Lab - Implement Traffic Management

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

Instructions

Exercise 1

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.
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**.

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 **az104-06-vms-template.json**, **az104-06-vm-template.json**, and **az104-06-vm-parameters.json** into the Cloud Shell home directory.
5. 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
```

6. From the Cloud Shell pane, run the following to create the first virtual network and deploy a pair of virtual machines into it by using the template and parameter files you uploaded:

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

7. From the Cloud Shell pane, run the following to create the second resource group that will be hosting the second virtual network and the third virtual machine

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

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

8. From the Cloud Shell pane, run the following to create the second virtual network and deploy a virtual machine into it by using the template and parameter files you uploaded:

```
New-AzResourceGroupDeployment `
   -ResourceGroupName $rgName `
   -TemplateFile $HOME/az104-06-vm-template.json `
   -TemplateParameterFile $HOME/az104-06-vm-parameters.json `
   -nameSuffix 2 `
   -AsJob
```

9. From the Cloud Shell pane, run the following to create the third resource group that will be hosting the third virtual network and the fourth virtual machine:

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

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

10. From the Cloud Shell pane, run the following to create the third virtual network and deploy a virtual machine into it by using the template and parameter files you uploaded:

```
New-AzResourceGroupDeployment `
   -ResourceGroupName $rgName `
   -TemplateFile $HOME/az104-06-vm-template.json `
   -TemplateParameterFile $HOME/az104-06-vm-parameters.json `
   -nameSuffix 3 `
   -AsJob
```

Note: Wait for the deployments to complete before proceeding to the next task. This should take about 5 minutes.

Note: To verify the status of the deployments, you can examine the properties of the resource groups you created in this task.

11. 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.

   Note: The template you used for deployment of the three virtual networks ensures that the IP address ranges of the three virtual networks do not overlap.

3. In the list of virtual networks, click **az104-06-vnet01**.
4. On the **az104-06-vnet01** 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
Name of the peering from az104-06-vnet01 to remote virtual network	**az104-06-vnet01_to_az104-06-vnet2**
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)**
Name of the peering from az104-06-vnet2 to az104-06-vnet01	**az104-06-vnet2_to_az104-06-vnet01**
Allow virtual network access from az104-06-vnet01 to az104-06-vnet2	**Enabled**
Allow virtual network access from az104-06-vnet2 to az104-06-vnet01	**Enabled**
Allow forwarded traffic from az104-06-vnet2 to az104-06-vnet01	**Enabled**
Allow forwarded traffic from az104-06-vnet01 to az104-06-vnet2	**Enabled**

Setting	Value
Allow gateway transit	**(Uncheck Box)**

6. **Note**: Wait for the operation to complete.
7. **Note**: This step establishes two local peerings - one from az104-06-vnet01 to az104-06-vnet2 and the other from az104-06-vnet2 to az104-06-vnet01.
8. **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.
9. On the **az104-06-vnet01** virtual network blade, in the **Settings** section, click **Peerings** and then click **+ Add**.
10. Add a peering with the following settings (leave others with their default values):

Setting	Value
Name of the peering from az104-06-vnet01 to remote virtual network	**az104-06-vnet01_to_az104-06-vnet3**
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)**
Name of the peering from az104-06-vnet3 to az104-06-vnet01	**az104-06-vnet3_to_az104-06-vnet01**
Allow virtual network access from az104-06-vnet01 to az104-06-vnet3	**Enabled**
Allow virtual network access from az104-06-vnet3 to az104-06-vnet01	**Enabled**
Allow forwarded traffic from az104-06-vnet3 to az104-06-vnet01	**Enabled**

Setting	Value
Allow forwarded traffic from az104-06-vnet01 to az104-06-vnet3	**Enabled**
Allow gateway transit	**(Uncheck Box)**

11. **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-vnet01. This completes setting up the hub and spoke topology (with two spoke virtual networks).
12. **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 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 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**

Setting	Value
URI, FQDN or IPv4	**10.62.0.4**
Protocol	**TCP**
Destination Port	**3389**

5. **Note**: **10.62.0.4** represents the private IP address of **az104-06-vm2**
6. 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**.

7. 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**

Setting	Value
Protocol	**TCP**
Destination Port	**3389**

8. **Note**: **10.63.0.4** represents the private IP address of **az104-06-vm3**
9. 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.

10. 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**

11. 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 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, 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.

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.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

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

9. 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.

10. In the Azure portal, search and select **Route tables** and, on the **Route tables** blade, click **+ Add**.
11. 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**

12. **Note**: Wait for the route table to be created. This should take about 3 minutes.
13. Back on the **Route tables** blade, click **Refresh** and then click **az104-06-rt23**.
14. On the **az104-06-rt23** route table blade, click **Routes** and then click **+ Add**.
15. 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	**10.63.0.0/20**
Next hop type	**Virtual appliance**
Next hop address	**10.60.0.4**

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

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

18. Navigate back to **Route tables** blade and click **+ Add**.
19. 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

Setting	Value
Virtual network gateway route propagation	**Disabled**

20. **Note**: Wait for the route table to be created. This should take about 3 minutes.
21. Back on the **Route tables** blade, click **Refresh** and then click **az104-06-rt32**.
22. On the **az104-06-rt32** route table blade, click **Routes** and then click **+ Add**.
23. 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	**10.62.0.0/20**
Next hop type	**Virtual appliance**
Next hop address	**10.60.0.4**

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

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

26. In the Azure portal, navigate back to the **Network Watcher - Connection troubleshoot** blade.
27. 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**

28. 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.
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 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 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**
SKU	**Standard**
Public IP address	**Create new**
Public IP address name	**az104-06-pip4**
Availability zone	**Zone-redundant**
Add a public IPv6 address	**No**

3. **Note**: Wait for the Azure load balancer to be provisioned. This should take about 2 minutes.
4. On the deployment blade, click **Go to resource**.
5. On the **az104-06-lb4** load balancer blade, click **Backend pools** and click **+ Add**.
6. Add a backend pool with the following settings (leave others with their default values):

Setting	Value
Name	**az104-06-lb4-be1**

Setting	Value
Virtual network	**az104-06-vnet01**
IP version	**IPv4**
Virtual machine	**az104-06-vm0**
Virtual machine IP address	**ipconfig1 (10.60.0.4)**
Virtual machine	**az104-06-vm1**
Virtual machine IP address	**ipconfig1 (10.60.1.4)**

7. Wait for the backend pool to be created, click **Health probes**, and then click **+ Add**.
8. 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**

9. Wait for the health probe to be created, click **Load balancing rules**, and then click **+ Add**.
10. 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**

11. Wait for the load balancing rule to be created, click **Overview**, and note the value of the **Public IP address**.
12. Start another browser window and navigate to the IP address you identified in the previous step.
13. Verify that the browser window displays the message **Hello World from az104-06-vm0** or **Hello World from az104-06-vm1**.
14. Open another browser window but this time by using InPrivate mode and verify whether the target vm changes (as indicated by the message).

Note: You might need to refresh the browser window or open it again by using InPrivate mode.

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):

Setting	Value
Name	**subnet-appgw**
Address range (CIDR block)	**10.60.3.224/27**
Network security group	**None**
Route table	**None**

5. **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.
6. In the Azure portal, search and select **Application Gateways** and, on the **Application Gateways** blade, click **+ Add**.
7. 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

Setting	Value
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-vnet01**
Subnet	**subnet-appgw**

8. 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**

Setting	Value
Firewall public IP address	the name of a new public ip address **az104-06-pip5**

9. 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**

10. **Note**: The targets represent the private IP addresses of virtual machines in the spoke virtual networks **az104-06-vm2** and **az104-06-vm3**.
11. Click **Add**, click **Next: Configuration >** and, on the **Configuration** tab of the **Create an application gateway** blade, click **+ Add a routing rule**.
12. 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**

Setting	Value
Frontend IP	**Public**
Protocol	**HTTP**
Port	**80**
Listener type	**Basic**
Error page url	**No**

13. 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**

14. On the **Backend targets** tab of the **Add a routing rule** blade, click **Create 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**

Setting	Value
Cookie-based affinity	**Disable**
Connection draining	**Disable**
Request time-out (seconds)	**20**

15. Click **Add** on the **Add an HTTP setting** blade, and back on the **Add a routing rule** blade, clik **Add**.
16. 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.

17. In the Azure portal, search and select **Application Gateways** and, on the **Application Gateways** blade, click **az104-06-appgw5**.
18. On the **az104-06-appgw5** Application Gateway blade, note the value of the **Frontend public IP address**.
19. Start another browser window and navigate to the IP address you identified in the previous step.
20. Verify that the browser window displays the message **Hello World from az104-06-vm2** or **Hello World from az104-06-vm3**.
21. Open another browser window but this time by using InPrivate mode and verify whether the target vm changes (based on the message displayed on the web page).

    Note: You might need to refresh the browser window or open it again by using InPrivate mode.

    Note: Targeting virtual machines on multiple virtual networks is not a common configuration, but it is meant to illustrate the point that Application Gateway is capable of targeting virtual machines on multiple virtual networks (as well as endpoints in other Azure regions or even outside of Azure), unlike Azure Load Balancer, which load balances across virtual machines in the same virtual network.

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*'
```

3. 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.

Review

In this lab, you have:

- Provisioned the lab environment
- Configured the hub and spoke network topology
- Tested 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