# Lab Answer Key: Module 2: Implementing and managing Azure networking

# Lab A: Using a deployment template, Azure PowerShell, and Azure CLI to implement Azure virtual networks

## Exercise 1: Creating an Azure virtual network by using a deployment template

#### Task 1: Review a GitHub Azure quickstart template

1. Ensure that you are signed in to MIA-CL1 as **Student** with the password **Pa55w.rd**.
2. Start Microsoft Edge and browse to the **Virtual Network with two Subnets** Github-hosted Azure quickstart template at [**http://aka.ms/Mt32e4**](http://aka.ms/Mt32e4).
3. In Microsoft Edge, on the **Virtual Network with two Subnets** page, click **Deploy to Azure**.
4. If prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
5. In the Azure portal, on the **Create a Virtual Network with two Subnets** blade, click **Edit template**.
6. Review the structure of the JavaScript Object Notation (JSON) file. Examine the placeholders for values that can be edited during the deployment. This template contains the following parameters: ***vnetName***, ***vnetAddressPrefix***, ***subnet1Prefix***, ***subnet1Name***, ***subnet2Prefix***, and ***subnet2Name***.
7. Review the content of the **Resources** section to identify type of the resource, its name, and properties.
8. Click **Discard** to close the Edit Template blade.

**Note:** If the template fails to load into the Azure portal, navigate to the following URL: [**http://aka.ms/Fpqovq**](http://aka.ms/Fpqovq). Then, select and copy all text on the page. Paste the copied text into the **Edit template** blade, then perform steps 6 to 8 to review the template and close the Edit Template blade without making any changes.

#### Task 2: Perform the deployment from the Azure portal

1. On the **Create a Virtual Network with two Subnets** blade, specify the following settings and then click **Purchase**.

* Subscription: select the name of your subscription in the drop down list
* Resource group: ensure that **Create new** option is selected and type **20533E0203-LabRG** in the text box below
* Location: in the drop-down list, select an Azure region you chose when running the provisioning script at the beginning of this module
* Vnet Name: **20533E0203-vnet**
* Vnet Address Prefix: **10.10.0.0/16**
* Subnet1Prefix: **10.10.0.0/24**
* Subnet1Name: **Subnet1**
* Subnet2Prefix: **10.10.1.0/24**
* Subnet2Name: **Subnet2**
* Location: **[resourceGroup().location]**
* I agree to the terms and conditions stated above: **enabled**

1. Verify that provisioning of the new virtual network with name **20533E0203-vnet** completed successfully.

**Result**: After completing this exercise, you should have created virtual networks by using an Azure Resource Manager deployment template

## Exercise 2: Creating a virtual network by using PowerShell

#### Task 1: Create a virtual network by using PowerShell

1. On MIA-CL1, click **Start**, in the Start menu, expand the **Windows PowerShell** folder, right-click **Windows PowerShell ISE**, click **More**, and then click **Run as administrator**. When prompted by User Account Control for confirmation, click **Yes**.
2. In the Windows PowerShell Integrated Scripting Environment (ISE), in the console pane, type the following cmdlet and then press Enter:

Add-AzureRmAccount

1. In the sign-in windows that appears, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. If you have multiple subscriptions associated with your Microsoft account, to identify the subscription in which you are going to create a virtual network, type the following command, and then press Enter:

Get-AzureRmSubscription

1. Note the value of the ***Id*** property for each subscription in the output of the previous command. To specify the subscription in which you are going to create a virtual network, type the following commands, and then press Enter (replace ***SubscriptionId*** with the actual SubscriptionId property of that subscription):

Set-AzureRmContext -SubscriptionId 'SubscriptionId'

1. To create a new resource group, type the following command, and then press Enter (replace ***AzureRegion*** with the name of the same Azure region you chose in the previous exercise):

$rg = New-AzureRMResourceGroup -Name '20533E0204-LabRG' -Location 'AzureRegion'

1. To create a new virtual network named **20533E0204-vnet** with the address space **10.11.0.0/16** and store a reference to it in the ***$vnet*** variable, type the following command, and then press Enter:

$vnet = New-AzureRmVirtualNetwork -ResourceGroupName $rg.ResourceGroupName -Name '20533E0204-vnet' -AddressPrefix '10.11.0.0/16' -Location $rg.Location

1. To add a subnet to the new virtual network, type the following command, and then press Enter:

Add-AzureRmVirtualNetworkSubnetConfig -Name 'Subnet1' -VirtualNetwork $vnet -AddressPrefix '10.11.0.0/24'

1. To update the configuration in the virtual network, type the following command, and then press Enter:

Set-AzureRmVirtualNetwork -VirtualNetwork $vnet

**Result**: After completing this exercise, you should have created a virtual network by using Azure PowerShell.

## Exercise 3: Creating a virtual network by using Azure CLI

#### Task 1: Creating a virtual network by using Azure CLI

1. On MIA-CL1, click **Start**, in the Start menu, expand the **Windows System** folder, right-click **Command Prompt**, click **More**, and click **Run as administrator**. When prompted by User Account Control for confirmation, click **Yes**.
2. From **Administrator: Command Prompt**, type the following command and then press Enter:

az login

1. You will be presented with the message instructing you to open a browser at the page [**https://aka.ms/devicelogin**](https://aka.ms/devicelogin) and provide the code included in the message to authenicate. Start Microsoft Edge and browse to [**https://aka.ms/devicelogin**](https://aka.ms/devicelogin).
2. On the **Device Login** page, type the code included in the message. This will identify Microsoft Azure Cross-platform Command Line Interface as the application publisher. Click **Continue**.
3. In the sign-in windows that appears, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. Note the message stating that you have signed in to the Microsoft Azure Cross-platform Command Line Interface application on your device. Close the Microsoft Edge window.
5. If you have multiple subscriptions associated with your Microsoft account, to identify the subscription in which you are going to create a virtual network, type the following command, and then press Enter:

az account show

1. Note the value of the '***id***' property for each subscription in the output of the previous command. To specify the subscription in which you are going to create a virtual network, type the following commands, and then press Enter (replace ***SubscriptionId*** with the actual SubscriptionId property of that subscription):

az account set --subscription "SubscriptionId"

1. To create a new resource group, type the following command, and then press Enter (replace ***AzureRegion*** with the name of the same Azure region you chose in the previous exercise):

az group create --name 20533E0205-LabRG --location "AzureRegion"

1. To create a new virtual network named **20533E0205-vnet** with the address space **10.12.0.0/16** and a subnet named Subnet1 with the address prefix of 10.12.0.0/24, type the following command, and then press Enter (replace ***AzureRegion*** with the name of the same Azure region you chose in the previous exercise):

az network vnet create --name 20533E0205-vnet --resource-group 20533E0205-LabRG --location "AzureRegion" --address-prefix 10.12.0.0/16 --subnet-name Subnet1 --subnet-prefix 10.12.0.0/24

1. To add a subnet to the new virtual network, type the following command, and then press Enter:

az network vnet subnet create --address-prefix 10.12.1.0/24 --name Subnet2 --resource-group 20533E0205-LabRG --vnet-name 20533E0205-vnet

**Result**: After completing this exercise, you should have created a virtual network by using Azure CLI.

# Lab B: Configuring VNet peering

## Exercise 1: Using the Azure portal to configure VNet peering

#### Task 1: Configure VNet peering for the first virtual network

1. Ensure that you are signed in to MIA-CL1 as **Student** with the password **Pa55w.rd** and that the **Add-20533EEnvironment** script successfully completed. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. In Microsoft Edge, in the Azure portal, click **All services** and, in the service menu, click **Virtual networks**.
3. On the **Virtual networks** blade, click **20533E0201-vnet**.
4. On the **20533E0201-vnet** blade, click **Peerings**.
5. Click **+ Add**.
6. On the **Add peering** blade, specify the following settings and click **OK**:

* Name: **20533E0201-vnet-To-20533E0202-vnet**
* Virtual network deployment model: **Resource manager**
* Subscription: the name of your Azure subscription
* Virtual network: click **Search virtual network** and select **20533E0202-vnet**
* Allow virtual network access: **Enabled**
* Allow forwarded traffic: enabled
* Allow gateway transit: disabled
* Use remote gateways: disabled

#### Task 2: Configure VNet peering for the second virtual network

1. In the Azure portal, navigate back to the **Virtual networks** blade and click **20533E0202-vnet**.
2. On the **20533E0202-vnet** blade, click **Peerings**.
3. Click **+ Add**.
4. On the **Add peering** blade, specify the following settings and click **OK**:

* Name: **20533E0202-vnet-To-20533E0201-vnet**
* Virtual network deployment model: **Resource manager**
* Subscription: the name of your Azure subscription
* Virtual network: click **Select virtual network** and select **20533E0201-vnet**
* Allow virtual network access: **Enabled**
* Allow forwarded traffic: enabled
* Allow gateway transit: disabled
* Use remote gateways: disabled

**Result**: After completing this exercise, you should have configured VNet peering between two virtual networks.

## Exercise 2: Configuring VNet peering–based service chaining

#### Task 1: Configure IP forwarding

1. In Microsoft Edge, in the Azure portal, click **All services** and, in the service menu, click **Virtual machines**.
2. On the **Virtual machines** blade, click **20533E0201-vm1**.
3. On the **20533E0201-vm1** blade, click **Networking**
4. Click **20533E0201-nic1**.
5. On the **20533E0201-nic1** blade, click **IP configurations**.
6. Set **IP forwarding** to **Enabled**.
7. Click **Save**.

#### Task 2: Configure user defined routing

1. In Microsoft Edge, in the Azure portal, click **+ Create resource**.
2. On the **New** blade, click **Networking** and then, click **Route table**
3. On the **Create route table** blade, specify the following and click **Create**:

* Name: **20533E02-rt1**
* Subscription: the name of your Azure subscription
* Resource group: click **Use existing** and then select **20533E0202-LabRG** in the drop-down list
* Location: the same Azure region in which you created the virtual network 20533E0202-vnet
* BGP route propagation: **Disabled**

1. Wait until the route table is provisioned. Next, in the Azure portal, in the hub menu, click **All services** and, in the service menu, click **Route tables**.
2. On the **Route tables** blade, click **20533E02-rt1**.
3. On the **20533E02-rt1** blade, click **Routes**.
4. Click **+ Add**.
5. On the **Add route** blade, specify the following settings and click **OK**:

* Route name: **custom-route-to-20533E0201-vnet**
* Address prefix: 10.0.0.0/22
* Next hop type: **Virtual appliance**
* Next hop address: **10.0.0.4**

1. Back on the **20533E02-rt1** blade, click **Subnets**.
2. Click **+ Associate**.
3. On the **Associate subnet** blade, click **Choose a virtual network**.
4. On the **Resource** blade, click **20533E0202-vnet**.
5. On the **Choose subnet** blade, click **subnet-1**.
6. On the **Associate subnet** blade, click **OK**.

#### Task 3: Configure routing on an Azure VM running Windows Server 2016

1. On MIA-CL1, in Microsoft Edge, in the Azure portal, in the hub menu, click **All services** and, in the list of services, click **Virtual machines**.
2. On the **Virtual machines** blade, click ellipsis to the right of the **20533E0201-vm1** entry and click **Connect**.
3. On the **Connect to virtual machine** blade, click **Download RDP File**. When prompted, click **Open**.
4. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
5. In the **Windows Security** dialog box, type the following credentials, and then click **OK**:

* User name: **Student**
* Password: **Pa55w.rd1234**

1. If another Remote Desktop Message displays, select the **Don't ask me again for connections to this computer** checkbox, and then click **Yes**.
2. If prompted in the Remote Desktop session whether to allow your PC to be discoverable, click **No**.
3. Once you are connected to 20533E0201-vm1 via the Remote Desktop session, in **Server Manager**, click **Manage** and then, in the drop-down menu, click **Add Roles and Features**. This will start Add Roles and Features Wizard.
4. On the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, ensure that the **Role-based or feature-based installation** option is selected and click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, select the **Remote Access** check box, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Remote Access** page, click **Next**.
10. On the **Select role services** page, select the **Routing** checkbox. When prompted whether to add features that are required for routing, click **Add Features**, and then click **Next**.
11. On the **web Server Role (IIS)** page, click **Next**.
12. On the **Select role services** page, click **Next**.
13. On the **Confirmation** page, click **Install**.
14. Wait for the installation to complete and, on the **Installation progress** page, click **Close**.
15. In **Server Manager**, click **Tools** and then, in the drop-down menu, click **Routing and Remote Access**.
16. In the **Routing and Remote Access** console, right-click the **20533E0201-vm1 (local)** node and, in the right-click menu, click **Configure and Enable Routing and Remote Access**. This will start **Routing and Remote Access Server Setup Wizard**.
17. On the **Welcome to the Routing and Remote Access Server Setup Wizard** page, click **Next**.
18. On the **Configuration** page, click **Custom configuration** and click **Next**.
19. On the **Custom Configuration** page, click **LAN routing** and click **Next**.
20. On the **Completing the Routing and Remote Access Server Setup Wizard** page, click **Finish**.
21. In the **Routing and Remote Access** dialog box, click **Start service**.
22. In **Server Manager**, click **Tools** and then, in the drop-down menu, click **Windows Firewall with Advanced Security**.
23. In the **Windows Firewall with Advanced Security** console, click **Inbound rules**.
24. In the list of rules, select **File and Printer Sharing (Echo Request - ICMPv4-In)** and click **Enable Rule**.

**Result**: After completing this exercise, you should have configured VNet peering–based service chaining.

## Exercise 3: Validating virtual network connectivity

#### Task 1: Configure Windows Firewall with Advanced Security on an Azure VM

1. On MIA-CL1, in Microsoft Edge, in the Azure portal, in the hub menu, from the **Virtual machines** blade, click ellipsis to the right of the **20533E0201-vm2** entry and click **Connect**.
2. On the **Connect to virtual machine** blade, click **Download RDP File**. When prompted, click **Open**.
3. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
4. In the **Windows Security** dialog box, type the following credentials, and then click **OK**:

* User name: **Student**
* Password: **Pa55w.rd1234**

1. If another Remote Desktop Message displays, select the **Don't ask me again for connections to this computer** checkbox, and then click **Yes**.
2. If prompted in the Remote Desktop session whether to allow your PC to be discoverable, click **No**.
3. In **Server Manager**, click **Tools** and then, in the drop-down menu, click **Windows Firewall with Advanced Security**.
4. In the **Windows Firewall with Advanced Security** console, click **Inbound rules**.
5. In the list of rules, select **File and Printer Sharing (Echo Request - ICMPv4-In)** and click **Enable Rule**.

#### Task 2: Test service chaining between peered virtual networks

1. On MIA-CL1, in Microsoft Edge, in the Azure portal, in the hub menu, from the **Virtual machines** blade, click ellipsis to the right of the **20533E0202-vm1** entry and click **Connect**.
2. On the **Connect to virtual machine** blade, click **Download RDP File**. When prompted, click **Open**.
3. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
4. In the **Windows Security** dialog box, type the following credentials, and then click **OK**:

* User name: **Student**
* Password: **Pa55w.rd1234**

1. If another Remote Desktop Message displays, select the **Don't ask me again for connections to this computer** checkbox, and then click **Yes**.
2. If prompted in the Remote Desktop session whether to allow your PC to be discoverable, click **No**.
3. Once you are connected to 20533E0202-vm1 via the Remote Desktop session, click **Start** and click **Windows PowerShell**.
4. In the **Windows PowerShell** window, type the following cmdlet and then press Enter:

Test-NetConnection -ComputerName 10.0.1.4 -TraceRoute

1. Verify that test is successful and note that the connection was routed over 10.0.0.4

#### Task 3: Remove the lab environment

1. On MIA-CL1, close all open windows without saving any files.
2. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**. In the User Account Control dialog box, click **Yes**.
3. Type the following command, and then press **Enter**:

Remove-20533EEnvironment

1. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. If you have multiple Azure subscriptions, select the one you want the script to target.
3. When prompted, specify the current lab number.
4. If prompted for confirmation, type **y**.
5. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
6. In the Azure portal, on Dashboard, click **Edit**.
7. Right-click unoccupied area of the dashboard and, in the right-click menu, click **Reset to default state**. When prompted to confirm, click **Yes**.
8. Click **Done customizing**.
9. Close all open windows.

**Result**: After completing this exercise, you should have validated virtual network connectivity in the VNet peering configuration

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.