Name: - Ayush Pandey

Batch: - Az-900 + Az-104

Assignment 07: - Network Watcher

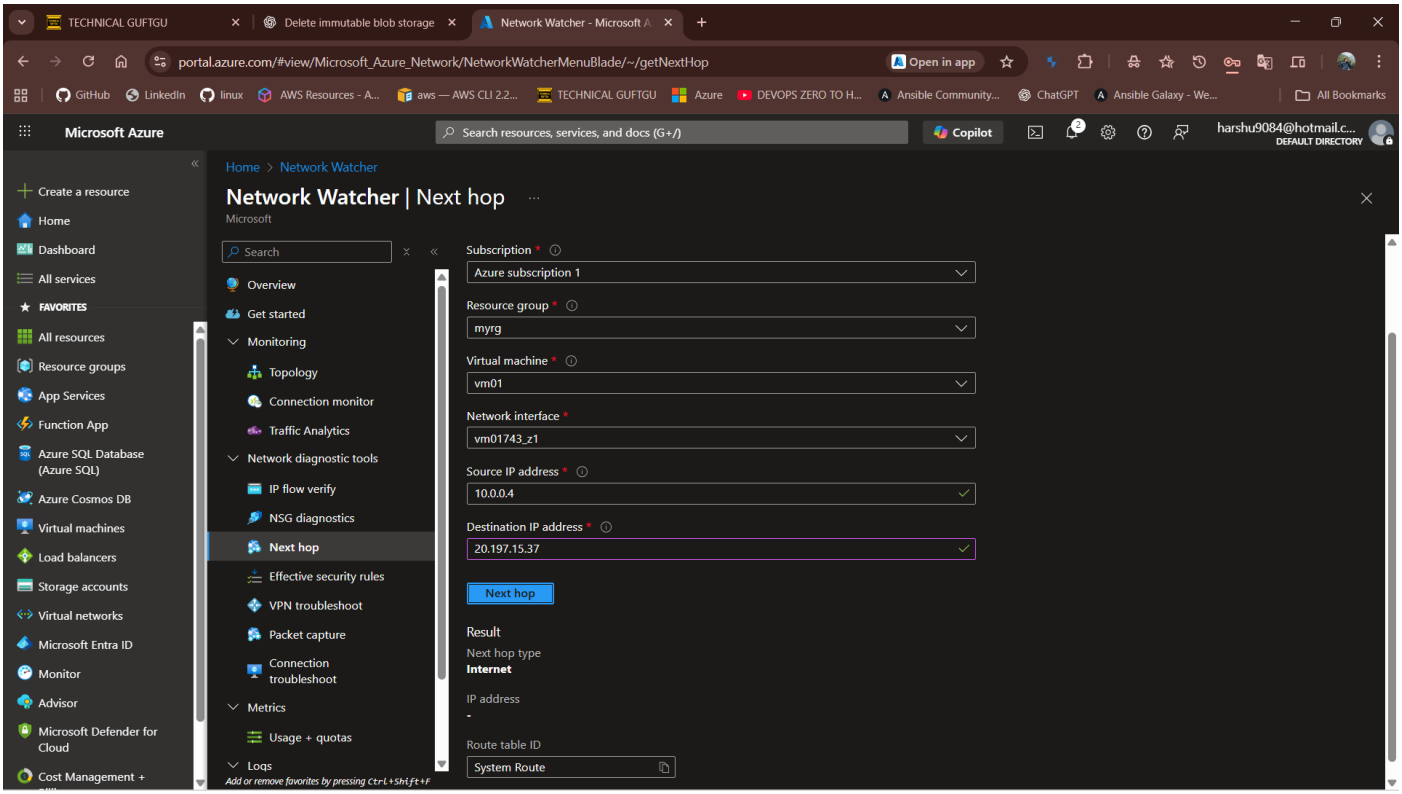
- **What is Next Hop?**

In Azure, a **Next Hop** means **the next stop (destination)** your network traffic takes **to reach its final target**.

When data travels from one virtual machine (VM) or subnet to another, Azure needs to decide **where to send that traffic next** — this is what **Next Hop** tells you.

👉 **Example:**
If VM1 wants to talk to VM2, Azure looks at the **route table** and says:

"The next hop is the virtual network" — meaning traffic goes directly inside the same VNet.



Or, if traffic is meant for the internet:

"The next hop is the Internet gateway."

So, **Next Hop = the next network device or path Azure uses to forward packets.**

Each route in Azure has **two main parts:**

1. **Address prefix** (destination network)
2. **Next hop type** (where to send the packet next)

- ## What is Effective Security Rule?

Effective Security Rules in Azure mean the **final list of network security rules** that actually apply to a **network interface (NIC)** or **virtual machine (VM)** — after combining all the rules from **Network Security Groups (NSGs)** attached to the subnet and the VM.

👉 Think of it like this:
Your VM can have **two sets of security rules** —

1. One from the **subnet's NSG**
2. One from the **VM's (NIC's) NSG**

Azure looks at **both** and combines them to figure out:

"What traffic is really allowed or denied for this VM?"

That **combined result** is called the **Effective Security Rules**.

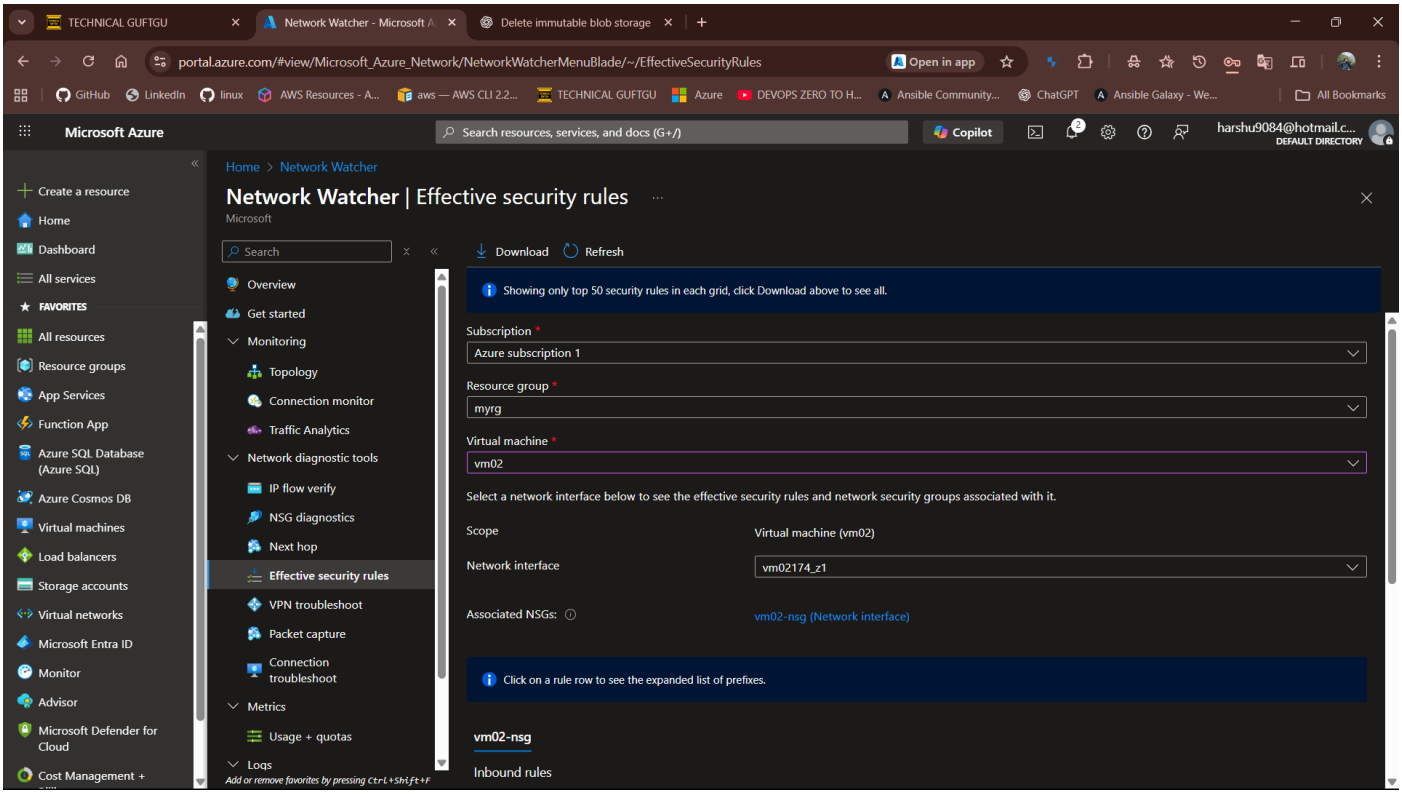
Example

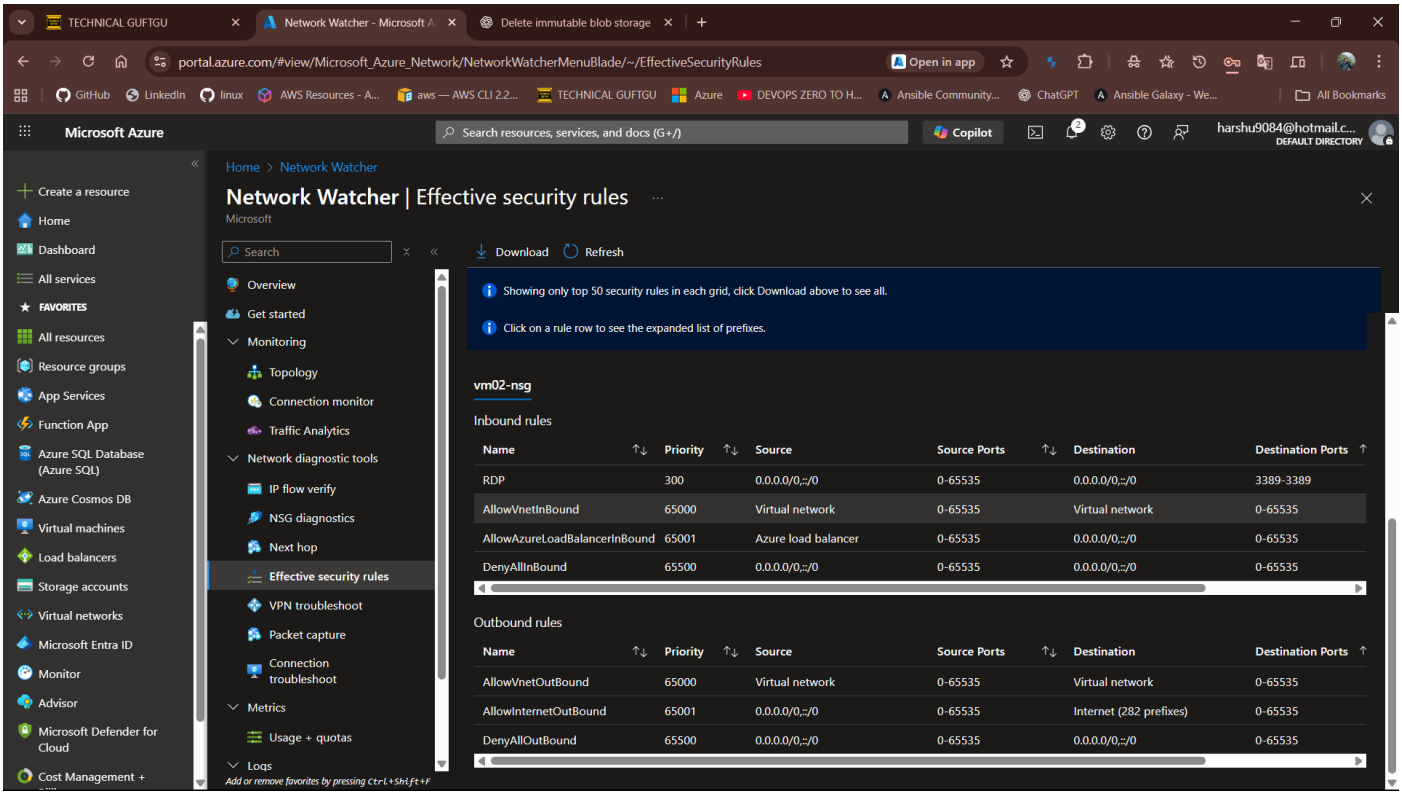
- Subnet NSG allows:
  ✅ Port 80 (HTTP)
- VM NSG allows:
  ✅ Port 22 (SSH)
  ❌ Denies everything else

When Azure calculates the **effective rules** for that VM, it means:

The VM will allow only Port 80 and Port 22.
Everything else is blocked.

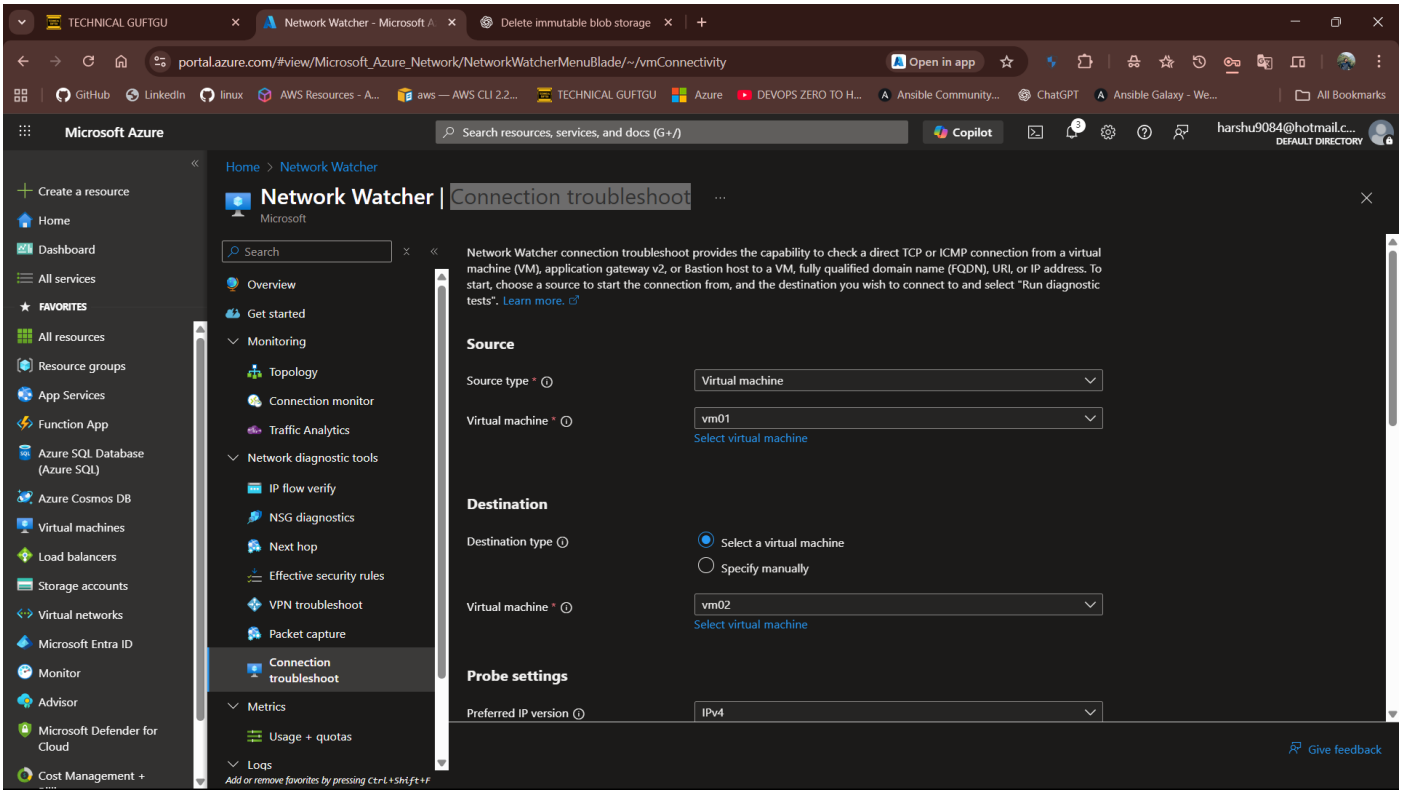
✅ **Effective Security Rules = Subnet rules + NIC rules (combined)**

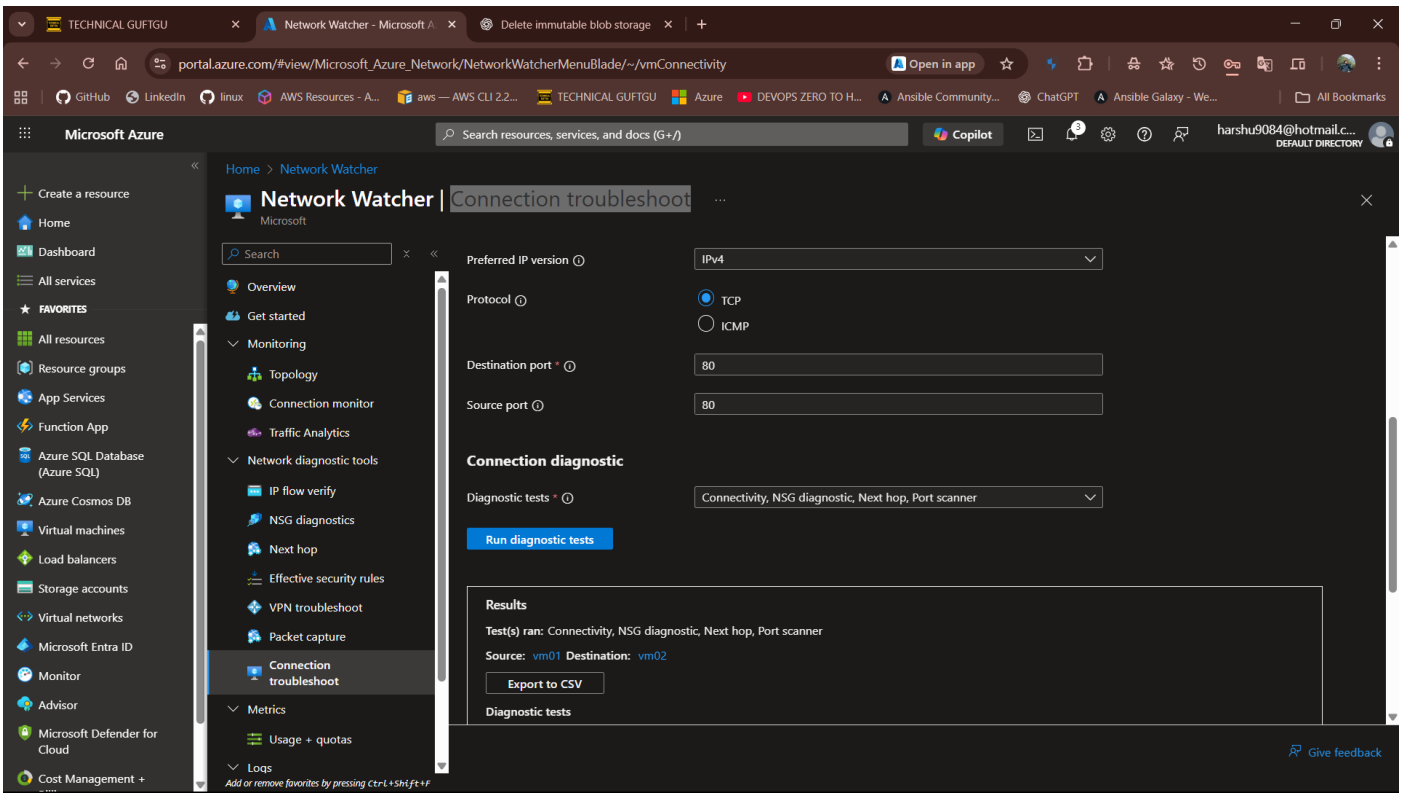


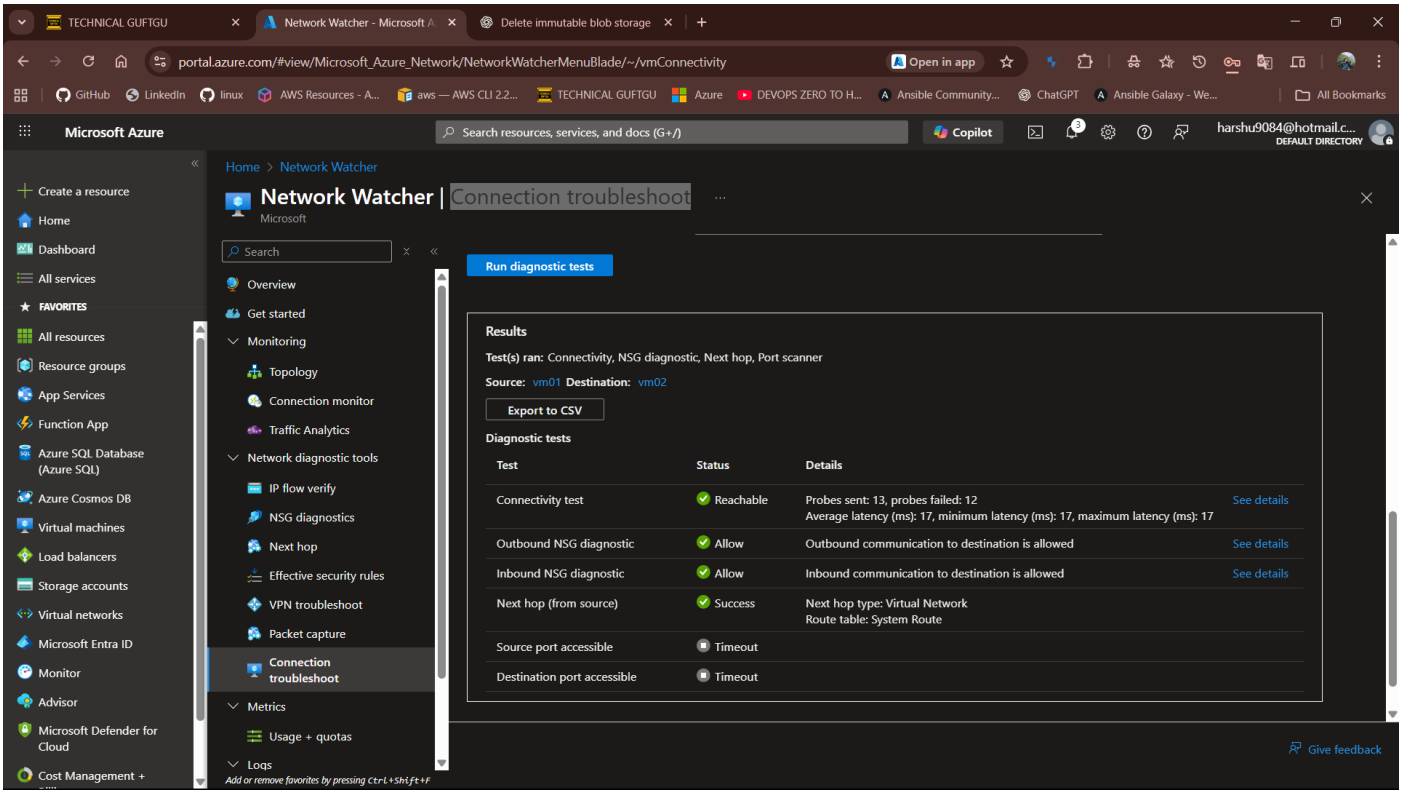


- **What is Connection troubleshooting?**

Connection Troubleshoot in Azure helps you check if two resources can connect to each other — for example, if your VM can reach another VM, database, or website — and tells you where the connection fails if it does not work.


TECHNICAL GUFTGU
Network Watcher - Microsoft A
Delete immutable blob storage
portal.azure.com/#view/Microsoft_Azure_Network/NetworkWatcherMenuBlade/~/vmConnectivity
Open in app
GitHub
LinkedIn
linux
AWS Resources - A...
aws — AWS CLI 2.2...
TECHNICAL GUFTGU
Azure
DEVOPS ZERO TO H...
Ansible Community...
ChatGPT
Ansible Galaxy - We...
All Bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
harshu9084@hotmail.c...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
Azure SQL Database (Azure SQL)
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Microsoft Entra ID
Monitor
Advisor
Microsoft Defender for Cloud
Cost Management +
Home > Network Watcher
Network Watcher | Connection troubleshoot
Microsoft
Search
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Usage + quotas
Logs
Add or remove favorites by pressing Ctrl+Shift+F
Network Watcher connection troubleshoot provides the capability to check a direct TCP or ICMP connection from a virtual machine (VM), application gateway v2, or Bastion host to a VM, fully qualified domain name (FQDN), URI, or IP address. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Run diagnostic tests". Learn more.
Source
Source type * Virtual machine
Virtual machine * vm01
Select virtual machine
Destination
Destination type Select a virtual machine
Specify manually
Virtual machine * vm02
Select virtual machine
Probe settings
Preferred IP version IPv4
Give feedback


TECHNICAL GUFTGU
Network Watcher - Microsoft A
Delete immutable blob storage
portal.azure.com/#view/Microsoft_Azure_Network/NetworkWatcherMenuBlade/~/vmConnectivity
Open in app
GitHub
LinkedIn
linux
AWS Resources - A...
aws — AWS CLI 2.2...
TECHNICAL GUFTGU
Azure
DEVOPS ZERO TO H...
Ansible Community...
ChatGPT
Ansible Galaxy - We...
All Bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
harshu9084@hotmail.c...
DEFAULT DIRECTORY
Home > Network Watcher
Network Watcher | Connection troubleshoot
Microsoft
Search
Overview
Get started
Monitoring
Topology
Connection monitor
Traffic Analytics
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Usage + quotas
Logs
Add or remove favorites by pressing Ctrl+Shift+F
Preferred IP version IPv4
Protocol TCP
ICMP
Destination port * 80
Source port 80
Connection diagnostic
Diagnostic tests * Connectivity, NSG diagnostic, Next hop, Port scanner
Run diagnostic tests
Results
Test(s) ran: Connectivity, NSG diagnostic, Next hop, Port scanner
Source: vm01 Destination: vm02
Export to CSV
Diagnostic tests
Give feedback



💡 What It Does

You give Azure:

- A **source** (like a VM or network interface)
- A **destination** (like another VM, IP address, or URL)
- A **port number** (like 22 for SSH, 3389 for RDP, 443 for HTTPS)

Then Azure checks the entire path and tells you:

- ✅ If the connection **succeeds**
- ❌ If it **fails**, where it failed — for example:
- NSG rule blocked it
- Route table problem
- Firewall issue
- Destination unreachable