CST 8912- LAB 2

By: Obaida Kandakji 041272028

Lab Instructions

Step 1 – Resource Group

1. In the **Azure portal**, create a new Resource Group named: CST8912-demo
    - Region: **Canada Central**

Step 2 – Virtual Networks

1. Navigate to **Virtual Networks**.
2. Create the following VNet resources:
    - **cst8912_vnet0** – Region: *Canada Central*
    - **cst8912_vnet1** – Region: *East US*
    - **cst8912_vnet2** – Region: *East US*

Step 3 – Review VNet Configurations

- Verify address space and subnets for each virtual network.
- Ensure no overlap in IP ranges to avoid routing conflicts.

Step 4 – Configure Peerings

1. On **cst8912_vnet0**, add peering to:
    - **cst8912_vnet1**
    - **cst8912_vnet2**

Example link names:

    - cst8912_vnet0_to_cst8912_vnet1
    - cst8912_vnet0_to_cst8912_vnet2

Note: Each peering creates a pair of links (e.g., vnet0_to_vnet1 and vnet1_to_vnet0).

2. On **cst8912_vnet1**, add peering to:
    - **cst8912_vnet2**
    - Example link name: cst8912_vnet1_to_cst8912_vnet2

Step 5 – Deploy Virtual Machines

1. Navigate to **Virtual Machines** in the portal.
2. Create the following VMs:
    - **VM0** – Region: Canada Central → Network: *cst8912_vnet0*
    - **VM1** – Region: East US → Network: *cst8912_vnet1*
    - **VM2** – Region: East US → Network: *cst8912_vnet2*

VM configuration:

- Image: *Windows Server 2022 Datacenter*
- Authentication: Username & Password
- Networking: Assign NIC to respective VNet

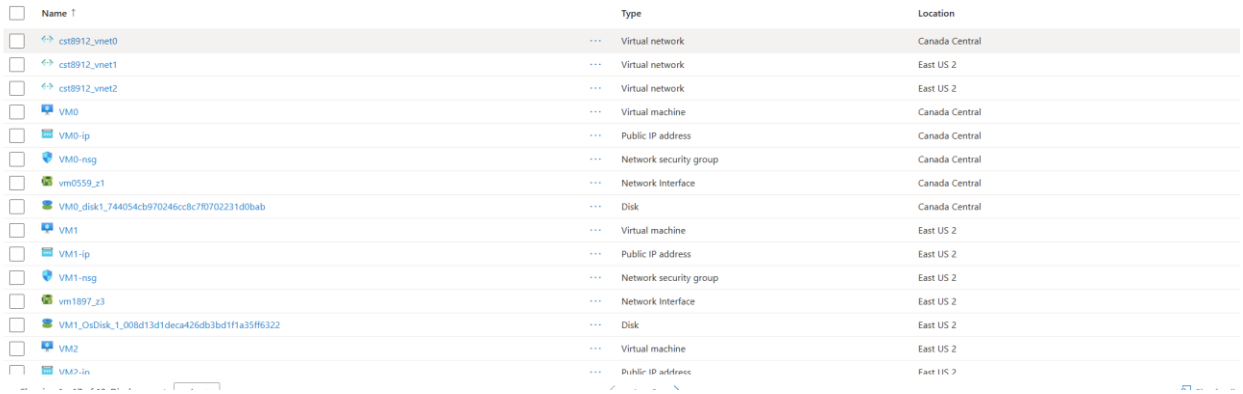
Step 6 – Verify Connectivity

1. Connect to **VM0** using RDP.
2. Open **PowerShell** inside VM0.
3. Run the following command to test connectivity to VM1 and VM2 (replace "ip" with the private IPs of VM1 and VM2):
4. Test-NetConnection -ComputerName "ip" -Port 3389 -InformationLevel Detailed
5. Repeat the test:
    - From **VM0 → VM1**
    - From **VM0 → VM2**
    - From **VM1 → VM2**
6. Verify results show **successful TCP connections** over private IPs.

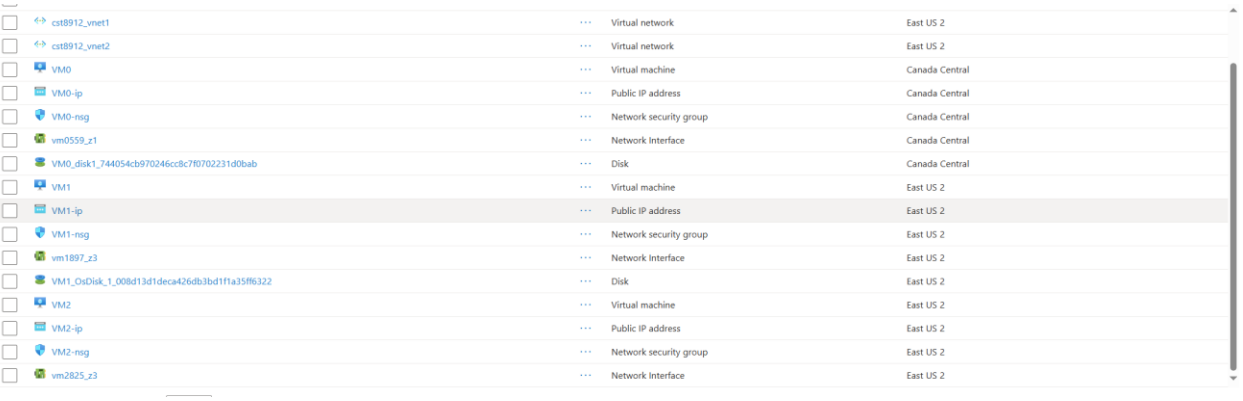
Step 7 – Cleanup

- Delete all resources (Resource Group CST8912-demo) after completing the lab.

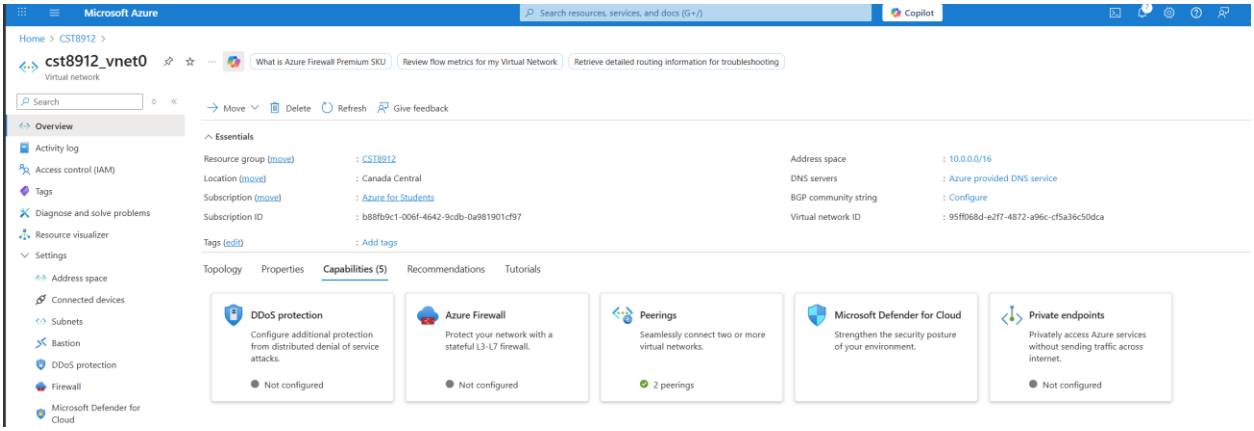
SCREENSHOTS

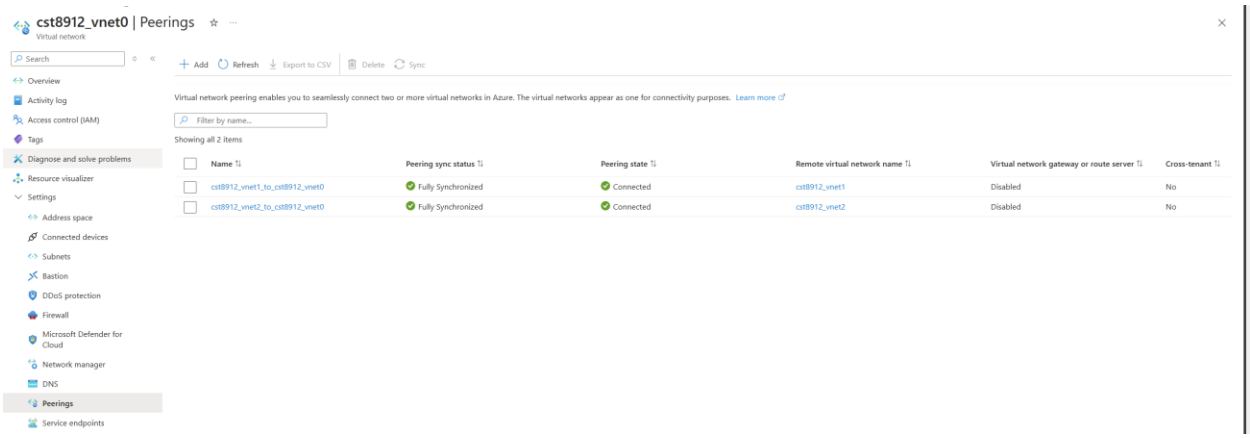


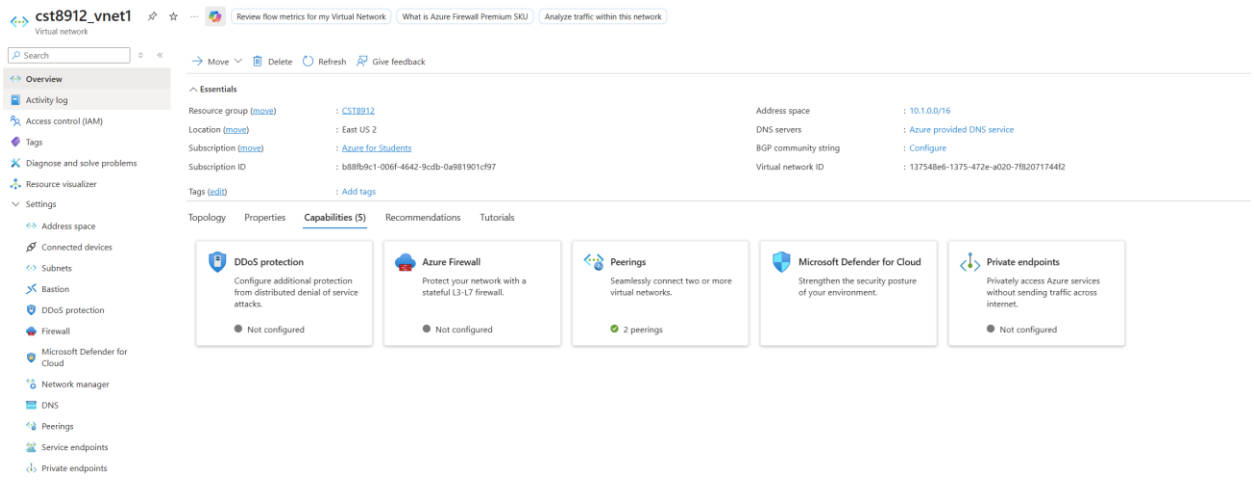
Name ↑	Type	Location
cst8912_vnet0	Virtual network	Canada Central
cst8912_vnet1	Virtual network	East US 2
cst8912_vnet2	Virtual network	East US 2
VM0	Virtual machine	Canada Central
VM0-ip	Public IP address	Canada Central
VM0-nsg	Network security group	Canada Central
vm0559_z1	Network Interface	Canada Central
VM0_disk1_744054cb970246cc8c7f0702231d0bab	Disk	Canada Central
VM1	Virtual machine	East US 2
VM1-ip	Public IP address	East US 2
VM1-nsg	Network security group	East US 2
vm1897_z3	Network Interface	East US 2
VM1_OsDisk_1_008d13d1deca426db3bd1f1a35ff6322	Disk	East US 2
VM2	Virtual machine	East US 2
VM2-ip	Public IP address	East US 2

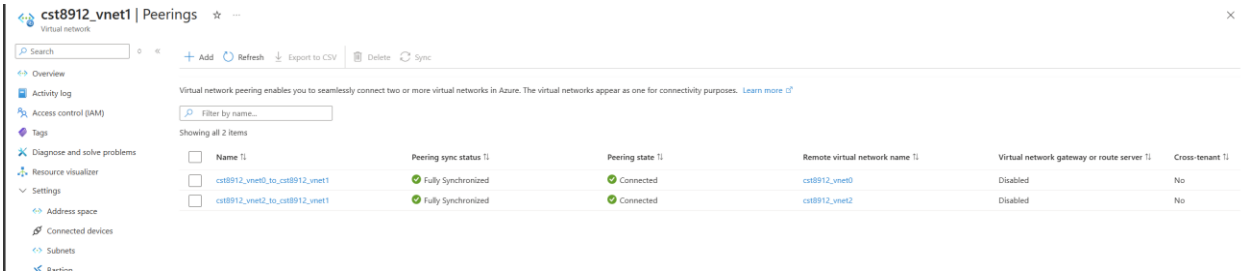


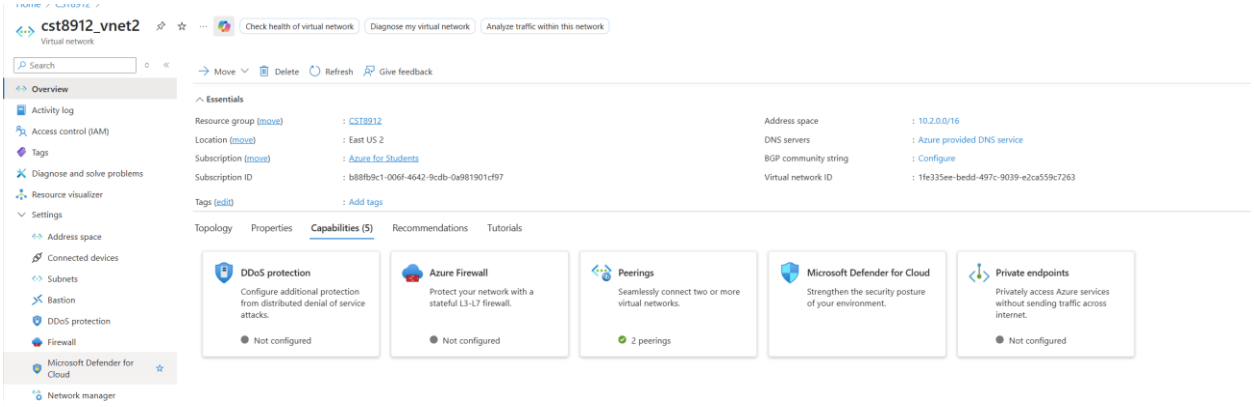
cst8912_vnet1	Virtual network	East US 2
cst8912_vnet2	Virtual network	East US 2
VM0	Virtual machine	Canada Central
VM0-ip	Public IP address	Canada Central
VM0-nsg	Network security group	Canada Central
vm0559_z1	Network Interface	Canada Central
VM0_disk1_744054cb970246cc8c7f0702231d0bab	Disk	Canada Central
VM1	Virtual machine	East US 2
VM1-ip	Public IP address	East US 2
VM1-nsg	Network security group	East US 2
vm1897_z3	Network Interface	East US 2
VM1_OsDisk_1_008d13d1deca426db3bd1f1a35ff6322	Disk	East US 2
VM2	Virtual machine	East US 2
VM2-ip	Public IP address	East US 2
VM2-nsg	Network security group	East US 2
vm2825_z3	Network Interface	East US 2

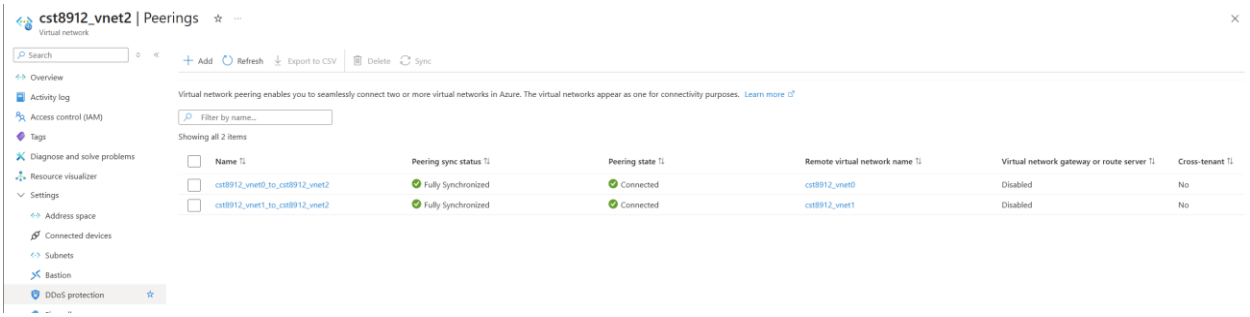


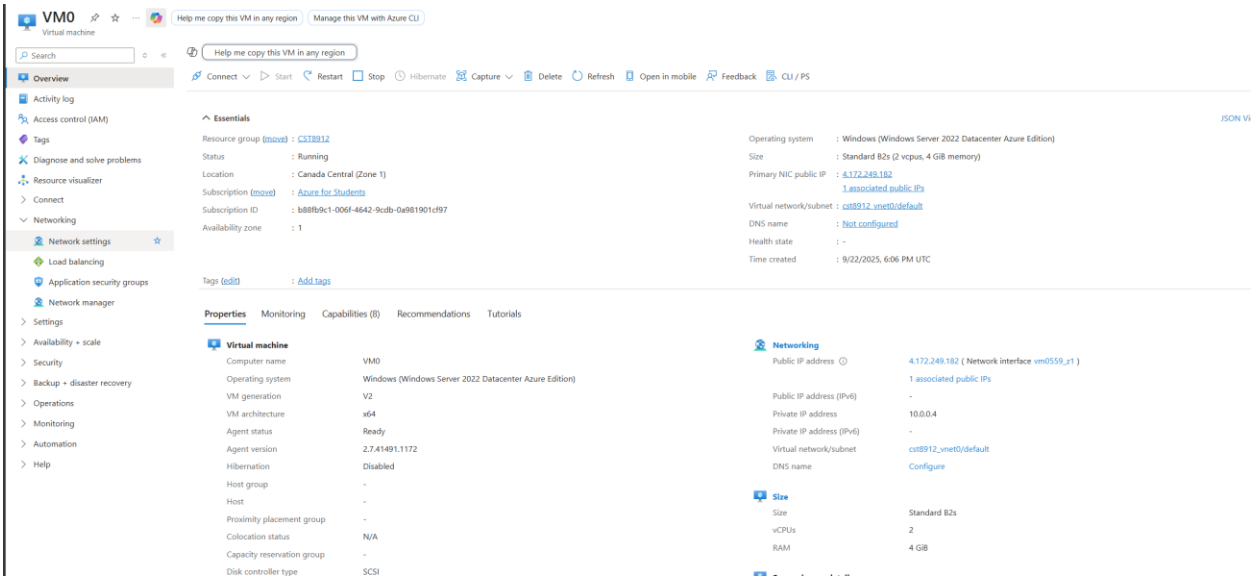

cst8912_vnet0 | Peerings
Virtual network
Search
Add
Refresh
Export to CSV
Delete
Sync
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS
Peerings
Service endpoints
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...
Showing all 2 items
Name
Peering sync status
Peering state
Remote virtual network name
Virtual network gateway or route server
Cross-tenant
cst8912_vnet1_to_cst8912_vnet0
Fully Synchronized
Connected
cst8912_vnet1
Disabled
No
cst8912_vnet2_to_cst8912_vnet0
Fully Synchronized
Connected
cst8912_vnet2
Disabled
No

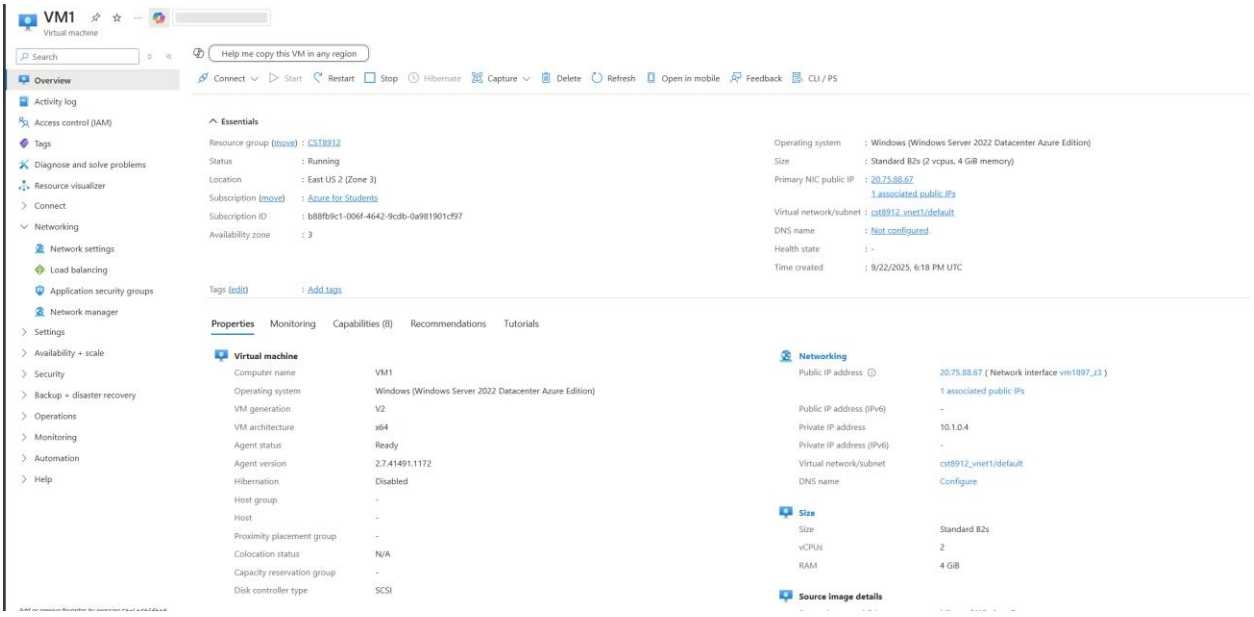

cst8912_vnet1
Virtual network
Review flow metrics for my Virtual Network
What is Azure Firewall Premium SKU
Analyze traffic within this network
Search
Move
Delete
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS
Peerings
Service endpoints
Private endpoints
Essentials
Resource group (move) : CST8912
Location (move) : East US 2
Subscription (move) : Azure for Students
Subscription ID : b88fb9c1-006f-4642-9cdb-0a981901cf97
Tags (edit) : Add tags
Address space : 10.1.0.0/16
DNS servers : Azure provided DNS service
BGP community string : Configure
Virtual network ID : 137548e6-1375-472e-a020-7f82071744f2
Topology
Properties
Capabilities (5)
Recommendations
Tutorials
DDoS protection
Configure additional protection from distributed denial of service attacks.
Not configured
Azure Firewall
Protect your network with a stateful L3-L7 firewall.
Not configured
Peerings
Seamlessly connect two or more virtual networks.
2 peerings
Microsoft Defender for Cloud
Strengthen the security posture of your environment.
Private endpoints
Privately access Azure services without sending traffic across internet.
Not configured


cst8912_vnet1 | Peerings
Virtual network
Search
Add
Refresh
Export to CSV
Delete
Sync
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
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...
Showing all 2 items
Name
Peering sync status
Peering state
Remote virtual network name
Virtual network gateway or route server
Cross-tenant
cst8912_vnet0_to_cst8912_vnet1
Fully Synchronized
Connected
cst8912_vnet0
Disabled
No
cst8912_vnet2_to_cst8912_vnet1
Fully Synchronized
Connected
cst8912_vnet2
Disabled
No


cst8912_vnet2
Virtual network
Check health of virtual network
Diagnose my virtual network
Analyze traffic within this network
Search
Move
Delete
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
Essentials
Resource group (move) : CST8912
Location (move) : East US 2
Subscription (move) : Azure for Students
Subscription ID : b88fb9c1-006f-4642-9cdb-0a981901cf97
Tags (edit) : Add tags
Address space : 10.2.0.0/16
DNS servers : Azure provided DNS service
BGP community string : Configure
Virtual network ID : 1fe335ee-bedd-497c-9039-e2ca559c7263
Topology
Properties
Capabilities (5)
Recommendations
Tutorials
DDoS protection
Configure additional protection from distributed denial of service attacks.
Not configured
Azure Firewall
Protect your network with a stateful L3-L7 firewall.
Not configured
Peerings
Seamlessly connect two or more virtual networks.
2 peerings
Microsoft Defender for Cloud
Strengthen the security posture of your environment.
Private endpoints
Privately access Azure services without sending traffic across internet.
Not configured


cst8912_vnet2 | Peerings
Virtual network
Search
Add
Refresh
Export to CSV
Delete
Sync
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
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...
Showing all 2 items
Name
Peering sync status
Peering state
Remote virtual network name
Virtual network gateway or route server
Cross-tenant
cst8912_vnet0_to_cst8912_vnet2
Fully Synchronized
Connected
cst8912_vnet0
Disabled
No
cst8912_vnet1_to_cst8912_vnet2
Fully Synchronized
Connected
cst8912_vnet1
Disabled
No


VM0
Virtual machine
Help me copy this VM in any region
Manage this VM with Azure CLI
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON Vi
Resource group (move) : CST8912
Status : Running
Location : Canada Central (Zone 1)
Subscription (move) : Azure for Students
Subscription ID : b88fb9c1-006f-4642-9cdb-0a981901cf97
Availability zone : 1
Operating system : Windows (Windows Server 2022 Datacenter Azure Edition)
Size : Standard B2s (2 vcpus, 4 GiB memory)
Primary NIC public IP : 4.172.249.182
1 associated public IPs
Virtual network/subnet : cst8912_vnet0/default
DNS name : Not configured
Health state : -
Time created : 9/22/2025, 6:06 PM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name VM0
Operating system Windows (Windows Server 2022 Datacenter Azure Edition)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.41491.1172
Hibernation Disabled
Host group -
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI
Networking
Public IP address 4.172.249.182 (Network interface vm0559_z1)
1 associated public IPs
Public IP address (IPv6) -
Private IP address 10.0.0.4
Private IP address (IPv6) -
Virtual network/subnet cst8912_vnet0/default
DNS name Configure
Size
Size Standard B2s
vCPUs 2
RAM 4 GiB


VM1
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
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
Resource group (move) : CST8912
Status : Running
Location : East US 2 (Zone 3)
Subscription (move) : Azure for Students
Subscription ID : b88fb9c1-006f-4642-9cdb-0a981901cf97
Availability zone : 3
Operating system : Windows (Windows Server 2022 Datacenter Azure Edition)
Size : Standard B2s (2 vcpus, 4 GiB memory)
Primary NIC public IP : 20.75.88.67
1 associated public IPs
Virtual network/subnet : cst8912_vnet1/default
DNS name : Not configured
Health state : -
Time created : 9/22/2025, 6:18 PM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name VM1
Operating system Windows (Windows Server 2022 Datacenter Azure Edition)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.41491.1172
Hibernation Disabled
Host group -
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI
Networking
Public IP address 20.75.88.67 (Network interface vm1897_z3)
1 associated public IPs
Public IP address (IPv6) -
Private IP address 10.1.0.4
Private IP address (IPv6) -
Virtual network/subnet cst8912_vnet1/default
DNS name Configure
Size
Size Standard B2s
vCPUs 2
RAM 4 GiB
Source image details

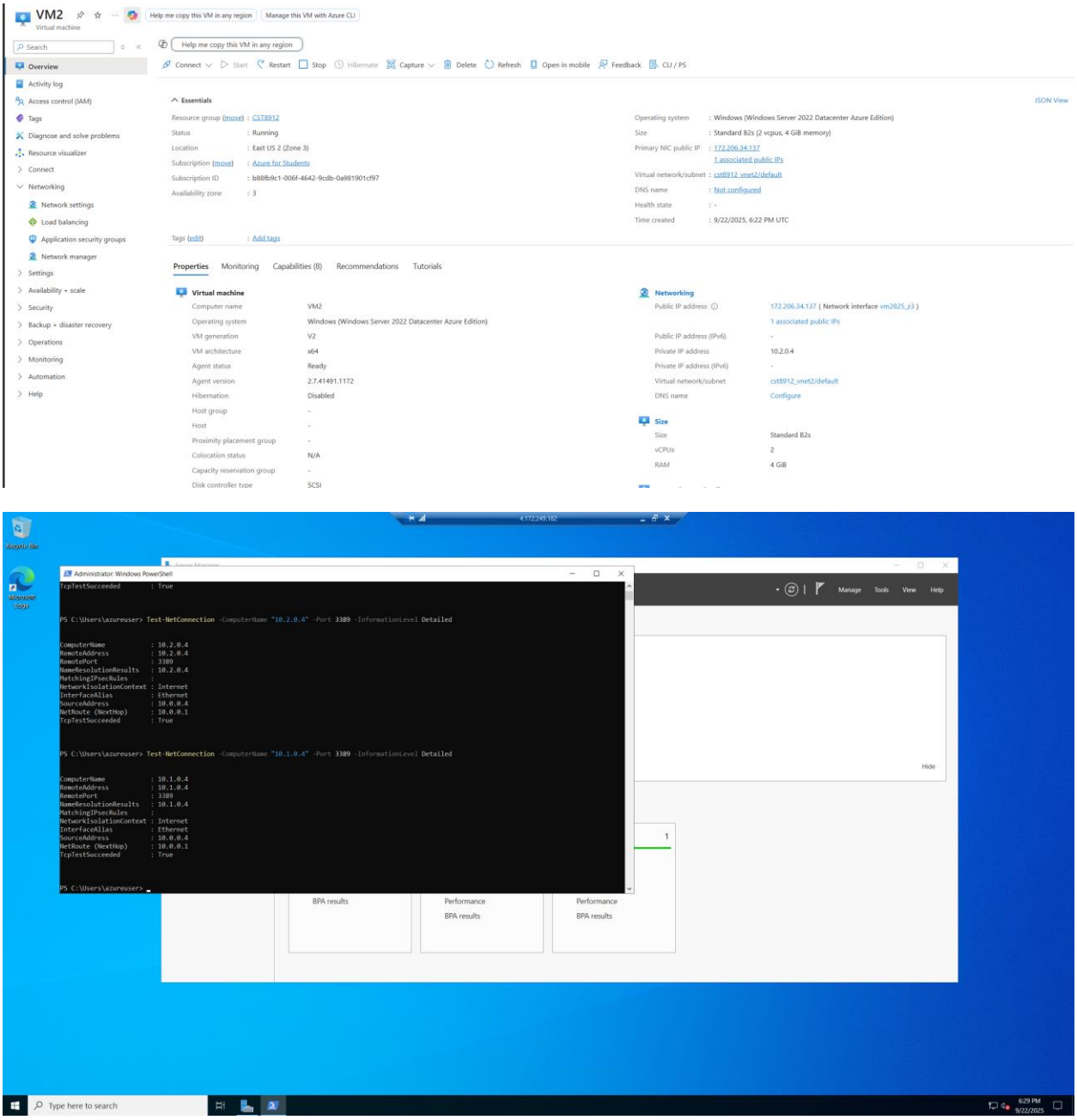


Figure 1:VM0 to vm1 and vm2

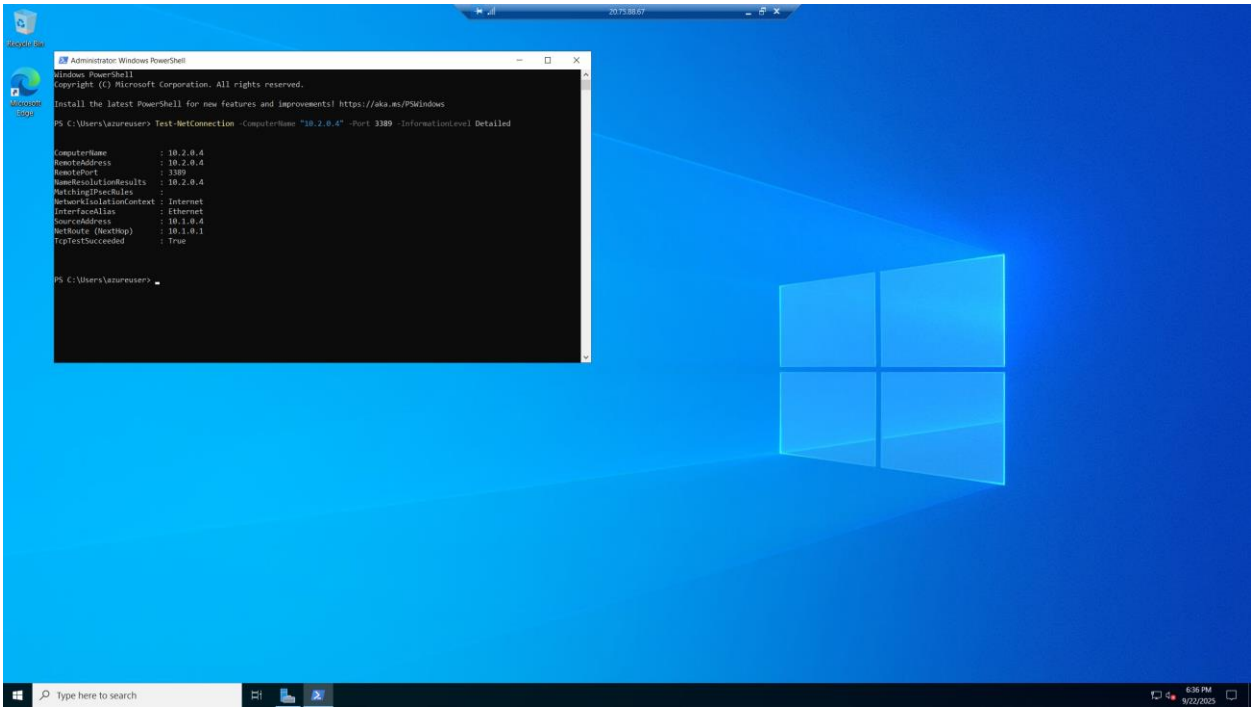


Figure 2: VM1 to VM2

Findings & Analysis:

Why VNet Peering is Important

VNet peering is an essential feature in cloud networking because it enables secure and seamless communication between separate virtual networks. By default, virtual networks in Azure are isolated and cannot exchange traffic. Through peering, these networks can operate as though they are part of a single network, allowing resources such as virtual machines to interact directly using private IP addresses. This is particularly valuable in scenarios where an organization maintains workloads across multiple regions or separates environments for development, testing, and production. Without peering, additional infrastructure such as VPN gateways would be required, increasing both cost and complexity. Therefore, VNet peering simplifies network design while improving efficiency.

How Private IP Communication Was Established

Private IP communication in this lab was established by combining subnet configuration and VNet peering. Each virtual machine was automatically assigned a private IP address within its respective virtual network's address space. Once peering was configured between the networks, Azure updated the route tables so that traffic could flow across VNets without requiring public IP addresses. When connectivity tests were conducted using PowerShell, the results confirmed that the communication occurred entirely over private IP addresses, contained within Microsoft's secure backbone infrastructure. This demonstrates how Azure provides isolated, internal connectivity that does not traverse the public internet, ensuring both security and reliability.

Benefits of Global Peering (Performance and Security)

Global VNet peering extends the advantages of local peering across different Azure regions. In this lab, networks in Canada Central and East US were connected, simulating a distributed architecture. One of the primary benefits of global peering is performance, as traffic remains within Microsoft's private global network rather than passing through the public internet. This results in reduced latency and higher throughput, which are critical for applications requiring real-time or high-performance communication. Security is another key advantage, since private IP traffic never leaves Azure's internal backbone. This minimizes exposure to external threats and eliminates the need for additional encryption or tunneling solutions. Together, these benefits highlight why global VNet peering is a recommended practice for organizations seeking resilient, high-performance, and secure cloud architectures.