Homework 11 – Lab 06 - Implement Traffic Management
Velibor Stanisic

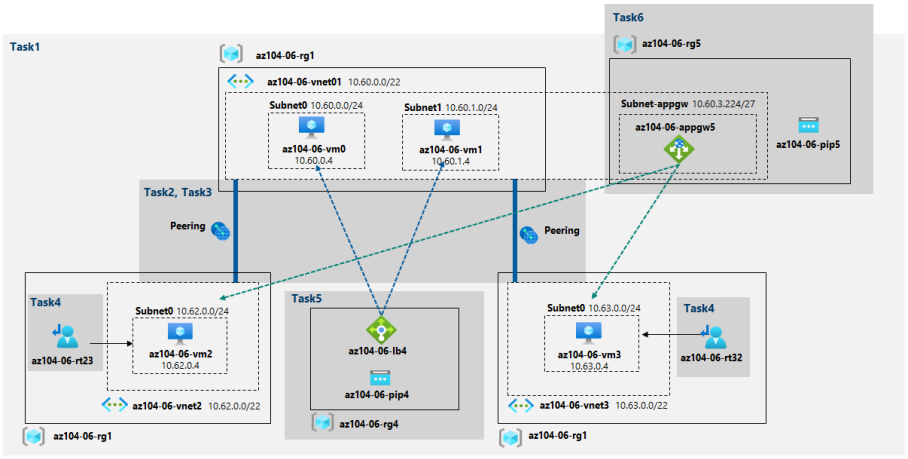
Lab scenario

You were tasked with testing managing network traffic targeting Azure virtual machines in the hub and spoke network topology, which Contoso considers implementing in its Azure environment (instead of creating the mesh topology, which you tested in the previous lab). This testing needs to include implementing connectivity between spokes by relying on user defined routes that force traffic to flow via the hub, as well as traffic distribution across virtual machines by using layer 4 and layer 7 load balancers. For this purpose, you intend to use Azure Load Balancer (layer 4) and Azure Application Gateway (layer 7).

Objectives

In this lab, you will:

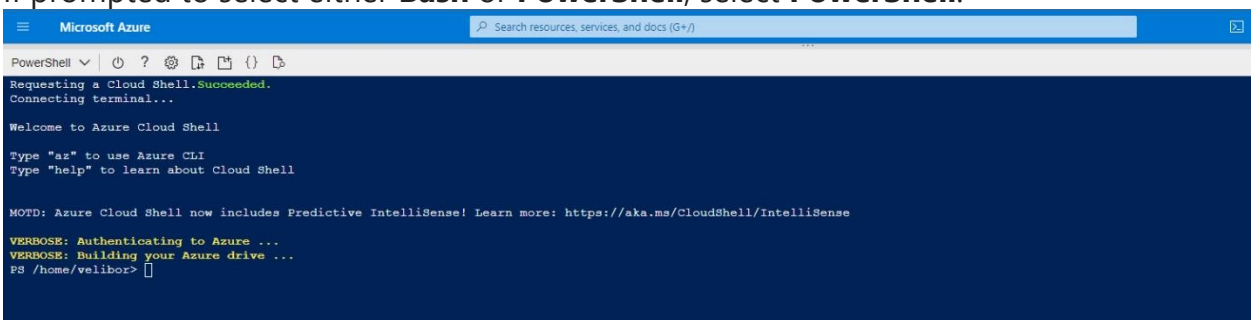
- Task 1: Provision the lab environment
- Task 2: Configure the hub and spoke network topology
- Task 3: Test transitivity of virtual network peering
- Task 4: Configure routing in the hub and spoke topology
- Task 5: Implement Azure Load Balancer
- Task 6: Implement Azure Application Gateway



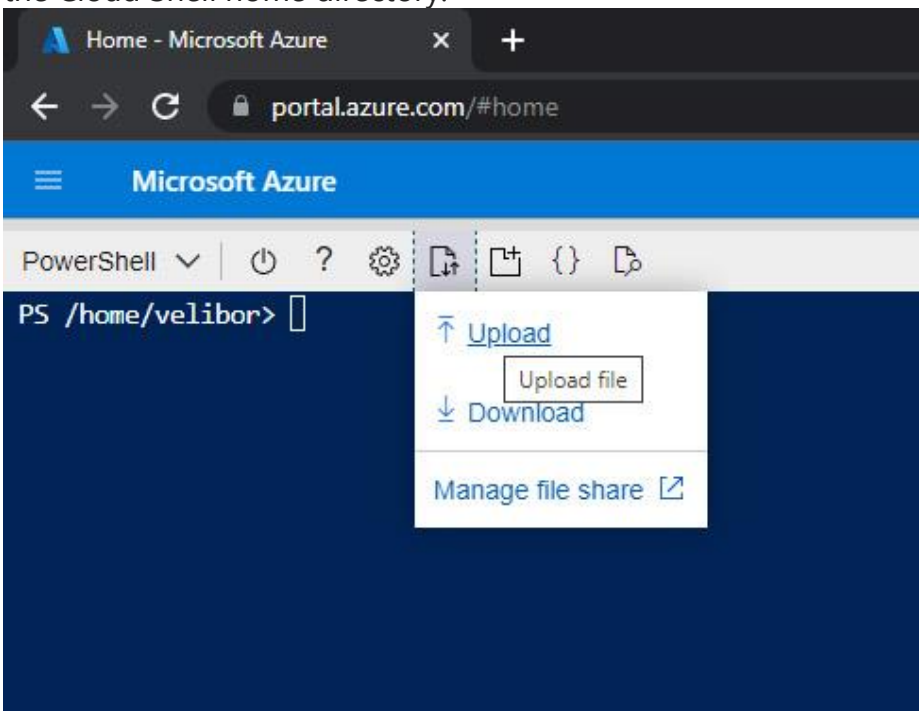
Task 1: Provision the lab environment

In this task, you will deploy four virtual machines into the same Azure region. The first two will reside in a hub virtual network, while each of the remaining two will reside in a separate spoke virtual network.

1. Sign in to the Azure portal.
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.



4. In the toolbar of the Cloud Shell pane, click the **Upload/Download files** icon, in the drop-down menu, click **Upload** and upload the files **\Allfiles\Labs\06\az104-06-vms-loop-template.json** and **\Allfiles\Labs\06\az104-06-vms-loop-parameters.json** into the Cloud Shell home directory.



5. Edit the **Parameters** file you just uploaded and change the password. If you need help editing the file in the Shell please ask your instructor for assistance. As a best practice, secrets, like passwords, should be more securely stored in the Key Vault.
6. From the Cloud Shell pane, run the following to create the first resource group that will be hosting the lab environment (replace the '[Azure_region]' placeholder with the name of an Azure region where you intend to deploy Azure virtual machines)(you can use the "(Get-AzLocation).Location" cmdlet to get the region list):

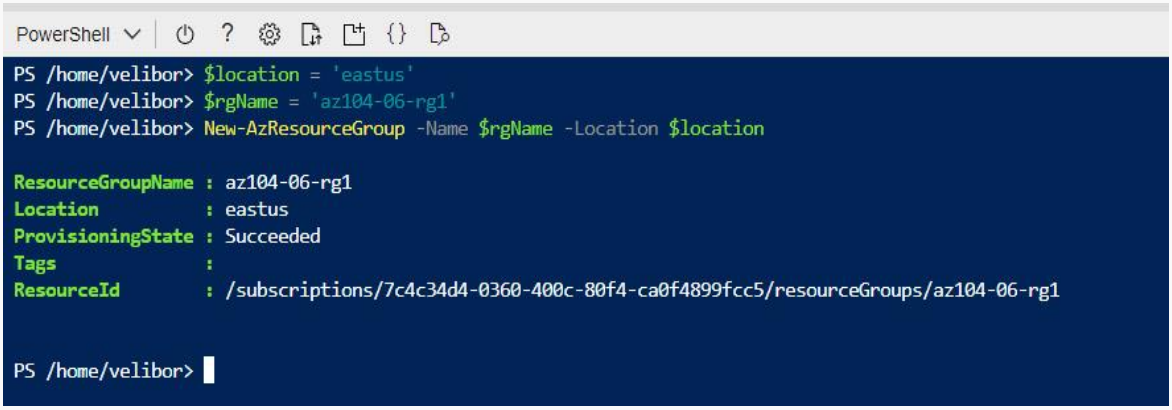
```
$location = 'eastus'
```

Now the resource group name:

```
$rgName = 'az104-06-rg1'
```

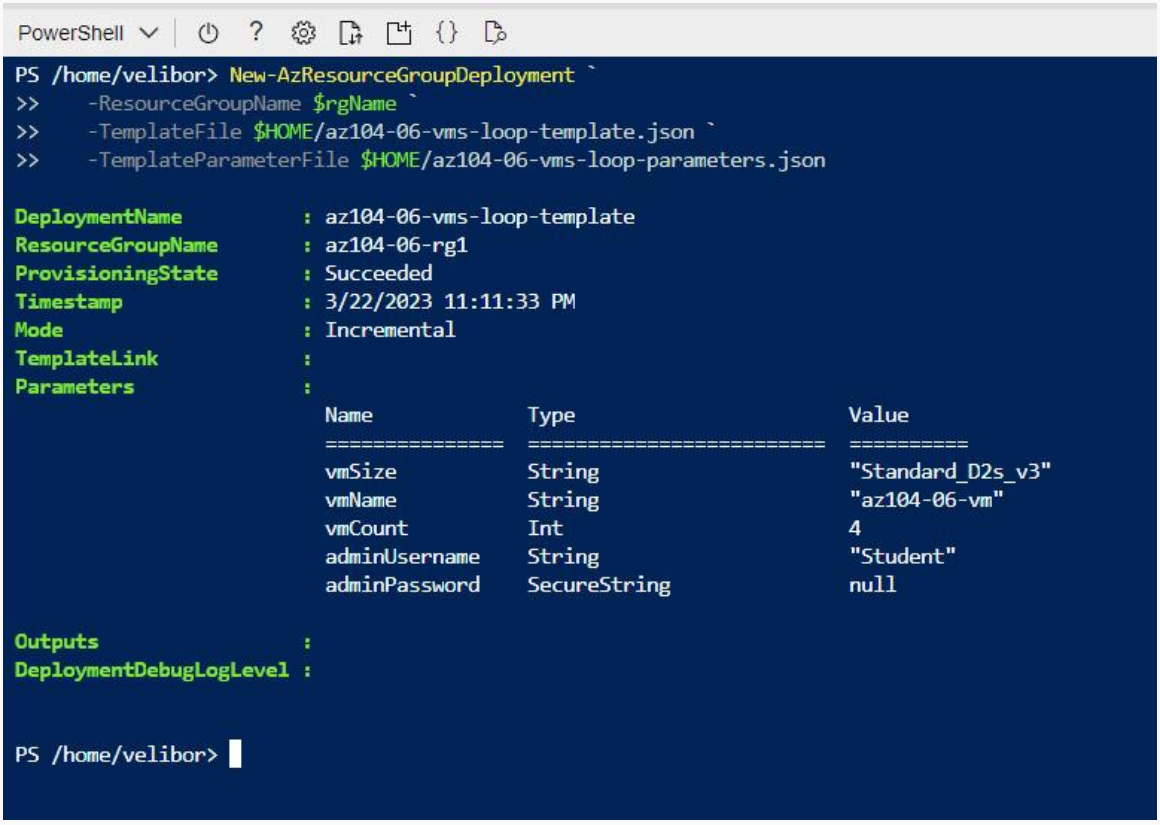
And finally create the resource group in your desired location:

```
New-AzResourceGroup -Name $rgName -Location $location
```



7. From the Cloud Shell pane, run the following to create the three virtual networks and four Azure VMs into them by using the template and parameter files you uploaded:

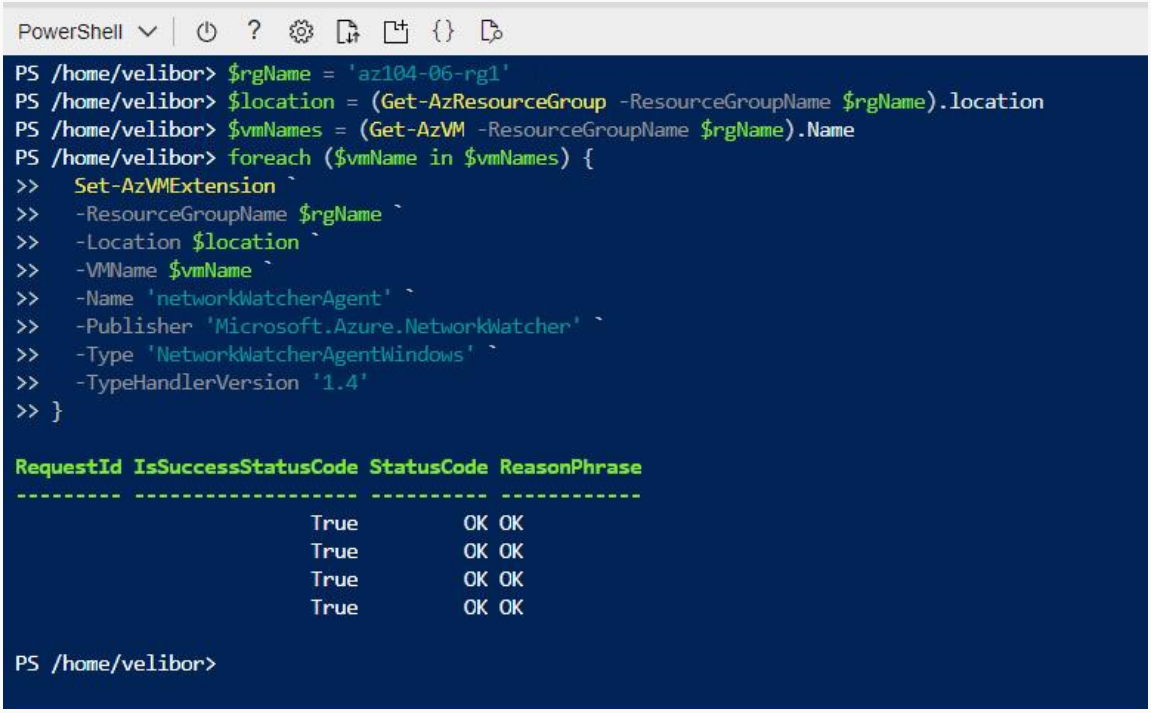
```
New-AzResourceGroupDeployment `
   -ResourceGroupName $rgName `
   -TemplateFile $HOME/az104-06-vms-loop-template.json `
   -TemplateParameterFile $HOME/az104-06-vms-loop-parameters.json
```



8. From the Cloud Shell pane, run the following to install the Network Watcher extension on the Azure VMs deployed in the previous step:

```
$rgName = 'az104-06-rg1'
$location = (Get-AzResourceGroup -ResourceGroupName $rgName).location
$vmNames = (Get-AzVM -ResourceGroupName $rgName).Name

foreach ($vmName in $vmNames) {
  Set-AzVMExtension `
  -ResourceGroupName $rgName `
  -Location $location `
  -VMName $vmName `
  -Name 'networkWatcherAgent' `
  -Publisher 'Microsoft.Azure.NetworkWatcher' `
  -Type 'NetworkWatcherAgentWindows' `
  -TypeHandlerVersion '1.4'
}
```

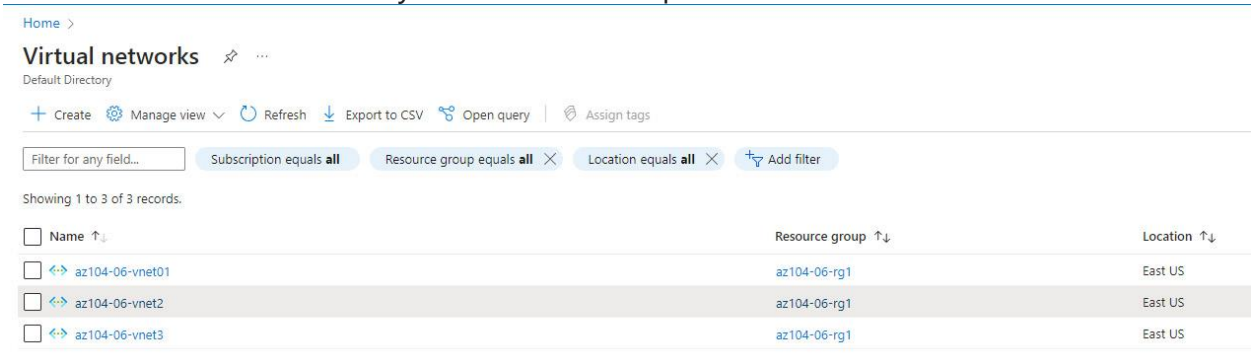


9. Close the Cloud Shell pane.

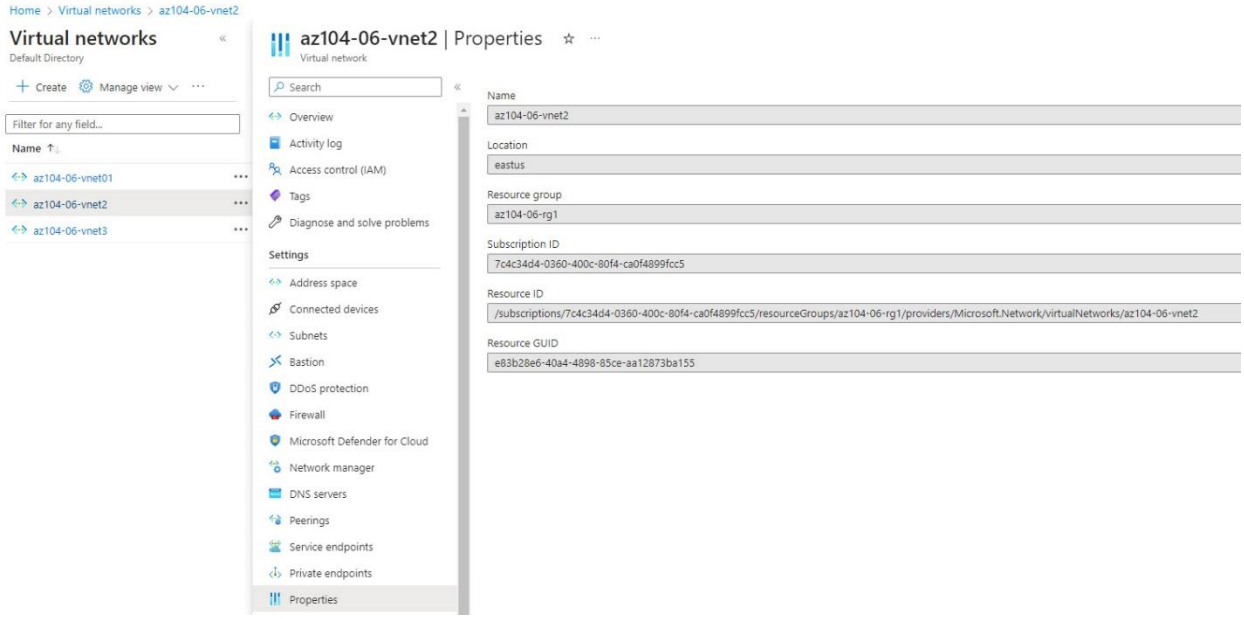
Task 2: Configure the hub and spoke network topology

In this task, you will configure local peering between the virtual networks you deployed in the previous tasks in order to create a hub and spoke network topology.

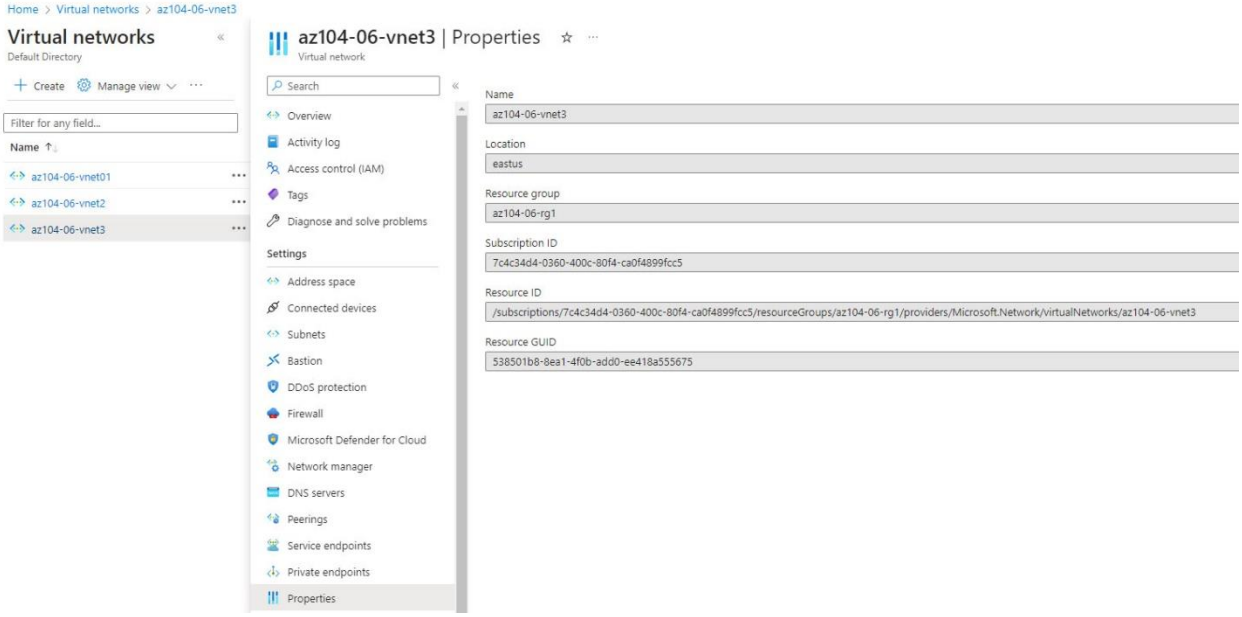
1. In the Azure portal, search for and select **Virtual networks**.
2. Review the virtual networks you created in the previous task.



3. In the list of virtual networks, select **az104-06-vnet2**.
4. On the **az104-06-vnet2** blade, select **Properties**.
5. On the **az104-06-vnet2 | Properties** blade, record the value of the **Resource ID** property.



6. Navigate back to the list of virtual networks and select **az104-06-vnet3**.
7. On the **az104-06-vnet3** blade, select **Properties**.
8. On the **az104-06-vnet3 | Properties** blade, record the value of the **Resource ID** property.



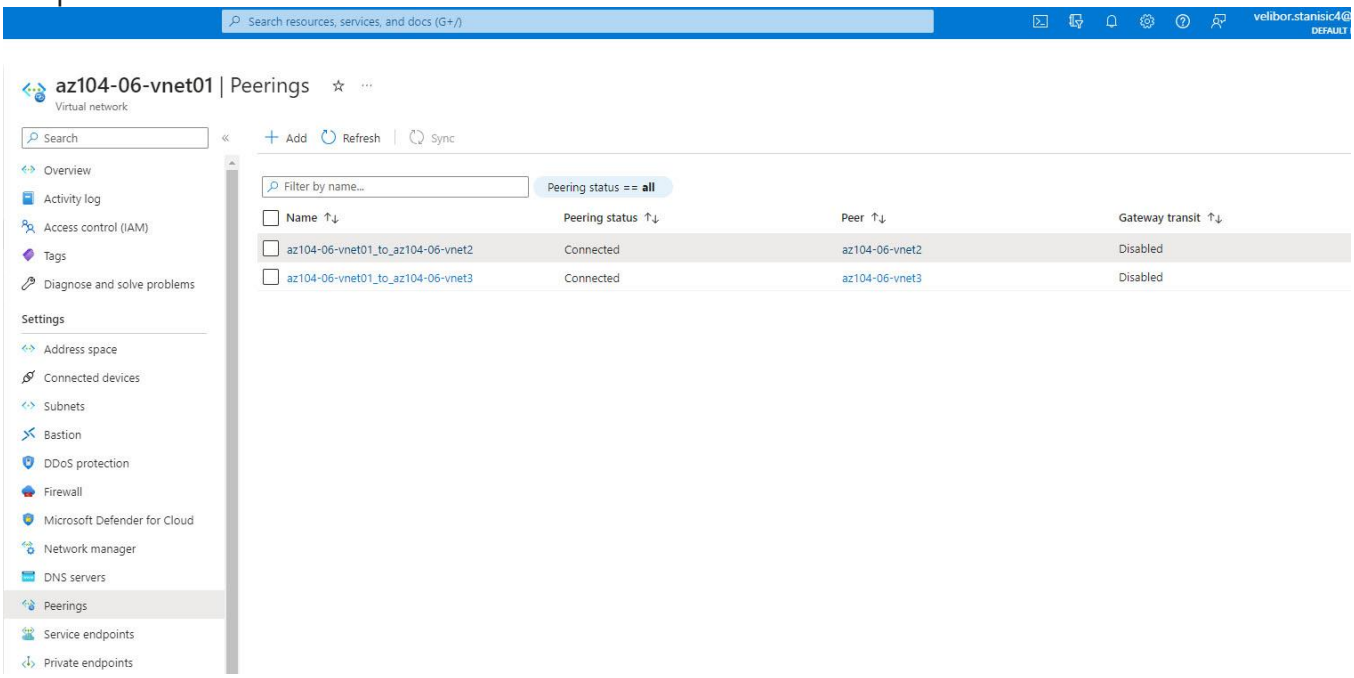
9. In the list of virtual networks, click **az104-06-vnet01**.
10. On the **az104-06-vnet01** virtual network blade, in the **Settings** section, click **Peerings** and then click **+ Add**.
11. Add a peering with the following settings (leave others with their default values) and click **Add**:

Setting	Value
This virtual network: Peering link name	**az104-06-vnet01_to_az104-06-vnet2**
Traffic to remote virtual network	**Allow (default)**
Traffic forwarded from remote virtual network	**Block traffic that originates from outside this virtual network**
Virtual network gateway	**None (default)**
Remote virtual network: Peering link name	**az104-06-vnet2_to_az104-06-vnet01**
Virtual network deployment model	**Resource manager**
I know my resource ID	enabled
Resource ID	the value of resourceID parameter of **az104-06-vnet2** you recorded earlier in this task
Traffic to remote virtual network	**Allow (default)**
Traffic forwarded from remote virtual network	**Allow (default)**
Virtual network gateway	**None (default)**

12. On the **az104-06-vnet01** virtual network blade, in the **Settings** section, click **Peerings** and then click **+ Add**.
13. Add a peering with the following settings (leave others with their default values) and click **Add**:

Setting	Value
This virtual network: Peering link name	**az104-06-vnet01_to_az104-06-vnet3**
Traffic to remote virtual network	**Allow (default)**
Traffic forwarded from remote virtual network	**Block traffic that originates from outside this virtual network**
Virtual network gateway	**None (default)**
Remote virtual network: Peering link name	**az104-06-vnet3_to_az104-06-vnet01**
Virtual network deployment model	**Resource manager**
I know my resource ID	enabled
Resource ID	the value of resourceID parameter of **az104-06-vnet3** you recorded earlier in this task
Traffic to remote virtual network	**Allow (default)**
Traffic forwarded from remote virtual network	**Allow (default)**
Virtual network gateway	**None (default)**

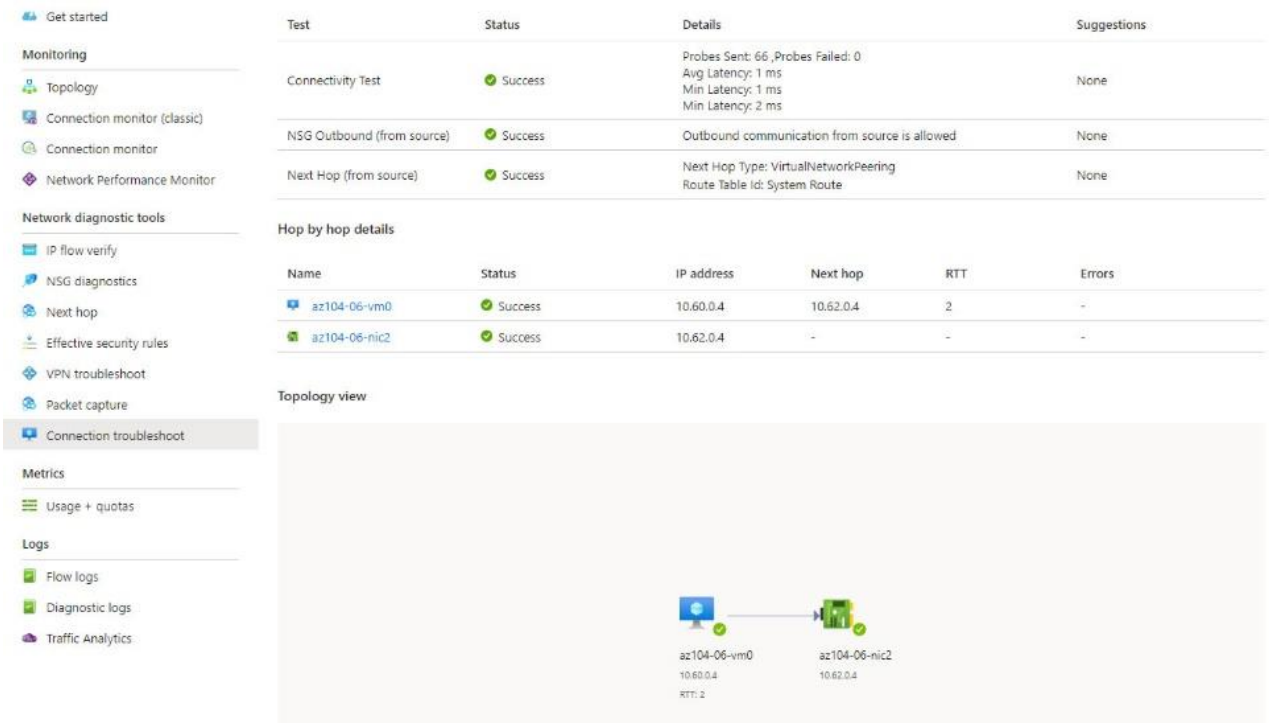
Output:



Task 3: Test transitivity of virtual network peering

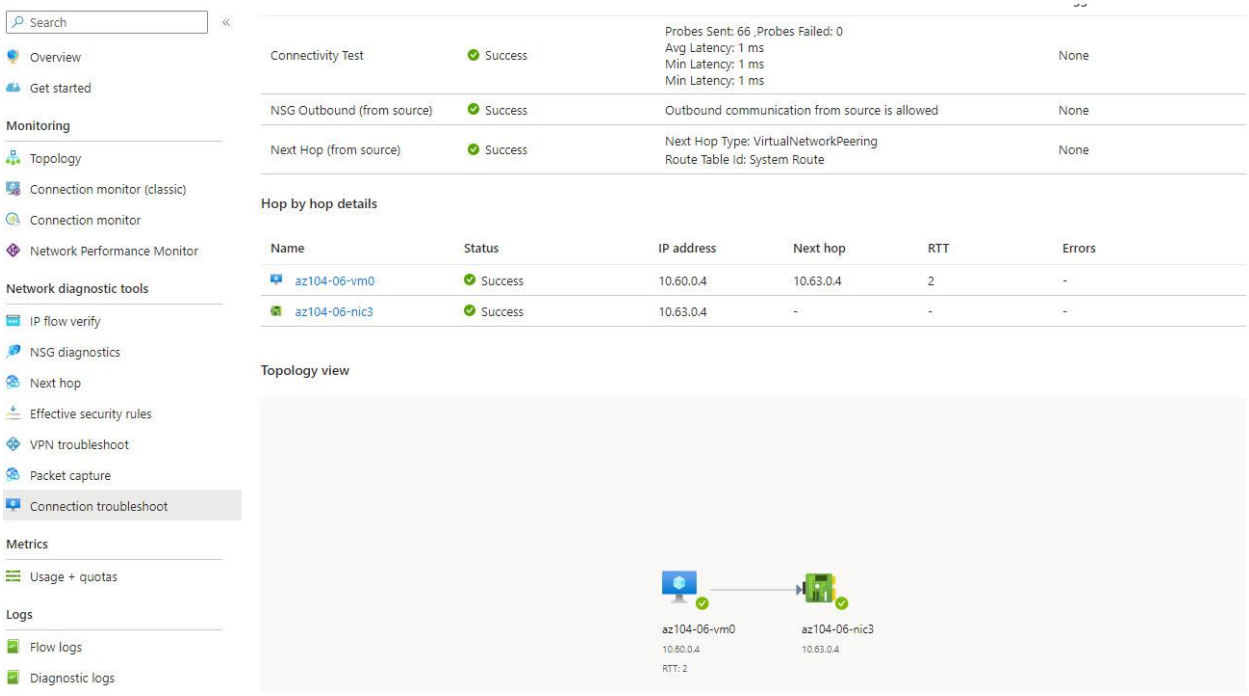
In this task, you will test transitivity of virtual network peering by using Network Watcher.

1. In the Azure portal, search for and select **Network Watcher**.
2. On the **Network Watcher** blade, expand the listing of Azure regions and verify the service is enabled in region you are using.
3. On the **Network Watcher** blade, navigate to the **Connection troubleshoot**.
4. On the **Network Watcher - Connection troubleshoot** blade, initiate a check with the following settings (leave others with their default values):
5. Click **Check** and wait until results of the connectivity check are returned. Verify that the status is **Reachable**. Review the network path and note that the connection was direct, with no intermediate hops in between the VMs.

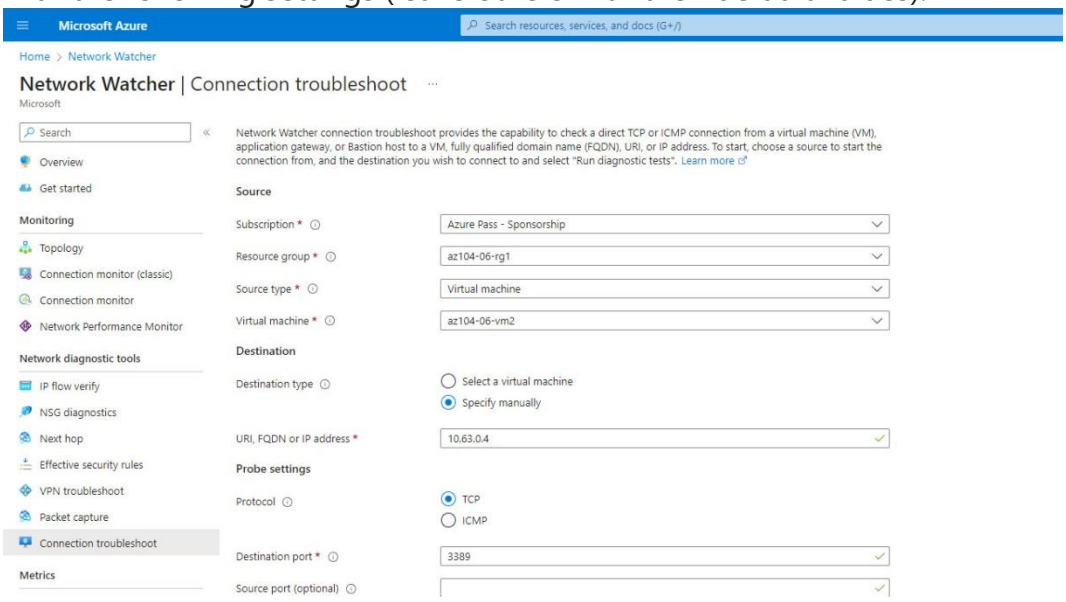


6. On the **Network Watcher - Connection troubleshoot** blade, initiate a check with the following settings (leave others with their default values):

7. Click **Check** and wait until results of the connectivity check are returned. Verify that the status is **Reachable**. Review the network path and note that the connection was direct, with no intermediate hops in between the VMs.



8. On the **Network Watcher - Connection troubleshoot** blade, initiate a check with the following settings (leave others with their default values):

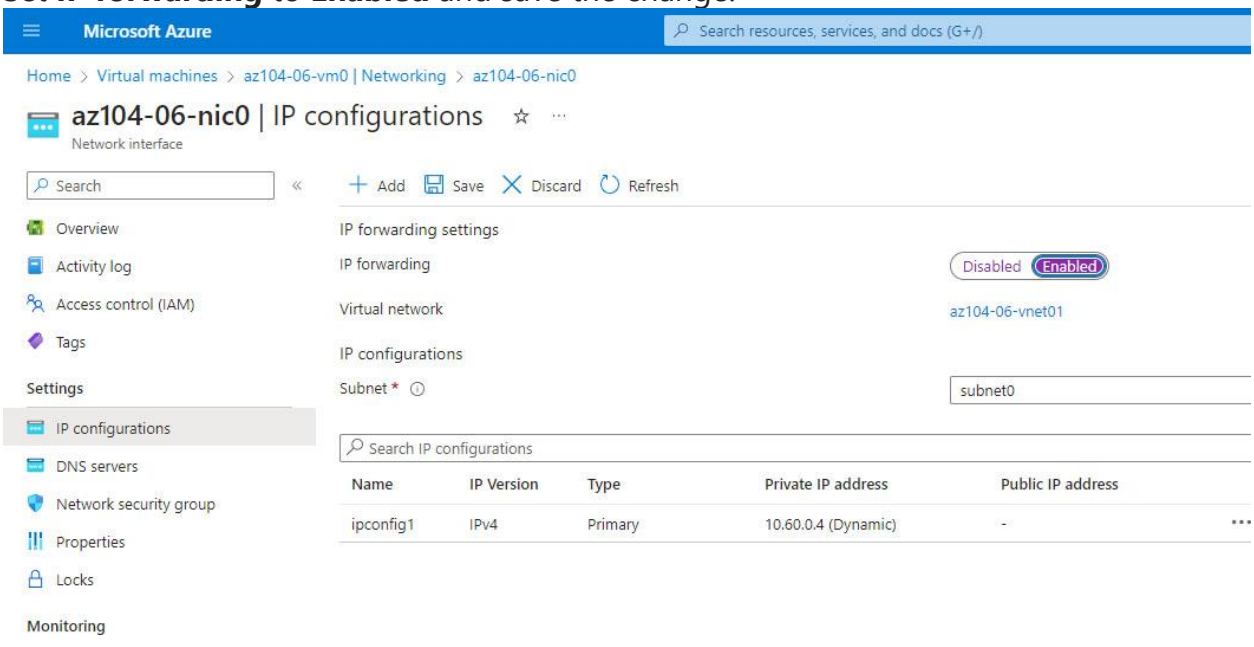


9. Click **Check** and wait until results of the connectivity check are returned. Note that the status is **Unreachable**.

Task 4: Configure routing in the hub and spoke topology

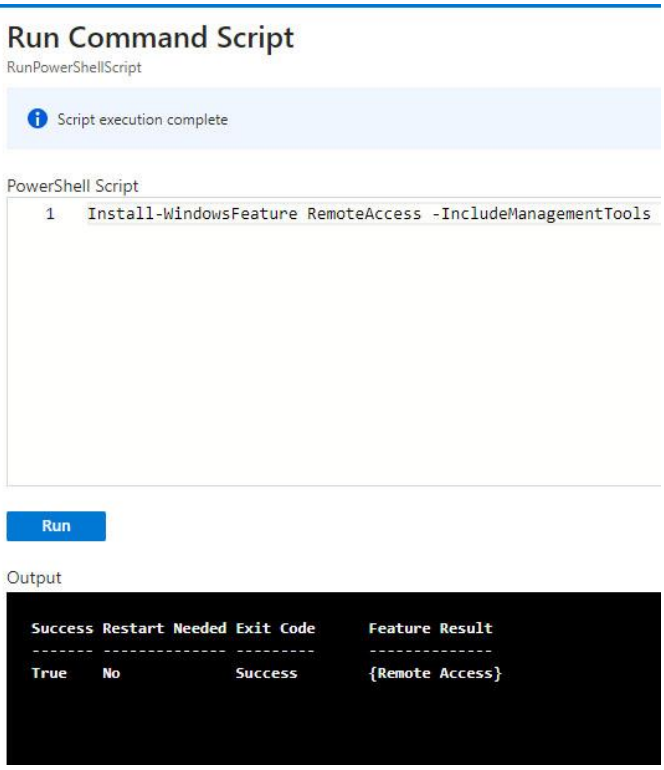
In this task, you will configure and test routing between the two spoke virtual networks by enabling IP forwarding on the network interface of the **az104-06-vm0** virtual machine, enabling routing within its operating system, and configuring user-defined routes on the spoke virtual network.

1. In the Azure portal, search and select **Virtual machines**.
2. On the **Virtual machines** blade, in the list of virtual machines, click **az104-06-vm0**.
3. On the **az104-06-vm0** virtual machine blade, in the **Settings** section, click **Networking**.
4. Click the **az104-06-nic0** link next to the **Network interface** label, and then, on the **az104-06-nic0** network interface blade, in the **Settings** section, click **IP configurations**.
5. Set **IP forwarding** to **Enabled** and save the change.

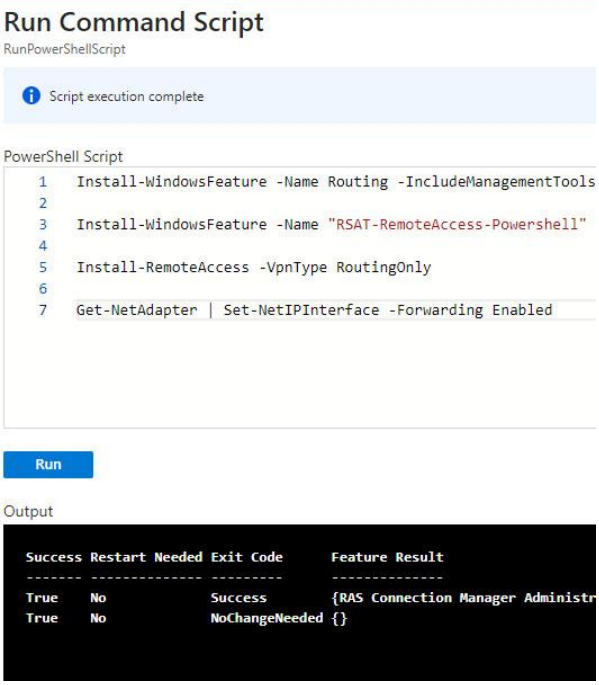


6. In the Azure portal, navigate back to the **az104-06-vm0** Azure virtual machine blade and click **Overview**.
7. On the **az104-06-vm0** blade, in the **Operations** section, click **Run command**, and, in the list of commands, click **RunPowerShellScript**.

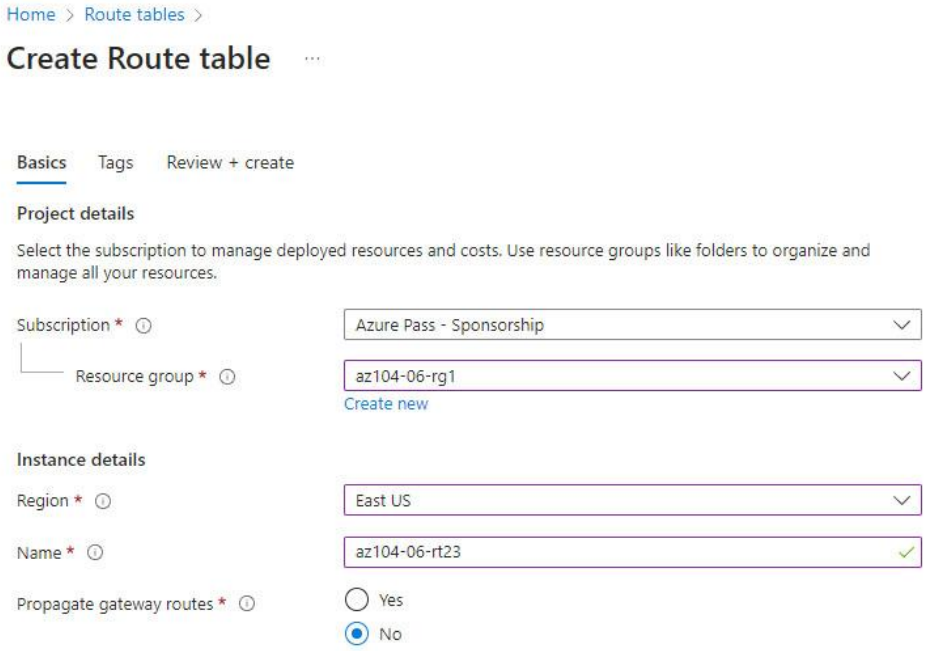
8. On the **Run Command Script** blade, type the following and click **Run** to install the Remote Access Windows Server role.



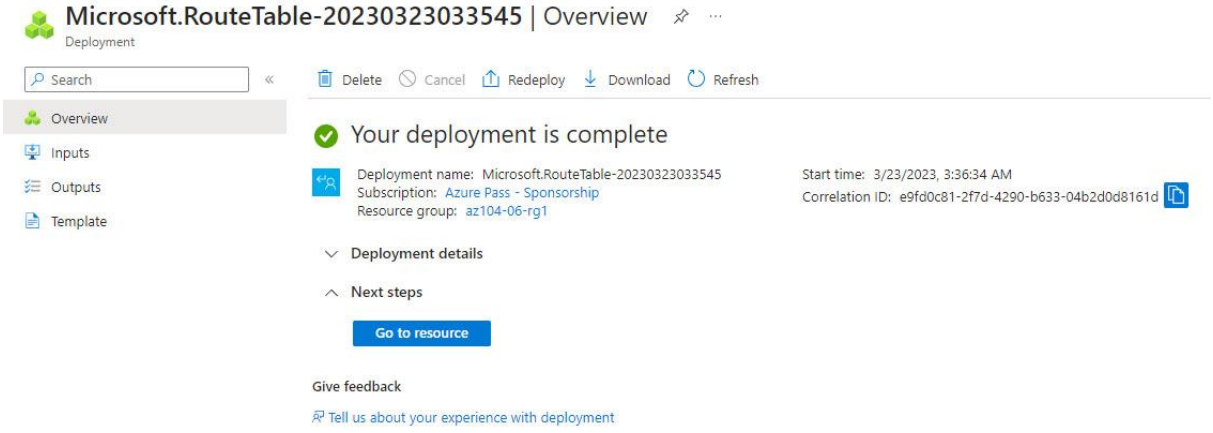
9. On the **Run Command Script** blade, type the following and click **Run** to install the Routing role service.



10. In the Azure portal, search and select **Route tables** and, on the **Route tables** blade, click **+ Create**.
11. Create a route table with the following settings (leave others with their default values):

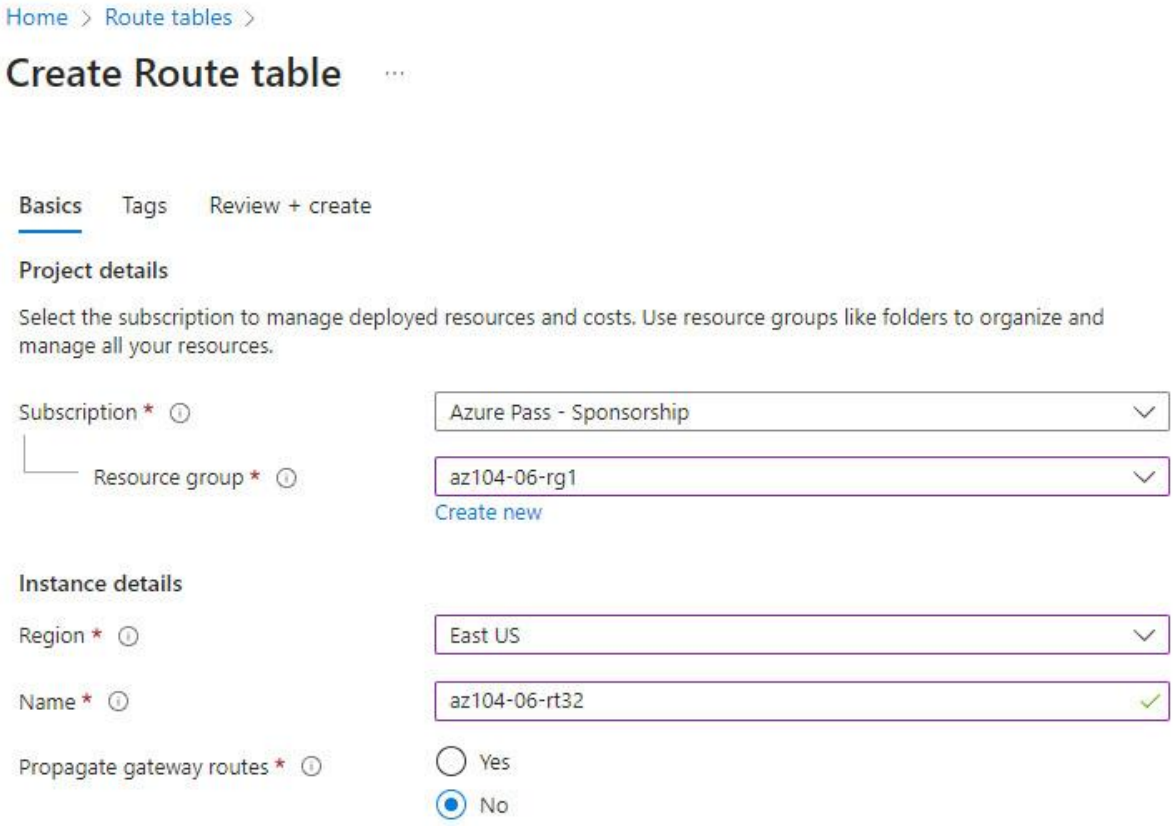


12. Click **Review and Create**. Let validation occur, and click **Create** to submit your deployment.
13. Click **Go to resource**.



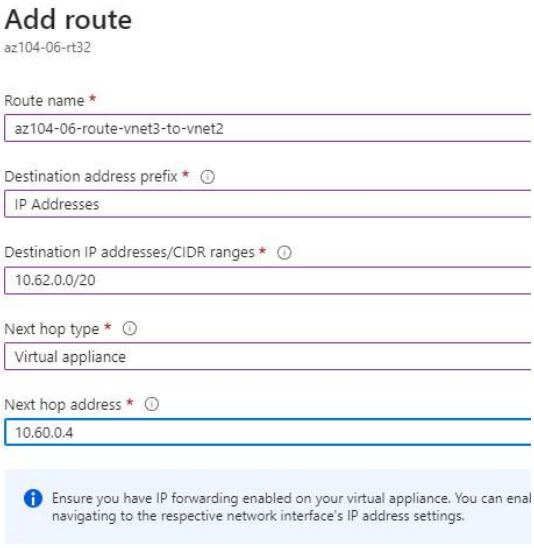
14. On the **az104-06-rt23** route table blade, in the **Settings** section, click **Routes**, and then click **+ Add**.

15. Add a new route with the following settings:
16. Click **Go to resource**.
17. On the **az104-06-rt23** route table blade, in the **Settings** section, click **Routes**, and then click **+ Add**.
18. Add a new route with the following settings:
19. Click **Add**
20. Navigate back to **Route tables** blade and click **+ Create**.
21. Create a route table with the following settings (leave others with their default values):

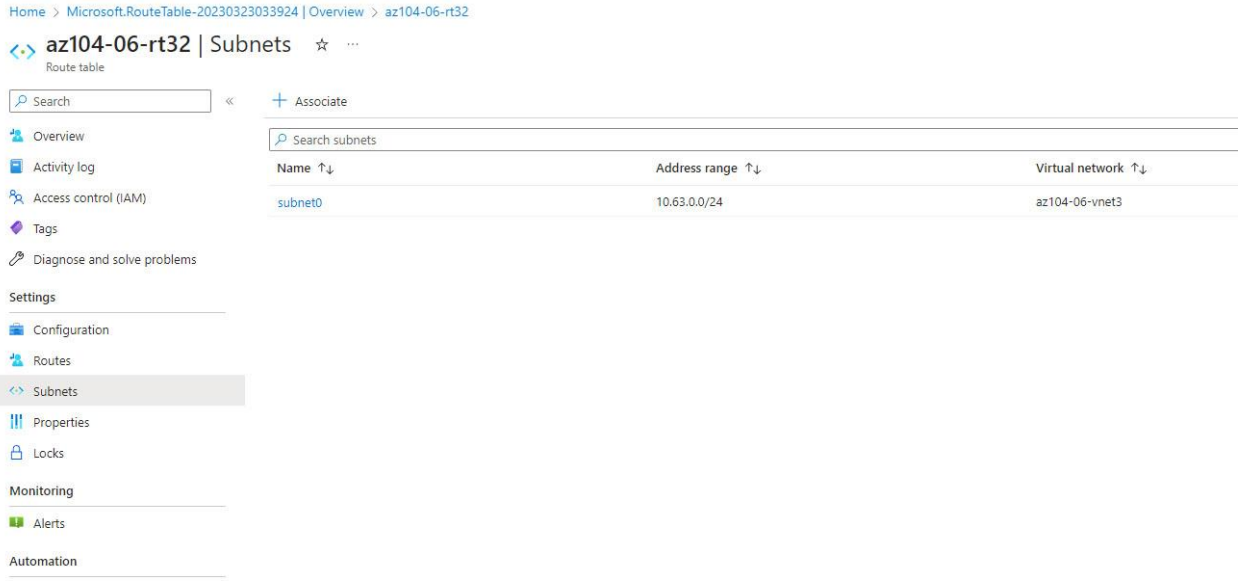


22. Click Review and Create. Let validation occur, and hit Create to submit your deployment.
23. Click **Go to resource**.
24. On the **az104-06-rt32** route table blade, in the **Settings** section, click **Routes**, and then click **+ Add**.

25. Add a new route with the following settings:

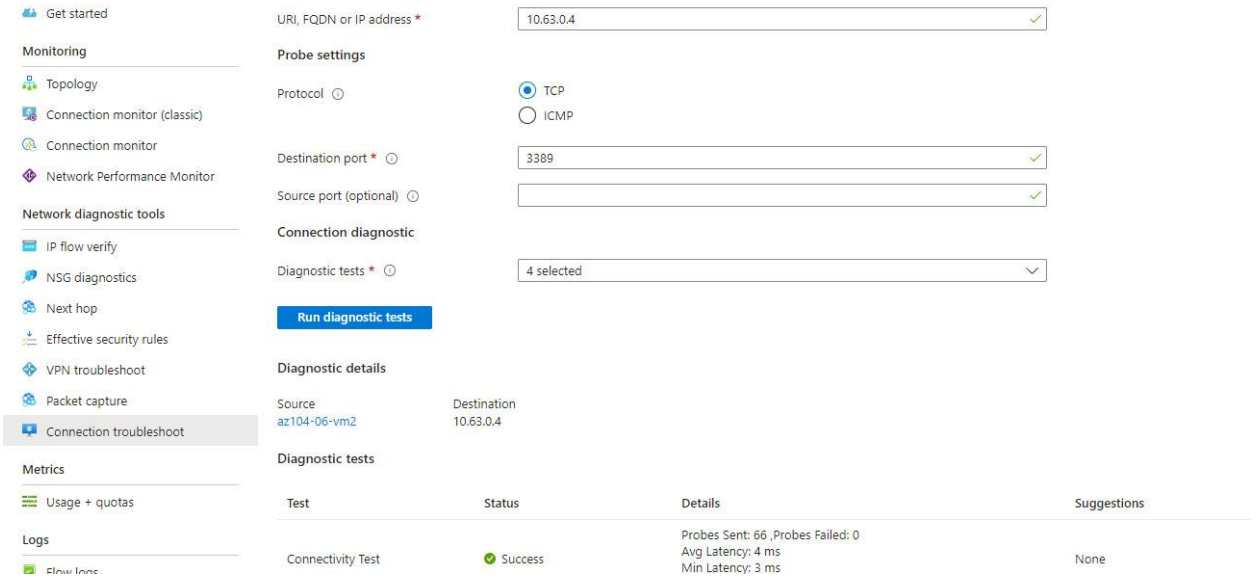


26. Click **OK**
27. Back on the **az104-06-rt32** route table blade, in the **Settings** section, click **Subnets**, and then click **+ Associate**.
28. Associate the route table **az104-06-rt32** with the following subnet:



29. Click **OK**
30. In the Azure portal, navigate back to the **Network Watcher - Connection troubleshoot** blade.

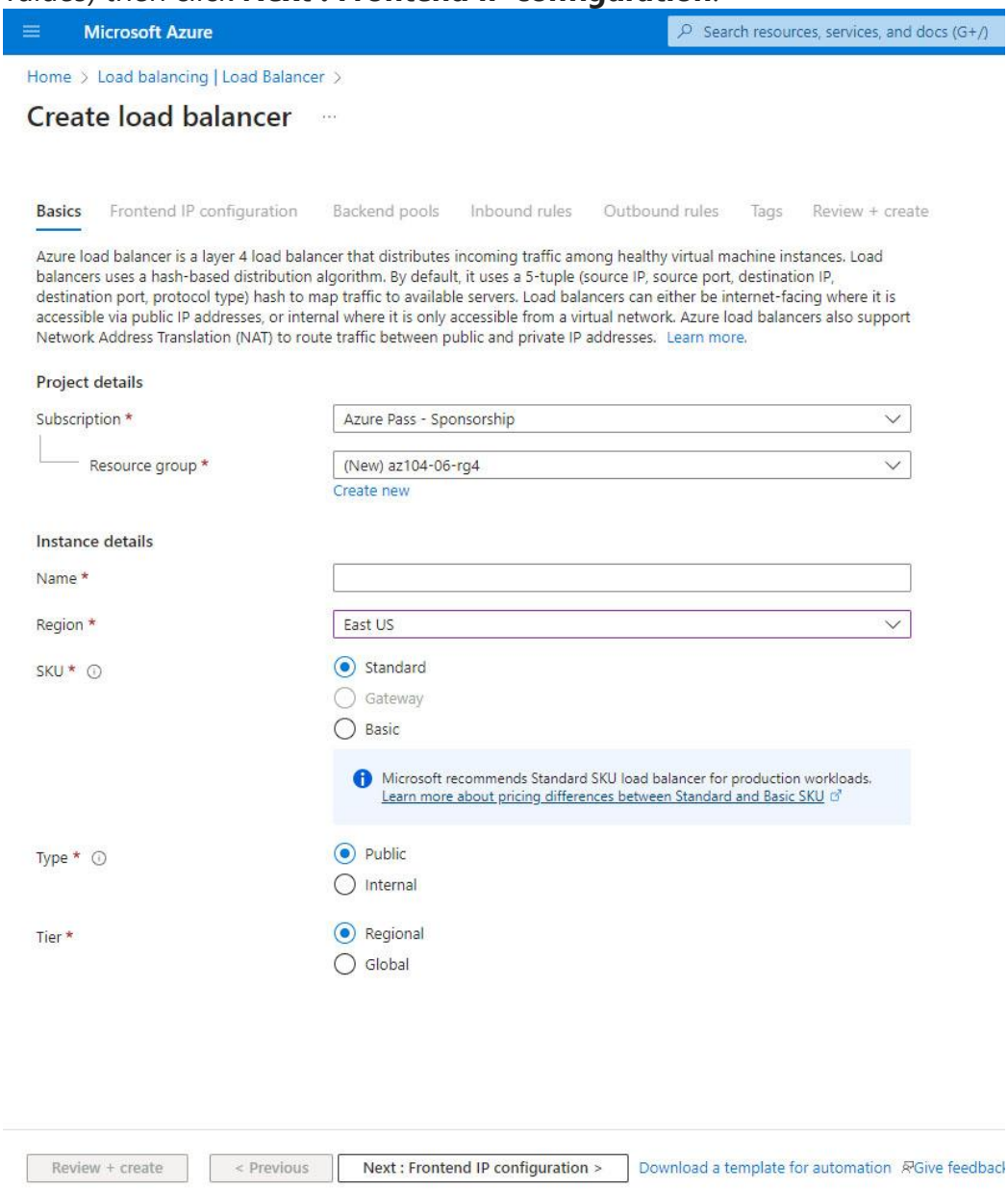
31. On the **Network Watcher - Connection troubleshoot** blade, initiate a check with the following settings (leave others with their default values):
32. Click **Check** and wait until results of the connectivity check are returned. Verify that the status is **Reachable**. Review the network path and note that the traffic was routed via **10.60.0.4**, assigned to the **az104-06-nic0** network adapter. If status is **Unreachable**, you should stop and then start az104-06-vm0.



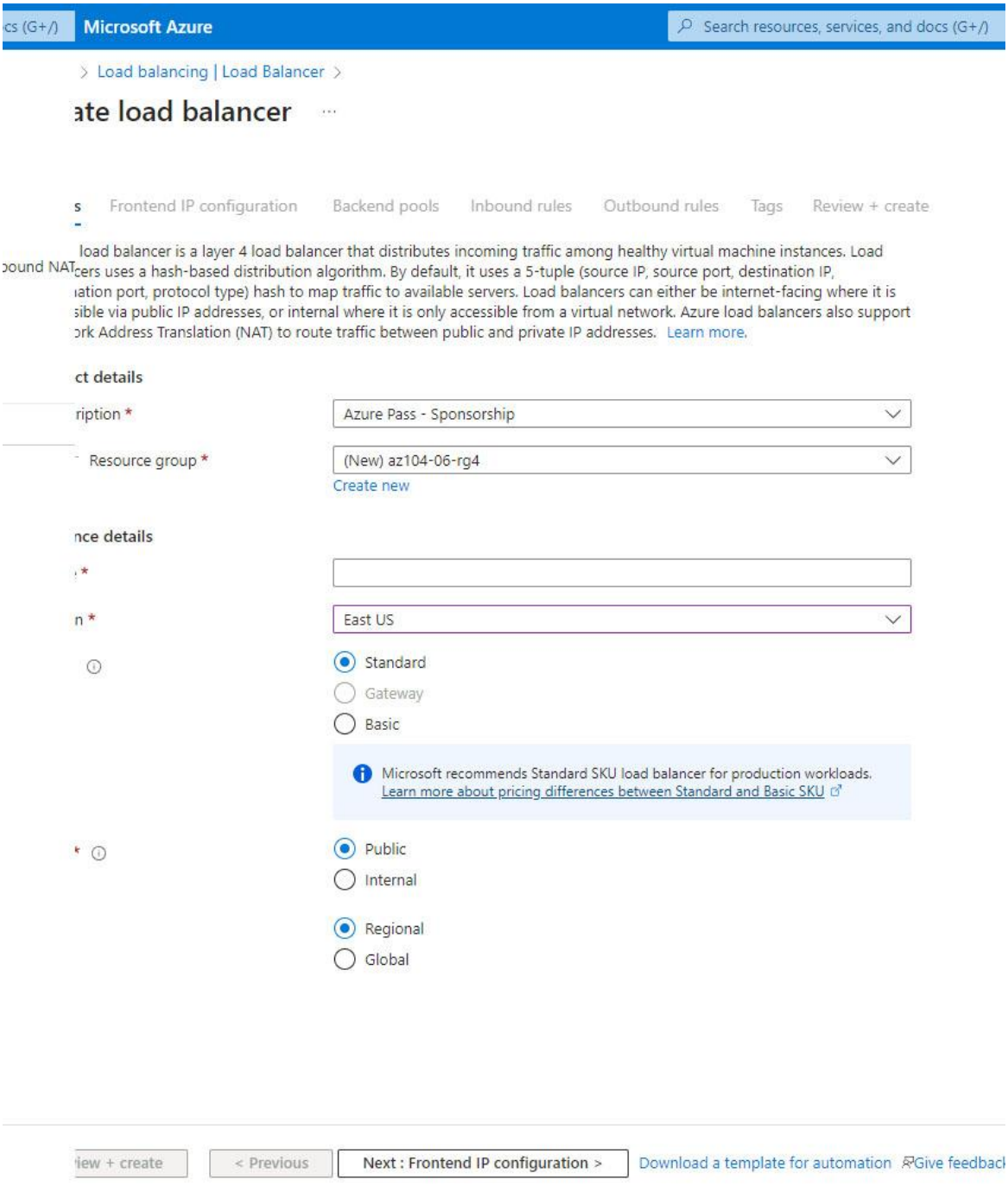
Task 5: Implement Azure Load Balancer

In this task, you will implement an Azure Load Balancer in front of the two Azure virtual machines in the hub virtual network.

1. In the Azure portal, search for and select **Load balancers** and, on the **Load balancers** blade, click **+ Create**.
2. Create a load balancer with the following settings (leave others with their default values) then click **Next : Frontend IP configuration**:

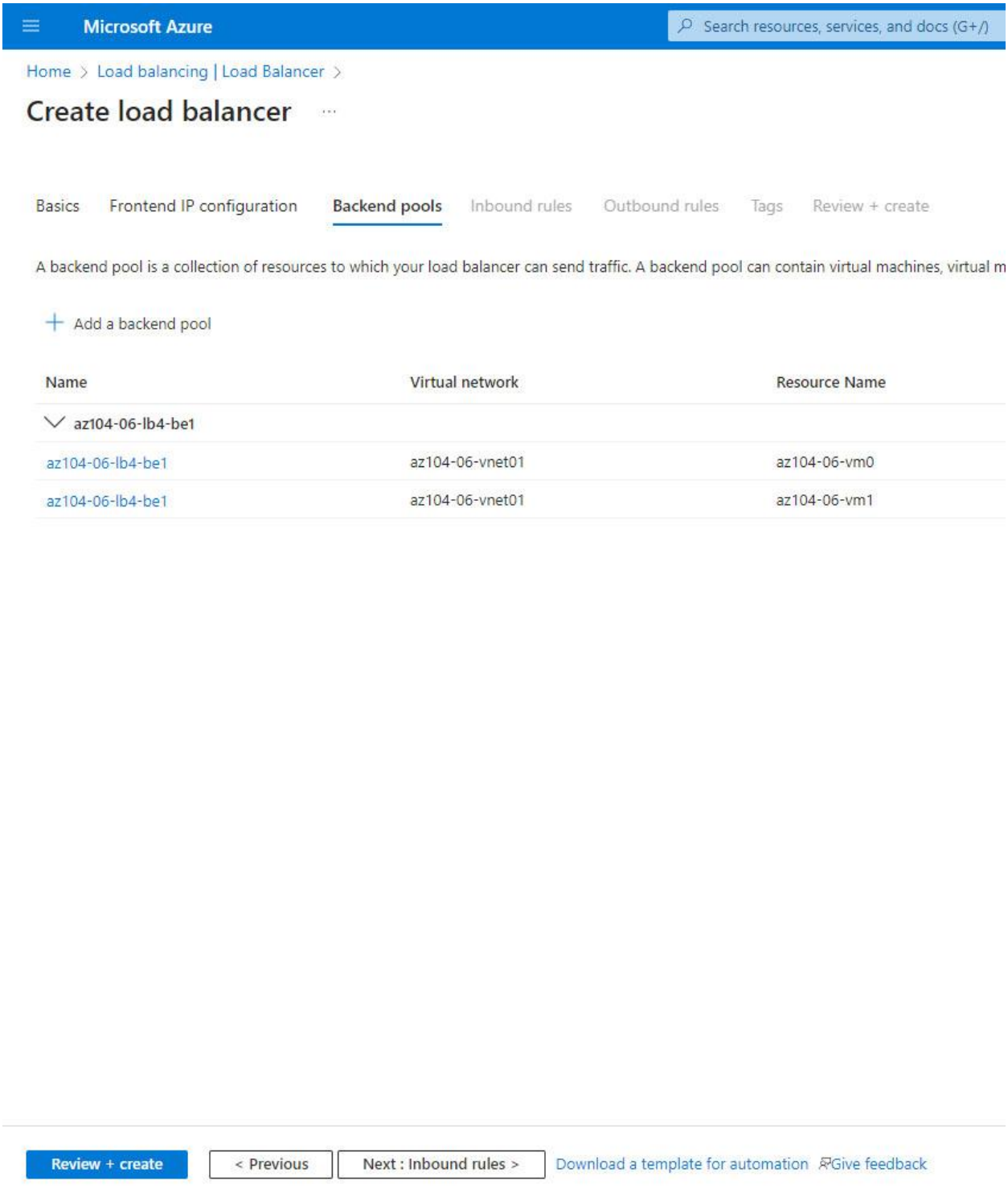


3. On the **Frontend IP configuration** tab, click **Add a frontend IP configuration** and use the following settings before clicking **OK** and then **Add**. When completed click **Next: Backend pools**.



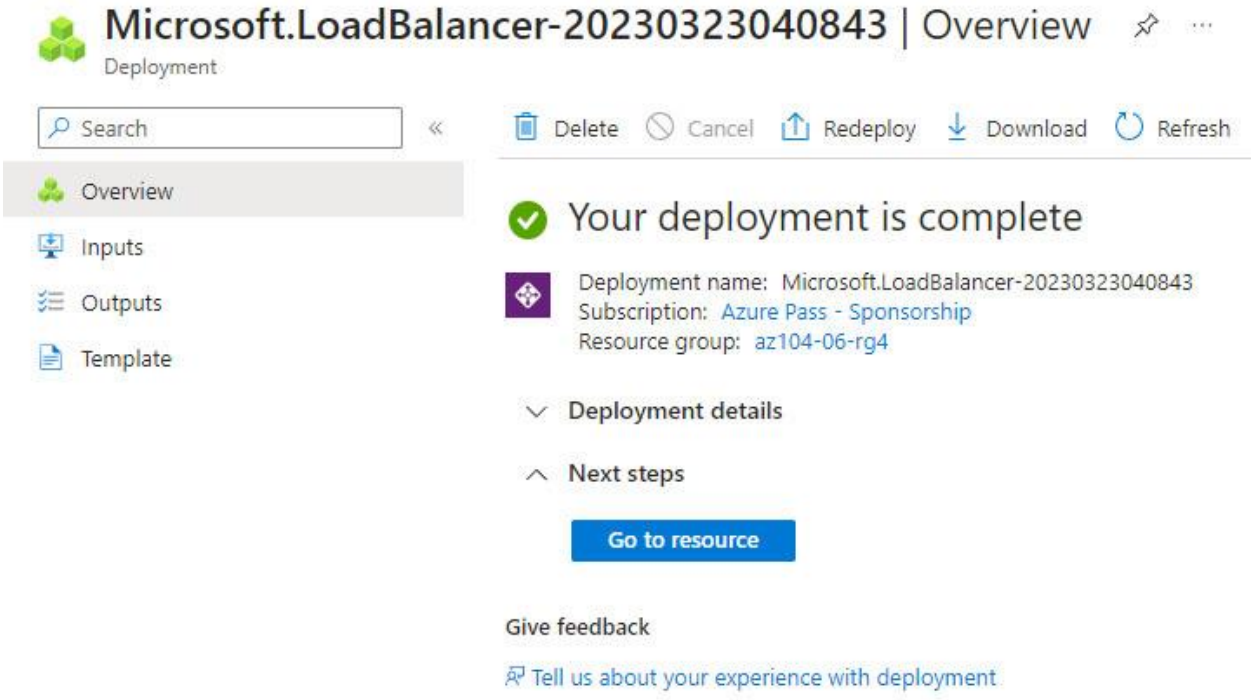
4. On the **Backend pools** tab, click **Add a backend pool** with the following settings (leave others with their default values). Click **+ Add** (twice) and then

click **Next:Inbound rules**.



5. On the **Inbound rules** tab, click **Add a load balancing rule**. Add a load balancing rule with the following settings (leave others with their default values). When completed click **Add**.

6. As you have time, review the other tabs, then click **Review and create**. Ensure there are no validation errors, then click **Create**.
7. Wait for the load balancer to deploy then click **Go to resource**.



8. Select **Frontend IP configuration** from the Load Balancer resource page. Copy the IP address.

9. Open another browser tab and navigate to the IP address. Verify that the browser window displays the message **Hello World from az104-06-vm0** or **Hello World from az104-06-vm1**.

Hello World from az104-06-vm1

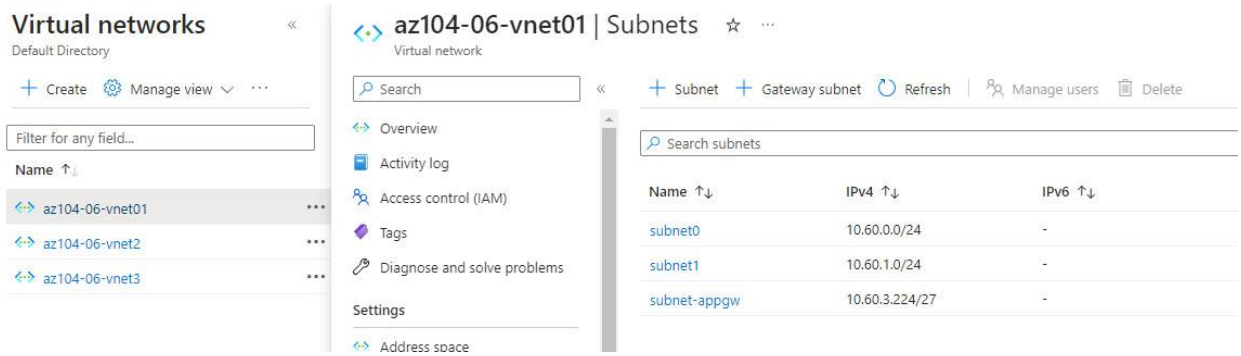
10. Refresh the window to verify the message changes to the other virtual machine. This demonstrates the load balancer rotating through the virtual machines.

Hello World from az104-06-vm0

Task 6: Implement Azure Application Gateway

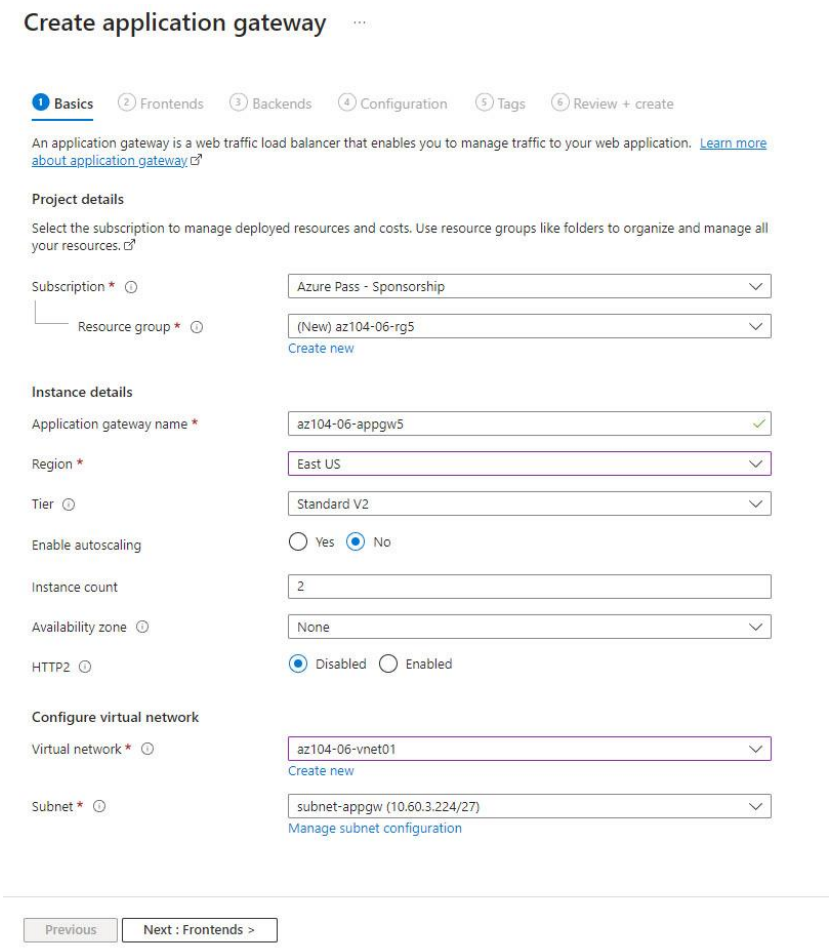
In this task, you will implement an Azure Application Gateway in front of the two Azure virtual machines in the spoke virtual networks.

1. In the Azure portal, search and select **Virtual networks**.
2. On the **Virtual networks** blade, in the list of virtual networks, click **az104-06-vnet01**.
3. On the **az104-06-vnet01** virtual network blade, in the **Settings** section, click **Subnets**, and then click **+ Subnet**.
4. Add a subnet with the following settings (leave others with their default values):
5. Click **Save**

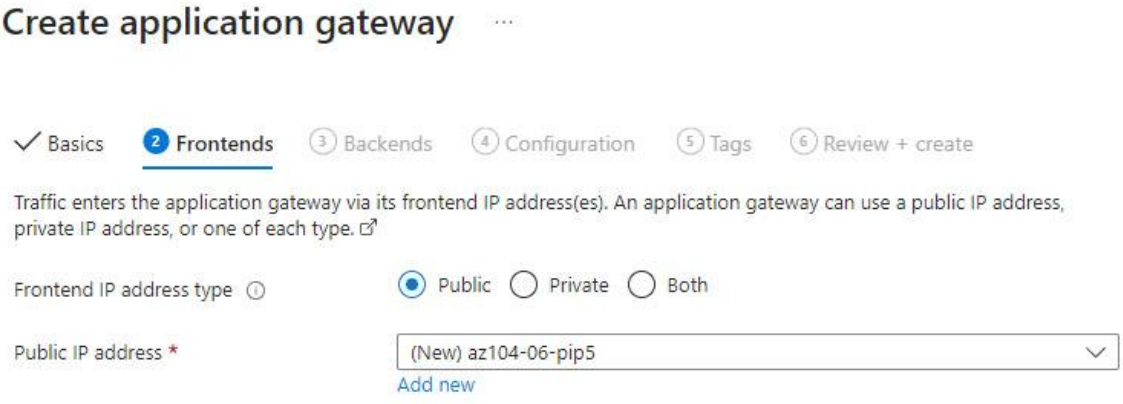


6. In the Azure portal, search and select **Application Gateways** and, on the **Application Gateways** blade, click **+ Create**.

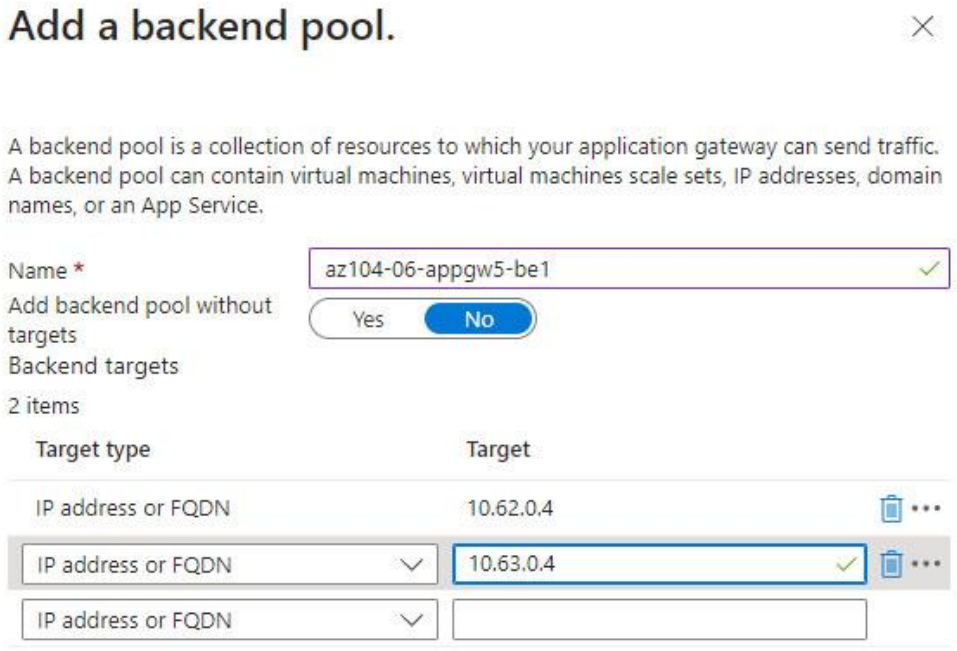
7. On the **Basics** tab, specify the following settings (leave others with their default values):



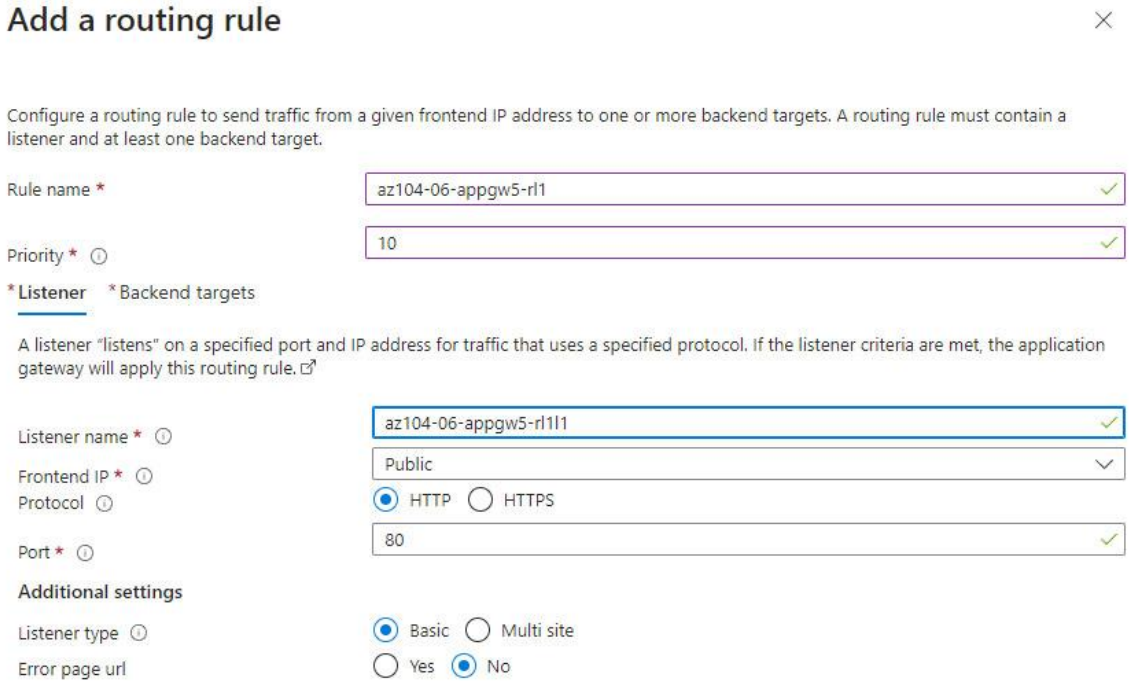
8. Click **Next: Frontends >** and specify the following settings (leave others with their default values). When complete, click **OK**.



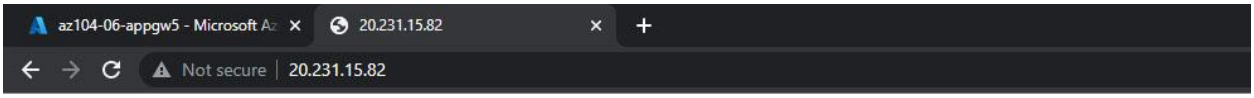
9. Click **Next: Backends >** and then **Add a backend pool**. Specify the following settings (leave others with their default values). When completed click **Add**.



10. Click **Next: Configuration >** and then **+ Add a routing rule**. Specify the following settings:

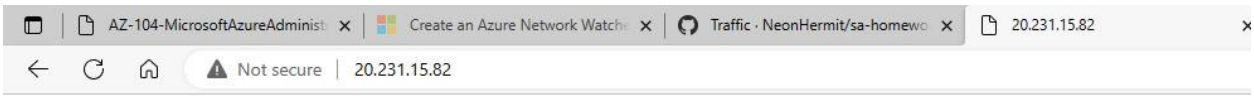


11. Switch to the **Backend targets** tab and specify the following settings (leave others with their default values). When completed click **Add** (twice).
12. Click **Next: Tags >**, followed by **Next: Review + create >** and then click **Create**.
13. In the Azure portal, search and select **Application Gateways** and, on the **Application Gateways** blade, click **az104-06-appgw5**.
14. On the **az104-06-appgw5** Application Gateway blade, copy the value of the **Frontend public IP address**.
15. Start another browser window and navigate to the IP address you identified in the previous step.
16. Verify that the browser window displays the message **Hello World from az104-06-vm2** or **Hello World from az104-06-vm3**.



Hello World from az104-06-vm2

17. Refresh the window to verify the message changes to the other virtual machine.



Hello World from az104-06-vm3