Module 15 - Lab 5A: Monitor network communication between two virtual machines using the Azure portal

Successful communication between a virtual machine (VM) and an endpoint such as another VM, can be critical for your organization. Sometimes, configuration changes are introduced which can break communication. In this tutorial, you learn how to:

- Create two VMs
- Monitor communication between VMs with the connection monitor capability of Network Watcher
- Generate alerts on Connection Monitor metrics
- Diagnose a communication problem between two VMs, and learn how you can resolve it

If you don't have an Azure subscription, create a **free account** before you begin.

Task 1: Create the first VM

□ 1. Sign in to the **Azure portal** **https://portal.azure.com** with the username **sheikhnasir3WHI5@gdcs0.com** and password **O7XgUFHcKzzR3AWD**

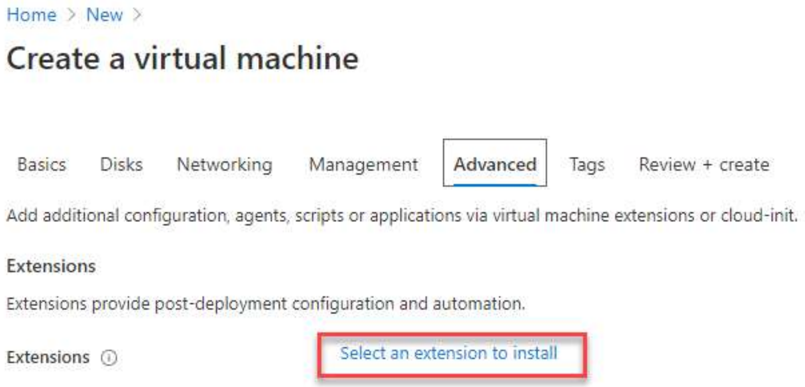
□ 2. Select **+ Create a resource** found on the upper, left corner of the Azure portal.

□ 3. Select **Compute**, and then select **Virtual Machine**.

□ 4. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **OK**:

Setting	Value
Subscription	Select your subscription.
Resource group	Select **myResourceGroup**
Name	**myVm1**
Location	Select **East US**
Image	Select **Windows Server 2016 Datacenter Gen2**
Suze	Select **Standard_DS1_v2**
User name	**localadmin**
Password	**O7XgUFHcKzzR3AWD**

□ 5. Select the **Advanced** tab, select **Select an Extension to install**.



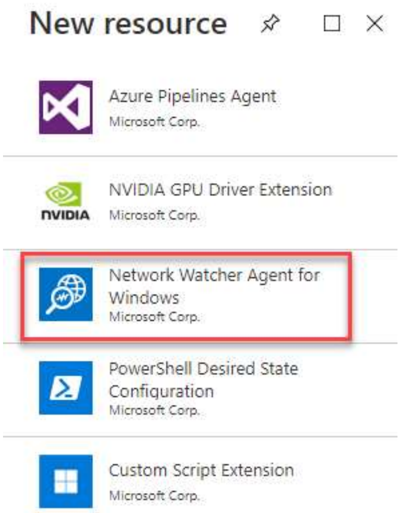
Create a virtual machine

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

□ 6. select **Network Watcher Agent for Windows**, as shown in the following picture:



☐ 7. Click **Create** and then click **OK**.

☐ 8. Click **Review + create** and then select **Create** to start VM deployment.

Task 2: Create the second VM

Complete the steps in Task 1 again, with the following changes:

Step	Setting	Value
1	Select a version of **Ubuntu Server**	
3	Name	myVm2
4	image	Ubuntu Server 20.04 LTS Gen 2
3	Authentication type	select **Password**, and enter localadmin and O7XgUFHcKzzR3AWD
3	Resource group	Select **Use existing** and select myResourceGroup.
6	Extensions	**Network Watcher Agent for Linux**

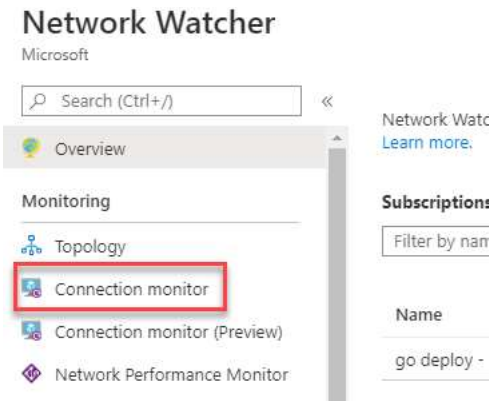
The **VM** takes a few minutes to **deploy**. Wait for the **VM** to finish **deploying** before continuing with the remaining steps.

Task 2a: Create a connection monitor

Create a connection monitor to monitor communication over TCP port 22 from *myVm1* to *myVm2*.

☐ 1. At the top of the Azure Portal search for and select **Network Watcher**.

☐ 2. Under **Monitoring**, select **Connection monitor (Classic)**.

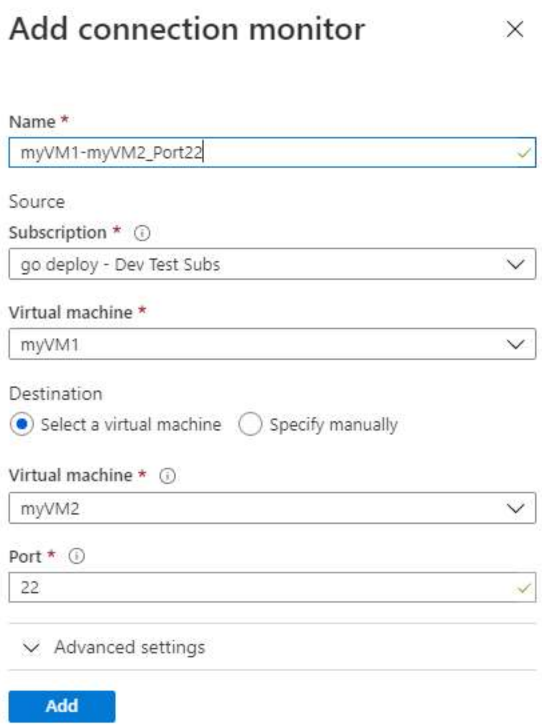


☐ 3. Select **+ Add**.

☐ 4. Enter or select the information for the connection you want to monitor, and then select **Add**. In the example shown in the following picture, the connection monitored is from the *myVm1* VM to the *myVm2* VM over port 22:

Setting	Value
Name	myVm1myVm2Port22
Source	

Setting	Value
Virtual machine	myVm1
Destination	
Select a virtual machine	
Virtual machine	myVm2
Port	22



Add connection monitor

Name *
myVM1-myVM2_Port22

Source
Subscription *
go deploy - Dev Test Subs

Virtual machine *
myVM1

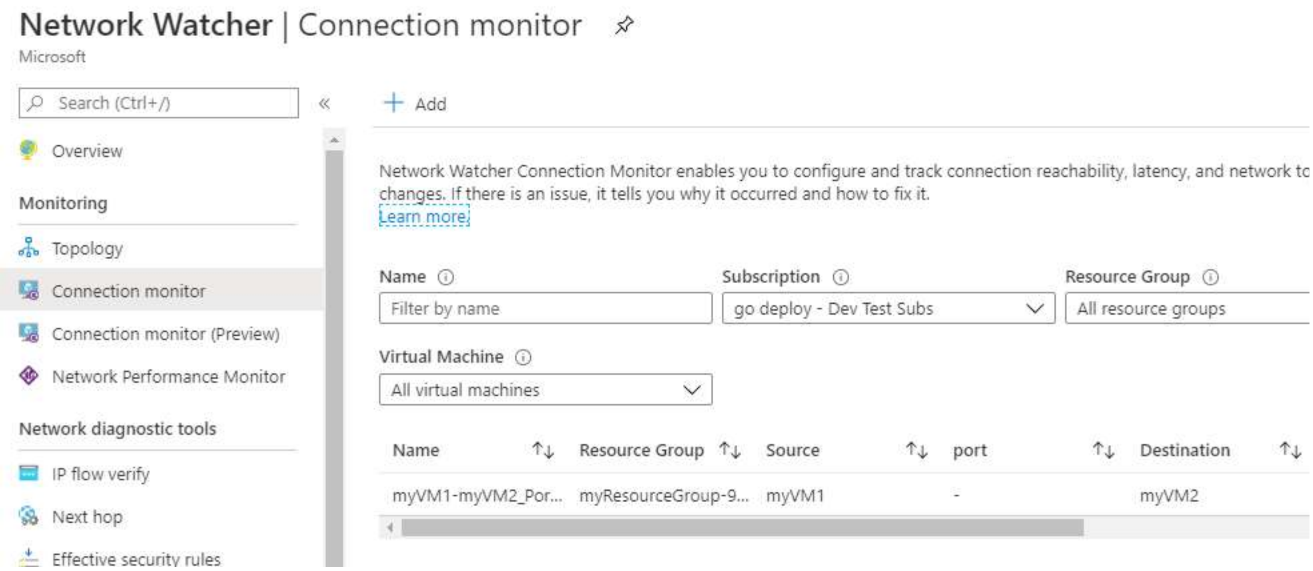
Destination
● Select a virtual machine ○ Specify manually

Virtual machine *
myVM2

Port *
22

Task 3: View a connection monitor

□ 1. You see a list of existing connection monitors, as shown in the following picture:



Network Watcher | Connection monitor
Microsoft

Network Watcher Connection Monitor enables you to configure and track connection reachability, latency, and network to changes. If there is an issue, it tells you why it occurred and how to fix it.
Learn more.

Name: Filter by name
Subscription: go deploy - Dev Test Subs
Resource Group: All resource groups
Virtual Machine: All virtual machines

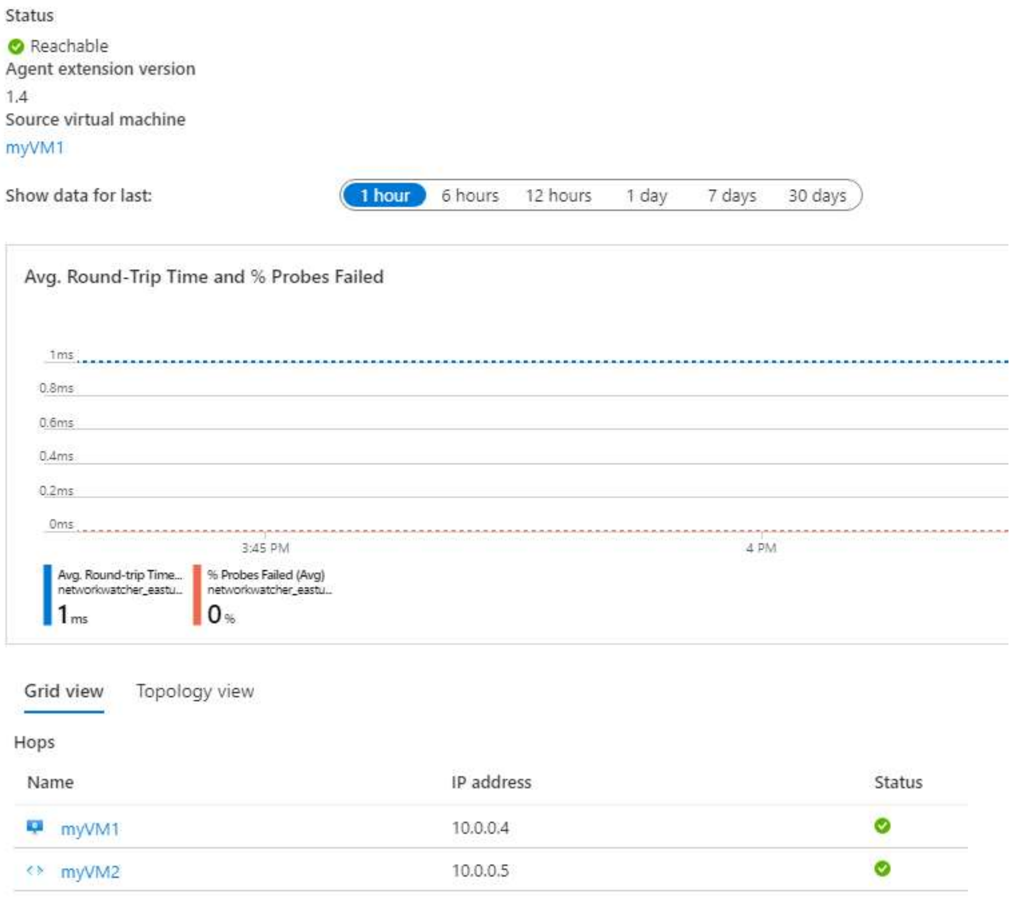
Name	Resource Group	Source	port	Destination
myVM1-myVM2_Por...	myResourceGroup-9...	myVM1	-	myVM2

□ 2. Select the monitor with the name **myVm1myVm2Port22**, as shown in the previous picture, to see details for the monitor, as shown in the following picture:

Note the following information:

Item	Value	Details
Status	Reachable	Lets you know whether the endpoint is reachable or not.

Item	Value	Details
AVG. ROUND-TRIP	Lets you know the round-trip time to make the connection, in milliseconds. Connection monitor probes the connection every 60 seconds, so you can monitor latency over time.	
Hops	Connection monitor lets you know the hops between the two endpoints. In this example, the connection is between two VMs in the same virtual network, so there is only one hop, to the 10.0.0.5 IP address. If any existing system or custom routes, route traffic between the VMs through a VPN gateway, or network virtual appliance, for example, additional hops are listed.	
STATUS	The green check marks for each endpoint let you know that each endpoint is healthy.	



Status

✓ Reachable

Agent extension version

1.4

Source virtual machine

myVM1

Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

Avg. Round-Trip Time and % Probes Failed

1ms
0.8ms
0.6ms
0.4ms
0.2ms
0ms
3:45 PM
4 PM
Avg. Round-trip Time... networkwatcher_eastu...
1 ms
% Probes Failed (Avg) networkwatcher_eastu...
0 %
Grid view
Topology view

Hops

Name	IP address	Status
myVM1	10.0.0.4	✓
myVM2	10.0.0.5	✓

Task 4: View a problem

> By default, Azure allows communication over all ports between VMs in the same virtual network. Over time, you, or someone in your organization, might override Azure's default rules, inadvertently causing a communication failure.

Complete the following steps to create a communication problem and then view the connection monitor again:

☐ 1. In the search box at the top of the portal, enter *myResourceGroup*. When the **myResourceGroup** resource group appears in the search results, select it.

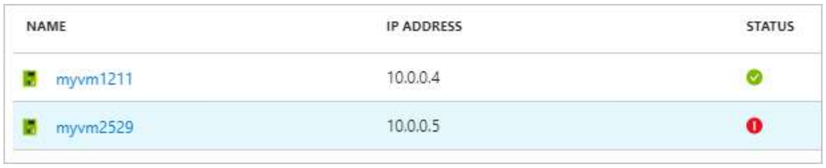
☐ 2. Select the **myVm2-nsg** network security group.

☐ 3. Select **Inbound security rules**, and then select **Add**, as shown in the following picture:

☐ 4. The default rule that allows communication between all VMs in a virtual network is the rule named **AllowVnetInBound**. Create a rule with a higher priority (lower number) than the **AllowVnetInBound** rule that denies inbound communication over port 22. Select, or enter, the following information, accept the remaining defaults, and then select **Add**:

Setting	Value
Destination port ranges	22
Action	Deny
Priority	100
Name	DenySshInbound

□ 5. Since connection monitor probes at 60-second intervals, wait a few minutes and then on the left side of the portal, select **Network Watcher**, then **Connection monitor (Classic)**, and then select the **myVm1-myVm2_Port22)** monitor again. The results are different now, as shown in the following picture:



NAME	IP ADDRESS	STATUS
myvm1211	10.0.0.4	✓
myvm2529	10.0.0.5	❗

You can see that there's a red exclamation icon in the status column for the **myvm2529** network interface.

□ 6. To learn why the status has changed, select 10.0.0.5, in the previous picture. Connection monitor informs you that the reason for the communication failure is: *Traffic blocked due to the following network security group rule: UserRule_DenySshInbound*.