# Lab Answer Key:  Module 5: Virtual Networking

## Lab 2: Configuring VNet Peering

The objective of this lab is to connect two virtual networks by using a VNet peering. In this lab, you will create two virtual machines on two different virtual network in the same Azure region, configure connection between the two virtual networks by using VNet peering, and verify direct network connectivity between the two virtual machines.

### Exercise 1: Create the lab virtual machines by using the Azure Portal

The main tasks for this exercise are as follows: 1. Create the first virtual machine 2. Create the second virtual machine

#### Task 1: Create the first virtual machine

1. Launch your Internet browser and navigate to https://portal.azure.com
2. Sign in to the Azure portal by using your administrative credentials.
3. In the Azure portal, in the hub menu, click **+New**.
4. Click **Compute** on the blade that comes up.
5. On the **Compute** blade, click **Windows Server 2016 Datacenter**
6. On the blade that comes up, at the bottom of the page, ensure that the deployment model is set to **Resource Manager** and click **Create**.
7. On the **Basics** blade, specify the following settings and click **OK**:

* Name: **VM1**
* VM disk type: **HDD**
* User name: **demouser**
* Password: **DemoPa$$w0rd**
* Confirm password: **DemoPa$$w0rd**
* Subscription: the name of the subscription you are using for this lab
* Resource Group: ensure that **Create new** is selected and type **VNet1RG** in the text box below
* Location: Choose the Azure region closest to your location.

1. On the **Choose a size** blade, click **View all**, click **A1 Basic**, and click **Select**.
2. On the **Settings** blade, click **Virtual network**.
3. On the **Create virtual network** blade, specify the following settings and click **OK**:

* Name: **VNet1**
* Address space: **10.0.0.0/22**
* Subnet name: **Subnet1**
* Subnet address range: **10.0.0.0/24**

1. In the **Monitoring** section, click **Disabled** under **Boot diagnostics** and click **OK**.
2. On the **Summary** blade, click **OK**.

Note: Do not wait for the first virtual machine to be provisioned but proceed to the next task

#### Task 2: Create the second virtual machine

1. In the Azure portal, in the hub menu, click **+New**.
2. Click **Compute** in the blade that comes up.
3. On the **Compute** blade, click **Windows Server 2016 Datacenter**
4. On the blade that comes up, at the bottom of the page, ensure that the deployment model is set to **Resource Manager** and click **Create**.
5. On the **Basics** blade, specify the following settings and click **OK**:

* Name: **VM2**
* VM disk type: **HDD**
* User name: **demouser**
* Password: **DemoPa$$w0rd**
* Confirm password: **DemoPa$$w0rd**
* Subscription: the name of the subscription you are using for this lab
* Resource Group: ensure that **Create new** is selected and type **VNet2RG** in the text box below
* Location: Choose the same region you chose in the first task of this exercise.

1. On the **Choose a size** blade, click **View all**, click **A1 Basic**, and click **Select**.
2. On the **Settings** blade, click **Virtual network**.
3. On the **Create virtual network** blade, specify the following settings and click **OK**. Note: To connect two virtual networks, they must have non-overlapping IP address space. The Azure portal provides visual clues that indicate whether the virtual network you are creating has an overlapping IP address space with any of the existing virtual networks in the same subscription):

* Name: **VNet2**
* Address space: **10.0.4.0/22**
* Subnet name: **Subnet1**
* Subnet address range: **10.0.4.0/24**

1. In the **Monitoring** section, click **Disabled** under **Boot diagnostics** and click **OK**.
2. On the **Summary** blade, click **OK**.

Note: Do not wait for the second virtual machine to be provisioned but proceed to the next exercise

### Exercise 2: Configure VNet Peering using the Azure Portal

The tasks for this exercise are as follows: 1. Create the first VNet Peering link 2. Create the second VNet Peering link 3. Verify connectivity between the two virtual networks 4. Reset the lab environment (optional)

#### Task 1: Create the first VNet Peering link

1. In the Azure portal, in the hub menu, click **More services**.
2. In the list of services, in the **NETWORKING** section, click **Virtual networks**.
3. On the **Virtual networks** blade, click **VNet1**
4. On the blade that comes up, click **Peerings**.
5. Click **+Add**.
6. On the **Add peering blade**, specify the following settings and click **OK**:

* Name: **VNet2\_peering**
* Virtual network deployment model: **Resource manager**
* I know my resource ID: leave the checkbox clear

Note: VNet peering is supported between a Resource manager VNet and a classic VNet if both are part of the same subscription. This restriction does not apply to VNet peering between two Resource manager VNets. They can belong to two different subscriptions, if both subscriptions are associated with the same Azure Active Directory tenant. However, there is no support for VNet peering between two classic VNets.

Note: If you know the resource ID, you can provide it directly at this point, rather than pointing to an existing virtual network by relying on the options available in the Azure portal interface (which we rely on in this case).

* Subscription: the name of the subscription you are using for this lab.
* Virtual network: click **Choose a virtual network** and, on the **Choose virtual network** blade, click **VNet2**.
* Allow virtual network access: **Enabled**
* Allow forwarded traffic: leave the checkbox clear
* Allow gateway transit: leave the checkbox clear
* Use remote gateways: leave the checkbox clear

Note: The **Allow forwarded traffic** setting, once enabled, makes possible for traffic that does not originate from the peer virtual network but is forwarded by it into your virtual network. The **Allow gateway transit** setting, once enabled, makes possible to for the peer virtual network to use the virtual gateway configured on your virtual network for connectivity with other networks. This requires that the Use remote gateways setting is enabled on the peer virtual network.

#### Task 2: Create the second VNet Peering link

1. In the Azure portal, in the hub menu, scroll back to the **Virtual networks** blade.
2. On the **Virtual networks** blade, click **VNet2**
3. On the blade that comes up, click **Peerings**
4. Click **+Add**
5. On the **Add peering** blade, specify the following settings and click **OK**:

* Name: **VNet1\_peering**
* Virtual network deployment model: **Resource manager**
* I know my resource ID: leave the checkbox clear
* Subscription: the name of the subscription you are using for this lab
* Virtual network: click **Choose a virtual network** and, on the **Choose virtual network** blade, click **VNet1**
* Allow virtual network access: **Enabled**
* Allow forwarded traffic: leave the checkbox clear
* Allow gateway transit: leave the checkbox clear
* Use remote gateways: leave the checkbox clear

#### Task 3: Verify connectivity between the two virtual networks

Note: Make sure that both virtual machines have been fully provisioned before you proceed with this task.

1. In the Azure portal, in the hub menu, click **More services**.
2. In the list of services, in the **COMPUTE** section, click **Virtual machines**
3. On the **Virtual machines** blade, click **VM1**
4. On the blade that comes up, click **Connect**
5. When prompted whether to open or save VM1.rdp, click **Open**
6. In the **Remote Desktop Connection** dialog box, click **Connect**
7. In the **Windows Security** dialog box, type in **demouser** as the user name and **DemoPa$$w0rd** as the password and click **OK**
8. In the **Remote Desktop Connection** dialog box, click **Yes**
9. Switch back to the Azure portal and scroll back to the **Virtual machines** blade.
10. On the **Virtual Machines** blade, click **VM2**
11. On the **VM2** blade, click **Network interfaces**
12. On the **VM2- Network interfaces** blade, note the entry appearing in the **PRIVATE IP ADDRESS** column of the network interface of VM2 (this should be 10.0.4.4).
13. Switch to the Remote Desktop session to VM1.
14. In the Remote Desktop session to VM1, right-click Start and, in the right-click menu, click **Run**
15. In the **Run** dialog box, type mstsc /v:10.0.4.4

Note: The built-in Azure DNS does not support name resolution between Azure virtual networks connected via VNet peering. This is the reason we cannot specify the VM name (i.e. VM2) in this scenario. However, you could implement your own custom DNS solution that would provide this capability.

1. When prompted for credentials to be used to connect to 10.0.4.4, type in **demouser** as the user name and **DemoPa$$w0rd** as the password.
2. In the **Remote Desktop Connection** dialog box, click **Yes**
3. Verify that you successfully connected to VM2.
4. Close the Remote Desktop Session to VM2.
5. Close the Remote Desktop Session to VM1.

#### Task 4: Reset the lab environment (optional)

Note: To minimize charges associated with running the lab environment, you should consider removing its resources. This is the purpose of this task.

Note: If you want to keep your lab environment in place, then you might want to consider stopping both virtual machines. This will eliminate compute charges associated with keeping these virtual machines online. To ensure that these charges do not accrue, stop the virtual machines from the Azure portal and ensure that they are listed on the Virtual machines blade with the Stopped (deallocated) state (rather than Stopped).

1. In the Azure portal, in the hub menu, click **Resource groups**
2. On the Resource groups blade, click **VNet1RG**
3. On the **VNet1RG** blade, click **Delete**
4. On the **Are you sure you want to delete "VNet1RG"?** blade, type **VNet1RG** in the **TYPE THE RESOURCE GROUP NAME** text box, and click **Delete**
5. On the Resource groups blade, click **VNet2RG**
6. On the **VNet2RG** blade, click **Delete**
7. On the **Are you sure you want to delete "VNet2RG"?** blade, type **VNet2RG** in the **TYPE THE RESOURCE GROUP NAME** text box, and click **Delete**