- It provides a dedicated, private connection between your on-premises resources and Azure. Extra security is by adding network security appliances between edge routers.

  This is the correct definition of an ExpressRoute
- It provides a base layer of security by allowing you to segment and isolate your Azure resources.
- It routes traffic from your network to Azure over the internet.

Next unit: Summary

Continue

Previous Unit 6 of 6

100 XP

Summary

1 minute

In this module, you've explored migrating your on-premises infrastructure to Azure by using the hub and spoke model. You covered the components that you need to create hub and spoke networks, including Azure ExpressRoute, and how to secure them in Azure.

A hub and spoke architecture in Azure allows your business to quickly and easily adapt to new requirements. You can add spokes to segrega workloads with network security groups and Azure Firewall.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire s resources.

More information

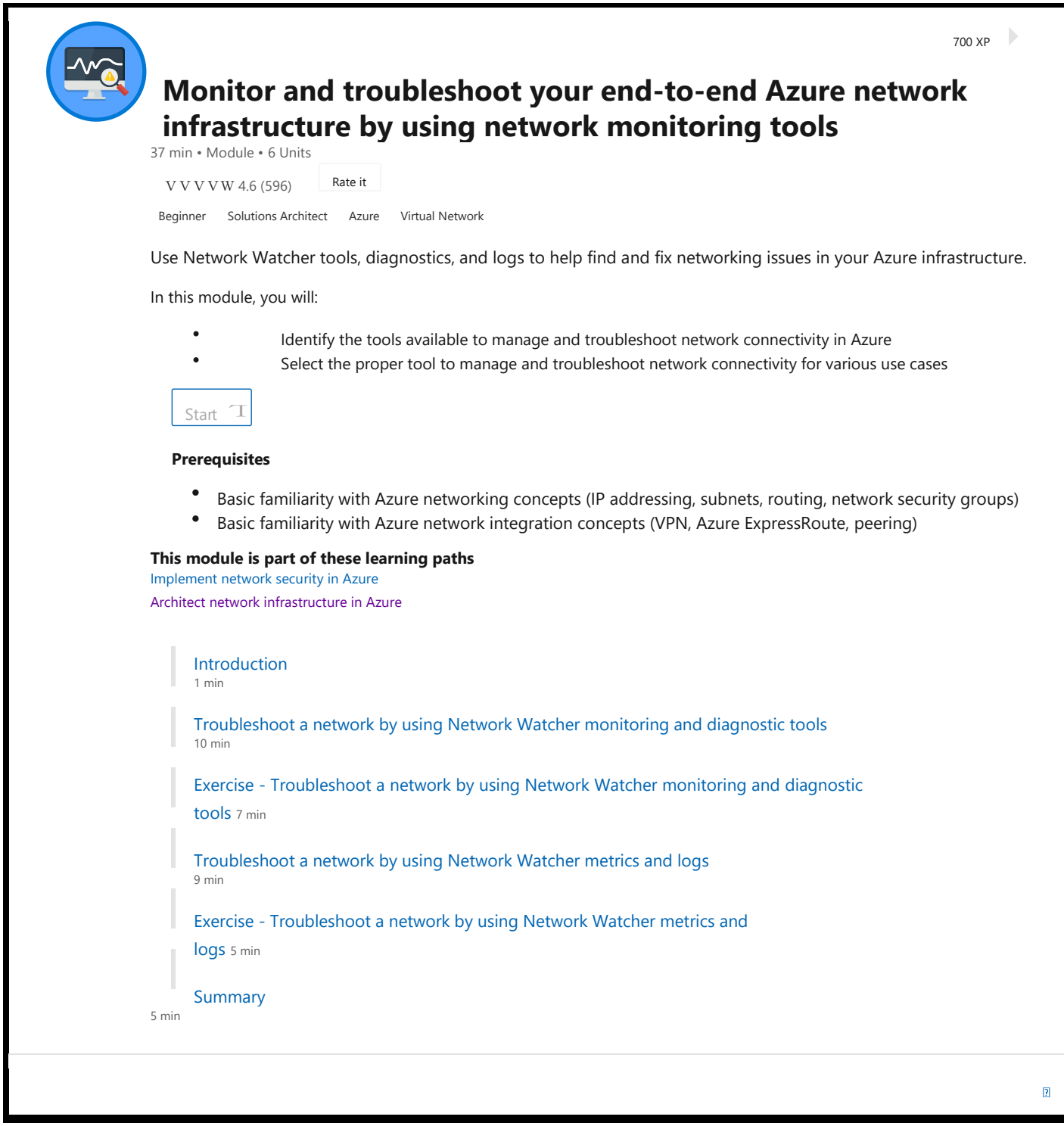
- Hub and spoke topology
- Connect to Azure by using ExpressRoute
- Azure DDoS protection

Module complete:

Unlock achievement

https://docs.microsoft.com/en-us/learn/modules/hub-and-spoke-network-architecture/6-summary 1/2

2/21/2020 Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools - Learn | Microsoft Docs



700 XP

Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools

37 min • Module • 6 Units

V V V V W 4.6 (596) Rate it

Beginner Solutions Architect Azure Virtual Network

Use Network Watcher tools, diagnostics, and logs to help find and fix networking issues in your Azure infrastructure.

In this module, you will:

- Identify the tools available to manage and troubleshoot network connectivity in Azure
- Select the proper tool to manage and troubleshoot network connectivity for various use cases

Start

Prerequisites

- Basic familiarity with Azure networking concepts (IP addressing, subnets, routing, network security groups)
- Basic familiarity with Azure network integration concepts (VPN, Azure ExpressRoute, peering)

This module is part of these learning paths

Implement network security in Azure

Architect network infrastructure in Azure

Introduction
1 min

Troubleshoot a network by using Network Watcher monitoring and diagnostic tools
10 min

Exercise - Troubleshoot a network by using Network Watcher monitoring and diagnostic tools 7 min

Troubleshoot a network by using Network Watcher metrics and logs
9 min

Exercise - Troubleshoot a network by using Network Watcher metrics and logs 5 min

Summary
5 min

https://docs.microsoft.com/en-us/learn/modules/troubleshoot-azure-network-infrastructure/index 1/1

2/21/2020 Introduction - Learn | Microsoft Docs

Unit 1 of 6 S Next T

100 XP

Introduction

1 minute

You can create complex and flexible setups in Azure that connect many virtual machines (VMs) together to meet your needs. But just like in an on-premises network, configuration errors can result in problems that are challenging to troubleshoot. When you have to diagnose network problems in Azure, use Azure Network Watcher.

Suppose you're the Azure architect for an engineering company. You have deployed a VM in Azure, and the VM has network connectivity issues. You want to learn how to troubleshoot and fix the problem so that you can help your colleagues to do the same if they face similar issues in the future.

In this module, you'll learn about the core Network Watcher features. Engineers use Network Watcher to monitor, diagnose, and gain insight into their network health and performance with metrics. The elements can be broken down into four areas: monitoring, network diagnostic tools, metrics, and logs.

By the end of this module, you'll be able to troubleshoot connectivity problems by using Network Watcher so that you can fix them.

Learning objectives

- Identify the tools available to manage and troubleshoot network connectivity in Azure
- Select the proper tool to manage and troubleshoot network connectivity for various use cases

Prerequisites

Basic familiarity with Azure 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

Next unit: Troubleshoot a network by using Network Watcher monitoring and diagnostic tools

Continue

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, we'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:

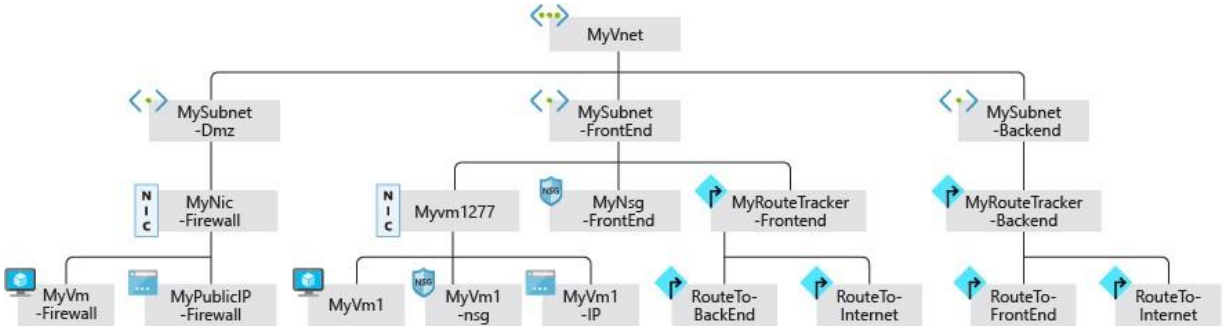
1. On the Azure portal menu, select **All services**. Then go to **Networking** > **Network Watcher**.

2. Select **Topology**.

3. Select a subscription, the resource group of a virtual network, and then the virtual network itself.

> **Not**
>
> 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. Use this tool to communicate if you want them to.

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

If there's an issue, Connection Monitor tells you why it occurred and how to fix it. Along with monitoring VMs, Connecti 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 v your network.

When you decide to monitor your hybrid connections by using Network Performance Monitor, check that the associate 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
- Security group view
- 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 grou 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 outbour from a VM. Within the tool, you specify a local and remote port, the protocol (TCP or UDP), the local IP, the remote IP, t 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 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 IP address, and destination IP address. The tool then determines the packet's destination. You can use this tool t caused by incorrect routing tables.

What is the security group view tool?

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

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

For example, if two VMs can't communicate because an NSG rule blocks them, it can be difficult to diagnose which rule You'll use the security group view tool in Network Watcher to display all the effective NSG rules and help you diagnose 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 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 captured to g 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 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 i sessions per region, and the overall limit is 10,000. These limits are for the number of sessions only, not saved captures 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. The "Learn more" section at the e module includes links to instructions that detail the installation of the extension on both Windows and Linux VMs.

What is the connection troubleshoot tool?

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

If the connection is successful, information about the communication is displayed, 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 d
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 re
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
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 a

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
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 (TC
the remote IP to check the connection status. It also lets you specify the direction of the connection (inbound or outbou
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 ad
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 rul

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
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 th
information. The diagnosis will show whether the VPN connection is working or not working. If the VPN connection isn't
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 th
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 problem and must be corrected to permit the connection.

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

- [x] Network Watcher Agent VM Extension

  The Network Watcher Agent VM Extension is required when you capture traffic on a VM. It's automatically installed when you start a packet capture session in the Azure portal.

- [ ] 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
- [x] Connection troubleshoot

  Connection troubleshoot displays the latency associated with each hop in a route.

Next unit: Exercise - Troubleshoot a network by using Network Watcher monitoring and diagnostic tools

Continue

100 XP

Exercise - Troubleshoot a network by using Network Watcher monitoring and diagnostic tools

7 minutes

Azure Network Watcher helps you diagnose configuration errors that prevent virtual machines (VMs) from communicating.

Suppose you have two VMs that can't communicate. You want to diagnose the problem and resolve it as fast as possible. You want to use Network Watcher to do that.

Here, you'll troubleshoot connectivity between two VMs in different subnets.

Importan

You need your own Azure subscription to run this exercise and you may incur charges. If you don't already have an Az create a free t before you begin.

Configure a virtual network and VMs

Let's start by creating the problematic infrastructure, which includes a configuration error:

1. Open the Azure Cloud Shell in your browser, and log in to the directory with access to the subscription you want to create resources in.

2. Run the following command in the Cloud Shell to create a variable to store your resource group name, and a resource group for your resources. Replace `<resource group name>` with a name for your resource group, and `<location>` with the Azure region you'd like to deploy your resources in.

   Azure CLI — Copy

   ```
   rg=<resource group name>
    az group create --name $rg --location <location>
   ```

3. In Azure Cloud Shell, run this command to create the virtual network **MyVNet1** and the subnet **FrontendSubnet**.

   Azure CLI — Copy

   ```
   az network vnet create \
       --resource-group $rg \
       --name MyVNet1 \
       --address-prefix 10.10.0.0/16 \
       --subnet-name FrontendSubnet \     --subnet-
   prefix 10.10.1.0/24 \
       --location EastUS
   ```

4. Run this command to deploy a VM in **FrontendSubnet**. Replace `<password>` with a complex password of your choice.

   Azure CLI — Copy

```
az vm create \
    --resource-group $rg \
    --no-wait \
    --name FrontendVM \     --
location EastUS \
    --vnet-name MyVNet1 \
    --subnet FrontendSubnet \
    --image Win2012R2Datacenter \
```

```
    --admin-username azureuser \
    --admin-password <password>
```

5. Run this command to create the subnet called **BackendSubnet**.

```
Azure CLI
az network vnet subnet create \
    --address-prefixes 10.10.2.0/24 \
    --name BackendSubnet \     --resource-
group $rg \
    --vnet-name MyVNet1
```

6. Run this command to deploy a virtual machine in **BackendSubnet**. Replace `<password>` with a complex password of your choice.

```
Azure CLI
az vm create \
    --resource-group $rg \
    --no-wait \
    --name BackendVM \
    --location EastUS \
    --vnet-name MyVNet1 \
    --subnet BackendSubnet \
    --image Win2012R2Datacenter \
    --admin-username azureuser \
    --admin-password <password>
```

7. Run this command to create a network security group (NSG).

```
Azure CLI
az network nsg create \     --
name MyNsg \
    --resource-group $rg \
    --location EastUS
```

8. Run this command to create an NSG configuration mistake that prevents communication between the VMs.

```
Azure CLI
az network nsg rule create \
    --resource-group $rg \
    --name MyNSGRule \
    --nsg-name MyNsg \
    --priority 4096 \
    --source-address-prefixes '*' \
    --source-port-ranges 80 443 3389 \
    --destination-address-prefixes '*' \
    --destination-port-ranges 80 443 3389 \
    --access Deny \
    --protocol TCP \
    --description "Deny from specific IP address ranges on 80, 443 and 3389."
```

9. Run this command to associate a network security group with a subnet.

```
Azure CLI
az network vnet subnet update \
    --resource-group $rg \     --
name BackendSubnet \
    --vnet-name MyVNet1 \
    --network-security-group MyNsg
```

able Network Watcher for your region

Now let's use the Azure CLI to set up Network Watcher in the same region as the infrastructure.

To enable Network Watcher, run this command:

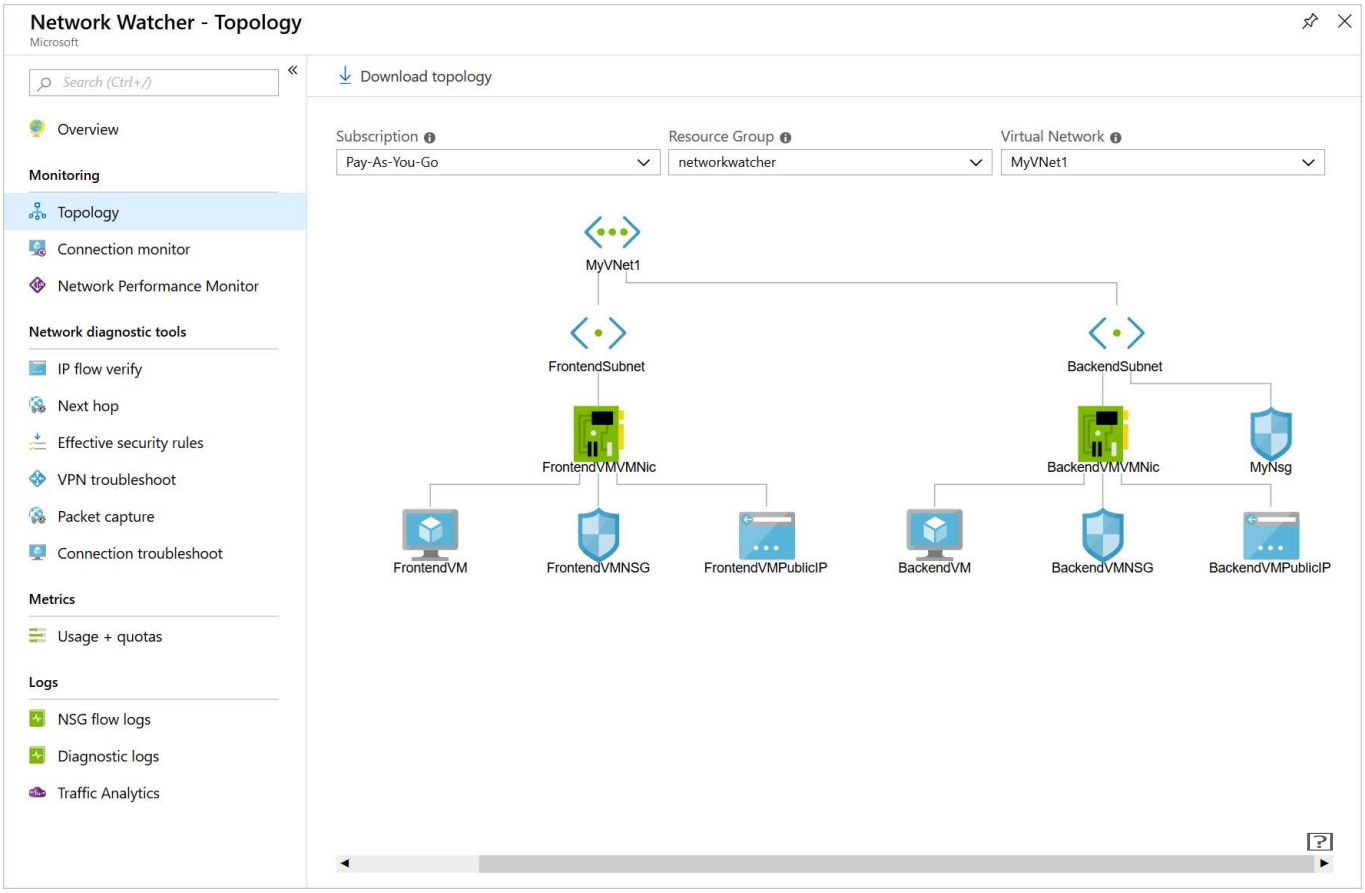
Azure CLI Copy

```
az network watcher configure \
    --resource-group $rg \
    --locations EastUS \
    --enabled
```

Use Network Watcher to show the topology

Now you can use Network Watcher to troubleshoot connectivity between two VMs in different subnets. Your colleague connectivity issue over HTTP/HTTPS and the RDP protocol between the two VMs. First, investigate the network topolog

1. Sign in to the Azure portal by using the account that you used to activate the sandbox.
2. On the Azure portal menu, select **All services**. Then go to **Networking** > **Network Watcher**.
3. Select **Topolog**
4. In the drop-down lists, select the subscription and resource group. Network Watcher displays your network topolo

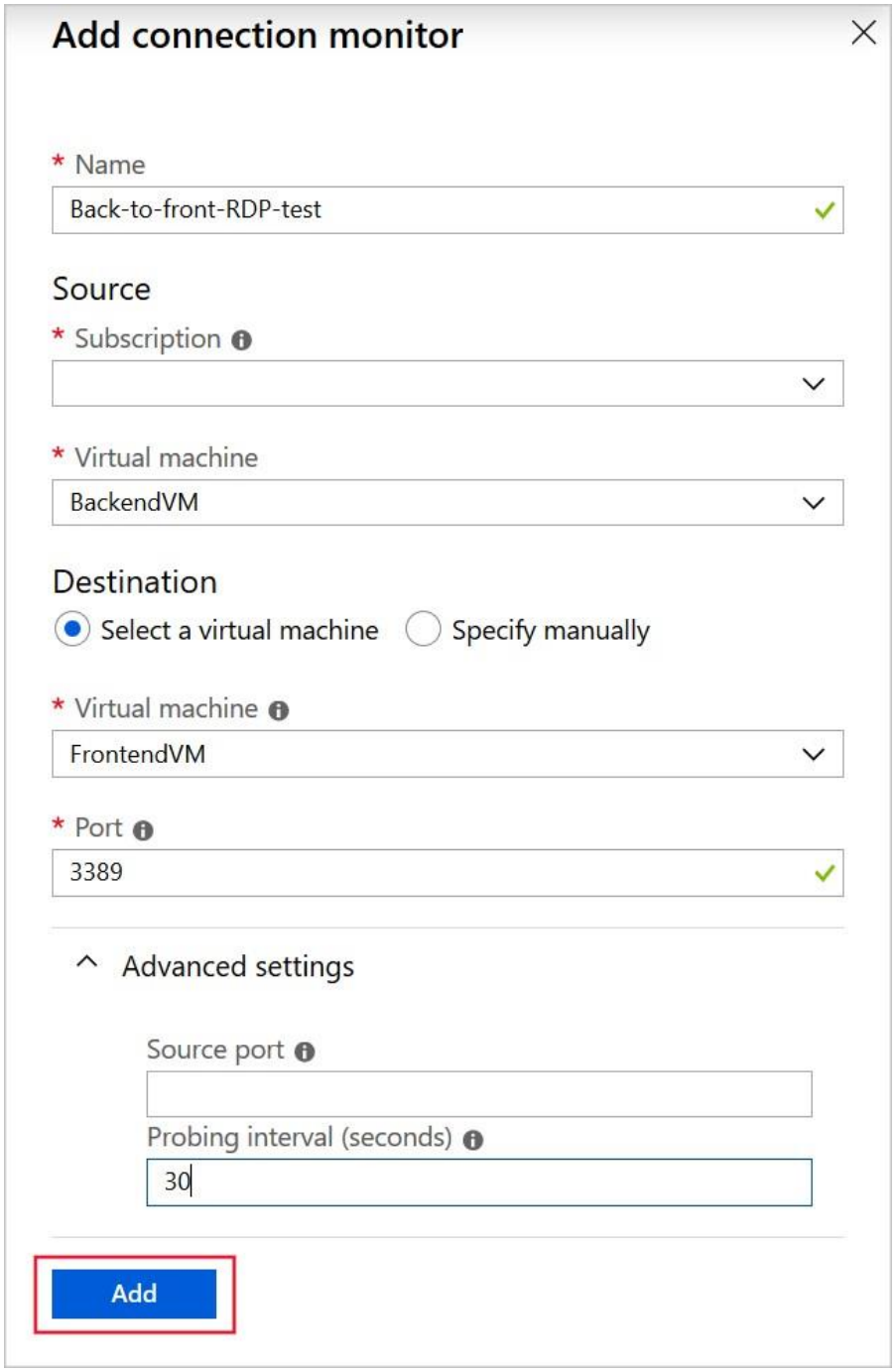


Use Connection Monitor to run tests from the back end to the front end

The topology appears to be correct. Let's set up some tests in Connection Monitor to get more information. Start by cre back-end VM to the front-end VM:

1. Under **Monitoring**, select **Connection Monitor**, and then select **+ Add**.
2. Configure Connection Monitor with these values, and then select **Add**.

Setting	Value
Name	Back-to-front-RDP-test
Subscription	Select your subscription
Virtual machine	BackendVM
Destination virtual machine	FrontendVM
Port	3389
Probing interval (seconds)	30



3. Select **+ Add**. Configure a second test with these values, and then select **Add**.

Setting	Value
Name	Back-to-front-HTTP-test
Subscription	Select your subscription
Virtual machine	BackendVM
Destination virtual machine	FrontendVM
Port	80
Probing interval (seconds)	30

4. In the list of tests, select **Back-to-front-RDP**. Select the ellipsis (...), and then select **Start**.
5. Examine the results.
6. In the list of tests, select **Back-to-front-HTTP**. Select ..., and then select **Start**.
7. Examine the results.

The results should show that no traffic flows from the back-end VM to the front-end VM.

Use Connection Monitor to run tests from the front end to the back end

Run the same tests in the opposite direction.

1. Under **Monitoring**, select **Connection monitor**, and then select **+ Add**.
2. Configure Connection Monitor with these values, and then select **Add**.

Setting	Value
Name	front-to-back-RDP-test
Subscription	Select your subscription
Virtual machine	FrontendVM
Destination virtual machine	BackendVM
Port	3389
Probing interval (seconds)	30

3. Select **+ Add**. Configure a second test with these values, and then select **Add**.

Setting	Value
Name	Front-to-back-HTTP-test
Subscription	Select your subscription
Virtual machine	FrontendVM
Destination virtual machine	BackendVM
Port	80

Setting	Value
Probing interval (seconds)	30

4. In the list of tests, select **Front-to-back-RDP**, select **...**, and then select **Start**.
5. Examine the results.
6. In the list of tests, select **Front-to-back-HTTP**, select **...**, and then select **Start**.
7. Examine the results.

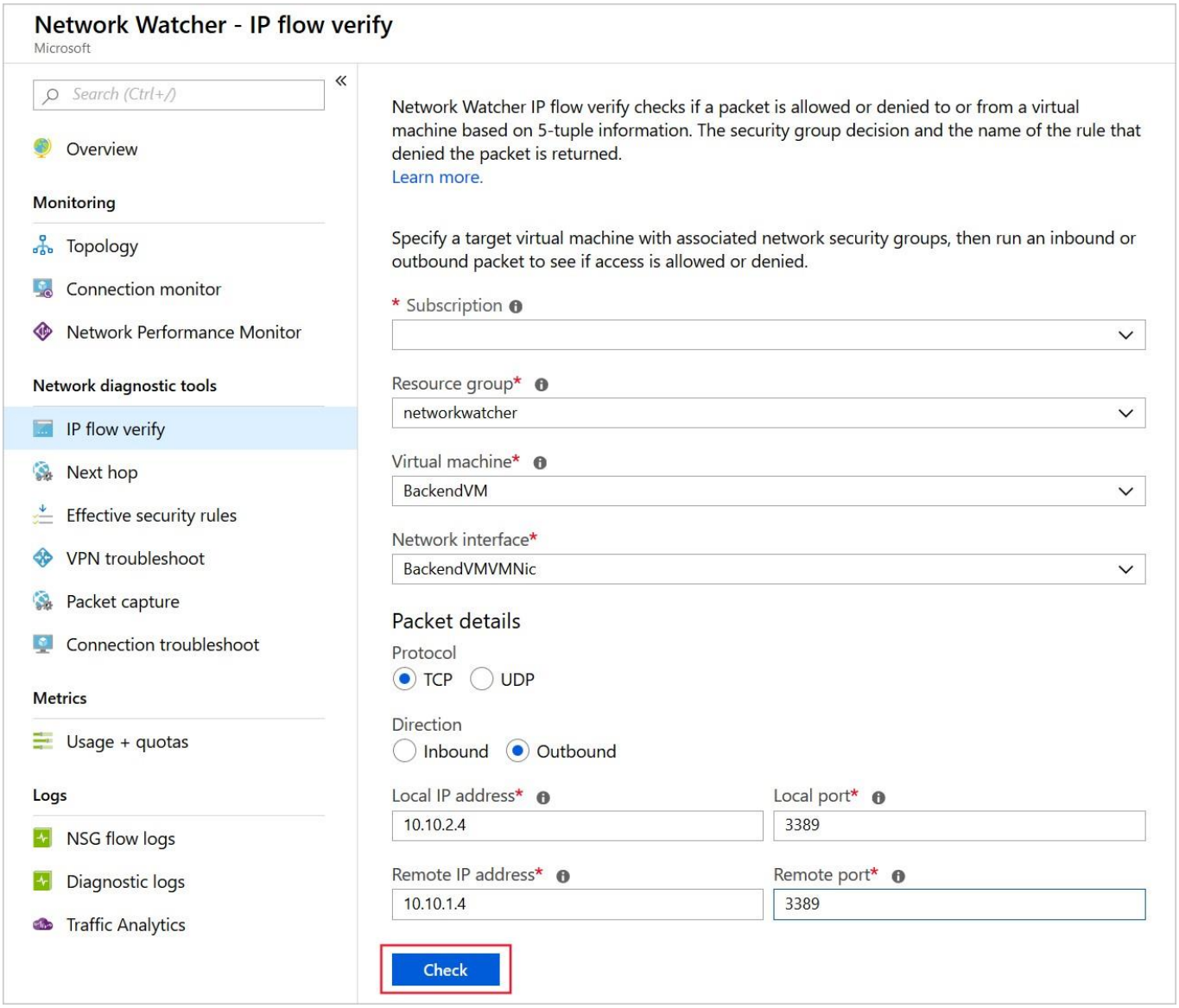
The results should show that traffic flows without problems from the front-end VM to the back-end VM.

Use IP flow verify to test the connection

Let's use the IP flow verify tool to get more information.

1. Under **Network diagnostic tools**, select **IP flow verify**.
2. Configure the test with these values, and then select **Check**.

Setting	Value
Subscription	Select your subscription
Resource group	Select your resource group
Virtual machine	BackendVM
Network interface	BackendVMVMNic
Protocol	TCP
Direction	Outbound
Local IP address	10.10.2.4
Local port	3389
Remote IP	10.10.1.4
Remote port	3389



3. Examine the results. They show that access is denied because of NSG and security rules.

In this exercise, you have successfully used Network Watcher tools to discover the connectivity issue between the two s
allowed one way but blocked the other way because of NSG rules.

Next unit: Troubleshoot a network by using Network Watcher metrics and logs

Continue

100 XP

Troubleshoot a network by using Network Watcher metrics and logs

9 minutes

If you want to diagnose a problem quickly, you have to understand the information that's available in the Azure Network

In your engineering company, you want to minimize the time it takes for your staff to diagnose and resolve any network c
You want to ensure they know which information is available in which logs.

In this module, you'll focus on flow logs, diagnostic logs, and traffic analytics. You'll learn how these tools can help to trou
network.

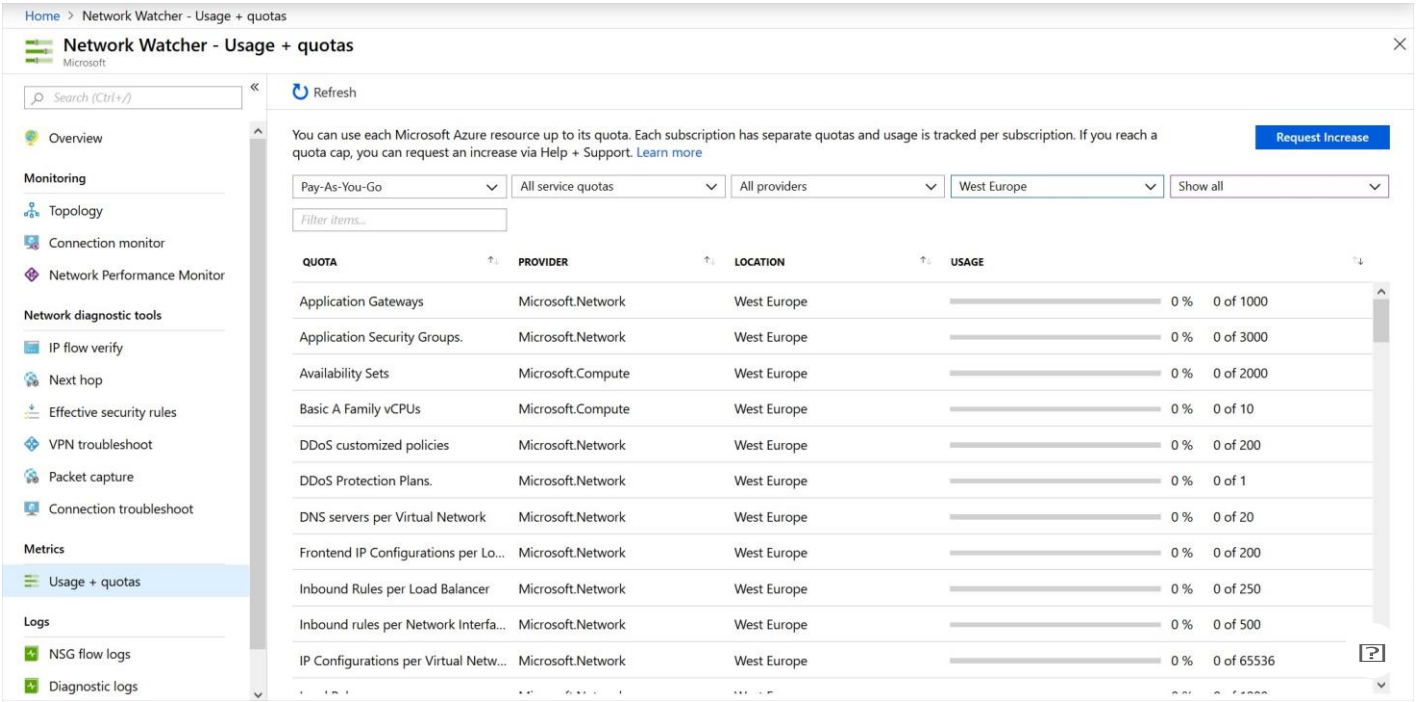
Usage and quotas

Each Microsoft Azure resource can be used up to its quota. Each subscription has separate quotas, and usage is tracked p
one instance of Network Watcher is required per subscription per region. This instance gives you a view of usage and quo
if you're at risk of hitting a quota.

To view the usage and quota information, go to **All services** > **Networking** > **Network Watcher**, and then select **Usage and quotas**. You'll see granular data based on usage and resource location. Data for the following metrics is captured:

- Network interfaces
- Network security groups (NSGs)
- Virtual networks
- Public IP addresses

Here's an example that shows usage and quotas in the portal:



Logs

Network diagnostic logs provide granular data. You'll use this data to understand connectivity and performance issues be
display tools in Network Watcher:

- Flow logs
- Diagnostic logs
- Traffic analytics

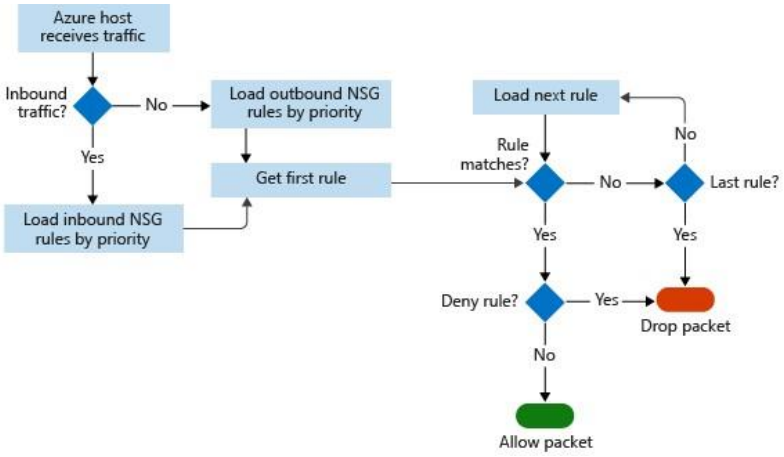
Let's look at each of these tools.

Flow logs

In flow logs, you can view information about ingress and egress IP traffic on network security groups. Flow logs show outb
flows on a per-rule basis, based on the network adapter that the flow applies. NSG flow logs show whether traffic was all
on the 5-tuple information captured. This information includes:

- Source IP
- Source port
- Destination IP
- Destination port
- Protocol

This diagram shows the workflow that the NSG follows:



Flow logs store data in a JSON file. It can be difficult to gain insights into this data by manually searching the log files, esp
large infrastructure deployment in Azure. You can solve this problem by using Power BI.

In Power BI, you can visualize NSG flow logs by (for example):

- Top talkers (IP address)
- Flows by direction (inbound and outbound)
- Flows by decision (allowed and denied)
- Flows by destination port

You can also use open-source tools to analyze your logs, such as Elastic Stack, Grafana, and Graylog.

> **Not**
>
> NSG flow logs don't support storage accounts on the Azure classic portal.

Diagnostic logs

In Network Watcher, diagnostic logs are a central place to enable and disable logs for Azure network resources. These res
NSGs, public IPs, load balancers, and application gateways. After you've enabled the logs that interest you, you can use th
view log entries.

You can import diagnostic logs into Power BI and other tools to analyze them.

Traffic analytics

Use traffic analytics to investigate user and application activity across your cloud networks.

The tool gives insights into network activity across subscriptions. You can diagnose security threats such as open ports, VI known bad networks, and traffic flow patterns. Traffic analytics analyzes NSG flow logs across Azure regions and subscrip data to optimize network performance.

This tool requires Log Analytics. The Log Analytics workspace must exist in a supported region.

Use case scenarios

Now let's look at some use case scenarios where Azure Network Watcher metrics and logs can be helpful.

Customer reports of slow performance

To resolve slow performance, you need to determine the root cause of the problem:

- Is there too much traffic throttling the server?
- Is the VM size appropriate for the job?
- Are the scalability thresholds set appropriately?
- Are any malicious attacks happening?
- Is the VM storage configuration correct?

First, check that the VM size is appropriate for the job. Next, enable Azure Diagnostics on the VM to get more granular da such as CPU usage and memory usage. To enable VM diagnostics via the portal, select the **VM**, select **Diagnostics Settings**, and then turn on diagnostics.

Let's assume you have a VM that has been running fine. However, the VM's performance has recently degraded. To ident resource bottlenecks, you need to review the captured data.

Start with a time range of captured data before, during, and after the reported problem to get an accurate view of perfor can also be useful for cross-referencing different resource behaviors in the same period. You'll check for:

- CPU bottlenecks
- Memory bottlenecks
- Disk bottlenecks

CPU

When you're looking at performance issues, examine trends and understand if they affect your server. Use the monitorin to spot trends. You might see different types of patterns on the monitoring graphs:

- **Isolated** . A spike might be related to a scheduled task or an expected event. If you know what this task is, does i performance level? If the performance is OK, you might not need to increase capacity.
- **Spike up and** . A new workload might cause this trend. Enable monitoring in the VM to find out what processes The increased consumption might be due to inefficient code or normal consumption. If the consumption is normal, d operate at the required performance level?
- **Constant** Has your VM always been like this? If so, you should identify the processes that consume most resources an capacity.
- **Steadily** . Do you see a constant increase in consumption? If so, this trend might indicate inefficient code or a more user workload.

If you do observe high CPU utilization, you can either:

- Increase the size of the VM to scale with more cores.
- Investigate the issue further. Locate the application and process, and troubleshoot accordingly.

If you scale up the VM and the CPU is still running at above 95 percent, is this offering better performance or higher application throughput to an acceptable level? If not, troubleshoot that individual application.

Memory bottlenecks

You can view the amount of memory that the VM uses. Logs will help you understand the trend and if it maps to the time at which you see issues. You should not have less than 100 MB of available memory at any time. Watch out for the following trends:

- **Spike up and constant consumption**. High memory utilization might not be the cause of bad performance. Some applications, such as relational database engines, are memory intensive by design. But if there are multiple memory-hungry applications, you might see bad performance because memory contention causes trimming and paging to disk. These processes will cause a negative performance impact. **Steadily increasing consumption**. This trend might be an application *warming up*. It's common when database engines start up. However, it might also be a sign of a memory leak in an application.
- **Page or swap file usage**. Check if you're using the Windows page file heavily, or the Linux swap file, located in /dev/sdb.

To resolve high memory utilization, consider these solutions:

- For immediate relief or page file usage, increase the size of the VM to add memory, and then monitor.
  Investigate the issue further. Locate that application or process and troubleshoot it. If you know the application, see if you can cap the memory allocation.

Disk bottlenecks

Network performance might also be related to the storage subsystem of the VM. You can investigate the storage account for the VM in the portal. To identify issues with storage, look at performance metrics from the storage account diagnostics and the VM diagnostics. Look for key trends when the issues occur within a particular time range.

- To check for Azure Storage timeout, use the metrics **ClientTimeOutError**, **ServerTimeOutError**, **AverageE2ELatency**, **AverageServerLatency**, and **TotalRequests**. If you see values in the **TimeOutError** metrics, an I/O operation took too long and timed out. If you see **AverageServerLatency** increase at the same time as **TimeOutErrors**, it might be a platform issue. Raise a case with Microsoft technical support.
  To check for Azure Storage throttling, use the storage account metric **ThrottlingError**. If you see throttling, you're hitting the IOPS limit of the account. You can check this problem by investigating the metric **TotalRequests**.

To remediate high disk utilization and latency issues:

- Optimize VM I/O to scale past virtual hard disk (VHD) limits.
  Increase throughput and reduce latency. If you find that you have a latency-sensitive application and require high throughput, migrate your VHDs to Azure Premium Storage.

Virtual machine firewall rules that block traffic

To troubleshoot an NSG flow issue, use the Network Watcher IP flow verify tool and NSG flow logging to determine whether an NSG or User Defined Routing (UDR) is interfering with traffic flow.

Run IP flow verify, and specify the local VM and the remote VM. After you select **Check**, Azure runs a logical test on rules in place. If the result is that access is allowed, use NSG flow logs.

In the portal, go to the NSGs. Under the flow log settings, select **On**. Now try to connect to the VM again. Use Network Watcher traffic analytics to visualize the data. If the result is that access is allowed, there's no NSG rule in the way.

If you've reached this point and still haven't diagnosed the problem, there might be something wrong on the remote VM. Disable the firewall on the remote VM, and then retest connectivity. If you can connect to the remote VM with the firewall disabled, verify the remote firewall settings.
Then re-enable the firewall.

Inability of the front-end and back-end subnets to communicate

By default, all subnets can communicate in Azure. If two VMs on two subnets can't communicate, there must be a configuration that's blocking communication. Before you check the flow logs, run the IP flow verify tool from the front-end VM to the back-end VM. This tool runs a logical test on the rules on the network.

If the result is an NSG on the back-end subnet blocking all communication, reconfigure that NSG. For security purposes, you must block some communication with the front end because the front end is exposed to the public internet.

By blocking communication to the back end, you limit the amount of exposure in the event of a malware or security attack. However, if the NSG blocks everything, then it's incorrectly configured. Enable the specific protocols and ports that are required.

Next unit: Exercise - Troubleshoot a network by using Network Watcher metrics and logs
Continue

Exercise - Troubleshoot a network by using Network Watcher metrics and logs

5 minutes

In Azure Network Watcher, metrics and logs can diagnose complex configuration problems.

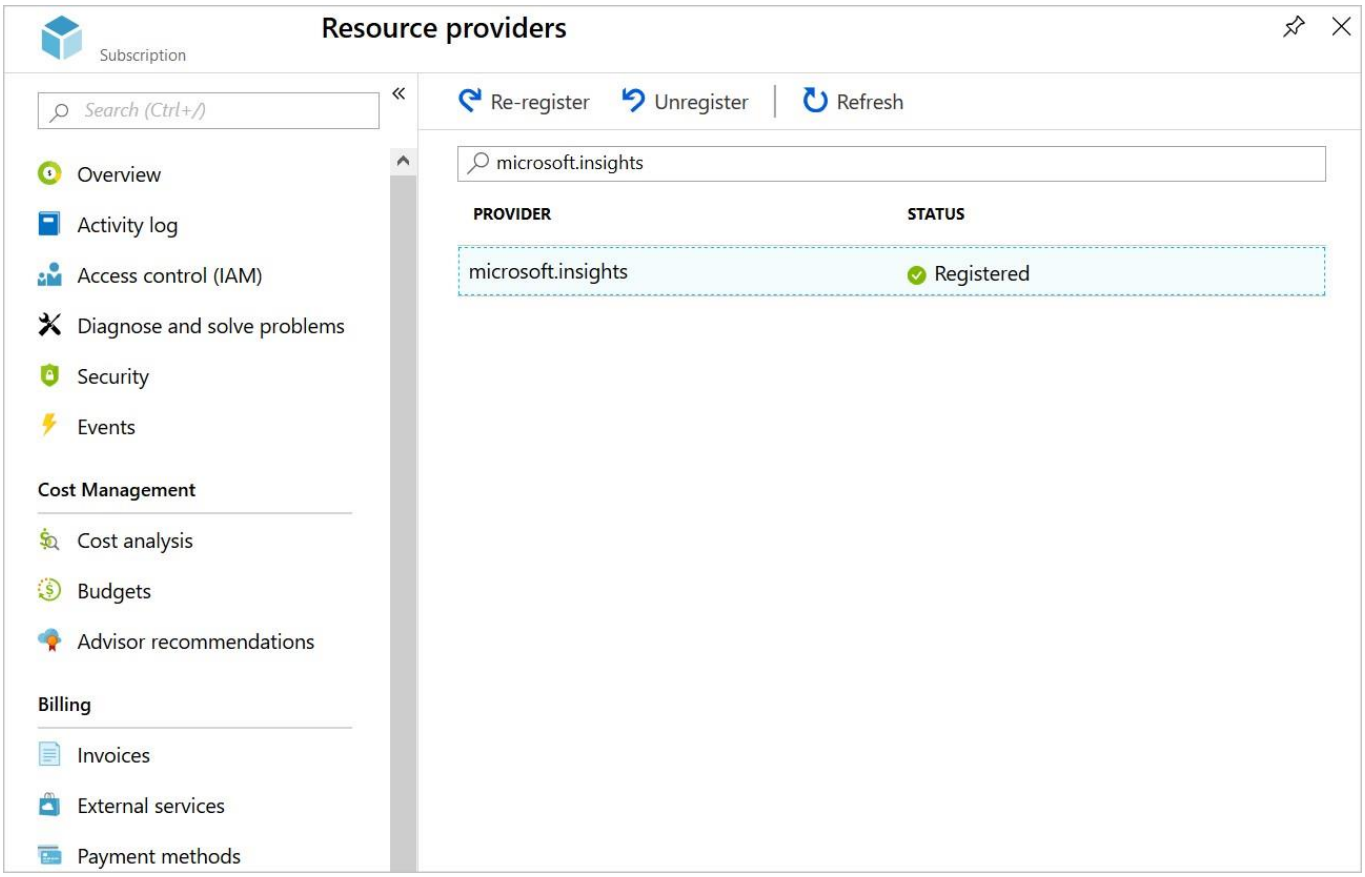
Suppose you have two virtual machines (VMs) that can't communicate. You want to obtain as much information as you can to diagnose the problem.

In this unit, you'll troubleshoot by using Network Watcher metrics and logs. You'll then use the network security group (NSG) flow logs to diagnose the connectivity issue between the two VMs.

Register the Microsoft.Insights provider

NSG flow logging requires the *Microsoft.Insights* provider. Complete the following steps to register for that provider.

1. Sign in to the Azure portal and log in to the directory with access to the subscription you created resources in.
2. In the Azure portal, search for and select **Subscriptions**. When **Subscriptions** appears in the search results, select it.
3. Select the your subscription. Then under **Settings**, select **Resource providers**.
4. In the search bar, enter **microsoft.insights**.
5. If the status of the **microsoft.insights** provider is **Unregistered**, select **Register**.



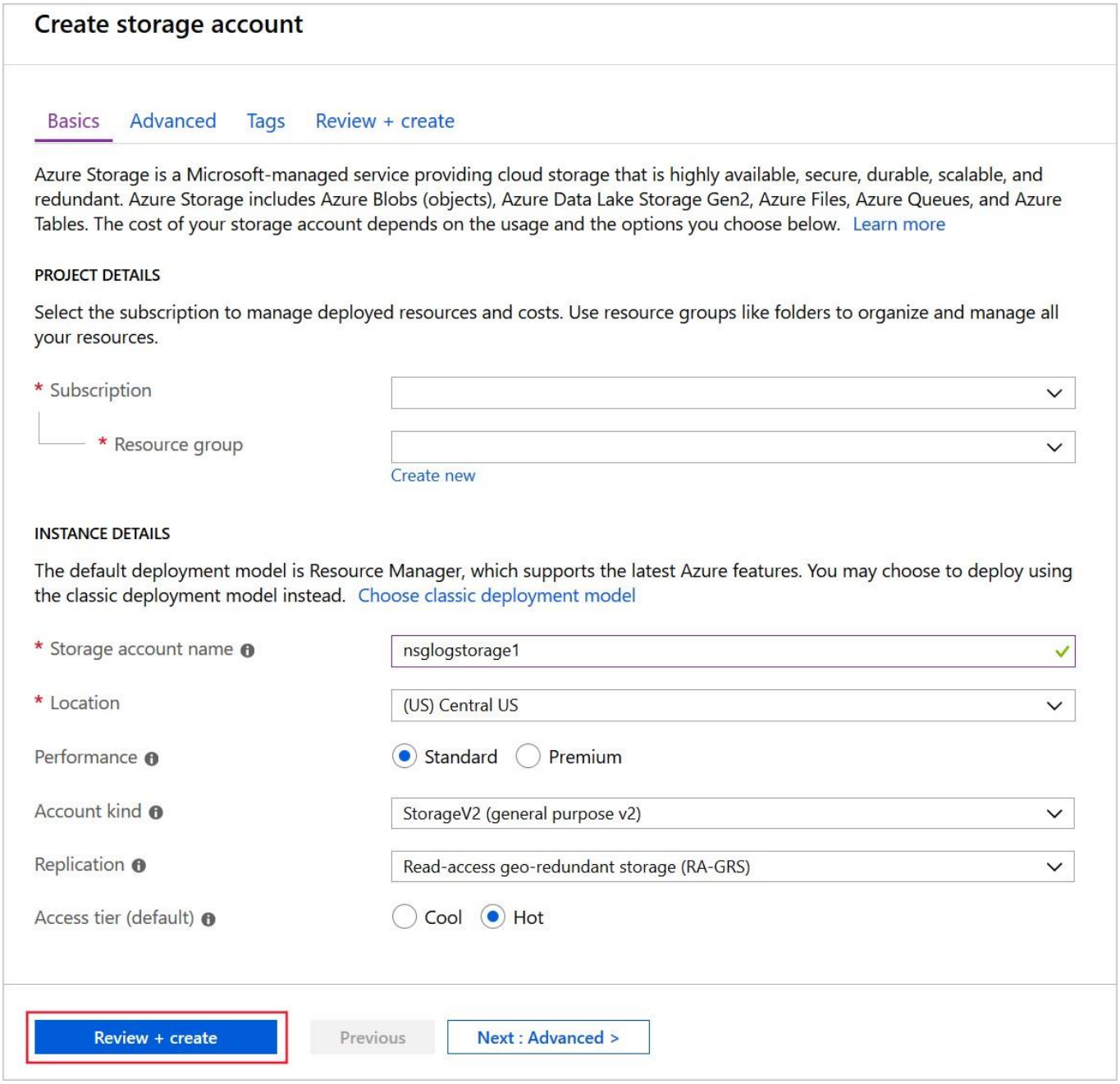
Create a storage account

Now, create a storage account for the NSG flow logs.

1. On the Azure portal menu or from the **Home** page, select **Create a resource** Then select **Storage** > **Storage account**
2. On the **Create storage account** page, fill in these settings:

Setting	Value
Subscription	Select your subscription
Resource group	Select your resource group
Storage account name	Create a unique name
Location	East US
Performance	Standard
Account kind	StorageV2
Replication	Read-access geo-redundant storage
Access tier	Hot

3. Select **Review + create**, and then select **Create**.



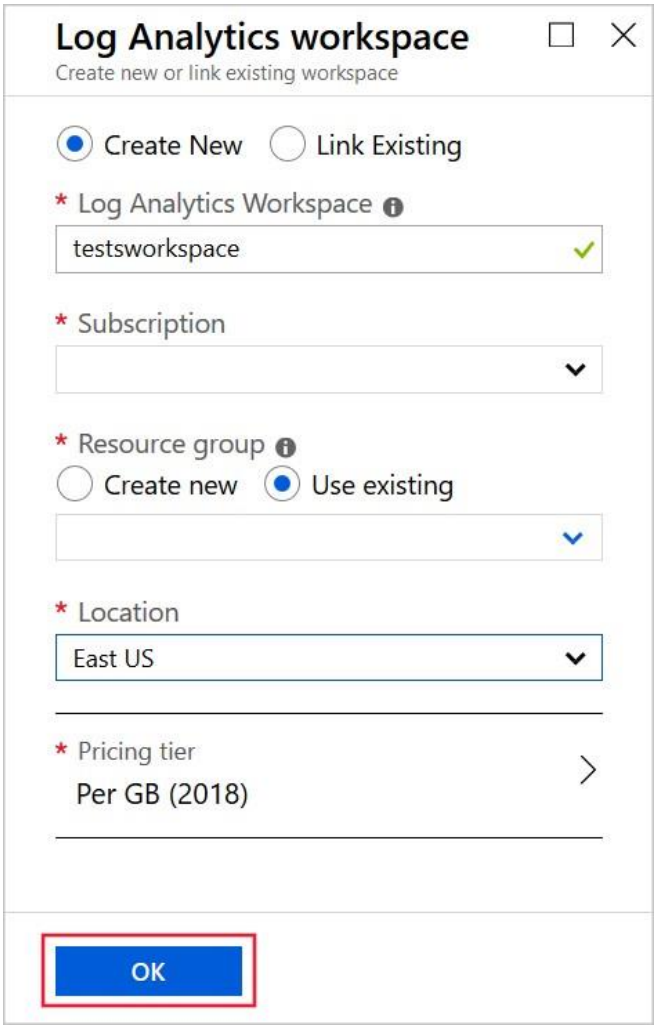
Create a Log Analytics workspace

To view the NSG flow logs, you'll use Log Analytics. To install Log Analytics.

1. In the Azure portal, search for and select **Log analytics workspaces**
2. Select **+ Add**, complete the page with these values, and then select **OK**:

Setting	Value
Log Analytics Workspace	testsworkspace
Subscription	Select your subscription
Resource group	Select your resource group
Location	East US

Setting	Value
Pricing tier	Per GB



Enable flow logs

To set up flow logs, you must configure the NSG to connect to the storage account, and add traffic analytics for the NSG.

1. On the Azure portal menu, select **All resources**. Then select the **MyNSG** network security group.
2. Under **Monitoring**, select **NSG flow logs**.
3. Select **MyNSG**, and then select **On**.
4. Under **Storage account**, select **Configure**. In the **Storage account** drop-down list, select the storage account you created earlier. Then select **OK**.
5. Under **Traffic Analytics status**, select **On**. Then in the **Traffic Analytics processing interval** drop-down list, select **Every 10 mins**.
6. Select **Log Analytics workspace**, and then select **testworkspace**.
7. Select **Save**.

Install Telnet on the front-end VM

You'll use the Telnet client to test connections between the VMs. Let's install that client now.

1. On the Azure portal menu, select **All resources**, select **FrontendVM**, and then select **Connect**.
2. Select **Download RDP File**, and then select **OK**. If you see a warning about the publisher of the remote connection, select **Connect**.
3. Sign in with the username **azureuser** and the password you specified when you created the VM, and then select **Yes**.
4. Select the **Start** button, enter **Windows features**, and then select **Turn Windows features on or off**.
5. In the **Add Roles and Features** wizard, select **Next** four times to advance to the **Features** page.
6. Select **Telnet Client**, select **Next**, and then select **Install**.
7. When the installation is complete, select **Close**.

Generate test traffic

Now you're ready to generate some network traffic between VMs to catch in the flow log:

1. Open a command prompt, and then run this command:

```
cmd
telnet 10.10.2.4 80
```

2. Run this command:

```
cmd
telnet 10.10.2.4 443
```

Both connections fail after a few seconds.

Diagnose the problem

Now, let's use log analytics to view the NSG flow logs.

1. On the Azure portal menu, select **All services**. Then select **Networking** > **Network Watcher**.
2. Under **Logs**, select **Traffic Analytics**.
3. In the **Log Analytics workspace** drop-down list, select **testworkspace**.
4. Use the different views to diagnose the problem that prevents communication from the front-end VM to the back-end VM.

Fix the problem

An NSG rule is blocking inbound traffic to the back-end subnet from everywhere over the ports 80, 443, and 3389 instead of just blocking inbound traffic from the Internet. Let's reconfigure that rule now.

1. On the Azure portal menu, select **All resources**, and then select **MyNsg**.
2. Under **Settings**, select **Inbound security rules**, and then select **MyNSGRule**.
3. Change **Source** to be **Service Tag** and configure **Source service tag** to be **Internet**.
4. Select **Save**.

Retest the connection

Connections on ports 80 and 443 should now work without problems.

1. In the RDP client, connect to **FrontendVM**. At the command prompt, run this command:

```
cmd
```

= Copy

```
telnet 10.10.2.4 80
```

2. Run this command:

```
cmd
```

= Copy

```
telnet 10.10.2.4 443
```

Both connections should now work.

Next unit: Summary

Continue T

100 XP

Summary

5 minutes

In this module, you learned about the four tool categories and the features offered. Azure Network Watcher provides all the tools you need t monitor, troubleshoot, and optimize your network. This module primarily focused on monitoring and diagnostic tools, such as:

- Connection Monitor
- IP flow verify
- Next hop
- Packet capture
- Connection troubleshoot
- Effective security rules
- NSG flow logs
- Diagnostic logs

Azure Network Watcher enables engineers to *monitor*, *diagnose*, and *gain insight* into their network health and performance.

Learn more

- Azure Network Watcher Agent virtual machine extension for Windows
- Network Watcher Agent virtual machine extension for Linux
- Visualizing network security group flow logs with Power BI
- Visualize Azure Network Watcher NSG flow logs using open-source tools
- Network Performance Monitor supported regions

Module complete:

Unlock achievement