Module 3 - Lab 4: Route network traffic with a route table using the Azure portal

> ❓ Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. Custom routes are helpful when, for example, you want to route traffic between subnets through a network virtual appliance (NVA). In this lab, you learn how to:
>
> - Create an NVA that routes traffic
> - Create a route table
> - Create a route
> - Associate a route table to a subnet
> - Deploy virtual machines (VM) into different subnets
> - Route traffic from one subnet to another through an NVA

Task 1: Create an NVA

> ❓ Network virtual appliances (NVAs) are virtual machines that help with network functions, such as routing and firewall optimization. This tutorial assumes you're using **Windows Server 2016 Datacenter**. You can select a different operating system if you want.

☐ 1. Login to the Azure Portal 📄 **https://portal.azure.com** with the username 📄 **sheikhnasirLXQMJ@gdcs2.com** and password 📄 **slfRj3jpSqHpnymh**.

☐ 2. Choose **Windows Server 2016 Datacenter**.
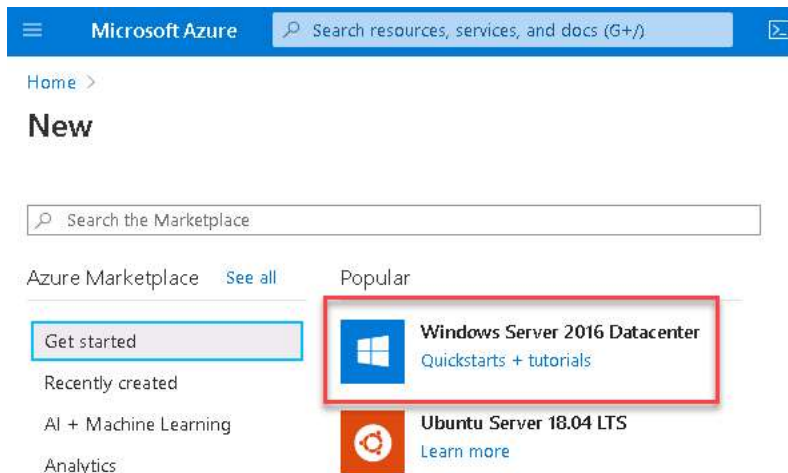
☐ 3. In the **Create a virtual machine** page, under **Basics**, enter or select this information:

Section	Setting	Action
Project details	Subscription	**CloudShare2**
	Resource group	**myResourceGroup-W1HR8Q1R85**
Instance details	Virtual machine name	📄 **myVmNva**
	Region	Choose **(US) East US**.
	Availability options	Choose **No infrastructure redundancy required**.
	Image	Choose **Windows Server 2016 Datacenter Gen2**.
	Size	**Standard DS1 v2**.
Administrator account	Username	📄 **localadmin**
	Password	📄 **slfRj3jpSqHpnymh**
	Confirm Password	Enter the password again 📄 **slfRj3jpSqHpnymh**
Inbound port rules	Public inbound ports	Pick **None**.
Save money	Already have a Windows Server license?	Pick **No**.

Then select **Next : Disks >**.

☐ 4. Under **Disks**, select the settings that are right for your needs, and then select **Next : Networking >**.

☐ 5. Under **Networking**:

      1. For **Virtual network**, select **Create new**.

      2. In the **Create virtual network** dialog box, under **Name**, enter 🔲 **myVirtualNetwork**.

      3. In **Address space**, replace the existing address range with 🔲 **10.0.0.0/16**

4. In **Subnets**, select the **Delete** icon to delete the existing subnet, and then enter the following combinations of **Subnet name** and **Address range**. Once a valid name and range is entered, a new empty row appears below it.

Subnet name	Address range
📄 Public	📄 10.0.0.0/24
📄 Private	📄 10.0.1.0/24
📄 DMZ	📄 10.0.2.0/24

5. Select **OK** to exit the dialog box.

6. In **Subnet**, choose **DMZ (10.0.2.0/24)**.

7. In **Public IP**, choose **None**, since this VM won't connect over the internet.

8. Select **Next : Management >**.

6. Under **Management**:

1. Select **Enable with customer storage account**.

2. In **Diagnostics storage account**, select **Create New**.

3. In the **Create storage account** dialog box, enter or select this information:

Setting	Value
Name	📄 **mynvastorageaccount**
Account kind	**Storage (general purpose v1)**
Performance	**Standard**
Replication	**Locally-redundant storage (LRS)**

4. Select **OK** to exit the dialog box.

5. Select **Review + create**. You're taken to the **Review + create** page, and Azure validates your configuration.

7. When you see the **Validation passed** message, select **Create**.

The VM takes a few minutes to create. Wait until Azure finishes creating the VM. The **Your deployment is underway** page shows you deployment details.

8. When your VM is ready, select **Go to resource**.

Task 2: Create a route table

1. In the Azure portal menu or from the **Home** page, select **Create a resource**.

2. In the search box, enter 📄 **Route table**. When **Route table** appears in the search results, select it.

3. In the **Route table** page, select **Create**.

4. In **Create route table**, enter or select this information:

Setting	Value
Name	📄 **myRouteTablePublic**
Subscription	**CloudShare2**
Resource group	**myResourceGroup-W1HR8Q1R85**
Location	**(US) East US**
Propagate gateway routes	**Yes**

Home > New > Route table > Create route table

Create route table □ ✕
You can add routes to this table after it's created.

Name *
myRouteTablePublic ✓

Subscription *
Contoso ▾

Resource group *
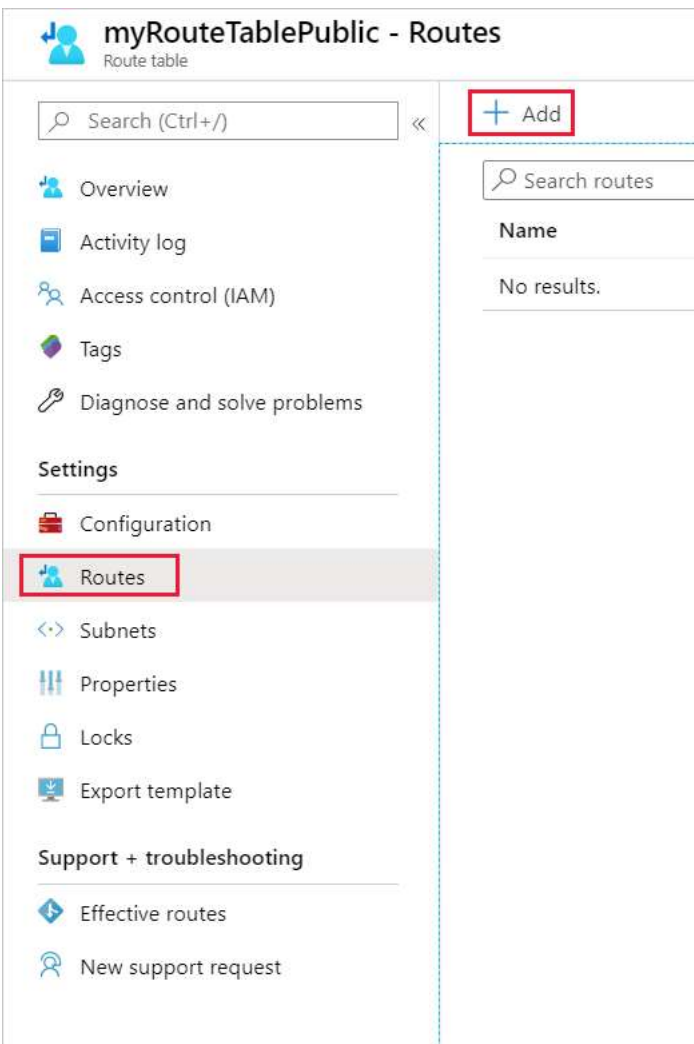myResourceGroup ▾
Create new

Location *
(US) East US ▾

Virtual network gateway route propagation
Disabled **Enabled**

Create   Automation options

☐ 5. Select **Review + Create** then **Create**.

Task 3: Create a route

☐ 1. Return to the Azure portal to manage your route table. Search for and select 🔲 **Route tables**.

☐ 2. Pick the name of your route table (**myRouteTablePublic**).

☐ 3. Choose **Routes** > **Add**.

4. In **Add route**, enter or select this information:

Setting	Value
Route name	📄 **ToPrivateSubnet**
Address prefix	📄 **10.0.1.0/24** (the address range of the *Private* subnet created earlier)
Next hop type	**Virtual appliance**
Next hop address	📄 **10.0.2.4** (an address within the address range of the *DMZ* subnet)

☐ 5. Select **OK**.

Task 4: Associate a route table to a subnet

☐ 1. Return to the Azure portal to manage your virtual network. Search for and select 📄 **Virtual networks**.

☐ 2. Pick the name of your virtual network **myVirtualNetwork**.

☐ 3. In the virtual network's menu bar, choose **Subnets**.

☐ 4. In the virtual network's subnet list, choose **Public**.

☐ 5. In **Route table**, choose the route table you created (**myRouteTablePublic**), and then select **Save** to associate your route table to the *Public* subnet.

Task 5: Turn on IP forwarding

> ❓ Next, turn on IP forwarding for your new NVA virtual machine, *myVmNva*. When Azure sends network traffic to *myVmNva*, if the traffic is destined for a different IP address, IP forwarding sends the traffic to the correct location.

☐ 1. Return to the Azure portal to manage your VM. Search for and select **Virtual machines**.

☐ 2. Pick the name of your VM (**myVmNva**).

☐ 3. In your NVA virtual machine's menu bar, select **Networking**.

☐ 4. Select **myvmnva(xxxx)**. That's the network interface Azure created for your VM. Azure adds numbers to ensure a unique name.

5. In the network interface menu bar, select **IP configurations**.

6. In the **IP configurations** page, set **IP forwarding** to **Enabled**, and select **Save**.

Task 6: Create public and private virtual machines

> ❓ Create a public VM and a private VM in the virtual network. Later, you'll use them to see that Azure routes the *Public* subnet traffic to the *Private* subnet through the NVA.
>
> To create the public VM and the private VM, follow the steps of Create an NVA task earlier. You don't need to wait for deployment to finish or go to the VM resource. You'll use most of the same settings, except as described below.
>
> Before you select **Create** to create the public or private VM, go to the following two subsections Public VM and Private VM, which show the values that have to be different. You may continue to the next section Route traffic through an NVA after Azure finishes deploying both VMs.

☐ 1. **Public VM**

Tab	Setting	Value
Basics	Resource group	**myResourceGroup-W1HR8Q1R85**
	Virtual machine name	📋 **myVmPublic**
	Public inbound ports	**Allow selected ports**
	Select inbound ports	**RDP**
Networking	Virtual network	**myVirtualNetwork**
	Subnet	**Public 📋 (10.0.0.0/24)**
	Public IP address	The default
Administrator account	Username	📋 **localadmin**
	Password	📋 **sIfRj3jpSqHpnymh**
	Confirm Password	Enter the password again 📋 **sIfRj3jpSqHpnymh**
Management	Diagnostics storage account	**mynvastorageaccount**

☐ 2. **Private VM**

Tab	Setting	Value
Basics	Resource group	**myResourceGroup-W1HR8Q1R85**
	Virtual machine name	📋 **myVmPrivate**
	Public inbound ports	**Allow selected ports**
	Select inbound ports	**RDP**
Networking	Virtual network	**myVirtualNetwork**
	Subnet	**Private (10.0.1.0/24)**
	Public IP address	The default
Administrator account	Username	📋 **localadmin**
	Password	📋 **sIfRj3jpSqHpnymh**
	Confirm Password	Enter the password again 📋 **sIfRj3jpSqHpnymh**
Management	Diagnostics storage account	**mynvastorageaccount**

Task 7: Sign in to myVmPrivate over remote desktop

☐ 1. Go to the Azure portal to manage your private VM. Search for and select **Virtual machines**.

☐ 2. Pick the name of your private VM (**myVmPrivate**).

☐ 3. In the VM menu bar, select **Connect** to create a remote desktop connection to the private VM.

☐ 4. In the **Connect with RDP** page, select **Download RDP File**. Azure creates a Remote Desktop Protocol (*.rdp*) file and downloads it to your computer.

☐ 5. Open the downloaded *.rdp* file. If prompted, select **Connect**. Select **More choices** > **Use a different account**, and then enter the user name and password you specified when creating the private VM.

☐ 6. Login using username 📋 **localadmin** and Password 📋 **sIfRj3jpSqHpnymh**

☐ 7. Select **OK**.

☐ 8. If you receive a certificate warning during the sign-in process, select **Yes** to connect to the VM.

Task 8: Enable ICMP through the Windows firewall

> ⓘ In a later step, you'll use the trace route tool to test routing. Trace route uses the Internet Control Message Protocol (ICMP), which the Windows Firewall denies by default. Enable ICMP through the Windows firewall.

☐ 1. In the Remote Desktop of *myVmPrivate*, open PowerShell.

☐ 2. Enter this command:

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

You'll be using trace route to test routing in this tutorial. For production environments, we don't recommend allowing ICMP through the Windows Firewall.

Task 9: Turn on IP forwarding within myVmNva

> ⓘ You **turned on IP forwarding** for the VM's network interface using Azure. The VM's operating system also has to forward network traffic. Turn on IP forwarding for *myVmNva* VM's operating system with these commands.

☐ 1. From a command prompt on the *myVmPrivate* VM, open a remote desktop to the *myVmNva* VM:

```
mstsc /v:myvmnva
```

☐ 2. Login using username 🔑 **localadmin** and Password 🔑 **sIfRj3jpSqHpnymh**

☐ 3. From PowerShell on the *myVmNva* VM, enter this command to turn on IP forwarding:

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name IpEnableRouter -Value 1
```

☐ 4. Restart the *myVmNva* VM: From the taskbar, select **Start** > **Power**, **Other (Planned)** > **Continue**.

This also disconnects the remote desktop session.

☐ 5. After the *myVmNva* VM restarts, create a remote desktop session to the *myVmPublic* VM. While still connected to the *myVmPrivate* VM, open a command prompt and run this command:

```
mstsc /v:myVmPublic
```

☐ 6. Login using username 🔑 **localadmin** and Password 🔑 **sIfRj3jpSqHpnymh**

☐ 7. In the remote desktop of *myVmPublic*, open PowerShell.

☐ 8. Enable ICMP through the Windows firewall by entering this command:

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

Task 10: Test the routing of network traffic

> ⓘ First, let's test routing of network traffic from the *myVmPublic* VM to the *myVmPrivate* VM.

☐ 1. From PowerShell on the *myVmPublic* VM, enter this command:

```
tracert myVmPrivate
```

The response is similar to this example:

```
Tracing route to myVmPrivate.vpgub4nqnocezhjgurw44dnxrc.bx.internal.cloudapp.net [10.0.1.4]
over a maximum of 30 hops:

1    <1 ms    *        1 ms  10.0.2.4
2     1 ms    1 ms     1 ms  10.0.1.4

Trace complete.
```

You can see the first hop is to 10.0.2.4, which is NVA's private IP address. The second hop is to the private IP address of the *myVmPrivate* VM: 10.0.1.4. Earlier, you added the route to the *myRouteTablePublic* route table and associated it to the *Public* subnet. As a result, Azure sent the traffic through the NVA and not directly to the *Private* subnet.

☐ 2. Close the remote desktop session to the *myVmPublic* VM, which leaves you still connected to the *myVmPrivate* VM.

☐ 3. From a command prompt on the *myVmPrivate* VM, enter this command:

```
tracert myVmPublic
```

This command tests the routing of network traffic from the *myVmPrivate* VM to the *myVmPublic* VM. The response is similar to this example:

```
Tracing route to myVmPublic.vpgub4nqnocezhjgurw44dnxrc.bx.internal.cloudapp.net [10.0.0.4]
over a maximum of 30 hops:

1     1 ms     1 ms     1 ms  10.0.0.4

Trace complete.
```

You can see that Azure routes traffic directly from the *myVmPrivate* VM to the *myVmPublic* VM. By default, Azure routes traffic directly between subnets.

4. Close the remote desktop session to the *myVmPrivate* VM.