

**CANTON WEKE OTIENO**

**SECURITY ENGINEER TRACK**

**STUDENT TRACKING NUMBER; ADC-SE01-24010**

**CYBER SHUJAA**

**INSTRUCTOR: DR. PAULA**

**CAROLINE TIPAPE**

**LAB 05 - IMPLEMENT INTERSITE CONNECTIVITY**

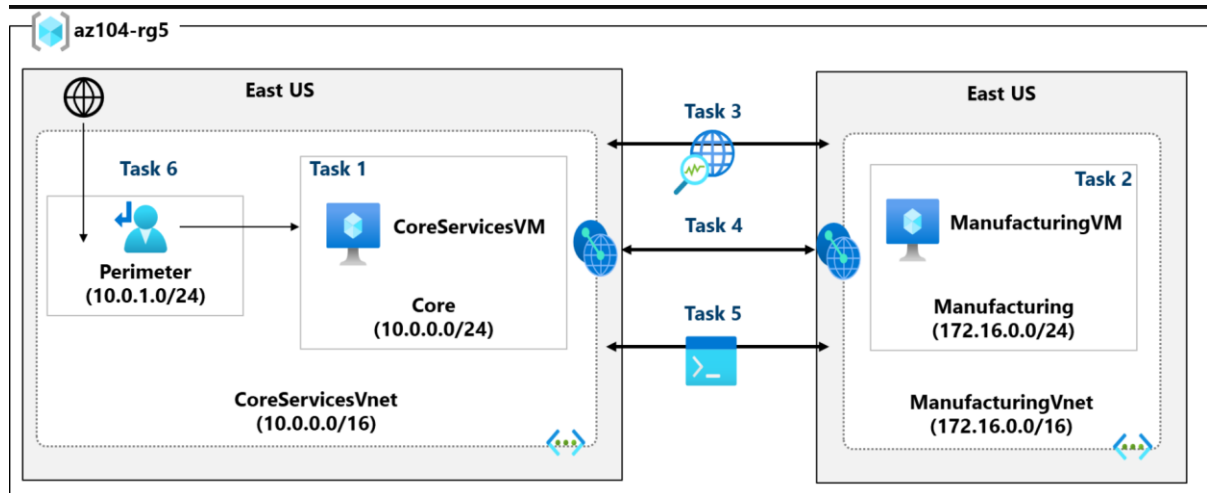
## INTRODUCTION

Inter-site connectivity means establishing connectivity between two sites. It's not necessarily that one is on-premises and the other is on the cloud. One can also establish private connectivity between two Azure regions as well. Each region can be considered as a site and establish connectivity between them.

This report explores the communication between virtual networks demonstrated in different six tasks explained in the report. By configuration and implementation of virtual network peering and testing connections through different labs and also involve creating custom routes.

This lab report is divided into six sections with the instruction on how to do the setup and full configuration that can help engineers to the full configuration. Task one involves Creating a virtual machine in a virtual network, task involves the process of creating and managing multiple VNets. Task three introduces the network watcher a vital diagnostic tool that tests the connection between different virtual networks. Fourth task then delves into configuring VNet peering allowing seamless communication between virtual networks. Task five involves Using Azure PowerShell to test the connection between virtual machines this allows one to demonstrate how to use command-line tools in managing and monitoring network resources. Finally, the report shows how to create custom routes to refine and control the traffic flow. The routing rules demonstrate how the rules created can be improved to optimize network performance and security.

## Architecture diagram



### Task 1: Create a core services virtual machine and virtual network

VMs allow you to more easily scale your apps by adding more physical or virtual servers to distribute the workload across multiple VMs

- **Instructions**
- Sign in to the Azure portal - <https://portal.azure.com>.
- Search for and select Virtual Machines.
- From the virtual machines page, select Create then select Azure Virtual Machine.
- On the Basics tab, use the following information to complete the form, and then select Next: Disks >. For any setting not specified, leave the default value
- Select the Monitoring tab. For Boot Diagnostics, select Disable.
- Select Review + Create, and then select Create.

Home >

## CreateVm-MicrosoftWindowsServer.WindowsServer-201-20240623133305 | Overview

Deployment

Search x << Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

**✓ Your deployment is complete**

Deployment name: CreateVm-MicrosoftWindowsServer.Wi... Start time: 6/23/2024, 1:57:31 PM  
Subscription: [Azure for Students](#) Correlation ID: 1cea6c73-2f0a-433e-86al  
Resource group: [az104-rg5](#)

▼ Deployment details

^ Next steps

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

[Run a script inside the virtual machine](#) Recommended

[Go to resource](#) [Create another VM](#)

Give feedback

[Tell us about your experience with deployment](#)

**Cost Management**

Get notified to stay within your budget and prevent unexpected charges on your bill.

[Set up cost alerts >](#)

**Microsoft Defender for Cloud**

Secure your apps and infrastructure

[Go to Microsoft Defender for Cloud >](#)

**Free Microsoft tutorials**

[Start learning today >](#)

**Work with an expert**

Home > Virtual machines >

## Create a virtual machine

[Click here to try out the Azure Copilot for additional recommendations while creating a virtual machine](#) →

### Project details

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

Subscription \* ⓘ

Resource group \* ⓘ   
[Create new](#)

### Instance details

Virtual machine name \* ⓘ

Region \* ⓘ

Availability options ⓘ

Security type ⓘ

[< Previous](#) [Next: Disks >](#) [Review + create](#)

## Task 2: Create a virtual machine in a different virtual network

### Instructions and steps

- From the Azure portal, search for and navigate to Virtual Machines.
- From the virtual machines page, select Create then select Azure Virtual Machine.
- On the Basics tab, use the following information to complete the form, and then select Next: Disks >. For any setting not specified, leave the default value.

Microsoft Azure

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

Copilot

cantonweke@hotmail.c...  
DEFAULT DIRECTORY

Home > Virtual machines >

Create a virtual machine

Basics Disks **Networking** Management Monitoring

Define network connectivity for your virtual machine by configuring n inbound and outbound connectivity with security group rules, or plac [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created f

Virtual network \*

CoreServicesVM-vnet  
[Create new](#)

Subnet \*

Core (10.0.0.0/24)  
[Manage subnet configura](#)

Public IP

(new) ManufacturingVM  
[Create new](#)

NIC network security group

☐ None  
☒ Basic

< Previous

Next : Management >

Review + create

Create virtual network

premises network. [Learn more](#)

Name \* ManufacturingVnet

Address space

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

<input type="checkbox"/> Address range *	Addresses	Overlap	
<input type="checkbox"/> 10.1.0.0/16	10.1.0.0 - 10.1.255.255 (65536 addresses)	None	<a href="#">...</a>
<input checked="" type="checkbox"/> 172.16.0.0/16	172.16.0.0 - 172.16.255.255 (65536 addresses)	None	<a href="#">...</a>
<input type="text"/>	(0 Addresses)	None	

Subnets

The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

<input type="checkbox"/> Subnet name	Address range	Addresses	
<input checked="" type="checkbox"/> Manufacturing	172.16.0.0/24	172.16.0.0 - 172.16.0.255 (256 addresses)	<a href="#">...</a>
<input type="text"/>	<input type="text"/>	(0 Addresses)	

OK

Discard

- select the Monitoring tab. For Boot Diagnostics, select Disable.

Home > Virtual machines >

Create a virtual machine

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Configure monitoring options for your VM.

Alerts

Enable recommended alert rules ☐

Diagnostics

Boot diagnostics

☐ Enable with managed storage account (recommended)  
☐ Enable with custom storage account  
☒ Disable

Enable OS guest diagnostics

☐

Health

Enable application health monitoring ☐

< Previous

Next : Advanced >

Review + create

Give feedback

Select Review + Create, and then select Create.

The screenshot displays the Azure portal interface for a deployment named 'CreateVm-MicrosoftWindowsServer.WindowsServer-201-20240623140102'. The 'Overview' tab is selected, showing a green checkmark and the message 'Your deployment is complete'. The deployment details include the name, subscription ('Azure for Students'), resource group ('az104-rg5'), start time ('6/23/2024, 2:07:26 PM'), and correlation ID. Under 'Next steps', there are three recommended actions: 'Setup auto-shutdown', 'Monitor VM health, performance and network dependencies', and 'Run a script inside the virtual machine'. At the bottom, there are buttons for 'Go to resource' and 'Create another VM'. On the right sidebar, there are links for 'Cost Management', 'Microsoft Defender for Cloud', 'Free Microsoft tutorials', and 'Work with an expert'.

### Task 3: Use Network Watcher to test the connection between virtual machines

Network Watcher provides tools to monitor, diagnose, and view connectivity-related metrics for your Azure deployments.

#### Instructions

- From the Azure portal, search for and select Network Watcher.
- From Network Watcher, in the Network diagnostic tools menu, select Connection troubleshoot.

Home >

## Network Watcher

Microsoft

Search

+ Create Manage view Refresh Export to CSV Open query Assign tags Disable

Overview

- Get started
- Monitoring
- Network diagnostic tools
  - IP flow verify
  - NSG diagnostics
  - Next hop
  - Effective security rules
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot
- Metrics
- Logs

Filter for any field...

Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 1 of 1 records.

No grouping List view

<input type="checkbox"/> Name ↑↓	Subscription ↑↓	Location ↑↓
<input type="checkbox"/> NetworkWatcher_eastus	Azure for Students	East US

< Previous Page 1 of 1 Next >

Give feedback

- Use the following information to complete the fields on the Connection troubleshoot page

Home > Network Watcher

## Network Watcher | Connection troubleshoot

Microsoft

Search

Overview

- Get started
- Monitoring
- Network diagnostic tools
  - IP flow verify
  - NSG diagnostics
  - Next hop
  - Effective security rules
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot
- Metrics
- Logs

Network Watcher connection troubleshoot provides the capability to check a direct TCP or ICMP connection from a virtual machine (VM), application gateway v2, or Bastion host to a VM, fully qualified domain name (FQDN), URI, or IP address. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Run diagnostic tests". [Learn more.](#)

**Source**

Source type \*

Virtual machine \*   
[Select virtual machine](#)

**Destination**

Destination type ☒ Select a virtual machine  
☐ Specify manually

Virtual machine \*   
[Select virtual machine](#)

Give feedback

# Network Watcher | Connection troubleshoot

- Overview
- Get started
- Monitoring
- Network diagnostic tools
  - IP flow verify
  - NSG diagnostics
  - Next hop
  - Effective security rules
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot**
- Metrics
- Logs

## Probe settings

Preferred IP version ⓘ

Protocol ⓘ ☒ TCP ☐ ICMP

Destination port \* ⓘ

Source port ⓘ

## Connection diagnostic

Diagnostics tests \* ⓘ

[Run diagnostic tests](#)[Give feedback](#)

- Run diagnostic tests.

# Network Watcher | Connection troubleshoot


- Overview
- Get started
- Monitoring
- Network diagnostic tools
  - IP flow verify
  - NSG diagnostics
  - Next hop
  - Effective security rules
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot**
- Metrics
- Usage + quotas

[Export to CSV](#)

## Diagnostics tests

Test	Status	Details
Connectivity test	Unreachable	Probes sent: 30, probes failed: 30 <a href="#">See details</a>
Outbound NSG diagnostic	Deny	There are failed tests in the following NSGs: <ul style="list-style-type: none"><li><a href="#">CoreServicesVM-nsg</a></li></ul> <a href="#">See details</a>
Inbound NSG diagnostic	Deny	There are failed tests in the following NSGs: <ul style="list-style-type: none"><li><a href="#">ManufacturingVM-nsg</a></li></ul> <a href="#">See details</a>
Next hop (from source)	Success	Next hop type: None Route table: System Route
Destination port accessible	Reachable	

## Still can't connect?

[Troubleshooting documentation](#) 

[Contact support](#)

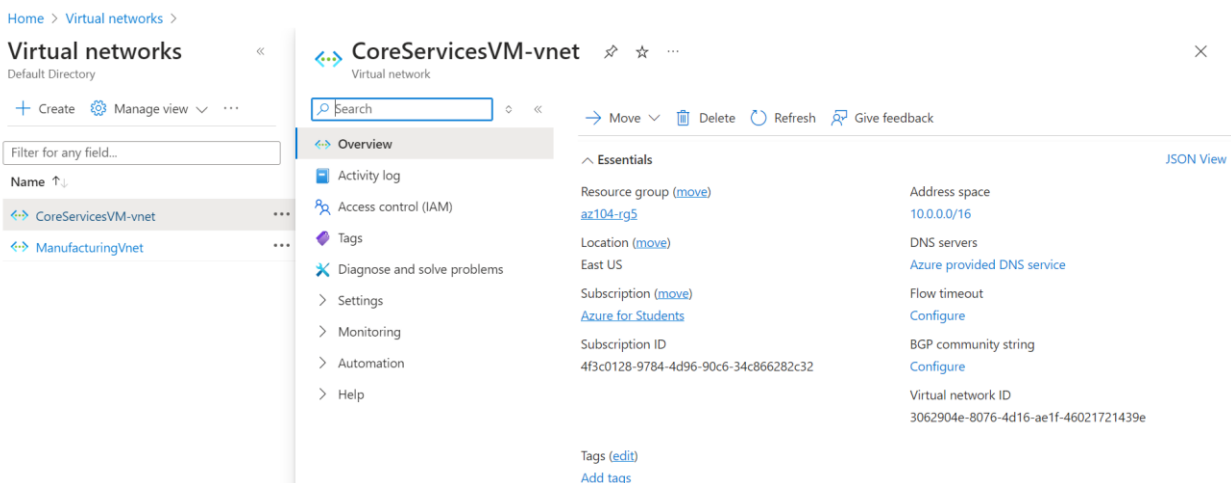


## Task 4: Configure virtual network peerings between virtual networks

Azure Virtual Network Peering, allows can easy link two or more Virtual Networks together. For the sake of connectivity, the virtual networks appear to be one. Peer virtual networks use the Microsoft backbone architecture to transport traffic between virtual machines.

### Instructions and step to do the configuration

- In the Azure portal, select the CoreServicesVnet virtual network.



- In CoreServicesVnet, under Settings, select Peerings.
- Use the information in the following table to create the peering.
- On CoreServicesVnet Peerings, select + Add.

Home > Virtual networks > CoreServicesVM-vnet | Peerings >

## Add peering

CoreServicesVM-vnet

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. This will allow resources in either virtual network to directly connect and communicate with resources in the peered virtual network.

### Remote virtual network summary

Peering link name \*

Virtual network deployment model ⓘ  
☒ Resource manager  
☐ Classic

I know my resource ID ⓘ ☐

Subscription \*

Virtual network \*

### Remote virtual network peering settings

- In CoreServicesVnet Peerings, verify that the CoreServicesVnet-to-ManufacturingVnet peering is listed. Refresh the page to ensure the Peering status is Connected.
- Switch to the ManufacturingVnet and verify the ManufacturingVnet-to-CoreServicesVnet peering is listed. Ensure the Peering status is Connected

Home > Virtual networks > CoreServicesVM-vnet

### Virtual networks

Default Directory

+ Create Manage view ...

Filter for any field...

Name ↑

- CoreServicesVM-vnet
- ManufacturingVnet

### CoreServicesVM-vnet | Peerings

Virtual network

Search

- Address space
- Connected devices
- Subnets
- Bastion
- DDoS protection
- Firewall
- Microsoft Defender for Cloud
- Network manager
- DNS servers
- Peerings**
- Service endpoints
- Private endpoints
- Properties

+ Add Refresh Export to CSV

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. [Learn more](#)

Filter by name...

Name	Peering s...	Peeri...	Remo...	Virtu...
ManufacturingVnet-to-CoreServicesVnet	Fully Synchroni	Connected	Manufac...	Disabled

Added virtual network peering  
Successfully added virtual network peering 'ManufacturingVnet-to-CoreServicesVnet' to 'CoreServicesVM-vnet'.

## Task 5: Use Azure PowerShell to test the connection between virtual machines

### Instruction and steps to the configuration

- In this task, you retest the connection between the virtual machines in different virtual networks.
- Verify the private IP address of the CoreServicesVM
- From the Azure portal, search for and select the CoreServicesVM virtual machine.
- On the Overview blade, in the Networking section, record the Private IP address of the machine. You need this information to test the connection.

The image displays two screenshots from the Azure portal. The top screenshot shows the 'Network settings' page for the 'CoreServicesVM' virtual machine. The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Bastion, Windows Admin Center, Networking, Network settings (selected), and Load balancing. The main content area shows details for the 'coreservicesvm721' network interface, including its virtual network/subnet ('CoreServicesVM-vnet / Core'), public IP address ('52.190.10.242'), private IP address ('10.0.0.4'), and associated network security group ('CoreServicesVM-nsg'). A 'Rules' section is partially visible. The bottom screenshot shows the 'Overview' page for the 'CoreServicesVM' virtual machine. The left sidebar lists navigation options: Overview (selected), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Bastion, Windows Admin Center, Networking, Settings, Disks, and Extensions + applications. The main content area shows essential information: Resource group ('az104-rg5'), Status ('Running'), Location ('East US'), Subscription ID ('4f3c0128-9784-4d96-90c6-34c866282c32'), Operating system ('Windows (Windows Server 2019 Datacenter)'), Size ('Standard D2s v3 (2 vcpus, 8 GiB memory)'), Public IP address ('52.190.10.242'), Virtual network/subnet ('CoreServicesVM-vnet/Core'), DNS name ('Not configured'), Health state ('-'), and Time created ('6/23/2024, 10:57 AM UTC').

**CoreServicesVM | Network settings**

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

This is a new experience. [Please provide feedback](#)

coreservicesvm721

Virtual network / subnet

CoreServicesVM-vnet / Core

Public IP address

52.190.10.242

Private IP address

10.0.0.4

Admin security rules

0 (Configure)

0 (Configure)

0 (Configure)

0 (Configure)

Network security group

CoreServicesVM-nsg

Accelerated networking

Enabled

Effective security rules

0

Rules

Collapse all

Network security group CoreServicesVM-nsg (attached to networkInterface: coreservicesvm721)

Impacts 0 subnets, 1 network interfaces

Create port rule

**CoreServicesVM**

Virtual machine

Search

Connect

Start

Restart

Stop

Hibernate

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Settings

Disks

Extensions + applications

Essentials

Resource group (move)

az104-rg5

Status

Running

Location

East US

Subscription (move)

Azure for Students

Subscription ID

4f3c0128-9784-4d96-90c6-34c866282c32

Operating system

Windows (Windows Server 2019 Datacenter)

Size

Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address

52.190.10.242

Virtual network/subnet

CoreServicesVM-vnet/Core

DNS name

Not configured

Health state

-

Time created

6/23/2024, 10:57 AM UTC

Tags (edit)

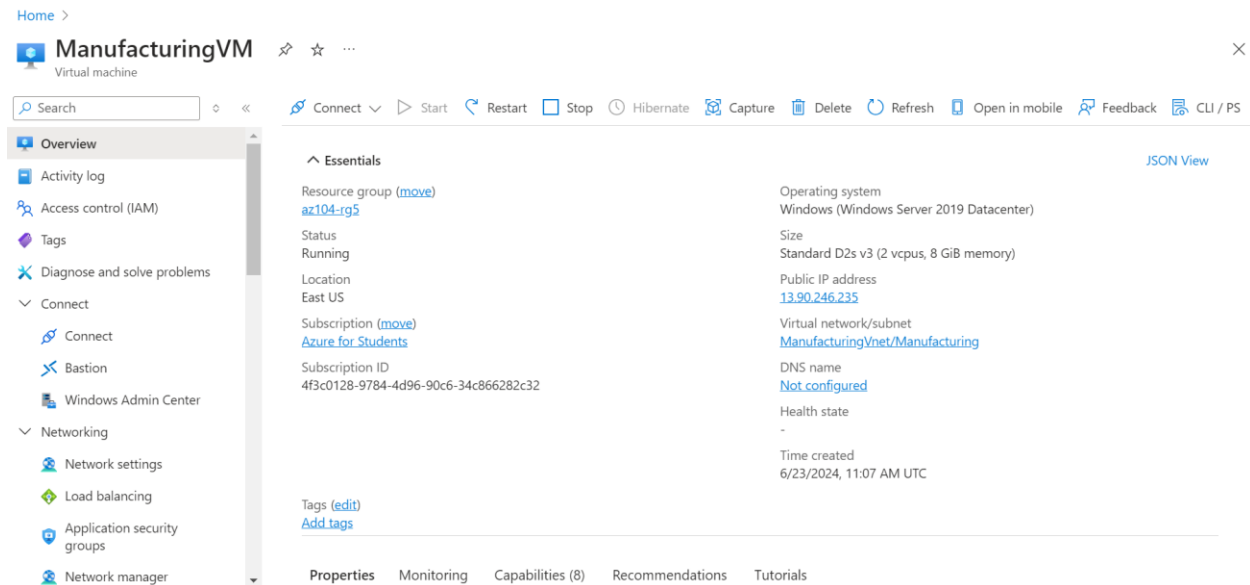
Add tags

JSON View

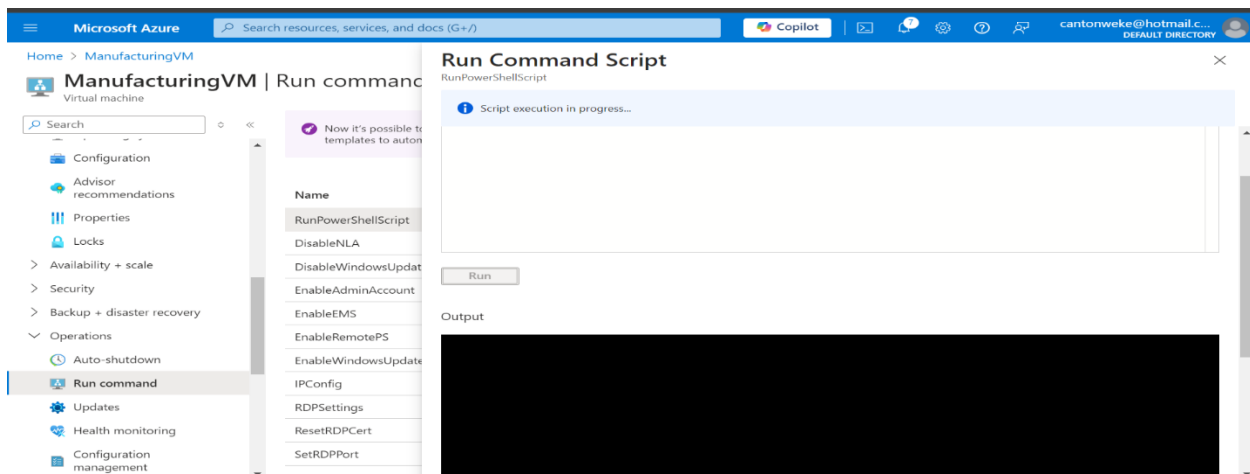
## Test the connection to the CoreServicesVM from the ManufacturingVM.

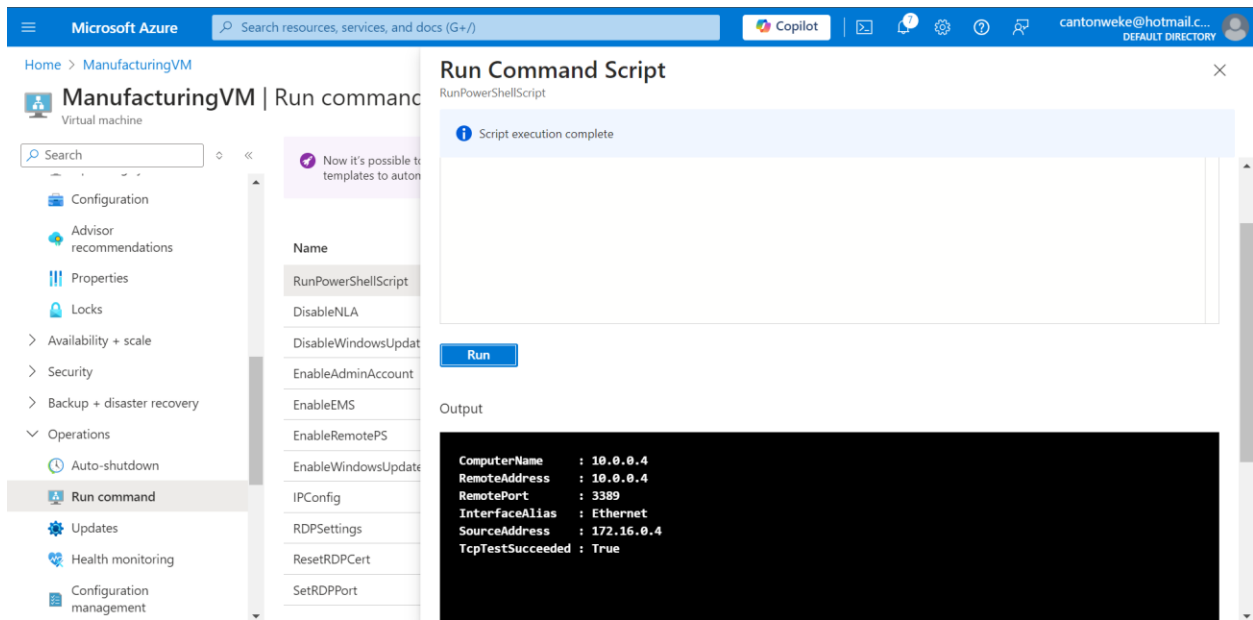
### intrusions

- Switch to the ManufacturingVM virtual machine.



- In the Operations blade, select the Run command blade.
- Select RunPowerShellScript and run the Test-NetConnection command. Be sure to use the private IP address of the CoreServicesVM.

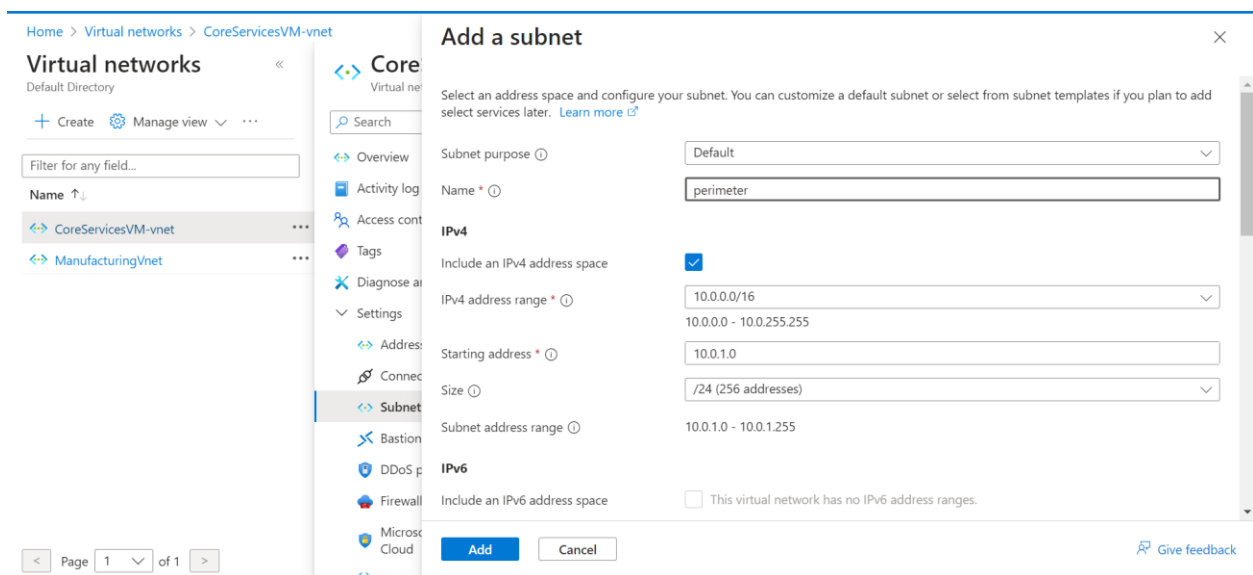




## Task 6: Create a custom route

### Instructions

- Search for select the CoreServicesVnet.
- Select Subnets and then + Create. Be sure to Save your changes.



- In the Azure portal, search for and select Route tables, and then select Create.

[Home](#) > [Route tables](#) >

## 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 \* ⓘ

Resource group \* ⓘ  [Create new](#)

### Instance details

Region \* ⓘ

Name \* ⓘ  ✓

Propagate gateway routes \* ⓘ ☐ Yes ☒ No

Previous

Next

Review + create

[Home](#) >



## Microsoft.RouteTable-20240623151141 | Overview

Deployment

[Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

**Overview**

[Inputs](#)

[Outputs](#)

[Template](#)

### ✓ Your deployment is complete

Deployment name : Microsoft.RouteTable-2024062... Start time : 6/23/2024, 3:17:15 PM  
Subscription : [Azure for Students](#) Correlation ID : 0938e7e4-905a-414b-b88a-44...  
Resource group : [az104-rg5](#)

> Deployment details

> Next steps

[Go to resource](#)

Give feedback

[Tell us about your experience with deployment](#)



### Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

[Set up cost alerts >](#)



### Microsoft Defender for Cloud

Secure your apps and infrastructure

[Go to Microsoft Defender for Cloud >](#)

### Free Microsoft tutorials

[Start learning today >](#)

### Work with an expert

Azure experts are service provider partners

<https://portal.azure.com/#blade/HubsExtension/ResourceMenuBlade/id/%2F...>

- After the route table deploys, select Go to resource.
- Select Routes and then + Add. Create a route from the future NVA to the CoreServices virtual network.

Microsoft Azure | Search resources, services, and docs (G+/I) | Copilot | cantonweke@hotmail.c... | DEFAULT DIRECTORY

Home > Microsoft.RouteTable-20240623151141 | Overview > rt-CoreServices

rt-CoreServices | Routes ☆ ...

Route table

Search routes

Name ↑↓ Address prefix ↑↓

No results.

**Add route**

rt-CoreServices

Route name \* PerimetertoCore ✓

Destination type \* ⓘ IP Addresses ✓

Destination IP addresses/CIDR ranges \* ⓘ 10.0.0/16 ✓

Next hop type \* ⓘ Virtual appliance ✓

Next hop address \* ⓘ 10.0.1.7 ✓

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Add Give feedback

rt-CoreServices | Routes ☆ ...

Route table

Search routes

Name ↑↓	Address prefix ↑↓	Next hop type ↑↓	Next hop IP address ↑↓
PerimetertoCore	10.0.0/16	VirtualAppliance	10.0.1.7

- Select + Add when the route is completed. The last thing to do is associate the route with the subnet.
- Select Subnets and then Associate. Complete the configuration.

Home > Microsoft.RouteTable-20240623151141 | Overview > rt-CoreServices

### rt-CoreServices | Subnets

Route table

Search  + Associate

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Settings  
Configuration  
Routes  
**Subnets**  
Properties  
Locks  
Monitoring  
Automation  
Help

Search subnets

Name ↑↓	Address range ↑↓
No results.	

#### Associate subnet

rt-CoreServices

Virtual network  CoreServicesVM-vnet (az104-rg5)

Subnet \*  Core

OK Give feedback

Home > Microsoft.RouteTable-20240623151141 | Overview > rt-CoreServices

### rt-CoreServices | Subnets

Route table

Search  + Associate

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Settings  
Configuration  
Routes  
**Subnets**  
Properties  
Locks  
Monitoring  
Automation  
Help








Search subnets

Name ↑↓	Address range ↑↓	Virtual network ↑↓	Security group ↑↓
Core	10.0.0.0/24	CoreServicesVM-vnet	-

Give feedback



## Overview of the resources

Resources		
<div>Recent</div> <div>Favorite</div>		
Name	Type	Last Viewed
 rt-CoreServices	Route table	10 minutes ago
 CoreServicesVM-vnet	Virtual network	23 minutes ago
 ManufacturingVM	Virtual machine	35 minutes ago
 CoreServicesVM	Virtual machine	38 minutes ago
 az104-rg5	Resource group	an hour ago
 NetworkWatcher_eastus	Network Watcher	18 hours ago
 NetworkWatcherRG	Resource group	18 hours ago
<a href="#">See all</a>		

## Conclusion

This lab report provided a comprehensive grasp of virtual network management in Azure by covering not only how each activity is implemented but also the underlying ideas and recommended practices. The report allows one have the ability to manage intricate network designs in the cloud, the report also acts as manual for creating, testing, and setting up virtual networks and virtual machines (VMs).

The abilities and information obtained from this lab on administering Azure virtual networks and virtual machines are invaluable in real-world situations. Cloud environments are widely used by organizations to grow their operations and provide high availability. IT workers can deploy and segregate applications based on performance or security needs with efficiency if they are skilled in creating and managing virtual machines (VMs) within various VNets. In the real world, this segregation is essential because, in order to reduce security threats, sensitive data and services must be kept separate from applications that are visible to the public. It is equally important to be able to use tools such as Network Watcher to identify and fix connectivity problems, since poor communication between virtual machines can have a big influence on corporate activities, ranging from internal enterprise apps to e-commerce platforms.

In addition, setting up VNet peering and routes in an actual setting highlights the necessity of complicated network architectures that can accommodate intricate business requirements. For example, VNet peering enables smooth connectivity between different divisions or subsidiaries

inside a big business, promoting cooperation and data sharing without sacrificing security. Network traffic is directed effectively with custom routing, enhancing performance and upholding legal compliance. The automation of these setups and monitoring processes by Azure PowerShell shows how businesses can use scripting to improve workflow, lower manual error rates, and maintain a reliable cloud infrastructure. Essentially, the practical expertise gained in this lab offers a guide for administering safe, effective, and scalable cloud networks that meet modern corporate needs.