

My client wants two different network in two different region. In one network, both sub-network should have internet access. But In another network, one sub-network should have internet access other sub-network should not have internet access. Establish network connectivity between 2 different networks.

Step 1: - Create a Virtual Machine with DB server with private network.

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The 'Subscription' dropdown is set to 'Azure subscription 1'. The 'Resource group' dropdown is set to 'azure-class' with a link to 'Create new'. Under 'Instance details', the 'Virtual machine name' is 'DB-Subnet', 'Region' is '(Europe) France Central', 'Availability options' is 'No infrastructure redundancy required', 'Security type' is 'Trusted launch virtual machines' (with a link to 'Configure security features'), 'Image' is 'Windows Server 2019 Datacenter - x64 Gen2 (free services eligible)' (with links to 'See all images' and 'Configure VM generation'), and 'VM architecture' is 'x64' (with a note that 'Arm64 is not supported with the selected image'). At the bottom, there are 'Review + create' and 'Next : Disks >' buttons, and a URL 'go.microsoft.com/fwlink/?LinkId=2126834'.

Step 2: - Select Virtual network as TVS-VNET and select DB Subnet and create a virtual machine.

The screenshot shows the 'Networking' tab of the 'Create a virtual machine' wizard. It includes tabs for Basics, Disks, Networking, Management, Monitoring, Advanced, Tags, and Review + create. The Networking tab has a note about defining network connectivity through NIC settings. Under 'Network interface', the 'Virtual network' is 'TVS-Vnet' (with a link to 'Create new'), the 'Subnet' is 'DB-subnet (10.10.2.0/24)' (with a link to 'Manage subnet configuration'), 'Public IP' is 'None' (with a link to 'Create new'), 'NIC network security group' is 'Basic' (selected), and 'Public inbound ports' is 'Allow selected ports' (selected). At the bottom, there are 'Review + create' and 'Next : Management >' buttons, and a URL 'go.microsoft.com/fwlink/?LinkId=2126834'.

Step 3: - Create a Web-Server-Vnet in different Region with 2 subnet mask.

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Learn more

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 network name * Region * [Deploy to an edge zone](#)

Previous Next Review + create Give feedback

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Add IPv4 address space

/16 (65,536 addresses) Delete address space

10.0.0.0 - 10.0.255.255 (65536 addresses)

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
sub-1	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-
sub-2	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-

Previous Next Review + create Give feedback

Step 4: - Now create a virtual machine in different region (West Europe) and select web-server VNET. (Default)

Home > Virtual machines >

Create a virtual machine ...

⚠️ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

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

Subscription *

Resource group *

Instance details

Virtual machine name *

Region *

Availability options

Security type

Image *

VM architecture

Review + create

Home > Virtual machines >

Create a virtual machine ...

Network interface

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

Virtual network *

Subnet *

Public IP

NIC network security group

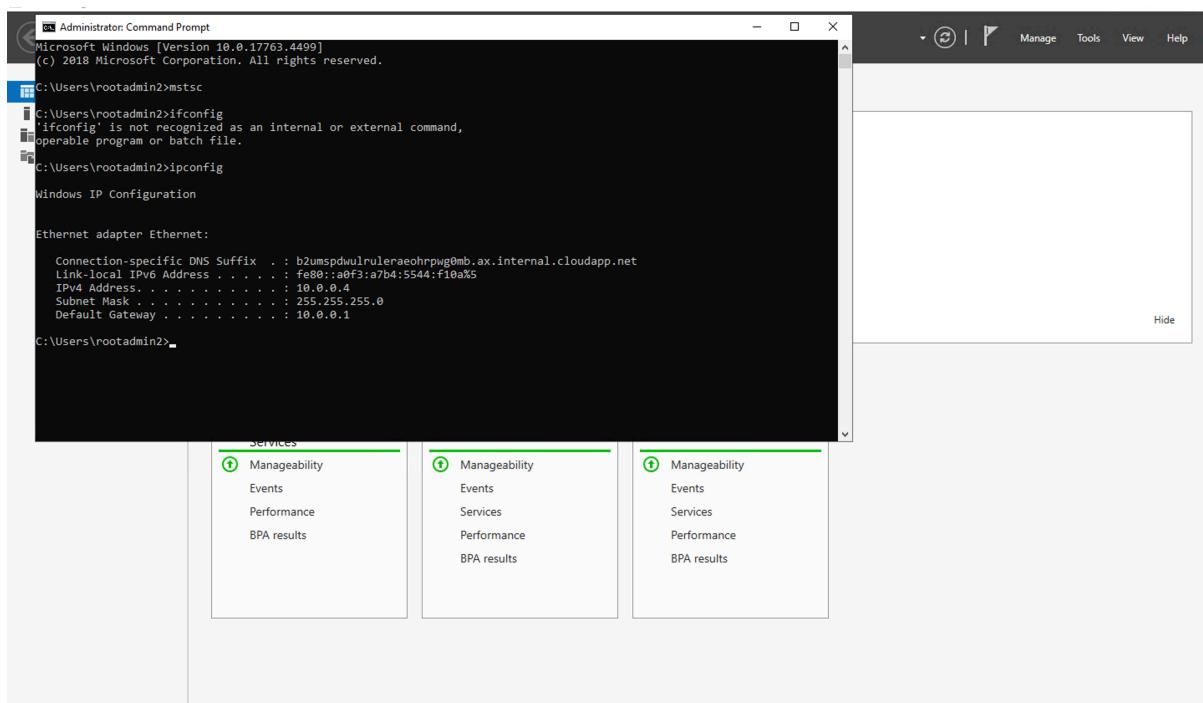
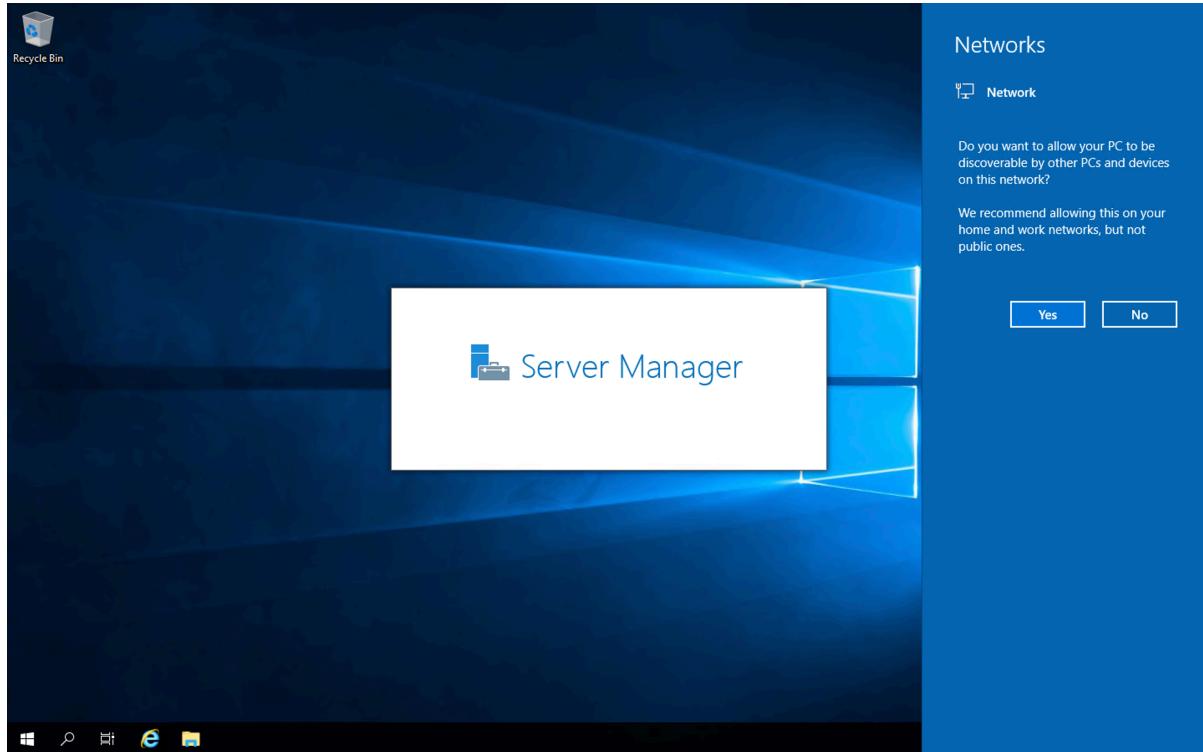
Public inbound ports *

Select inbound ports *

⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

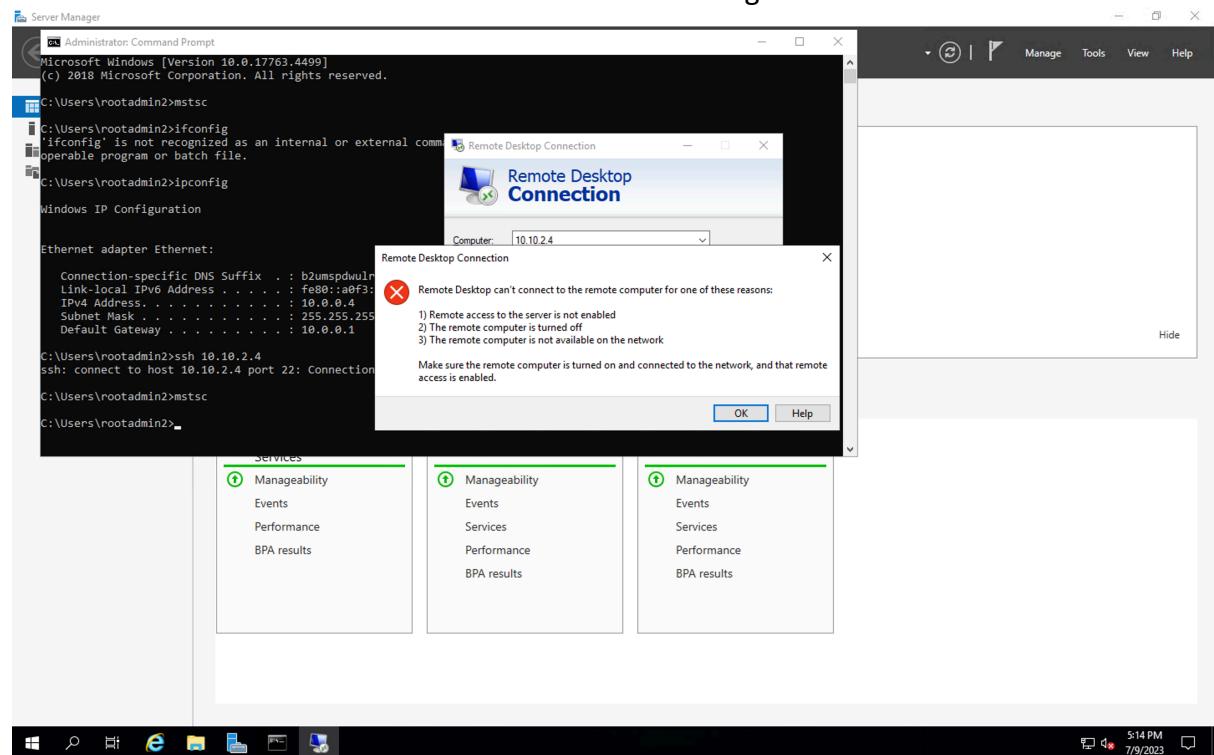
Review + create

Step 5:- Connect to a web-server VNet virtual machine using RDP and check IP using ipconfig.



Step 6:- Try Connecting DB server using Remote desktop in web-server-vnet virtual machine.

Note:- You will not be able to connect due to different region.



Step 7: - Create a VPC Peering

Go to TVS-VNET and select peering option.

Type Peering link name: - tvs -vnet

Remote Virtual network Peering link name: - webserver-vnet

Subscription

Virtual Network: - Web-Server-Vnet and click on add.

The screenshot shows the Azure portal interface for managing virtual networks. The current view is 'Peering' for the 'tvs-vnet'. Key settings visible include:

- Peering link name:** tvs -vnet
- Peering status:** Fully Synchronized
- Peering state:** Succeeded
- Traffic to remote virtual network:** Allow (default) is selected.
- Traffic forwarded from remote virtual network:** Allow (default) is selected.
- Virtual network gateway or Route Server:** None (default) is selected.
- Remote virtual network:** Remote Vnet Id is listed.

At the bottom, there are 'Save' and 'Cancel' buttons.

Step 8: - Now try connecting to DB server using Remote desktop.

