

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

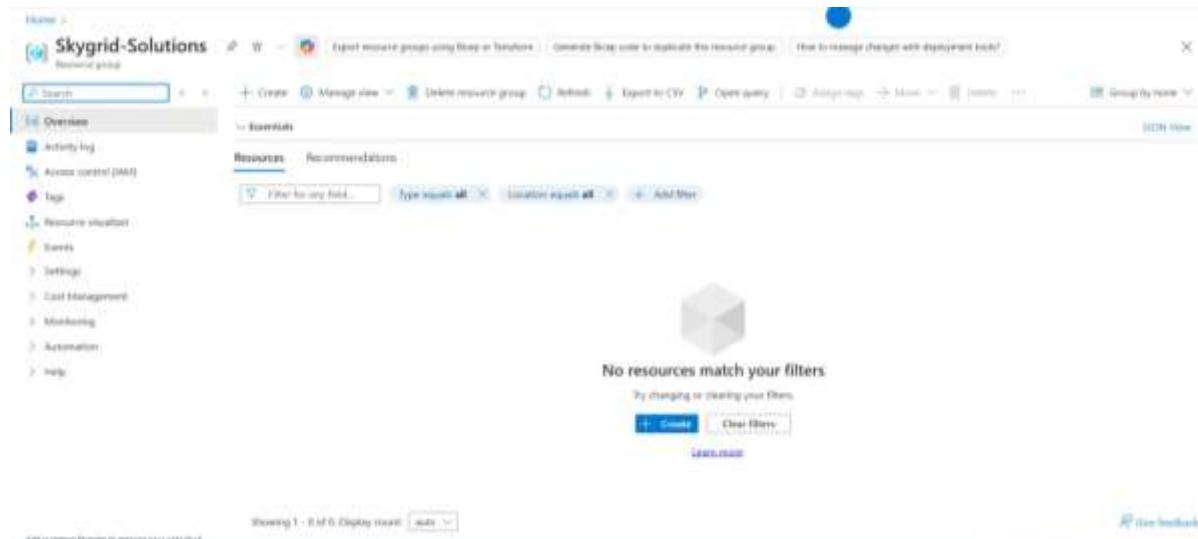
As per project compliance rules, **exactly one Azure Resource Group** was created.

- **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
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 Azure portal interface for creating a virtual network. The top navigation bar includes Home, Skygrid Solutions, Marketplace, Explore Marketplace products and solutions with AI-powered, Virtual networks, and a close button (X).

The main content area is titled "Create virtual network". Below it, there are tabs for Basics, Security, IP addresses, Tags, Review + create, and a feedback link.

The "IP addresses" tab is active, showing the configuration of the virtual network's address space. It includes fields for the subnet range (10.0.1.0/24 and 10.0.2.0/24), a note about defining address space, and a checkbox for "Allocate using IP address pools". A "Delete address space" button is also present.

Below the address space configuration, the "Subnets" section lists the two defined subnets:

- Internal-Subnet:** IP address range 10.0.1.0 - 10.0.1.255, size 256 addresses, and no NAT gateway.
- DMZ-Subnet:** IP address range 10.0.2.0 - 10.0.2.255, size 256 addresses, and no NAT gateway.

At the bottom of the IP addresses section, there is a "Add IPv4 address space" button.

At the very bottom of the page, there are "Previous", "Next", and "Review + create" buttons, along with a "Feedback" link.

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.

Home > Network Security Groups >

Internal-NSG Network security group

Analyze security rules for this network security group | How do I create an alert to track firewall metric values? | Diagnose connectivity issues related to this security group

Search Mode Refresh Give feedback

Overview

Resource group (2222) > Internal-NSG

Location: Central India
Subscription: Azure Dev Spaces
Subscription ID: /subscriptions/0c11-48a7-4b17-03a2a000fb

Tags: None

Custom security rules: 2 inbound, 0 outbound
Associated with: 1 subnet, 0 network interfaces

Essentials

Table: Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action	Actions
Inbound Security Rules							
100	Allow SSH	22	TCP	Any	Any	Allow	
499	Allow HTTP	80	TCP	Any	Any	Allow	
8000	AllowHttpsAndHttp	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
8001	AllowHttpsAndHttpS	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
8100	DenyAllInbound	Any	Any	Any	Any	Deny	
8200	AllowHttpsOutbound	443	TCP	Any	VirtualNetwork	Allow	
8300	AllowHttpOutbound	80	TCP	Any	Internet	Allow	
8400	DenyAllOutbound	Any	Any	Any	Any	Deny	

Add or remove favorites (0 to 1000)

Internal-NSG showing unrestricted inbound and outbound access.

Home > Network Security Groups >

DMZ-NSG Network security group

Analyze security rules for this network security group | Diagnose connectivity issues related to this security group | Review default settings for troubleshooting security rules

Search Mode Refresh Give feedback

Overview

Resource group (2222) > DMZ-NSG

Location: Central India
Subscription: Azure Dev Spaces
Subscription ID: /subscriptions/0c11-48a7-4b17-03a2a000fb

Tags: None

Custom security rules: 2 inbound, 0 outbound
Associated with: 0 subnets, 0 network interfaces

Essentials

Table: Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action	Actions
Inbound Security Rules							
100	Allow SSH	22	TCP	Any	Any	Allow	
499	Allow HTTP	80	TCP	Any	Any	Allow	
8000	AllowHttpsAndHttp	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
8001	AllowHttpsAndHttpS	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
8100	DenyAllInbound	Any	Any	Any	Any	Deny	
8200	AllowHttpsOutbound	443	TCP	Any	VirtualNetwork	Allow	
8300	AllowHttpOutbound	80	TCP	Any	Internet	Allow	
8400	DenyAllOutbound	Any	Any	Any	Any	Deny	

Add or remove favorites (0 to 1000)

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 Azure Portal interface for the 'Skygrid-Solutions' resource group. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Points, Settings, Cost Management, Monitoring, Automation, Help, and Feedback. The main content area has tabs for Overview, Manage view, Delete resource group, Network, Export to CSV, Open query, Assign tags, More, and Delete. The 'Resources' tab is active, showing a list of 15 resources. The resources are categorized by type: Network security group (2), Network interface (3), Virtual network (1), Virtual machine (3), Public IP address (2), and Disk (1). All resources are located in the 'Central India' region. The list includes: NAME / ID, Type, and Location.

Name / ID	Type	Location
NAME / ID: NAME / ID: Internal-NSG	Network security group	Central India
NAME / ID: Internal-PIG	Network security group	Central India
NAME / ID: Skygrid-Solutions-VNet	Virtual network	Central India
NAME / ID: VM-Internal-Server	Virtual machine	Central India
NAME / ID: VM-Internal-Server-ip	Public IP address	Central India
NAME / ID: VM-Internal-Server-Intf	Network interface	Central India
NAME / ID: VM-Internal-Server-Disk	Disk	Central India
NAME / ID: VM-Web-Server	Virtual machine	Central India
NAME / ID: VM-Web-Server-ip	Public IP address	Central India
NAME / ID: VM-Web-Server-Intf	Network interface	Central India
NAME / ID: VM-SIEM	Virtual machine	Central India
NAME / ID: VM-SIEM-ip	Public IP address	Central India
NAME / ID: VM-SIEM-Intf	Network interface	Central India

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 Azure portal interface for a virtual machine named 'VM-Internal-Server'. The main pane displays the 'Essentials' section with the following information:

Resource group (parent)	Virtual Machine	Operating system	Last modified
Microsoft Solutions	VM-Internal-Server	Linux (Ubuntu 24.04)	2024-01-18T14:49:49Z
	Status: Warning	OS disk: Standard Blob v2 (16 GiB, 8 HFR, managed)	
	Location: Central India	Private IP address: 10.1.1.104	Associated public IP: 52.227.131.144
	Subscription (parent): Azure Dev/Test	Virtual network/Subnet: Microsoft-VNet/Internal-Subnet	
	Subscription ID: 1e1d9fca-ec11-4ba7-9b17-d1cde06fb6	DNS name: test.sudipmehra.com	
		Health state: Green	
		Time created: 2023-09-25T11:38:05Z	

The left sidebar contains a navigation menu with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizations, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, and Help.

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

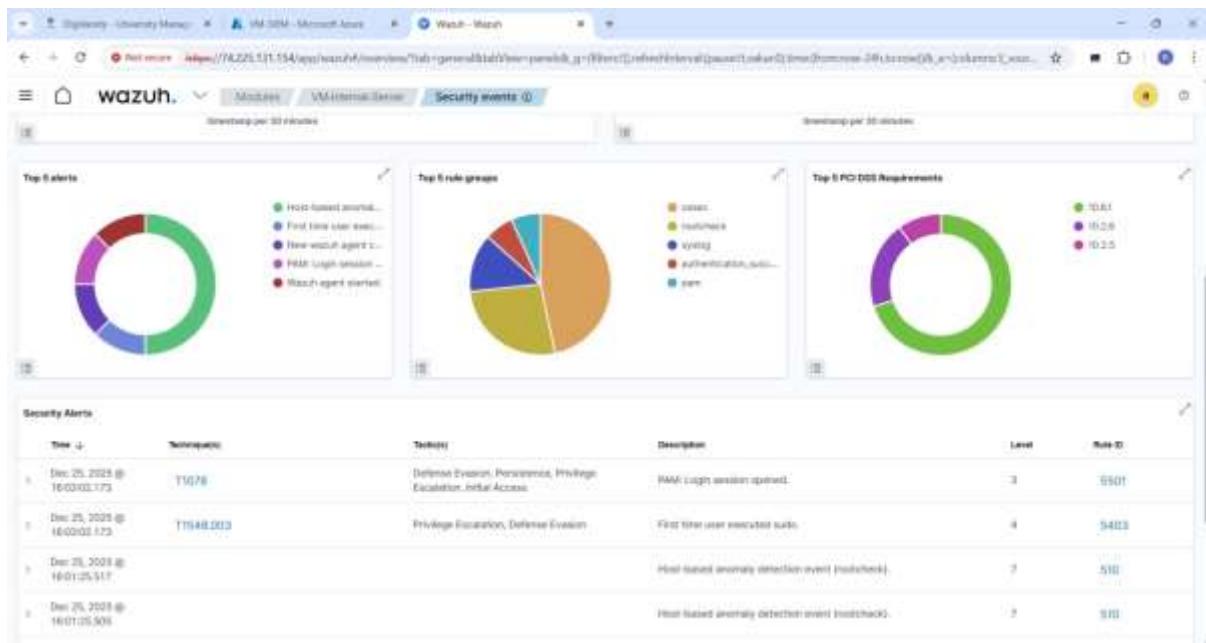
VM	Logs Generated
VM-Internal	Syslog, Authentication logs, Auditd
VM-Web	Apache access and error logs
VM-SIEM	Centralized collected logs

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.

The screenshot shows the Wazuh UI interface. At the top, there's a navigation bar with tabs for 'Dashboard', 'Agents', 'Logs', 'Metrics', and 'Events'. Below the navigation is a search bar with placeholder text 'Search' and a 'WQL' button. The main area has three main sections: 'STATUS' (with a large green circle icon), 'DETAILS' (showing 2 Active, 0 Disconnected, 1 Pending, 0 Never connected, and 100.00% Agents coverage), and 'EVOLUTION' (a chart showing recent activity). Below these is a table titled 'Agents (2)'. The table has columns for 'Name', 'IP Address', 'Group(s)', 'Operating system', 'Cluster node', 'Version', 'Status', and 'Actions'. It lists two agents: 'VM-Internal-Server' and 'VM-Web-Server', both active and running on Ubuntu 20.04.3 LTS with node01 and version v4.7.5. There are buttons for 'Deploy new agent', 'Refresh', 'Export formatted', and another 'Refresh' button.

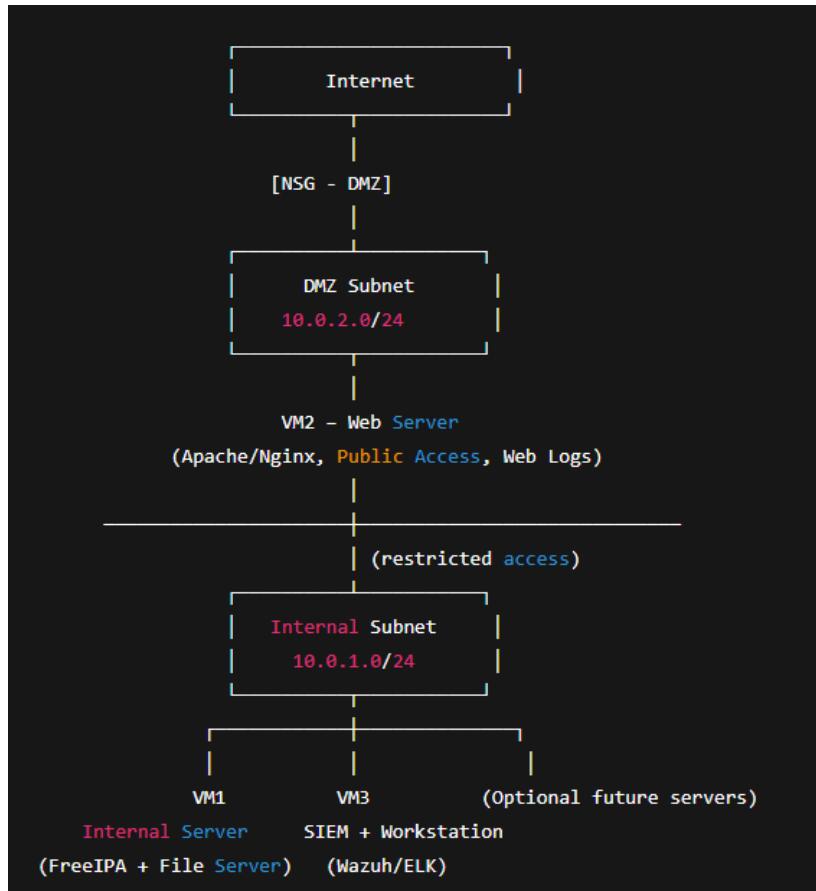


Wazuh SIEM dashboard displaying logs received from Internal and Web servers.

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