**Module 4: Virtual Networking**

**Exercise 1: Implement Virtual Networking**

#### 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](https://portal.azure.com/).
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 use 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** |

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

1. On the **Virtual networks** blade, click **Refresh** and click **az104-04-vnet1**.
2. On the **az104-04-vnet1** virtual network blade, click **Subnets** and then click **+ Subnet**.
3. 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**.

1. 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.

1. 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](https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-cli).

**Note**: Wait for the deployment to complete before proceeding to the next task. This should take about 2 minutes.

1. 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 actually assigned to the network interfaces, which, in turn are attached to Azure virtual machines, however, it is fairly 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.

1. In the list IP configurations, click **ipconfig1**.
2. On the **ipconfig1** blade, set **Assignment** to **Static**, leave the default value of **IP address** set to **10.40.0.4**.
3. On the **ipconfig1** blade, in the **Public IP address settings** section, select **Associate** and then click **IP address - Configure required settings**.
4. 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** |

1. Back on the **ipconfig1** blade, save the changes.
2. 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**.
3. 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.
4. 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.

1. In the Azure portal, search for and select **Network security groups**, and, on the **Network security groups** blade, click **+ Add**.
2. 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** |

**Note**: Wait for the deployment to complete. This should take about 2 minutes.

1. On the deployment blade, click **Go to resource** to open the **az104-04-nsg01** network security group blade.
2. On the **az104-04-nsg01** network security group blade, in the **Settings** section, click **Inbound security rules**.
3. 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** |
| Action | **Allow** |
| Priority | **300** |
| Name | **AllowRDPInBound** |

1. On the **az104-04-nsg01** network security group blade, in the **Settings** section, click **Network interfaces** and then click **+ Associate**.
2. 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.

1. Navigate back to the **az104-04-vm0** virtual machine blade.

**Note**: Now verify that you can successfully connect to the target virtual machine and sign in by using the **Student** username and **Pa55w.rd1234** password.

1. 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.

1. 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** |

**Note**: Wait for the private DNS zone to be created. This should take about 2 minutes.

1. Click **Go to resource** to open the **contoso.org** DNS private zone blade.
2. On the **contoso.org** private DNS zone blade, in the **Settings** section, click **Virtual network links**
3. 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** |

**Note:** Wait for the virtual network link to be created. This should take less than 1 minute.

1. On the **contoso.org** private DNS zone blade, in the sidebar, click **Overview**
2. 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.

1. 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)**.
2. 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:

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

1. 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 web browser, open a new tab and navigate to <https://www.godaddy.com/domains/domain-name-search>
2. Use the domain name search to identify a domain name which is not in use.
3. In the Azure portal, search for and select **DNS zones** and, on the **DNS zones** blade, click **+ Add**.
4. 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 | **the DNS domain name you identified earlier in this task** |

**Note**: Wait for the DNS zone to be created. This should take about 2 minutes.

1. Click **Go to resource** to open the blade of the newly created DNS zone.
2. On the DNS zone blade, click **+ Record set**.
3. 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** |
| TTL unit | **Hours** |
| IP address | **the public IP address of az104-04-vm0 which you identified in the third exercise of this lab** |

1. 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** |

1. On the DNS zone blade, note the name of the **Name server 1** entry.
2. In the Azure portal, open the **PowerShell** session in **Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. 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] including the [] brackets, with the name of **Name server 1** you noted earlier in this task and the `[domain name] placeholder with the name of the DNS domain you created earlier in this task):

*nslookup az104-04-vm0.[domain name] [Name server 1]*

1. Verify that the output of the command includes the public IP address of **az104-04-vm0**.
2. 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 and the `[domain name] placeholder with the name of the DNS domain you created earlier in this task):

*nslookup az104-04-vm1.[domain name] [Name server 1]*

1. 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:

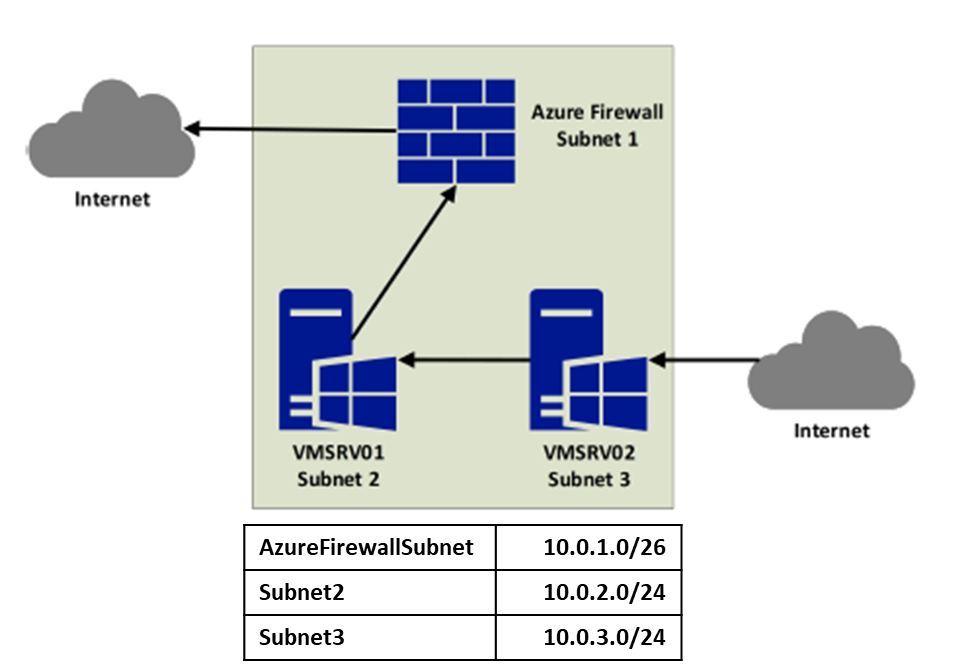
*Get-AzResourceGroup -Name 'az104-04\*'*

1. 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.

**Exercise 2: Create Azure Firewall on Virtual Network**



#### Task 1: 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**.

1. 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 **az104-04b-vms-template.json** and **az104-04b-vms-parameters.json** into the Cloud Shell home directory.

**Note**: You might need to upload each file separately.

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

*$rgName = 'az104-04b-rg1'*

*New-AzResourceGroup -name $rgname -location "westeurope"*

*New-AzResourceGroupDeployment `*

*-ResourceGroupName $rgName `*

*-TemplateFile $HOME/az104-04b-vms-template.json `*

*-TemplateParameterFile $HOME/az104-04b-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](https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-cli).

**Note**: Wait for the deployment to complete before proceeding to the next task. This should take about 2 minutes.

1. Close the Cloud Shell pane.
2. In the Azure portal, search for and select **Public IP addresses**, and click **+ Create**.
3. In the **Create public IP address** blade, create the public IP address with the following settings and then click **Create**:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| IP Version | **IPv4** |
| SKU | **Standard** |
| Tier | **Regional** |
| Name | **az104-04b-vmpip** |
| Resource group | **az104-04b-rg1** |
| Location | **the name of any Azure region available in the subscription you will use in this lab** |
| Availability zone | **Zone-redundant** |

1. In the Azure portal, search for and select **Network interfaces**, and then select **vmsrv02-nic1**.
2. In the **vmsrv02-nic1** settings blade, click **Networking – IP configurations**.
3. In the **IP configurations** select **ipconfig1**.
4. In the **ipconfig1 – Public IP address settings**, click **Associate** and then select **az104-04b-vmpip**, click **Save**.
5. In the Azure portal, search for and select **Virtual Machine**, and select the VM named **vmsrv01**.
6. In the **vmsrv01 – overview** take note about the private IP address assigned to virtual machine **vmsrv01**.
7. In the Azure portal, search for and select **Network security groups**, and click **Create network security group**.
8. In the **Create network security group** blade, create the security group with the following settings and then click **Review +** **Create**:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource group | **az104-04b-rg1** |
| Name | **az104-04b-sg01** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |

1. In the **az104-04b-sg01 – settings** blade, click **Inbound security rules** and then click **+ Add** to create a NSG rule with following settings, and then click **Add**:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Source | **Any** |
| Source port ranges | **\*** |
| Destination | **Any** |
| Service | **RDP** |
| Action | **Allow** |
| Priority | **100** |
| Name | **Port\_3389** |

1. In the **az104-04b-sg01 – settings** blade, click **Subnets** and then click **+ Associate** to associate the NSG with subnet3 with following settings, and then click **Ok**:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-04b-vnet1** |
| Subnet | **subnet3** |

#### Task 2: Create Firewall subnet

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, search for and select **Virtual networks**, and select **az104-04b-vnet1**.
3. In the Settings blade select Subnets and the click **+ Subnet**.
4. In the **Add subnet** create the **Firewall** subnet with the following settings (leave others with their default values), and the click **Save**.

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **AzureFirewallSubnet** |
| Subnet address range | **10.0.1.0/26** |

#### Task 3: Create Azure Firewall

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

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **the name of a new resource group az104-04b-rg1** |
| Name | **az104-04b-fw** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Availability zone | **1** |
| Firewall tier | **Standard** |
| Firewall management | **Use Firewall rules (classic) to manage this firewall** |
| Virtual Network | **az104-04b-vnet1** |
| Public IP address | **New, az104-04b-fwpip** |
| Forced tunneling | **Disabled** |

1. Take note about the Firewall private IP address assigned to the Firewall.

#### Task 4: Create a Route Table

In this task, you will create a Static Route to manage the private Subnets.

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

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | **the name of the Azure subscription you will use in this lab** |
| Resource Group | **the name of a new resource group az104-04b-rg1** |
| Region | **the name of any Azure region available in the subscription you will use in this lab** |
| Name | **az104-04b-rt** |

1. In the **Route table** click **Subnets** and then click **+ Associate** to associate subnet with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Virtual network | **az104-04b-vnet1** |
| Subnet | **subnet2** |

1. In the **Route table** click **Routes** and then click **+ Add** to add a static route with the following settings, and then click **Add**.

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Route name | **fw-internet** |
| Address prefix source | **IP Addresses** |
| Source IP Address/CIDR ranges | **0.0.0.0/0** |
| Next hop type | **Virtual appliance** |
| Next hop address | **The Firewall private IP Address noted in task 3** |

#### Task 5: Create an Application Firewall Rule

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, search for and select **Firewalls**, and select **az104-04b-fw**.
3. In the **az104-04b-fw** select Rules (classic) and then select **Application rule collection**.
4. Click **+ Add application rule collection** to create the rule with the following settings, and then click **Add**.

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **appcollection01** |
| Priority | **150** |
| Action | **Allow** |
| **Rules – Target FQDNs** | |
| Name | **allow-google** |
| Source type | **IP Address** |
| Source | **10.0.2.0/24** |
| Protocol: Port | **HTTP, HTTPS** |
| Target FQDNs | [www.google.com](http://www.google.com)**,\*.google.com** |
| Name | **allow-microsoft** |
| Source type | **IP Address** |
| Source | **10.0.2.0/24** |
| Protocol: Port | **HTTP, HTTPS** |
| Target FQDNs | [www.microsoft.com](http://www.microsoft.com)**,\*.microsoft.com** |

#### Task 6: Create a Network Firewall Rule

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, search for and select **Firewalls**, and select **az104-04b-fw**.
3. In the **az104-04b-fw** select Rules (classic) and then select **Network rule collection**.
4. Click **+ Add network rule collection** to create the rule with the following settings, and then click **Add**.

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **netcollection01** |
| Priority | **150** |
| Action | **Allow** |
| **Rules – IP Addresses** | |
| Name | **allow-google** |
| Protocol | **UDP** |
| Source type | **IP Address** |
| Source | **10.0.2.0/24** |
| Destination type | **IP Address** |
| Destination Address | **8.8.8.8, 8.8.4.4** |
| Destination Port | **53** |

#### Task 7: Testing a Network Firewall Rule

1. Connect by RDP to the virtual machine named **VMSRV02**.
2. From **VMSRV02** connect by RDP to the private IP address assigned to virtual machine named **VMSRV01**.
3. In the VMSRV01 open Internet Explorer Browser and the try to connect to the following URLs:
   * [www.microsoft.com](http://www.microsoft.com)
   * [www.google.com](http://www.google.com)
   * www.cisco.com
4. Check which the above URLs are ready to connect.