

AZ-700

Module 08

Design and Implement Network Monitoring



AZ-700 Agenda

Module 01: Introduction to Azure Virtual Networks

Module 02: Designing and Implementing Hybrid Networking

Module 03: Designing and Implementing Azure ExpressRoute

Module 04: Load balance non-HTTP(S) traffic in Azure

LB — Basic?
— Standard!

Module 05: Load balance HTTP(S) traffic in Azure

Module 06: Design and Implement Network Security

Module 07: Design and Implement private access to Azure Services

Module 08: Design and Implement Network Monitoring



Module Overview

- Monitor your networks using Azure Monitor
- Use Azure Network Watcher to troubleshoot and analyze your network
- Exercise – Monitor a load balancer resource using Azure Monitor

vg - ~

Monitor your networks using Azure Monitor



Azure Monitor

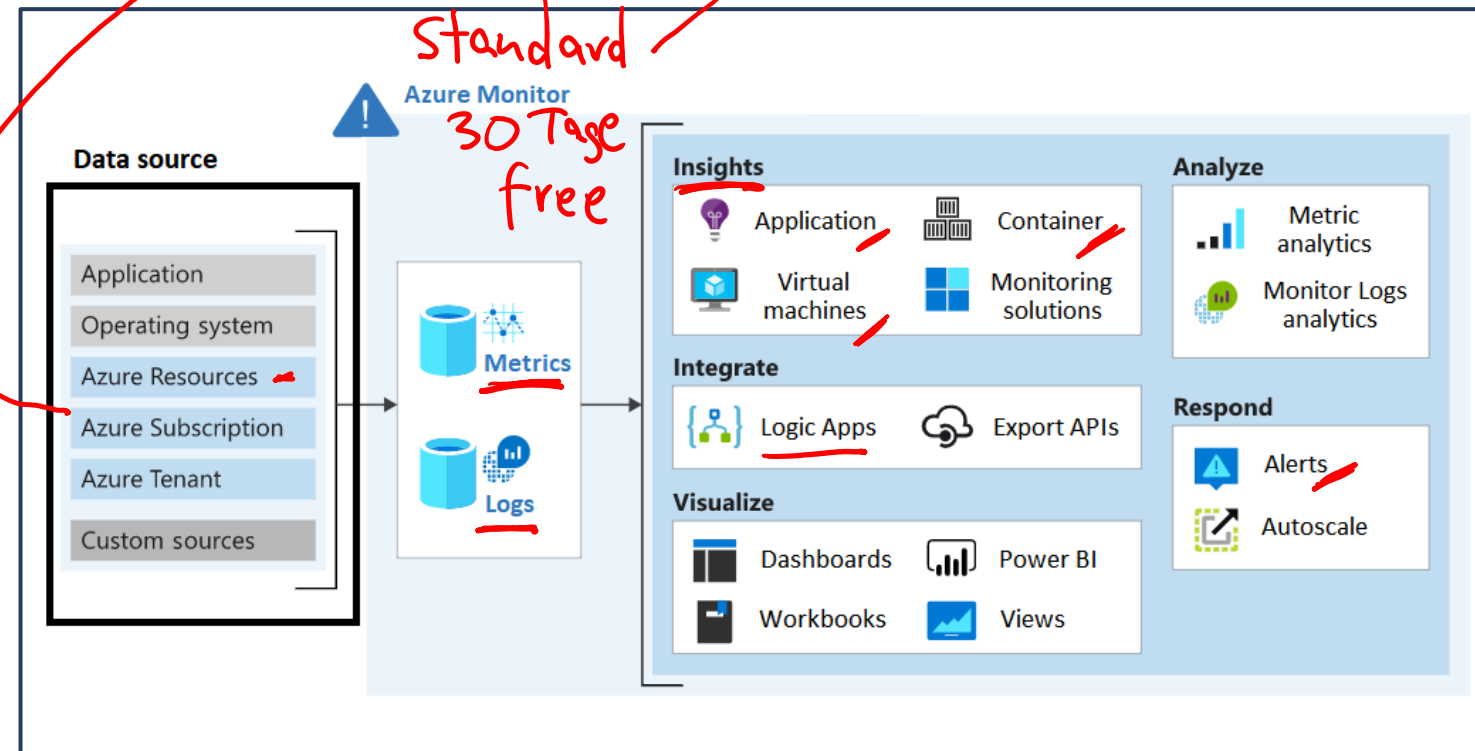
Monitoring data types: Metrics & Logs

Metrics are numerical values that describe some aspect of a system at a point in time

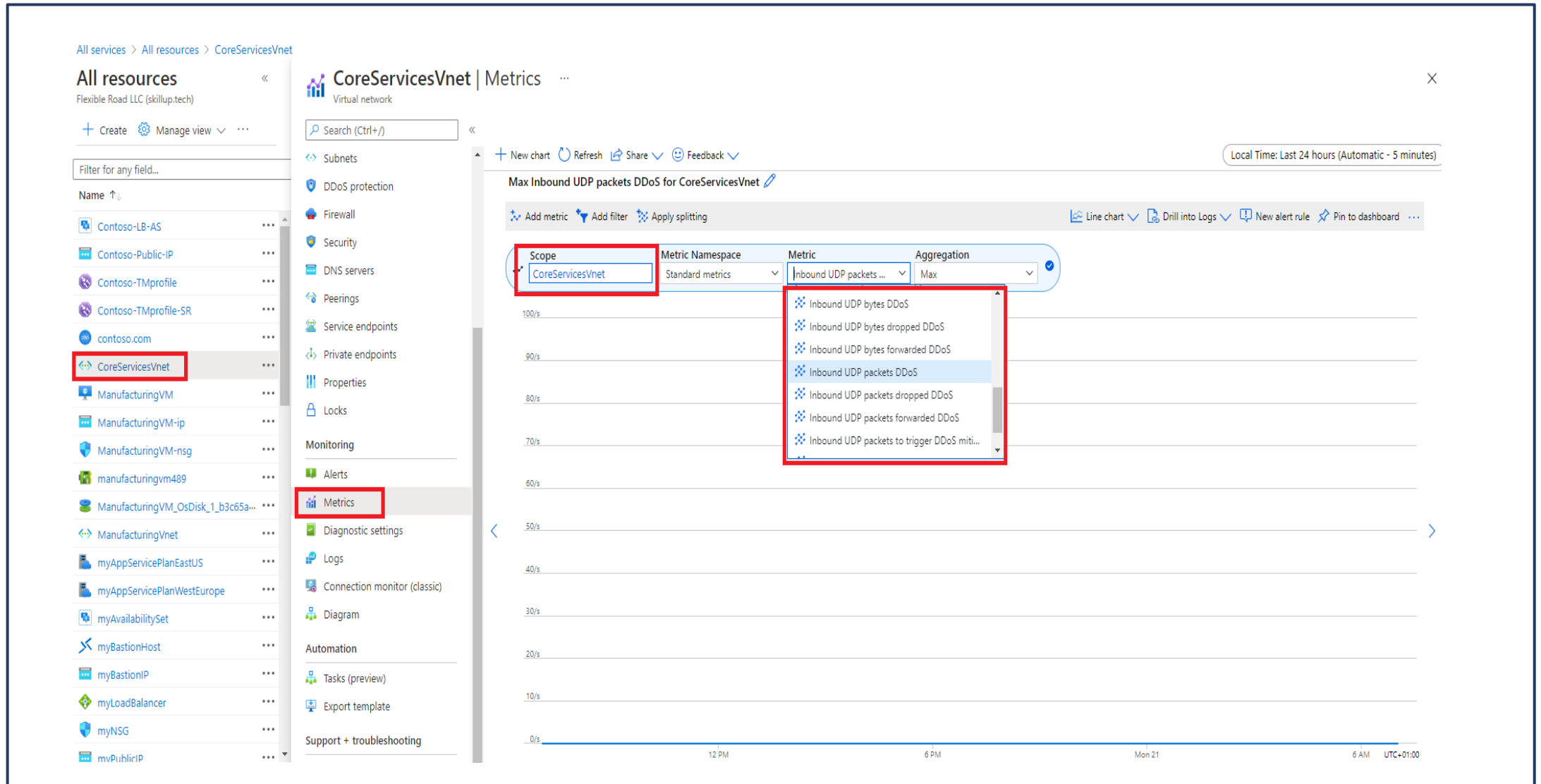
They are lightweight and capable of supporting near real-time scenarios

Logs contain different kinds of data organized into records with different sets of properties for each type

Telemetry (events, traces) and performance data can be combined for analysis



Metrics explorer



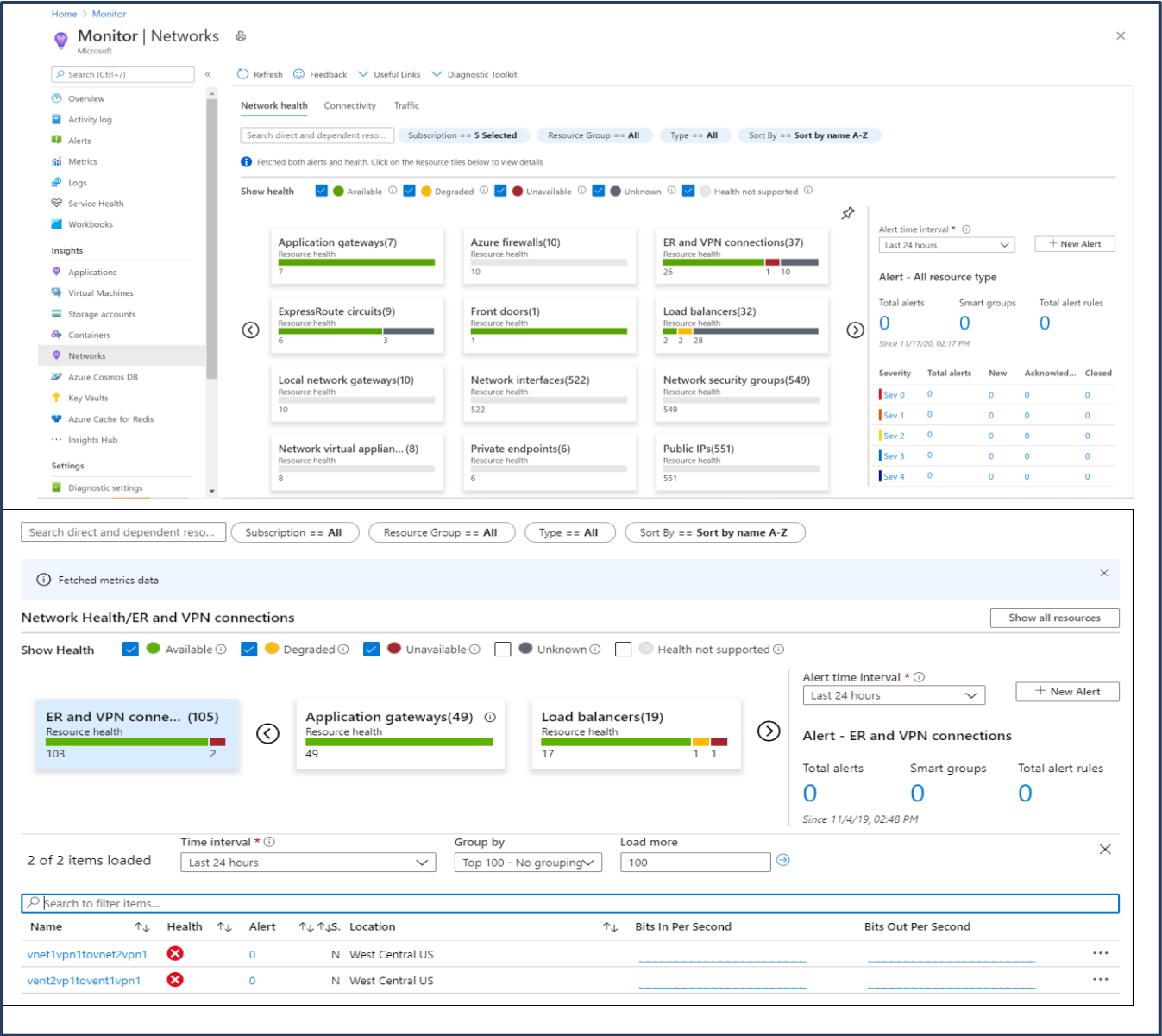
Azure Monitor Network Insights

Network health and metrics

Connectivity

Traffic

Diagnostic Toolkit



Monitor your networks using Azure Network Watcher



Network Watcher

A **regional service** ^{RG} that provides various network diagnostic and monitoring tools

IP Flow Verify diagnoses connectivity issues


Next Hop determines if traffic is being correctly routed

VPN Diagnostics troubleshoots gateways and connections

NSG Flow Logs maps IP traffic through a network security group

Connection troubleshoot shows connectivity between source VM and destination





Topology generates a visual diagram of resources






Network Watcher

Microsoft








Monitoring

-  **Topology**
-  Connection monitor (classic)
-  Connection monitor
-  Network Performance Monitor

Logs

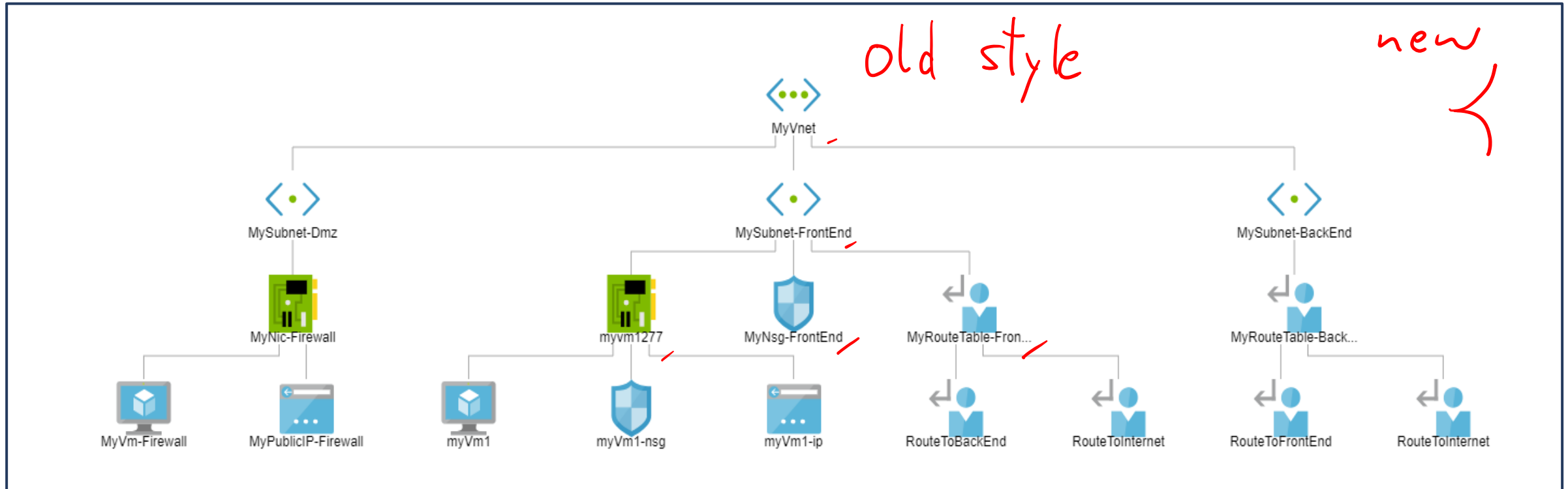
-  Flow logs
-  Diagnostic logs
-  Traffic Analytics

Network diagnostic tools

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

Topology

Diagram



Provides a visual representation of your networking elements

View all the resources in a virtual network, resource to resource associations, and relationships between the resources

The Network Watcher instance is in the same region as the virtual network

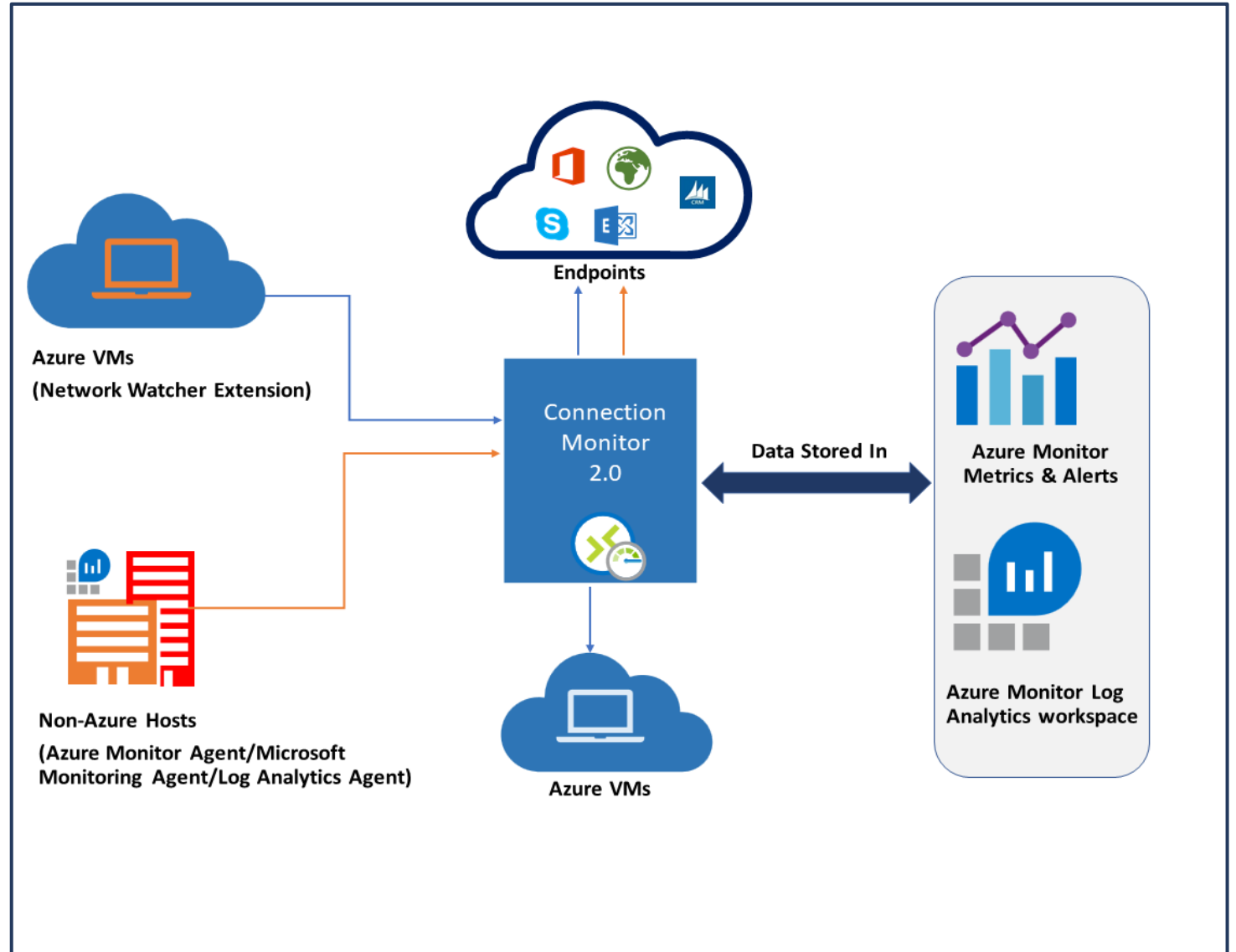
Connection Monitor

Check network connectivity between the two VMs

Compare cross-region network latencies.

Compare the latencies of the on-premises site to the latencies of the Azure application.

Check the connectivity between your on-premises setups and the Azure VMs that host your cloud application



IP Flow Verify

Checks if a packet is allowed or denied to or from a virtual machine

Network diagnostic tools

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

Metrics

- Usage + quotas

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics


Packet details

Protocol
☒ TCP ☐ UDP

Direction
☒ Inbound ☐ Outbound

Local IP address *	Local port *
<input type="text" value="10.1.1.4"/>	<input type="text" value="3389"/>
Remote IP address *	Remote port *
<input type="text" value="13.24.35.46"/>	<input type="text" value="3389"/>

[Check](#)

 Access denied

Security rule
DenyAllInBound

NSG Diagnostics

Used to understand which traffic flows will be allowed or denied in your Azure Virtual Network

Tool outputs whether traffic was allowed or denied

Outputs the NSG rules that were evaluated for the specified flow

Detailed information for debugging.

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Direction

☒ Inbound

☐ Outbound

Source type * ⓘ

IPv4 address/CIDR

IPv4 address/CIDR *

10.1.0.0/16 ✓


Destination IP address * ⓘ


10.2.0.4 ✓

Destination port * ⓘ

3389 ✓

Traffic will be allowed if all NSGs allow it.

Traffic status:  Denied

NSG name ↑↓	Applied to ↑↓	Applied action
from-nsg	from961	 Denied

Check

Next Hop

Helps with determining whether traffic is being directed to the intended destination by showing the next hop

Subscription * ⓘ

MSDN Platforms Subscription

Resource group * ⓘ

Demo

Virtual machine * ⓘ

vm01

Network interface *

vm01165

Source IP address * ⓘ

10.1.1.4

Destination IP address * ⓘ

13.24.35.46

Next hop

Result


Next hop type

None

IP address

10.1.1.100

Route table ID

/subscriptions/2301e3a0-8420-... 

Effective Security Rules

nsg01

Inbound rules

Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access ↑↓
RDP_Inbound		100		13.23.34.45/32	0-65535		0.0.0.0/0	3389-3389		TCP		✓ Allow
AllowVnetInBound		65000		Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All		✓ Allow
AllowAzureLoadBalancerInBound		65001		Azure load balancer (2 prefixes)	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		✓ Allow
DenyAllInBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		✗ Deny

Outbound rules

Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access ↑↓
AllowVnetOutBound		65000		Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All		✓ Allow
AllowInternetOutBound		65001		0.0.0.0/0,0.0.0.0/0	0-65535		Internet (216 prefixes)	0-65535		All		✓ Allow
DenyAllOutBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		✗ Deny

Details the Effective Security Rules (inbound and outbound) of the Network Interface card of a Virtual Machine

VPN Troubleshoot

KQL
Kusto Query Lang

LA workspace
= Data Lake

Subscription ⓘ
MSDN Platforms Subscription ▼

Resource group ⓘ
Demo ▼

Location ⓘ
East US ▼

*Storage account

<https://samcteusvmiagnostics.blob.core.windows.net/vpn> >

	Name	↑↓	Troubleshooting s...↑↓	Resource status	↑↓	Resource Group	↑↓	Location	↑↓
<input checked="" type="checkbox"/>	▼ vng01		Running	Succeeded		Demo		East US	
<input checked="" type="checkbox"/>	cn01		-	Succeeded		Demo		East US	

Helps you troubleshoot gateways and connections

Provides summary information and detailed information

Can troubleshoot multiple gateways or connections simultaneously

Packet Capture

Captures inbound and outbound traffic from a Virtual Machine

Saves data to a storage account, a local file, or both

Add packet capture

Subscription *
MSDN Platforms Subscription

Resource group *
Demo

Target virtual machine *
vm01

Packet capture name *
capture01

Capture configuration
The packet capture output file (.cap) can be stored in a storage account and/or on the target VM.

☒ Storage account ☐ File ☐ Both

Storage accounts *
samcteusvmdiagnosics

Maximum bytes per packet ⓘ
default: 0 (entire packet)

Maximum bytes per session ⓘ
default: 1073741824

Time limit (seconds) ⓘ
default: 18000

+ Add filter

Connection Troubleshoot *ping*

Check connectivity between source VM and destination

Identify configuration issues that are impacting reachability

Provide all possible hop by hop paths from the source to destination

Review hop by hop latency – min, max, and average between source and destination

View a graphical topology from your source to destination

Source

Subscription * ⓘ
MSDN Platforms Subscription

Resource group *
Demo

Source type *
Virtual machine

*Virtual machine
vm01

Destination
☐ Select a virtual machine ☒ Specify manually

URI, FQDN or IPv4 *
13.24.35.46 ✓

Probe Settings

Protocol ⓘ
☒ TCP ☐ ICMP

Destination port * ⓘ
3389 ✓

^ Advanced settings

Source port ⓘ
3389 ✓

Check

NSG Flow Logs




Metrics

Usage + quotas

Logs

NSG flow logs

Diagnostic logs

Name	Resource type	Resource group	Status	Location
 nsg01	Network security gro...	Demo	✔ Enabled	East US
 nsg02	Network security gro...	Demo	✔ Enabled	East US
 nsg03	Network security gro...	Demo	✔ Enabled	East US

View information about ingress and egress IP traffic through an NSG

Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis

The JSON format can be visually displayed in Power BI or third-party tools like Kibana

Traffic Analytics

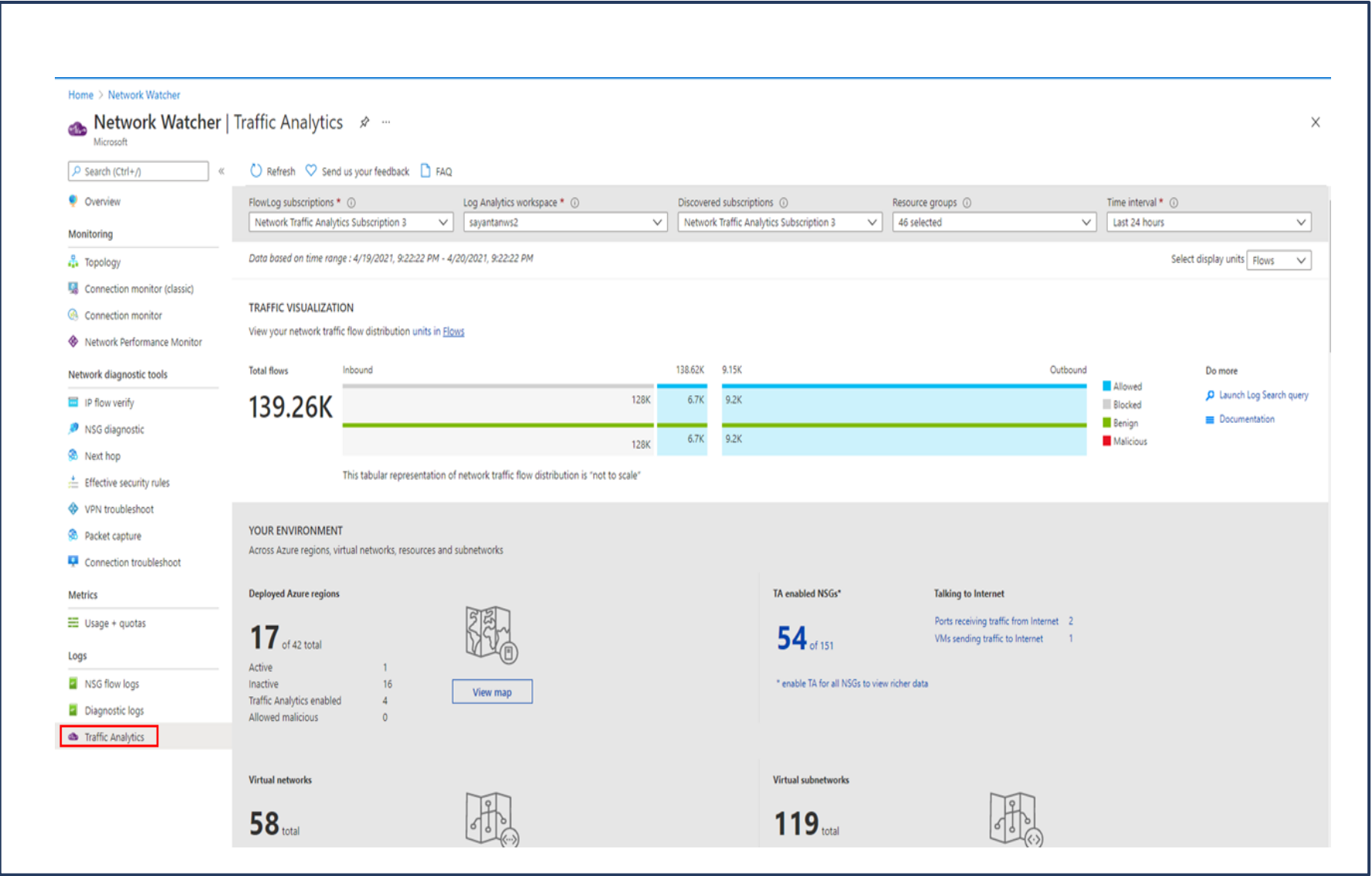
Network security group (NSG)

Network security group (NSG) flow logs

Log Analytics

Log Analytics workspace

Network Watcher



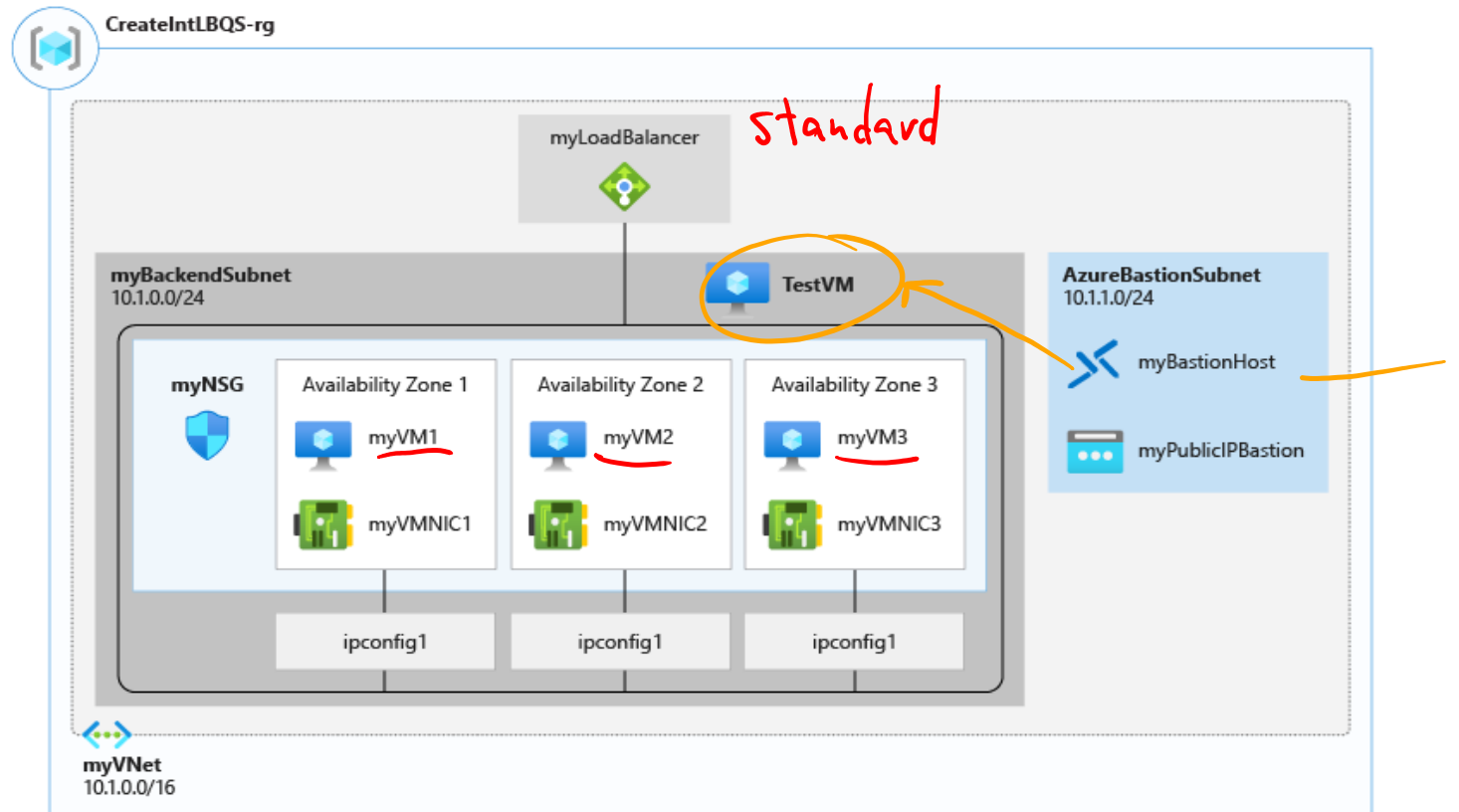
Exercise – Monitor a load balancer resource using Azure Monitor



Exercise: Monitor a load balancer resource using Azure Monitor



- Create an internal load balancer ✓
- Create a Log Analytics workspace ✓
- Use Azure Monitor Insights
- Configure the load balancer's diagnostic settings ✓



End of presentation

