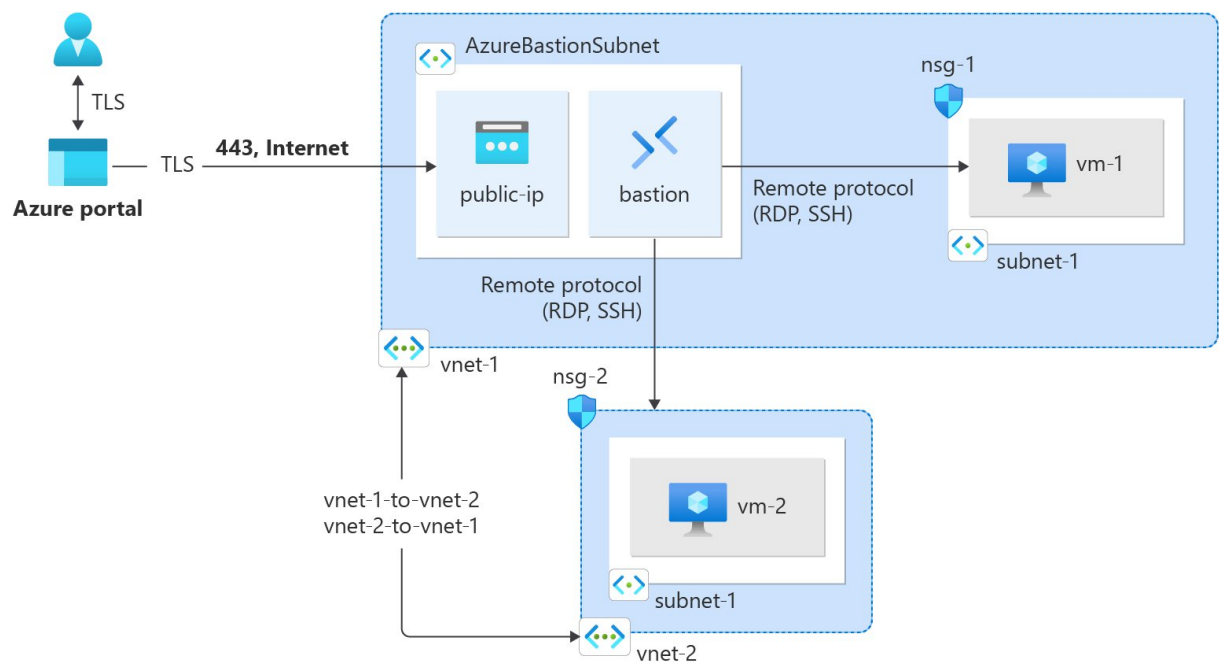


# Connect virtual networks with virtual network peering using the Azure portal

You can connect virtual networks to each other with virtual network peering. These virtual networks can be in the same region or different regions (also known as global virtual network peering). Once virtual networks are peered, resources in both virtual networks can communicate with each other over a low-latency, high-bandwidth connection using Microsoft backbone network.



In this , you learn how to:

- Create virtual networks
- Connect two virtual networks with a virtual network peering
- Deploy a virtual machine (VM) into each virtual network
- Communicate between VMs

## Prerequisites

- An Azure account with an active subscription.

# Sign in to Azure

Sign in to the Azure portal.

## Create a virtual network and an Azure Bastion host

The following procedure creates a virtual network with a resource subnet, an Azure Bastion subnet, and a Bastion host:

1. In the portal, search for and select **Virtual networks**.
2. On the **Virtual networks** page, select **+ Create**.
3. On the **Basics** tab of **Create virtual network**, enter or select the following information:

1. In the portal, search for and select Virtual networks.

[Collapse table](#)

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select <b>Create new</b> . Enter <b>test-rg</b> for the name. Select <b>OK</b> .
Instance details	
Name	Enter <b>vnet-1</b> .
Region	Select <b>East US 2</b> .

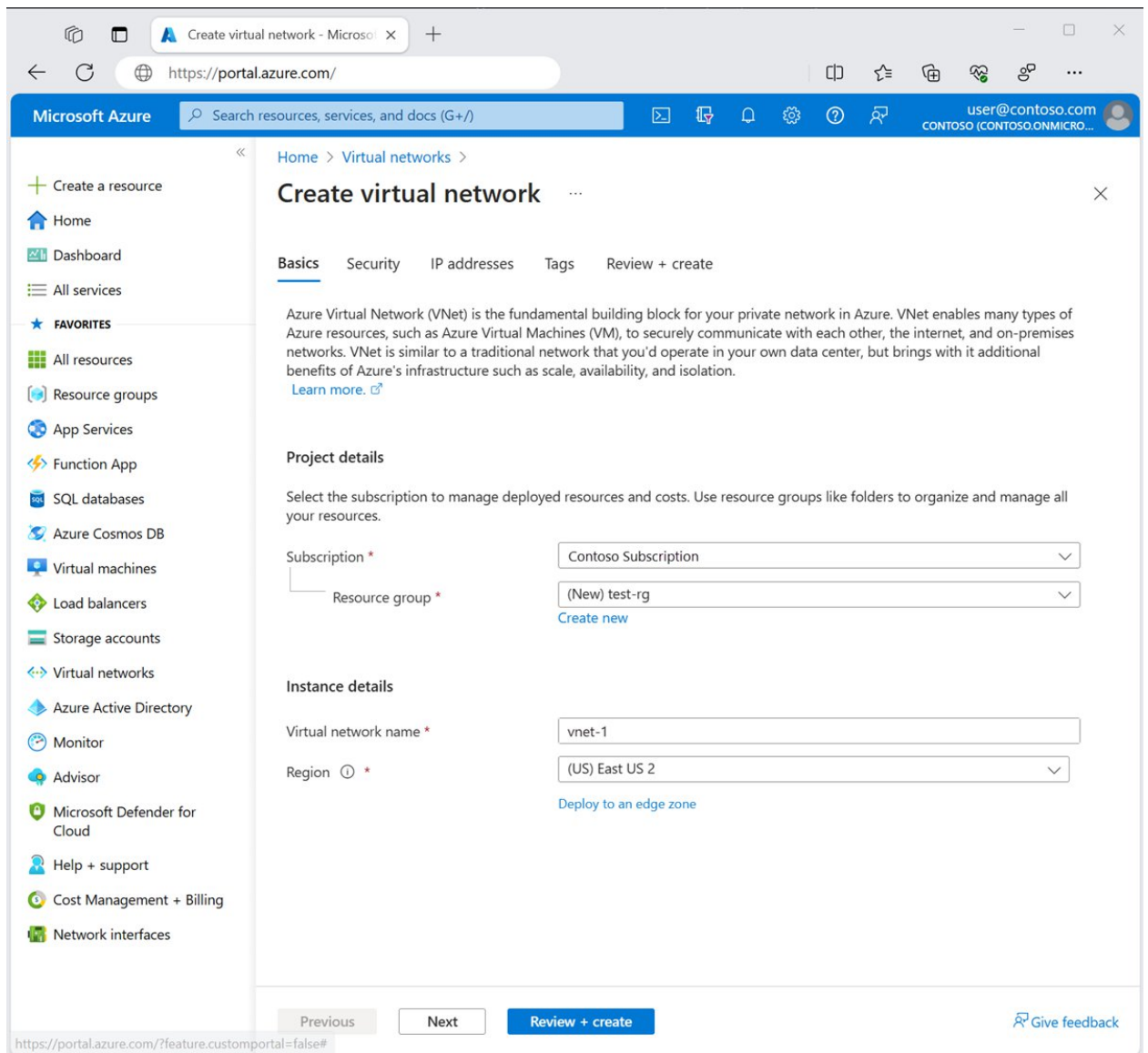
Resources

Create a resource

Home > Virtual networks > Create virtual network

peering

Learn how to create, change, or delete a virtual



4. Select **Next** to proceed to the **Security** tab.

5. In the **Azure Bastion** section, select **Enable Bastion**.

Bastion uses your browser to connect to VMs in your virtual network over Secure Shell (SSH) or Remote Desktop Protocol (RDP) by using their private IP addresses. The VMs don't need public IP addresses, client software, or special configuration. For more information

6. In **Azure Bastion**, enter or select the following information:

**Expand table**

Setting	Value
Azure Bastion host name	Enter <b>bastion</b> .
Azure Bastion public IP address	Select <b>Create a public IP address</b> . Enter <b>public-ip-bastion</b> in Name. Select <b>OK</b> .

[Home](#) > [Virtual networks](#) >

Create virtual network ...

×

Basics Security IP addresses Tags Review + create

Enhance the security of your virtual network with these additional paid security services. [Learn more](#)

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more](#)

Enable Azure Bastion ⓘ ☒

Azure Bastion host name

Azure Bastion public IP address \* 

(New) public-ip ▼

[Create a public IP address](#)

Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. [Learn more](#)

Enable Azure Firewall ⓘ ☐

Azure DDoS Network Protection

Azure DDoS Network Protection is a paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network. [Learn more](#)

Enable Azure DDoS Network Protection ⓘ ☐

Setting	Value
<b>Subnet details</b>	
Subnet template	Leave the default of <b>Default</b> .
Name	Enter <b>subnet-1</b> .
Starting address	Leave the default of <b>10.0.0.0</b> .
Subnet size	Leave the default of <b>/24 (256 addresses)</b> .

Home > Virtual networks >

## Create virtual network

Basics

Security

IP addresses

Tags

Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and sizes.

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. You can also define the address space into smaller ranges for use by your applications. When you create a virtual network, you assign the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space

10.0.0.0/16

10.0.0.0
/16

10.0.0.0 - 10.0.255.255
65,536 addresses

+ Add a subnet

Subnets	IP address range	Size
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)
AzureBastionSubnet	10.0.1.0 - 10.0.1.63	/26 (64 addresses)

Address space '10.0.0.0/16 (10.0.0.0 - 10.0.255.255)' overlaps with address space '10.0.0.0/16 (10.0.0.0 - 10.0.255.255)' of virtual network 'vnet-1'. Virtual networks with overlapping address space cannot be created. To create a virtual network, change address space '10.0.0.0/16 (10.0.0.0 - 10.0.255.255)'. [Learn more](#)

A NAT gateway is recommended for outbound internet access from subnets. Edit the virtual network to add a NAT gateway. [Learn more](#)

### Edit subnet

Subnet purpose
Default

Name \*
subnet-1

#### IPv4

Include an IPv4 address space
☒

IPv4 address range \*
10.0.0.0/16
10.0.0.0 - 10.0.255.255

Starting address \*
10.0.0.0

Size
/24 (256 addresses)

Subnet address range
10.0.0.0 - 10.0.0.255

#### IPv6

Include an IPv6 address space
☐ This virtual network has no IPv6 address ranges.

#### Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access)
☐

This setting can't be changed after the subnet is created

#### Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway
None
Create new

Network security group
None
Create new

Route table
None

Previous
Next
Review + create

Save
Cancel

10. Select **Add**.

11. Select **Review + create** at the bottom of the window. When validation passes, select **Create**.

Repeat the previous steps to create a second virtual network with the following values:

Setting	Value
Name	vnet-2
Address space	10.1.0.0/16
Resource group	test-rg
Subnet name	subnet-1
Subnet address range	10.1.0.0/24

## Create virtual network peer

Use the following steps to create a two way network peer between **vnet1** and **vnet2**.

1. In the search box at the top of the portal, enter **Virtual network**. Select **Virtual networks** in the search results.
2. Select **vnet-1**.
3. In **Settings** select **Peerings**.
4. Select **+ Add**.
5. Enter or select the following information in **Add peering**:

Setting	Value
<b>This virtual network</b>	
Peering link name	Enter <b>vnet-1-to-vnet-2</b> .
Allow 'vnet-1' to access 'vnet-2'	Leave the default of selected.
Allow 'vnet-1' to receive forwarded traffic from 'vnet-2'	Select the checkbox.
Allow gateway in 'vnet-1' to forward traffic to 'vnet-2'	Leave the default of cleared.
Enable 'vnet-1' to use 'vnet-2' remote gateway	Leave the default of cleared.
<b>Remote virtual network</b>	
Peering link name	Enter <b>vnet-2-to-vnet-1</b> .
Virtual network deployment model	Leave the default of <b>Resource Manager</b> .
Subscription	Select your subscription.
Virtual network	Select <b>vnet-2</b> .
Allow 'vnet-2' to access 'vnet-1'	Leave the default of selected.
Allow 'vnet-2' to receive forwarded traffic from 'vnet-1'	Select the checkbox.
Allow gateway in 'vnet-2' to forward traffic to 'vnet-1'	Leave the default of cleared.
Enable 'vnet-2' to use 'vnet-1's' remote gateway	Leave the default of cleared.

## Add peering ...

vnet-1

**i** For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name \*

vnet-1-to-vnet-2



- ☒ Allow 'vnet-1' to access 'vnet-2' ⓘ
- ☒ Allow 'vnet-1' to receive forwarded traffic from 'vnet-2' ⓘ
- ☐ Allow gateway in 'vnet-1' to forward traffic to 'vnet-2' ⓘ
- ☐ Enable 'vnet-1' to use 'vnet-2's' remote gateway ⓘ

Remote virtual network

Peering link name \*

vnet-2-to-vnet-1



Virtual network deployment model ⓘ

- ☒ Resource manager
- ☐ Classic
- ☐ I know my resource ID ⓘ

Subscription \* ⓘ

Azure Subscription



Virtual network \*

vnet-2



- ☒ Allow 'vnet-2' to access 'vnet-1' ⓘ
- ☒ Allow 'vnet-2' to receive forwarded traffic from 'vnet-1' ⓘ
- ☐ Allow gateway in 'vnet-2' to forward traffic to 'vnet-1' ⓘ
- ☐ Enable 'vnet-2' to use 'vnet-1's' remote gateway ⓘ

Add

1. Select **Add**.

## Create virtual machines

Create a virtual machine in each virtual network to test the communication between them.



# Create test virtual machine

The following procedure creates a test virtual machine (VM) named **vm-1** in the virtual network.

1. In the portal, search for and select **Virtual machines**.
2. In **Virtual machines**, select + **Create**, then **Azure virtual machine**.
3. On the **Basics** tab of **Create a virtual machine**, enter or select the following information:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select <b>test-rg</b> .
Instance details	
Virtual machine name	Enter <b>vm-1</b> .
Region	Select <b>East US 2</b> .
Availability options	Select <b>No infrastructure redundancy required</b> .
Security type	Leave the default of <b>Standard</b> .
Image	Select <b>Ubuntu Server 22.04 LTS - x64 Gen2</b> .
VM architecture	Leave the default of <b>x64</b> .
Size	Select a size.
Size	Select a size.
Administrator account	
Authentication type	Select <b>Password</b> .
Username	Enter <b>azureuser</b> .
Password	Enter a password.
Confirm password	Reenter the password.
Inbound port rules	
Public inbound ports	Select <b>None</b> .

4. Select the **Networking** tab at the top of the page.
5. Enter or select the following information in the **Networking** tab:

Setting	Value
<b>Network interface</b>	
Virtual network	Select <b>vnet-1</b> .
Subnet	Select <b>subnet-1 (10.0.0.0/24)</b> .
Public IP	Select <b>None</b> .
NIC network security group	Select <b>Advanced</b> .
Configure network security group	Select <b>Create new</b> . Enter <b>nsg-1</b> for the name. Leave the rest at the defaults and select <b>OK</b> .

6. Leave the rest of the settings at the defaults and select **Review + create**.

7. Review the settings and select **Create**.

Repeat the previous steps to create a second virtual machine in the second virtual network with the following values:

**Expand table**

Setting	Value
Virtual machine name	<b>vm-2</b>
Region	<b>East US 2</b> or same region as <b>vnet-2</b> .
Virtual network	Select <b>vnet-2</b> .
Subnet	Select <b>subnet-1 (10.1.0.0/24)</b> .
Public IP	<b>None</b>
Network security group name	<b>nsg-2</b>

Wait for the virtual machines to be created before continuing with the next steps.

## Connect to a virtual machine

Use ping to test the communication between the virtual machines.

1. In the portal, search for and select **Virtual machines**.
2. On the **Virtual machines** page, select **vm-1**.
3. In the **Overview** of **vm-1**, select **Connect**.
4. In the **Connect to virtual machine** page, select the **Bastion** tab.
5. Select **Use Bastion**.
6. Enter the username and password you created when you created the VM, and then select **Connect**.

## Communicate between VMs

1. At the bash prompt for **vm-1**, enter `ping -c 4 vm-2`.
2. You get a reply similar to the following message:

OUTPUT:

```
azureuser@vm-1:~$ ping -c 4 vm-2
```

```
PING vm-2.3bnkevn3313ujpr5l1kqop4n4d.cx.internal.cloudapp.net (10.1.0.4) 56(84) bytes of data.
```

```
64 bytes from vm-2.internal.cloudapp.net (10.1.0.4): icmp_seq=1 ttl=64 time=1.83 ms
```

```
64 bytes from vm-2.internal.cloudapp.net (10.1.0.4): icmp_seq=2 ttl=64 time=0.987 ms
```

```
64 bytes from vm-2.internal.cloudapp.net (10.1.0.4): icmp_seq=3 ttl=64 time=0.864 ms
```

```
64 bytes from vm-2.internal.cloudapp.net (10.1.0.4): icmp_seq=4 ttl=64 time=0.890 ms
```

3. Close the Bastion connection to **vm-1**.
4. Repeat the steps in Connect to a virtual machine to connect to **vm-2**.
5. At the bash prompt for **vm-2**, enter `ping -c 4 vm-1`.
6. You get a reply similar to the following message:

OUTPUT:

```
azureuser@vm-2:~$ ping -c 4 vm-1
```

```
PING vm-1.3bnkevn3313ujpr5l1kqop4n4d.cx.internal.cloudapp.net (10.0.0.4) 56(84) bytes of data.
```

```
64 bytes from vm-1.internal.cloudapp.net (10.0.0.4): icmp_seq=1 ttl=64 time=0.695 ms
```

```
64 bytes from vm-1.internal.cloudapp.net (10.0.0.4): icmp_seq=2 ttl=64 time=0.896 ms
```

```
64 bytes from vm-1.internal.cloudapp.net (10.0.0.4): icmp_seq=3 ttl=64 time=3.43 ms
```

```
64 bytes from vm-1.internal.cloudapp.net (10.0.0.4): icmp_seq=4 ttl=64 time=0.780 ms
```

7. Close the Bastion connection to **vm-2**.

## Clean up resources

When you finish using the resources that you created, you can delete the resource group and all its resources:

1. In the Azure portal, search for and select **Resource groups**.
2. On the **Resource groups** page, select the **test-rg** resource group.
3. On the **test-rg** page, select **Delete resource group**.
4. Enter **test-rg** in **Enter resource group name to confirm deletion**, and then select **Delete**.

## Next steps

In this , you:

- Created virtual network peering between two virtual networks.
- Tested the communication between two virtual machines over the virtual network peering with ping.