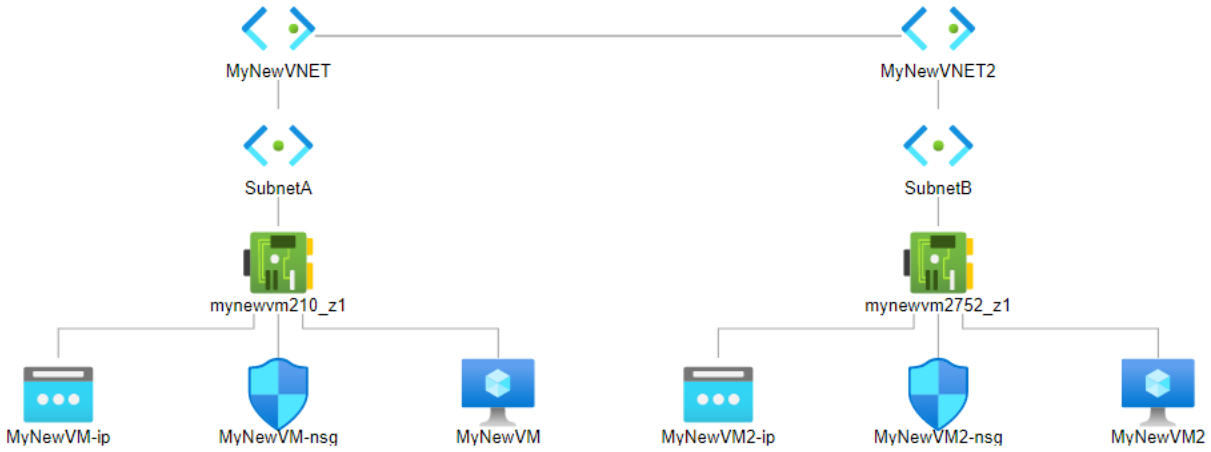
Your company has its data centers in the East US offices connected via mesh wide-area network links, with full connectivity between them. You need to implement a lab environment that will reflect the topology of your company's on-premises networks and verify its functionality. I would like you to create and test the following:

- **Provision the lab environment**
- **Configure local virtual network peering**
- **Test intersite connectivity**
- **Secure the virtual network with an NSG**

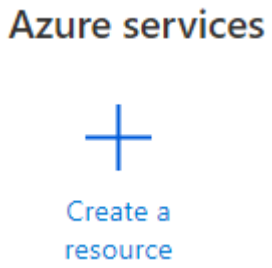
The network overview of the to-be-created lab:



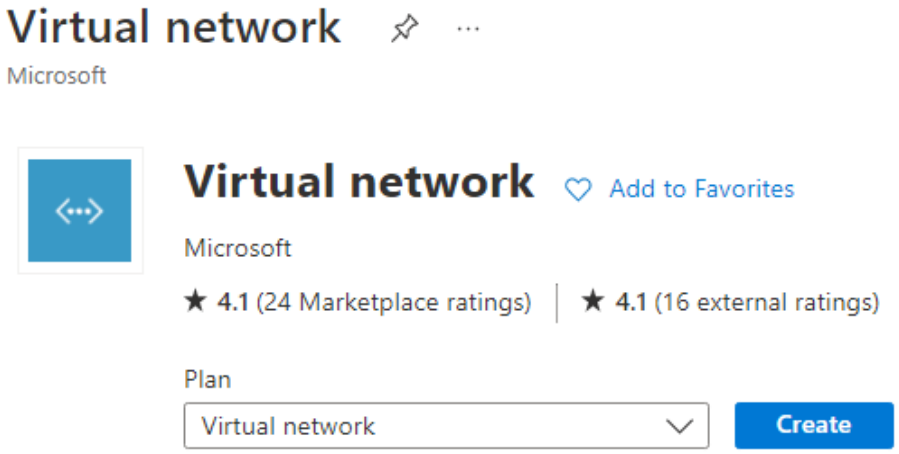
Tasks

1. Provision the lab environment

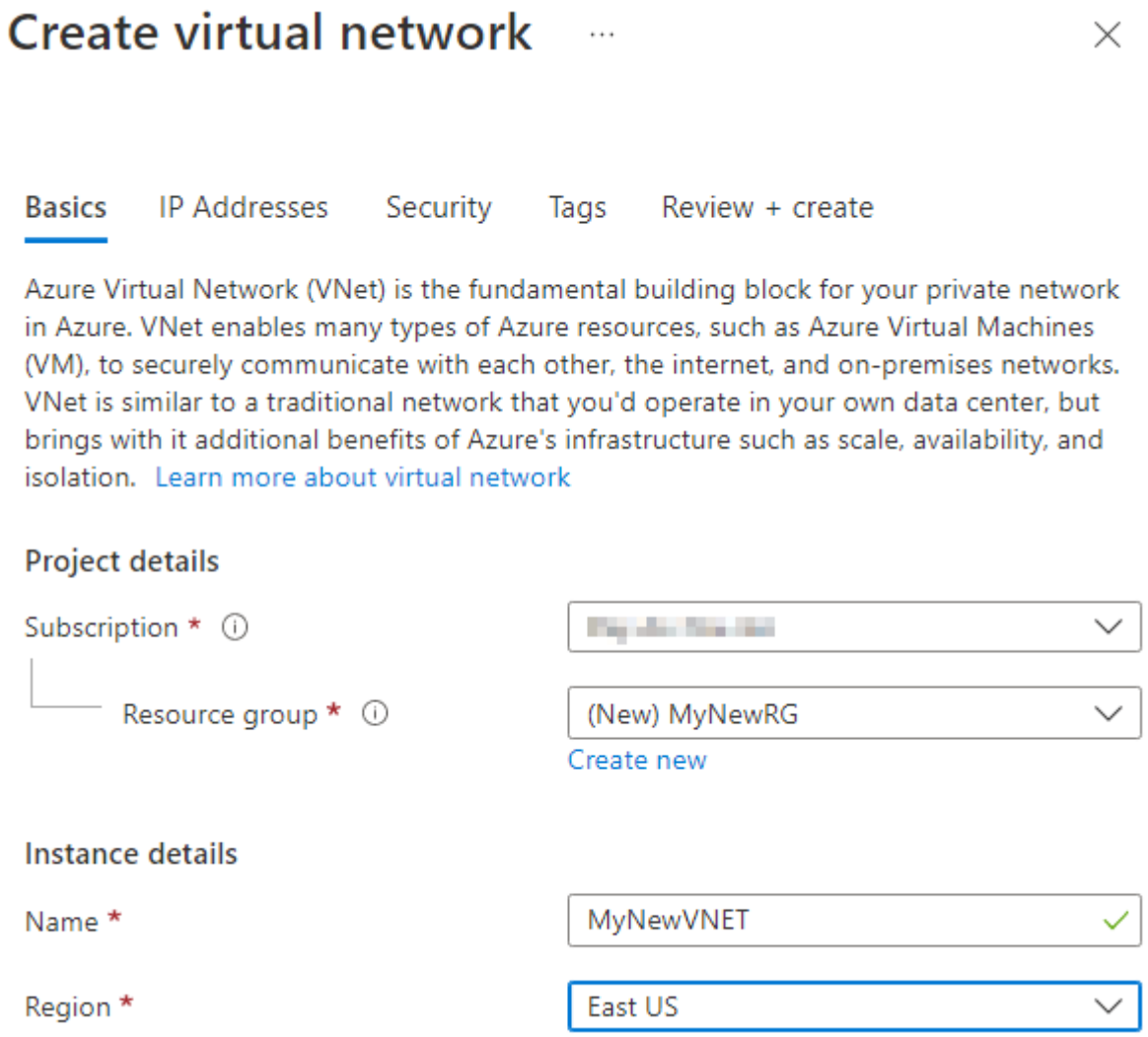
1. From the Azure Portal, click on **Create** a resource button:



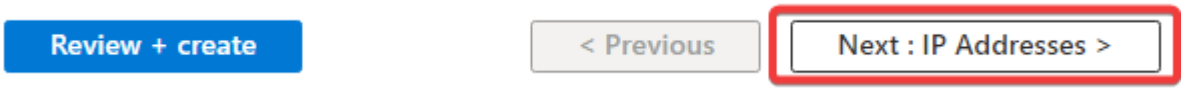
2. In the search box, enter **Virtual Network**:



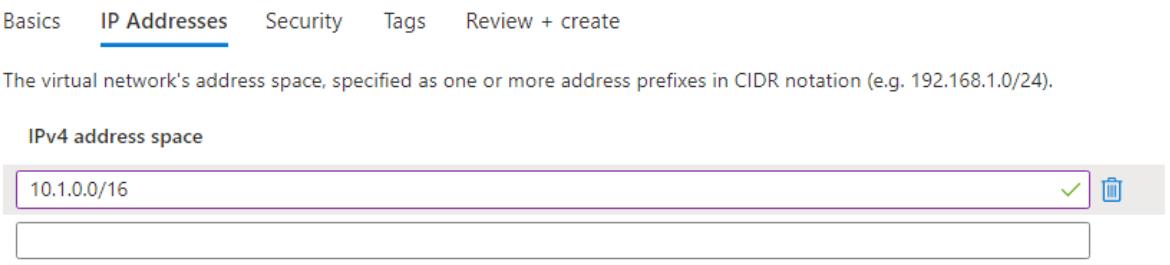
3. Select **Create** and enter the following values in the **Basics tab**:
   - Resource group : **MyNewRG**
   - Instance details:
     - Virtual Network Name: **MyNewVNET**
     - Region: **East US**



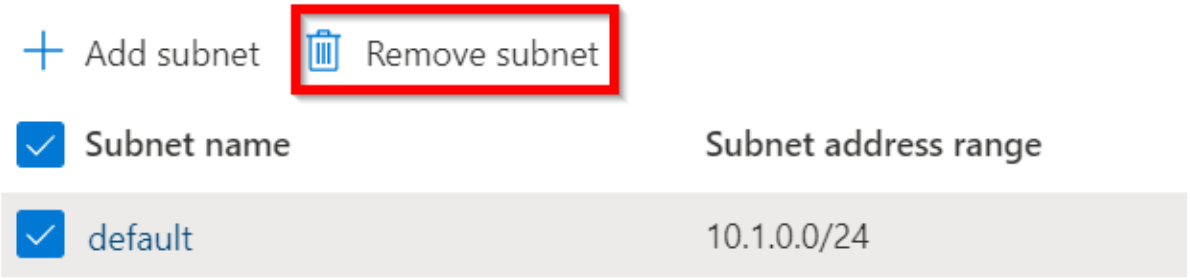
4. Click on the **Next: IP Addresses** button:



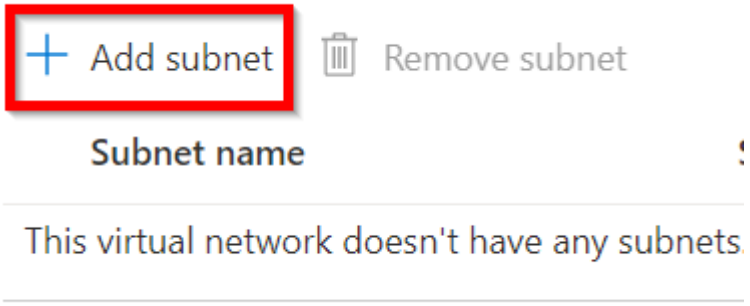
5. Enter or select the following details:
    - IPv4 address space: **10.1.0.0/16**



6. Check the box on the left of the **default** subnet, and click on the **Remove Subnet** button:

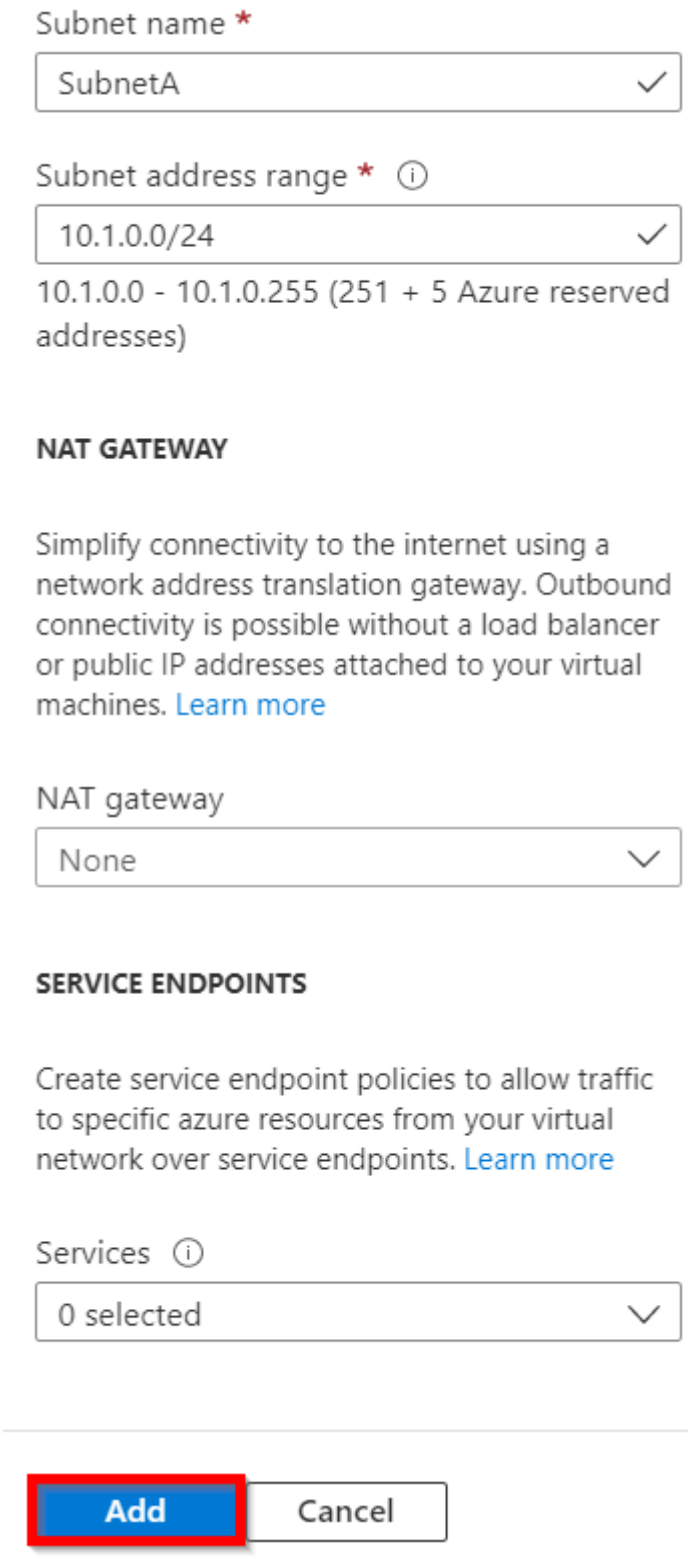


7. Click on the **+Add Subnet** button:

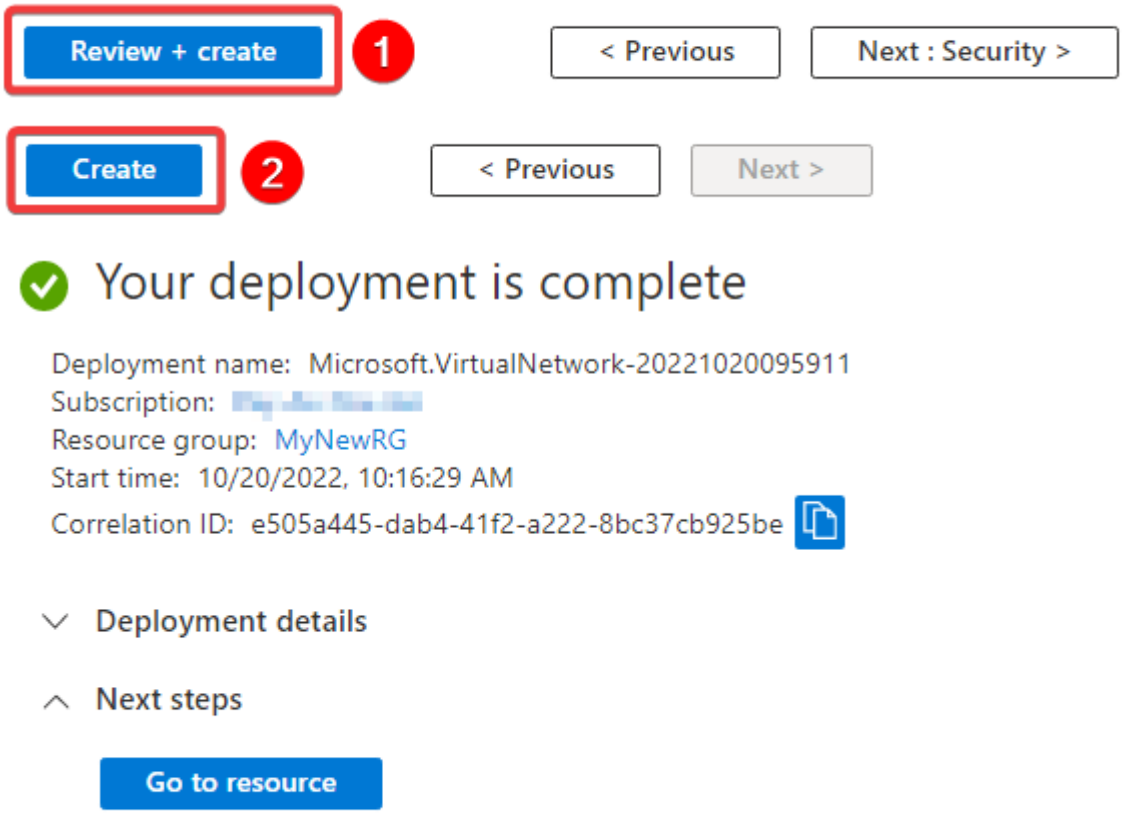


8. On the Add Subnet page, enter the following details and click on **Add**:

   Subnet Name: Subnet A
   Subnet Address range: 10.1.0.0/24
   NAT gateway: Leave the defaults
   Service gateway: Leave the defaults



9. Click on **Review + Create** and then click on **Create**:



10. Repeat steps 1-9 to create the second Virtual Network with the following details:
    - Basics tab
        - Resource group: **MyNewRG**
        - Instance details:
            - Virtual Network Name: **MyNewVNET2**
            - Region: **East US**
    - IP Addresses tab
        - IPv4 address space: **10.2.0.0/16**
        - Subnet details:
            - Subnet Name: **SubnetB**
            - Subnet Address range: **10.2.0.0/24**
            - NAT gateway: Leave the defaults
            - Service gateway: Leave the defaults

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription * [redacted]

Resource group * MyNewRG

Create new

Instance details

Name * MyNewVNET2

Region * East US

Basics IP Addresses Security Tags Review + create

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

IPv4 address space

10.2.0.0/16 1

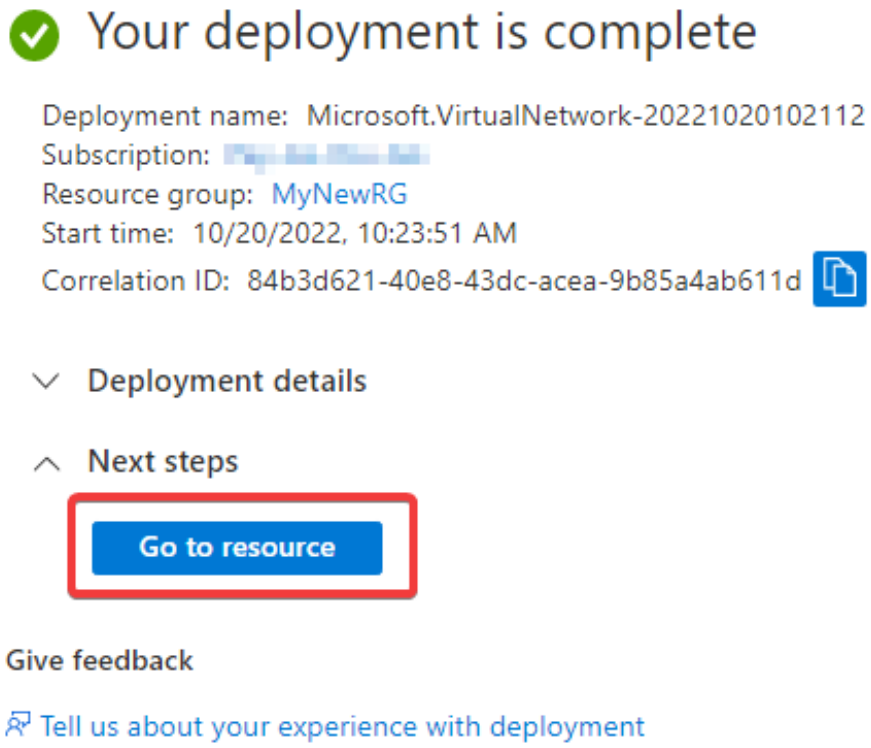
Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

Add subnet Remove subnet

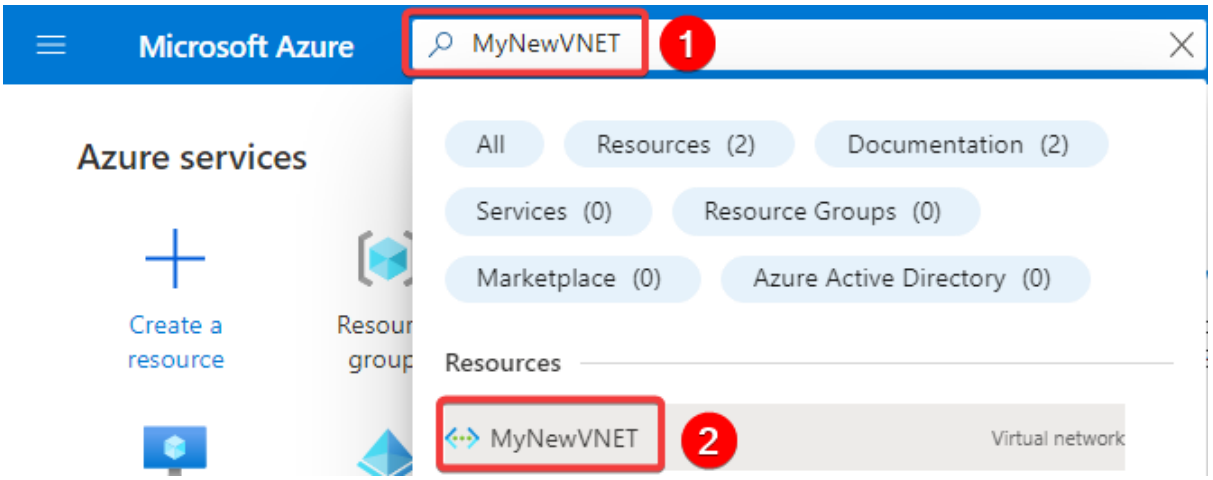
Subnet name	Subnet address range	NAT gateway
SubnetB	10.2.0.0/24 2	-

11. Click on **Go to resource**:

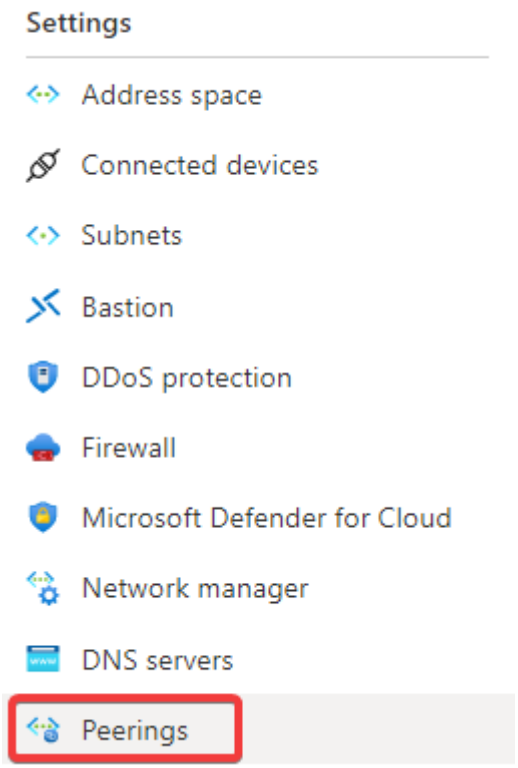


2. Peer the Virtual Networks

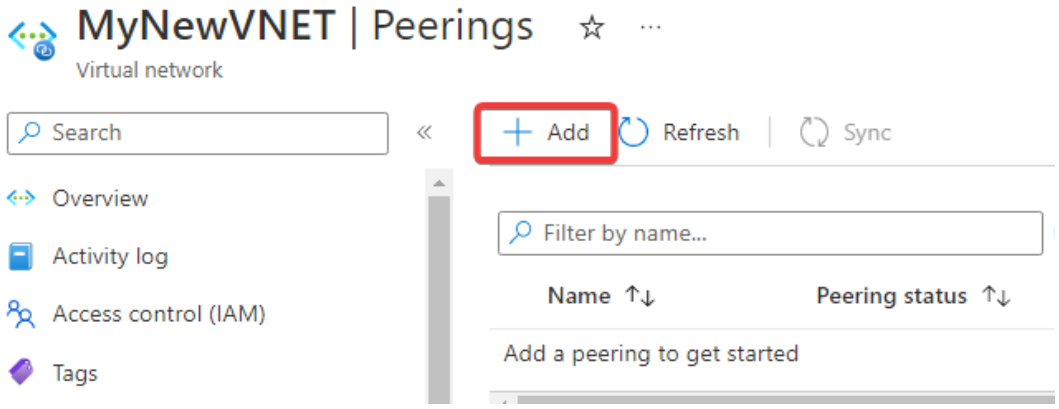
1. In the search box at the top of the Azure Portal, search for **MyNewVNET** and select it from the list:



2. From the left menu, scroll down under the **Settings** section and click on **Peerings**:

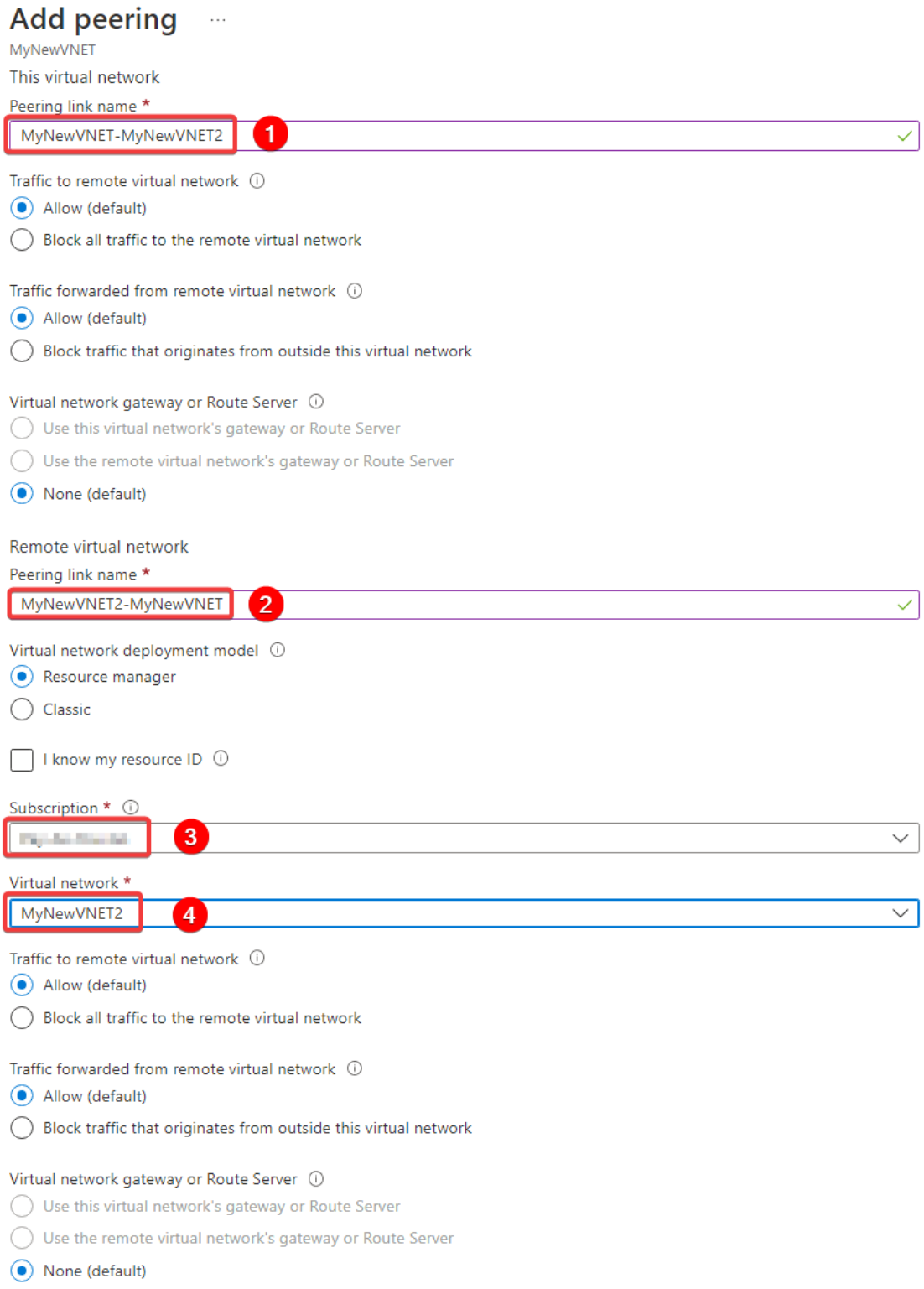


3. Click on the **+Add** button:



4. Enter or select the following details and click on **Add**:

    - This Virtual Network:
        - Peering Link Name: **MyNewVNET-MyNewVNET2**
    - Remote Virtual Network:
        - Peering Link Name: **MyNewVNET2-MyNewVNET**
    - Subscription: **Your Subscription**
    - Virtual Network: **MyNewVNET2**

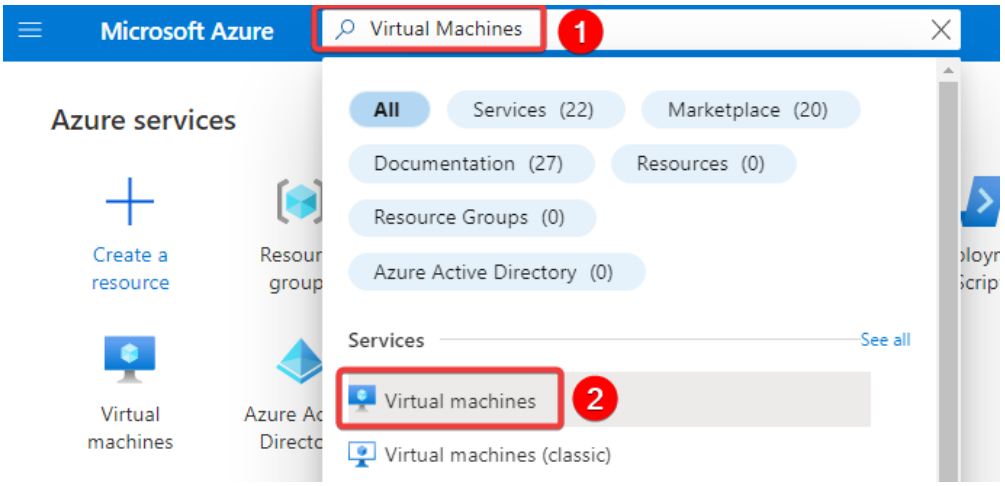


5. Both the VNets are now peered as the Peering Status shows **Connected**:

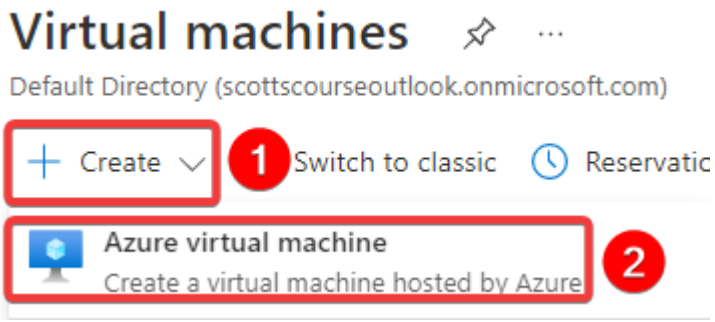
Name	Peering status	Peer	Gateway transit
MyNewVNET-MyNewVN···	Connected	MyNewVNET2	Disabled

3. Creating Virtual Machines

1. In the search box at the top of the Azure Portal, search for **Virtual Machines** and select it from the list:



2. Click on the **+Create** button and select **Azure Virtual Machine**:



3. On the **Basics** tab, enter or select the following details:
   - Resource group: MyNewRG
   - Instance details:
     - Virtual Machine Name: **MyNewVM**
     - Region: **East US**
     - Image: **Windows Server 2019 Datacenter - Gen2**
     - Azure Spot instance: **Leave the default (unchecked)**
     - Size: **Standard_B2s**
   - Administrator Account:
     - Username: **VM1**
     - Password: Enter a password
     - Confirm password: Re-enter password
   - Inbound Port rules:
     - Public inbound ports: **Allow selected ports**
     - Select inbound ports: **RDP (3389)**

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. 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 * [redacted]

Resource group * MyNewRG

Create new

Instance details

Virtual machine name * MyNewVM

Region * (US) East US

Availability options Availability zone

Availability zone * Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type Standard

Image * Windows Server 2019 Datacenter - Gen2

See all images | Configure VM generation

VM architecture
- Arm64
- x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * Standard_B2s - 2 vcpus, 4 GiB memory ($36.21/month)

See all sizes

Administrator account

Username * VM1

Password * ••••••••••••

Confirm password * ••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *
- None
- Allow selected ports

Select inbound ports * RDP (3389)

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.

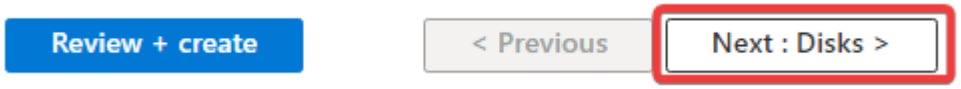
Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

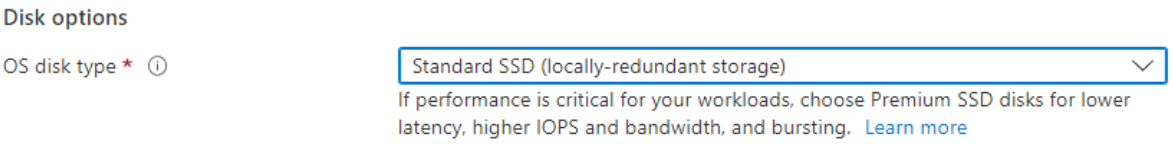
Would you like to use an existing Windows Server license? *

Review Azure hybrid benefit compliance

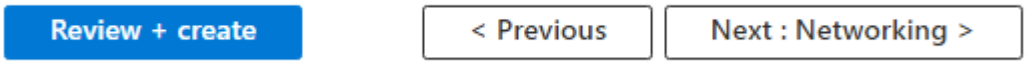
4. Click on the **Next: Disks** button:



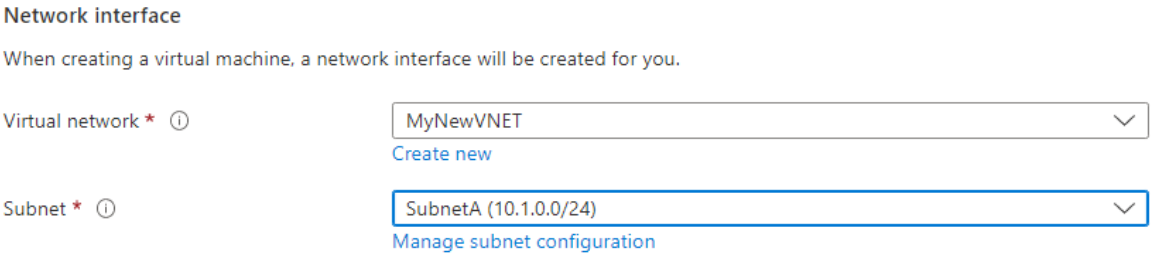
5. Select the following:



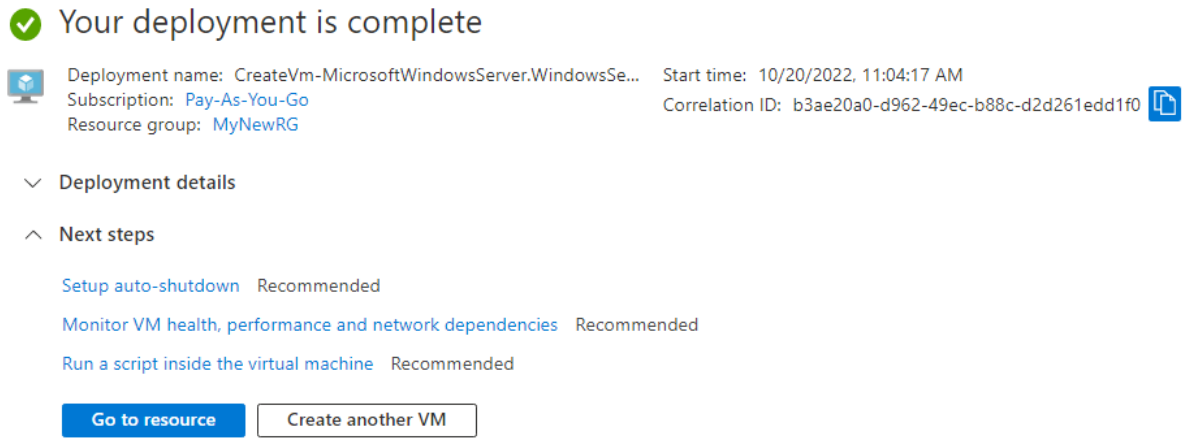
6. Click on the **Next: Networking** button:



7. Select following details.
    - Network Interface:
        - Virtual Network: **MyNewVNET**
        - Subnet: **SubnetA**



8. Click on the **Review + Create** button and then select **Create**:



9. Repeat steps 1 - 8 and enter or select the following details.

- Basics tab:
    - Resource group: **MyNewRG**
    - Instance details:
        - Virtual Machine Name: **MyNewVM2**
        - Region: **East US**
        - Image: **Windows Server 2019 Datacenter - Gen2**
        - Azure Spot instance: Leave the default (unchecked).
        - Size: **Standard_B2s**
    - Administrator Account:
        - Username: **VM2**
        - Password: Enter a password
        - Confirm password: Re-enter password
    - Inbound Port rules:
        - Public inbound ports: **None**
- Disks tab:
    - OS disk type: **Standard SSD**
- Networking tab:
    - Network Interface:
        - Virtual Network: **MyNewVNET2**
        - Subnet: **SubnetB**

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. 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 * [redacted]

Resource group * MyNewRG

Create new

Instance details

Virtual machine name * MyNewVM2

Region * (US) East US

Availability options Availability zone

Availability zone * Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type Standard

Image * Windows Server 2019 Datacenter - Gen2

See all images | Configure VM generation

VM architecture
- Arm64
- x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * Standard_B2s - 2 vcpus, 4 GiB memory ($36.21/month)

See all sizes

Administrator account

Username * VM2

Password * ••••••••••••

Confirm password * ••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *
- None
- Allow selected ports

Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Would you like to use an existing Windows Server license? *

Review Azure hybrid benefit compliance

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * ⓘ

Standard SSD (locally-redundant storage)

If performance is critical for your workloads, choose Premium SSD disks for lower latency, higher IOPS and bandwidth, and bursting. Learn more

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 * ⓘ

MyNewVNET2

Create new

Subnet * ⓘ

SubnetB (10.2.0.0/24)

Manage subnet configuration

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsSe...
Subscription: [redacted]
Resource group: MyNewRG

Start time: 10/20/2022, 11:17:47 AM
Correlation ID: 44975f5c-1f1a-483d-81b4-a53aba7248d0

Deployment details

Next steps

Setup auto-shutdown Recommended

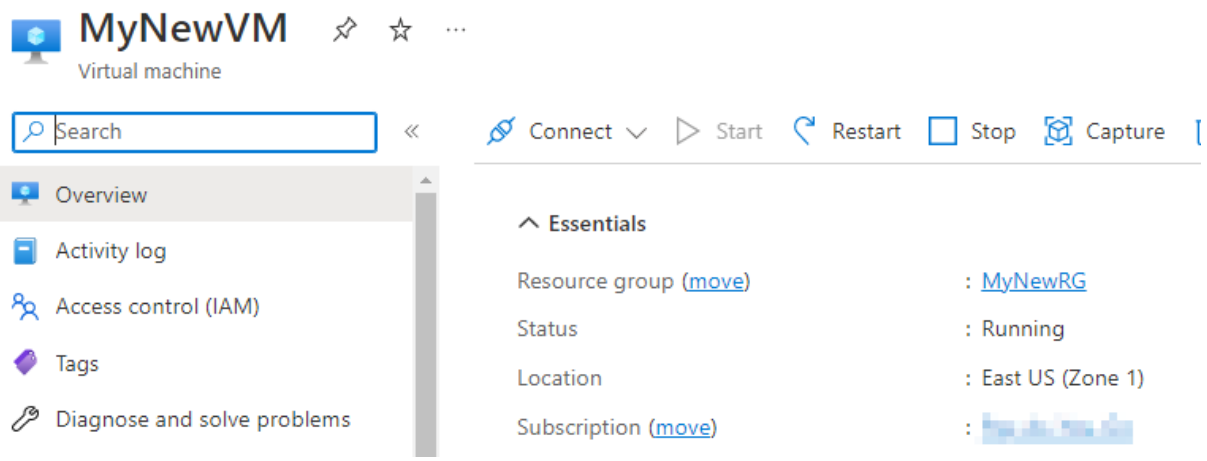
Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

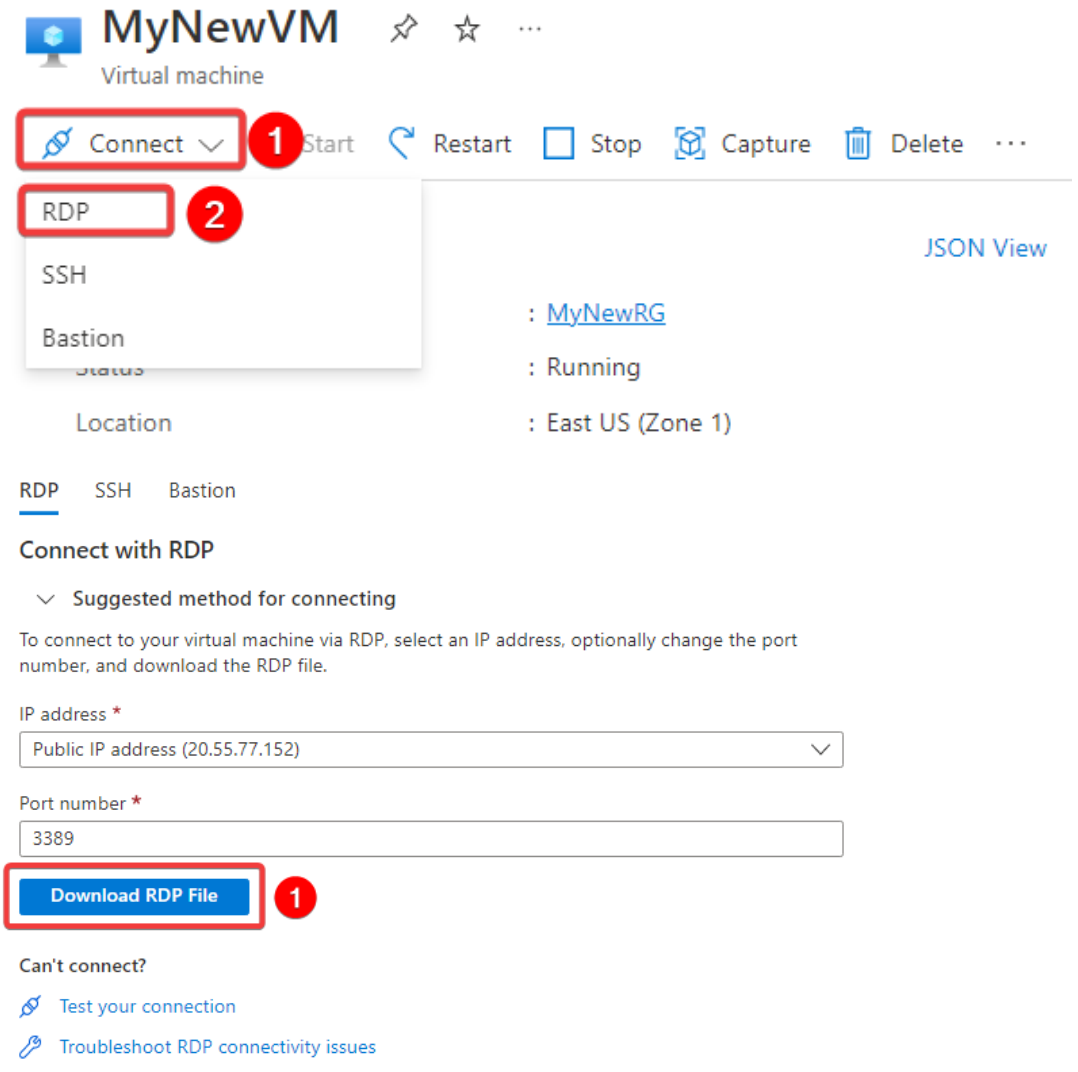
Go to resource | Create another VM

4. Establish communication between Virtual Machines

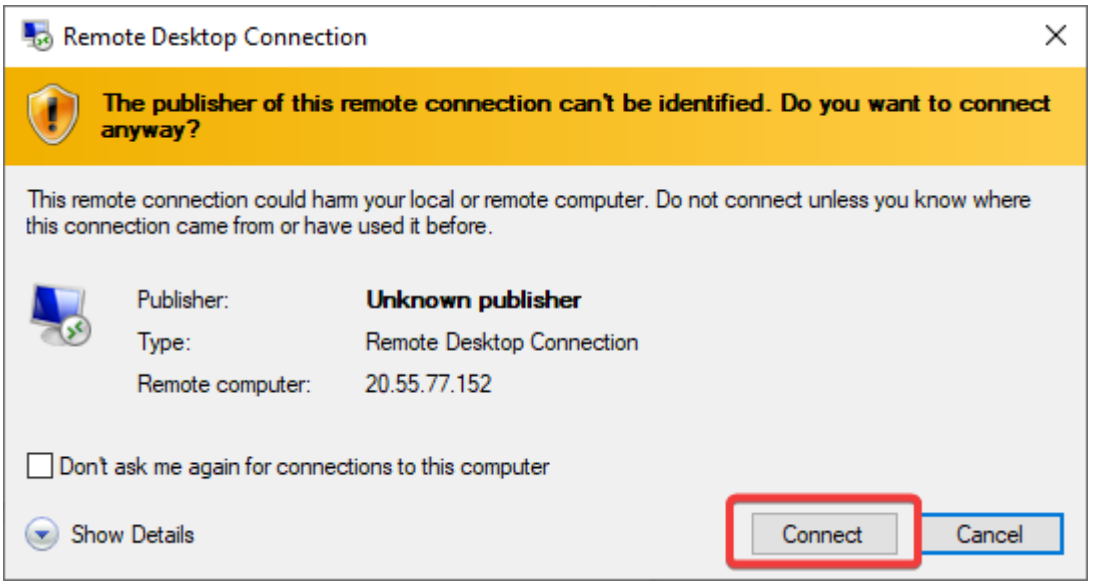
1. In the search box at the top of the Azure Portal, search for **Virtual Machines** and select **MyNewVM** from the list:



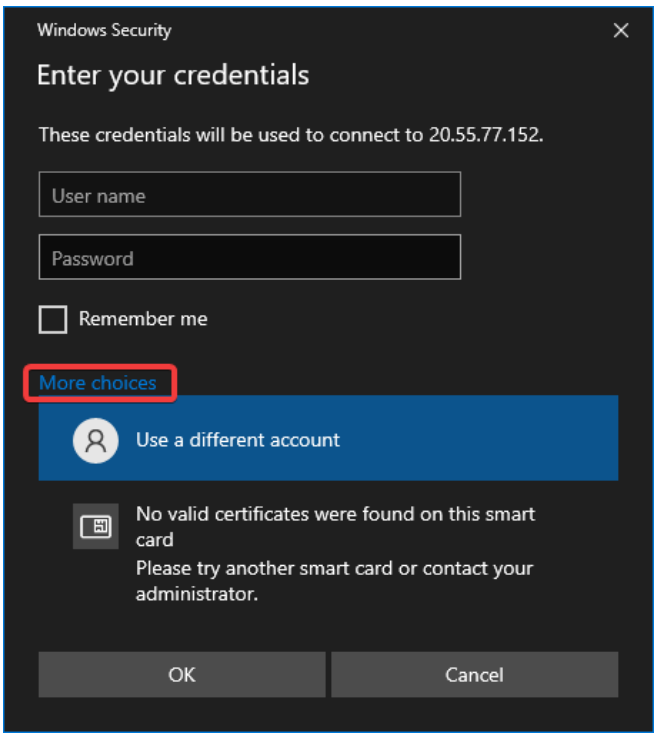
2. To connect to the virtual machine, select **Connect** and then select **RDP** from the dropdown list. Select **Download RDP File** to download the remote desktop file:



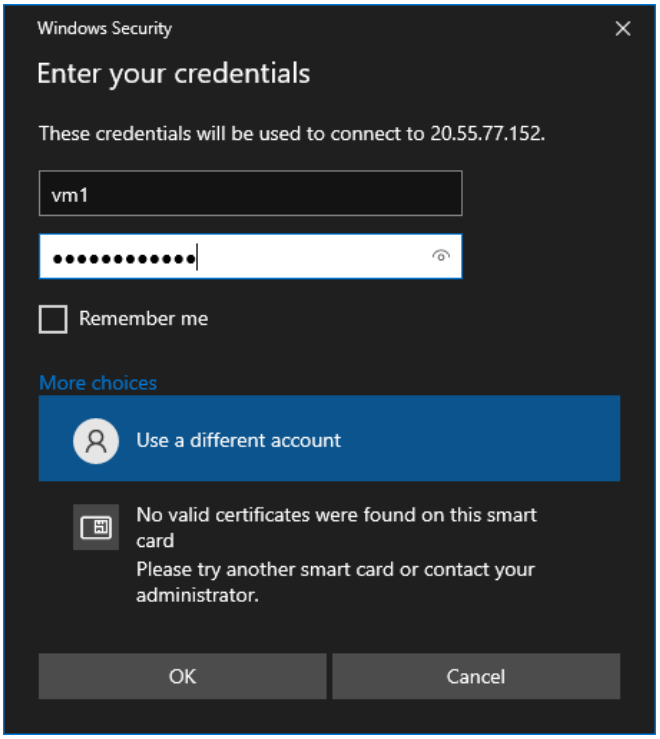
3. Open the download **RDP** file and select **Connect** on the displayed prompt:



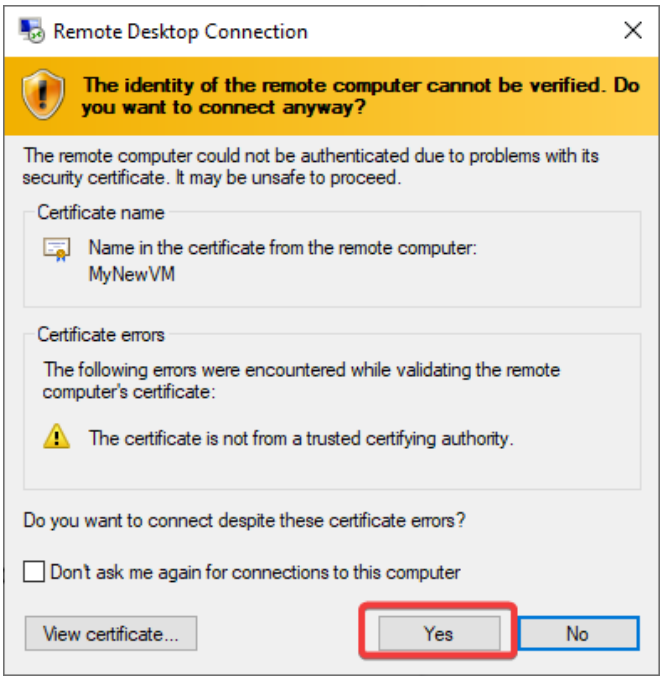
4. On the **Windows Security** prompt, click on **More choices**:



5. Click on **Use a different account** and enter the username and password you specified while creating the Virtual Machine and click **OK**:

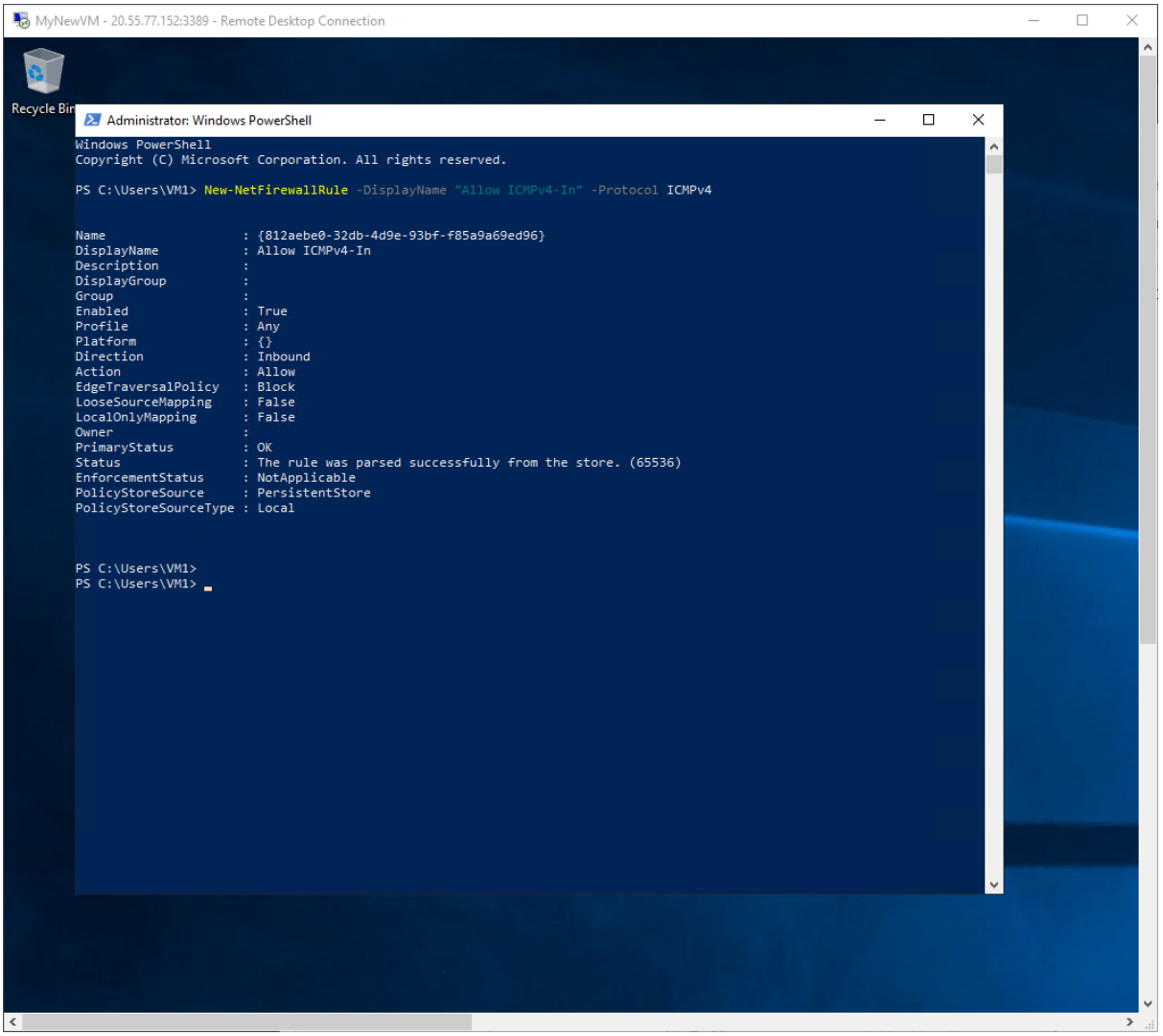


6. You may receive a certificate warning during the sign-in process. Click **Yes** to continue:

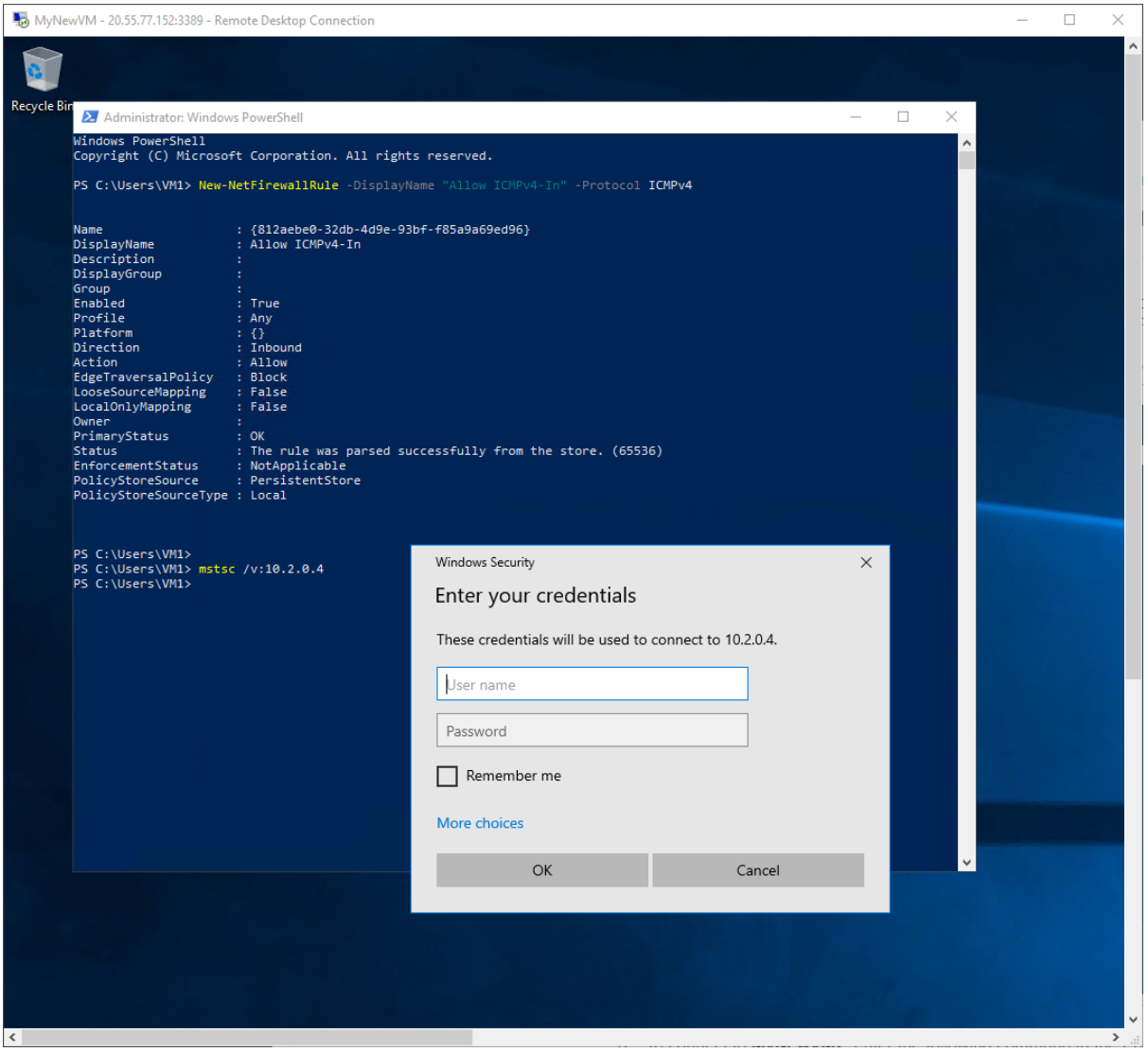


7. In the VM, open Powershell and enter the below command to enable Internet Control Message Protocol (ICMP), which is denied through the Windows Firewall by default:

    - New-NetFirewallRule –DisplayName "Allow ICMPv4-In" –Protocol ICMPv4

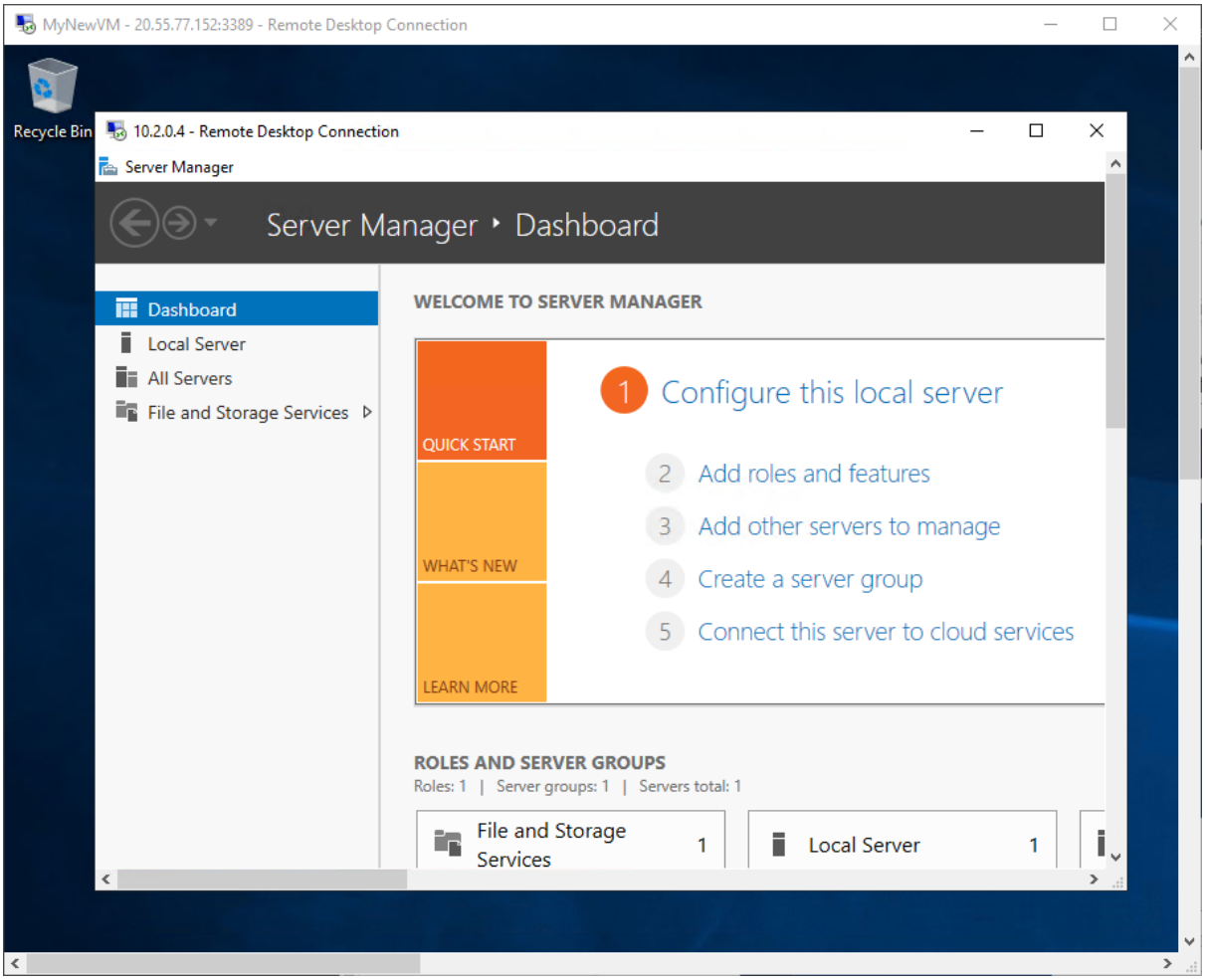


8. To connect to **MyNewVM2**, enter the following command in the Powershell window on **MyNewVM** and enter the credentials of **MyNewVM2** on the login prompt:



9. You have successfully logged into **MyNewVM2** from **MyNewVM**:

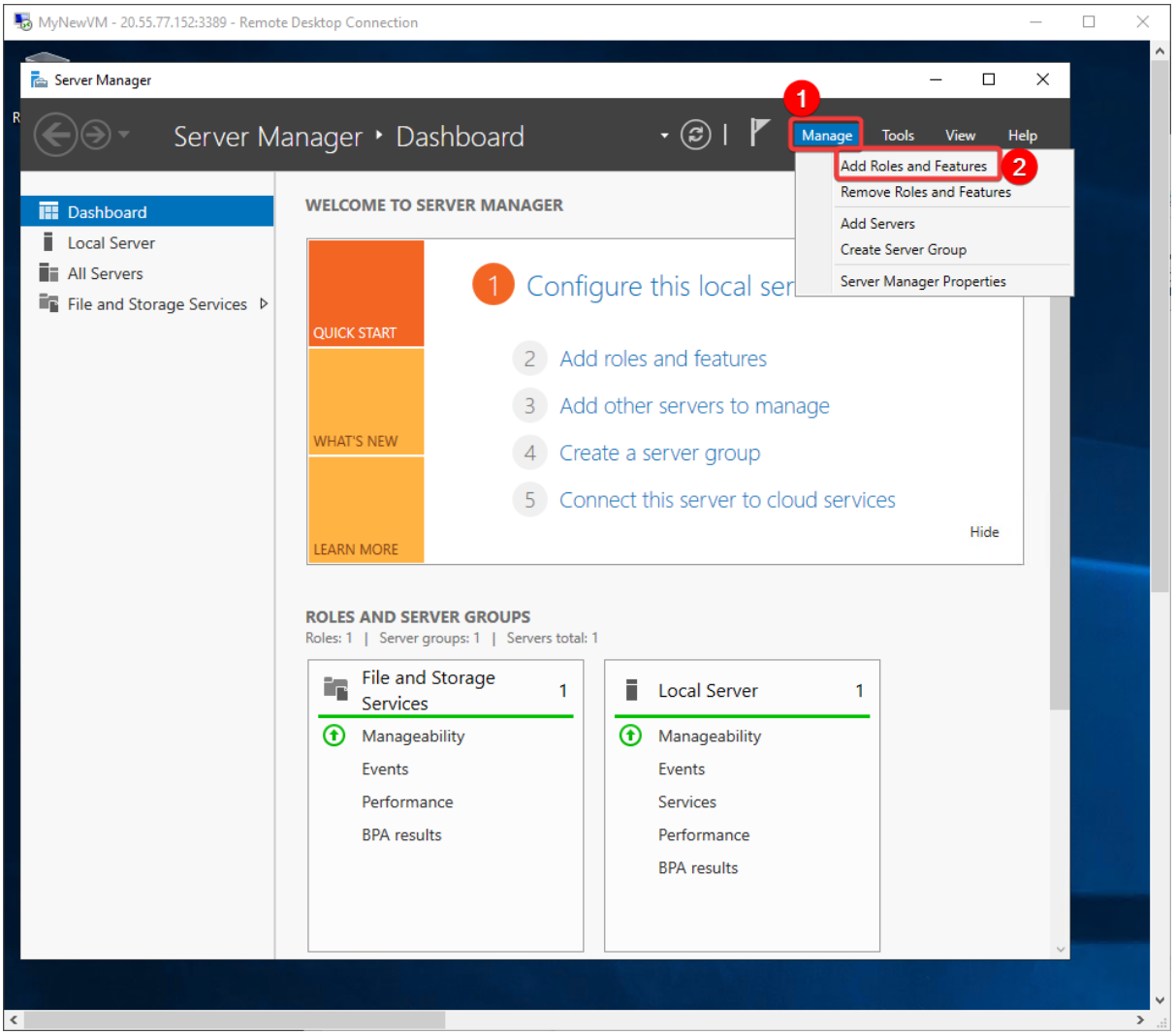
.



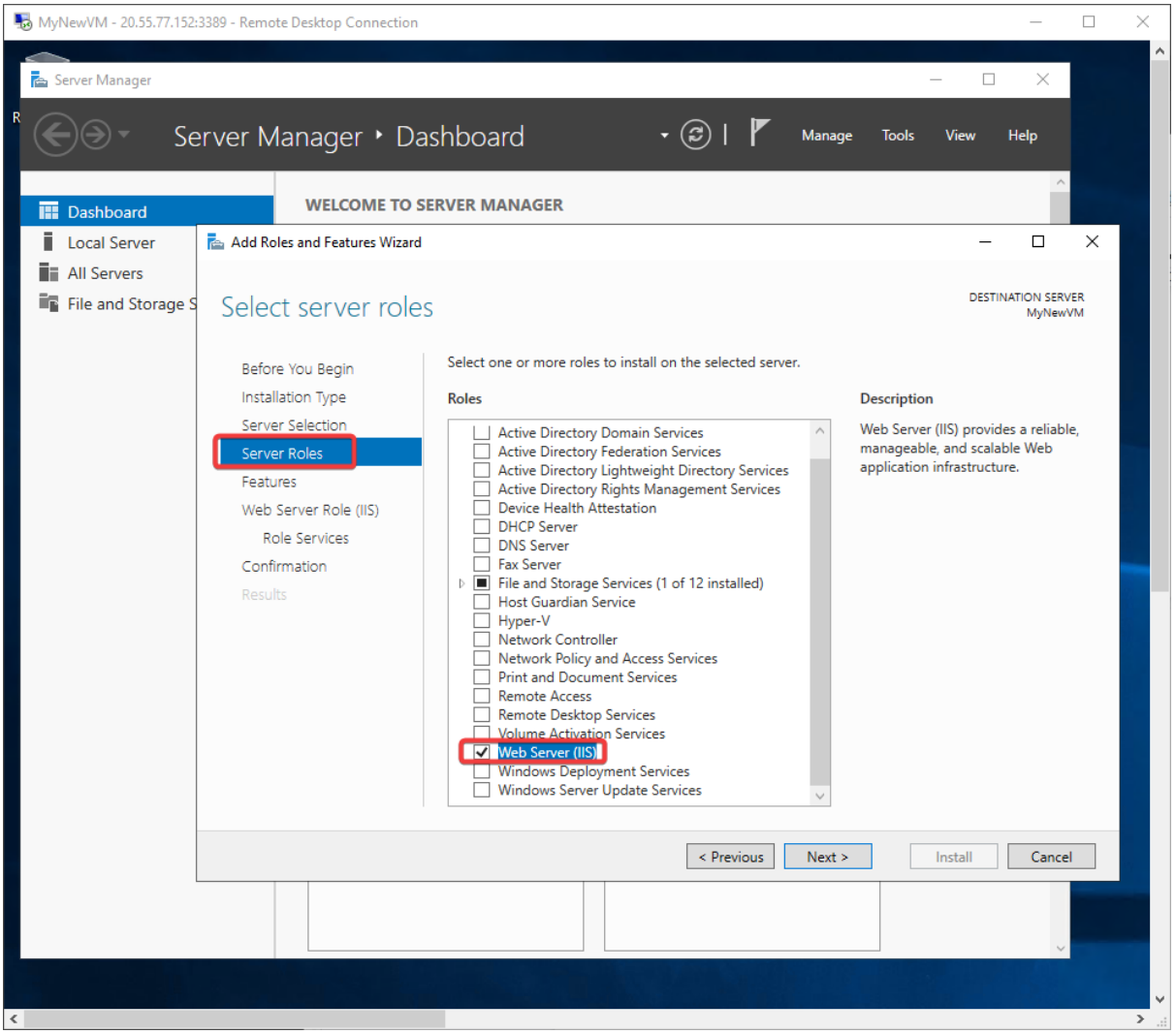
5. Secure virtual network with an NSG

You should be able to browser to your internal website for development purposes. Install IIS on MyNewVM and make sure you can navigate to the website from outside your office network.

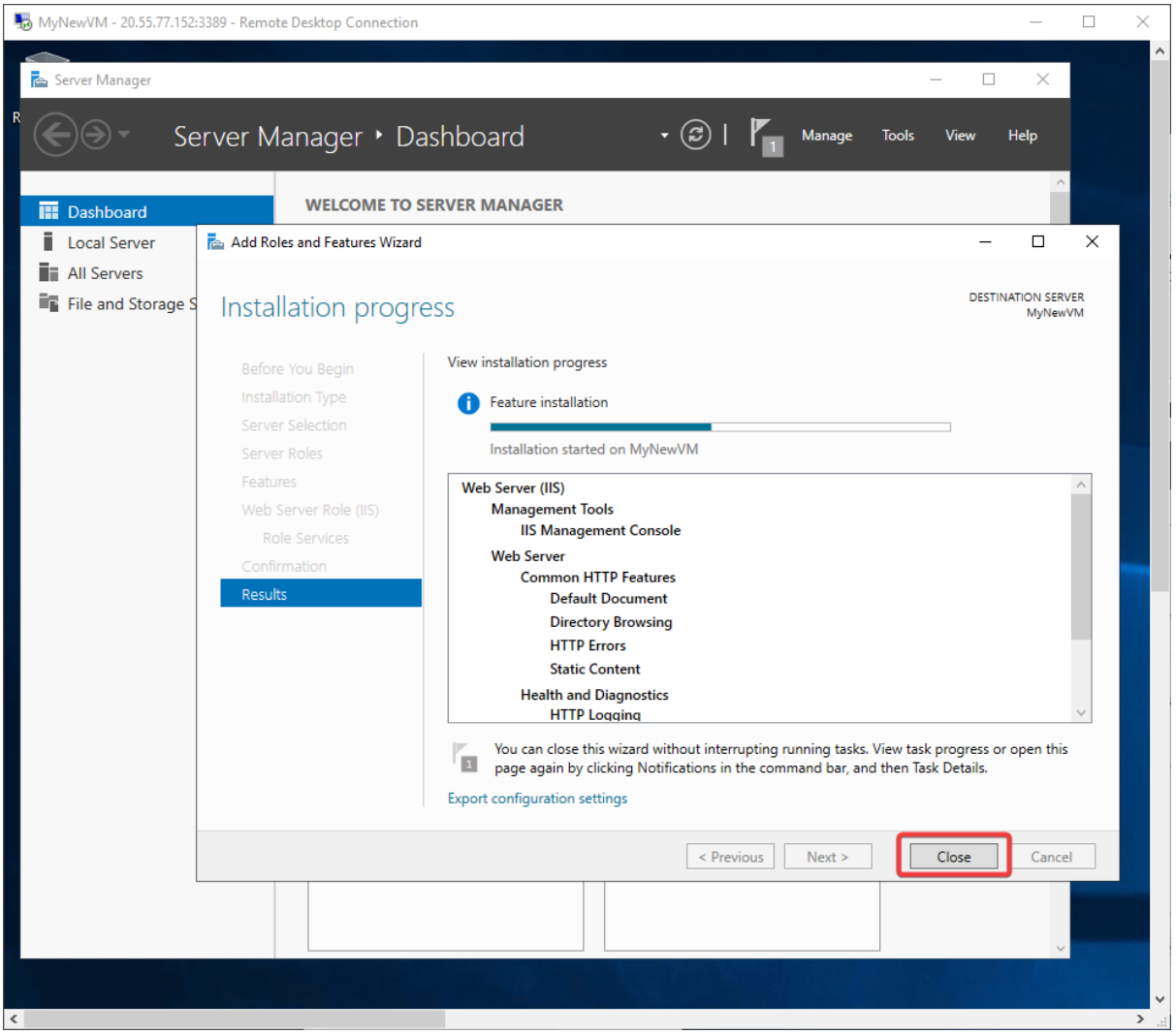
1. In **MyNewVM**, open the **Server Manager** and click on **Add Roles and Features**. You will install a web server on this particular machine. By adding a network security group rule you'll allow traffic to flow into this virtual machine on Port 80 so that you and the colleagues can access the web server:



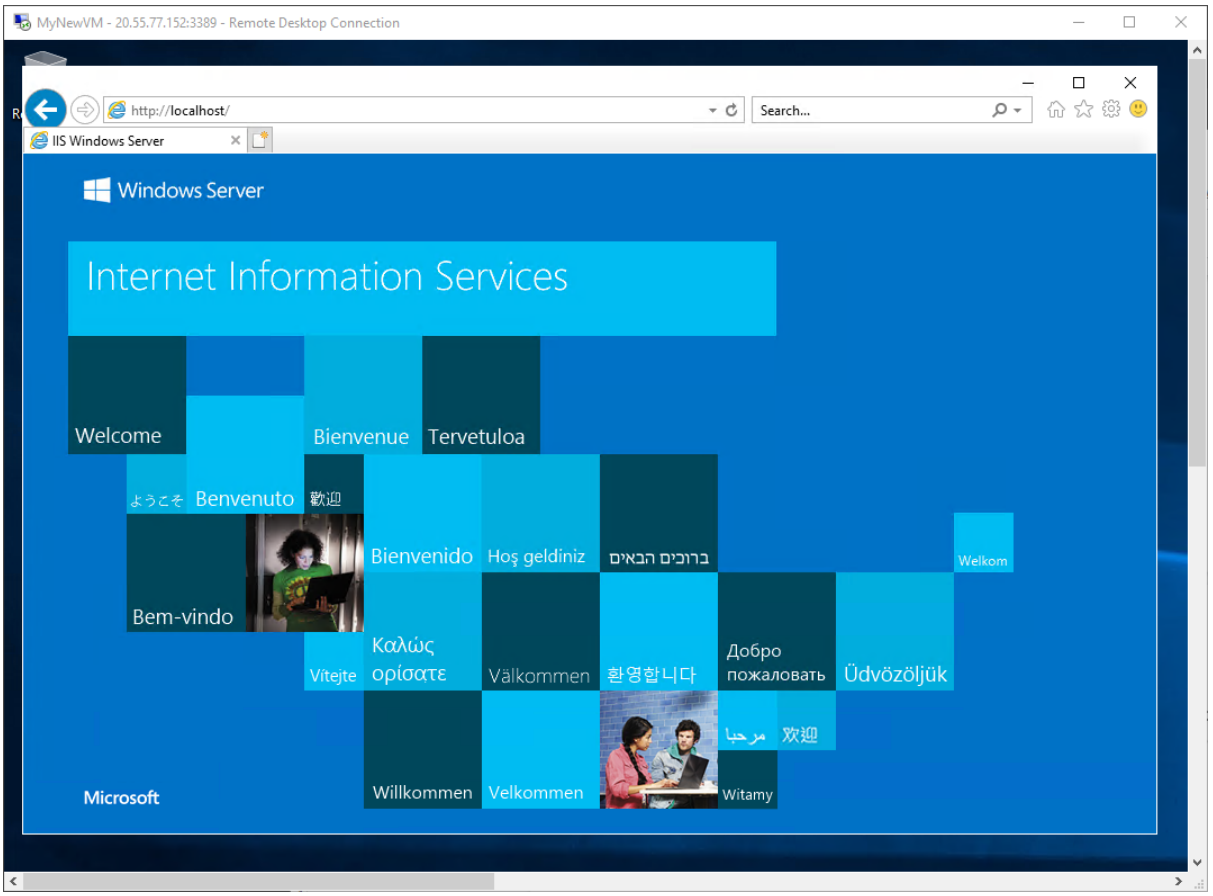
2. Click on **Next** until you get an option to select **Web Server (IIS)**. Choose to install all features. Then, again click on **Next** until you get an option to install:



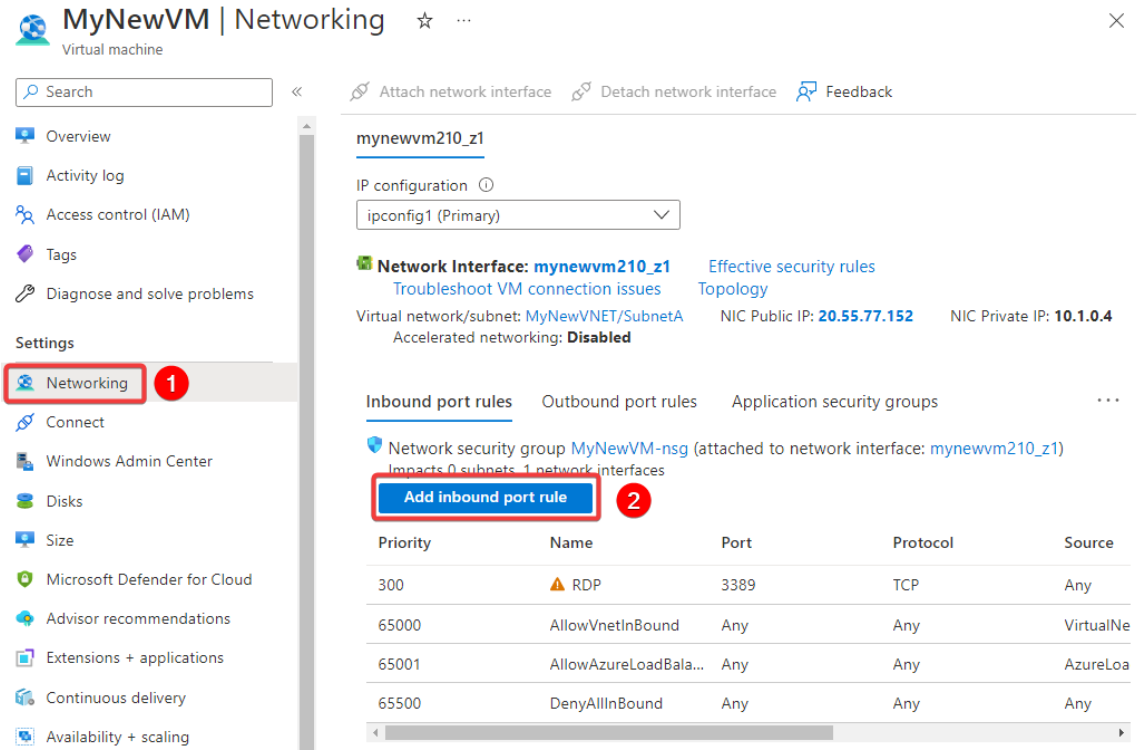
3. Click **Next** until you see the **Install** button. Click on it, and once the installation is complete, click on **Close**:

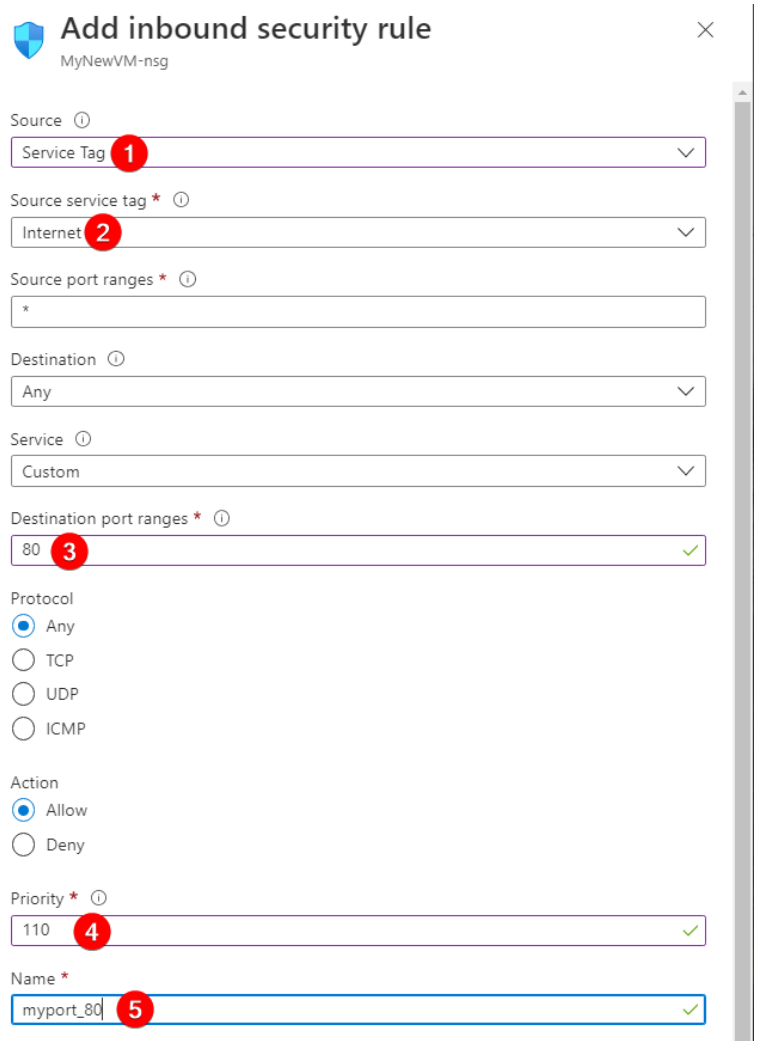


4. Open **Internet explorer** on the windows machine and enter **http://localhost/** in the search bar to confirm that Internet Information Services (IIS) is installed on the machine:

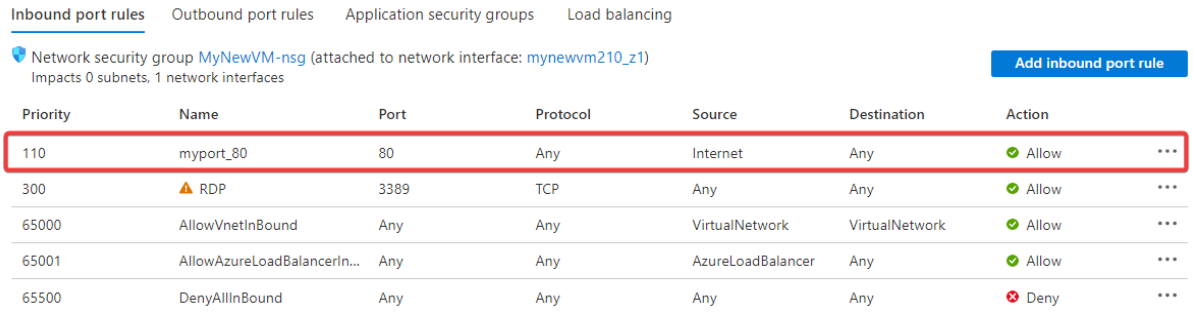


5. Return to the Azure portal. In the **Networking** section of the virtual machine **MyNewVM**, select **Add inbound port rule** and enter or select the following information:
    - Source: **Service Tag**
    - Source service tag: **Internet**
    - Destination: **Any**
    - Destination port ranges: **80**
    - Action: **Allow**
    - Priority: **110**
    - Name: **myport_80**


MyNewVM | Networking
Virtual machine
Search
Attach network interface
Detach network interface
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
1
Connect
Windows Admin Center
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
mynewvm210_z1
IP configuration
ipconfig1 (Primary)
Network Interface: mynewvm210_z1
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: MyNewVNET/SubnetA
NIC Public IP: 20.55.77.152
NIC Private IP: 10.1.0.4
Accelerated networking: Disabled
Inbound port rules
Outbound port rules
Application security groups
Network security group MyNewVM-nsg (attached to network interface: mynewvm210_z1)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule
2
Priority
Name
Port
Protocol
Source
300
RDP
3389
TCP
Any
65000
AllowVnetInBound
Any
Any
VirtualNe
65001
AllowAzureLoadBala...
Any
Any
AzureLoa
65500
DenyAllInBound
Any
Any
Any


Add inbound security rule
MyNewVM-nsg
Source
Service Tag
1
Source service tag *
Internet
2
Source port ranges *
*
Destination
Any
Service
Custom
Destination port ranges *
80
3
Protocol
Any
TCP
UDP
ICMP
Action
Allow
Deny
Priority *
110
4
Name *
myport_80
5

6. Click on the **Add** button. The security rule will be created:



7. In the **Networking** section, you will find the **public IP address**. Copy the **public IP**:

8. Paste the public IP in your web browser. You will see the page displaying Internet Information Services: