

My Project on Virtual Network Peering

by Lukman Olatunbosun Kolawole

1. What Is Azure VNet Peering?

Azure Virtual Network is used for the Virtual Network Peering which helps users to communicate with virtual networks in Azure network. **Virtual network Peering in Azure** helps the traffic of one virtual network to communicate to another virtual network. This can be used for database failover, cross-region data replication or disaster recovery. Virtual network Peering provides connection sharing in different regions.

2. Types Of VNet Peering

1. **Regional Virtual Network Peering:** This is connectivity between different Virtual Network within the same region.
2. **Global Virtual Network Peering:** This is connectivity across different regions, the connection is private peering that has low latency with high bandwidth in Azure backbone infrastructure.

3. Importance Of VNet Peering

- VNet peering is similar to an inter-VLAN Routing in VLAN of On-premise networks so it works similarly to inter-VLAN connect to one VLAN to another VLAN for communication.
- In Azure infrastructure, need to connect to virtual networks to each other for sharing traffic which can be applications, backup, replication, recovery, or information sharing.
- The virtual machines of virtual network connections to other virtual machines of different Virtual network via connection of VNet Peering in the same region or across the region

4. Benefits of Vnet peering

- The network traffic of peered Virtual networks will be private.
- It configures the connection with high bandwidth with low latency in the Virtual network region.
- This allows transferring data across Azure deployment models, subscriptions, and other regions.
- virtual network peering has no downtime issue.
- The use of global Virtual network peering has erased the need for Vnet to Vnet peering Azure configuration. It disabled the use of VPN encryption, public internet, or any gateways.
- This is time-saving process that controlling the backup, traffic, sharing from different regions and cost-effective.

5. Step-by-Step Configuration

1. Log into the Azure portal <https://portal.azure.com>.. if you don't have an account try to sign-up.
2. Kindly follow this pictures to create two Virtual Machines with two Virtual networks in two Different regions like **Uksouth-Vnet and UkWest-Vnet**.

This is my potal page. Here I want to start creating my VM1 and VM2.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The 'Project details' step is selected. The 'Subscription' dropdown is set to 'Azure subscription 1' and the 'Resource group' dropdown is set to '(None) UK South'. The 'Virtual machine name' field contains 'VM1'. The 'Region' dropdown is set to '(Europe) UK South'. Under 'Availability options', 'No infrastructure redundancy required' is selected. Under 'Security type', 'Trusted launch virtual machines' is selected. The 'Image' dropdown is set to 'Windows Server 2022 Datacenter: Azure Edition - x64 Gen2 (free services included)'. At the bottom, there are 'Review + create' and 'Next: Disks >' buttons.

Input your username and password, I choose none because I want to use Azure Bastion instead of Rdp.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The 'Basic options' step is selected. In the 'Administrator account' section, the 'Username' field is 'VM1' and the 'Password' and 'Confirm password' fields are empty. In the 'Inbound port rules' section, the 'Public inbound ports' dropdown is set to 'None'. There is a note: 'All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.' At the bottom, there are 'Review + create' and 'Next: Disks >' buttons.

This is where i created my Virtual Network as UkSouth-Vnet

Create virtual network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more ↗

Name *

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).

Address range	Addresses	Overlap
<input type="checkbox"/> 10.0.0.0/16	10.0.0 - 10.0.255.255 (65536 addresses)	None
	(0 Addresses)	

Subnets

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

Subnet name	Address range	Addresses
<input type="checkbox"/> default	10.0.0/24	10.0.0 - 10.0.0.255 (256 addresses)
	(0 Addresses)	

OK **Discard**

Here I want to use NSG(NETWORK SECURITY GROUP), no Public IP. I want to use Azure Bastion instead of Rdp.

Create a virtual machine

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

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more ↗

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *

Subnet *

Public IP

NIC network security group

Configure network security group

Delete NIC when VM is deleted

Review + create **< Previous** **Next : Management >**

Here I created My NSG as South-NSG

Create network security group

Name *

Inbound rules

- Allow RDP (TCP/3389)
- + Add an inbound rule

Outbound rules

- No results
- + Add an outbound rule

OK

Click review and create, then wait for validation.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The current step is 'Configure networking'. The configuration includes:

- Virtual network: [new] UK-SouthNet
- Subnet: [new] default (10.0.0.0/24)
- Public IP: None
- NIC network security group: Advanced (selected)
- Configure network security group: [new] South-nsg
- Delete NIC when VM is deleted: Unchecked
- Enable accelerated networking: Unchecked (disabled)

Load balancing section: You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?

At the bottom, the 'Review + create' button is highlighted with a red border, and the 'Next : Management >' button is visible.

I Click Create to create my VM1

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The current step is 'Review + create'. The validation status is 'Validation passed'. The summary shows:

- Basics: Validation passed
- Disks: Not specified
- Networking: Not specified
- Management: Not specified
- Monitoring: Not specified
- Advanced: Not specified
- Tags: Not specified
- Review + create: Selected

A note at the top states: 'Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.'

Price section: 1 X Standard B1s by Microsoft. Subscription credits apply: 0.0158 USD/hr. Pricing for other VM sizes.

TERMS: By clicking 'Create', (a) agree to the legal terms and privacy statements associated with the offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

At the bottom, the 'Create' button is highlighted with a red border, and the 'Next >' button is visible.

To create VM2 Just follow the same step on how we created VM1

The screenshot shows the 'Create a virtual machine' wizard on the 'Basics' tab. Key fields highlighted in red include:

- Subscription:** Azure subscription 1
- Resource group:** RG (highlighted)
- Virtual machine name:** VM2
- Region:** (Europe) UK West
- Availability options:** No infrastructure redundancy required
- Security type:** Trusted launch virtual machines

Buttons at the bottom include 'Review + create' (blue), '< Previous' (grey), 'Next : Disks >' (red), and 'Give feedback'.

Input your username and password, I choose none because I want to use VM1 Azure Bastion instead of Rdp as jump server to check connection.

The screenshot shows the 'Create a virtual machine' wizard on the 'Basics' tab. Key fields highlighted in red include:

- Size:** Standard_B1s - 1 vcpu, 1 GiB memory (US\$11.53/month) (free services elig...)
- Administrator account:**
 - Username:** VM2
 - Password:** (redacted)
 - Confirm password:** (redacted)

Under 'Inbound port rules', the 'Public inbound ports' section shows 'None' selected (radio button highlighted).

Buttons at the bottom include 'Review + create' (blue), '< Previous' (grey), 'Next : Disks >' (red), and 'Give feedback'.

This is how I created my second Virtual Network as UKWest-Vnet

Create virtual network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more ↗

Name *

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).

Address range	Addresses	Overlap
<input type="checkbox"/> 10.1.0.0/16	10.1.0.0 - 10.1.255.255 (55536 addresses)	None
	(0 Addresses)	None

Subnets

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

Subnet name	Address range	Addresses
<input type="checkbox"/> default	10.1.0.0/24	10.1.0.0 - 10.1.0.255 (256 addresses)
	(0 Addresses)	

OK **Discard**

No Public IP and no Rdp.

Create virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more ↗

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *

Subnet *

Public IP

NIC network security group

Configure network security group *

Delete NIC when VM is deleted

Review + create **< Previous** **Next : Management >** **OK** **Discard** **Give feedback**

Here I created My NSG as West-NSG,

Create network security group

Home > Virtual machines > Create a virtual machine > Create network security group

Name *

Inbound rules

- 1000: default-allow-rdp
- Any
- RDP (TCP/3389)
- + Add an inbound rule

Outbound rules

- No results
- + Add an outbound rule

OK

Click review and create to wait for validation.

This screenshot shows the 'Review + create' step of the Azure VM creation wizard. It displays the configuration details entered previously:

- Virtual network:** (new) UKWest-Vnet
- Subnet:** (new) default (10.1.0.0/24)
- Public IP:** None
- NIC network security group:** Advanced (selected)
- Configure network security group:** (new) West-nsg
- Delete NIC when VM is deleted:** Unchecked
- Enable accelerated networking:** Unchecked (Note: The selected VM size does not support accelerated networking.)

Load balancing: You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution:

Review + create < Previous Next : Management > Give feedback

I Click Create to create my VM2

This screenshot shows the 'Review + create' step of the Azure VM creation wizard, indicating validation has passed:

Validation passed

Price: 1 X Standard B1s by Microsoft **Subscription credits apply:** 0.0158 USD/hr **Pricing for other VM sizes**

TERMS: Clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Basics **Create** < Previous Next > Download a template for automation Give feedback

Now that my VMs are ready, I want to use Azure Bastion for more security. I deploy my Bastion. It will take approximately up to five minutes for the deployment.

This screenshot shows the 'Virtual machines' blade for VM1. The 'Bastion' section is highlighted, showing the 'Deploy Bastion' button:

VM1 | Bastion

Azure Bastion protects your virtual machines by providing lightweight, browser-based connectivity without the need to expose them through public IP addresses. Deploying will automatically create a Bastion host on a subnet in your virtual network. [Learn more](#)

Create Bastion

Name: Uk-SouthVNet-bastion
Resource group: RG
Virtual network: Uk-SouthVNet
Public IP address: Uk-SouthVNet-ip

Bastion pricing starts with an hourly base rate. [Learn more](#)

Deploy Bastion Configure manually

Tell us what you think of the Bastion experience

Page 1 of 1

Now go to either of the two **Virtual Networks** and select **Peerings**, from the **Settings blade**, and select **Add**.

Now, I go back to my UkSouth-Vnet to peer it with UkWest-Vnet. On my UkSouth-Vnet blade I will click on peering then click on Add.

I Add my peering as SouthVnet-WestVnet in the peering link name space and WestVnet-SouthVnet on the remote virtual network peering link space.

I choose my subscription and the virtual network i.e WestVnet then click Add

The status of the peering is Connected, as shown in the picture below.

The screenshot shows the 'Virtual networks' section in the Azure portal. Under 'Peering', it lists a single entry:

Name	Peer	Gateway transit
westNet-SouthVnet	Connected	Disabled

Now that my both Vnet are connected, I need to connect to my VM1 with Bastion already deployed. I will use the Bastion to connect to my VM1 by clicking Use Bastion.

The screenshot shows the 'Virtual machines' section in the Azure portal. Under 'Connect', the 'Bastion' tab is selected. A callout box points to the 'Use Bastion' button.

On this page I will click on use Bastion

The screenshot shows the 'Virtual machines' section in the Azure portal. Under 'Connect', the 'Bastion' tab is selected. A callout box points to the 'Use Bastion' button.

Here the Bastion will give option for username and password then fill it in then I will click connect.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named VM1. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a list of settings including Networking, Connect, Windows Admin Center, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Availability + scaling, Configuration, Identity, and Properties. A search bar at the top has the placeholder 'Search resources, services, and docs (G+J)'. The main area is titled 'VM1 | Bastion' and contains a message: 'Azure Bastion protects your virtual machines by providing lightweight, browser-based connectivity without the need to expose them through public IP addresses. Deploying will automatically create a Bastion host on a subnet in your virtual network. Learn more' and 'Using Bastion: Uk-SouthVnet-bastion, Provisioning State: Succeeded'. Below this, a section says 'Please enter username and password to your virtual machine to connect using Bastion.' It includes fields for 'Username' (VM1), 'Authentication Type' (Windows Authentication), and 'Password'. There's a 'Show' link next to the password field. A red box highlights the 'Connect' button, which is blue with white text. A red arrow points from the text above to this button. There's also a checked checkbox for 'Open in new browser tab'. At the bottom, there's a link to 'Tell us what you think of the Bastion experience'.

Here is my VM1 after signing in. To show connection to my Ukwest-Vnet I will go to Remote Desktop connection on my VM1.

The screenshot shows the Server Manager dashboard. The left navigation pane includes 'Dashboard', 'Local Server', 'All Servers', and 'File and Storage Services'. The main area is titled 'WELCOME TO SERVER MANAGER' and features a 'QUICK START' section with numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this, there's a 'WHAT'S NEW' section and a 'LEARN MORE' button. The 'ROLES AND SERVER GROUPS' section shows the following data:

File and Storage Services	Local Server	All Servers
1	1	1
Manageability	Manageability	Manageability
Events	Events	Events
Performance	Services	Services

At the bottom, there's a search bar with the placeholder 'Type here to search', a taskbar with icons for File Explorer, Task View, and File History, and a system tray showing the date and time as '10:16 AM 6/24/2023'.

Before I go to Remote Desktop connection on my VM1, I will go to my VM2 overview to copy VM2 Private IP to connect.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with 'Virtual machines' and a list of VMs: VM1 and VM2. The main area is titled 'VM2' and has a 'Overview' tab selected. Under 'Networking', the 'Virtual machine' section shows the following details:

- Computer name: VM2
- Operating system: Windows (Windows Server 2022 Datacenter Azure Edition)
- Image publisher: MicrosoftWindowsServer
- Image offer: WindowsServer
- Image plan: 2022-datacenter-azure-edition
- VM generation: V2
- VM architecture: x64
- Agent status: Ready

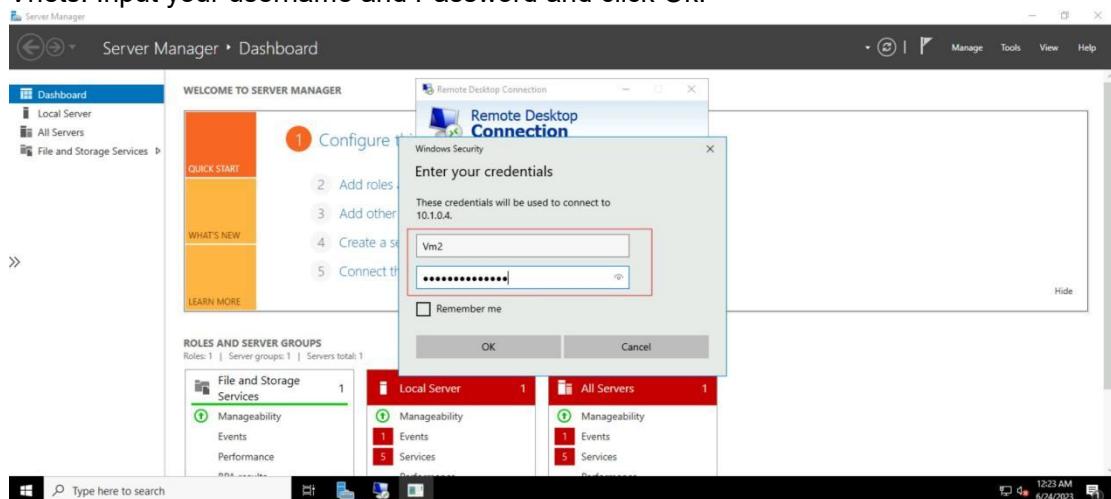
Under 'Networking', the 'Size' section shows:

- Public IP address: 51.140.244.7 (Network interface vm2142)
- Private IP address (IPv4): 10.1.0.4 (highlighted in red)
- Private IP address (IPv6):
- Virtual network/subnet: UKWest-Vnet/default
- DNS name: Configure

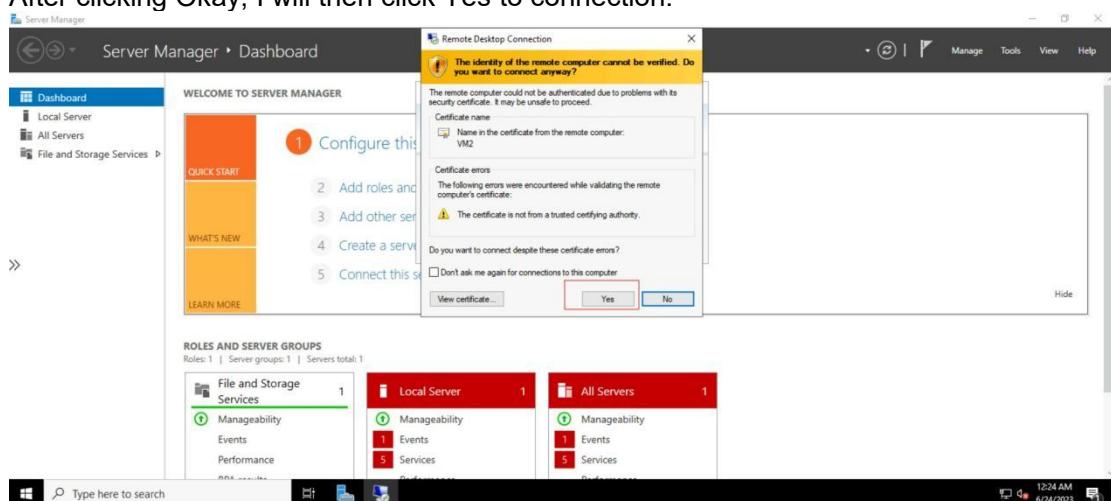
Input my VM2 private IP into the Remote Desktop connection of my VM1 then click connect.

The screenshot shows the Windows Server Manager dashboard. On the left, there's a sidebar with 'Dashboard', 'Local Server', 'All Servers', and 'File and Storage Services'. In the center, there's a 'WELCOME TO SERVER MANAGER' panel with a 'Configure this server' list and a 'File and Storage Services' section. To the right, a 'Remote Desktop Connection' window is open, prompting for a computer name. The 'Computer' field contains '10.1.0.4' (highlighted in red), and the 'User name' field is 'None specified'. At the bottom, there are 'Show Options', 'Connect', and 'Help' buttons. The taskbar at the bottom shows the date and time as '12:21 AM 6/24/2023'.

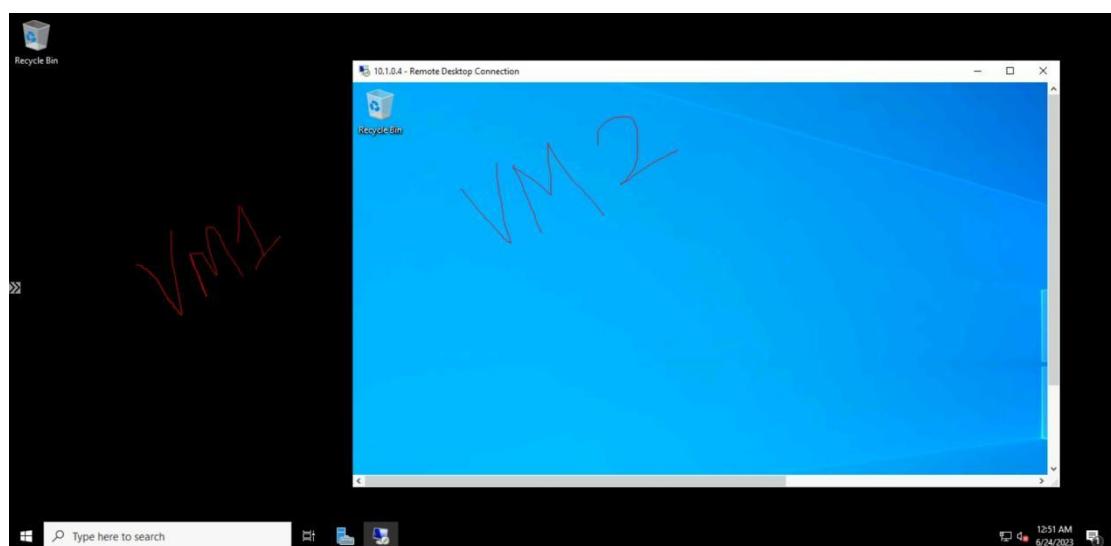
It will prompt for username and password to shows connection between the two Vnets. Input your username and Password and click Ok.



After clicking Okay, I will then click Yes to connection.



Here is my VM1 and VM2



I have successfully configured and tested the **VNet Peering**, I hope you can use the step by step to understand on how configure **VNet Peering in Azure**. The virtual network establishes the connection between two different **Virtual network Peering** (UkSouthVnet-UkWestVnet) but this depends on the condition and requirements.

References.

- [Virtual Networks In Microsoft Azure: VNet Peering,](#)
- [Microsoft Azure VNet Peering \(Microsoft Official\)](#)