😊 Azure Network Watcher

Azure Network Watcher is a robust network monitoring and troubleshooting service provided by Microsoft Azure. It offers a suite of tools and capabilities to monitor, diagnose, and gain insights into the network infrastructure deployed within Azure. Here's an overview of its features and functionalities:

1. **Topology:** Network Watcher provides a visual representation of the network topology within an Azure subscription. This helps users understand the layout of their network resources, including virtual networks (VNets), subnets, and connected devices.
2. **Connection Monitor:** This feature allows you to monitor connectivity between virtual machines, VMSS instances, and other endpoints within your Azure network. It provides insights into network latency, packet loss, and availability, helping you diagnose connectivity issues and optimize network performance.
3. **Network Performance Monitor (NPM):** NPM is a comprehensive monitoring solution within Network Watcher that offers insights into network performance across hybrid and multi-cloud environments. It enables you to monitor network latency, packet loss, and throughput between various endpoints, helping you identify and resolve performance bottlenecks.
4. **Packet Capture:** Network Watcher allows you to capture network traffic to and from Azure VMs for analysis and troubleshooting purposes. You can initiate packet captures on specific VMs or subnets, filter traffic based on various criteria, and download captured packets for offline analysis.
5. **Security Group View:** This feature provides visibility into the effective security rules applied to network security groups (NSGs) within your Azure environment. It helps you understand how NSG rules are evaluated and applied to network traffic, facilitating better security posture and compliance.
6. **Next Hop:** Network Watcher allows you to determine the next hop for traffic leaving a virtual machine in your Azure network. This is useful for troubleshooting routing issues and verifying network connectivity paths.
7. **VPN Diagnostics:** For Azure Virtual Network Gateways and VPN connections, Network Watcher offers diagnostic tools to identify and resolve connectivity issues. It helps troubleshoot VPN tunnel establishment, routing, and security configuration problems.
8. **IP Flow Verify:** This tool allows you to verify if traffic is allowed or denied based on NSG rules and route tables. It helps ensure that network traffic is following the expected path and security policies within your Azure environment.
9. **DNS Analytics:** Network Watcher provides DNS analytics to monitor and troubleshoot DNS queries originating from Azure VMs. It helps identify DNS-related issues, such as misconfigurations or DNS resolution failures.

Overall, Azure Network Watcher is a valuable tool for monitoring, troubleshooting, and optimizing network performance and security within Azure environments, helping organizations ensure reliable and efficient operation of their network infrastructure.

😄 Use cases of Network Watcher:

Azure Network Watcher offers several use cases across network monitoring, diagnostics, and optimization within Azure environments:

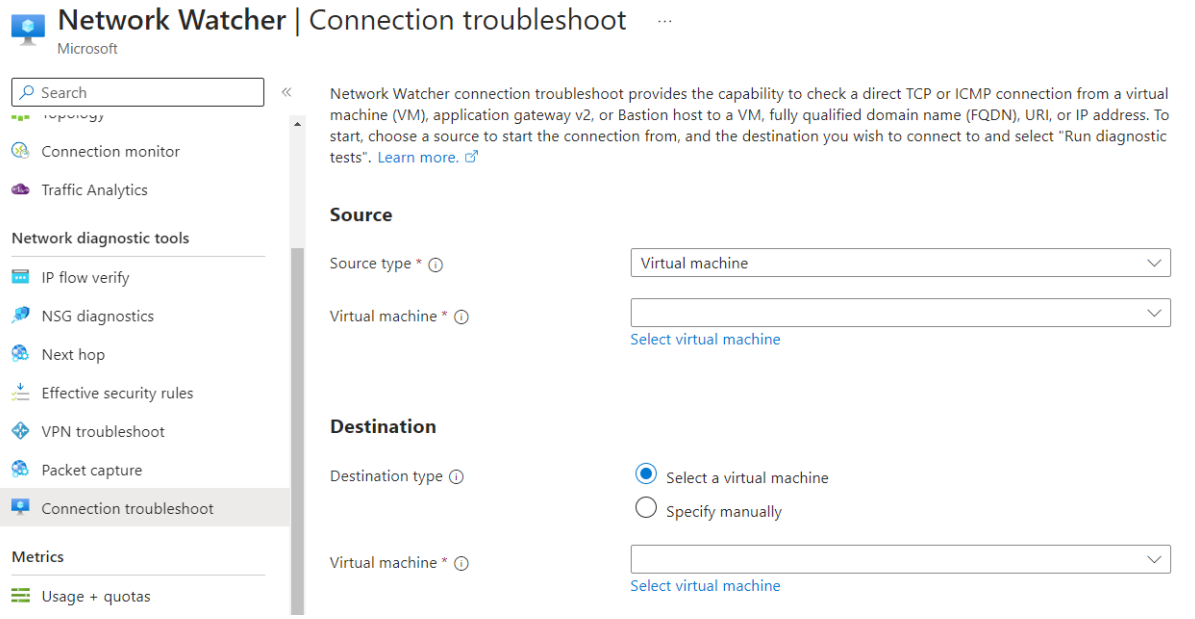
1. **Connectivity Monitoring:** Network Watcher's Connection Monitor feature enables continuous monitoring of connectivity between Azure VMs, VMSS instances, and other endpoints. Use this to ensure reliable communication between critical resources and detect connectivity issues in real-time.
2. **Performance Optimization:** With Network Performance Monitor (NPM), you can monitor network latency, packet loss, and throughput between various Azure resources. Use this data to identify performance bottlenecks, optimize network configurations, and enhance the user experience of applications hosted in Azure.
3. **Troubleshooting Connectivity Issues:** When experiencing connectivity problems between Azure VMs or between Azure and on-premises resources, Network Watcher's diagnostic tools such as Next Hop and IP Flow Verify can help pinpoint the root cause of connectivity failures and assist in troubleshooting.
4. **Security Policy Verification:** Network Watcher provides Security Group View to visualize and verify the effective security rules applied by Network Security Groups (NSGs). Use this feature to ensure that NSG configurations align with security policies and regulatory compliance requirements.
5. **Packet Capture and Analysis:** Network Watcher's Packet Capture feature allows capturing network traffic to and from Azure VMs for offline analysis. Use packet capture to investigate network anomalies, diagnose application performance issues, or troubleshoot security incidents.
6. **DNS Troubleshooting:** DNS Analytics in Network Watcher helps monitor and troubleshoot DNS queries originating from Azure VMs. Use this feature to diagnose DNS resolution failures, identify misconfigured DNS servers, and optimize DNS infrastructure for improved reliability and performance.
7. **VPN Connectivity Diagnostics:** Network Watcher provides diagnostic tools for troubleshooting VPN connections and Virtual Network Gateway configurations. Use these tools to identify and resolve issues related to VPN tunnel establishment, routing, and security settings, ensuring seamless connectivity between on-premises and Azure networks.
8. **Topology Visualization:** Network Watcher offers a visual representation of the network topology within Azure subscriptions. Use this feature to understand the layout of Azure resources, identify network dependencies, and design network architectures that meet performance, scalability, and security requirements.

The end goal is to ensure reliable connectivity between the two VMs, gain insights into the network performance, identify any connectivity issues, and verify that the

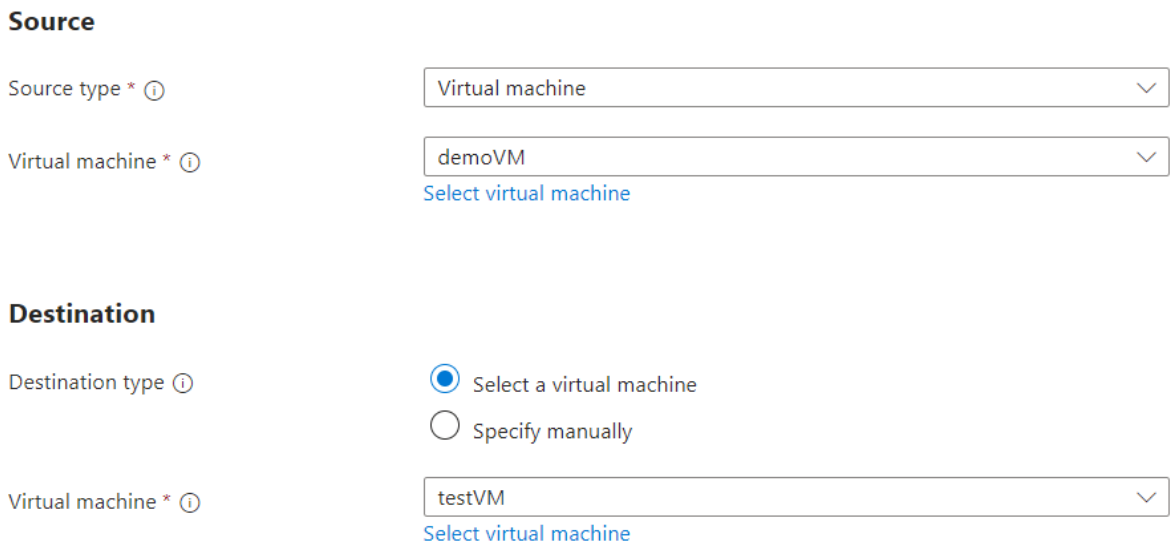
network configuration meets the desired performance and security standards. This helps in optimizing the network setup and ensuring seamless communication between the VMs.

😄 To begin with the Lab:

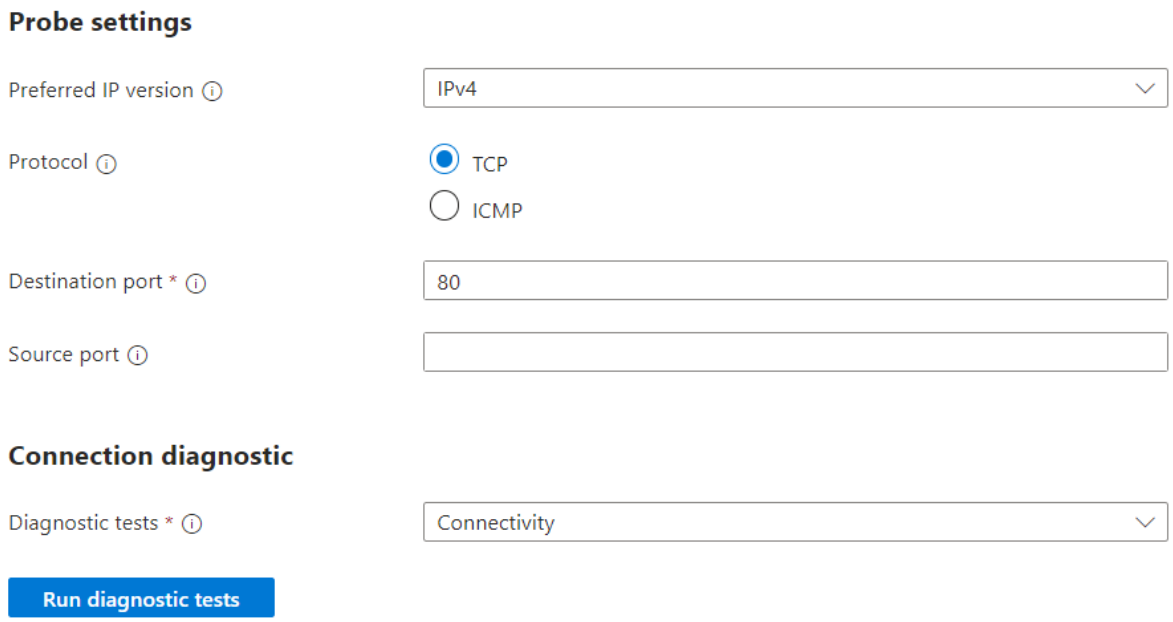
1. In this lab you should have a peering connection in place between two Virtual machines. For that you can refer to our previous lab on Peering connection you have to create the same connection as displayed in that document. But this time you don't need to delete the Public IP address of the test VM.
2. After that search for Network Watcher service and navigate to it. In network watcher the first service you are going to try is connection troubleshoot.



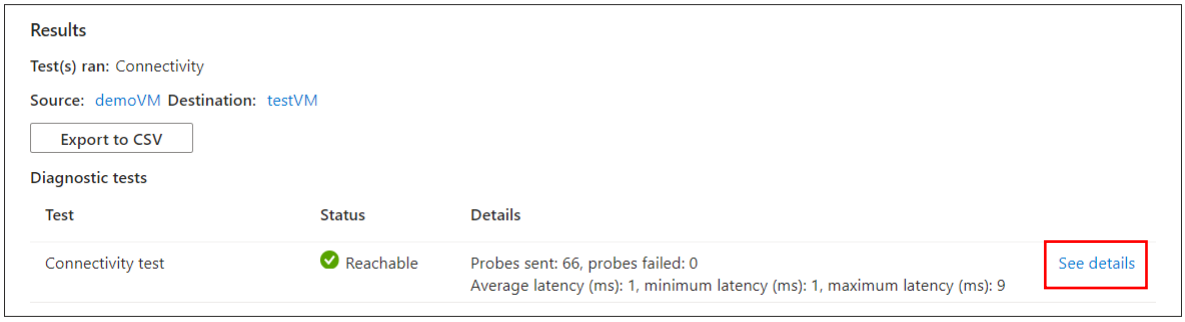
3. Now in the source you have to choose the demo VM and your destination is the test VM.



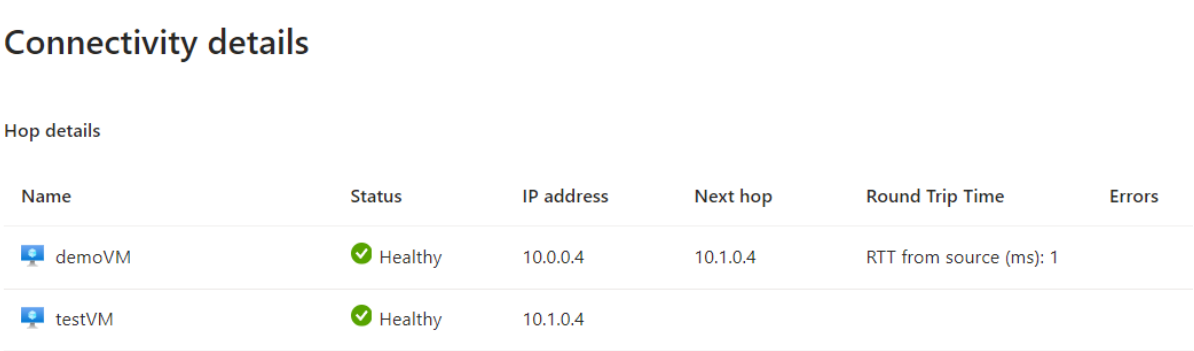
4. Now in the preferred IP version choose IPv4 and your destination port is 80. In terms of diagnostic tests, we will choose connectivity. We want the demo VM to have the ability to connect to the test VM on the destination port of port 80.
5. Then just click on run diagnostic tests.



6. When your test is complete you will see this results tab under the run diagnostic tests button.

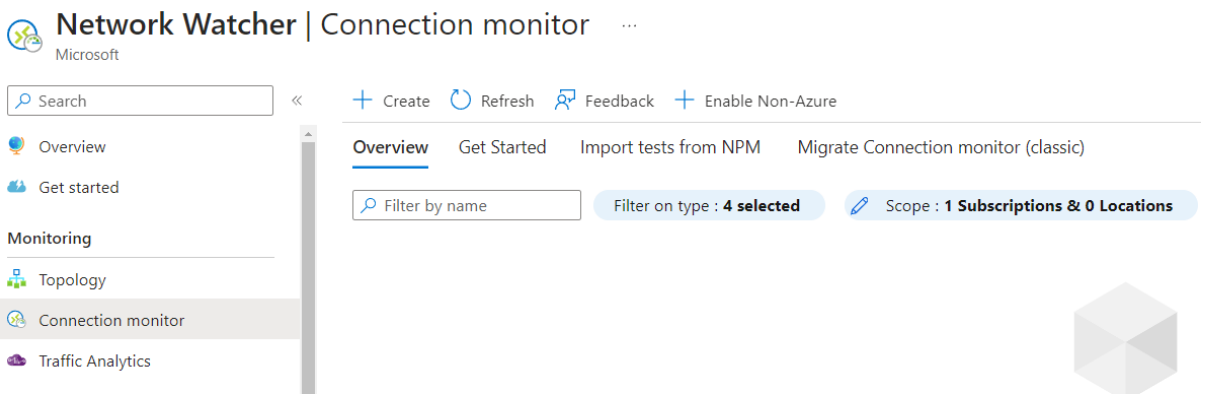


7. Now if you click on see details then you will see the connectivity details.

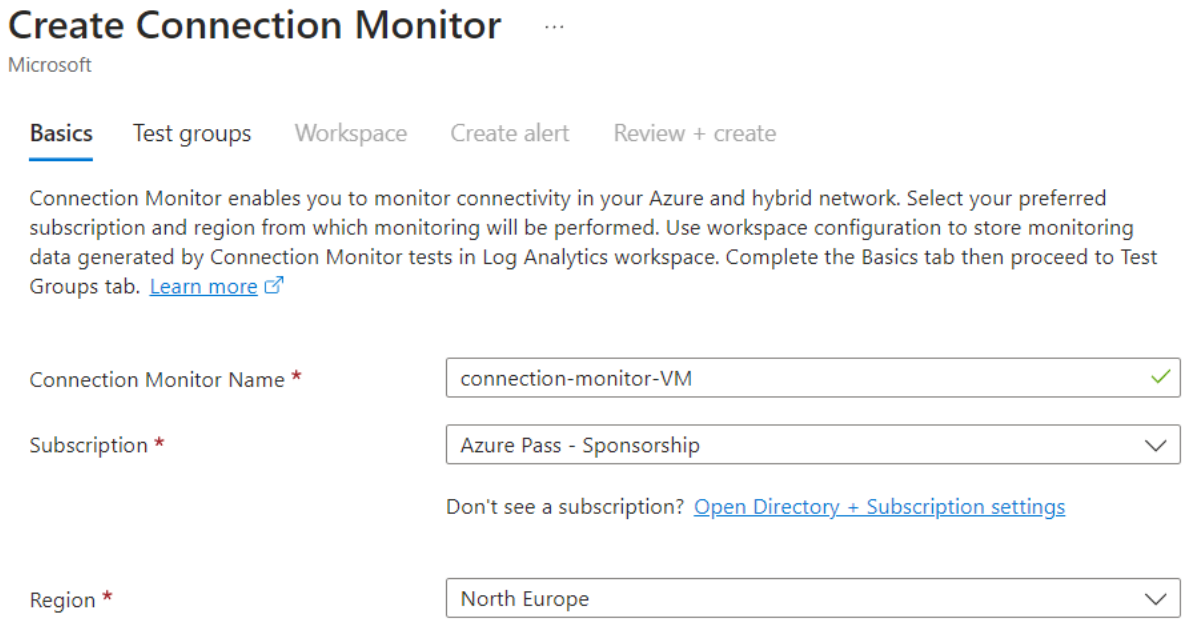


😊 Connection Monitor

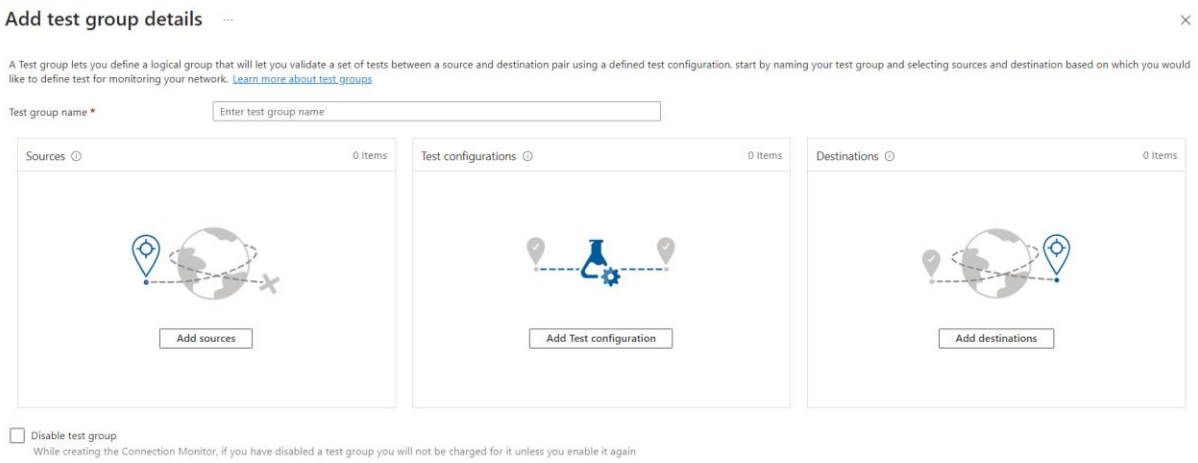
1. Now we are going to see another service in Network Watcher which is connection monitor.
2. For that go to connection monitor and click on Create.



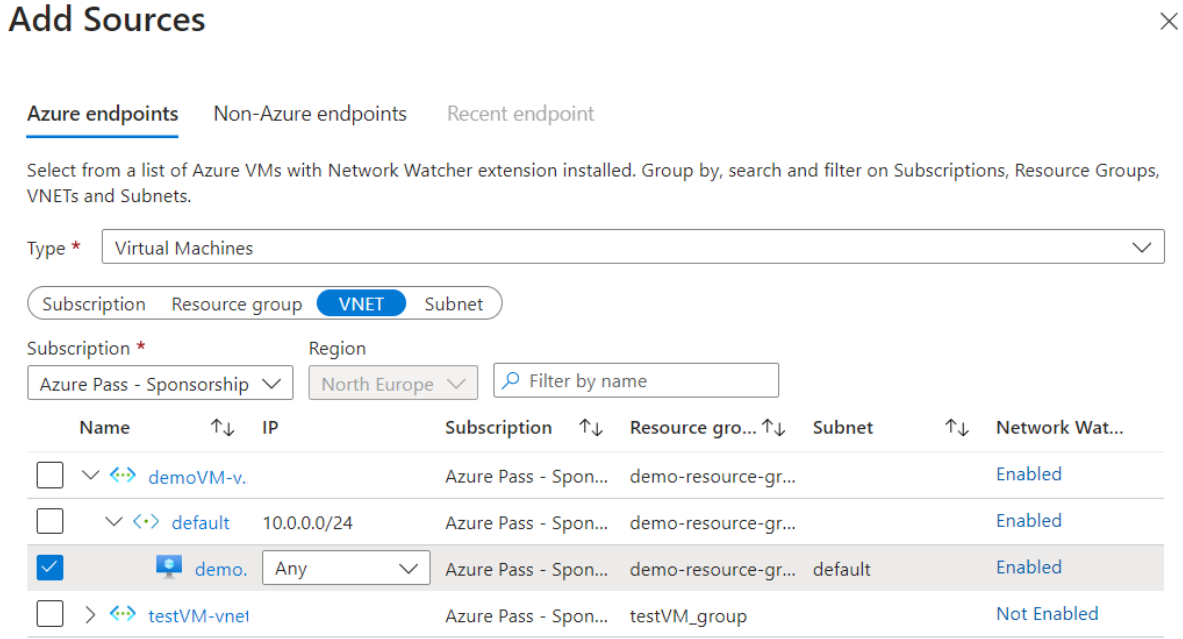
3. Now you need to give it a name and then choose your region.



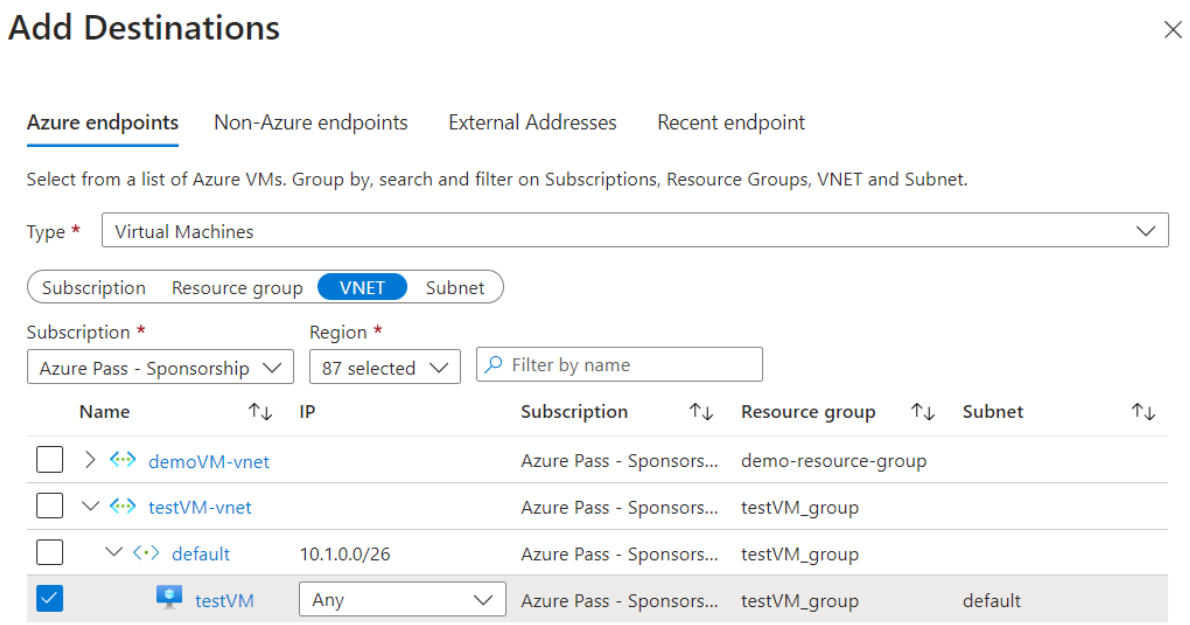
4. Then we need to create something known as test group details. First we will create source then the destination.



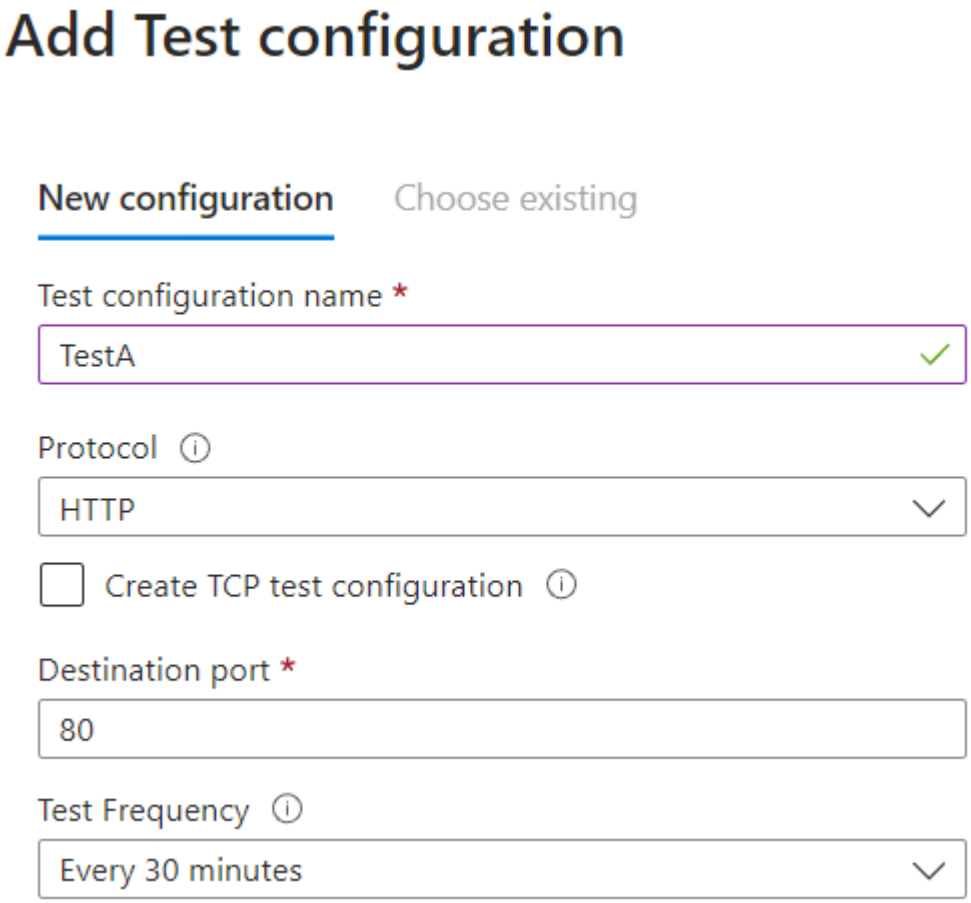
5. Now to add a source you need to choose your demo VM as shown below.



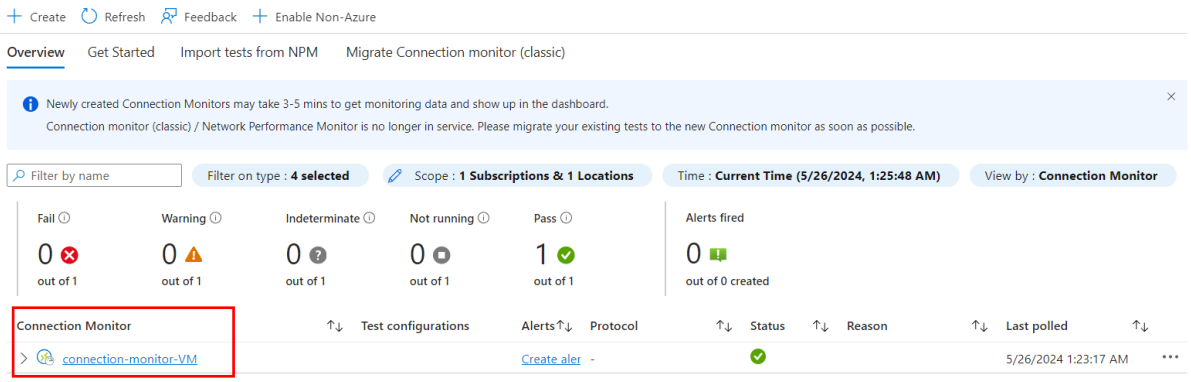
6. Then to add your destination you need to choose your test VM.



7. After that you need to add your test configuration.



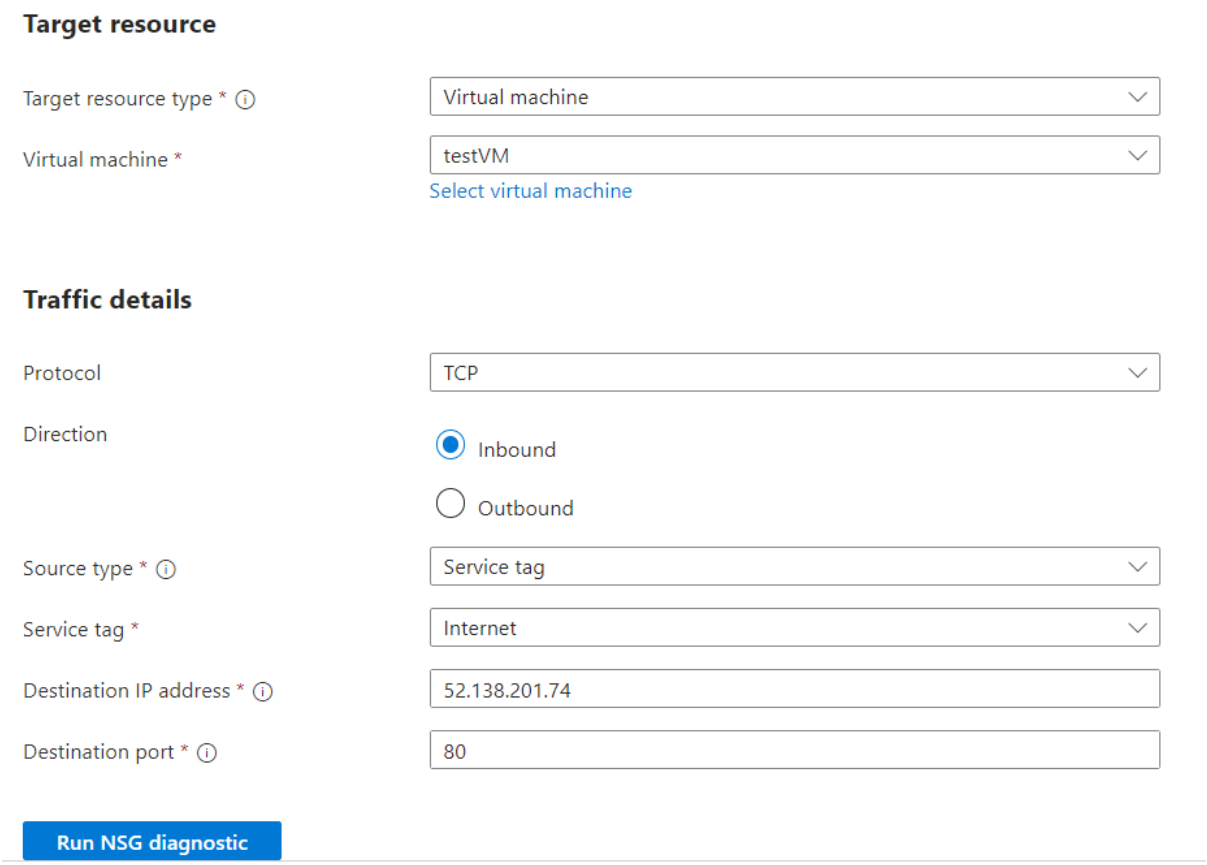
8. After just move to the review page and create your resource. After around 30-40 minutes we can see that our test has been passed.
9. Also, if you want to check for more information you can click on the highlighted place and get the information for yourself.



10. Once you are done delete it.

😊 NSG Diagnostics

1. This is another service in Network Watcher, navigate towards it and here you need to fill in the same information as shown below.
2. Then just click on Run Diagnostics.



3. Once your run is complete you can see the results as expected. Now click on view details and you will see more information about it.

Results

Traffic will be allowed if all NSGs allow it.

Traffic status: Allowed

NSG name	Applied to	Applied action	Additional info
testVM-nsg	testvm47	Allow	View details

Add security rule Recheck

A Network Security Group contains a list of security rules that are evaluated in priority order and allow or deny network packet. The first security rule that matches the network traffic in all 5 criteria (protocol, source, source port, destination, and destination port) will have the allow or deny action applied. After a security rule is matched with the network traffic, no further security rules are evaluated. Learn more

Inputs

Resource	: testVM
Protocol	: TCP
Source	: Internet
Destination IP address	: 52.138.201.74
Destination port	: 80
Direction	: Inbound

Results

Applied action	: Allowed
Applied rule	: HTTP
Network security group	: testVM-nsg
Applied to	: testvm47

Priority	Rule name	Status	Protocol	Source	Source port	Destination	Destination port
300	RDP	Not applied					Not matched
320	HTTP	Allowed	Matched	Matched	Matched	Matched	Matched
65000	AllowVnetInBound	Not evaluated	Any	VirtualNetwork	Any	VirtualNetwork	Any
65001	AllowAzureLoadBalancerInB...	Not evaluated	Any	AzureLoadBalancer	Any	Any	Any
65500	DenyAllInBound	Not evaluated	Any	Any	Any	Any	Any