Azure Network Watcher (Portal)

(LAB-103-06-05)

Part A: Create Azure Virtual Machine

1. Create Azure Virtual Machine
    a. Region: East US
    b. OS: Windows 2109
    c. Port: None
    d. Resource group: RG-103-06-05
    e. Virtual machine name: VM01-LAB-1030605

Part B: Enable Network Watcher

1. In the portal, go to left side, select **All services**. In the **Filter box**, enter ***Network Watcher***.
2. When **Network Watcher** appears in the results, select it. Also enable the star to make it favourite. Now it should be shown on the left side
3. Go to the left side & select **Network Watcher**
4. Enable a network watcher in the East US region, because that's the region the VM was deployed to in a previous step.
   Select **Regions**, to expand it, and then right click on the right of **East US.**
5. Select **Enable Network Watcher**.

Part C: Use IP flow verify

When you create a VM, Azure allows and denies network traffic to and from the VM, by default. You might later override Azure's defaults, allowing or denying additional types of traffic.

1. Go to the left side, select **Network Watcher**.
2. Select **IP flow verify**, under **Network diagnostic tools** blade
3. Enter or select the following values, and then select **Check**
    a. Subscription: Select your default subscription

b. Resource group Select **RG-103-06-05**

c. Virtual machine Select **VM01-LAB-1030605**

d. Network interface: Select the default network interface

e. Protocol: **TCP**

f. Direction: **Outbound**

g. Local IP address: It will show the Private IP Address of the VM

h. Local port: **60000**

i. Remote IP address: **13.107.21.200** - One of the addresses for <www.bing.com>.

j. Remote port: **80**

4. After a few seconds, the result returned informs you that access is allowed because of a security rule named **AllowInternetOutbound**.

   Note: Refer the NSG mapped to the virtual machine to review the rules

5. Complete step 3 again but change the **Remote IP address** to **172.31.0.100**. The result returned informs you that access is denied because of a security rule named **DefaultOutboundDenyAll**.

6. Complete step 3 again, but change the **Direction** to **Inbound**, the **Local port** to **80** and the **Remote port** to **60000**. The result returned informs you that access is denied because of a security rule named **DefaultInboundDenyAll**.

7. Now that you know which security rules are allowing or denying traffic to or from a VM, you can determine how to resolve the problems.

   Open the Port 80 of VM01-LAB-1030605 virtual machine

8. Open below URL to check your public IP address

   https://www.whatismyip.com

9. Complete step 3 again but change **Remote IP address** to <**your Public IP Address**>. The result returned informs you that access is allowed because of a network security group security rule (Rule for Port 80)

Part D: Use next hop

Azure automatically creates routes to default destinations. You may create custom routes that override the default routes. Sometimes, custom routes can cause communication to fail. Use the next hop capability of Network Watcher to determine which route Azure is using to route traffic.

1. In the Azure portal, select **Next hop**, under **Network Watcher**.
2. Enter or select the following values, and then select **Next hop**
    a. Subscription: Select your default subscription
    b. Resource group Select **RG-103-06-05**
    c. Virtual machine Select **VM01-LAB-1030605**
    d. Network interface: Select the default network interface
    e. Source IP address: It will show the Private IP Address of the VM
    f. Destination IP address: **13.107.21.200** - One of the addresses for <www.bing.com>.
3. After a few seconds, the result informs you that the next hop type is **Internet**, and that the **Route table ID** is **System Route**. This result lets you know that there is a valid system route to the destination.
4. Change the **Destination IP address** to ***172.31.0.100*** and select **Next hop** again. The result returned informs you that **None** is the **Next hop type**, and that the **Route table ID** is also **System Route**. This result lets you know that, while there is a valid system route to the destination, there is no next hop to route the traffic to the destination.