

INFRASTRUCTURE DEPLOYMENT

GROUP 2

GROUP MEMBERS

Srishti Anand (301313123052)
Roshan Sahu (301313123044)
Rahul Kumar Gupta (301313123039)
Subham Gupta (301313123053)
Leman Kumar Sahu (301313123034)
Aryan (301313123010)

PROJECT DESCRIPTION

Overview

In this project, students will act as the Infrastructure Team of a simulated company.

They will deploy a small-scale enterprise environment using the Microsoft Azure Student Account, consisting of three Linux-based virtual machines.

This phase focuses ONLY on building the core infrastructure and enabling basic logging.

Objective

To design and deploy a functional but intentionally unsecured mini-company infrastructure using Linux servers on Azure, enable basic event logging, and prepare the environment for cyber-attacks and SOC analysis in the next phase.

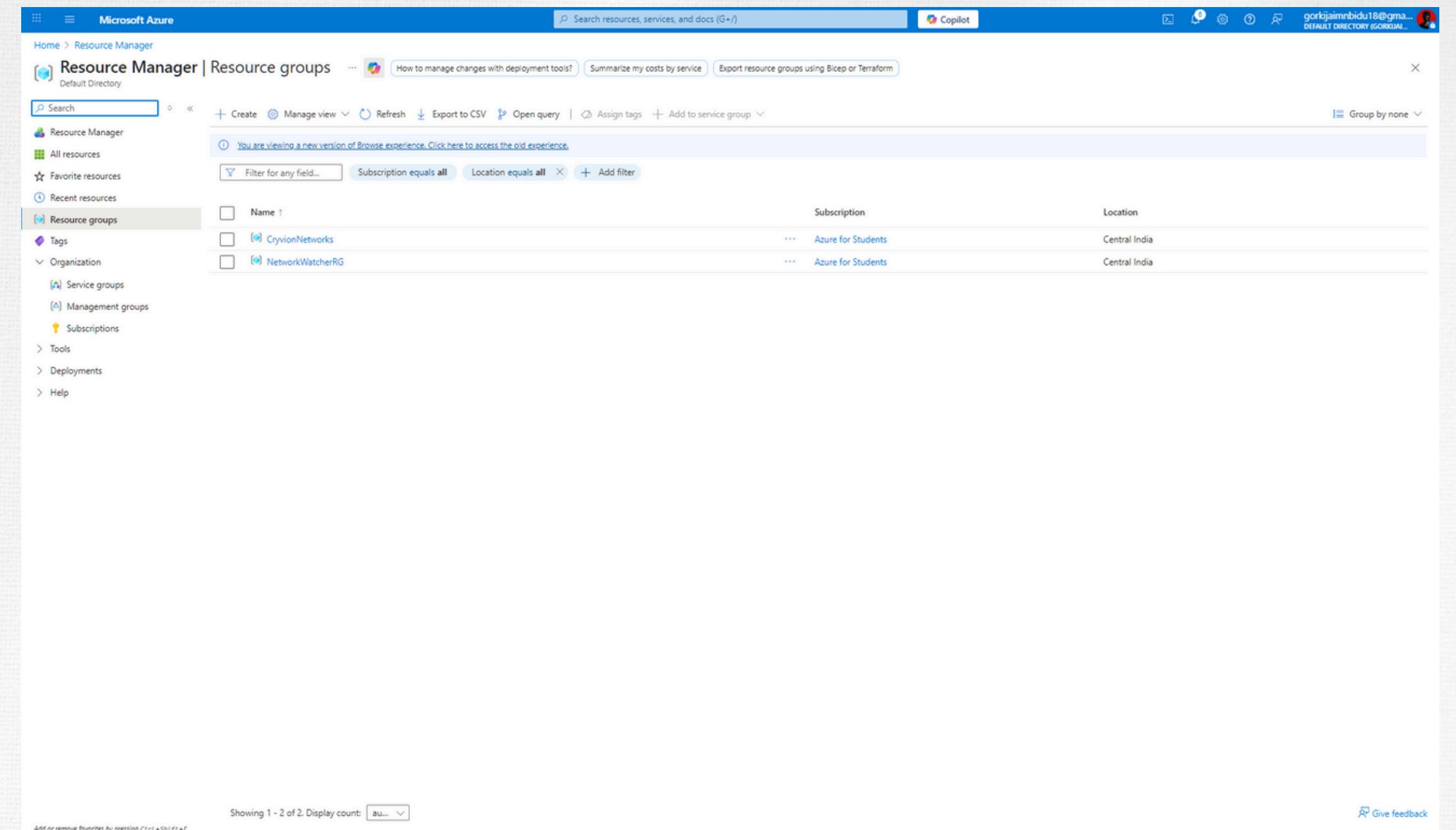
PHASE - 1

CREATE RESOURCE GROUP

The objective for each group of the project is clearly defined and the resource group name should be same as the designated one.

For group 2 it is the same as Cryvion Network.

The following screenshot shows the creation of the Resource group, Cryvion Network.



The screenshot displays the Microsoft Azure Resource Manager interface. The left sidebar shows navigation options: Home, Resource Manager (selected), All resources, Favorite resources, Recent resources, Resource groups (selected), Tags, Organization (Service groups, Management groups, Subscriptions), Tools, Deployments, and Help. The main content area shows a table of existing Resource Groups. The table has columns for Name, Subscription, and Location. Two entries are listed:

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

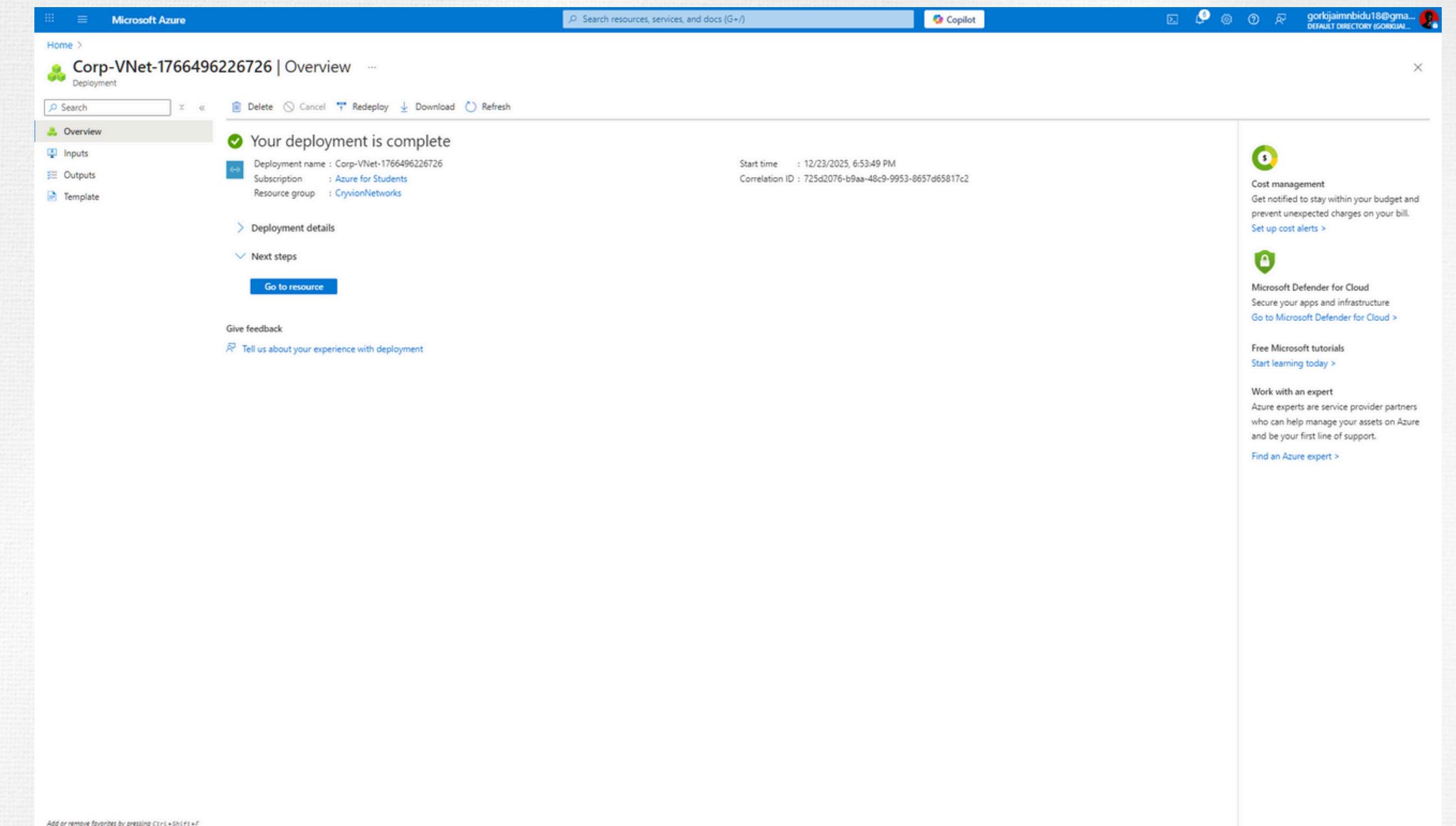
At the bottom of the page, there is a note: "Showing 1 - 2 of 2. Display count: au...".

PHASE - 2

CREATE VIRTUAL NETWORK (A)

The virtual machines also require the creation of an isolated environment to work in.

The following screenshot shows the creation of the Virtual network called Corp-VNet.



PHASE - 2

CREATE VIRTUAL NETWORK (B)

The virtual machines which will be created will need to have IP addresses on the same subnet for two of the three virtual machines whereas one of the VM's will be on a separate subnet.

The following screenshot shows the creation of the 3 subnets for 3 separate VM's.

The screenshot shows the Microsoft Azure portal interface for managing network interfaces. The left sidebar navigation includes Home, Network foundation, Network interfaces (selected), Preview, Overview, Virtual network, Virtual network overview, Virtual networks, NAT gateways, Public IP addresses, Network interfaces (selected), Network security groups, Application security groups, Bastions, Route tables, Route servers, Private Link, DNS, and Monitoring and management. The main content area displays a table of network interfaces:

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

At the bottom of the table, there are filter options: Filter for any field..., Subscription equals all, Resource Group equals all, Type equals all, Location equals all, and Add filter. The status bar at the bottom indicates "Showing 1 - 3 of 3. Display count: 20...".

PHASE - 2

CREATE VIRTUAL NETWORK (C)

While creating the subnets we would also require separate Network Security Groups for all the machines, namely one group for the DMZ server and another for the Internal Server and the SIEM Workstation.

The following screenshot shows the creation of the 2 Network security Groups.

This screenshot shows the Microsoft Azure portal interface for managing Network Security Groups. It displays two separate Network Security Groups: NSG-DMZ and NSG-Internal. The NSG-DMZ group is selected, showing its settings and security rules. The NSG-Internal group is also listed in the left sidebar. The security rules for NSG-DMZ include various inbound and outbound rules for ports like 80, 443, 22, 8080, and 5601, along with default allow and deny rules. The NSG-Internal group has similar but slightly different rule configurations.

This screenshot shows the Microsoft Azure portal interface for managing Network Security Groups. It displays two separate Network Security Groups: NSG-DMZ and NSG-Internal. The NSG-Internal group is selected, showing its settings and security rules. The NSG-Internal group has security rules for ports 22, 8080, 5601, and 56000, along with default allow and deny rules. The NSG-DMZ group is also listed in the left sidebar. The interface includes standard Azure navigation and search bars at the top.

PHASE - 3

CREATE VIRTUAL MACHINES

The virtual machines would be on the server with different public IP and different internal IP on the same subnet.

The machines on the same subnet would be the Internal Server and SIEM Workstation.

Whereas the DMZ server will be on a different subnet.

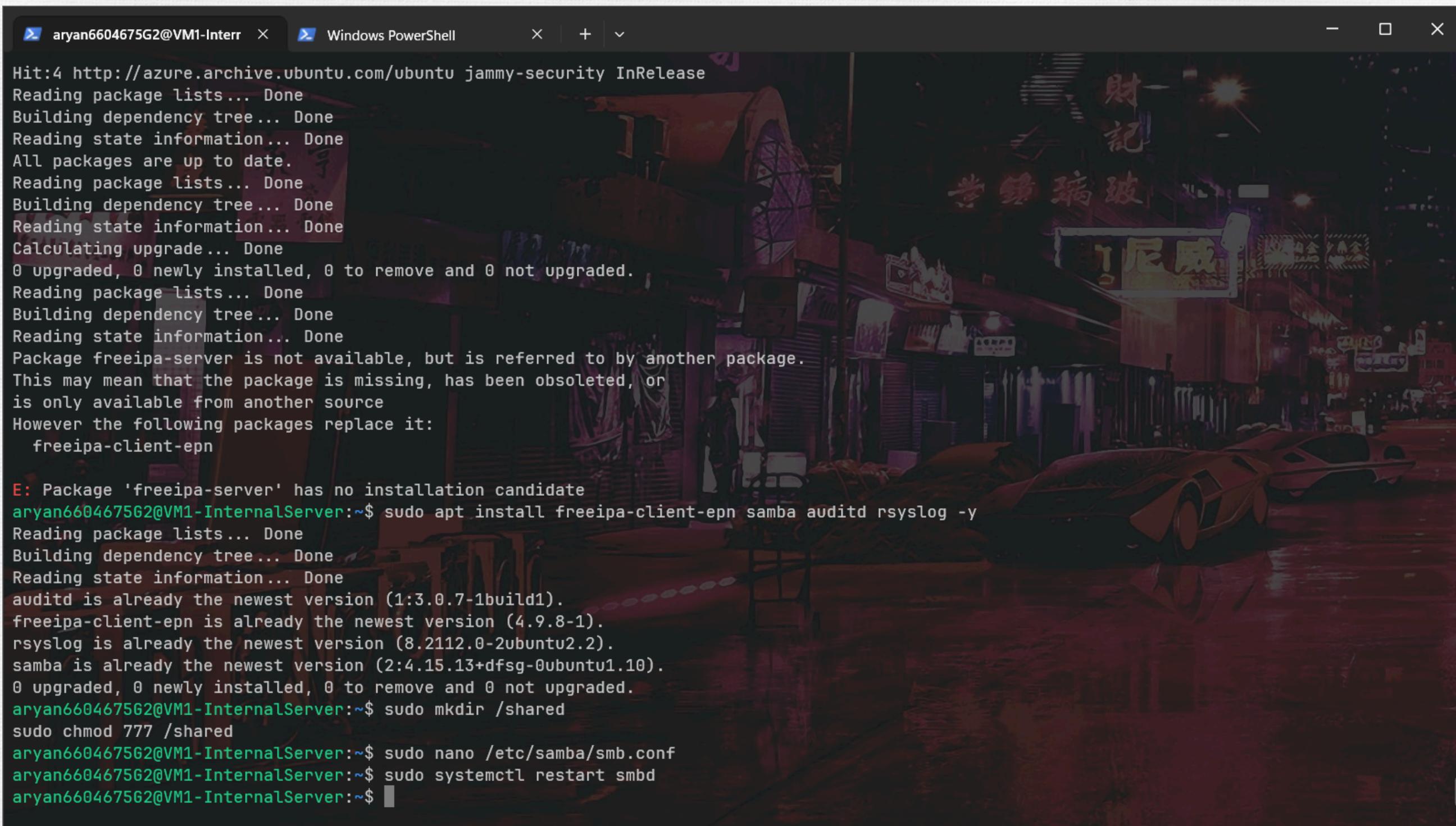
The following screenshot shows the creation of the 3 separate VM's.

The screenshot shows the Microsoft Azure Compute Infrastructure Virtual Machines page. The left sidebar navigation includes Home, Compute infrastructure, Infrastructure, and Virtual machines, which is currently selected. The main content area displays a table of three virtual machines:

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...

At the bottom of the page, there is a note: "Showing 1 - 3 of 3. Display count: au..".

PHASE - 4 (SCREENSHOTS)



A screenshot of a Windows PowerShell window titled "aryan6604675G2@VM1-InternalServer". The window shows terminal command-line output. The background of the window is a dark, stylized image of a futuristic city at night with neon signs and a flying car.

```
aryan6604675G2@VM1-InternalServer ~$ Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
aryan6604675G2@VM1-InternalServer ~$ Reading package lists... Done
aryan6604675G2@VM1-InternalServer ~$ Building dependency tree... Done
aryan6604675G2@VM1-InternalServer ~$ Reading state information... Done
aryan6604675G2@VM1-InternalServer ~$ All packages are up to date.
aryan6604675G2@VM1-InternalServer ~$ Reading package lists... Done
aryan6604675G2@VM1-InternalServer ~$ Building dependency tree... Done
aryan6604675G2@VM1-InternalServer ~$ Reading state information... Done
aryan6604675G2@VM1-InternalServer ~$ Calculating upgrade... Done
aryan6604675G2@VM1-InternalServer ~$ 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
aryan6604675G2@VM1-InternalServer ~$ Reading package lists... Done
aryan6604675G2@VM1-InternalServer ~$ Building dependency tree... Done
aryan6604675G2@VM1-InternalServer ~$ Reading state information... Done
aryan6604675G2@VM1-InternalServer ~$ Package freeipa-server is not available, but is referred to by another package.
aryan6604675G2@VM1-InternalServer ~$ This may mean that the package is missing, has been obsoleted, or
aryan6604675G2@VM1-InternalServer ~$ is only available from another source
aryan6604675G2@VM1-InternalServer ~$ However the following packages replace it:
aryan6604675G2@VM1-InternalServer ~$   freeipa-client-epn

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

PHASE - 4 (SCREENSHOTS)

```
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:~$
```

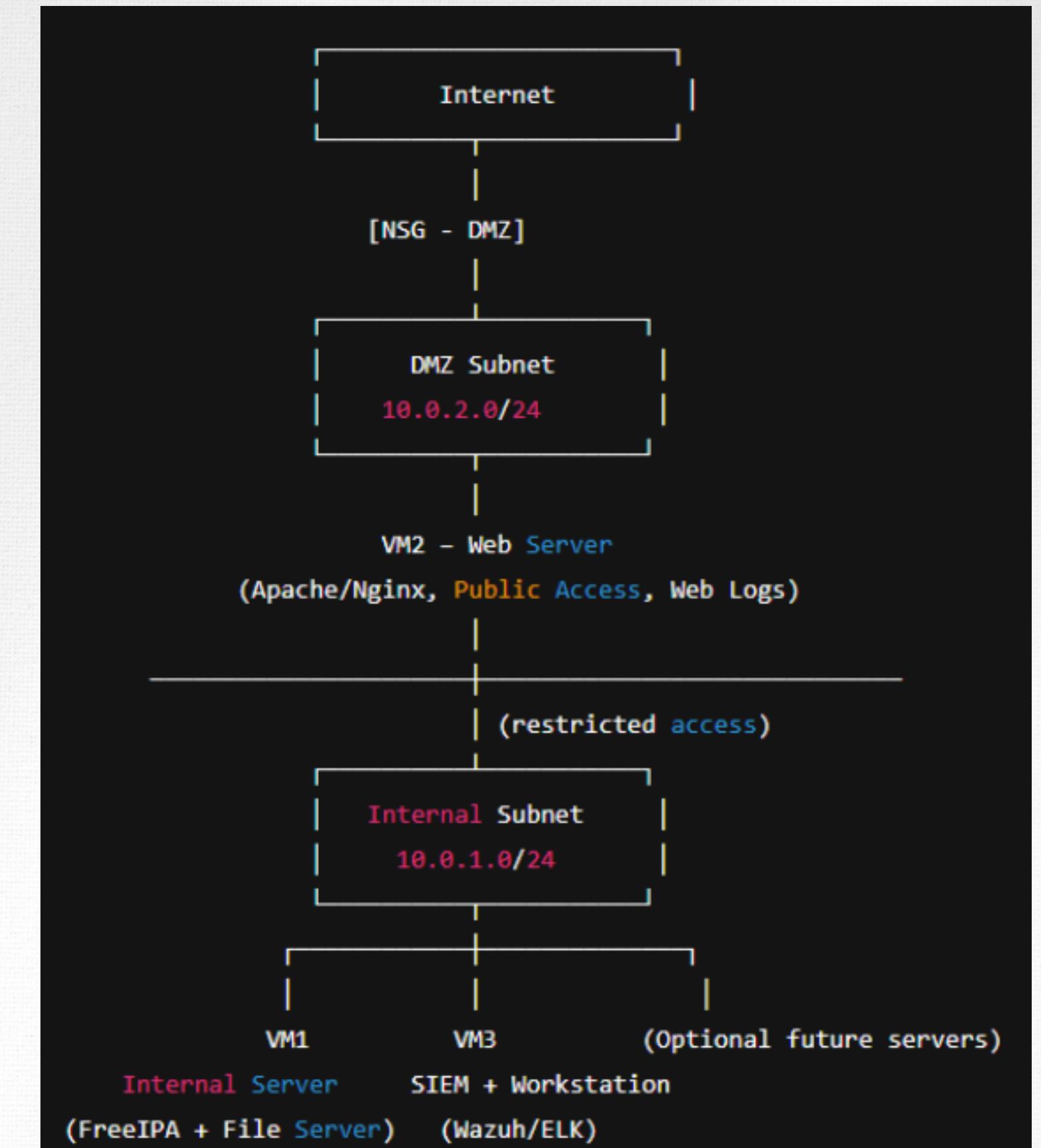
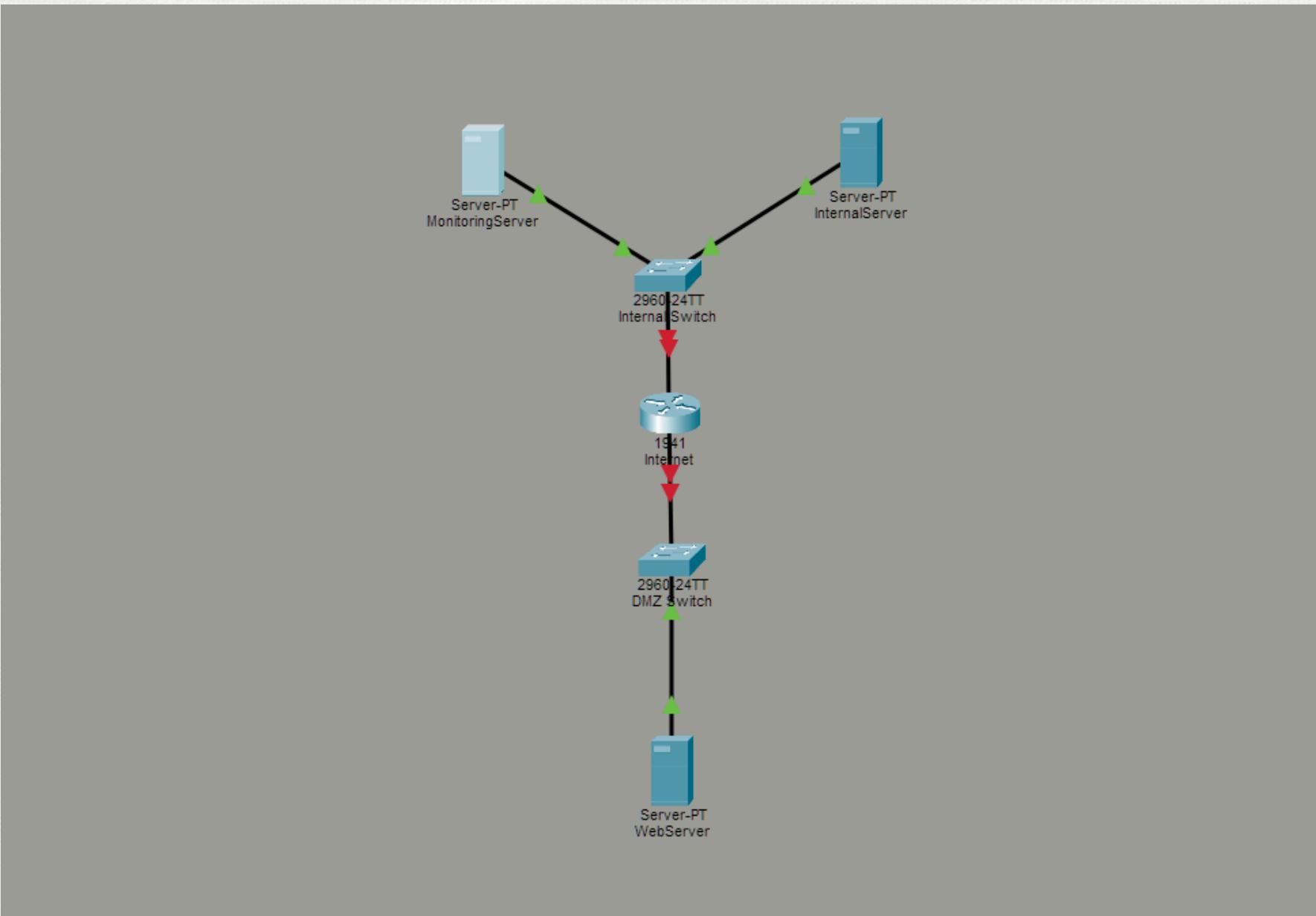
PHASE - 4 (SCREENSHOTS)

```
aryan6604675G2@VM1-Internal ~
aryan6604675G2@VM2-WebS ~
aryan6604675G2@VM3-SIEM:~$ + ^

23/12/2025 16:20:49 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
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-SIEM:~$
```

PHASE - 5

NETWORK STRUCTURE



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.

This confirms that the environment is operational, observable, and ready for security testing and SOC analysis in the subsequent project phase.

THANK YOU