Infrastructure Deployment Report

(Minor Project – Infrastructure & Logging Phase)

1. Project Overview

This project involves the deployment of a simulated enterprise infrastructure on **Microsoft Azure** as part of the Minor Project requirements.
Students act as the Infrastructure Team of a fictional organization and deploy a small-scale, Linux-based environment designed to be **functional yet intentionally unsecured**.

The primary focus of this phase is:

- Infrastructure provisioning
- Network design
- Basic logging enablement

No security hardening or access restrictions have been applied, as the environment is intended to be analyzed and secured during the Major Project phase.

---

2. Administrative & Academic Disclaimer

The Azure Student account used for this project is registered with the email address:

gorkijaimnbidu18@gmail.com

This email address is a **personal email account owned and operated solely by the student** and does not explicitly contain the student's full name.
Its usage is strictly for academic purposes related to this project and complies with institutional submission requirements.

---

3. Tenant & Resource Group Details

- **Azure Tenant Name:** `YOUR_ERPFIRST_NAMEG2`
- **Resource Group Name:** `COMPANY-NAME` (Exact match with assigned company name)

  Here : Cryvion Network

- **Operating System (All VMs):** Ubuntu 22.04 LTS
- **Project Group:** G2

All Azure resources were created within a **single Resource Group**, as mandated by the project compliance rules.

---

4. Network Architecture

4.1 Virtual Network Configuration

- **VNet Name:** Company-VNet
- **Address Space:** 10.0.0.0/16

4.2 Subnet Design

Subnet Name	CIDR Range	Purpose
Internal Subnet	10.0.1.0/24	Internal services & SIEM
DMZ Subnet	10.0.2.0/24	Public-facing web server

The DMZ subnet isolates the externally accessible server, while internal services and log analysis components remain within the internal subnet.

---

5. Virtual Machine Inventory

VM 1 – Internal Server

- **OS:** Ubuntu 22.04 LTS
- **Subnet:** Internal
- **Roles:**
  - FreeIPA (Identity Management – LDAP & Kerberos)
  - File Server (Samba/NFS)
  - Internal service hosting
- **Purpose:** Simulates corporate identity and internal resource management

---

VM 2 – Web Server (DMZ)

- **OS:** Ubuntu 22.04 LTS
- **Subnet:** DMZ
- **Roles:**
  - Apache / Nginx Web Server
  - Hosts a basic web page

- **Purpose:** Represents an external-facing service and primary attack surface

---

VM 3 – SIEM & Analyst Workstation

- **OS:** Ubuntu 22.04 LTS
- **Subnet:** Internal
- **Roles:**
  - **Wazuh SIEM**
  - Log aggregation and analysis
- **Purpose:** Centralized logging and monitoring system

---

6. Network Security Groups (NSGs)

- Basic NSGs were configured to allow required communication
- No firewall hardening or restrictive rules were applied
- The infrastructure remains intentionally vulnerable for future security testing

---

Network Diagram (Cisco Packet Tracer Representation)

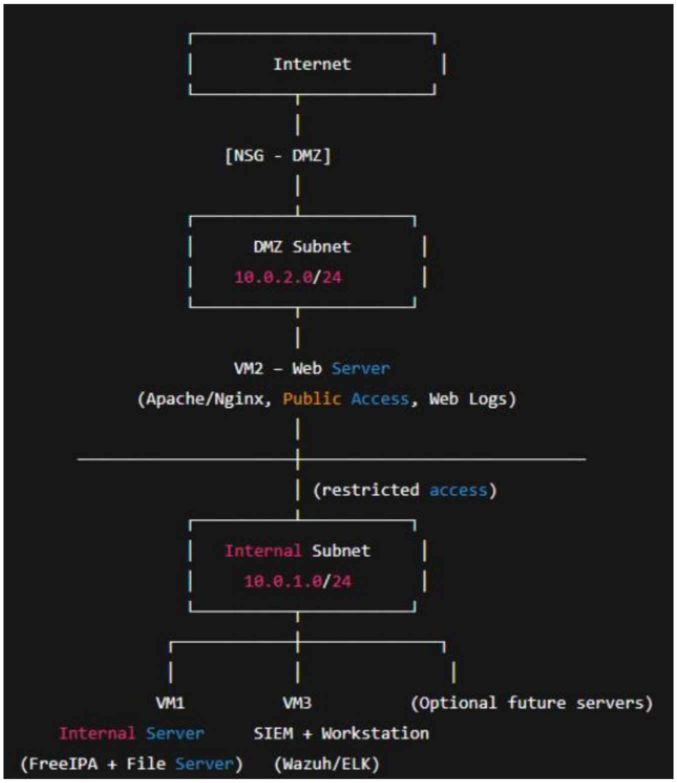
Logical Representation

Since Azure cannot be simulated directly, a logical network diagram was created using **Cisco Packet Tracer**.

Traffic Flow

- Internet → Web Server (HTTP/HTTPS)
- Web Server → SIEM (Web access & error logs)
- Internal Server → SIEM (Auth, Syslog, Audit logs)

All subnets, servers, and traffic paths are clearly labeled in the diagram.



```
                ┌────────────────────┐
                │      Internet      │
                └─────────┬──────────┘
                          │
                     [NSG - DMZ]
                          │
                ┌─────────┴────────┐
                │    DMZ Subnet    │
                │   10.0.2.0/24    │
                └─────────┬────────┘
                          │
                  VM2 - Web Server
         (Apache/Nginx, Public Access, Web Logs)
                          │
      ────────────────────┼────────────────────
                          │ (restricted access)
                ┌─────────┴────────┐
                │ Internal Subnet  │
                │   10.0.1.0/24    │
                └─────────┬────────┘
              ┌───────────┼────────────┐
              │           │            │
             VM1         VM3       (Optional future servers)
      Internal Server   SIEM + Workstation
  (FreeIPA + File Server)   (Wazuh/ELK)
```

Logging Summary

7. Logging Configuration Overview

Basic logging was enabled on all servers without modification of default security parameters.

7.1 Logs Generated

VM 1 – Internal Server

- `/var/log/syslog`
- `/var/log/auth.log`
- FreeIPA authentication logs
- File server access logs
- `auditd` logs (default configuration)

VM 2 – Web Server

- Web access logs (`access.log`)

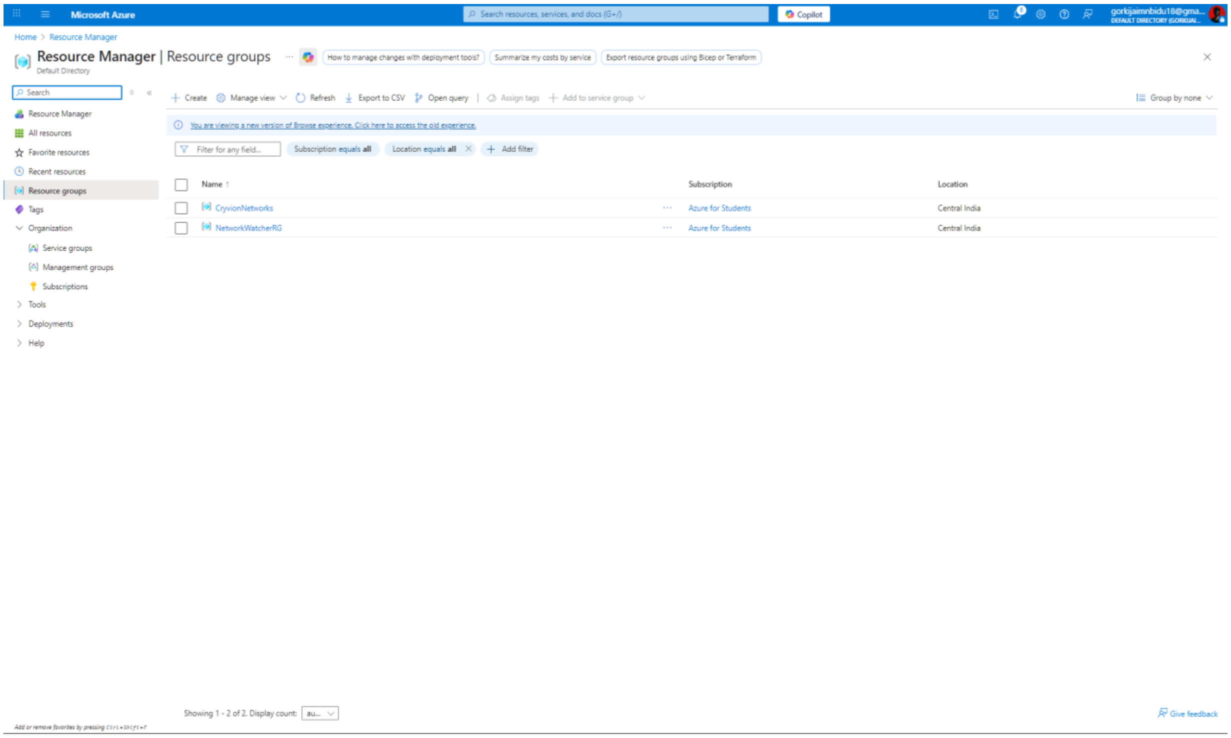
- Web error logs (`error.log`)
- `/var/log/syslog`
- `/var/log/auth.log`
- `auditd` logs

7.2 Log Forwarding Setup

- **Wazuh agent** installed on:
  - VM 1 (Internal Server)
  - VM 2 (Web Server)
- Logs are forwarded to:
  - VM 3 (Wazuh SIEM Server)

No log filtering, tuning, or correlation rules were applied.

<u>Screenshots from the project:</u>

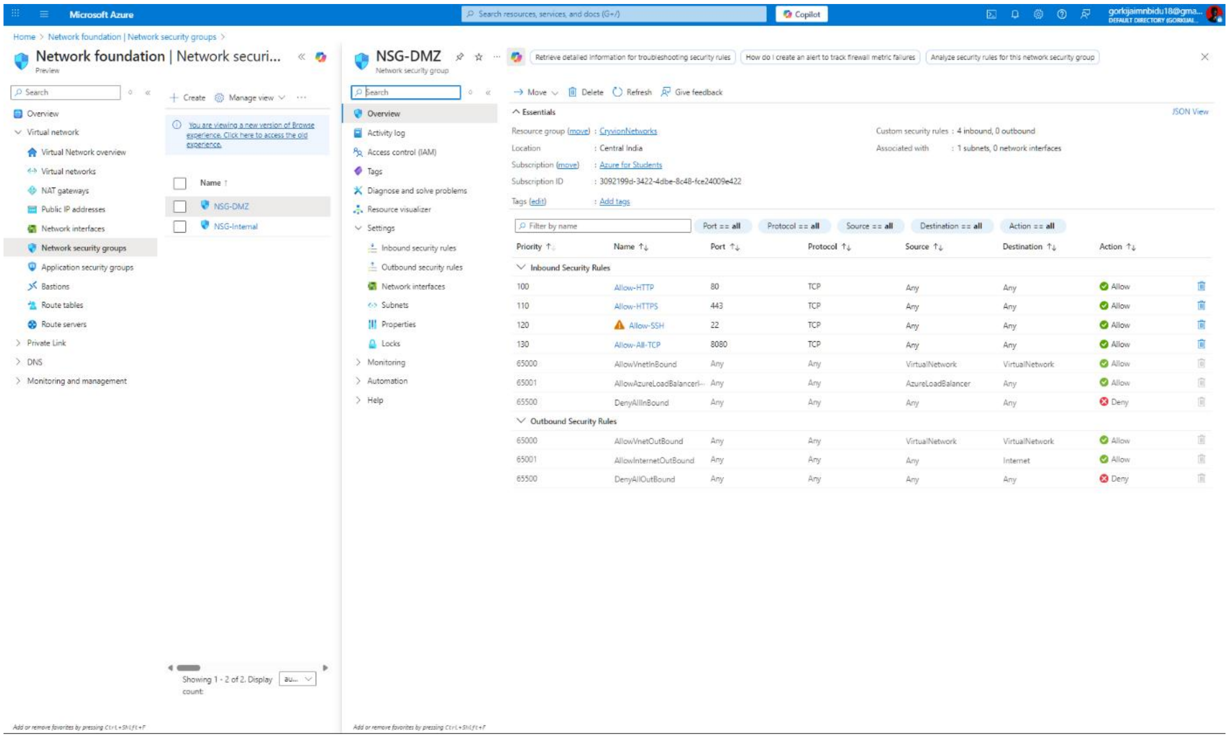


You are viewing a new version of Browse experience. Click here to access the old experience.

□	Name ↑	Subscription	Location
□	CryvionNetworks	Azure for Students	Central India
□	NetworkWatcherRG	Azure for Students	Central India

Showing 1 - 2 of 2.

Add or remove favorites by pressing Ctrl+Shift+F


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
gorkijaimnbidu18@gma...
DEFAULT DIRECTORY (GORKIJAL...
Home > Network foundation | Network security groups >
Network foundation | Network securi...
Preview
Search
Overview
Virtual network
Virtual Network overview
Virtual networks
NAT gateways
Public IP addresses
Network interfaces
Network security groups
Application security groups
Bastions
Route tables
Route servers
Private Link
DNS
Monitoring and management
+ Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name ↑
NSG-DMZ
NSG-Internal
Showing 1 - 2 of 2. Display count:
au...
Add or remove favorites by pressing Ctrl+Shift+F
NSG-DMZ
Network security group
Retrieve detailed information for troubleshooting security rules
How do I create an alert to track firewall metric failures
Analyze security rules for this network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Add or remove favorites by pressing Ctrl+Shift+F

Resource group (move) : CryvionNetworks

Location : Central India

Subscription (move) : Azure for Students

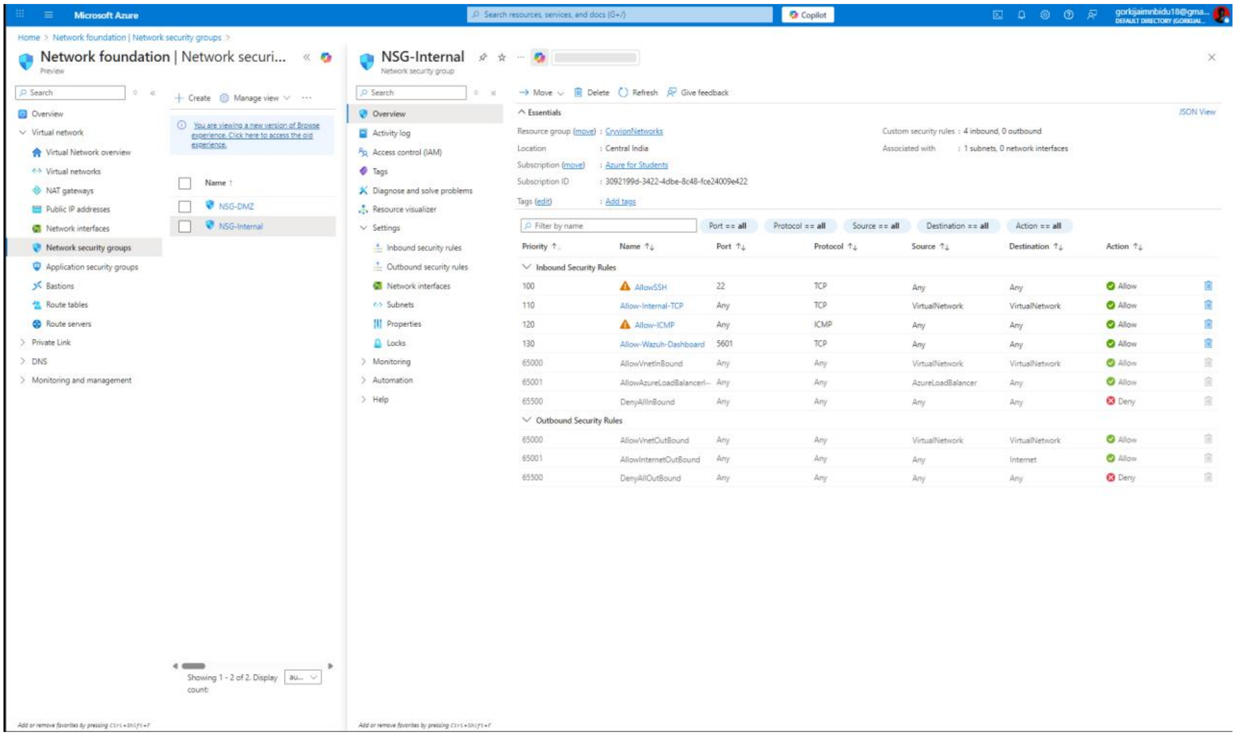
Subscription ID : 3092199d-3422-4dbe-8c48-fce24009e422

Tags (edit) : Add tags

Custom security rules : 4 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
100	Allow-HTTP	80	TCP	Any	Any	✓ Allow
110	Allow-HTTPS	443	TCP	Any	Any	✓ Allow
120	⚠ Allow-SSH	22	TCP	Any	Any	✓ Allow
130	Allow-All-TCP	8080	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny



Resource group (move) : CryvionNetworks

Location : Central India

Subscription (move) : Azure for Students

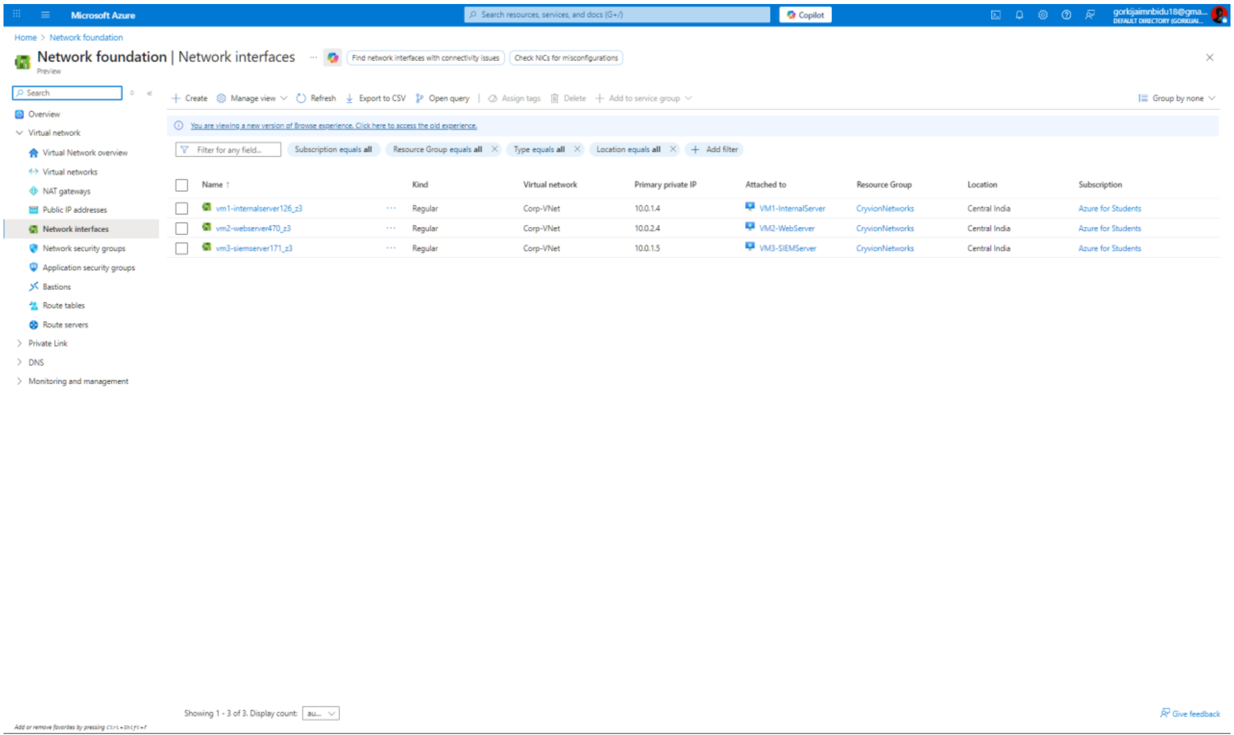
Subscription ID : 3092199d-3422-4dbe-8c48-fce24009e422

Tags (edit) : Add tags

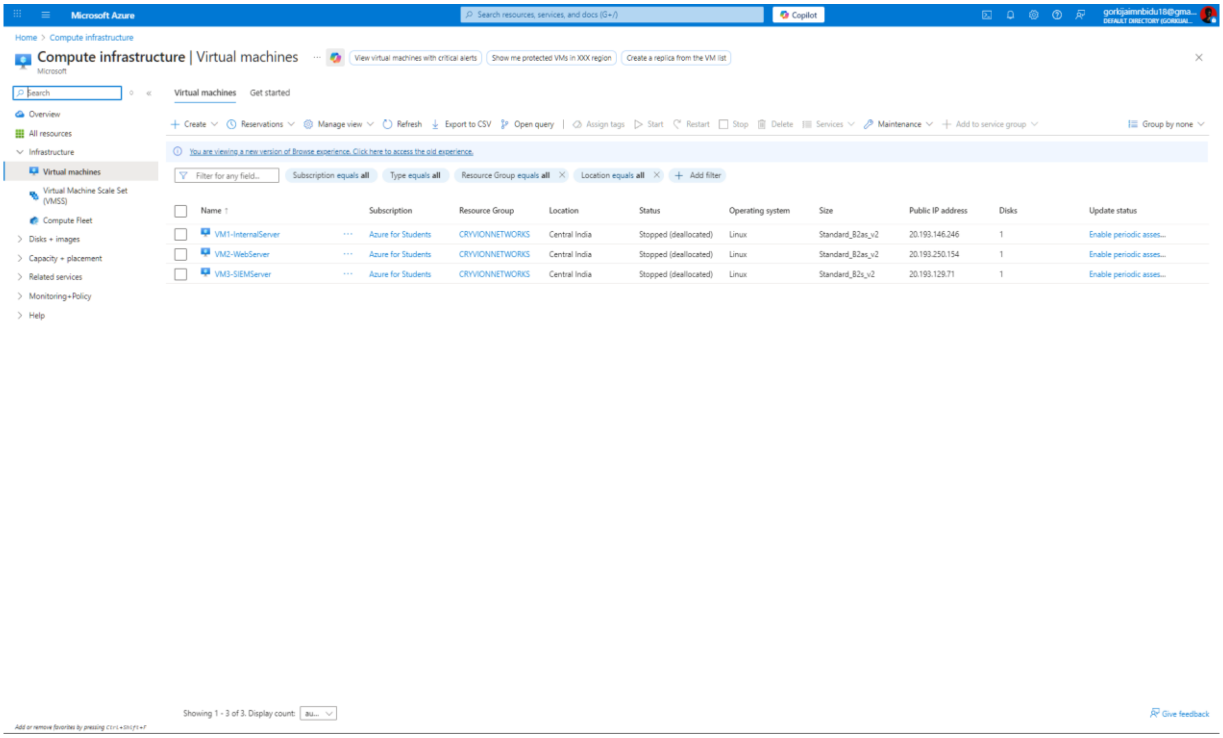
Custom security rules : 4 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

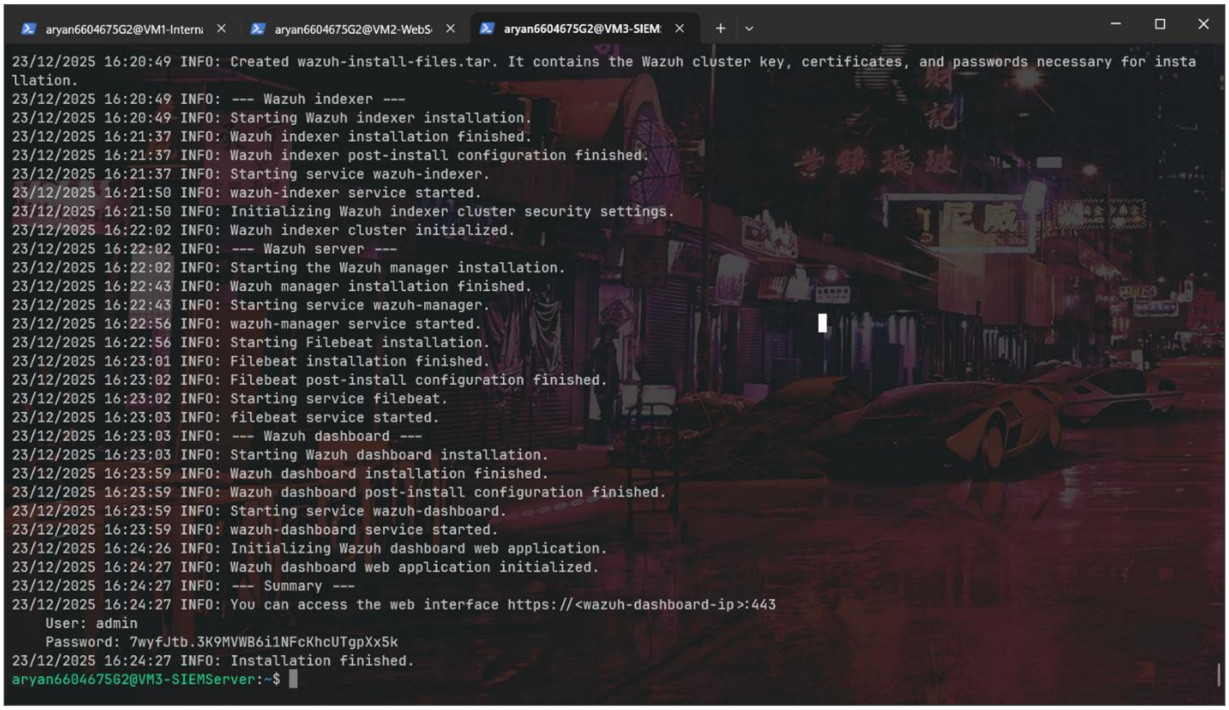
Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
100	⚠ AllowSSH	22	TCP	Any	Any	✓ Allow
110	Allow-Internal-TCP	Any	TCP	VirtualNetwork	VirtualNetwork	✓ Allow
120	⚠ Allow-ICMP	Any	ICMP	Any	Any	✓ Allow
130	Allow-Wazuh-Dashboard	5601	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
gorkijaimnbidu18@gma...
DEFAULT DIRECTORY (GORKIJAI...
Home > Network foundation
Network foundation | Network interfaces
Preview
Find network interfaces with connectivity issues
Check NICs for misconfigurations
Search
Overview
Virtual network
Virtual Network overview
Virtual networks
NAT gateways
Public IP addresses
Network interfaces
Network security groups
Application security groups
Bastions
Route tables
Route servers
Private Link
DNS
Monitoring and management
+ Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
+ Add to service group
Group by none
You are viewing a new version of Browse experience. Click here to access the old experience.
Filter for any field...
Subscription equals all
Resource Group equals all
Type equals all
Location equals all
+ Add filter
Showing 1 - 3 of 3. Display count: au...
Give feedback
Add or remove favorites by pressing Ctrl+Shift+F

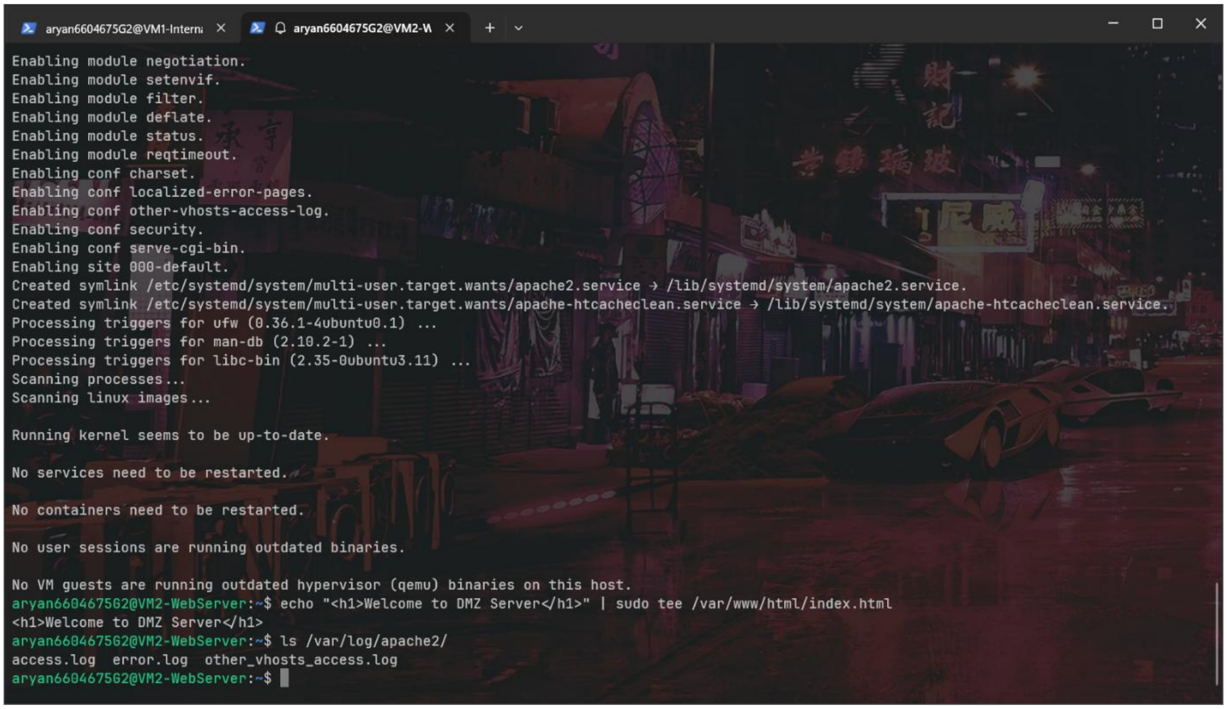
□	Name ↑		Kind	Virtual network	Primary private IP	Attached to	Resource Group	Location	Subscription
□	vm1-internalserver126_z3	···	Regular	Corp-VNet	10.0.1.4	VM1-InternalServer	CryvionNetworks	Central India	Azure for Students
□	vm2-webserver470_z3	···	Regular	Corp-VNet	10.0.2.4	VM2-WebServer	CryvionNetworks	Central India	Azure for Students
□	vm3-siemserver171_z3	···	Regular	Corp-VNet	10.0.1.5	VM3-SIEMServer	CryvionNetworks	Central India	Azure for Students


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
gorkijaimnbidu18@gma...
DEFAULT DIRECTORY (GORKIJAI...
Home > Compute infrastructure
Compute infrastructure | Virtual machines
Microsoft
View virtual machines with critical alerts
Show me protected VMs in XXX region
Create a replica from the VM list
Search
Overview
All resources
Infrastructure
Virtual machines
Virtual Machine Scale Set (VMSS)
Compute Fleet
Disks + images
Capacity + placement
Related services
Monitoring+Policy
Help
Virtual machines
Get started
+ Create
Reservations
Manage view
Refresh
Export to CSV
Open query
Assign tags
Start
Restart
Stop
Delete
Services
Maintenance
+ Add to service group
Group by none
You are viewing a new version of Browse experience. Click here to access the old experience.
Filter for any field...
Subscription equals all
Type equals all
Resource Group equals all
Location equals all
+ Add filter
Showing 1 - 3 of 3. Display count: au...
Give feedback
Add or remove favorites by pressing Ctrl+Shift+F

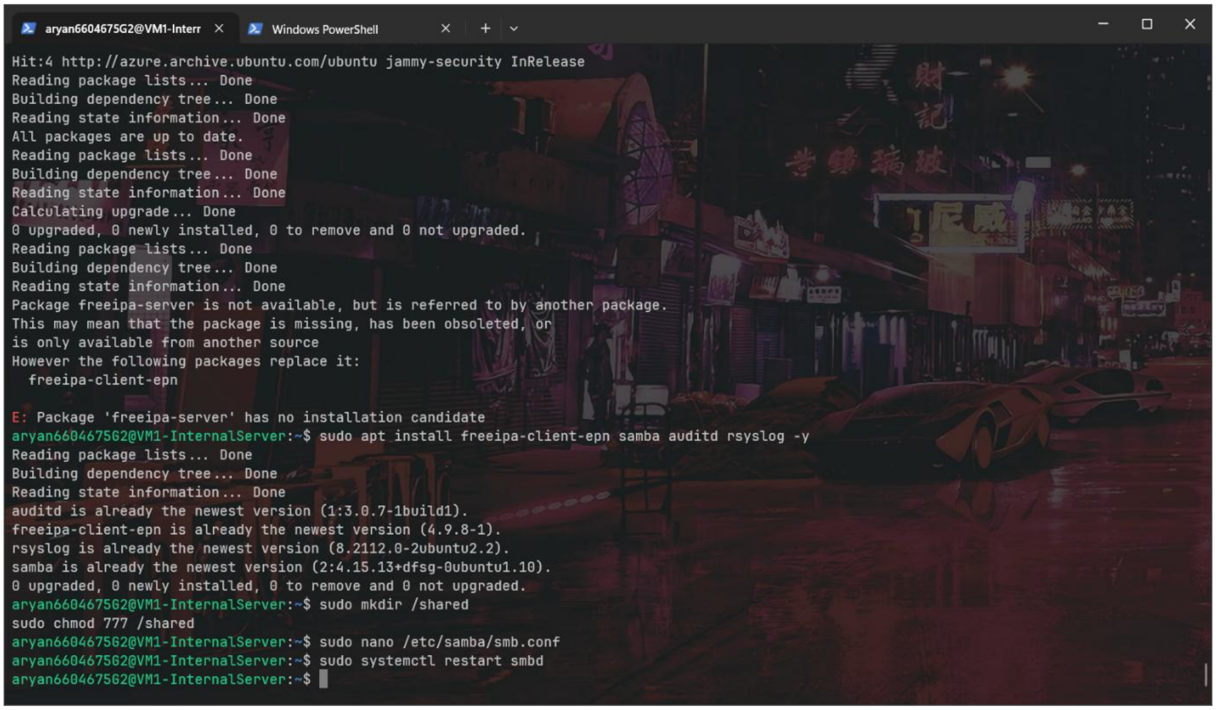
□	Name ↑		Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address	Disks	Update status
□	VM1-InternalServer	···	Azure for Students	CRYVIONNETWORKS	Central India	Stopped (deallocated)	Linux	Standard_B2as_v2	20.193.146.246	1	Enable periodic asses...
□	VM2-WebServer	···	Azure for Students	CRYVIONNETWORKS	Central India	Stopped (deallocated)	Linux	Standard_B2as_v2	20.193.250.154	1	Enable periodic asses...
□	VM3-SIEMServer	···	Azure for Students	CRYVIONNETWORKS	Central India	Stopped (deallocated)	Linux	Standard_B2s_v2	20.193.129.71	1	Enable periodic asses...



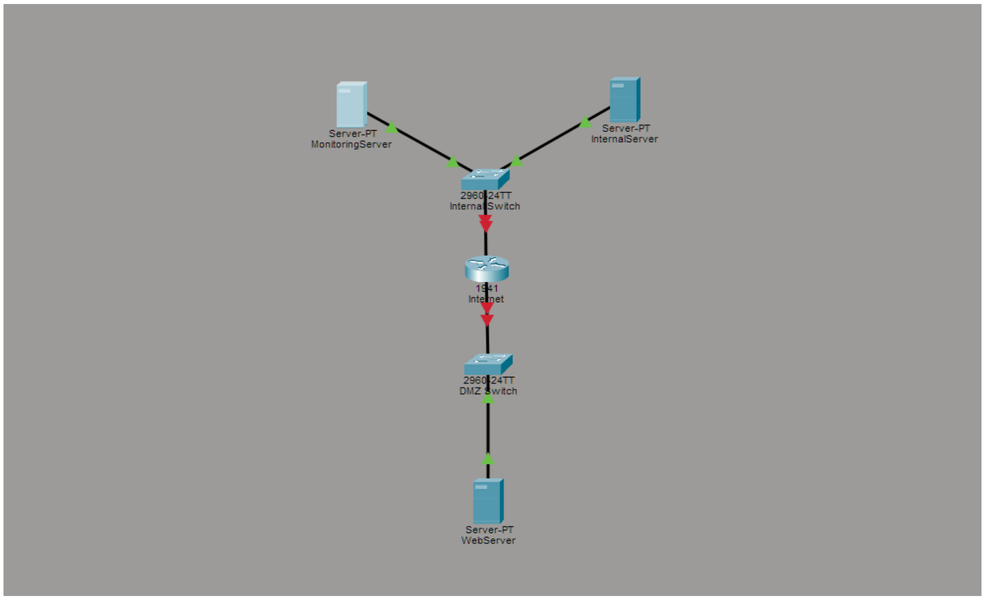
```
23/12/2025 16:20:49 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for insta
llation.
23/12/2025 16:20:49 INFO: --- Wazuh indexer ---
23/12/2025 16:20:49 INFO: Starting Wazuh indexer installation.
23/12/2025 16:21:37 INFO: Wazuh indexer installation finished.
23/12/2025 16:21:37 INFO: Wazuh indexer post-install configuration finished.
23/12/2025 16:21:37 INFO: Starting service wazuh-indexer.
23/12/2025 16:21:50 INFO: wazuh-indexer service started.
23/12/2025 16:21:50 INFO: Initializing Wazuh indexer cluster security settings.
23/12/2025 16:22:02 INFO: Wazuh indexer cluster initialized.
23/12/2025 16:22:02 INFO: --- Wazuh server ---
23/12/2025 16:22:02 INFO: Starting the Wazuh manager installation.
23/12/2025 16:22:43 INFO: Wazuh manager installation finished.
23/12/2025 16:22:43 INFO: Starting service wazuh-manager.
23/12/2025 16:22:56 INFO: wazuh-manager service started.
23/12/2025 16:22:56 INFO: Starting Filebeat installation.
23/12/2025 16:23:01 INFO: Filebeat installation finished.
23/12/2025 16:23:02 INFO: Filebeat post-install configuration finished.
23/12/2025 16:23:02 INFO: Starting service filebeat.
23/12/2025 16:23:03 INFO: filebeat service started.
23/12/2025 16:23:03 INFO: --- Wazuh dashboard ---
23/12/2025 16:23:03 INFO: Starting Wazuh dashboard installation.
23/12/2025 16:23:59 INFO: Wazuh dashboard installation finished.
23/12/2025 16:23:59 INFO: Wazuh dashboard post-install configuration finished.
23/12/2025 16:23:59 INFO: Starting service wazuh-dashboard.
23/12/2025 16:23:59 INFO: wazuh-dashboard service started.
23/12/2025 16:24:26 INFO: Initializing Wazuh dashboard web application.
23/12/2025 16:24:27 INFO: Wazuh dashboard web application initialized.
23/12/2025 16:24:27 INFO: --- Summary ---
23/12/2025 16:24:27 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: 7wyfJtb.3K9MVWB6i1NFcKhcUTgpXx5k
23/12/2025 16:24:27 INFO: Installation finished.
aryan6604675G2@VM3-SIEMServer:~$
```



```
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.11) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
aryan6604675G2@VM2-WebServer:~$ echo "<h1>Welcome to DMZ Server</h1>" | sudo tee /var/www/html/index.html
<h1>Welcome to DMZ Server</h1>
aryan6604675G2@VM2-WebServer:~$ ls /var/log/apache2/
access.log  error.log  other_vhosts_access.log
aryan6604675G2@VM2-WebServer:~$
```



```
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package freeipa-server is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source
However the following packages replace it:
  freeipa-client-epn

E: Package 'freeipa-server' has no installation candidate
aryan6604675G2@VM1-InternalServer:~$ sudo apt install freeipa-client-epn samba auditd rsyslog -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
auditd is already the newest version (1:3.0.7-1build1).
freeipa-client-epn is already the newest version (4.9.8-1).
rsyslog is already the newest version (8.2112.0-2ubuntu2.2).
samba is already the newest version (2:4.15.13+dfsg-0ubuntu1.10).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
aryan6604675G2@VM1-InternalServer:~$ sudo mkdir /shared
sudo chmod 777 /shared
aryan6604675G2@VM1-InternalServer:~$ sudo nano /etc/samba/smb.conf
aryan6604675G2@VM1-InternalServer:~$ sudo systemctl restart smbd
aryan6604675G2@VM1-InternalServer:~$ 
```



Conclusion :

This project establishes a functional enterprise-style infrastructure deployed on Microsoft Azure, consisting of segmented internal and DMZ networks hosting core services and an external-facing web server.

All systems were deployed using Ubuntu 22.04 and intentionally left without security hardening to reflect realistic baseline environments. Centralized logging was implemented using Wazuh, enabling effective collection and visibility of system, authentication, audit, and web server logs.