Lab 04 - Implement Virtual Networking

Lab scenario

You need to explore Azure virtual networking capabilities.

To start, you plan to create a virtual network in Azure that will host a couple of Azure virtual machines. Since you intend to implement network-based segmentation, you will deploy them into different subnets of the virtual network.

You also want to make sure that their private and public IP addresses will not change over time.

To comply with Contoso security requirements, you need to protect public endpoints of Azure virtual machines accessible from Internet.

Finally, you need to implement DNS name resolution for Azure virtual machines both within the virtual network and from Internet.

Objectives

In this lab, you will:

- Task 1: Create and configure a virtual network
- Task 2: Deploy virtual machines into the virtual network
- Task 3: Configure private and public IP addresses of Azure VMs
- Task 4: Configure network security groups
- Task 5: Configure Azure DNS for internal name resolution
- Task 6: Configure Azure DNS for external name resolution

Instructions

Exercise 1

Task 1: Create and configure a 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.
2. In the Azure portal, search for and select **Virtual networks**, and, on the **Virtual networks** blade, click **+ Add**.

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 be using in this lab
Resource Group	the name of a new resource group **az104-04-rg1**
Name	**az104-04-vnet1**
Region	the name of any Azure region available in the subscription you will use in this lab
IPv4 address space	**10.40.0.0/20**
Subnet name	**subnet0**
Subnet address range	**10.40.0.0/24**

4. **Note:** Wait for the virtual network to be provisioned. This should take less than a minute.
5. On the **Virtual networks** blade, click **Refresh** and click **az104-04-vnet1**.
6. On the **az104-04-vnet1** virtual network blade, click **Subnets** and then click **+ Subnet**.
7. Create a subnet with the following settings (leave others with their default values):

Setting	Value
Name	**subnet1**
Address range (CIDR block)	**10.40.1.0/24**
Network security group	**None**
Route table	**None**

Task 2: Deploy virtual machines into the virtual network

In this task, you will deploy Azure virtual machines into different subnets of the virtual network by using an ARM template

1. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
2. 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**.

3. 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 **az104-04-vms-template.json** and **az104-04-vms-parameters.json** into the Cloud Shell home directory.
   Note: You might need to upload each file separately.

4. From the Cloud Shell pane, run the following to deploy two virtual machines by using the template and parameter files you uploaded:

```
$rgName = 'az104-04-rg1'

New-AzResourceGroupDeployment `
   -ResourceGroupName $rgName `
   -TemplateFile $HOME/az104-04-vms-template.json `
   -TemplateParameterFile $HOME/az104-04-vms-parameters.json
```

   Note: This method of deploying ARM templates uses Azure PowerShell. You can perform the same task by running the equivalent Azure CLI command **az deployment create** (for more information, refer to Deploy resources with Resource Manager templates and Azure CLI.
   Note: Wait for the deployment to complete before proceeding to the next task. This should take about 2 minutes.

5. Close the Cloud Shell pane.

Task 3: Configure private and public IP addresses of Azure VMs

In this task, you will configure static assignment of public and private IP addresses assigned to network interfaces of Azure virtual machines.
Note: Private and public IP addresses are assigned to the network interfaces, which, in turn are attached to Azure virtual machines, however, it is common to refer to IP addresses assigned to Azure VMs instead.

1. In the Azure portal, search for and select **Resource groups**, and, on the **Resource groups** blade, click **az104-04-rg1**.
2. On the **az104-04-rg1** resource group blade, in the list of its resources, click **az104-04-vnet1**.

3. On the **az104-04-vnet1** virtual network blade, review the **Connected devices** section and verify that there are two network interfaces **az104-04-nic0** and **az104-04-nic1** attached to the virtual network.
4. Click **az104-04-nic0** and, on the **az104-04-nic0** blade, click **IP configurations**.
   Note: Verify that **ipconfig1** is currently set up with a dynamic private IP address.

5. In the list IP configurations, click **ipconfig1**.
6. On the **ipconfig1** blade, set **Assignment** to **Static**, leave the default value of **IP address** set to **10.40.0.4**.
7. On the **ipconfig1** blade, in the **Public IP address settings** section, select **Associate** and then click **IP address - Configure required settings**.
8. On the **Choose public IP address blade**, click **+ Create new** and create a new public IP address with the following settings:

Setting	Value
Name	**az104-04-pip0**
SKU	**Standard**

9. Back on the **ipconfig1** blade, save the changes.
10. Navigate back to the **az104-04-vnet1** blade and repeat the previous six steps to change the IP address assignment of **ipconfig1** of **az104-04-nic1** to **Static** and associate **az104-04-nic1** with a new Standard SKU public IP address named **az104-04-pip1**.
11. Navigate back to the **az104-04-rg1** resource group blade, in the list of its resources, click **az104-04-vm0**, and from the **az104-04-vm0** virtual machine blade, note the public IP address entry.
12. Navigate back to the **az104-04-rg1** resource group blade, in the list of its resources, click **az104-04-vm1**, and from the **az104-04-vm1** virtual machine blade, note the public IP address entry.
    Note: You will need both IP addresses in the last task of this lab.

Task 4: Configure network security groups

In this task, you will configure network security groups in order to allow for restricted connectivity to Azure virtual machines.

1. In the Azure portal, navigate back to the **az104-04-rg1** resource group blade, and in the list of its resources, click **az104-04-vm0**.
2. On the **az104-04-vm0** blade, click **Connect**, in the drop-down menu, click **RDP**, on the **Connect with RDP** blade, click **Download RDP File** and follow the prompts to start the Remote Desktop session.
3. Note that the connection attempt fails.
   Note: This is expected, because public IP addresses of the Standard SKU, by default, require that the network interfaces to which they are assigned are protected by a network security group. In order to

allow Remote Desktop connections, you will create a network security group explicitly allowing inbound RDP traffic from Internet and assign it to network interfaces of both virtual machines.

4. In the Azure portal, search for and select **Network security groups**, and, on the **Network security groups** blade, click **+ Add**.
5. 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 are using in this lab
Resource Group	**az104-04-rg1**
Name	**az104-04-nsg01**
Region	the name of the Azure region where you deployed all other resources in this lab

6. **Note**: Wait for the deployment to complete. This should take about 2 minutes.
7. On the deployment blade, click **Go to resource** to open the **az104-04-nsg01** network security group blade.
8. On the **az104-04-nsg01** network security group blade, in the **Settings** section, click **Inbound security rules**.
9. Add an inbound rule with the following settings (leave others with their default values):

Setting	Value
Source	**Any**
Source port ranges	*
Destination	**Any**
Destination port ranges	**3389**
Protocol	**TCP**

Setting	Value
Action	**Allow**
Priority	**300**
Name	**AllowRDPInBound**

10. On the **az104-04-nsg01** network security group blade, in the **Settings** section, click **Network interfaces** and then click **+ Associate**.
11. Associate the **az104-04-nsg01** network security group with the **az104-04-nic0** and **az104-04-nic1** network interfaces.
    Note: It may take up to 5 minutes for the rules from the newly created Network Security Group to be applied to the Network Interface Card.

12. Navigate back to the **az104-04-vm0** virtual machine blade.
    Note: Now verify that you can successfully to the target virtual machine and sign in by using the **Student** username and **Pa55w.rd1234** password.

13. On the **az104-04-vm0** blade, click **Connect**, click **Connect**, in the drop-down menu, click **RDP**, on the **Connect with RDP** blade, click **Download RDP File** and follow the prompts to start the Remote Desktop session.
    Note: This step refers to connecting via Remote Desktop from a Windows computer. On a Mac, you can use Remote Desktop Client from the Mac App Store and on Linux computers you can use an open source RDP client software.
    Note: You can ignore any warning prompts when connecting to the target virtual machines.

14. When prompted, sign in by using the **Student** username and **Pa55w.rd1234** password.
    Note: Leave the Remote Desktop session open. You will need it in the next task.

Task 5: Configure Azure DNS for internal name resolution

In this task, you will configure DNS name resolution within a virtual network by using Azure private DNS zones.

1. In the Azure portal, search for and select **Private DNS zones** and, on the **Private DNS zones** blade, click **+ Add**.
2. Create a private DNS zone 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	**az104-04-rg1**
Name	**contoso.org**

3. **Note**: Wait for the private DNS zone to be created. This should take about 2 minutes.
4. Click **Go to resource** to open the **contoso.org** DNS private zone blade.
5. On the **contoso.org** private DNS zone blade, in the **Settings** section, click **Virtual network links**
6. Add a virtual network link with the following settings (leave others with their default values):

Setting	Value
Link name	**az104-04-vnet1-link**
Subscription	the name of the Azure subscription you are using in this lab
Virtual network	**az104-04-vnet1**
Enable auto registration	enabled

7. **Note:** Wait for the virtual network link to be created. This should take less than 1 minute.
8. On the **contoso.org** private DNS zone blade, in the **Settings** section, click **Overview**
9. Verify that the DNS records for **az104-04-vm0** and **az104-04-vm1** appear in the list of record sets as **Auto registered**.

   Note: You might need to wait a few minutes and refresh the page if the record sets are not listed.

10. Switch to the Remote Desktop session to **az104-04-vm0**, right-click the **Start** button and, in the right-click menu, click **Windows PowerShell (Admin)**.
11. In the Windows PowerShell console window, run the following to test internal name resolution of the **az104-04-vm1** DNS record set in the newly created private DNS zone:

    CodeCopy

```
nslookup az104-04-vm1.contoso.org
```

12. Verify that the output of the command includes the private IP address of **az104-04-vm1** (**10.40.1.4**).

Task 6: Configure Azure DNS for external name resolution

In this task, you will configure external DNS name resolution by using Azure public DNS zones.

1. In the Azure portal, search for and select **DNS zones** and, on the **DNS zones** blade, click **+ Add**.
2. Create a DNS zone 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	**az104-04-rg1**
Name	**contoso.org**

3. **Note**: Wait for the DNS zone to be created. This should take about 2 minutes.
4. Click **Go to resource** to open the **contoso.org** DNS zone blade.
5. On the **contoso.org** DNS zone blade, click **+ Record set**.
6. Add a record set with the following settings (leave others with their default values):

Setting	Value
Name	**az104-04-vm0**
Type	**A**
Alias record set	**No**
TTL	**1**

Setting	Value
TTL unit	**Hours**
IP address	the public IP address of **az104-04-vm0** which you identified in the third exercise of this lab

7. Add a record set with the following settings (leave others with their default values):

Setting	Value
Name	**az104-04-vm1**
Type	**A**
Alias record set	**No**
TTL	**1**
TTL unit	**Hours**
IP address	the public IP address of **az104-04-vm1** which you identified in the third exercise of this lab

8. On the **contoso.org** DNS zone blade, note the name of the **Name server 1** entry.
9. In the Azure portal, open the **PowerShell** session in **Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
10. From the Cloud Shell pane, run the following to test external name resolution of the **az104-04-vm0** DNS record set in the newly created DNS zone (replace the placeholder `[Name server 1]` with the name of **Name server 1** you noted earlier in this task):

CodeCopy

```
nslookup az104-04-vm0.contoso.org [Name server 1]
```

11. Verify that the output of the command includes the public IP address of **az104-04-vm0**.
12. From the Cloud Shell pane, run the following to test external name resolution of the **az104-04-vm1** DNS record set in the the newly created DNS zone (replace the placeholder `[Name server 1]` with the name of **Name server 1** you noted earlier in this task):

    CodeCopy

    ```
    nslookup az104-04-vm1.contoso.org [Name server 1]
    ```

13. Verify that the output of the command includes the public IP address of **az104-04-vm1**.

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 'az104-04*'
    ```

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

    ```
    Get-AzResourceGroup -Name 'az104-04*' | 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:

- Created and configured a virtual network
- Deployed virtual machines into the virtual network
- Configured private and public IP addresses of Azure VMs
- Configured network security groups
- Configured Azure DNS for internal name resolution
- Configured Azure DNS for external name resolution