

MINOR PROJECT REPORT

Infrastructure Deployment & Basic Logging on Microsoft Azure

Student Details

- **Name:** Rohitaksh Nag
 - **ERP / Roll Number:** 6604723
 - **Group Number:** G1
-

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.**

The screenshot shows the Microsoft Azure portal's resource group management interface. At the top, there's a header with the Microsoft Azure logo, a search bar, and user information (rohitaksh186@gmail.com). Below the header, the 'Skygrid-Solutions' resource group is selected. The left sidebar has sections like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main content area is titled 'Overview' under 'Essentials' and shows 'Resources' and 'Recommendations'. It features a search bar with filters ('Type equals all', 'Location equals all') and buttons for '+ Create' and 'Clear filters'. A central message says 'No resources match your filters' with a note to 'Try changing or clearing your filters.' At the bottom, it shows 'Showing 1 - 0 of 0' and a 'Give feedback' link.

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
-------------	---------------	---------

Internal-Subnet	10.0.1.0/24	Internal services and SIEM
DMZ-Subnet	10.0.2.0/24	Public-facing web server

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The current step is 'IP addresses'. The address space is defined as 10.0.0.0/16, covering 65,536 addresses. Two subnets are listed:

Subnets	IP address range	Size	NAT gateway
Internal-Subnet	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-
DMZ-Subnet	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-

At the bottom, there are 'Previous' and 'Next' buttons, and a 'Review + create' button.

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

Resource group (move) : Skygrid-Solutions
Location : Central India
Subscription (move) : Azure for Students
Subscription ID : c5df8c6a-ac31-48a7-a817-d3e2ce269fc
Tags (edit) : Add tags

Priority ↑	Name ↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	Allow-SSH	22	TCP	Any	Any	Allow
200	Allow-All-Internal	Any	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Internal-NSG showing unrestricted inbound and outbound access.

DMZ-NSG

Resource group (move) : Skygrid-Solutions
Location : Central India
Subscription (move) : Azure for Students
Subscription ID : c5df8c6a-ac31-48a7-a817-d3e2ce269fc
Tags (edit) : Add tags

Priority ↑	Name ↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	Allow-SSH	22	TCP	Any	Any	Allow
200	Allow-HTTP	80	TCP	Any	Any	Allow
300	Allow-HTTPS	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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	FreelPA + 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

The screenshot shows the Microsoft Azure portal's 'Overview' blade for the 'Skygrid-Solutions' resource group. The left sidebar lists navigation items like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main area displays a table of resources with columns for Name, Type, and Location. The table includes entries for DMZ-NSG, Internal-NSG, Skygrid-Solution-VNet, VM-Internal-Server, VM-Internal-Server-ip, vm-internal-server241, VM-Internal-Server_OsDisk_1_696decc3810942ff3d77d1010bffd71, VM-SIEM, VM-SIEM-ip, and vm-siem60. The VM-Internal-Server row is currently selected. At the bottom, there are pagination controls (Showing 1 - 10 of 15, Display count: auto) and a feedback link.

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**.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'VM-Internal-Server'. The left sidebar contains navigation links such as Home, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, and Help. The main content area is titled 'Overview' and displays the following details:

Essentials		Properties		Networking	
Resource group	(move) : Skygrid-Solutions	Operating system	: Linux (ubuntu 24.04)	Public IP address	: 52.172.191.84 (Network interface vm-internal-server241)
Status	: Running	Size	: Standard B2as v2 (2 vcpus, 8 GiB memory)	1 associated public IPs	
Location	: Central India	Primary NIC public IP	: 52.172.191.84	Private IP address	-
Subscription	(move) : Azure for Students	Subscription ID	: c6df8c6a-ac31-48a7-a817-d3e2ce269fcb	Virtual network/subnet	: Skygrid-Solution-VNet/Internal-Subnet
				DNS name	: Not configured
				Health state	: -
				Time created	: 23/12/2025, 11:28 UTC
Tags (edit) : Add tags					
Virtual machine				Networking	
Computer name	VM-Internal-Server	Operating system	Linux (ubuntu 24.04)	Public IP address	: 52.172.191.84 (Network interface vm-internal-server241)
VM generation	V2	VM architecture	x64	1 associated public IPs	
Agent status	Ready	Agent version	2.15.0.1	Private IP address	: 10.0.1.4
Hibernation	Disabled			Virtual network/subnet	: Skygrid-Solution-VNet/Internal-Subnet
				DNS name	: Configure

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**.

VM-Web-Server Overview

Essentials

- Resource group: Skagrid-Solutions
- Status: Running
- Location: Central India
- Subscription: Azure for Students
- Subscription ID: c6df8c6a-ac31-48a7-a817-d3e2ce269fc
- Operating system: Linux (ubuntu 24.04)
- Size: Standard B2as v2 (2 vcpus, 8 GiB memory)
- Primary NIC public IP: 4.213.58.177 (1 associated public IPs)
- Virtual network/subnet: Skagrid-Solution-VNet/DMZ-Subnet
- DNS name: Not configured
- Health state: -
- Time created: 23/12/2025, 11:32 UTC

Properties Monitoring Capabilities (7) Recommendations (14) Tutorials

Virtual machine

Computer name	VM-Web-Server
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.15.0.1
Hibernation	Disabled

Networking

Public IP address	4.213.58.177 (Network interface vm-web-server354) 1 associated public IPs
Public IP address (IPv6)	-
Private IP address	10.0.2.4
Private IP address (IPv6)	-
Virtual network/subnet	Skygrid-Solution-VNet/DMZ-Subnet
DNS name	Configure

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.

VM-SIEM Overview

Essentials

- Resource group: Skagrid-Solutions
- Status: Running
- Location: Central India
- Subscription: Azure for Students
- Subscription ID: c6df8c6a-ac31-48a7-a817-d3e2ce269fc
- Operating system: Linux (ubuntu 24.04)
- Size: Standard B2as v2 (2 vcpus, 8 GiB memory)
- Primary NIC public IP: 74.225.131.154 (1 associated public IPs)
- Virtual network/subnet: Skagrid-Solution-VNet/Internal-Subnet
- DNS name: Not configured
- Health state: -
- Time created: 23/12/2025, 11:35 UTC

Properties Monitoring Capabilities (7) Recommendations (14) Tutorials

Virtual machine

Computer name	VM-SIEM
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.15.0.1
Hibernation	Disabled

Networking

Public IP address	74.225.131.154 (Network interface vm-siem60) 1 associated public IPs
Public IP address (IPv6)	-
Private IP address	10.0.1.5
Private IP address (IPv6)	-
Virtual network/subnet	Skygrid-Solution-VNet/Internal-Subnet
DNS name	Configure

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.

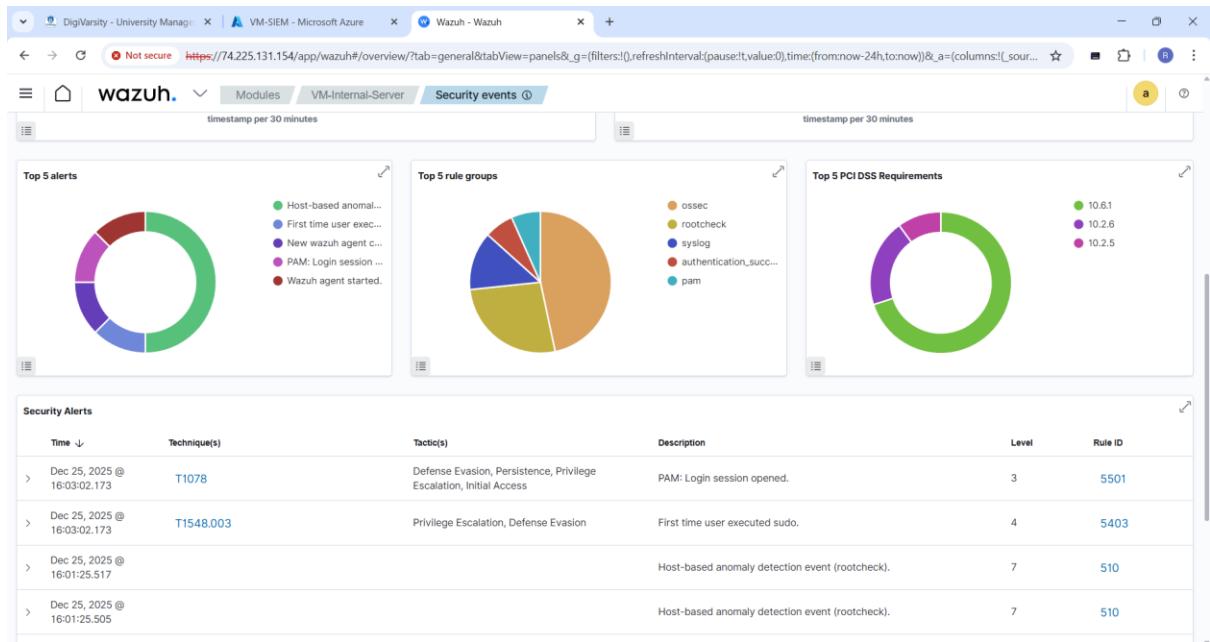
The screenshot shows the Wazuh UI interface. At the top, there are three tabs: 'DigiVarsity - University Manager', 'VM-SIEM - Microsoft Azure', and 'Wazuh - Wazuh'. The 'Wazuh - Wazuh' tab is active. Below the tabs, the URL is https://74.225.131.154/app/wazuh#/agents-preview/?_g=(filters:!{!refreshInterval:(pause:!t,value:0)},time:(from:now-24h,to:now))&_a=(columns:_source,filters:!{(\$state':!isImpl...').

The main area has a header 'wazuh.' with a dropdown and a search bar. The 'Agents' tab is selected. On the left, there's a large green circle icon with a white outline. To its right, a 'STATUS' section shows counts for Active (2), Disconnected (0), Pending (0), and Never connected (0). Below this, it lists the 'Last registered agent' as 'VM-Web-Server' and the 'Most active agent' as 'VM-Internal-Server'. A 'DETAILS' section shows metrics: Active (2), Disconnected (0), Pending (0), Never connected (0), and Agents coverage (100.00%). A 'EVOLUTION' section shows a chart for the last 24 hours with the note 'No results found'.

Below these sections is a table titled 'Agents (2)'. It has columns for ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions. Two rows are listed:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	VM-Internal-Server	10.0.1.4	default	Ubuntu 24.04.3 LTS	node01	v4.7.5	active ⓘ	⟳ ⏺
002	VM-Web-Server	10.0.2.4	default	Ubuntu 24.04.3 LTS	node01	v4.7.5	active ⓘ	⟳ ⏺

At the bottom of the table, there are buttons for 'Deploy new agent', 'Refresh', 'Export formatted', and 'WQL'. There's also a 'Rows per page: 10' dropdown and navigation arrows.

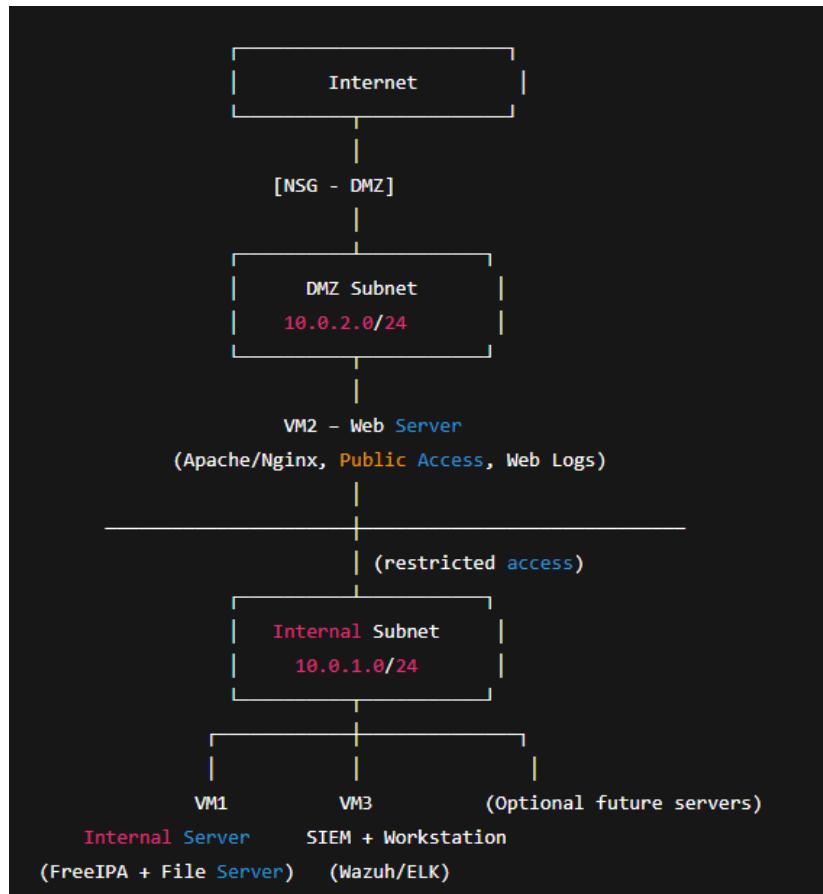


Wazuh SIEM dashboard displaying logs received from Internal and Web servers.

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