03 - Create a virtual network

In this walkthrough, we will create a virtual network, deploy two virtual machines onto that virtual network and then configure them to allow one virtual machine to ping the other over that virtual network.

Estimated time: 45 minutes

Task 1: Create a virtual network

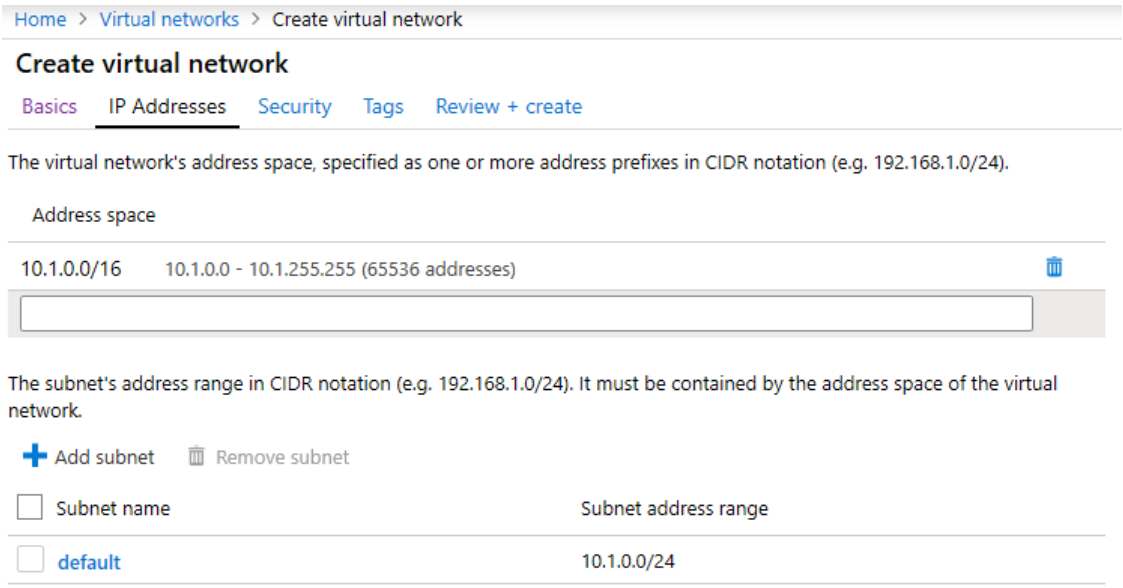
In this task, we will create a new virtual network.

1. Sign in to the Azure portal at https://portal.azure.com
2. Search for **Virtual networks**, and then click **+Add**.
3. On the **Create virtual network Basics** tab, fill in the following.

Setting	Value
Subscription	**Select your subscription**
Resource group	**myRGVNet** (create new)
Name	**vnet1**
Region	**East US**

4. Move to the **IP Addresses** tab. Take the defaults. Use the IP Address Space delete icon if you need to make changes.

Setting	Value
Address space	**10.1.0.0/16**
Subnet - Name	**default**
Subnet Address range	**10.1.0.0/24**



Screenshot of the Create virtual network IP Addresses tab with the default fields.

5. Click the **Review + create** button. Ensure the validation passes.
6. Click the **Create** button to deploy the virtual network.
7. For your organization how will you know which virtual networks and IP addressing you will need?

Task 2: Create two virtual machines

In this task, we will create two virtual machines in the virtual network.

1. Search for **Virtual machines** and then click **+Add**.
2. In Create a **virtual machine** - **Basics** tab, enter or select this information. Use the defaults for other fields.

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGVNet**
Virtual machine name	**vm1**
Region	**(US) East US**
Image	Leave the default **Windows Server 2016 Datacenter**
Username	**azureuser**
Password	**Pa$$w0rd1234**
Public inbound ports	Select **Allow selected ports**

Selected inbound ports	**RDP**

3. Select the **Networking** tab. Make sure the virtual machine is placed in the vnet1 virtual network. Review the default settings, but do not make any other changes.

Setting	Value
Virtual network	**vnet1**

4. Select **Review + create**. After the Validation passes, select **Create**. Deployment times can vary but it can generally take between three to six minutes to deploy.
5. Monitor your deployment, but continue on to the next step.
6. Create a second virtual machine by repeating steps **2 to 4** above. Make sure you use a different virtual machine name and that the virtual machine is in the new virtual network.

Setting	Value
Resource group	**myRGVNet**
Virtual machine name	**vm2**
Virtual network	**vnet1**
Public IP	**vm2-ip** (new)

7. When finished creating **vm2**, validate the configuration by clicking **Review + create** and once successfully validated click **Create**.
8. Wait for your virtual machines to deploy.

Task 3: Test the connection

In this task, we will allow ICMP connections and test that the virtual machines can communicate (ping) each other.

1. Search for **vm1**, make sure the **Status** is **Running**. You may need to **Refresh** the page.
2. On the **Overview** blade, click the **Connect** button.

   Note: The following directions tell you how to connect to your VM from a Windows computer.

3. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP File**.
4. Open the downloaded RDP file and click **Connect** when prompted.

5. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as **azureuser**. Enter password, **Pa$$w0rd1234** and then click **OK**.

6. You may receive a certificate warning during the sign-in process. Click **Yes** or to create the connection and connect to your deployed VM. You should connect successfully.

7. Open up a PowerShell command prompt on the virtual machine, by clicking the **Start** button, typing **PowerShell** right clicking **Windows PowerShell** in the menu and selecting **Run as administrator**

8. Try to ping vm2 (make sure vm2 is running). You will receive an error, saying request timed out. The `ping` fails, because `ping` uses the **Internet Control Message Protocol (ICMP)**. By default, ICMP isn't allowed through the Windows firewall.

   ```
   ping vm2
   ```

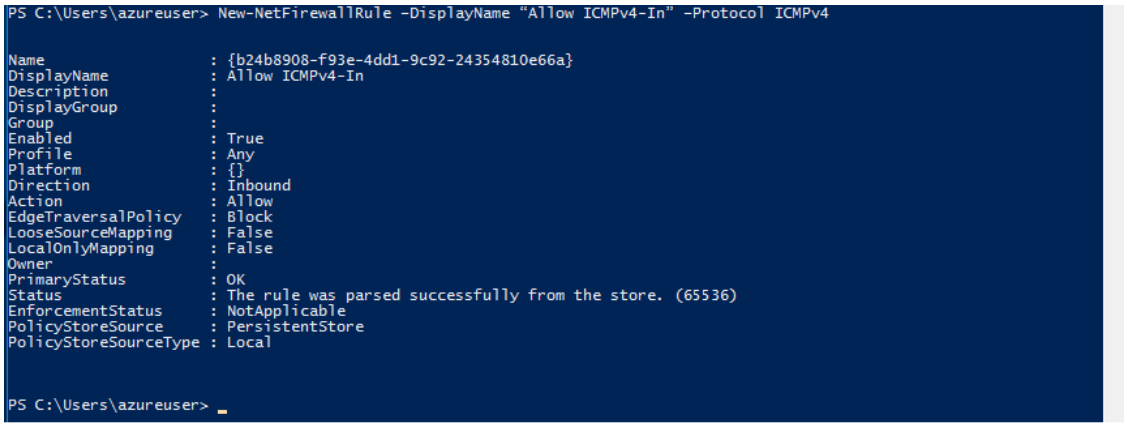
   Screenshot of PowerShell command prompt with the command ping vm2 after been run and the output indicating the command wasn't successful.

You will now switch to vm2 and allow ICMP

8. Connect to **vm2** using RDP. You can follow steps **2 to 6**.

9. Open a **PowerShell** prompt and allow ICMP. This command allows ICMP inbound through the Windows firewall.

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



Screenshot of PowerShell command prompt with the command New-NetFirewallRule DisplayName Allow ICMPv4-In –Protocol ICMPv4 after been run and the output indicating the command was successful.

You will now switch to vm1 and try the ping again

10. Return to the vm1 remote session and try the ping again. You should now be successful.

```
ping vm2
```

Congratulations! You have configured and deployed two virtual machines in a virtual network. You have also configured the firewall so one of the virtual machines allows ping requests.

Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.