Seneca

Lab 4: Create a virtual network

At the end of each lab, any resources you created in your account will be preserved. Some Azure resources, such as VM instances, may be automatically shut down, while other resources, such as storage services will be left running. Keep in mind that some Azure features cannot be stopped and can still incur charges (i.e. Azure Bastion). To minimize your costs, delete all resources and recreate them as needed to test your work during a session.

Reference: [AZ-900T0X-MICROSOFTAZUREFUNDAMENTALS](#)

04 - 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 within that virtual network.

Task 1: Create a virtual network (20 min)

In this task, we will create a virtual network.

1. Sign in to the Azure portal at https://portal.azure.com
2. From the **All services** blade, search for and select **Virtual networks**, and then click **+ Add**.
3. On the **Create virtual network** blade, fill in the following (leave the defaults for everything else):

Setting	Value
Name	**vnet1**
Address space	**Use the address space assigned in Blackboard (example: 10.1.0.0/16)**
Subscription	**Select your subscription**
Resource group	**myRGVNet** (create new)
Location	**(US) East US**

Setting	Value
Subnet - Name	**default**
Subnet Address range	**Use an appropriate subnet address range (example: 10.1.0.0/24)**

Create virtual network

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 * ⓘ

> Azure Pass - Sponsorship ⌄

    Resource group * ⓘ

> (New) myRGVnet ⌄

Create new

Instance details

Name *

> vnet1 ✓

Region *

> (US) East US ⌄

4.

Create virtual network

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

10.1.0.0/16	10.1.0.0 - 10.1.255.255 (65536 addresses) 🗑

☐ 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
☐ default	10.1.0.0/24

5. Click the **Review + create** button. Ensure the validation passes.
6. Click the **Create** button to deploy the virtual network.

Note: In 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. From the **All services** blade, search for **Virtual machines** and then click **+ Add**.
2. On the **Basics** tab, fill in the following information (leave the defaults for everything else):

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGVNet**
Virtual machine name	**vm1**
Region	**(US) East US**
Image	**Windows Server 2019 Datacenter**
Username	**azureuser**
Password	**Pa$$w0rd1234**
Public inbound ports	Select **Allow selected ports**
Selected inbound ports	**RDP (3389)**

Setting	Value

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. Click **Review + create**. After the Validation passes, click **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, that the virtual machine is within the same virtual network, and is using a new public IP address:

Setting	Value
Resource group	**myRGVNet**
Virtual machine name	**vm2**
Virtual network	**vnet1**

Setting	Value
Public IP	(new) **vm2-ip**

7. Wait for both virtual machines to deploy.

Task 3: Test the connection

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

1. From the **All resources** blade, search for **vm1**, open its **Overview** blade, and make sure its **Status** is **Running**. You may need to **Refresh** the page.
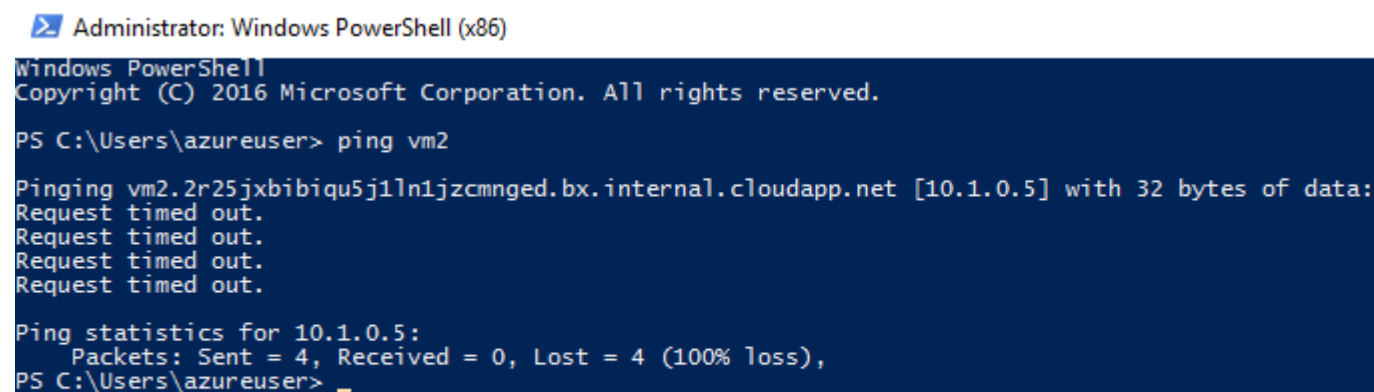2. On the **Overview** blade, click the **Connect** button.

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

3. On the **Connect to virtual machine** blade, keep the default options to connect by IP address 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, type the username **azureuser** and 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 right-click menu, and clicking **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.

CodeCopy

```
ping vm2
```

```
Administrator: Windows PowerShell (x86)                                    —    □    ✕

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> ping vm2

Pinging vm2.2r25jxbibiqu5j1ln1jzcmnged.bx.internal.cloudapp.net [10.1.0.5] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\azureuser> _
```

Note: You will now open an RDP session to vm2 and allow incoming ICMP connections

9. Connect to **vm2** using RDP. You can follow steps **2 to 6**.
10. Open a **PowerShell** prompt and allow ICMP. This command allows ICMP inbound connections through the Windows firewall.

CodeCopy

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

```
PS C:\Users\azureuser> New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4

Name                  : {b24b8908-f93e-4dd1-9c92-24354810e66a}
DisplayName           : Allow ICMPv4-In
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local


PS C:\Users\azureuser> _
```

Note: You will now switch to the RDP session to vm1 and try the ping again

1. Return to the RDP session to vm1 and try the ping again. You should now be successful.

CodeCopy

```
ping vm2
```

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

Note: To avoid additional costs, you can remove all resources in the resource group. Search for resource groups, click your resource group, and then delete the resources within the resource group. **DO NOT DELETE YOUR RESOURCE GROUP.**

Submission Requirements

Submit a screenshot with the following information:

Screenshot #1:

- Successful ping request from vm1 to vm2 using your assigned IP address space
- The Azure Portal with your login ID [requires another browser window]
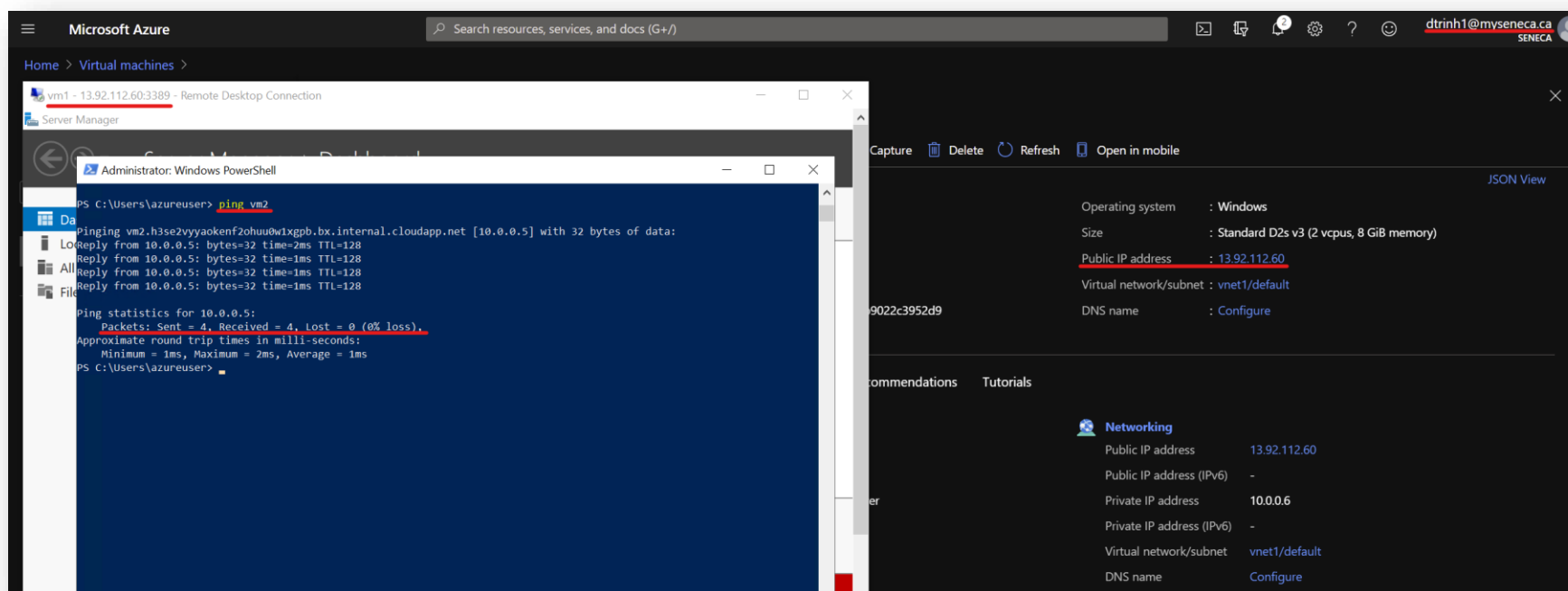
Screenshot #2:

- Successful deletion of resources within resource group. **DO NOT DELETE YOUR RESOURCE GROUP!**