Implementing Advanced Virtual Networking

Lab: Implementing Azure Load Balancer Standard

Scenario

Adatum Corporation wants to implement Azure Load Balancer Standard to direct inbound and outbound traffic of Azure VMs.

Objectives

After completing this lab, you will be able to:

- Implement inbound load balancing by using Azure Load Balancer Standard
- Configure outbound SNAT traffic by using Azure Load Balancer Standard

Lab Setup

Estimated Time: 45 minutes

User Name: **Student**

Password: **Pa55w.rd**

Exercise 1: Implement inbound load balancing and NAT by using Azure Load Balancer Standard

The main tasks for this exercise are as follows:

1. Deploy Azure VMs in an availability set by using an Azure Resource Manager template
2. Create an instance of Azure Load Balancer Standard
3. Create a load balancing rule of Azure Load Balancer Standard
4. Create a NAT rule of Azure Load Balancer Standard
5. Test functionality of Azure Load Balancer Standard

Task 1: Deploy Azure VMs in an availability set by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **Bash** session within the **Cloud Shell**.
3. If you are presented with the **You have no storage mounted** message, configure storage by clicking on **Show advanced settings** and using the following settings:
   - Subsciption: the name of the target Azure subscription
   - Cloud Shell region: the name of the Azure region that is available in your subscription and which is closest to the lab location

- Resource group: the name of a new resource group **az3000800-LabRG**
- Storage account: a name of a new storage account
- File share: a name of a new file share

4. From the Cloud Shell pane, create a resource groups by running (replace the `<Azure region>` placeholder with the name of the Azure region that is available in your subscription and which is closest to the lab location)

```
az group create --name az3000801-LabRG --location <Azure region>
```

5. From the Cloud Shell pane, upload the Azure Resource Manager template **C:\allfiles\AZ-300T03\Module_03\azuredeploy0801.json** into the home directory.

6. From the Cloud Shell pane, upload the parameter file **C:\allfiles\AZ-300T03\Module_03\azuredeploy0801.parameters.json** into the home directory.

7. From the Cloud Shell pane, deploy a pair of Azure VMs hosting Windows Server 2016 Datacenter by running:

```
az group deployment create --resource-group az3000801-LabRG \
--template-file azuredeploy0801.json \
--parameters @azuredeploy0801.parameters.json

> **Note**: Wait for the deployment before you proceed to the next task.
This might take about 10 minutes.
```

8. In the Azure portal, close the Cloud Shell pane.

Task 2: Create an instance of Azure Load Balancer Standard

1. In the Azure portal, create a new Azure Load Balancer with the following settings:
   - Name: **az3000801-lb**
   - Type: **Public**
   - SKU: **Standard**
   - Public IP address: **Create new** named **az3000801-lb-pip01**
   - Availability zone: **Zone-redundant**
   - Subsciption: the name of the target Azure subscription
   - Resource group: **az3000801-LabRG**
   - Location: the name of the Azure region in which you deployed Azure VMs in the previous task of this exercise

Task 3: Create a load balancing rule of Azure Load Balancer Standard

1. In the Azure portal, navigate to the blade displaying the properties of the newly deployed Azure Load Balancer **az3000801-lb**.

2. On the **az3000801-lb** blade, click **Backend pools**.

3. On the **az3000801-lb - Backend pools** blade, click **+ Add**.
4. On the **Add backend pool** blade, specify the following settings and click **Add**:
   - Name: **az3000801-bepool**
   - Virtual network: **az3000801-vnet (2 VM)**
   - VIRTUAL MACHINE: **az3000801-vm0**
     IP ADDRESS: **ipconfig1 (10.0.0.4)** or **ipconfig1 (10.0.0.5)**
   - VIRTUAL MACHINE: **az3000801-vm1**
     IP ADDRESS: **ipconfig1 (10.0.0.5)** or **ipconfig1 (10.0.0.4)**

   Note: It is possible that the IP addresses of VMs are assigned in the reversed order.

   Note: Wait for the operation to complete. This should not take more than 1 minute.
5. Back on the **az3000801-lb - Backend pools** blade, click **Health probes**.
6. On the **az3000801-lb - Health probes** blade, click **+ Add**.
7. On the **Add health probe** blade, specify the following settings and click **OK**:
   - Name: **az3000801-healthprobe**
   - Protocol: **TCP**
   - Port: **80**
   - Interval: **5**
   - Unhealthy threshold: **2**

   Note: Wait for the operation to complete. This should not take more than 1 minute.
8. Back on the **az3000801-lb - Health probes** blade, click **Load balancing rules**.
9. On the **az3000801-lb - Load balancing rules** blade, click **+ Add**.
10. On the **Add load balancing rule** blade, specify the following settings and click **OK**:
    - Name: **az3000801-lbrule01**
    - IP Version: **IPv4**
    - Frontend IP address: select the public IP address assigned to the **LoadBalancedFrontEnd** from the drop-down list
    - Protocol: **TCP**
    - Port: **80**
    - Backend port: **80**
    - Backend pool: **az3000801-bepool (2 virtual machines)**
    - Health probe: **az3000801-healthprobe (TCP:80)**

- Session persistence: **None**
- Idle timeout (minutes): **4**
- Floating IP (direct server return): **Disabled**

Note: Wait for the operation to complete. This should not take more than 1 minute.

Task 4: Create a NAT rule of Azure Load Balancer Standard

1. In the Azure portal, on the **az3000801-lb** blade, click **Inbound NAT rules**.
2. On the **az3000801-lb - Inbound NAT rules** blade, click **+ Add**.
3. On the **Add inbound NAT rule** blade, specify the following settings and click **OK**:
   - Name: **az3000801-vm0-RDP**
   - Frontend IP address: select the public IP address assigned to the **LoadBalancedFrontEnd** from the drop-down list
   - IP Version: **IPv4**
   - Service: **RDP**
   - Protocol: **TCP**
   - Port: **33890**
   - Target virtual machine: **az3000801-vm0**
   - Network IP configuration: **ipconfig1 (10.0.0.4)** or **ipconfig1 (10.0.0.5)**
   - Port mapping: **Custom**
   - Floating IP (direct server return): **Disabled**
   - Target port: **3389**

   Note: Wait for the operation to complete. This should not take more than 1 minute.
4. Back on the **az3000801-lb - Inbound NAT rules** blade, click **+ Add**.
5. On the **Add inbound NAT rule** blade, specify the following settings and click **OK**:
   - Name: **az3000801-vm1-RDP**
   - Frontend IP address: select the public IP address assigned to the **LoadBalancedFrontEnd** from the drop-down list
   - IP Version: **IPv4**
   - Service: **RDP**
   - Protocol: **TCP**
   - Port: **33891**

- Target virtual machine: **az3000801-vm1**
- Network IP configuration: **ipconfig1 (10.0.0.5)** or **ipconfig1 (10.0.0.4)**
- Port mapping: **Custom**
- Floating IP (direct server return): **Disabled**
- Target port: **3389**

Note: Wait for the operation to complete. This should not take more than 1 minute.

Task 5: Test functionality of Azure Load Balancer Standard

1. In the Azure portal, navigate to the **az3000801-lb** blade and note the value of the **Public IP address** entry.
2. On the lab computer, start Microsoft Edge and navigate to the IP address you identified in the previous step.
3. Verify that you are presented with the default **Internet Information Services Welcome** page.
4. On the lab computer, right-click **Start**, click **Run**, and, from the **Open** text box, run the following (replace the `<IP address>` placeholder with the public IP address you identified earlier in this task):

   ```
   mstsc /v:<IP address>:33890
   ```

5. When prompted, authenticate by specifying the following values:
   - User name: **Student**
   - Password: **Pa55w.rd1234**
6. Within the Remote Desktop session, switch to the **Local Server** view in the Server Manager window and verify that you are connected to **az3000801-vm0** Azure VM.
7. Switch to the lab computer, right-click **Start**, click **Run**, and, from the **Open** text box, run the following (replace the `<IP address>` placeholder with the IP address you identified earlier in this task):

   ```
   mstsc /v:<IP address>:33891
   ```

8. When prompted, authenticate by specifying the following values:
   - User name: **Student**
   - Password: **Pa55w.rd1234**
9. Within the Remote Desktop session, switch to the **Local Server** view in the Server Manager window and verify that you are connected to **az3000801-vm1** Azure VM.
10. Within the Remote Desktop session, start a Windows PowerShell session and run the following to determine your current public IP address:

    ```
    Invoke-RestMethod http://ipinfo.io/json
    ```

11. Review the output of the cmdlet and verify that the IP address entry matches the public IP address you identified earlier in this task.

12. Leave the Remote Desktop sessions open. You will use them in the next exercise.

Result: After you completed this exercise, you have implemented and tested Azure Load Balancer Standard inbound load balancing and NAT rules

Exercise 2: Configure outbound SNAT traffic by using Azure Load Balancer Standard

The main tasks for this exercise are as follows:

1. Deploy Azure VMs into an existing virtual network by using an Azure Resource Manager template
2. Create an Azure Standard Load Balancer and configure outbound SNAT rules
3. Test outbound rules of Azure Standard Load Balancer

Task 1: Deploy Azure VMs into an existing virtual network by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **Bash** session within the **Cloud Shell**.
3. From the Cloud Shell pane, upload the Azure Resource Manager template **C:\allfiles\AZ-300T03\Module_03\azuredeploy0802.json** into the home directory.
4. From the Cloud Shell pane, upload the parameter file **C:\allfiles\AZ-300T03\Module_03\azuredeploy0802.parameters.json** into the home directory.
5. From the Cloud Shell pane, deploy a pair of Azure VMs hosting Windows Server 2016 Datacenter by running:

```
az group deployment create --resource-group az3000801-LabRG \
--template-file azuredeploy0802.json \
--parameters @azuredeploy0802.parameters.json

> **Note**: Wait for the deployment before you proceed to the next task. This might take about 5 minutes.
```

6. In the Azure portal, close the Cloud Shell pane.

Task 2: Create an Azure Standard Load Balancer and configure outbound SNAT rules

1. In the Azure portal, in the Microsoft Edge window, start a **Bash** session within the **Cloud Shell**.

2. In the Azure portal, from the Cloud Shell pane, run the following to create an outbound public IP address of the load balancer:

```
az network public-ip create --resource-group az3000801-LabRG \
--name az3000802-lb-pip01 --sku standard
```

1. In the Azure portal, from the Cloud Shell pane, run the following to create an Azure Load Balancer Standard:

```
LOCATION=$(az group show --name az3000801-LabRG \
--query location --out tsv)

az network lb create --resource-group az3000801-LabRG \
--name az3000802-lb --sku standard --backend-pool-name az3000802-bepool \
--frontend-ip-name loadBalancedFrontEndOutbound --location $LOCATION \
--public-ip-address az3000802-lb-pip01
```

1. From the Cloud Shell pane, run the following to create an outbound rule:

```
az network lb outbound-rule create --resource-group az3000801-LabRG \
--lb-name az3000802-lb --name outboundRuleaz30000802 \
--frontend-ip-configs loadBalancedFrontEndOutbound --protocol All \
--idle-timeout 15 --outbound-ports 10000 --address-pool az3000802-bepool
```

```
> **Note**: Wait for the operation to complete. This should not take more
than 1 minute.
```

1. Close the Cloud Shell pane.

2. In the Azure portal, navigate to the blade displaying the properties of the Azure Load Balancer **az3000802-lb**.

3. On the **az3000802-lb** blade, click **Backend pools**.

4. On the **az3000802-lb - Backend pools** blade, click **az3000802-bepool**.

5. On the **az3000802-bepool** blade, specify the following settings and click **Save**:

   - Virtual network: **az3000801-vnet (4 VM)**
   - VIRTUAL MACHINE: **az3000802-vm0**
     IP ADDRESS: **ipconfig1 (10.0.1.4)** or **ipconfig1 (10.0.1.5)**
   - VIRTUAL MACHINE: **az3000802-vm1**
     IP ADDRESS: **ipconfig1 (10.0.1.5)** or **ipconfig1 (10.0.1.4)**

   Note: Wait for the operation to complete. This should not take more than 1 minute.

Task 3: Verify that the outbound rule took effect

1. In the Azure portal, navigate to the **az3000802-lb** blade and note the value of the **Public IP address** entry.

2. On the lab computer, from the Remote Desktop session to **az3000801-vm0**, run the following to start a Remote Desktop session to **az3000802-vm0**.

```
mstsc /v:az3000802-vm0
```

1. When prompted, authenticate by specifying the following values:
   - User name: **Student**
   - Password: **Pa55w.rd1234**
2. Within the Remote Desktop session to **az3000802-vm0**, start a Windows PowerShell session and run the following to determine your current public IP address:

   ```
   Invoke-RestMethod http://ipinfo.io/json
   ```

1. Review the output of the cmdlet and verify that the IP address entry matches the public IP address you identified earlier in this task.

Result: After you completed this exercise, you have configured and tested Azure Load Balancer Standard outbound rules