Project Title:
Infrastructure Deployment, Logging & SOC Readiness on Cloud

Student Name: Pooja Shriwas
Company Name (Resource Group): Hexaroot-Systems
Cloud Platform: Microsoft Azure
Project Type: Minor + Major Project

1. INTRODUCTION

This project focuses on deploying a small-scale enterprise infrastructure on cloud and preparing it for security monitoring and SOC analysis.
The project is divided into two phases:

- **Minor Project:** Infrastructure deployment and basic logging
- **Major Project:** Log analysis, attack simulation, and security monitoring

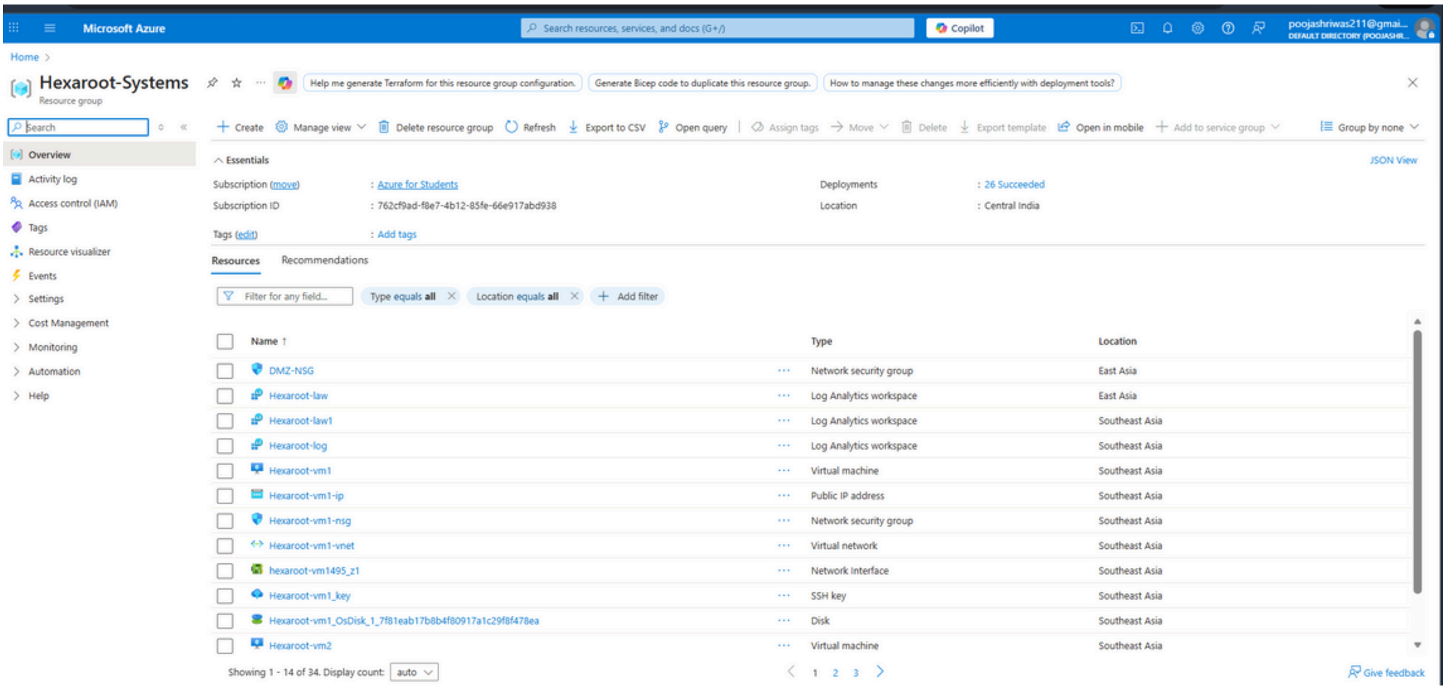
2. MINOR PROJECT – INFRASTRUCTURE DEPLOYMENT

2.1 Objective

To deploy a basic enterprise infrastructure with multiple Linux servers and enable logging without applying any security hardening.

2.2 Resource Group

- A single Azure Resource Group named **Hexaroot-Systems** was created.
- All cloud resources were deployed inside this resource group.



Essentials

Subscription (move) : Azure for Students
Subscription ID : 762cf9ad-f8e7-4b12-85fe-66e917abd938
Tags (edit) : Add tags
Deployments : 26 Succeeded
Location : Central India

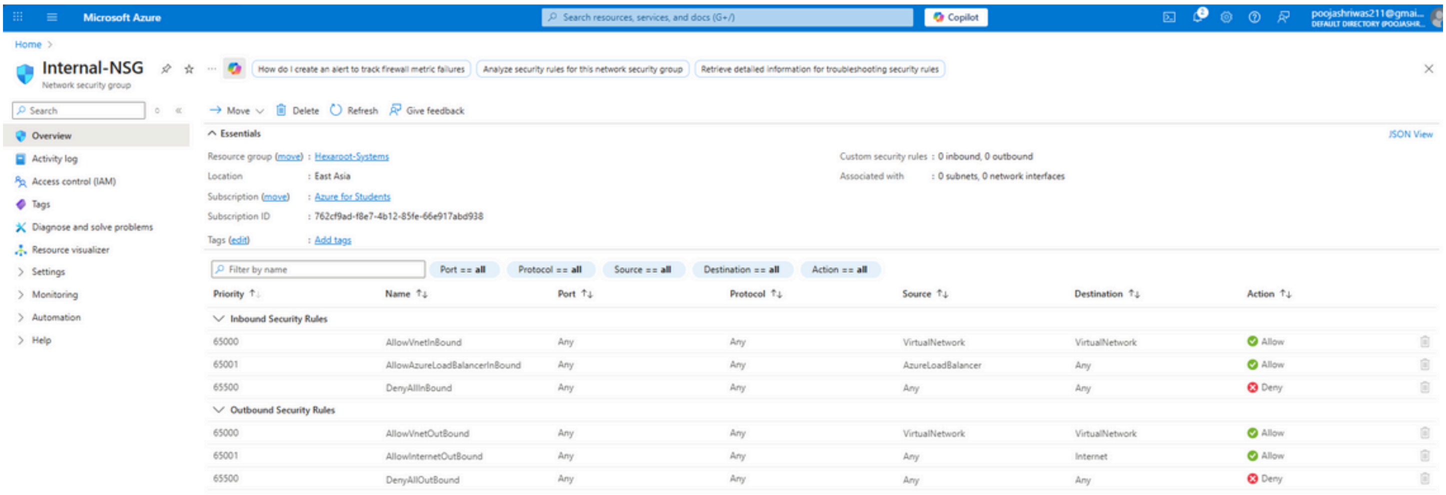
Name ↑	Type	Location
DMZ-NSG	Network security group	East Asia
Hexaroot-law	Log Analytics workspace	East Asia
Hexaroot-law1	Log Analytics workspace	Southeast Asia
Hexaroot-log	Log Analytics workspace	Southeast Asia
Hexaroot-vm1	Virtual machine	Southeast Asia
Hexaroot-vm1-ip	Public IP address	Southeast Asia
Hexaroot-vm1-nsg	Network security group	Southeast Asia
Hexaroot-vm1-vnet	Virtual network	Southeast Asia
hexaroot-vm1495_z1	Network Interface	Southeast Asia
Hexaroot-vm1_key	SSH key	Southeast Asia
Hexaroot-vm1_OsDisk_1_7f81eab17b8b4f80917a1c29f8f478ea	Disk	Southeast Asia
Hexaroot-vm2	Virtual machine	Southeast Asia

Showing 1 - 14 of 34. Display count: auto

< 1 2 3 >

- One Virtual Network was created
- Two subnets were configured:

- Internal Subnet
- DMZ Subnet

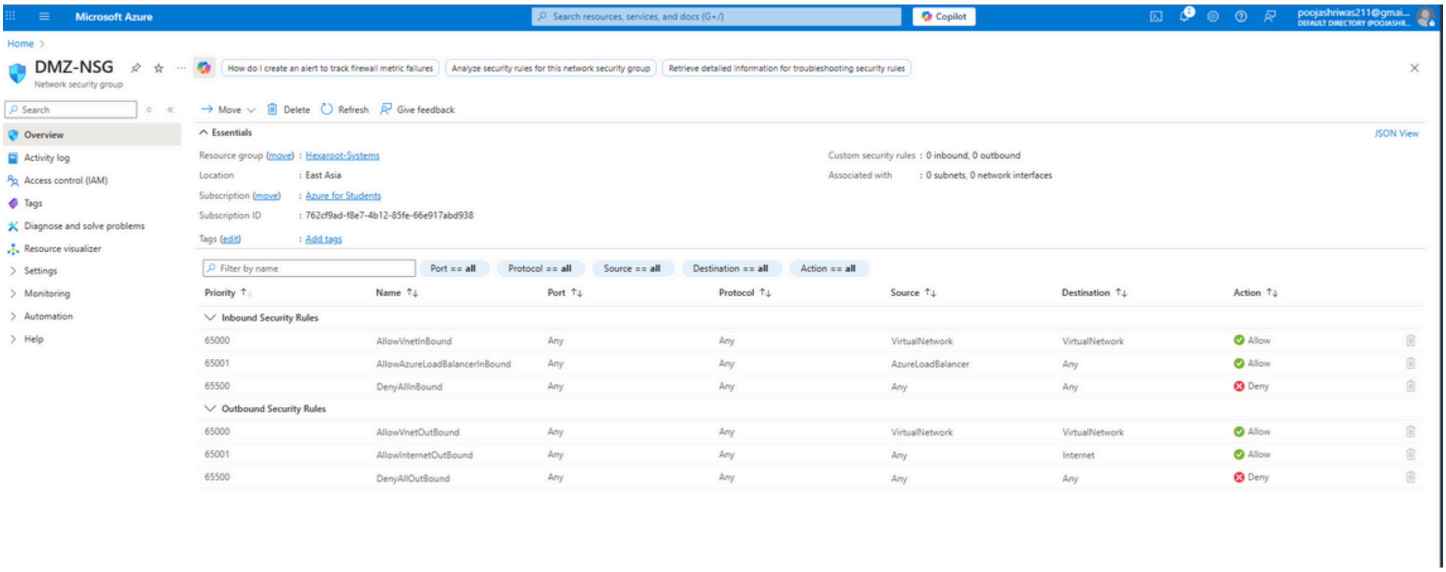


Internal-NSG
Network security group

Resource group (move) : Hexaroot-Systems
Location : East Asia
Subscription (move) : Azure for Students
Subscription ID : 762cf9ad-f8e7-4b12-85fe-66e917abd938
Tags (edit) : Add tags

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

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	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



DMZ-NSG
Network security group

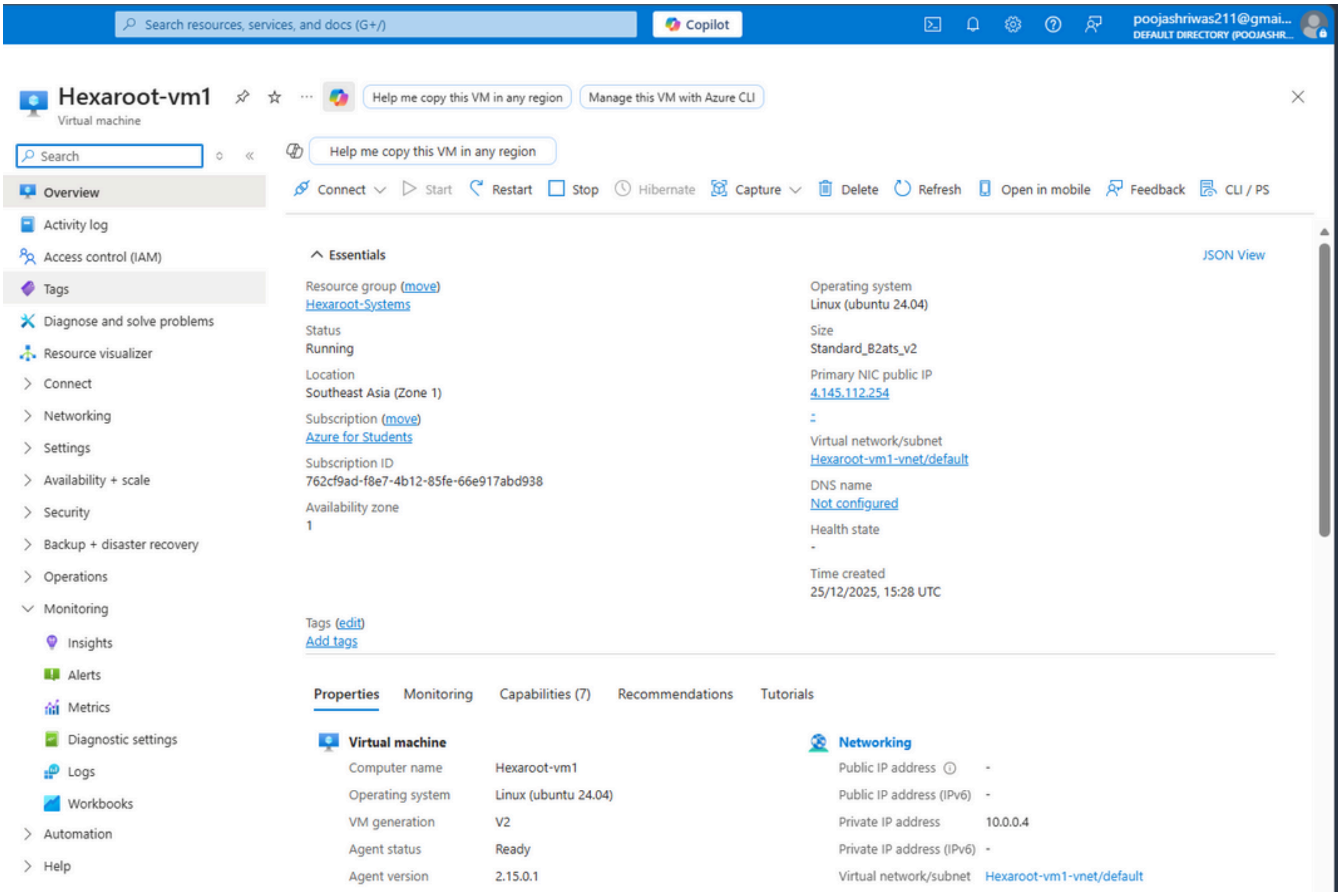
Resource group (move) : Hexaroot-Systems
Location : East Asia
Subscription (move) : Azure for Students
Subscription ID : 762cf9ad-f8e7-4b12-85fe-66e917abd938
Tags (edit) : Add tags

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

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	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

2.4 Virtual Machines Deployed

VM Name	Role	Subnet
VM1	Internal Server	Internal
VM2	Web Server	DMZ
VM3	SIEM / Log Server	Internal



Hexaroot-vm1

Virtual machine

Essentials

Resource group (move)
Hexaroot-Systems

Status
Running

Location
Southeast Asia (Zone 1)

Subscription (move)
Azure for Students

Subscription ID
762cf9ad-f8e7-4b12-85fe-66e917abd938

Availability zone
1

Operating system
Linux (ubuntu 24.04)

Size
Standard_B2ats_v2

Primary NIC public IP
4.145.112.254
-

Virtual network/subnet
Hexaroot-vm1-vnet/default

DNS name
Not configured

Health state
-

Time created
25/12/2025, 15:28 UTC

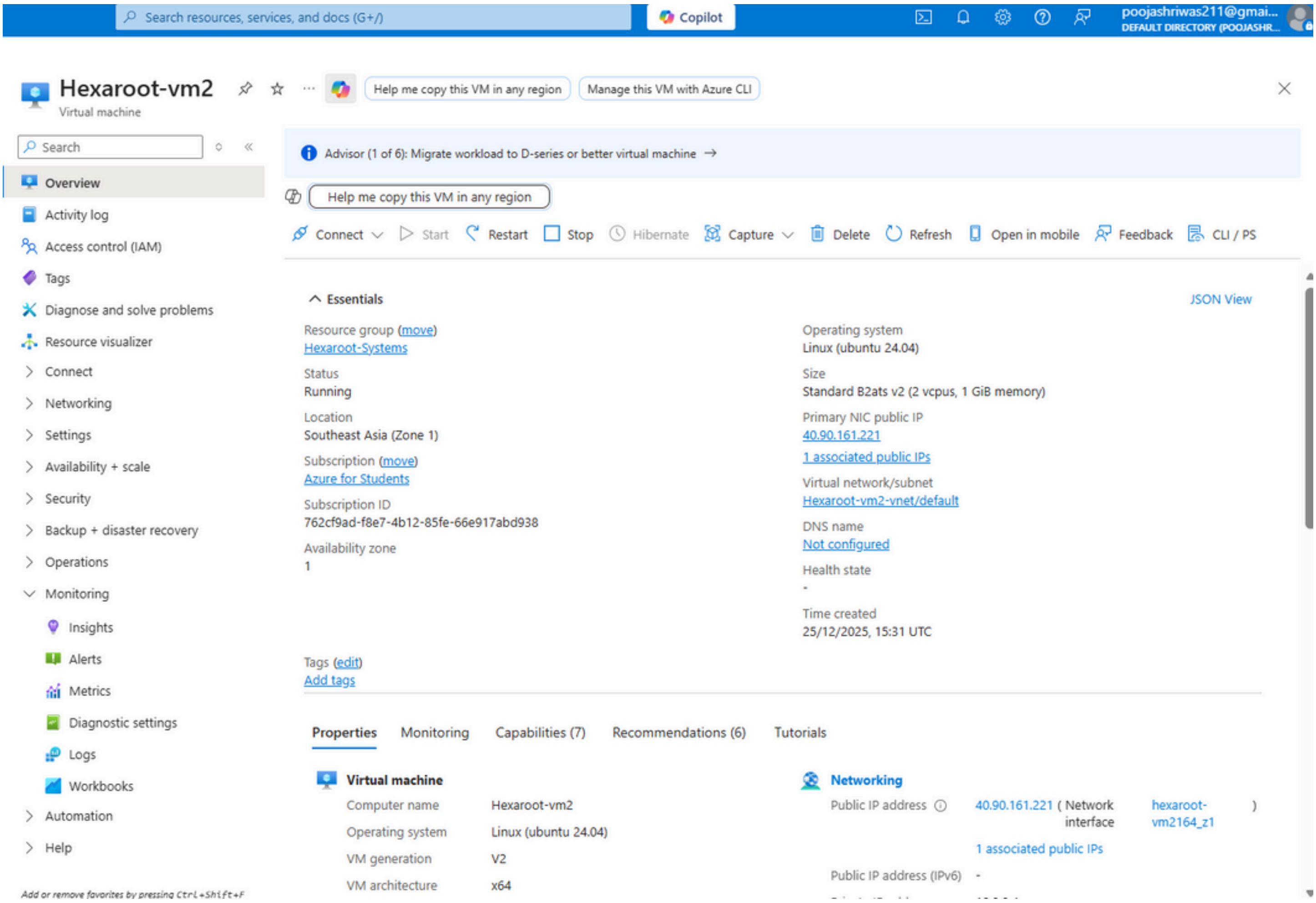
Tags (edit)
Add tags

Virtual machine

Computer name	Hexaroot-vm1
Operating system	Linux (ubuntu 24.04)
VM generation	V2
Agent status	Ready
Agent version	2.15.0.1

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	Hexaroot-vm1-vnet/default



Hexaroot-vm2

Virtual machine

Advisor (1 of 6): Migrate workload to D-series or better virtual machine →

Essentials

Resource group (move)
Hexaroot-Systems

Status
Running

Location
Southeast Asia (Zone 1)

Subscription (move)
Azure for Students

Subscription ID
762cf9ad-f8e7-4b12-85fe-66e917abd938

Availability zone
1

Operating system
Linux (ubuntu 24.04)

Size
Standard B2ats v2 (2 vcpus, 1 GiB memory)

Primary NIC public IP
40.90.161.221
1 associated public IPs

Virtual network/subnet
Hexaroot-vm2-vnet/default

DNS name
Not configured

Health state
-

Time created
25/12/2025, 15:31 UTC

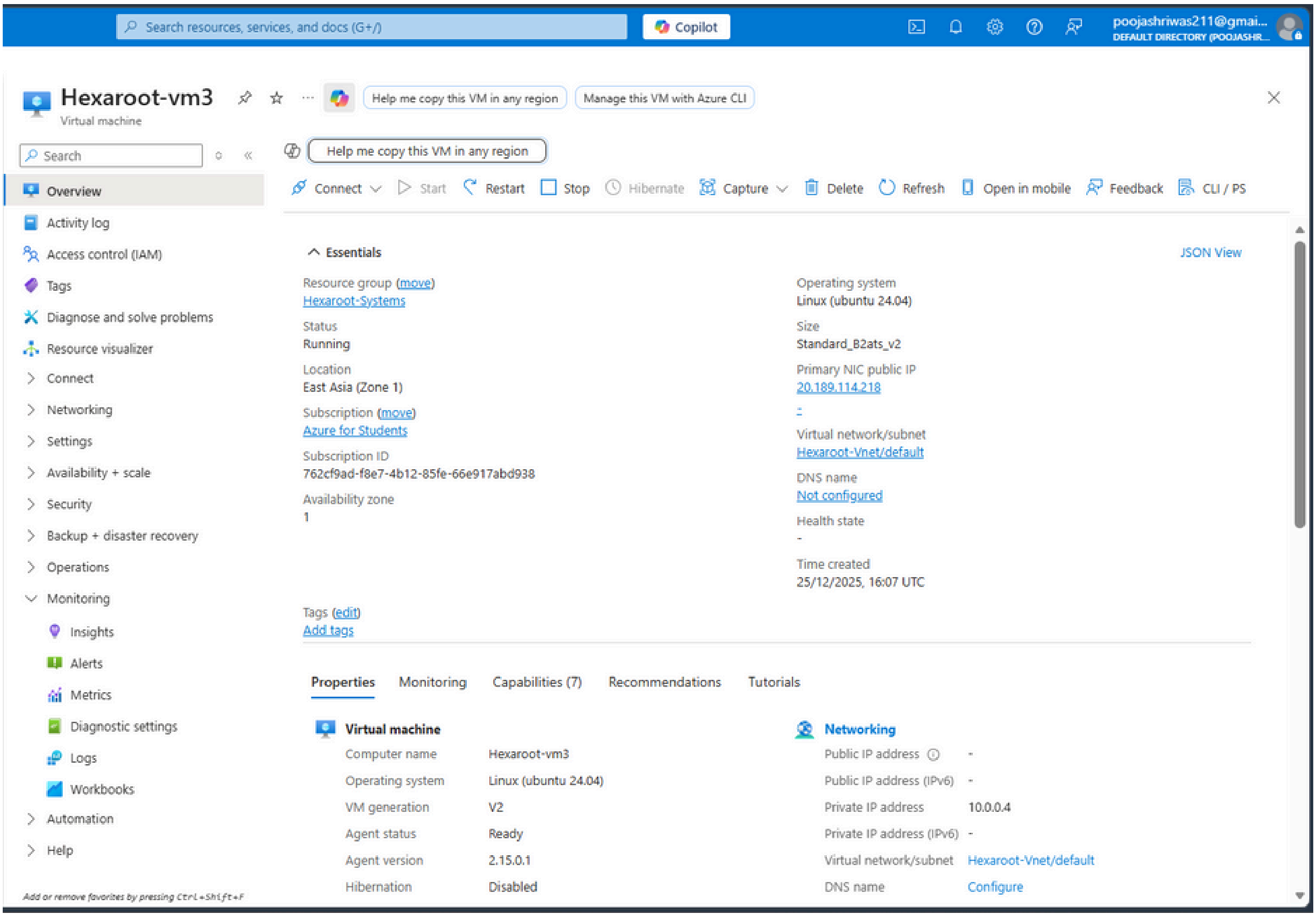
Tags (edit)
Add tags

Virtual machine

Computer name	Hexaroot-vm2
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64

Networking

Public IP address	40.90.161.221 (Network interface hexaroot-vm2164_z1) 1 associated public IPs
Public IP address (IPv6)	-



Hexaroot-vm3
Virtual machine

Essentials

Resource group (move)
Hexaroot-Systems

Status
Running

Location
East Asia (Zone 1)

Subscription (move)
Azure for Students

Subscription ID
762cf9ad-f8e7-4b12-85fe-66e917abd938

Availability zone
1

Operating system
Linux (ubuntu 24.04)

Size
Standard_B2ats_v2

Primary NIC public IP
20.189.114.218
-

Virtual network/subnet
Hexaroot-Vnet/default

DNS name
Not configured

Health state
-

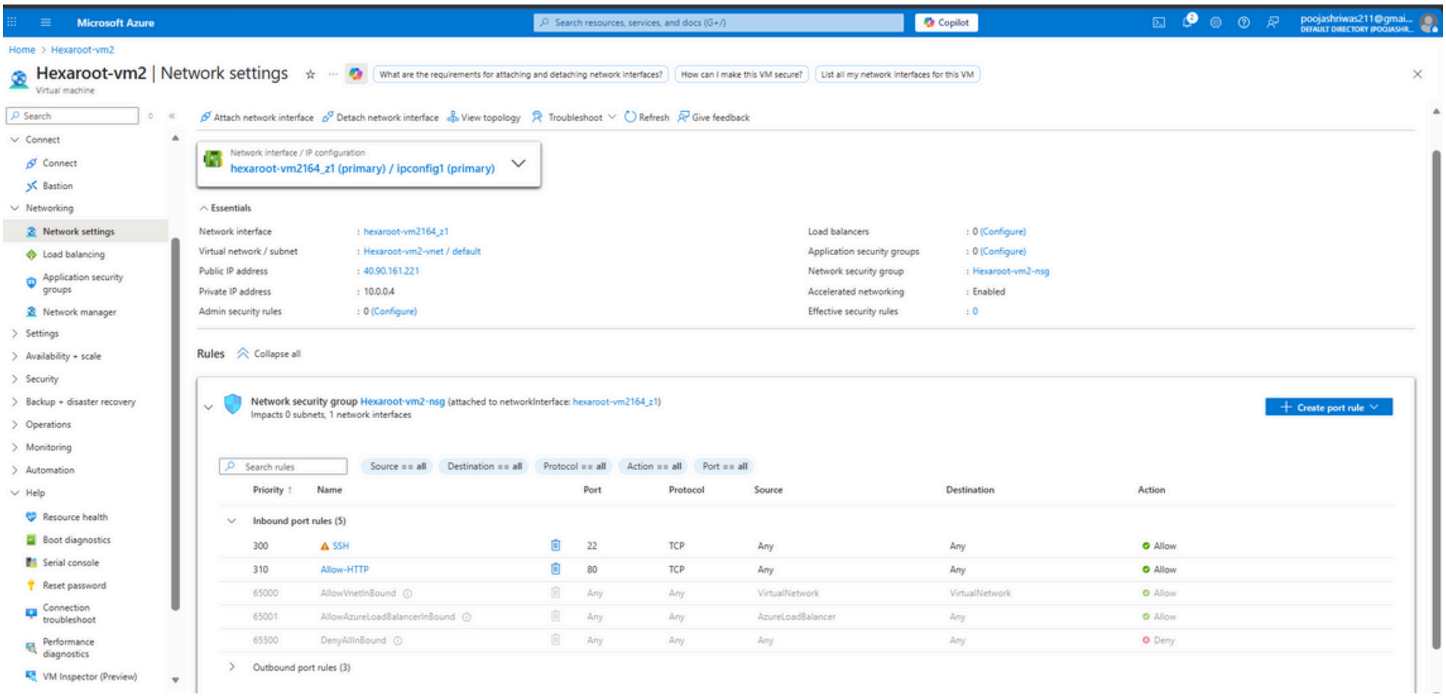
Time created
25/12/2025, 16:07 UTC

Tags (edit)
Add tags

Virtual machine		Networking	
Computer name	Hexaroot-vm3	Public IP address	-
Operating system	Linux (ubuntu 24.04)	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.0.0.4
Agent status	Ready	Private IP address (IPv6)	-
Agent version	2.15.0.1	Virtual network/subnet	Hexaroot-Vnet/default
Hibernation	Disabled	DNS name	Configure

2.5 Network Security Groups

- Basic NSG rules were applied
- SSH and HTTP allowed
- No security hardening applied



Hexaroot-vm2 | Network settings
Virtual machine

Network interface / IP configuration
hexaroot-vm2164_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface : hexaroot-vm2164_z1
Virtual network / subnet : Hexaroot-vm2-vnet / default
Public IP address : 40.90.161.221
Private IP address : 10.0.0.4
Admin security rules : 0 (Configure)
Load balancers : 0 (Configure)
Application security groups : 0 (Configure)
Network security group : Hexaroot-vm2-nsg
Accelerated networking : Enabled
Effective security rules : 0

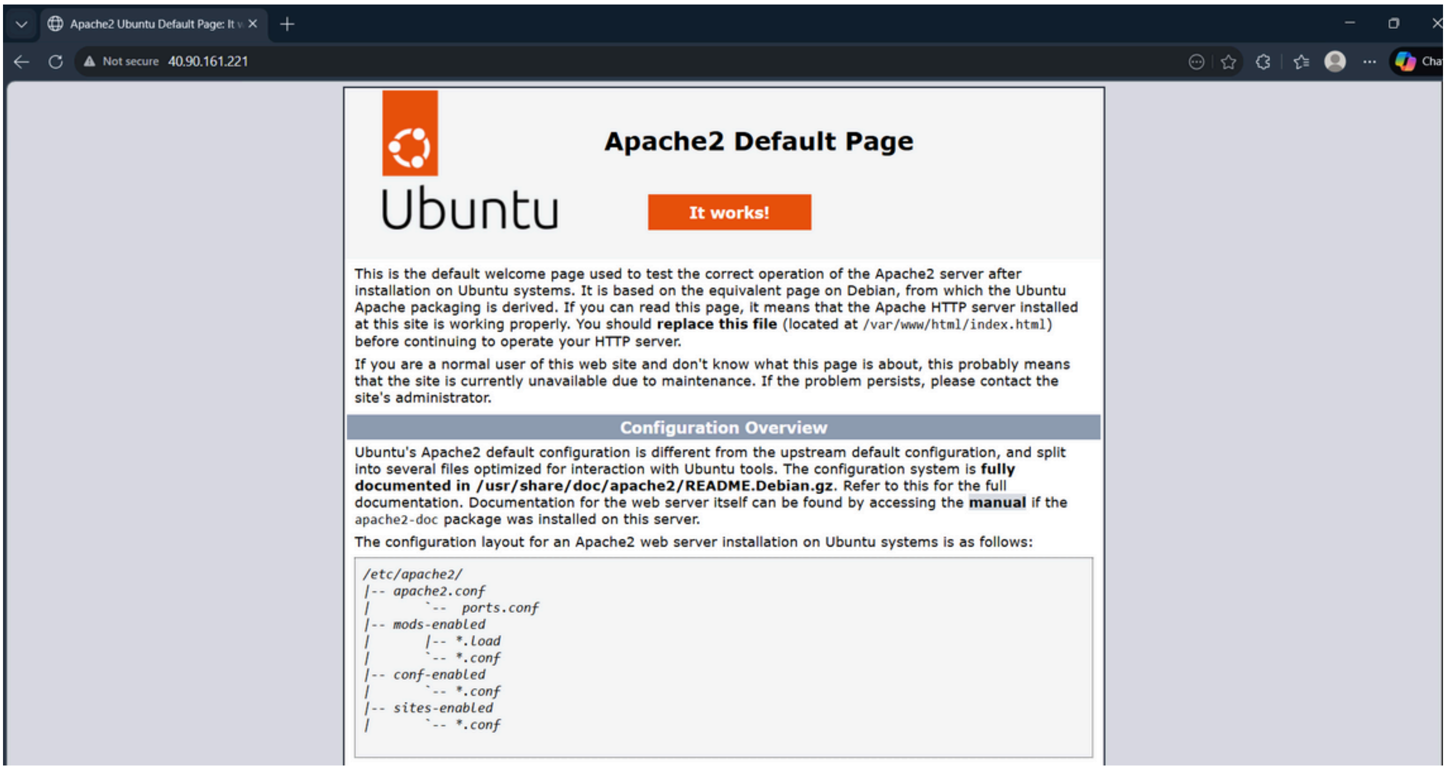
Rules

Network security group Hexaroot-vm2-nsg (attached to networkInterface: hexaroot-vm2164_z1)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
300	⚠ SSH	22	TCP	Any	Any	✓ Allow
310	Allow-HTTP	80	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
Outbound port rules (3)						

2.6 Web Server Deployment

- Apache web server installed on VM2
- Web page accessed using public IP



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

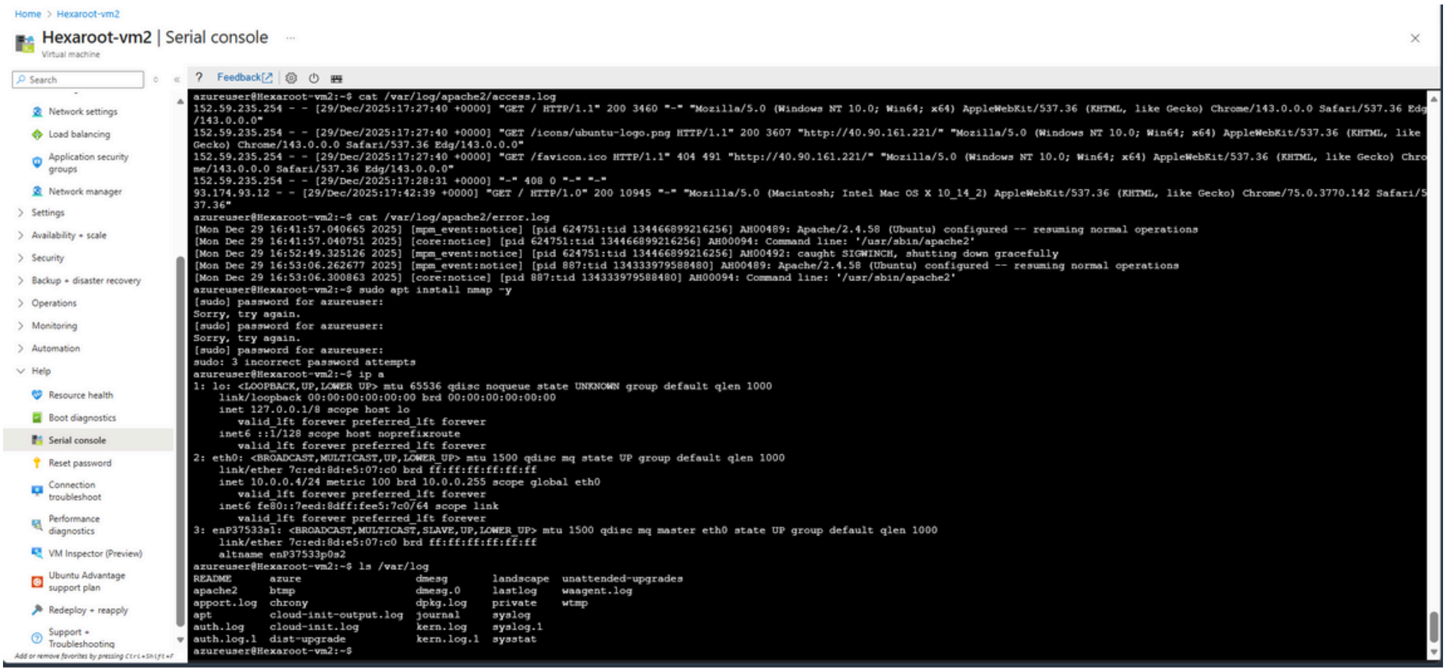
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `-- ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

2.7 Logging Enabled

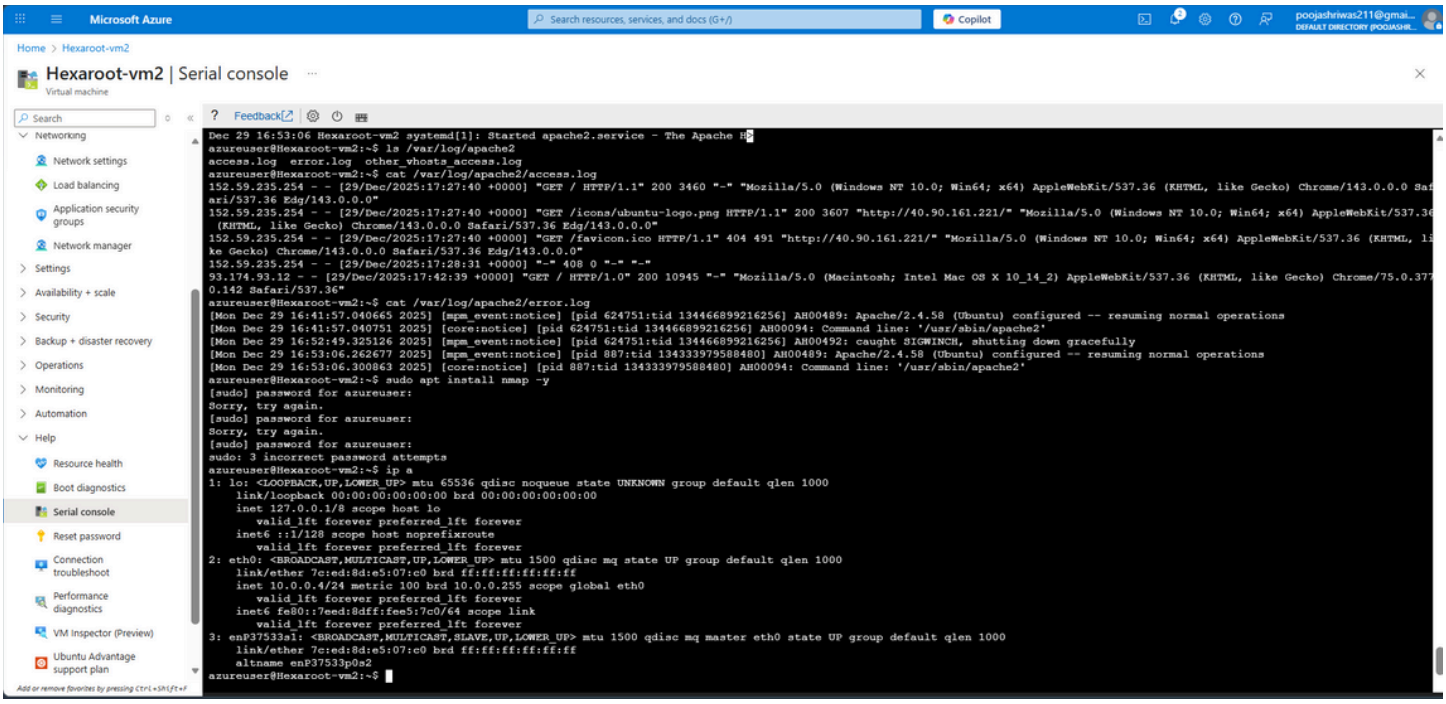
- System logs (syslog)
- Authentication logs
- Web server logs

/var/log directory



```
azureuser@Hexaroot-vm2:~$ cat /var/log/apache2/access.log
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg
/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://40.90.161.221/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "http://40.90.161.221/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
me/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:28:31 +0000] "-" 408 0 "-" "-"
93.174.93.12 - - [29/Dec/2025:17:42:39 +0000] "GET / HTTP/1.0" 200 10945 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/5
37.36"
azureuser@Hexaroot-vm2:~$ cat /var/log/apache2/error.log
[Mon Dec 29 16:41:57.040665 2025] [mpm_event:notice] [pid 624751:tid 134466899216256] AH00489: Apache/2.4.58 (Ubuntu) configured -- resuming normal operations
[Mon Dec 29 16:41:57.040751 2025] [core:notice] [pid 624751:tid 134466899216256] AH00094: Command line: '/usr/sbin/apache2'
[Mon Dec 29 16:52:49.325126 2025] [mpm_event:notice] [pid 624751:tid 134466899216256] AH00492: caught SIGWINCH, shutting down gracefully
[Mon Dec 29 16:53:06.262677 2025] [mpm_event:notice] [pid 887:tid 134333979588480] AH00489: Apache/2.4.58 (Ubuntu) configured -- resuming normal operations
[Mon Dec 29 16:53:06.300863 2025] [core:notice] [pid 887:tid 134333979588480] AH00094: Command line: '/usr/sbin/apache2'
azureuser@Hexaroot-vm2:~$ sudo apt install nmap -y
[sudo] password for azureuser:
Sorry, try again.
[sudo] password for azureuser:
Sorry, try again.
[sudo] password for azureuser:
sudo: 3 incorrect password attempts
azureuser@Hexaroot-vm2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 7c:ed:8d:e5:07:c0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.4/24 metric 100 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::7eed:8dff:fee5:7c0/64 scope link
       valid_lft forever preferred_lft forever
3: enP37533s1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc mq master eth0 state UP group default qlen 1000
    link/ether 7c:ed:8d:e5:07:c0 brd ff:ff:ff:ff:ff:ff
    altname enP37533p0s2
azureuser@Hexaroot-vm2:~$ ls /var/log
README      azure                  dmesg       landscape  unattended-upgrades
apache2     btmp                   dmesg.0     lastlog    waagent.log
apport.log  chrony                 dpkg.log    private    wtmp
apt         cloud-init-output.log  journal     syslog
auth.log    cloud-init.log         kern.log    syslog.1
auth.log.1  dist-upgrade           kern.log.1  sysstat
azureuser@Hexaroot-vm2:~$
```

👉 /var/log/apache2 directory



```
Dec 29 16:53:06 Hexaroot-vm2 systemd[1]: Started apache2.service - The Apache H>
azureuser@Hexaroot-vm2:~$ ls /var/log/apache2
access.log  error.log  other_vhosts_access.log
azureuser@Hexaroot-vm2:~$ cat /var/log/apache2/access.log
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Saf
ari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://40.90.161.221/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "http://40.90.161.221/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
ke Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:28:31 +0000] "-" 408 0 "-" "-"
93.174.93.12 - - [29/Dec/2025:17:42:39 +0000] "GET / HTTP/1.0" 200 10945 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
0.142 Safari/537.36"
azureuser@Hexaroot-vm2:~$ cat /var/log/apache2/error.log
[Mon Dec 29 16:41:57.040665 2025] [mpm_event:notice] [pid 624751:tid 134466899216256] AH00489: Apache/2.4.58 (Ubuntu) configured -- resuming normal operations
[Mon Dec 29 16:41:57.040751 2025] [core:notice] [pid 624751:tid 134466899216256] AH00094: Command line: '/usr/sbin/apache2'
[Mon Dec 29 16:52:49.325126 2025] [mpm_event:notice] [pid 624751:tid 134466899216256] AH00492: caught SIGWINCH, shutting down gracefully
[Mon Dec 29 16:53:06.262677 2025] [mpm_event:notice] [pid 887:tid 134333979588480] AH00489: Apache/2.4.58 (Ubuntu) configured -- resuming normal operations
[Mon Dec 29 16:53:06.300863 2025] [core:notice] [pid 887:tid 134333979588480] AH00094: Command line: '/usr/sbin/apache2'
azureuser@Hexaroot-vm2:~$ sudo apt install nmap -y
[sudo] password for azureuser:
Sorry, try again.
[sudo] password for azureuser:
Sorry, try again.
[sudo] password for azureuser:
sudo: 3 incorrect password attempts
azureuser@Hexaroot-vm2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 7c:ed:8d:e5:07:c0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.4/24 metric 100 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::7eed:8dff:fee5:7c0/64 scope link
       valid_lft forever preferred_lft forever
3: enP37533s1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc mq master eth0 state UP group default qlen 1000
    link/ether 7c:ed:8d:e5:07:c0 brd ff:ff:ff:ff:ff:ff
    altname enP37533p0s2
azureuser@Hexaroot-vm2:~$
```

3. MAJOR PROJECT – SECURITY & SOC OVERVIEW

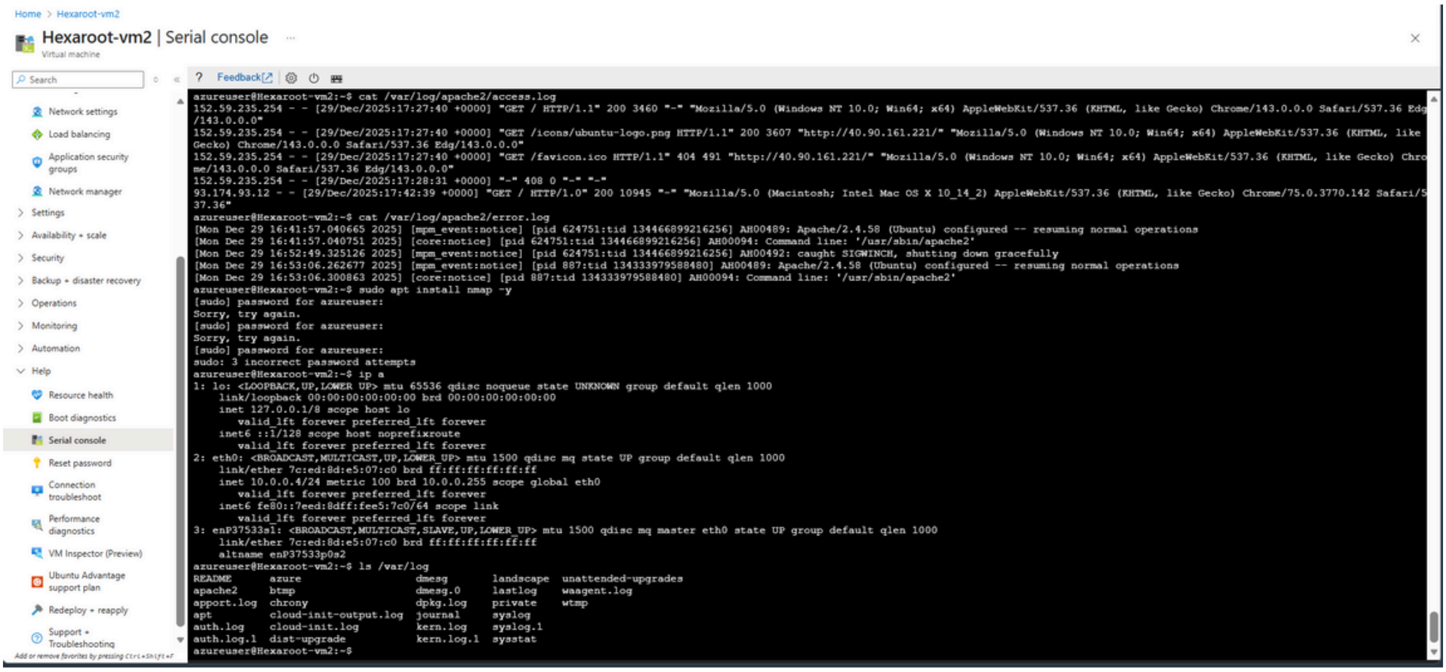
3.1 Objective

To use the deployed infrastructure for security monitoring, log analysis, and attack simulation.

3.2 Log Collection

- Logs generated by Linux servers
- Logs prepared for centralized monitoring
- SIEM (VM3) used for log analysis

Log files / monitoring screen



```
azureuser@Hexaroot-vm2:~$ cat /var/log/apache2/access.log
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg
/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://40.90.161.221/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:27:40 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "http://40.90.161.221/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
me/143.0.0.0 Safari/537.36 Edg/143.0.0.0"
152.59.235.254 - - [29/Dec/2025:17:28:31 +0000] "-" 408 0 "-" "-"
93.174.93.12 - - [29/Dec/2025:17:42:39 +0000] "GET / HTTP/1.0" 200 10945 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/5
37.36"
azureuser@Hexaroot-vm2:~$ cat /var/log/apache2/error.log
[Mon Dec 29 16:41:57.040665 2025] [mpm_event:notice] [pid 624751:tid 134466899216256] AH00489: Apache/2.4.58 (Ubuntu) configured -- resuming normal operations
[Mon Dec 29 16:41:57.040751 2025] [core:notice] [pid 624751:tid 134466899216256] AH00094: Command line: '/usr/sbin/apache2'
[Mon Dec 29 16:52:49.325126 2025] [mpm_event:notice] [pid 624751:tid 134466899216256] AH00492: caught SIGWINCH, shutting down gracefully
[Mon Dec 29 16:53:06.262677 2025] [mpm_event:notice] [pid 887:tid 134333979588480] AH00489: Apache/2.4.58 (Ubuntu) configured -- resuming normal operations
[Mon Dec 29 16:53:06.300863 2025] [core:notice] [pid 887:tid 134333979588480] AH00094: Command line: '/usr/sbin/apache2'
azureuser@Hexaroot-vm2:~$ sudo apt install nmap -y
[sudo] password for azureuser:
Sorry, try again.
[sudo] password for azureuser:
Sorry, try again.
[sudo] password for azureuser:
sudo: 3 incorrect password attempts
azureuser@Hexaroot-vm2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 7c:ed:8d:e5:07:c0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.4/24 metric 100 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::7eed:8dff:fee5:7c0/64 scope link
       valid_lft forever preferred_lft forever
3: enP37533s1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc mq master eth0 state UP group default qlen 1000
    link/ether 7c:ed:8d:e5:07:c0 brd ff:ff:ff:ff:ff:ff
    altname enP37533p0s2
azureuser@Hexaroot-vm2:~$ ls /var/log
README      azure                   dmesg       landscape  unattended-upgrades
apache2     btmp                    dmesg.0     lastlog    waagent.log
apport.log  chrony                  dpkg.log    private    wtmp
apt         cloud-init-output.log   journal     syslog
auth.log    cloud-init.log          kern.log    syslog.1
auth.log.1  dist-upgrade            kern.log.1  sysstat
azureuser@Hexaroot-vm2:~$
```

3.3 Attack Simulation (Overview)

The following activities will be performed:

- Failed login attempts
- Web access pattern analysis
- Authentication log review

(No real attacks were executed in minor phase.)

3.4 SOC Monitoring Concept

- Logs are analyzed to detect suspicious activity
- Alerts help identify security threats
- This simulates a real Security Operations Center (SOC)

4. CONCLUSION

This project demonstrates how cloud infrastructure is deployed, monitored, and prepared for security analysis.
The minor project focuses on infrastructure and logging, while the major project focuses on SOC readiness and attack analysis.