

Beth Israel Lahey Health (CareGroup)

Network Administration



Team 8 - Network Admin.

TEAM MEMBERS

Daniel Thach
Christian Najera
Angel Contreras

CIS 4900, Dr. Howell

Meet the team

Christian Najera - Team Lead

Angel Contreras – Project Coordinator

Daniel Thach – Technical Coordinator

Team Lead:

- Guides delegation of meetings
- Ensures deliverables are produced
- Responsible for final submission

Project Coordinator:

- Leads project timeframes
- Guides delegation of deliverables

Technical Coordinator:

- Leads feedback review
 - Ensures consistency of reports
 - Guides technical review
-

CareGroup/BILH

- 100+ year old medical network
- State-of-the art inpatient/outpatient facilities
- Manages over 39,000 employees
- Committed to excellence in healthcare
- Notorious for IT collapse of 2002



Virtualization - A comprehensive solution

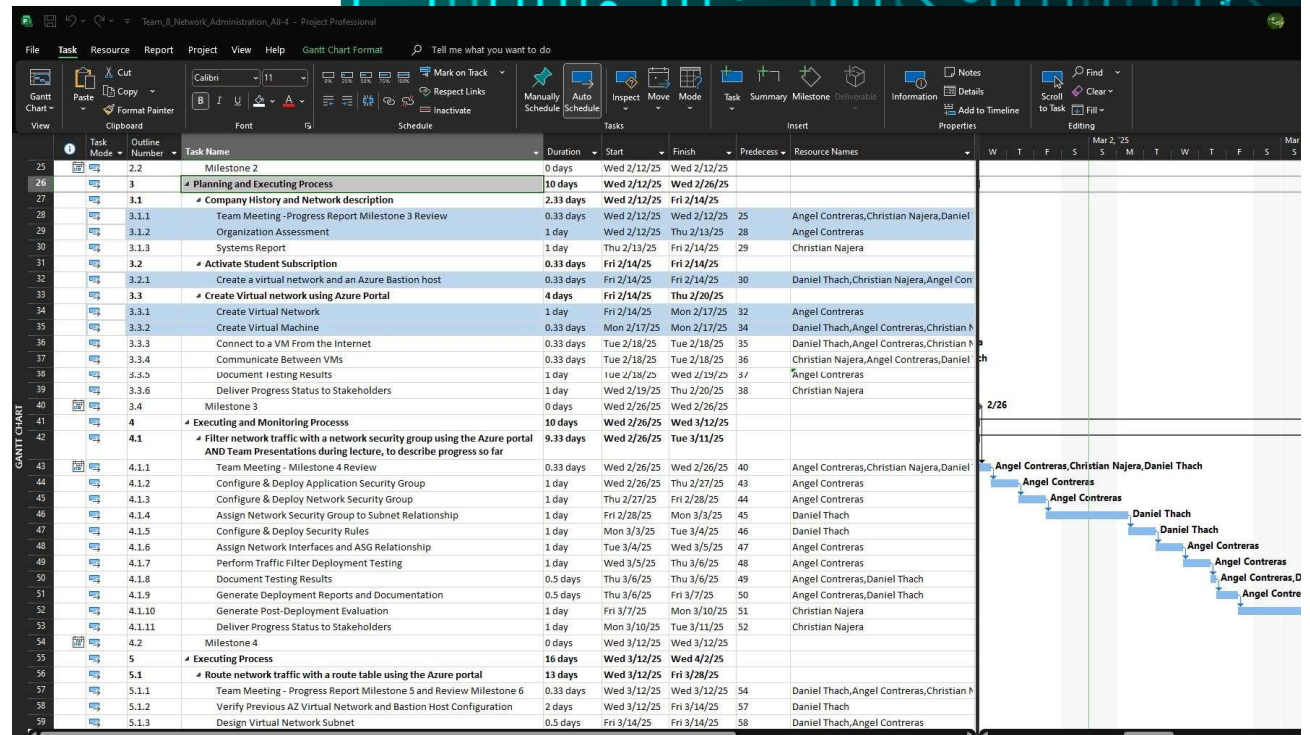
- An inarguable need
- Tailored to accessibility
- Tailored to scalability
- Virtualization on Microsoft Azure Platform



Milestone 3

Planning and Executing Process

- Project Scope
- Roles & Responsibilities
- Virtual Network for Beth Isreal Lahey Health

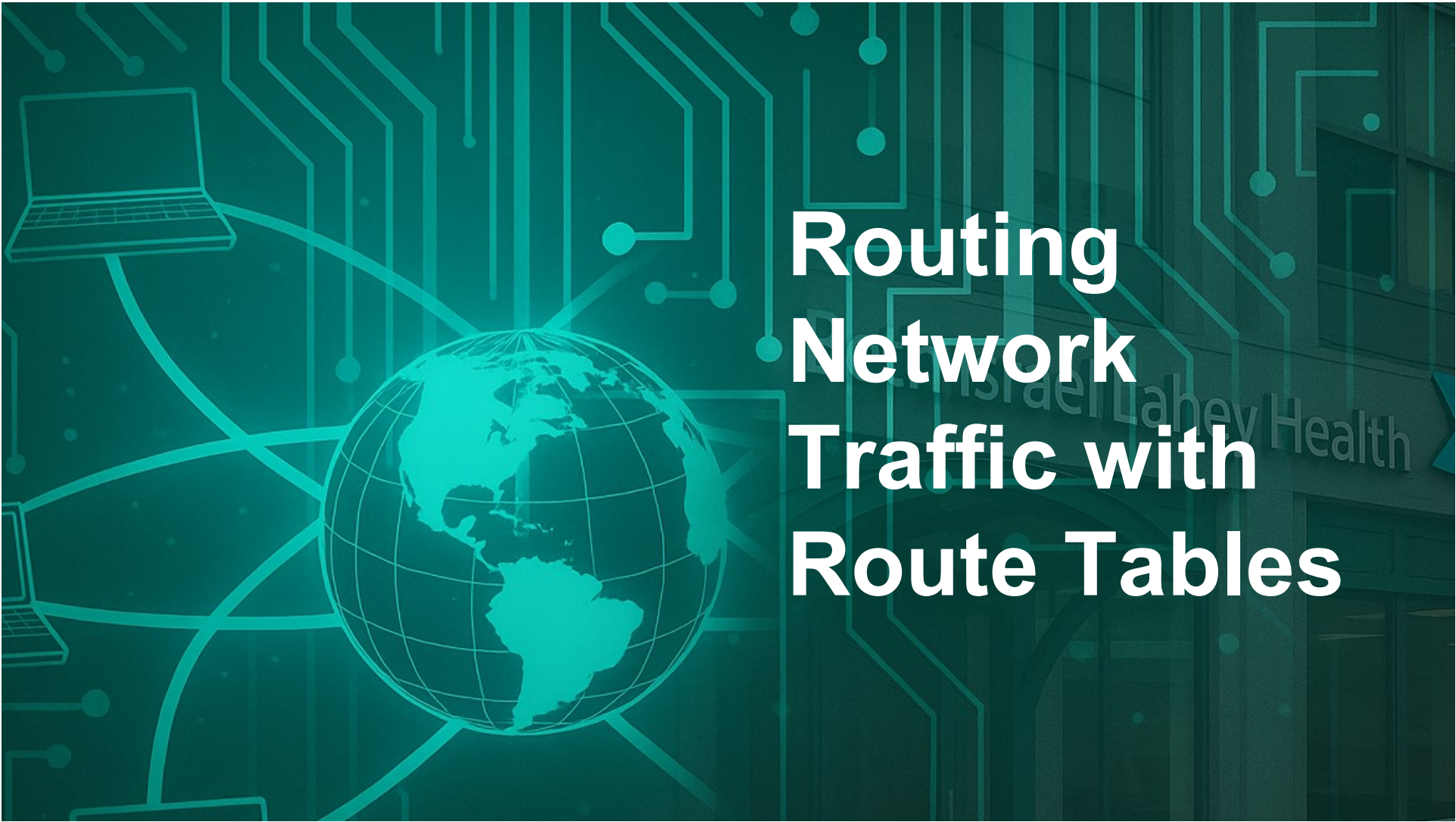


Milestone 4

Executing and Monitoring Process

- PowerPoint Outline
- Networking Lab Guides
- Tested Traffic Filters





Routing Network Traffic with Route Tables

Routing Network Traffic with Route Tables

- Creating a NVA
- Creating a Route Table
- Creating a route
- Configuring IP forwarding
- Protocol Mapping



Creating a Network Virtual Appliance

The screenshot displays the Microsoft Azure portal interface. At the top, the header shows 'Microsoft Azure' and a search bar. Below the header, the breadcrumb trail indicates the path: 'Home > CreateVM > ubuntu-server-jammy-2-20250403204938 | Overview >'. The main content area is titled 'CGNetVM-NVA3' with a red box highlighting the VM name and its icon. Below the title, it says 'Virtual machine'. A search bar and a button 'Help me copy this VM in any region' are present. The left sidebar contains a list of navigation options: Overview (selected), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, and a section for 'Connect' and 'Action'. The main content area is divided into two sections. The 'Essentials' section lists key VM details: Resource group (move) : CGNetVM, Status : Running, Location : East US 2, Subscription (move) : Azure for Students, and Subscription ID : eb7c73d0-b299-4137-81d8-b00a83c4e9d7. The 'Properties' section on the right lists various attributes: Operating system, Size, Public IP address, Virtual network/s, DNS name, and Health state. A red box highlights the 'Operating system' field in the Properties section.

Microsoft Azure

Search resources, services, and docs (G+)

Home > CreateVM > ubuntu-server-jammy-2-20250403204938 | Overview >

CGNetVM-NVA3 ☆ ...

Virtual machine

Search

Help me copy this VM in any region

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Connect

Action

Essentials

Resource group (move) : [CGNetVM](#)

Status : Running

Location : East US 2

Subscription (move) : [Azure for Students](#)

Subscription ID : eb7c73d0-b299-4137-81d8-b00a83c4e9d7

Operating system

Size

Public IP address

Virtual network/s

DNS name

Health state

Creating a Route Table

Create Route table ...

Basics

Tags

Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure for Students

Resource group *

CGnetVM

Create new

Instance details

Region *

East US 2

Name *

route-table-public

Propagate gateway routes *

☒ Yes

☐ No

Adding a route

Add route

route-table-public

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more](#)

Route name *

to-private-subnet

✓

Destination type * ⓘ

IP Addresses

✓

Destination IP addresses/CIDR ranges * ⓘ

10.0.2.0/24

✓

Next hop type * ⓘ

Virtual appliance

✓

Next hop address * ⓘ

10.0.3.4

✓



Configure IP Forwarding

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar shows 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb trail reads: 'Home > Compute infrastructure | Virtual machines > vm-nva | Network settings > vm-nva167'. The main heading is 'CGNetVM-NVA3 | IP configurations', with 'Network interface' as a subtitle. A search bar and a 'Refresh' button are located below the heading. On the left sidebar, the 'Settings' section is expanded, and 'IP configurations' is selected. The 'IP Settings' tab is highlighted with a red rectangle. The settings include: 'Enable IP forwarding' (checked), 'Virtual network' (vnet3), and 'Subnet' (subnet-dmz (10.0.3.0/24) 250 free IP addresses). A note at the bottom states: 'Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. [Learn more](#)'. At the bottom, there are buttons for '+ Add', 'Make primary', and 'Delete'.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Compute infrastructure | Virtual machines > vm-nva | Network settings > vm-nva167

CGNetVM-NVA3 | IP configurations

Network interface

Search Refresh

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Settings

IP configurations

DNS servers

Network security group

Properties

IP Settings

Enable IP forwarding ☒

Virtual network vnet3

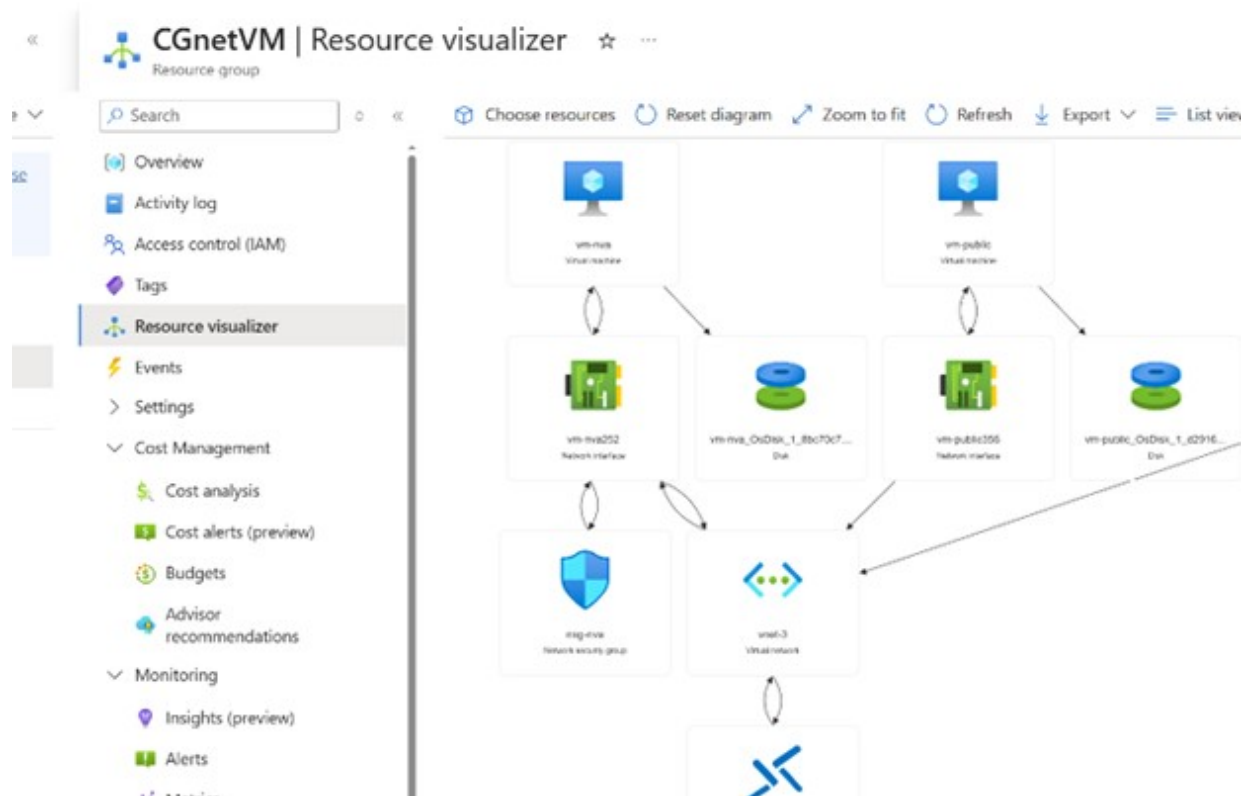
Subnet * subnet-dmz (10.0.3.0/24) 250 free IP addresses

250 free IP addresses

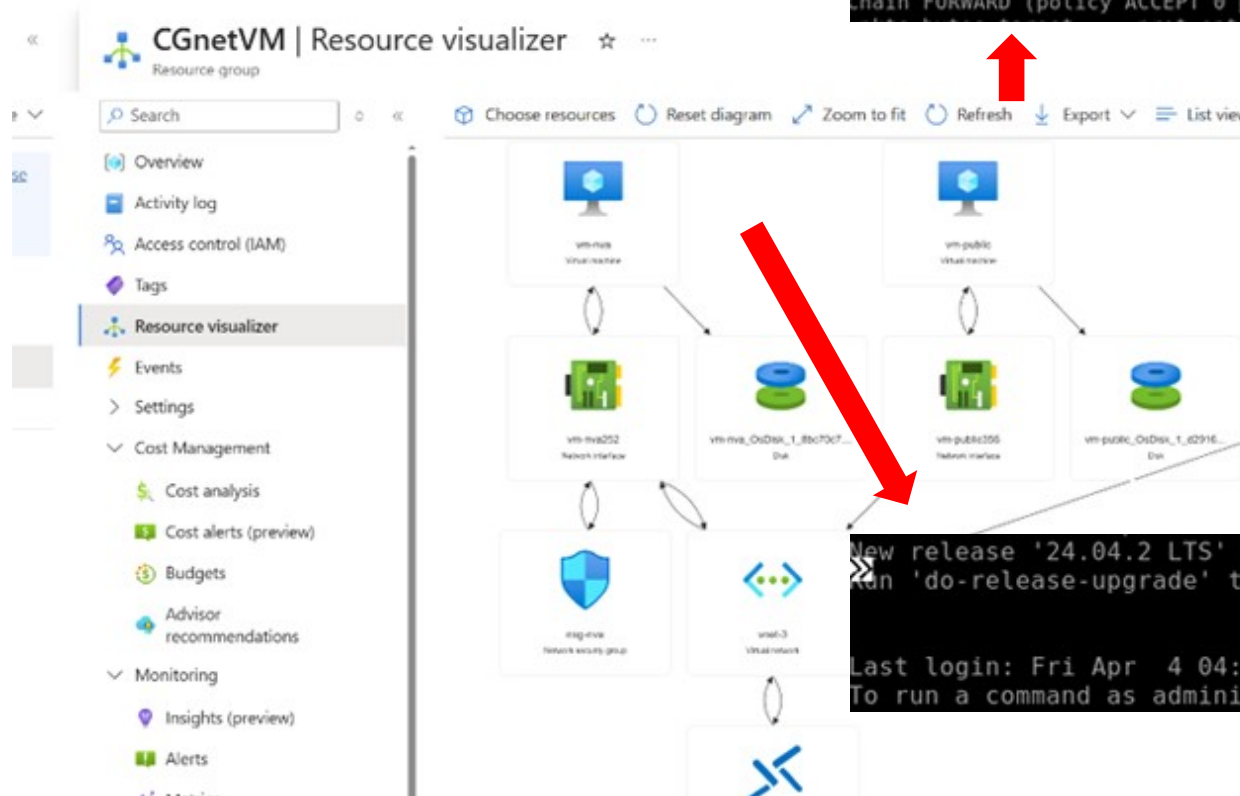
Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. [Learn more](#)

+ Add Make primary Delete

Protocol Mapping



Protocol Mapping



MyCalStateLA - Ho... Dashboard AWS course ISACA LinkedIn Readings - Google... Capstone - F

```
root@vm-nva:~# iptables -L -v -n
Chain INPUT (policy ACCEPT 126 packets, 24232 bytes)
  pkts bytes target     prot opt in     out     source            destination
    0    0 ACCEPT     1    --  *      *           0.0.0.0/0         0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

```
New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Apr  4 04:59:07 2025 from 10.0.1.4
To run a command as administrator (user "root"), use "sudo <command>"
```




Connecting Virtual Networks and Peering

Connecting Virtual Networks

- Connecting Virtual Networks via Peering
- Testing the Peering connection



Connecting Virtual Networks and Peering

Search resources, services, and docs (G+)

CGVNet-1 | Peerings

Virtual network

Search

+ Add Refresh Export to CSV Delete Sync

Virtual network peering enables you to seamlessly connect two or more v

Filter by name...

Showing all 1 items

<input type="checkbox"/>	Name	Peering
<input type="checkbox"/>	vnet-1-to-vnet-3	Full

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Address space
- Connected devices
- Subnets
- Bastion
- DDoS protection
- Firewall

Search resources, services, and docs (G+)

CGVNet-3 | Peerings

Virtual network

Search

+ Add Refresh Export to CSV Delete Sync

Virtual network peering enables you to seamlessly connect two or more virtual netw

Filter by name...

Showing all 1 items

<input type="checkbox"/>	Name	Peering sync statu
<input type="checkbox"/>	vnet-3-to-vnet-1	Fully Synchroni

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Address space
- Connected devices
- Subnets
- Bastion
- DDoS protection
- Firewall

Testing the Peering connection

```
Chain ufw-user-input (1 references)
target      prot opt source      destination

Chain ufw-user-limit (0 references)
target      prot opt source      destination
LOG         all  -- anywhere          anywhere          limit: avg 3/min burst 5 LOG 1U
FW LIMIT BLOCK] "
REJECT      all  -- anywhere          anywhere          reject-with icmp-port-unreachae

Chain ufw-user-limit-accept (0 references)
target      prot opt source      destination
ACCEPT      all  -- anywhere          anywhere

Chain ufw-user-logging-forward (0 references)
target      prot opt source      destination

Chain ufw-user-logging-input (0 references)
target      prot opt source      destination

Chain ufw-user-logging-output (0 references)
target      prot opt source      destination

Chain ufw-user-output (1 references)
target      prot opt source      destination
dthach2@vm-5:~$ sudo ufw status
Status: active
dthach2@vm-5:~$
```

```
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

dthach2@vm-5:~$ ping -c 4 10.1.0.4
PING 10.1.0.4 (10.1.0.4) 56(84) bytes of data.
--- 10.1.0.4 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3057ms

dthach2@vm-5:~$ ping -c 10.0.0.4
ping: invalid argument: '10.0.0.4'
dthach2@vm-5:~$ ping -c 4 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=1.70 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.913 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=0.723 ms
--- 10.0.0.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.723/1.107/1.702/0.367 ms
dthach2@vm-5:~$
```




Takeaways and Considerations

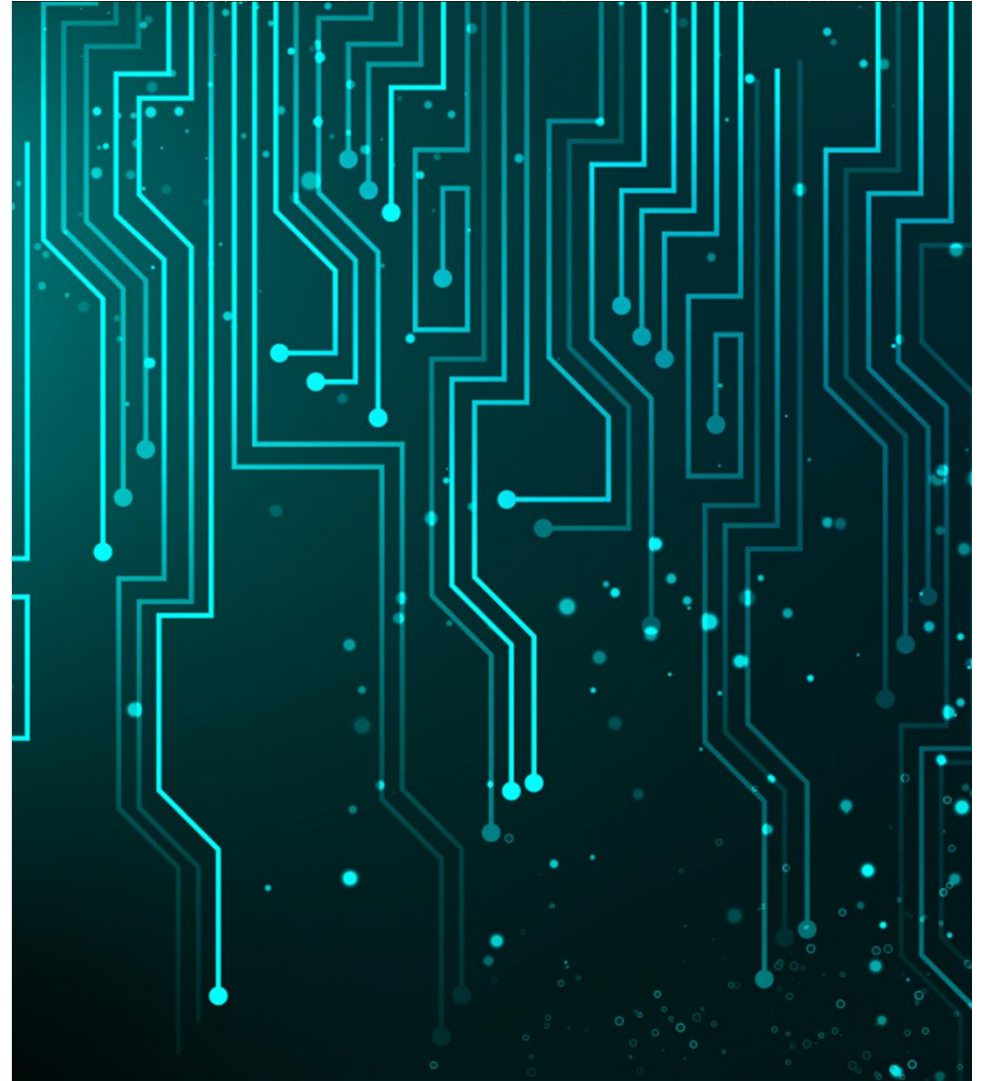
Summary

- Designed to support BILH's mission of secure, scalable, and collaborative healthcare.
 - Built a virtual network with public and private VMs for flexibility and security.
 - Implemented NSGs and ASGs to manage traffic and protect resources.
 - Used route tables and NVAs to control traffic flow securely.
 - Tested connectivity and routing to validate configurations.
-

Considerations

- Balance between accessibility and security in VM deployment.
 - Complex configuration of NSGs, ASGs, and routing requires accuracy.
 - Compliance with healthcare regulations requires ongoing updates.
 - Early planning is essential for future scalability and integration.
-

QUESTIONS?



REFERENCES

- asudbring. (2023, May 4). *Network security group – How it works*. Microsoft. <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>
- asudbring. (2024, August 20). *Tutorial: Filter network traffic with a network security group (NSG)*. Microsoft. <https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic?tabs=portal>
- GeeksforGeeks. (2022, July 22). *Fundamentals of virtual networking*. <https://www.geeksforgeeks.org/fundamentals-of-virtual-networking/>
- Khan, A. (2023, March 6). *How network security groups filter network traffic*. LinkedIn. <https://www.linkedin.com/pulse/how-network-security-groups-filter-traffic-ali-khan-/>
- KumudD. (n.d.). *Route network traffic – Tutorial – Azure Portal*. Microsoft. <https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal>
- Massachusetts Health Policy Commission. (2018). *Final CMIR report – Beth Israel Lahey Health – Executive summary*. <https://www.mass.gov>
- McFarlan, F. W., & Austin, R. D. (2005). *CareGroup* (Case No. 9-303-097). Harvard Business School.
- Microsoft. (2024a). *What is Azure Virtual Network?* <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
- Microsoft. (2025a). *What is a virtual machine and how does it work | Microsoft Azure*. <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine/?msockid=1b50d6747d616ea30770c3467cf36f18>
- Samanro. (n.d.). *Microsoft cloud architecture models – Enterprise resource planning*. Microsoft. <https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models?view=o365-worldwide>
- Susnjara, S., & Smalley, I. (2024, March 3). *What is a virtual machine (VM)?* IBM. <https://www.ibm.com/think/topics/virtual-machines>