

Introduction to Azure Network Watcher

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-network-watcher/1-introduction>

Introduction

Completed

Organizations can use Azure Network Watcher to detect and monitor issues related to the network performance of infrastructure as a service (IaaS) resources in Microsoft Azure.

Adatum is a new and expanding online commerce store. You work in DevOps at Adatum, and you're responsible for networking. Adatum has several three-tier applications running on virtual machines that were migrated from on-premises datacenters to Azure. The applications are hosted across multiple Azure virtual networks. Adatum also has several hybrid applications that have compute tiers in both on-premises and cloud locations.

This module explains what Azure Network Watcher does, how it works, and when you should choose to use Azure Network Watcher as a solution to meet your organization's needs.

Learning objectives

In this module, you'll:

- Learn what Azure Network Watcher is and the functionality it provides.
- Determine whether Azure Network Watcher meets the needs of your organization.

Prerequisites

- Understanding of basic networking concepts such as IP addressing, subnetting, routing, and network security groups.
- Basic familiarity with Azure network integration concepts such as VPNs, Azure ExpressRoute, and peering.

2. What is Azure Network Watcher?

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-network-watcher/2-what-is-azure-network-watcher>

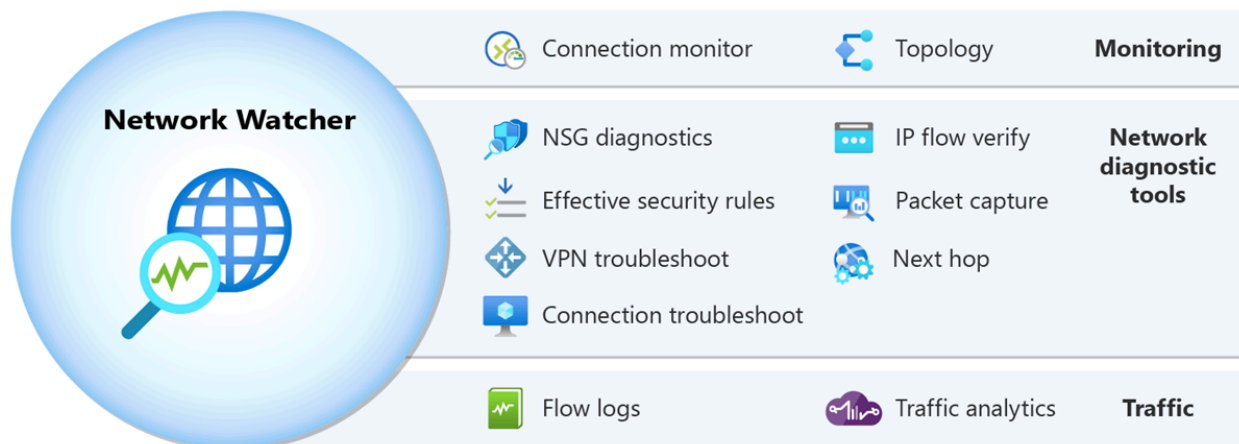
What is Azure Network Watcher?

Completed

Azure Network Watcher provides a suite of tools to monitor, diagnose, view metrics, and enable or disable logs for Azure IaaS (Infrastructure-as-a-Service) resources. Network Watcher enables you to monitor and repair the network health of IaaS products like virtual machines (VMs), virtual networks (VNETs), application gateways, load balancers, etc. Network Watcher isn't designed or intended for PaaS monitoring or Web analytics.

Network Watcher consists of three major sets of tools and capabilities:

- Monitoring
 - Topology
 - Connection monitor
- Network diagnostic
 - IP flow verify
 - NSG diagnostics
 - Next hop
 - Effective security rules
 - Connection troubleshoot
 - Packet capture
 - VPN troubleshoot
- Traffic
 - Flow logs
 - Traffic analytics



Monitoring

Network Watcher offers two monitoring tools that help you view and monitor resources:

- Topology
- Connection monitor

Topology

The **Topology** tool provides a visualization of the entire network for understanding network configuration. It provides an interactive interface to view resources and their relationships in Azure spanning across multiple subscriptions, resource groups, and locations. At the beginning of the troubleshooting process, this tool helps you visualize all of the elements involved in the problem, allowing you to find something that isn't apparent by looking at the contents of resource groups.

Connection monitor

Connection monitor provides end-to-end connection monitoring for Azure and hybrid endpoints. It helps you understand network performance between various endpoints in your network infrastructure. You can use connection monitor to verify that two IaaS VMs that host the components of a multi-tier application can communicate with each other. You can also use it to verify connectivity in hybrid scenarios.

Network diagnostic tools

Network Watcher offers seven network diagnostic tools that help troubleshoot and diagnose network issues:

- IP flow verify
- NSG diagnostics
- Next hop
- Effective security rules
- Connection troubleshoot

- Packet capture
- VPN troubleshoot

IP flow verify

IP flow verify allows you to detect traffic filtering issues at a virtual machine level. It checks if a packet is allowed or denied to or from an IP address (IPv4 or IPv6 address). It also tells you which security rule allowed or denied the traffic.

NSG diagnostics

NSG diagnostics allows you to detect traffic filtering issues at a virtual machine, virtual machine scale set, or application gateway level. It checks if a packet is allowed or denied to or from an IP address, IP prefix, or a service tag. It tells you which security rule allowed or denied the traffic. It also allows you to add a new security rule with a higher priority to allow or deny the traffic.

Next hop

Next hop allows you to detect routing issues. It checks if traffic is routed correctly to the intended destination. It provides you with information about the Next hop type, IP address, and Route table ID for a specific destination IP address.

Effective security rules

Effective security rules allows you to view the effective security rules applied to a network interface. It shows you all security rules applied to the network interface, the subnet the network interface is in, and the aggregate of both.

Connection troubleshoot

Connection troubleshoot enables you to test a connection between a virtual machine, a virtual machine scale set, an application gateway, or a Bastion host and a virtual machine, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor tool, but tests the connection at a point in time instead of monitoring it over time, as connection monitor does.

Packet capture

Packet capture allows you to remotely create packet capture sessions to record all network traffic to and from a virtual machine (VM) or a virtual machine scale set.

VPN troubleshoot

VPN troubleshoot enables you to troubleshoot virtual network gateways and their connections.

Traffic

Network Watcher offers two traffic tools that help you log and visualize network traffic:

- Flow logs
- Traffic analytics

Flow logs

Flow logs allows you to log information about your Azure IP traffic and stores the data in Azure storage. You can log IP traffic flowing through a network security group or Azure virtual network.

Traffic analytics

Traffic analytics provides rich visualizations of flow logs data.

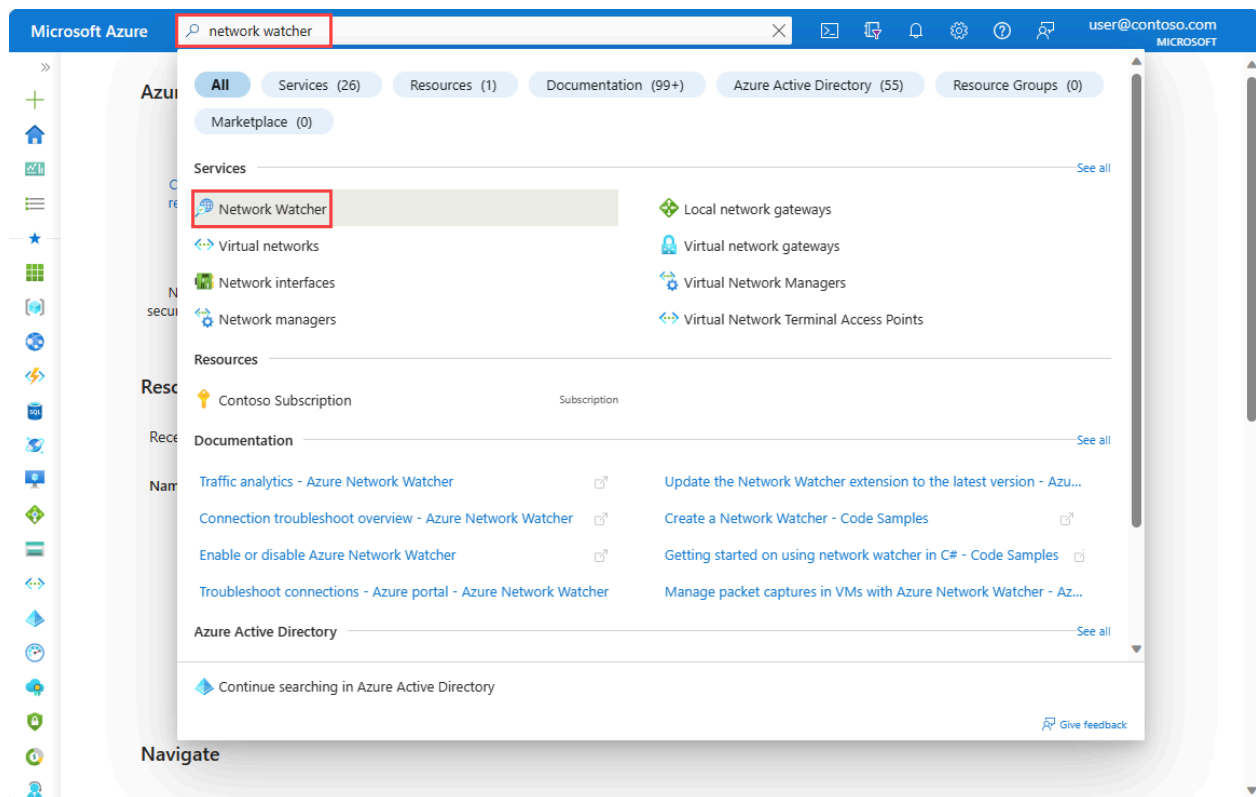
3. How Azure Network Watcher works

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-network-watcher/3-how-azure-network-watcher-works>

How Azure Network Watcher works

Completed

Network Watcher becomes automatically available when you create a virtual network in an Azure region in your subscription. You can access Network Watcher directly in the Azure portal by typing **Network Watcher** in the **Search** bar.



Network Watcher Topology tool

The topology capability of Azure Network Watcher allows you to view all of the following resources in a virtual network. Including, the resources associated to resources in a virtual network and the relationships between the resources.

- Subnets
- Network interfaces
- Network security groups
- Load balancer
- Load balancer health probes
- Public IP addresses
- Virtual network peering
- Virtual network gateways
- VPN gateway connections
- Virtual machines
- Virtual Machine Scale Sets

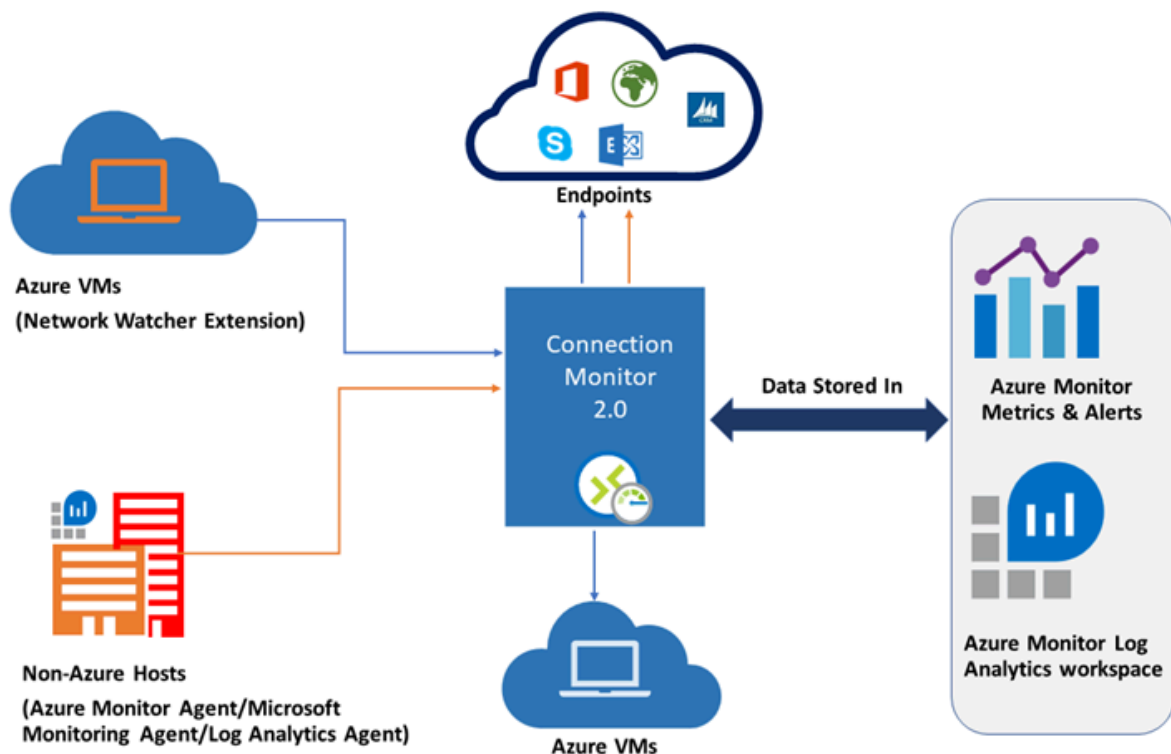
All resources returned in a topology have the following properties:

- **Name:** The name of the resource.
- **Id:** The URI of the resource.
- **Location:** The Azure region the resource is in.
- **Associations:** A list of associations to the referenced object. Each association has the following properties:

- **AssociationType:** References the relationship between the child object and the parent. Valid values are `Contains` and `Associated`.
- **Name:** The name of the referenced resource.
- **ResourceId:** The URI of the resource referenced in the association.

Connection Monitor tool

Connection Monitor provides unified, end-to-end connection monitoring in Azure Network Watcher. Connection Monitor supports both hybrid and Azure cloud deployments. You can use the Connection Monitor tool to measure the latency between resources. Connection Monitor can detect changes that affect connectivity, such as network configuration changes or modifications to NSG rules. You can configure Connection Monitor to probe VMs at regular intervals to look for failures or changes. Connection Monitor can diagnose problems and provide explanations about why the issue occurred and the steps that you can take to fix an issue.



To use Connection Monitor for monitoring, you need to install monitoring agents on the hosts that you monitor. Connection Monitor uses lightweight executable files to run connectivity checks, whether a host is located in an Azure virtual network or in an on-premises network. With Azure VMs, you can install the Network Watcher Agent VM, also known as the Network Watcher extension.

IP flow verify

The IP flow verify tool uses a 5-tuple packet parameter-based verification mechanism to detect whether packets that are inbound or outbound are allowed or denied from a VM. Within the tool,

you can 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.

Next hop

Traffic from an IaaS VM is sent to a destination based on the effective routes associated with a network interface (NIC). Next hop gets the next hop type and IP address of a packet from a specific VM and NIC. Knowing the next hop helps you determine whether traffic is being directed to the intended destination or whether the traffic is being sent nowhere. An improper configuration of routes, in which traffic is directed to an on-premises location or to a virtual appliance, might lead to connectivity issues. Next hop also returns the route table associated with the next hop. If the route is defined as a user-defined route, that route is returned. Otherwise, next hop returns **System Route**.

Effective security rules

Network security groups (NSGs) filter packets based on their source and destination IP address and port numbers. More than one NSG can apply to an IaaS resource on an Azure virtual network. By taking into account all rules that are applied across all NSGs for a resource, the Effective Security Rules tool allows you to determine why some traffic might be denied or allowed.

Packet capture

Packet capture is a virtual machine extension that is remotely started through Network Watcher. This capability eases the burden of running a packet capture manually on a specific virtual machine by using operating system tools or third-party utilities. Packet capture can be triggered through the portal, PowerShell, the Azure CLI, or REST API. Network Watcher allows you to configure filters for the capture session to ensure you capture traffic you want to monitor. Filters are based on 5-tuple (protocol, local IP address, remote IP address, local port, and remote port) information. The captured data is stored on the local disk or in a storage blob.

Connection troubleshoot

The connection troubleshoot tool checks TCP connectivity between a source and a 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, the tool displays details about the fault. You might see the following fault types:

- **CPU**: The connection failed because of high CPU utilization.

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

VPN troubleshoot

Network Watcher provides the capability to troubleshoot gateways and connections. The capability can be called through the portal, PowerShell, the Azure CLI, or REST API. When called, Network Watcher diagnoses the health of the gateway or connection, and then it returns the appropriate results. The request is a long-running transaction. The preliminary results that are returned give an overall picture of the health of the resource.

The following list describes the values that are returned by calling the VPN troubleshoot API:

- **startTime:** The time the troubleshooting started.
- **endTime:** The time the troubleshooting ended.
- **code:** This value is `UnHealthy` if there's a single diagnosis failure.
- **results:** A collection of results returned on the connection or the virtual network gateway.
 - **id:** The fault type.
 - **summary:** A summary of the fault.
 - **detailed:** A detailed description of the fault.
 - **recommendedActions:** A collection of recommended actions to take.
 - **actionText:** Text that describes what action to take.
 - **actionUri:** The URI for documentation that describes what action to take.
 - **actionUriText:** A short description of the action text.

4. When to use Azure Network Watcher

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-network-watcher/4-when-to-use-azure-network-watcher>

When to use Azure Network Watcher

Completed

Azure Network Watcher is useful when you're attempting to troubleshoot networking issues related to Azure IaaS products. For example, you can use the tools included in Azure Network Watcher in the following scenarios:

- Resolve connectivity issues related to IaaS VMs.
- Troubleshoot VPN connections.
- Determine cross region network latencies.

Resolve connectivity issues related to IaaS VMs

Recently, a Windows Server IaaS VM was deployed to Azure. The developers who deployed the VM are unable to establish a remote PowerShell session to this IaaS VM from another IaaS VM on the same virtual network.

You can troubleshoot this issue using 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, you can use IP flow verify to specify the VM's IP address and the TCP port 5986 (used by PowerShell when using HTTPS). Then, specify the remote VM's IP address and port. Choose the TCP protocol, then select **Check**. If an NSG rule is blocking traffic, the IP flow verify rule reports which rule is responsible for the dropped traffic.

Troubleshoot VPN connections

An IaaS VM is deployed on an Azure virtual network. Connections to this IaaS VM from on-premises hosts are made through a site-to-site VPN connection.

You can troubleshoot this VPN connection using the Azure VPN troubleshoot tool. 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 shows whether the VPN connection is working. If the VPN connection isn't working, the Azure VPN troubleshoot tool suggests ways to resolve the issue.

Determine cross-region network latency

You can use Network Watcher tools to determine the best location to place IaaS resources based on network latencies. For example, you can use Network Watcher to have IaaS VMs in different regions regularly ping each other to determine cross region network latency. This information can allow you to determine whether all your IaaS VMs need to be located in a single region. Or, if they can be spread across different regions to support specific application architectures.

Let's say you have an on-premises hybrid application and an application running in an Azure IaaS VM that connects to the same storage account endpoint. You could use Network Watcher to perform a comparison of latencies for the two applications. If the latency for the on-premises application is too

high, it might strengthen a case for migrating that application to Azure. If the latency for the Azure IaaS VM is too high, it might strengthen a case for migrating the VM to another region with lower latency.

When not to use Network Watcher

Network Watcher tools provide intermediate levels of network diagnostic functionality. These tools don't provide some of the advanced features available in some third-party tools. If your organization needs access to this advanced functionality, you might need to deploy a third-party tool that includes this advanced functionality to accomplish your diagnostic goals.

It's important to realize that Network Watcher is mostly used for IaaS resources on Azure virtual networks. You can't use Azure Network Watcher to diagnose connectivity issues related to PaaS services or Web analytics. If you're encountering problems related to these services, you should check the Azure status or service health dashboard.

5. Module assessment

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-network-watcher/5-knowledge-check>

Module assessment

Completed

6. Summary

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-network-watcher/6-summary>

Summary

Completed

In this module, you learned about Azure Network Watcher, a service you can use to perform monitoring and diagnostic tasks on IaaS resources deployed on Azure virtual networks. You learned about the monitoring and diagnostic tools that are available in Network Watcher, and which tool is appropriate for specific troubleshooting scenarios.

Learn more

- [What is Azure Network Watcher?](#)
- [Enable or disable Azure Network Watcher](#)
- [Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools](#)
- [Configure Network Watcher](#)
- [Design and implement network monitoring](#)