

MINOR PROJECT REPORT

Infrastructure Deployment & Basic Logging on Microsoft Azure

Student Details

- **Name:** Abhay Raj
 - **ERP :** 6604180
 - **Group Number:** G29
-

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:** ObscuraNetCorp
- **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 Azure Resource Manager interface for the resource group 'ObscuraNetCorp'. The left sidebar lists navigation options like Overview, Activity log, Access control (IAM), Tags, and Resource visualizer. The main content area shows a table of resources with columns for Name, Type, and Location. The resources listed are:

Name	Type	Location
6604180-Abhay-G29	Virtual network	East Asia
internal-nsg	Network security g...	East Asia
SIEM-public-IP	Public IP address	East Asia
VM-internal	Virtual machine	East Asia
VM-internal-ip	Public IP address	East Asia
vm-internal158	Network Interface	East Asia
VM-internal_OsDisk_1_2813def855954c	Disk	East Asia
VM-SIEM	Virtual machine	East Asia
VM-SIEM-nsg	Network security g...	East Asia
vm-siem43	Network Interface	East Asia
VM-SIEM_OsDisk_1_c41d949cefda4809	Disk	East Asia
VM-Web	Virtual machine	East Asia

Azure Portal showing the Resource Group **ObscuraNetCorp** 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:** obscura-Net-Corp-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 Microsoft Azure Resource Manager interface. The main view is titled "6604180-Abhay-G29 | Subnets". It displays a table of subnets with the following data:

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
dmz-zone	10.0.0.0/24	-	248	-	-	-
internal-VM	10.0.1.0/24	-	251	-	-	-

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 Network security group

Resource group (move) : ObscuraNetCorp
Location : East Asia
Subscription (move) : Azure for Students
Subscription ID : 71612ab2-c704-4cb4-bc52-fa7b4296a94d
Tags (edit) : Add tags

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	⚠ ssh	22	Any	Any	Any	Allow
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
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.

Web-NSG Network security group

Resource group (move) : ObscuraNetCorp
Location : East Asia
Subscription (move) : Azure for Students
Subscription ID : 71612ab2-c704-4cb4-bc52-fa7b4296a94d
Tags (edit) : Add tags

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	⚠ ssh	22	Any	Any	Any	Allow
110	http	80	Any	Any	Any	Allow
120	Allow-Wazuh-Agent	1514	TCP	Any	Any	Allow
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow

DMZ-NSG showing unrestricted inbound and outbound access.

6. Virtual Machine Deployment

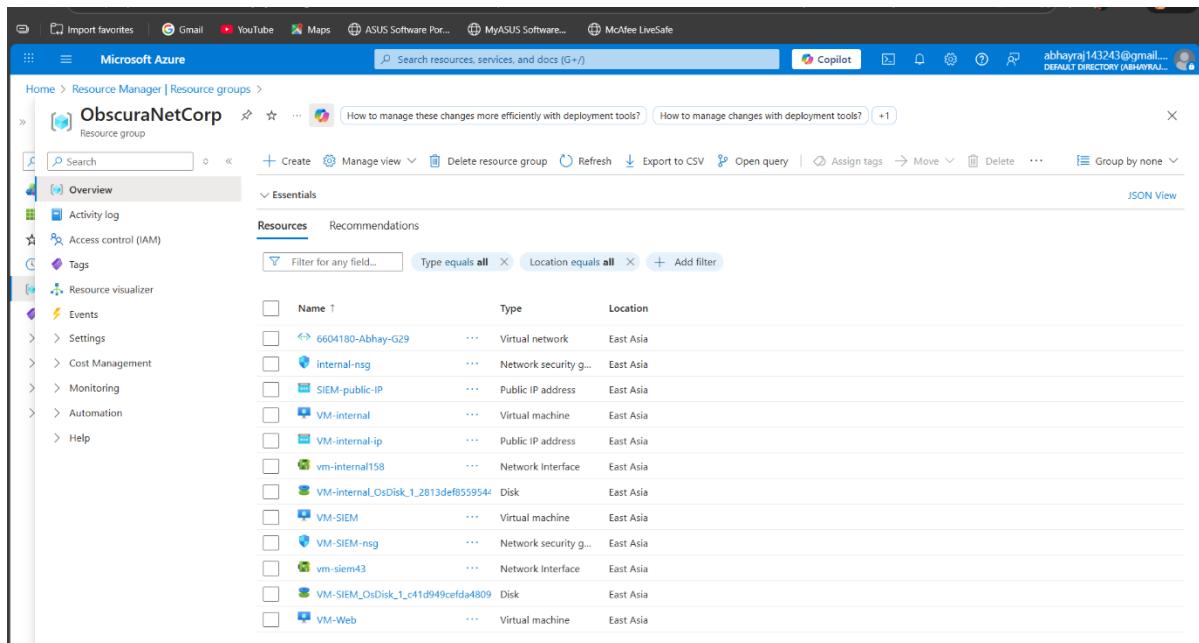
Exactly **three Linux virtual machines** were deployed as required.

6.1 Common VM Configuration

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

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



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. The top navigation bar includes links for Import favorites, Gmail, YouTube, Maps, ASUS Software Port, MyASUS Software, McAfee LiveSafe, Copilot, and user account information (abhayraj143243@gmail.com). The main content area displays the 'VM-internal' virtual machine details. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, and Automation. The right pane is divided into sections: 'Essentials' (Resource group: ObscuraNetCorp, Status: Running, Location: East Asia, Subscription: Azure for Students, Subscription ID: 71612ab2-c704-4cb4-bc52-fa7b4296a94d), 'Properties' (Virtual machine: Computer name: VM-internal, Operating system: Linux (ubuntu 22.04), VM generation: V2, VM architecture: x64), and 'Networking' (Public IP address: 20.24.64.141, 1 associated public IPs, Private IP address: 10.0.0.6). A 'Tags' section at the bottom allows for adding tags.

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 Virtual machine

Overview

Essentials

- Resource group (move) : ObscuraNetCorp
- Status : Running
- Location : East Asia
- Subscription (move) : Azure for Students
- Subscription ID : 71612ab2-c704-4cb4-bc52-fa7b4296a94d
- Operating system : Linux (ubuntu 22.04)
- Size : Standard B2s v2 (2 vcpus, 1 GiB memory)
- Primary NIC public IP : 20.24.104.58 (1 associated public IPs)
- Virtual network/subnet : 6604180-Abhay-G29/dmz-zone
- DNS name : Not configured
- Health state : -
- Time created : 12/25/2025, 9:23 PM UTC

Tags (edit) : Add tags

Properties Monitoring Capabilities (7) Recommendations (15) Tutorials

Virtual machine		Networking	
Computer name	VM-Web	Public IP address	20.24.104.58 (Network interface vm-web882) 1 associated public IPs
Operating system	Linux (ubuntu 22.04)	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.0.0.5
VM architecture	x64		

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 Virtual machine

Overview

Essentials

- Resource group (move) : ObscuraNetCorp
- Status : Running
- Location : East Asia
- Subscription (move) : Azure for Students
- Subscription ID : 71612ab2-c704-4cb4-bc52-fa7b4296a94d
- Operating system : Linux (ubuntu 22.04)
- Size : Standard B2s v2 (2 vcpus, 4 GiB memory)
- Primary NIC public IP : 20.187.164.160 (1 associated public IPs)
- Virtual network/subnet : 6604180-Abhay-G29/dmz-zone
- DNS name : Not configured
- Health state : -
- Time created : 12/25/2025, 8:30 PM UTC

Tags (edit) : Add tags

Properties Monitoring Capabilities (7) Recommendations (16) Tutorials

Virtual machine		Networking	
Computer name	VM-SIEM	Public IP address	20.187.164.160 (Network interface vm-siem43) 1 associated public IPs
Operating system	Linux (ubuntu 22.04)	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.0.0.4
VM architecture	x64		

8. Conclusion

This Minor Project successfully demonstrates the deployment of a basic enterprise-style cloud infrastructure using Microsoft Azure. A structured virtual network was designed with separated Internal and DMZ subnets to simulate a real corporate environment. Three Linux-based virtual machines were deployed with clearly defined roles, including identity management, web hosting, and centralized monitoring.

Only basic logging and monitoring mechanisms were implemented, and no security hardening was applied intentionally. This created a vulnerable but realistic environment that is suitable for conducting cyber-attack simulations, SOC monitoring exercises, and defensive security testing in the Major Project phase.

- 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.