**Module 6: Network Traffic Management**

**Exercise 1: Implement Traffic Management**

#### 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 to will reside in a separate spoke virtual network.

1. Sign in to the [Azure portal](https://portal.azure.com/).
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**.

**Note**: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and click **Create storage**.

1. From the Cloud Shell pane, run the following to create the first resource group that will be hosting the first virtual network and the pair of virtual machines (replace the [Azure\_region] placeholder with the name of an Azure region where you intend to deploy Azure virtual machines):

*$location = '[Azure\_region]'*

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

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

*$rgName = 'az104-06-rg2'*

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

*$rgName = 'az104-06-rg3'*

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

1. Close the Cloud Shell pane.

#### Task 2: Creating virtual network

In this task, you will create a virtual network with multiple subnets by using the Azure portal

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, search for and select **Virtual networks**, and, on the **Virtual networks** blade, click **+Create**.
3. Create a virtual network with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **the name of a new resource group az104-06-rg1** |
| Name | **az104-06-vnet1** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| IPv4 address space | **10.61.0.0/22** |
| Subnet name | **subnet0** |
| Subnet address range | **10.61.0.0/24** |
| Subnet name | **subnet1** |
| Subnet address range | **10.61.1.0/24** |

**Note:** Wait for the virtual network to be provisioned. This should take less than a minute.

1. Click **Review + Create** to create the virtual network.
2. In the Azure portal, search for and select **Virtual networks**, and, on the **Virtual networks** blade, click **+Create**.
3. Create a virtual network with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **the name of a new resource group az104-06-rg2** |
| Name | **az104-06-vnet2** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| IPv4 address space | **10.62.0.0/22** |
| Subnet name | **subnet0** |
| Subnet address range | **10.62.0.0/24** |

**Note:** Wait for the virtual network to be provisioned. This should take less than a minute.

1. Click **Review + Create** to create the virtual network.
2. In the Azure portal, search for and select **Virtual networks**, and, on the **Virtual networks** blade, click **+Create**.
3. Create a virtual network with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **the name of a new resource group az104-06-rg3** |
| Name | **az104-05-vnet3** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| IPv4 address space | **10.63.0.0/22** |
| Subnet name | **subnet0** |
| Subnet address range | **10.63.0.0/24** |

**Note:** Wait for the virtual network to be provisioned. This should take less than a minute.

1. Click **Review + Create** to create the virtual network.

#### Task 3: Creating Network Security Group

In this task, you will create a Network Security Group by using the Azure portal

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, search for and select **Network security groups**, and click **+Create**.
3. Create a Network Security Group with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg1** |
| Name | **az104-06-nsg1** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |

1. Click **Review + Create** to create the Network Security Group.
2. Click **Go to resource**.
3. Under **Settings** for **az104-06-nsg1**, click **Inbound security rules** to add rules with the following settings (leave others with their default values) after click **+ Add**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **RDP** |
| Action | **Allow** |
| Priority | **1000** |
| Name | **allow-rdp** |

1. Click **Add** to create the rule.
2. Under **Settings** for **az104-06-nsg1**, click **Inbound security rules** to add rules with the following settings (leave others with their default values) after click **+ Add**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **HTTP** |
| Action | **Allow** |
| Priority | **1100** |
| Name | **allow-http** |

1. Click **Add** to create the rule.
2. In the Azure portal, search for and select **Network security groups**, and click **+Create**.
3. Create a Network Security Group with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg2** |
| Name | **az104-06-nsg2** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |

1. Click **Review + Create** to create the Network Security Group.
2. Click **Go to resource**.
3. Under **Settings** for **az104-06-nsg2**, click **Inbound security rules** to add rules with the following settings (leave others with their default values) after click **+ Add**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **RDP** |
| Action | **Allow** |
| Priority | **1000** |
| Name | **allow-rdp** |

1. Click **Add** to create the rule.
2. Under **Settings** for **az104-06-nsg2**, click **Inbound security rules** to add rules with the following settings (leave others with their default values) after click **+ Add**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **HTTP** |
| Action | **Allow** |
| Priority | **1100** |
| Name | **allow-http** |

1. Click **Add** to create the rule.
2. In the Azure portal, search for and select **Network security groups**, and click **+Create**.
3. Create a Network Security Group with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg3** |
| Name | **az104-06-nsg3** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |

1. Click **Review + Create** to create the Network Security Group.
2. Click **Go to resource**.
3. Under **Settings** for **az104-06-nsg3**, click **Inbound security rules** to add rules with the following settings (leave others with their default values) after click **+ Add**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **RDP** |
| Action | **Allow** |
| Priority | **1000** |
| Name | **allow-rdp** |

1. Click **Add** to create the rule.
2. Under **Settings** for **az104-06-nsg3**, click **Inbound security rules** to add rules with the following settings (leave others with their default values) after click **+ Add**

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **HTTP** |
| Action | **Allow** |
| Priority | **1100** |
| Name | **allow-http** |

1. Click **Add** to create the rule.

#### Task 4: Creating Virtual Machines

In this task, you will create a Virtual Machine by using the Azure portal

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, search for and select **Virtual Machines**, and click **+Create**.
3. Create a Virtual Machine with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg1** |
| Name | **az104-06-vm0** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Availability options | **Availability zone** |
| Availability zone | **Zones 1** |
| Security type | **Standard** |
| Image | **Windows Server 2019 Datacenter – Gen2** |
| Size | **Standard\_B2s – 2 vcpus, 4 GiB memory (34,47 €/month)** |
| Username | **vmadmin** |
| Password | **Pa55w.rd1234** |
| Public inbound ports | **None** |

1. Click **Next: Disks** to select **Premium SSD (locally-redundant storage) as OS disk type, and click Next: Networking to** configure the virtual machine networking with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-06-vnet01** |
| Subnet | **subnet0** |
| Public IP | **None** |
| NIC network security group | **Advanced: az104-06-nsg1** |
| Public inbound ports | **None** |
| Delete NIC when VM is deleted | **Check** |

1. Click **Review + Create** to create the virtual machine.
2. In the Azure portal, search for and select **Virtual Machines**, and click **+Create**.
3. Create a Virtual Machine with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg1** |
| Name | **az104-06-vm1** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Availability options | **Availability zone** |
| Availability zone | **Zones 1** |
| Security type | **Standard** |
| Image | **Windows Server 2019 Datacenter – Gen2** |
| Size | **Standard\_B2s – 2 vcpus, 4 GiB memory (34,47 €/month)** |
| Username | **vmadmin** |
| Password | **Pa55w.rd1234** |
| Public inbound ports | **None** |

1. Click **Next: Disks** to select **Premium SSD (locally-redundant storage) as OS disk type, and click Next: Networking to** configure the virtual machine networking with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-06-vnet01** |
| Subnet | **subnet1** |
| Public IP | **None** |
| NIC network security group | **Advanced: az104-06-nsg1** |
| Public inbound ports | **None** |
| Delete NIC when VM is deleted | **Check** |

1. Click **Review + Create** to create the virtual machine.
2. In the Azure portal, search for and select **Virtual Machines**, and click **+Create**.
3. Create a Virtual Machine with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg2** |
| Name | **az104-06-vm2** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Availability options | **Availability zone** |
| Availability zone | **Zones 1** |
| Security type | **Standard** |
| Image | **Windows Server 2019 Datacenter – Gen2** |
| Size | **Standard\_B2s – 2 vcpus, 4 GiB memory (34,47 €/month)** |
| Username | **vmadmin** |
| Password | **Pa55w.rd1234** |
| Public inbound ports | **None** |

1. Click **Next: Disks** to select **Premium SSD (locally-redundant storage) as OS disk type, and click Next: Networking to** configure the virtual machine networking with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-06-vnet2** |
| Subnet | **subnet0** |
| Public IP | **None** |
| NIC network security group | **Advanced: az104-06-nsg2** |
| Public inbound ports | **None** |
| Delete NIC when VM is deleted | **Check** |

1. Click **Review + Create** to create the virtual machine.
2. In the Azure portal, search for and select **Virtual Machines**, and click **+Create**.
3. Create a Virtual Machine with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **az104-06-rg3** |
| Name | **az104-06-vm3** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Availability options | **Availability zone** |
| Availability zone | **Zones 1** |
| Security type | **Standard** |
| Image | **Windows Server 2019 Datacenter – Gen2** |
| Size | **Standard\_B2s – 2 vcpus, 4 GiB memory (34,47 €/month)** |
| Username | **vmadmin** |
| Password | **Pa55w.rd1234** |
| Public inbound ports | **None** |

1. Click **Next: Disks** to select **Premium SSD (locally-redundant storage) as OS disk type, and click Next: Networking to** configure the virtual machine networking with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-06-vnet3** |
| Subnet | **subnet0** |
| Public IP | **None** |
| NIC network security group | **Advanced: az104-06-nsg3** |
| Public inbound ports | **None** |
| Delete NIC when VM is deleted | **Check** |

1. Click **Review + Create** to create the virtual machine.
2. On the **az104-06-vm0** blade, in the **Operations** section, click **Run command**, and, in the list of commands, click **RunPowerShellScript**.
3. On the **Run Command Script** blade, type the following and click **Run** to install the Remote Access Windows Server role.

*Install-WindowsFeature -name Web-Server -IncludeManagementTools*

**Note**: Wait for the confirmation that the command completed successfully.

1. On the **az104-06-vm1** blade, in the **Operations** section, click **Run command**, and, in the list of commands, click **RunPowerShellScript**.
2. On the **Run Command Script** blade, type the following and click **Run** to install the Remote Access Windows Server role.

*Install-WindowsFeature -name Web-Server -IncludeManagementTools*

**Note**: Wait for the confirmation that the command completed successfully.

#### Task 5: 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, click **az104-06-vnet1**.
4. On the **az104-06-vnet1** virtual network blade, in the **Settings** section, click **Peerings** and then click **+ Add**.
5. Add a peering with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| **This virtual network** | |
| Peering link name | **az104-06-vnet1\_to\_az104-06-vnet2** |
| Traffic to remote virtual network | **Allow** |
| Traffic forwarded from remote virtual network | **Allow** |
| Virtual network gateway or Route Server | **None** |
| **Remote virtual network** | |
| Peering link name | **az104-06-vnet2\_to\_az104-06-vnet1** |
| Virtual network deployment model | **Resource manager** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Virtual network | **az104-06-vnet2 (az104-06-rg2)** |
| Traffic to remote virtual network | **Allow** |
| Traffic forwarded from remote virtual network | **Allow** |
| Virtual network gateway or Route Server | **None** |

**Note**: This step establishes two local peerings - one from az104-06-vnet1 to az104-06-vnet2 and the other from az104-06-vnet2 to az104-06-vnet1.

**Note**: **Allow forwarded traffic** needs to be enabled in order to facilitate routing between spoke virtual networks, which you will implement later in this lab.

1. On the **az104-06-vnet1** virtual network blade, in the **Settings** section, click **Peerings** and then click **+ Add**.
2. Add a peering with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| **This virtual network** | |
| Peering link name | **az104-06-vnet1\_to\_az104-06-vnet3** |
| Traffic to remote virtual network | **Allow** |
| Traffic forwarded from remote virtual network | **Allow** |
| Virtual network gateway or Route Server | **None** |
| **Remote virtual network** | |
| Peering link name | **az104-06-vnet3\_to\_az104-06-vnet1** |
| Virtual network deployment model | **Resource manager** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Virtual network | **az104-06-vnet3 (az104-06-rg3)** |
| Traffic to remote virtual network | **Allow** |
| Traffic forwarded from remote virtual network | **Allow** |
| Virtual network gateway or Route Server | **None** |

**Note**: This step establishes two local peerings - one from az104-06-vnet01 to az104-06-vnet3 and the other from az104-06-vnet3 to az104-06-vnet1. This completes setting up the hub and spoke topology (with two spoke virtual networks).

**Note**: **Allow forwarded traffic** needs to be enabled in order to facilitate routing between spoke virtual networks, which you will implement later in this lab.

#### Task 6: 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 that the service is enabled in the Azure into which you deployed resources in the first task of this lab.
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):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **az104-06-rg1** |
| Source type | **Virtual machine** |
| Virtual machine | **az104-06-vm0** |
| Destination | **Specify manually** |
| URI, FQDN or IPv4 | **10.62.0.4** |
| Protocol | **TCP** |
| Destination Port | **3389** |

**Note**: **10.62.0.4** represents the private IP address of **az104-06-vm2**

1. 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.

**Note**: This is expected, since the hub virtual network is peered directly with the first spoke virtual network.

**Note**: The initial check can take about 2 minutes because it requires installation of the Network Watcher Agent virtual machine extension on **az104-06-vm0**.

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

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **az104-06-rg1** |
| Source type | **Virtual machine** |
| Virtual machine | **az104-06-vm0** |
| Destination | **Specify manually** |
| URI, FQDN or IPv4 | **10.63.0.4** |
| Protocol | **TCP** |
| Destination Port | **3389** |

**Note**: **10.63.0.4** represents the private IP address of **az104-06-vm3**

1. 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.

**Note**: This is expected, since the hub virtual network is peered directly with the second spoke virtual network.

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

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **az104-06-rg2** |
| Source type | **Virtual machine** |
| Virtual machine | **az104-06-vm2** |
| Destination | **Specify manually** |
| URI, FQDN or IPv4 | **10.63.0.4** |
| Protocol | **TCP** |
| Destination Port | **3389** |

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

**Note**: This is expected, since the two spoke virtual networks are not peered with each other (virtual network peering is not transitive).

#### Task 7: 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.

**Note**: This setting is required in order for **az104-06-vm0** to function as a router, which will route traffic between two spoke virtual networks.

**Note**: Now you need to configure operating system of the **az104-06-vm0** virtual machine to support routing.

1. In the Azure portal, navigate back to the **az104-06-vm0** Azure virtual machine blade and click **Overview**.
2. On the **az104-06-vm0** blade, in the **Operations** section, click **Run command**, and, in the list of commands, click **RunPowerShellScript**.
3. On the **Run Command Script** blade, type the following and click **Run** to install the Remote Access Windows Server role.

*Install-WindowsFeature RemoteAccess -IncludeManagementTools*

**Note**: Wait for the confirmation that the command completed successfully.

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

*Install-WindowsFeature -Name Routing -IncludeManagementTools -IncludeAllSubFeature*

*Install-WindowsFeature -Name "RSAT-RemoteAccess-Powershell"*

*Install-RemoteAccess -VpnType RoutingOnly*

*Get-NetAdapter | Set-NetIPInterface -Forwarding Enabled*

**Note**: Wait for the confirmation that the command completed successfully.

**Note**: Now you need to create and configure user defined routes on the spoke virtual networks.

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

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-06-rt23** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **az104-06-rg2** |
| Location | **the name of the Azure region in which you created the virtual networks** |
| Virtual network gateway route propagation | **Disabled** |

**Note**: Wait for the route table to be created. This should take about 3 minutes.

1. Back on the **Route tables** blade, click **Refresh** and then click **az104-06-rt23**.
2. On the **az104-06-rt23** route table blade, click **Routes** and then click **+ Add**.
3. Add a new route with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Route name | **az104-06-route-vnet2-to-vnet3** |
| Address prefix | **IP Addresses** |
| Destination IP addresses CIDR | **10.63.0.0/22** |
| Next hop type | **Virtual appliance** |
| Next hop address | **10.61.0.4** |

1. Back on the **az104-06-rt23** route table blade, click **Subnets** and then click **+ Associate**.
2. Associate the route table **az104-06-rt23** with the following subnet:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-06-vnet2** |
| Subnet | **subnet0** |

1. Navigate back to **Route tables** blade and click **+ Add**.
2. Create a route table with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-06-rt32** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **az104-06-rg3** |
| Location | **the name of the Azure region in which you created the virtual networks** |

**Note**: Wait for the route table to be created. This should take about 3 minutes.

1. Back on the **Route tables** blade, click **Refresh** and then click **az104-06-rt32**.
2. On the **az104-06-rt32** route table blade, click **Routes** and then click **+ Add**.
3. Add a new route with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Route name | **az104-06-route-vnet3-to-vnet2** |
| Address prefix | **10.62.0.0/22** |
| Next hop type | **Virtual appliance** |
| Next hop address | **10.61.0.4** |

1. Back on the **az104-06-rt32** route table blade, click **Subnets** and then click **+ Associate**.
2. Associate the route table **az104-06-rt32** with the following subnet:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-06-vnet3** |
| Subnet | **subnet0** |

1. In the Azure portal, navigate back to the **Network Watcher - Connection troubleshoot** blade.
2. On the **Network Watcher - Connection troubleshoot** blade, initiate a check with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **az104-06-rg2** |
| Source type | **Virtual machine** |
| Virtual machine | **az104-06-vm2** |
| Destination | **Specify manually** |
| URI, FQDN or IPv4 | **10.63.0.4** |
| Protocol | **TCP** |
| Destination Port | **3389** |

1. 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 **10.61.0.4**, assigned to the **az104-06-nic0** network adapter. If status is **Unreachable**, you should restart az104-06-vm0.

**Note**: This is expected, since the traffic between spoke virtual networks is now routed via the virtual machine located in the hub virtual network, which functions as a router.

**Note**: You can use **Network Watcher** to view topology of the network.

#### Task 8: 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 and select **Load balancers** and, on the **Load balancers** blade, click **+ Add**.
2. Create a load balancer with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **the name of a new resource group az104-06-rg4** |
| Name | **az104-06-lb4** |
| Region | **name of the Azure region into which you deployed all other resources in this lab** |
| Type | **Public** |
| Tier | **Regional** |
| SKU | **Standard** |
| Public IP address | **Create new** |
| Public IP address name | **az104-06-pip4** |
| Availability zone | **Zone-redundant** |
| Add a public IPv6 address | **No** |

**Note**: Wait for the Azure load balancer to be provisioned. This should take about 2 minutes.

1. On the deployment blade, click **Go to resource**.
2. On the **az104-06-lb4** load balancer blade, click **Backend pools** and click **+ Add**.
3. Add a backend pool with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-06-lb4-be1** |
| Virtual network | **az104-06-vnet1** |
| IP version | **IPv4** |
| Virtual machine | **az104-06-vm0** |
| Virtual machine IP address | **ipconfig1 (10.61.0.4)** |
| Virtual machine | **az104-06-vm1** |
| Virtual machine IP address | **ipconfig1 (10.61.1.4)** |

1. Wait for the backend pool to be created, click **Health probes**, and then click **+ Add**.
2. Add a health probe with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-06-lb4-hp1** |
| Protocol | **TCP** |
| Port | **80** |
| Interval | **5** |
| Unhealthy threshold | **2** |

1. Wait for the health probe to be created, click **Load balancing rules**, and then click **+ Add**.
2. Add a load balancing rule with the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-06-lb4-lbrule1** |
| IP Version | **IPv4** |
| Protocol | **TCP** |
| Port | **80** |
| Backend port | **80** |
| Backend pool | **az104-06-lb4-be1** |
| Health probe | **az104-06-lb4-hp1** |
| Session persistence | **None** |
| Idle timeout (minutes) | **4** |
| TCP reset | **Disabled** |
| Floating IP (direct server return) | **Disabled** |
| Create implicit outbound rules | **Yes** |

1. Wait for the load balancing rule to be created, click **Overview**, and note the value of the **Public IP address**.
2. Start another browser window and navigate to the IP address you identified in the previous step. Verify that the browser window displays the IIS Home Page.

#### Task 9: 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-vnet1** 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):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **subnet-appgw** |
| Address range (CIDR block) | **10.61.3.224/27** |
| Network security group | **None** |
| Route table | **None** |

**Note**: This subnet will be used by the Azure Application Gateway instances, which you will deploy later in this task. The Application Gateway requires a dedicated subnet of /27 or larger size.

1. In the Azure portal, search and select **Application Gateways** and, on the **Application Gateways** blade, click **+ Add**.
2. On the **Basics** tab of the **Create an application gateway** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you are using in this lab** |
| Resource group | **the name of a new resource group az104-06-rg5** |
| Application gateway name | **az104-06-appgw5** |
| Region | **name of the Azure region into which you deployed all other resources in this lab** |
| Tier | **Standard V2** |
| Enable autoscaling | **No** |
| Scale units | **1** |
| Availability zone | **1, 2, 3** |
| HTTP2 | **Disabled** |
| Virtual network | **az104-06-vnet1** |
| Subnet | **subnet-appgw** |

1. Click **Next: Frontends >** and, on the **Frontends** tab of the **Create an application gateway** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Frontend IP address type | **Public** |
| Firewall public IP address | **the name of a new public IP address az104-06-pip5** |

1. Click **Next: Backends >**, on the **Backends** tab of the **Create an application gateway** blade, click **Add a backend pool**, and, on the **Add a backend pool** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **az104-06-appgw5-be1** |
| Add backend pool without targets | **No** |
| Target type | **IP address or FQDN** |
| Target | **10.62.0.4** |
| Target type | **IP address or FQDN** |
| Target | **10.63.0.4** |

**Note**: The targets represent the private IP addresses of virtual machines in the spoke virtual networks **az104-06-vm2** and **az104-06-vm3**.

1. Click **Add**, click **Next: Configuration >** and, on the **Configuration** tab of the **Create an application gateway** blade, click **+ Add a routing rule**.
2. On the **Add a routing rule** blade, on the **Listener** tab, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Rule name | **az104-06-appgw5-rl1** |
| Listener name | **az104-06-appgw5-rl1l1** |
| Frontend IP | **Public** |
| Protocol | **HTTP** |
| Port | **80** |
| Listener type | **Basic** |
| Error page url | **No** |

1. Switch to the **Backend targets** tab of the **Add a routing rule** blade and specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Target type | **Backend pool** |
| Backend target | **az104-06-appgw5-be1** |

1. On the **Backend targets** tab of the **Add a routing rule** blade, click **Add new** next to the **HTTP setting** text box, and, on the **Add an HTTP setting** blade, specify the following settings (leave others with their default values):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| HTTP setting name | **az104-06-appgw5-http1** |
| Backend protocol | **HTTP** |
| Backend port | **80** |
| Cookie-based affinity | **Disable** |
| Connection draining | **Disable** |
| Request time-out (seconds) | **20** |

1. Click **Add** on the **Add an HTTP setting** blade, and back on the **Add a routing rule** blade, click **Add**.
2. Click **Next: Tags >**, followed by **Next: Review + create >** and then click **Create**.

**Note**: Wait for the Application Gateway instance to be created. This might take about 8 minutes.

1. In the Azure portal, search and select **Application Gateways** and, on the **Application Gateways** blade, click **az104-06-appgw5**.
2. On the **az104-06-appgw5** Application Gateway blade, note the value of the **Frontend public IP address**.
3. Start another browser window and navigate to the IP address you identified in the previous step.
4. Verify that the browser window displays the IIS home page.

#### Clean up resources

**Note**: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges.

1. In the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.
2. List all resource groups created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-06\*'*

1. Delete all resource groups you created throughout the labs of this module by running the following command:

*Get-AzResourceGroup -Name 'az104-06\*' | Remove-AzResourceGroup -Force -AsJob*

**Note**: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.