# Module 2: Implementing and managing Azure networking

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

### Scenario

A. Datum Corporation plans to create several virtual networks in their Azure subscription. They will all reside in the same Azure region. You want to test the deployment of Azure virtual networks by using both imperative and declarative methods.

### Objectives

After completing this lab, you will be able to:

* Create a virtual network by using deployment templates.
* Create a virtual network by using Azure PowerShell.
* Create a virtual network by using Azure CLI

### Lab Setup

Estimated Time: 30 minutes

Virtual Machine: **20533E-MIA-CL1**

User Name: **Student**

Password: **Pa55w.rd**

**Note:** The Microsoft Azure portal is continually improved, and the user interface might have been updated since this lab was written. Your instructor will make you aware of any differences between the steps described in the lab and the current Azure portal user interface.

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

### Scenario

A. Datum wants to test the provisioning of virtual networks. You must configure these virtual networks by using deployment templates from GitHub

The main tasks for this exercise are as follows:

1. Review a GitHub Azure quickstart template
2. Perform the deployment from the Azure portal

#### 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. From 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, 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. Close the Edit Template blade without making any changes.

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

1. From the **Create a Virtual Network with two Subnets** blade, deploy the template with the following settings:

* Subscription: the name of your subscription
* Resource group: create a new group named **20533E0203-LabRG**
* Location: 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]**

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

**Result**: After completing this exercise, you should have created virtual networks for A. Datum HQ.

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

### Scenario

A. Datum is expanding their services in Azure by using both declarative and imperative deployment methods and they ask you to test provisioning of a new network by using Azure PowerShell.

The main tasks for this exercise are as follows:

1. Create a virtual network by using PowerShell

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

1. On MIA-CL1, start Windows PowerShell ISE as Administrator.
2. From the console pane of the Windows PowerShell ISE window, authenticate to Azure Resource Manager endpoint of your Azure subscription.
3. From the console pane of the Windows PowerShell ISE window, review the list of subscriptions associated with the account you used to sign in. Identify the value of the subscription Id property of the Azure subscription you want to use in this lab.
4. If there are multiple Azure subscriptions associated with your account, run the **Set-AzureRmContext** with the **-SubscriptionId** parameter to designate the one you want to use in this lab.
5. Run the **New-AzureRMResourceGroup** cmdlet to create a new resource group named **20533E0204-LabRG** in the same Azure region you chose in the previous exercise.
6. Run the **New-AzureRmVirtualNetwork** cmdlet to create a new virtual network named **20533E0204-vnet** with the address space **10.11.0.0/16** in the **20533E0204-LabRG** resource group and the same Azure region as the resource group.
7. Run the **Add-AzureRmVirtualNetworkSubnetConfig** cmdlet to add a subnet named **Subnet1** with the address prefix **10.11.0.0/24** to the virtual network **20533E0204-vnet**.
8. Finalize your configuration by running the **Set-AzureRmVirtualNetwork** cmdlet.

**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

### Scenario

A. Datum is expanding their services in Azure by using both declarative and imperative deployment methods. They have asked you to test the provisioning of a new network by using Azure CLI.

The main tasks for this exercise are as follows:

1. Creating a virtual network by using Azure CLI

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

1. On MIA-CL1, start **Command Prompt** as Administrator
2. From **Administrator: Command Prompt**, use Azure CLI 2.0 to sign in to your Azure subscription.
3. From **Administrator: Command Prompt**, use Azure CLI 2.0 to display properties of the Azure subscription associated with the account you used to sign in. Take note of the value of the **id** parameter, representing your Azure subscription ID.
4. Run the **az account set** command to specify the subscription in which you are going to create a virtual network.
5. Run the **az group create** command to create a new resource group named **20533E0205-LabRG** in the same Azure region you chose in the previous exercise.
6. Run the **az network vnet create** command to create a 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** in the **20533E0205-LabRG** resource group and the same Azure region as the resource group.
7. Run the **az network vnet subnet create** command to add a subnet named **Subnet2** with the address prefix **10.12.1.0/24** to the virtual network **20533E0205-vnet**.

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

**Question** What are some of the methods you can use to create an Azure virtual network?

# Lab B: Configuring VNet peering

### Scenario

Now that A. Datum Corporation has deployed Azure Resource Manager VNets, the company wants to be able to provide direct connectivity between them. Your plan is to implement VNet peering to provide the optimal performance with minimum cost.

### Objectives

After completing this lab, you will be able to:

* Connect Azure virtual networks using VNet peering.
* Configure VNet peering-based service chaining
* Validate virtual network connectivity using Azure-based and VM-based tools.

### Lab Setup

Estimated Time: 35 minutes

Virtual Machine: **20533E-MIA-CL1**

User Name: **Student**

Password: **Pa55w.rd**

Before starting this lab, ensure that you have performed the "Preparing the Environment" demonstration tasks at the beginning of the first lesson in this module, and that the setup script has completed.

**Note:** The Microsoft Azure portal is continually improved, and the user interface might have been updated since this lab was written. Your instructor will make you aware of any differences between the steps described in the lab and the current Azure portal user interface.

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

### Scenario

A. Datum wants to use VNet peering to provide connectivity between pairs of virtual networks.

The main tasks for this exercise are as follows:

1. Configure VNet peering for the first virtual network
2. Configure VNet peering for the second virtual network

#### 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, and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. In Microsoft Edge, navigate to the **20533E0201-vnet** virtual network blade.
3. From the **20533E0201-vnet** blade, create a VNet peering with the following settings:

* Name: **20533E0201-vnet-To-20533E0202-vnet**
* Virtual network deployment model: **Resource manager**
* Subscription: the name of your Azure subscription
* Virtual network: **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 Microsoft Edge, navigate to the **20533E0202-vnet** virtual network blade.
2. From the **20533E0202-vnet** blade, create a VNet peering with the following settings:

* Name: **20533E0202-vnet-To-20533E0201-vnet**
* Virtual network deployment model: **Resource manager**
* Subscription: the name of your Azure subscription
* Virtual network: **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

### Scenario

A. Datum now wants to test the service chaining capabilities of VNet peering to minimize cost and management overhead of the Azure virtual network infrastructure.

The main tasks for this exercise are as follows:

1. Configure IP forwarding
2. Configure user defined routing
3. Configure routing on an Azure VM running Windows Server 2016

#### Task 1: Configure IP forwarding

1. In Microsoft Edge, navigate to the **20533E0201-nic1** blade.
2. On the **20533E0201-nic1** blade, modify the **IP configurations** by setting **IP forwarding** to **Enabled**.

#### Task 2: Configure user defined routing

1. In the Azure portal, create a new route table with the following settings:

* Name: **20533E02-rt1**
* Subscription: the name of your Azure subscription
* Resource group: **20533E0202-LabRG**
* Location: the same Azure region in which you created the virtual network 20533E0202-vnet
* BGP route propagation: **Disabled**

1. In the Azure portal, add to the route table a route with the following settings:

* 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. In the Azure portal, associate the route table with the **subnet-1** of the **20533E0202-vnet**.

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

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **20533E0201-vm1** Azure VM.
2. When prompted to authenticate, specify the following credentials:

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

1. Once you are connected to 20533E0201-vm1 via the Remote Desktop session, from **Server Manager**, install the **Remote Access** server role with the **Routing** role service and all required features.
2. In the Remote Desktop session to 20533E0201-vm1, start the **Routing and Remote Access** console.
3. In the **Routing and Remote Access** console, run **Routing and Remote Access Server Setup Wizard** and enable **LAN routing**.
4. Start **Routing and Remote Access** service.
5. In the Remote Desktop session to 20533E0201-vm1, start the **Windows Firewall with Advanced Security** console and enable **File and Printer Sharing (Echo Request - ICMPv4-In)** inbound rule for all profiles.

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

## Exercise 3: Validating virtual network connectivity

### Scenario

A. Datum now wants to validate the VNet peering configuration by testing connectivity between virtual machines on different virtual networks.

The main tasks for this exercise are as follows:

1. Configure Windows Firewall with Advanced Security on an Azure VM
2. Test service chaining between peered virtual networks
3. Remove the lab environment

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

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **20533E0201-vm2** Azure VM.
2. When prompted to authenticate, specify the following credentials:

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

1. In the Remote Desktop session to 20533E0201-vm2, start the **Windows Firewall with Advanced Security** console and enable **File and Printer Sharing (Echo Request - ICMPv4-In)** inbound rule for all profiles.

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

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **20533E0202-vm1** Azure VM.
2. When prompted to authenticate, specify the following credentials:

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

1. Once you are connected to 20533E0202-vm1 via the Remote Desktop session, start **Windows PowerShell**.
2. In the **Windows PowerShell** window, run the following:

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. Start **Windows PowerShell** as Administrator and, from the **Administrator: Windows PowerShell** window, run **Remove-20533EEnvironment**.
3. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. If you have multiple Azure subscriptions, select the one you want the script to target.
5. If prompted, specify the current lab number.
6. When prompted for confirmation, type **y**.
7. Start Microsoft Edge, browse to the Azure portal, and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
8. In the Azure portal, reset the dashboard to the default state.
9. Close all open windows.

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

**Question** What do you consider to be the most important advantages of VNet peering?

©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.