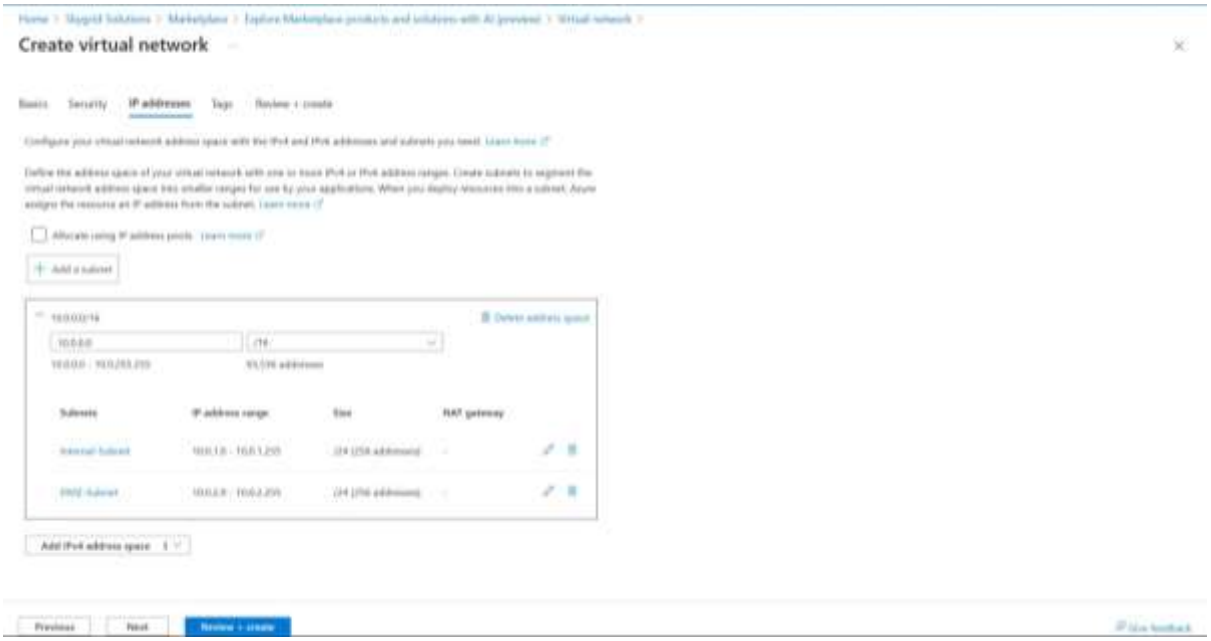
A Virtual Network was created to host the company infrastructure.

- **VNet Name:** Skygrid-Solutions-VNet
- **Address Space:** 10.0.0.0/16

4.2 Subnet Configuration

Two subnets were created to separate internal and external services.

Subnet Name	Address Range	Purpose
Inernal-Subnet	10.0.1.0/24	Internal services and SIEM
DMZ-Subnet	10.0.2.0/24	Public-facing web server



Virtual Network showing Internal and DMZ subnets under the Skygrid-Solutions resource group.

---

5. Network Security Groups (Basic Configuration)

Basic Network Security Groups (NSGs) were created to allow required traffic **without any hardening**.

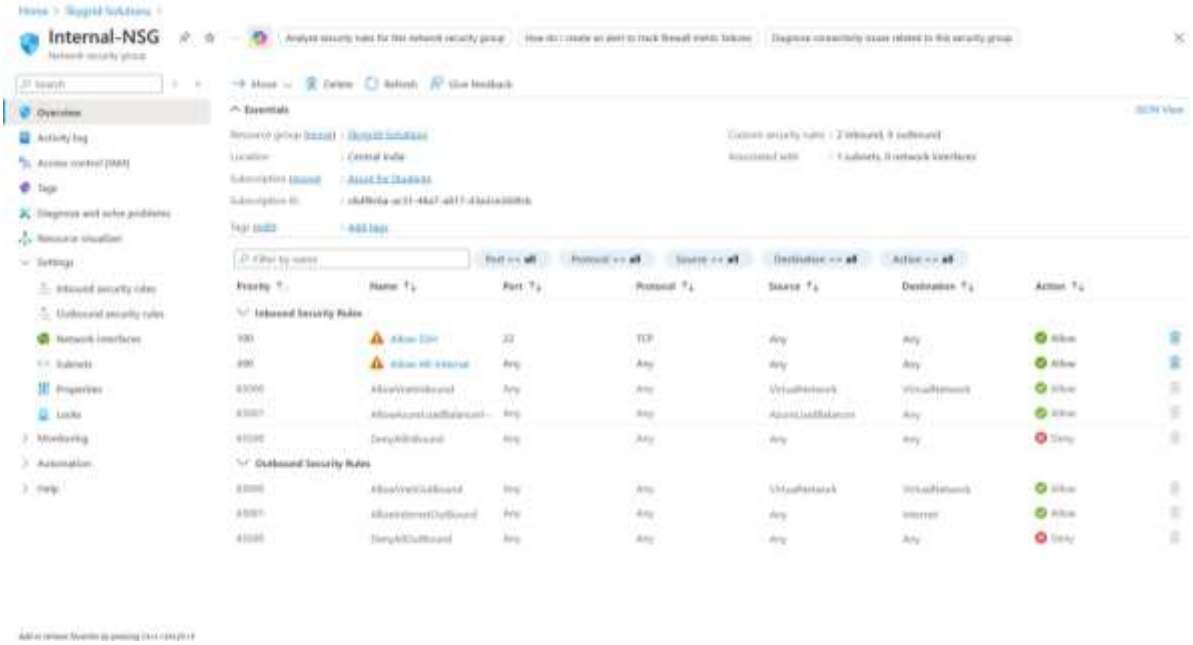
Internal Subnet NSG

- SSH (Port 22) – Allowed from any source
- All outbound traffic – Allowed

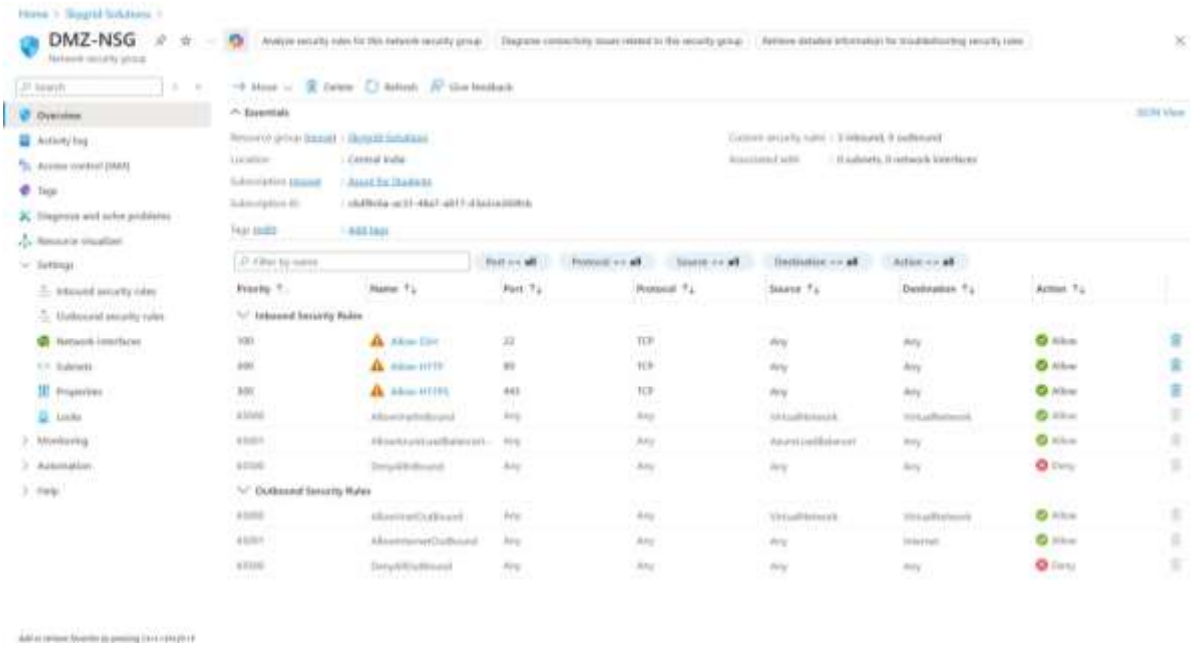
DMZ Subnet NSG

- SSH (Port 22) – Allowed
- HTTP (Port 80) – Allowed
- HTTPS (Port 443) – Allowed
- All outbound traffic – Allowed

No restrictive firewall rules were applied.



Internal-NSG showing unrestricted inbound and outbound access.



DMZ-NSG showing unrestricted inbound and outbound access.

---

6. Virtual Machine Deployment

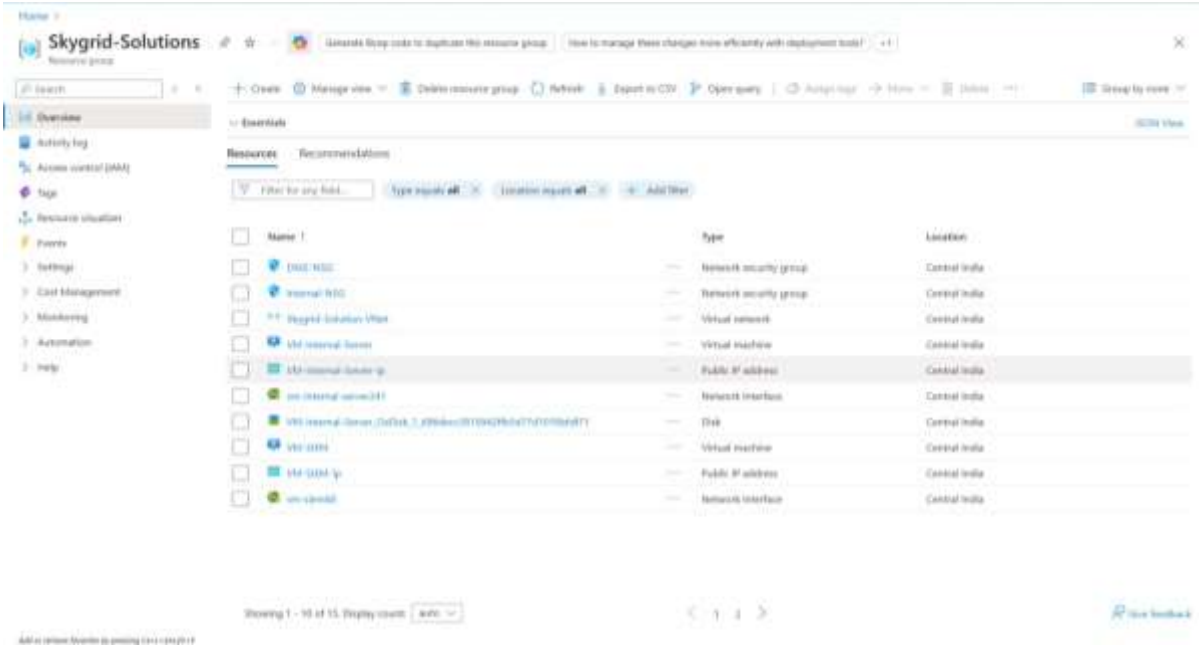
Exactly **three Linux virtual machines** were deployed as required.

6.1 Common VM Configuration

- Operating System: Ubuntu 22.04 LTS
- Authentication: Username and Password
- Public IP Address: Enabled
- Resource Group: Skygrid-Solutions

6.2 VM Inventory

VM Name	OS	Purpose	Private IP	Subnet	Size
VM-Internal-Server	Ubuntu	FreeIPA + File Server	10.0.1.x	Internal	B1s
VM-Web-Server	Ubuntu	Web Server	10.0.2.x	DMZ	B1s
VM-SIEM	Ubuntu	SIEM + Analyst	10.0.1.x	Internal	B2s



Azure Portal showing all three virtual machines deployed in the correct subnets.

---

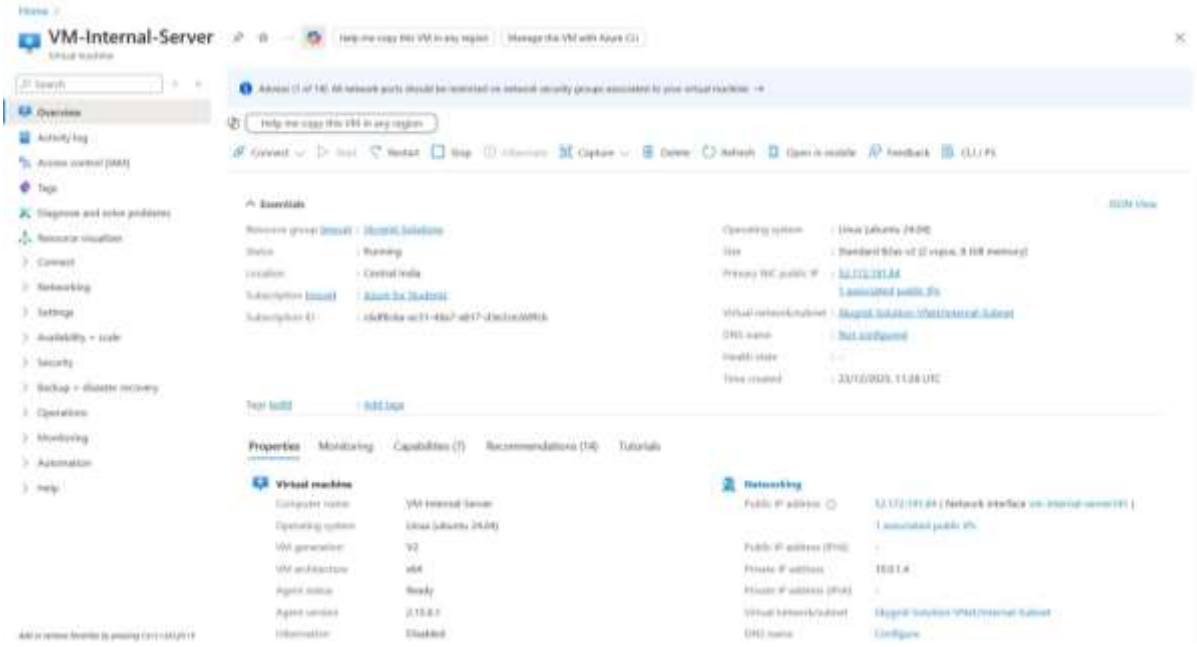
7. Server Roles and Configuration

7.1 VM 1 – Internal Server

Roles Implemented:

- FreeIPA (LDAP + Kerberos)
- Samba File Server
- Internal service hosting

This server simulates corporate **identity management and internal file services**.



7.2 VM 2 – Web Server (DMZ)

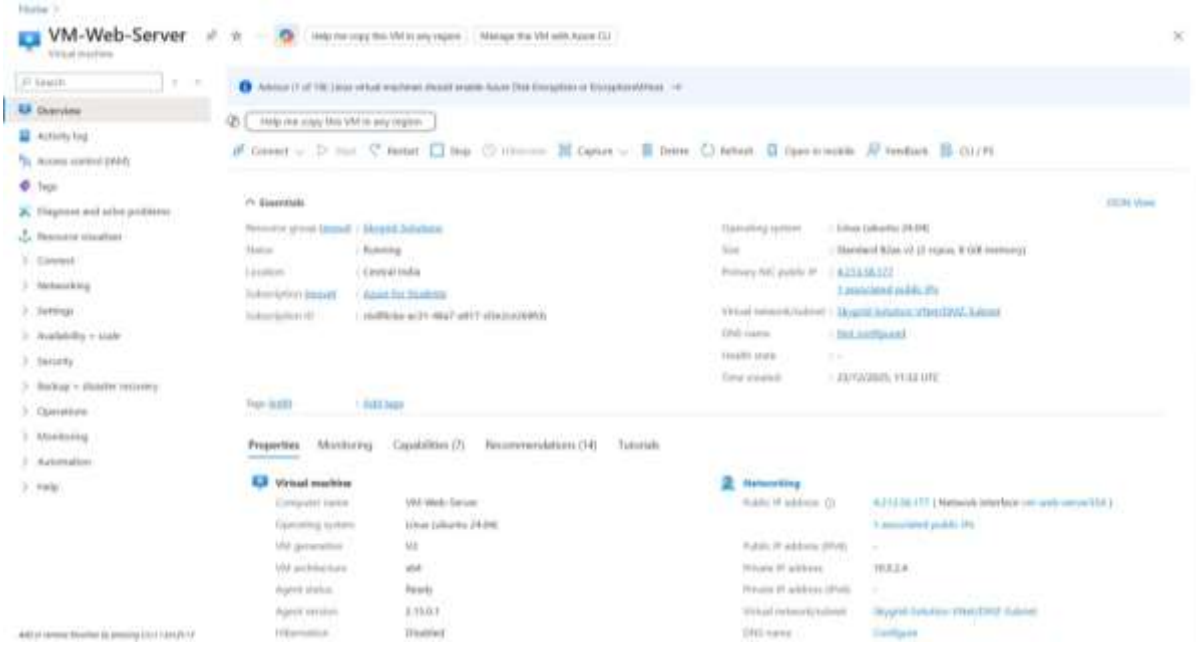
Roles Implemented:

- Apache Web Server
- Static web page hosting

The web server generates:

- Access logs
- Error logs

This server represents an **external-facing application server**.

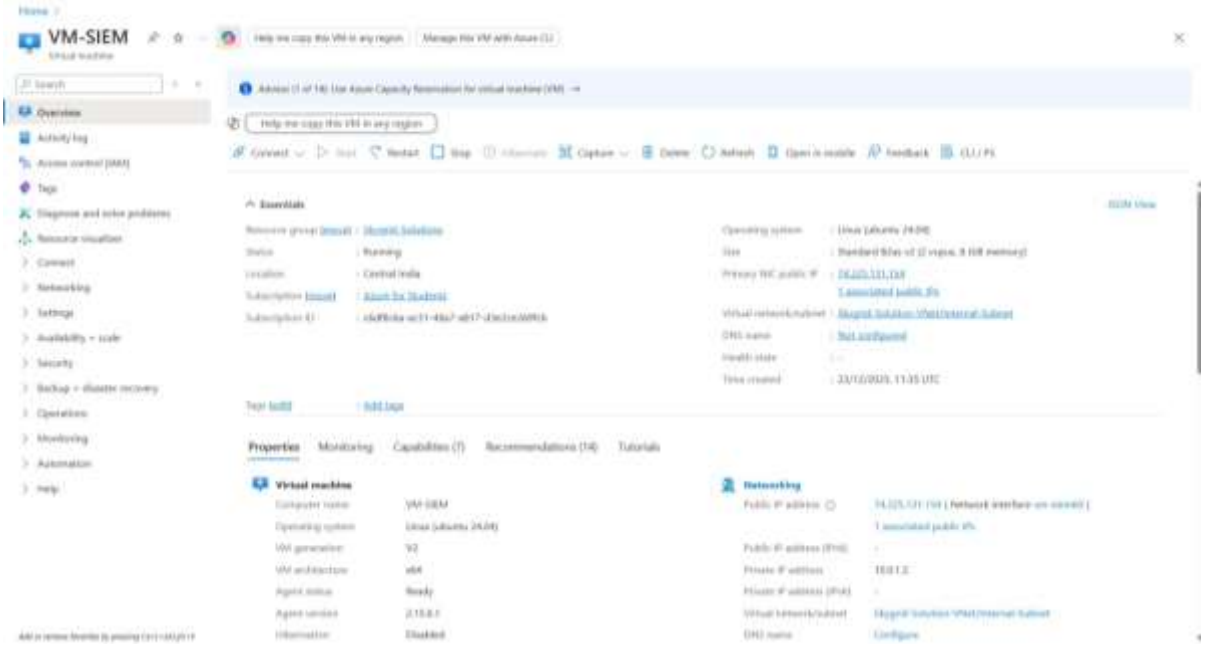


7.3 VM 3 – SIEM + Analyst Workstation

Roles Implemented:

- Wazuh SIEM
- Centralized log monitoring and analysis

This server acts as the **Security Operations Center (SOC)** workstation.



8. Basic Logging Configuration

Only default logging mechanisms were enabled.

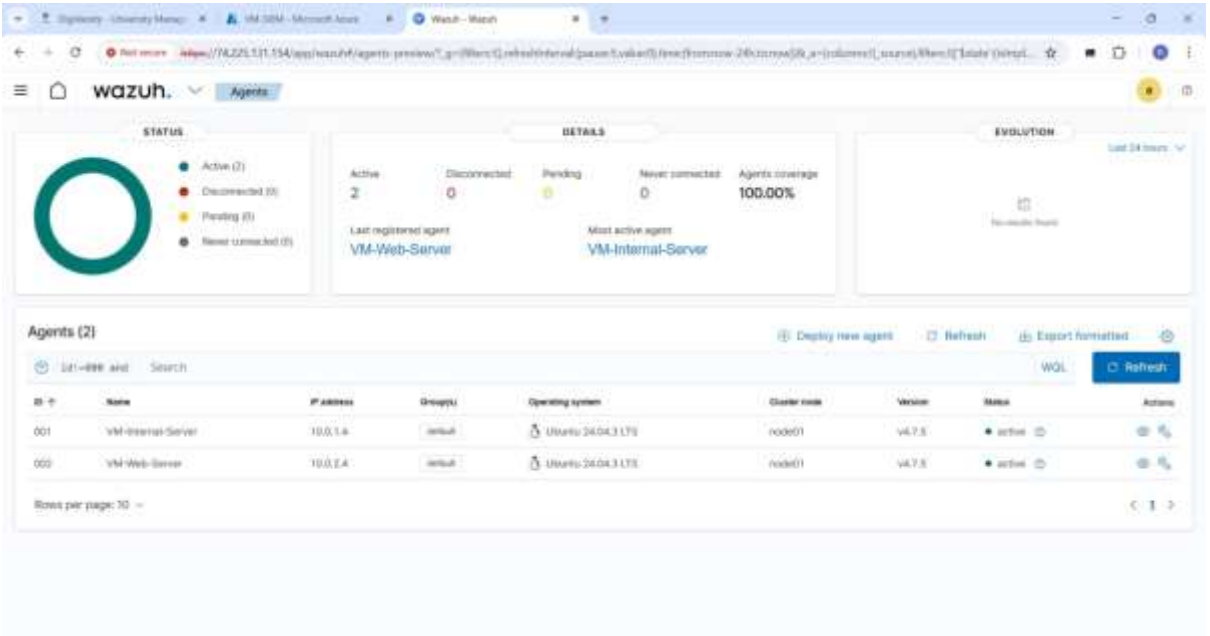
8.1 Logs Generated

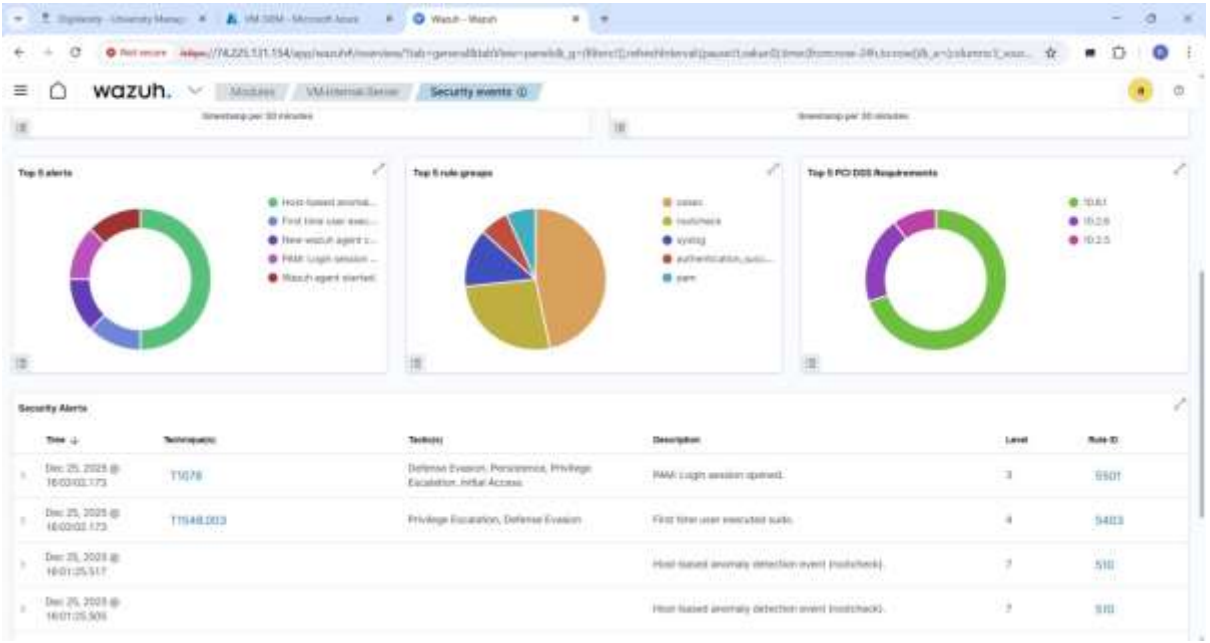
VM	Logs Generated
VM-Internal	Syslog, Authentication logs, Auditd
VM-Web	Apache access and error logs
VM-SIEM	Centralized collected logs

8.2 Log Forwarding

- Wazuh agents were installed on:
    - VM-Internal-Server
    - VM-Web-Server
- Logs were forwarded to:
    - VM-SIEM (Wazuh Manager)

No firewall rules, SSH hardening, or security baselines were applied.





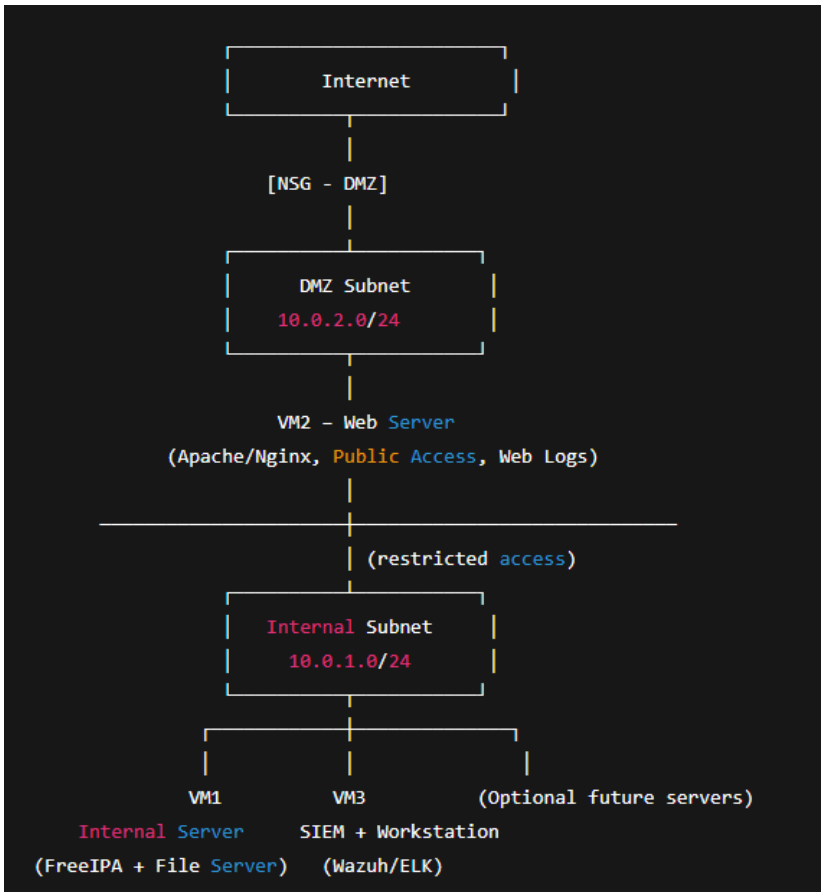
Wazuh SIEM dashboard displaying logs received from Internal and Web servers.

---

9. Network Diagram

A network diagram was created to represent:

- Virtual Network
- Subnets
- VM placement
- Traffic flow



---

10. Deliverables Summary

The following deliverables were completed:

- Infrastructure Deployment Report
- Network Diagram
- VM Inventory
- Logging Summary
- Screenshot Proof with student name visible

---

11. Conclusion

This project successfully deployed a **mini enterprise cloud infrastructure** on Microsoft Azure with **basic logging enabled**.
The environment was intentionally left **unsecured**, fulfilling the requirement for future **attack simulation, log analysis, and SOC operations** in the Major Project phase.

Through this project, practical knowledge was gained in:

- Cloud infrastructure deployment
- Linux server roles
- Network segmentation
- Centralized logging using SIEM

Declaration

I declare that this project has been completed by me using my Azure Student Account, and all screenshots submitted clearly show my name and resource group as required.

Date: 22 Dec 2025