Configuring and Managing Virtual Networks

Lab: Configuring VNet peering and service chaining

Scenario

ADatum Corporation wants to implement service chaining between Azure virtual networks in its Azure subscription.

Objectives

After completing this lab, you will be able to:

- Deploy Azure VMs by using Azure Resource Manager templates.
- Configure VNet peering.
- Implement routing
- Validate service chaining

Lab Setup

Estimated Time: 45 minutes

User Name: **Student**

Password: **Pa55w.rd**

Exercise 1: Creating an Azure lab environment by using deployment templates

The main tasks for this exercise are as follows:

1. Create the first Azure virtual network environment by using an Azure Resource Manager template
2. Create the second Azure virtual network environment by using an Azure Resource Manager template

Task 1: Create the first Azure virtual network environment by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **Bash** session within the **Cloud Shell**.
3. If you are presented with the **You have no storage mounted** message, configure storage by clicking on **Show advanced settings** and using the following settings:
   - Subscription: the name of the target Azure subscription

- Cloud Shell region: the name of the Azure region that is available in your subscription and which is closest to the lab location
- Resource group: the name of a new resource group **az3000400-LabRG**
- Storage account: a name of a new storage account
- File share: a name of a new file share

4. From the Cloud Shell pane, create two resource groups by running (replace the `<Azure region>` placeholder with the name of the Azure region that is available in your subscription and which is closest to the lab location)

```
az group create --resource-group az3000401-LabRG \
--location <Azure region>

az group create --resource-group az3000402-LabRG \
--location <Azure region>
```

1. From the Cloud Shell pane, upload the first Azure Resource Manager template **C:\allfiles\AZ-300T02\Module_03\azuredeploy0401.json** into the home directory.

2. From the Cloud Shell pane, upload the parameter file **C:\allfiles\AZ-300T02\Module_03\azuredeploy04.parameters.json** into the home directory.

3. From the Cloud Shell pane, deploy the two Azure VMs hosting Windows Server 2016 Datacenter into the first virtual network by running:

```
az group deployment create --resource-group az3000401-LabRG \
--template-file azuredeploy0401.json \
--parameters @azuredeploy04.parameters.json

> **Note**: Deployment should take about 5 minutes.
```

Task 1: Create the second Azure virtual network environment by using an Azure Resource Manager template

1. From the Cloud Shell pane, upload the second Azure Resource Manager template **C:\allfiles\AZ-300T02\Module_03\azuredeploy0402.json** into the home directory.

2. From the Cloud Shell pane, deploy an Azure VM hosting Windows Server 2016 Datacenter into the second virtual network by running:

```
az group deployment create --resource-group az3000402-LabRG \
--template-file azuredeploy0402.json \
--parameters @azuredeploy04.parameters.json

> **Note**: The second template uses the same parameter file.

> **Note**: Deployment should take about 5 minutes.
```

Result: After completing this exercise, you should have created two Azure virtual networks hosting Azure VMs running Windows Server 2016 Datacenter.

Exercise 2: Configuring VNet peering

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. In the Microsoft Edge window displaying the Azure portal, navigate to the **az3000401-vnet** virtual network blade.
2. From the **az3000401-vnet** blade, create a VNet peering with the following settings:
   - Name: **az3000401-vnet-to-az3000402-vnet**
   - Virtual network deployment model: **Resource manager**
   - Subscription: the name of the Azure subscription you are using for this lab
   - Virtual network: **az3000402-vnet**
   - Allow virtual network access: **Enabled**
   - Allow forwarded traffic: disabled
   - 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 **az3000402-vnet** virtual network blade.
2. From the **az3000402-vnet** blade, create a VNet peering with the following settings:
   - Name: **az3000402-vnet-to-az3000401-vnet**
   - Virtual network deployment model: **Resource manager**
   - Subscription: the name of the Azure subscription you are using for this lab
   - Virtual network: **az3000401-vnet**
   - Allow virtual network access: **Enabled**
   - Allow forwarded traffic: disabled
   - Allow gateway transit: disabled
   - Use remote gateways: disabled

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

Exercise 3: Implementing routing

The main tasks for this exercise are as follows:

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

Task 1: Enable IP forwarding

1. In Microsoft Edge, navigate to the **az3000401-nic2** blade (the NIC of **az3000401-vm2**)
2. On the **az3000401-nic2** 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: **az3000402-rt1**
   - Subscription: the name of the Azure subscription you use for this lab
   - Resource group: **az3000402-LabRG**
   - Location: the same Azure region in which you created the virtual networks
   - BGP route propagation: **Disabled**
2. In the Azure portal, add to the route table a route with the following settings:
   - Route name: **custom-route-to-az3000401-vnet**
   - Address prefix: **10.0.0.0/22**
   - Next hop type: **Virtual appliance**
   - Next hop address: **10.0.1.4**
3. In the Azure portal, associate the route table with the **subnet-1** of the **az3000402-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 **az3000401-vm2** Azure VM.
2. When prompted to authenticate, specify the following credentials:
   - User name: **Student**
   - Password: **Pa55w.rd1234**

3. Once you are connected to az3000401-vm2 via the Remote Desktop session, from **Server Manager**, install the **Remote Access** server role with the **Routing** role service and all required features.

4. In the Remote Desktop session to az3000401-vm2, from Server Manager - Tools start the **Routing and Remote Access** console.

5. In the **Routing and Remote Access** console, run **Routing and Remote Access Server Setup Wizard** by right-clicking on **az3000401-vm1** and selecting **Configure and Enable Routing and Remote Access.** Click Next, then select Custom Configuration. Click Next again and select LAN routing. Click Next, then Finish.

6. When prompted click **Start Service** to start **Routing and Remote Access** service.

7. In the Remote Desktop session to az3000401-vm2, from Server Manager – Tools, start the **Windows Firewall with Advanced Security** console, select **Inbound Rules** and enable **File and Printer Sharing (Echo Request - ICMPv4-In)** inbound rule for all profiles.

Result: After completing this exercise, you should have configured custom routing within the second virtual network.

Exercise 4: Validating service chaining

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

Task 1: Configure Windows Firewall with Advanced Security on the target Azure VM

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **az3000401-vm1** Azure VM.

2. When prompted to authenticate, specify the following credentials:

   - User name: **Student**

   - Password: **Pa55w.rd1234**

3. In the Remote Desktop session to az3000401-vm1, from Server Manager – Tools, start the **Windows Firewall with Advanced Security** console, select **Inbound Rules** 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 **az3000402-vm1** Azure VM.

2. When prompted to authenticate, specify the following credentials:

   - User name: **Student**

   - Password: **Pa55w.rd1234**

3. Once you are connected to az3000402-vm1 via the Remote Desktop session, start **Windows PowerShell**.

4. In the **Windows PowerShell** window, run the following:

```
Test-NetConnection -ComputerName 10.0.0.4 -TraceRoute
```

1. Verify that test is successful and note that the connection was routed over 10.0.1.4

Result: After completing this exercise, you should have validated service chaining between peered virtual networks.