200 XP

Troubleshoot a network by using Network Watcher monitoring and diagnostic tools

10 minutes

Azure Network Watcher includes several tools that you can use to monitor your virtual networks and virtual machines (VMs). To effectively make use of Network Watcher, it's essential to understand all the available options and the purpose of each tool.

In your engineering company, you want to enable your staff to choose the right Network Watcher tool for each troubleshooting task. They need to understand all the options available and the kinds of problems that each tool can solve.

Here, you'll look at the Network Watcher tool categories, the tools in each category, and how each tool is applied in example use cases.

What is Network Watcher?

Network Watcher is an Azure service that combines tools in a central place to diagnose the health of Azure networks. The Network Watcher tools are divided into two categories:

- Monitoring tools
- Diagnostic tools

With tools to monitor for and diagnose problems, Network Watcher gives you a centralized hub for identifying network glitches, CPU spikes, connectivity problems, memory leaks, and other issues before they affect your business.

Network Watcher monitoring tools

Network Watchers provides three monitoring tools:

- Topology
- Connection Monitor
- Network Performance Monitor

Let's look at each of these tools.

What is the topology tool?

The topology tool generates a graphical display of your Azure virtual network, its resources, its interconnections, and their relationships with each other.

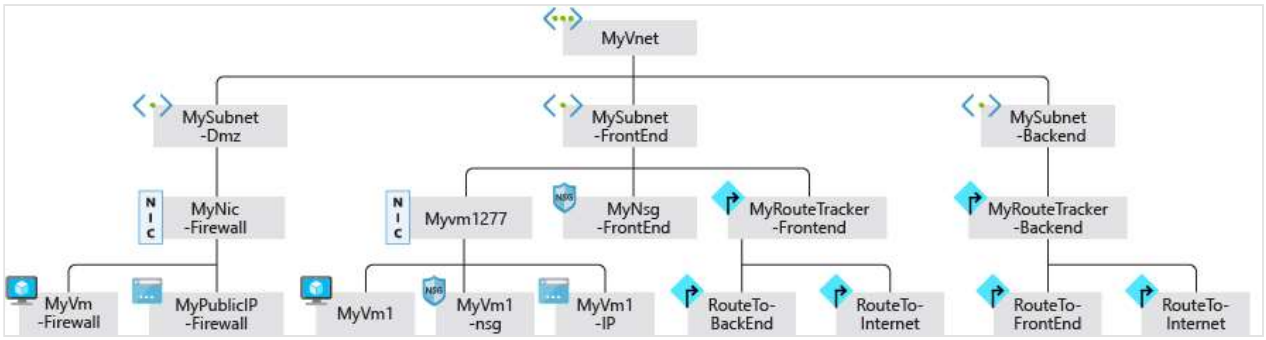
Suppose you have to troubleshoot a virtual network created by your colleagues. Unless you were involved in the creation process of the network, you might not know about all the aspects of the infrastructure. You can use the topology tool to visualize and understand the infrastructure you're dealing with before you start troubleshooting.

You use the Azure portal to view the topology of an Azure network. In the Azure portal:

1. Sign in to the Azure portal , and select **All services**. Then, search for **Network Watcher**.
2. Select **Topology**.
3. Select a subscription, the resource group of a virtual network, and then the virtual network itself.

> **Note**
>
> To generate the topology, you need a Network Watcher instance in the same region as the virtual network.

Here's an example of a topology generated for a virtual network named MyVNet.



What is the Connection Monitor tool?

The Connection Monitor tool provides a way to check that connections work between Azure resources. To check that two VMs can communicate if you want them to, use this tool.

This tool also measures the latency between resources. It can catch changes that will affect connectivity, such as changes to the network configuration or changes to network security group (NSG) rules. It can probe VMs at regular intervals to look for failures or changes.

If there's an issue, Connection Monitor tells you why it occurred and how to fix it. Along with monitoring VMs, Connection Monitor can examine an IP address or fully qualified domain name (FQDN).

What is the Network Performance Monitor tool?

The Network Performance Monitor tool enables you to track and alert on latency and packet drops over time. It gives you a centralized view of your network.

When you decide to monitor your hybrid connections by using Network Performance Monitor, check that the associated workspace is in a supported region.

You can use Network Performance Monitor to monitor endpoint-to-endpoint connectivity:

- Between branches and datacenters.
- Between virtual networks.
- For your connections between on-premises and the cloud.
- For Azure ExpressRoute circuits.

Network Watcher diagnostic tools

Network Watcher includes six diagnostic tools:

- IP flow verify
- Next hop
- Effective security rules
- Packet capture
- Connection troubleshoot
- VPN troubleshoot

Let's examine each tool and find out how they can help you solve problems.

What is the IP flow verify tool?

The IP flow verify tool tells you if packets are allowed or denied for a specific virtual machine. If a network security group denies a packet, the tool tells you the name of that group so that you can fix the problem.

This tool uses a 5-tuple packet parameter-based verification mechanism to detect whether packets inbound or outbound are allowed or denied from a VM. Within the tool, you specify a local and remote port, the protocol (TCP or UDP), the local IP, the remote IP, the VM, and the VM's network adapter.

What is the next hop tool?

When a VM sends a packet to a destination, it might take multiple hops in its journey. For example, if the destination is a VM in a different virtual network, the next hop might be the

virtual network gateway that routes the packet to the destination VM.

With the next hop tool, you can determine how a packet gets from a VM to any destination. You specify the source VM, source network adapter, source IP address, and destination IP address. The tool then determines the packet's destination. You can use this tool to diagnose problems caused by incorrect routing tables.

What is the effective security rules tool?

The effective security rules tool in Network Watcher displays all the effective NSG rules applied to a network interface.

Network security groups (NSGs) are used in Azure networks to filter packets based on their source and destination IP address and port numbers. NSGs are vital to security because they help you carefully control the surface area of the VMs that users can access. Keep in mind, though, that a mistakenly configured NSG rule might prevent legitimate communication. As a result, NSGs are a frequent source of network problems.

For example, if two VMs can't communicate because an NSG rule blocks them, it can be difficult to diagnose which rule is causing the problem. You'll use the effective security rules tool in Network Watcher to display all the effective NSG rules and help you diagnose which rule is causing the specific problem.

To use the tool, you choose a VM and its network adapter. The tool displays all the NSG rules that apply to that adapter. It's easy to determine a blocking rule by viewing this list.

You can also use the tool to spot vulnerabilities for your VM caused by unnecessary open ports.

What is the packet capture tool?

You use the packet capture tool to record all of the packets sent to and from a VM. You'll then review the capture to gather statistics about network traffic or diagnose anomalies, such as unexpected network traffic on a private virtual network.

The packet capture tool is a virtual machine extension that is remotely started through Network Watcher and happens automatically when you start a packet capture session.

Keep in mind that there is a limit to the amount of packet capture sessions allowed per region. The default usage limit is 100 packet capture sessions per region, and the overall limit is 10,000. These limits are for the number of sessions only, not saved captures. You can save packets captured in Azure Storage or locally on your computer.

Packet capture has a dependency on the *Network Watcher Agent VM Extension* installed on the VM. For links to instructions that detail the installation of the extension on both Windows and Linux VMs, see the "Learn more" section at the end of this module.

What is the connection troubleshoot tool?

You use the connection troubleshoot tool to check TCP connectivity between a source and destination VM. You can specify the destination VM by using an FQDN, a URI, or an IP address.

If the connection is successful, information about the communication appears, including:

- The latency in milliseconds.
- The number of probe packets sent.
- The number of hops in the complete route to the destination.

If the connection is unsuccessful, you'll see details of the fault. Fault types include:

- **CPU**. The connection failed because of high CPU utilization.
- **Memory**. The connection failed because of high memory utilization.
- **GuestFirewall**. The connection was blocked by a firewall outside Azure.
- **DNSResolution**. The destination IP address couldn't be resolved.
- **NetworkSecurityRule**. The connection was blocked by an NSG.
- **UserDefinedRoute**. There's an incorrect user route in a routing table.

What is the VPN troubleshoot tool?

You can use the VPN troubleshoot tool to diagnose problems with virtual network gateway connections. This tool runs diagnostics on a virtual network gateway connection and returns a health diagnosis.

When you start the VPN troubleshoot tool, Network Watcher diagnoses the health of the gateway or connection, and returns the appropriate results. The request is a long-running transaction.

The following table shows examples of different fault types.

Fault Type	Reason	Log
NoFault	No error is detected.	Yes
GatewayNotFound	A gateway can't be found or isn't provisioned.	No
PlannedMaintenance	A gateway instance is under maintenance.	No

Fault Type	Reason	Log
UserDrivenUpdate	A user update is in progress. The update might be a resize operation.	No
VipUnResponsive	The primary instance of the gateway can't be reached because of a health probe failure.	No
PlatformInActive	There's an issue with the platform.	No

Azure Network Watcher use case scenarios

Let's examine some scenarios that you can investigate and troubleshoot by using Azure Network Watcher monitoring and diagnostics.

There are connectivity issues in a single-VM network

Your colleagues have deployed a VM in Azure and are having network connectivity issues. Your colleagues are trying to use Remote Desktop Protocol (RDP) to connect to the virtual machine, but they can't connect.

To troubleshoot this issue, use the IP flow verify tool. This tool lets you specify a local and remote port, the protocol (TCP/UDP), the local IP, and the remote IP to check the connection status. It also lets you specify the direction of the connection (inbound or outbound). IP flow verify runs a logical test on the rules in place on your network.

In this case, use IP flow verify to specify the VM's IP address and the RDP port 3389. Then, specify the remote VM's IP address and port. Choose the TCP protocol, and then select **Check**.

Suppose the result shows that access was denied because of the NSG rule **DefaultInboundDenyAll**. The solution is to change the NSG rule.

A VPN connection isn't working

Your colleagues have deployed VMs in two virtual networks and can't connect between them.

To troubleshoot a VPN connection, use Azure VPN troubleshoot. This tool runs diagnostics on a virtual network gateway connection, and returns a health diagnosis. You can run this tool from the Azure portal, PowerShell, or the Azure CLI.

When you run the tool, it checks the gateway for common issues and returns the health diagnosis. You can also view the log file to get more information. The diagnosis will show whether the VPN connection is working. If the VPN connection isn't working, VPN troubleshoot will suggest ways to resolve the issue.

Suppose the diagnosis shows a key mismatch. To resolve the problem, reconfigure the remote gateway to make sure the keys match on both ends. Pre-shared keys are case-sensitive.

No servers are listening on designated destination ports

Your colleagues have deployed VMs in a single virtual network and can't connect between them.

Use the connection troubleshoot tool to troubleshoot this issue. In this tool, you specify the local and remote VMs. In the probe setting, you can choose a specific port.

Suppose the results show the remote server is **Unreachable**, along with the message "Traffic blocked due to virtual machine firewall configuration." On the remote server, disable the firewall, and then test the connection again.

Suppose the server is now reachable. This result indicates that firewall rules on the remote server are the issue, and must be corrected to permit the connection.

1. To capture traffic on a VM, Azure Network Watcher requires:

- ○ Network Watcher Agent VM Extension
- ○ Azure Traffic Manager
- ○ An Azure storage account

2. To resolve latency issues on the network, which Azure Network Watcher features can you use?

- ○ IP flow verify
- ○ Next hop
- ○ Connection troubleshoot

Check your answers