Microsoft

AZ-801

Configure
Windows Server Hybrid
Advanced Services

Agenda AZ-801

1 Security – Windows Server
2 Security – Hybrid

3 Failover Cluster

4 Disaster Recovery – Windows Server
5 Disaster Recovery – Hybrid

6 Upgrade and Migrate – Windows Server
7 Migrate Windows Server to the Cloud

8 Monitoring – Windows Server
9 Monitoring – Hybrid

Monitor and troubleshoot Windows Server environment
(Implementing operational monitoring in hybrid scenarios)

- Monitor Windows Server Virtual Machines and hybrid instances

- Monitor your Azure virtual machines with Azure Monitor

- Troubleshoot Windows Server Virtual Machines in Azure

- Troubleshoot on-premises and hybrid networking

- Lab 09 – Implementing operational monitoring in hybrid scenarios

Monitor Windows Server Virtual Machines and hybrid instances

Learning Objectives – Monitor Windows Server VMs and hybrid instances

- Enable Azure Monitor for virtual machines and hybrid scenarios

- Demonstration – Monitor VMs with Azure Monitor

- Learning recap

What is Azure Monitor?

You can use Azure Monitor to optimize administration of your existing deployments and forecast capacity requirements for future deployments.

Three main capabilities
- Monitoring and metrics visualization
- Querying and analyzing logs
- Alerting and remediation

Azure Monitor delivers focused, in-depth monitoring capabilities through:
- Deep infrastructure monitoring.
- Deep application monitoring.

Enable Azure Monitor for VMs and hybrid scenarios (2 of 4)
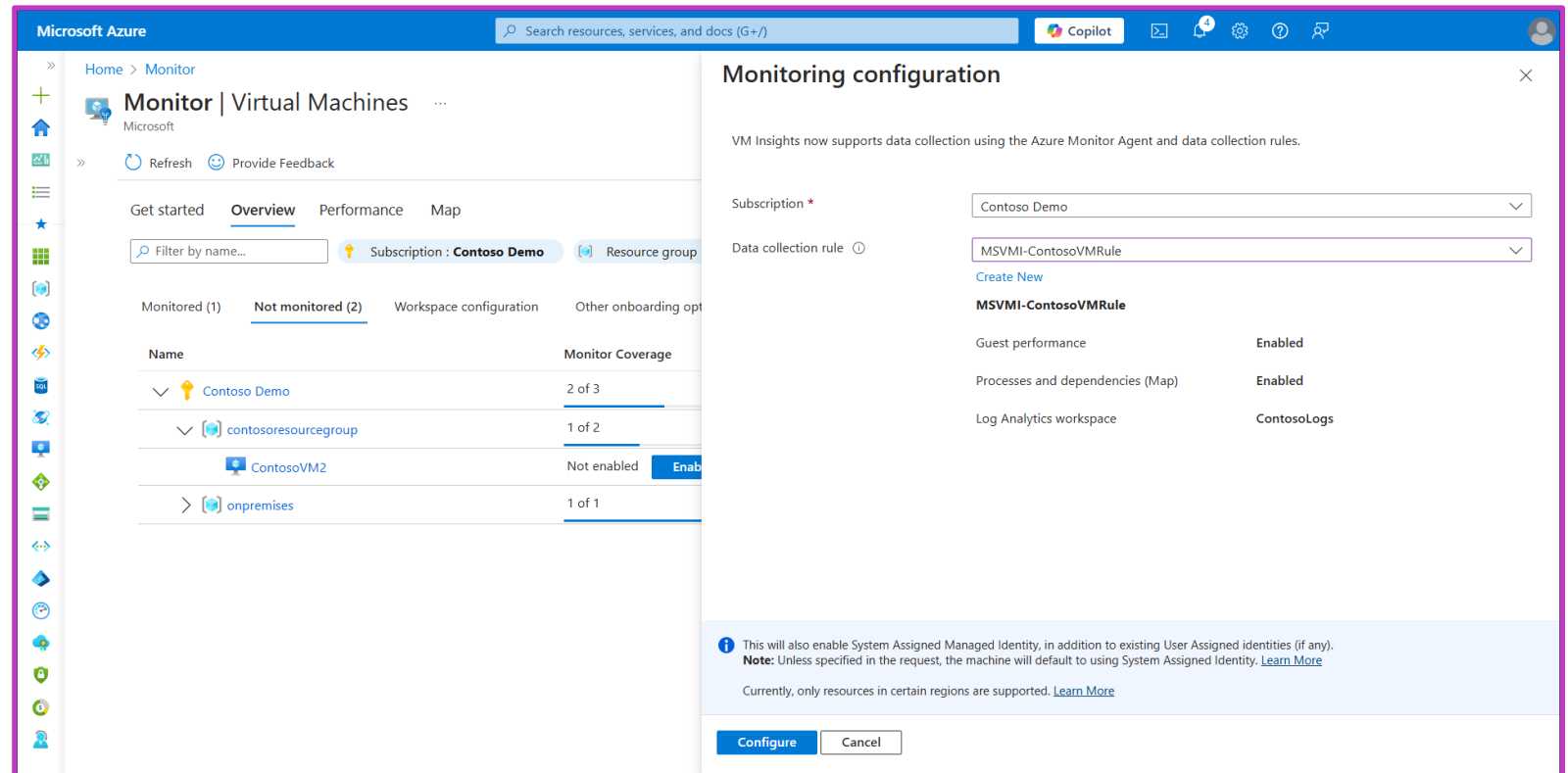
Monitor VMs

Azure Monitor for VMs enables you to monitor both:

- Azure VMs

- Hybrid VMs

Prerequisites:

- Log analytics

- Supported Windows operating systems

- ~~Dependency~~ Agent

- Security

- For hybrid, Azure Arc-enabled VMs

AMA

LA

Microsoft Azure — Search resources, services, and docs (G+/) — Copilot

Home > Monitor

Monitor | Virtual Machines
Microsoft

Refresh   Provide Feedback

Get started   **Overview**   Performance   Map

Filter by name...   Subscription : **Contoso Demo**   Resource group

Monitored (1)   **Not monitored (2)**   Workspace configuration   Other onboarding opt

Name	Monitor Coverage
Contoso Demo	2 of 3
contosoresourcegroup	1 of 2
ContosoVM2	Not enabled Enab
onpremises	1 of 1

Monitoring configuration

VM Insights now supports data collection using the Azure Monitor Agent and data collection rules.

Subscription *   Contoso Demo

Data collection rule ⓘ   MSVMI-ContosoVMRule
Create New

MSVMI-ContosoVMRule

Guest performance   Enabled

Processes and dependencies (Map)   Enabled

Log Analytics workspace   ContosoLogs

ⓘ This will also enable System Assigned Managed Identity, in addition to existing User Assigned identities (if any).
Note: Unless specified in the request, the machine will default to using System Assigned Identity. Learn More

Currently, only resources in certain regions are supported. Learn More

Configure   Cancel

Enable Azure Monitor for VMs and hybrid scenarios (3 of 4)

Review monitored data

After you have enabled Insights, you can monitor your VM. In the Azure portal, navigate to and select the appropriate VM. Then, under **Monitoring**, select **Insights**. This will open the **Map** tab for your VM.

You can also use the icons on the right of the Map to access the following information:

- PropertiesLog Events
- Log Events
- Alerts
- Connections
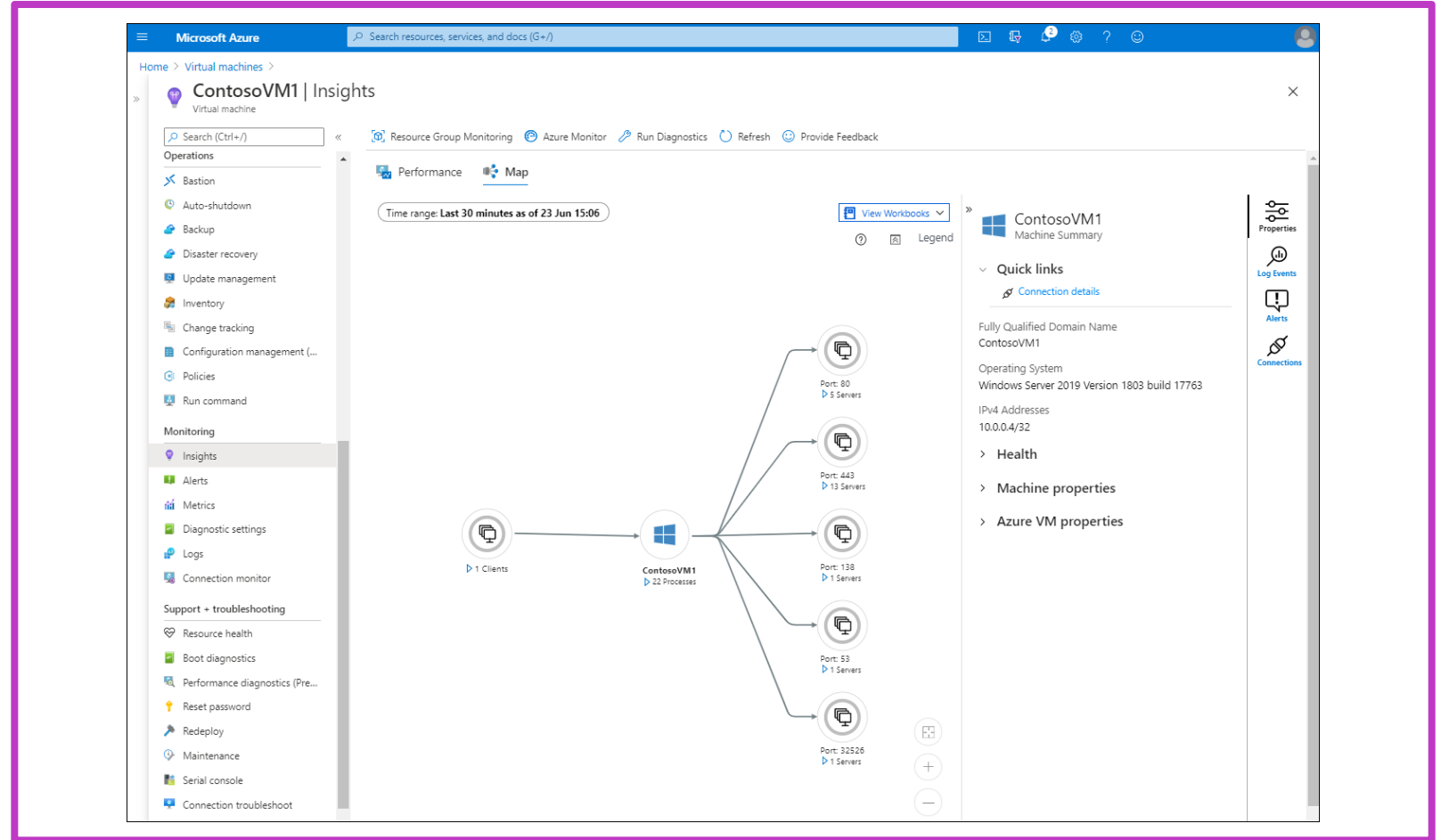
Enable Azure Monitor for VMs and hybrid scenarios (4 of 4)

To review performance data, select the Performance tab in Insights:

- CPU Utilization %

- Available Memory

- Logical disk IOPS

- Logical disk MB/s

- Max Logical Disk Used %

- Bytes Sent Rate

- Bytes Received Rate
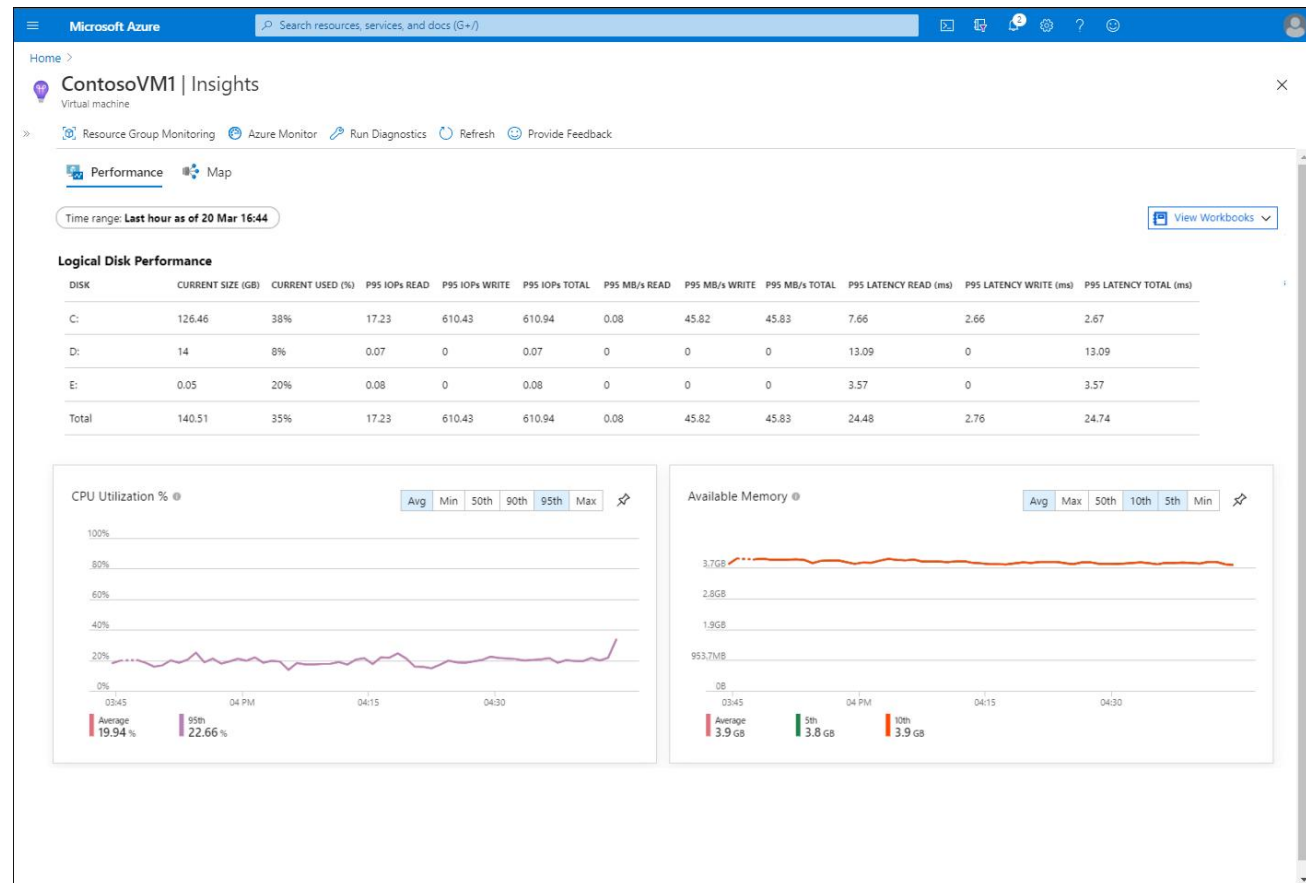
Enable Azure Monitor in hybrid scenarios

Azure Arc

You must onboard your on-premises VMs to Azure Arc before you can monitor them

Windows Admin Center

You can onboard your on-premises machines using the Azure Hybrid center in Windows Admin Center
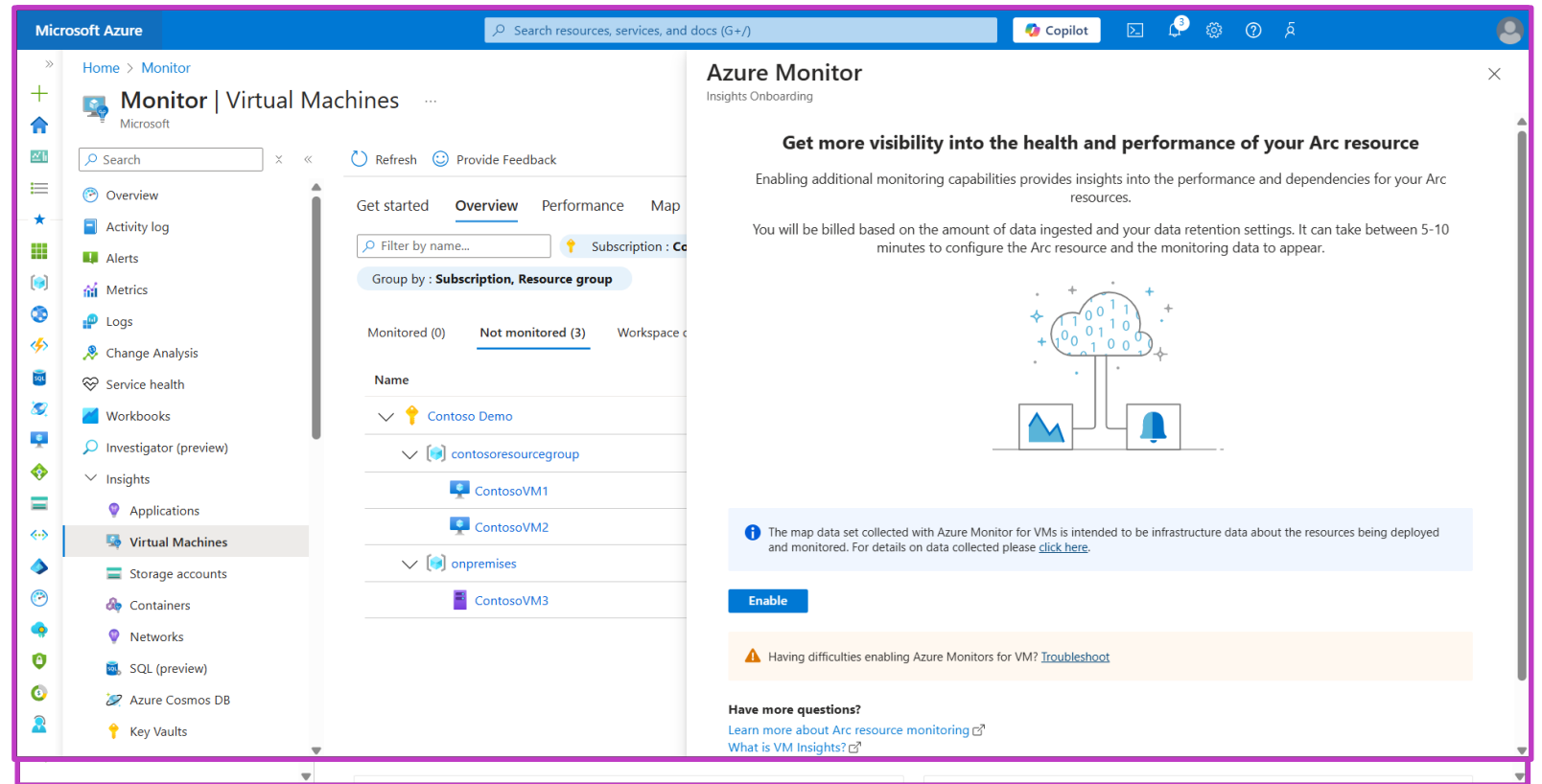
What are Azure Monitor Logs and Azure Monitor VM Insights? (1 of 2)

Definition of Azure Monitor Logs and Azure Monitor VM Insights:

- Azure Monitor Logs collects and organizes log data generated from Azure resources.

- Azure Monitor VM Insights provides a predefined, curated monitoring experience, with little configuration required.

What is the relationship between all the Azure native monitoring tools?

There are a few different resources and services that complete the native monitoring toolkit in Azure. Azure Monitor becomes the service at the top, which spans across all monitoring tools, while everything else lives underneath.

What are Azure Monitor Logs and Azure Monitor VM Insights? (2 of 2)

Plan a Log Analytics workspace deployment

- The right diagram provides more insight into all the different types of logs that can be ingested.

- The following Azure features help Log Analytics workspace adoption within enterprises.
  - Access mode
  - Access control mode
  - Table-level RBAC

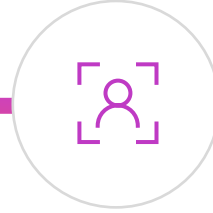**Azure collects compute monitoring data by using agents**

- The following lists each agent:
  - Azure Monitor Agent
  - Log Analytics agent
  - Dependency agent
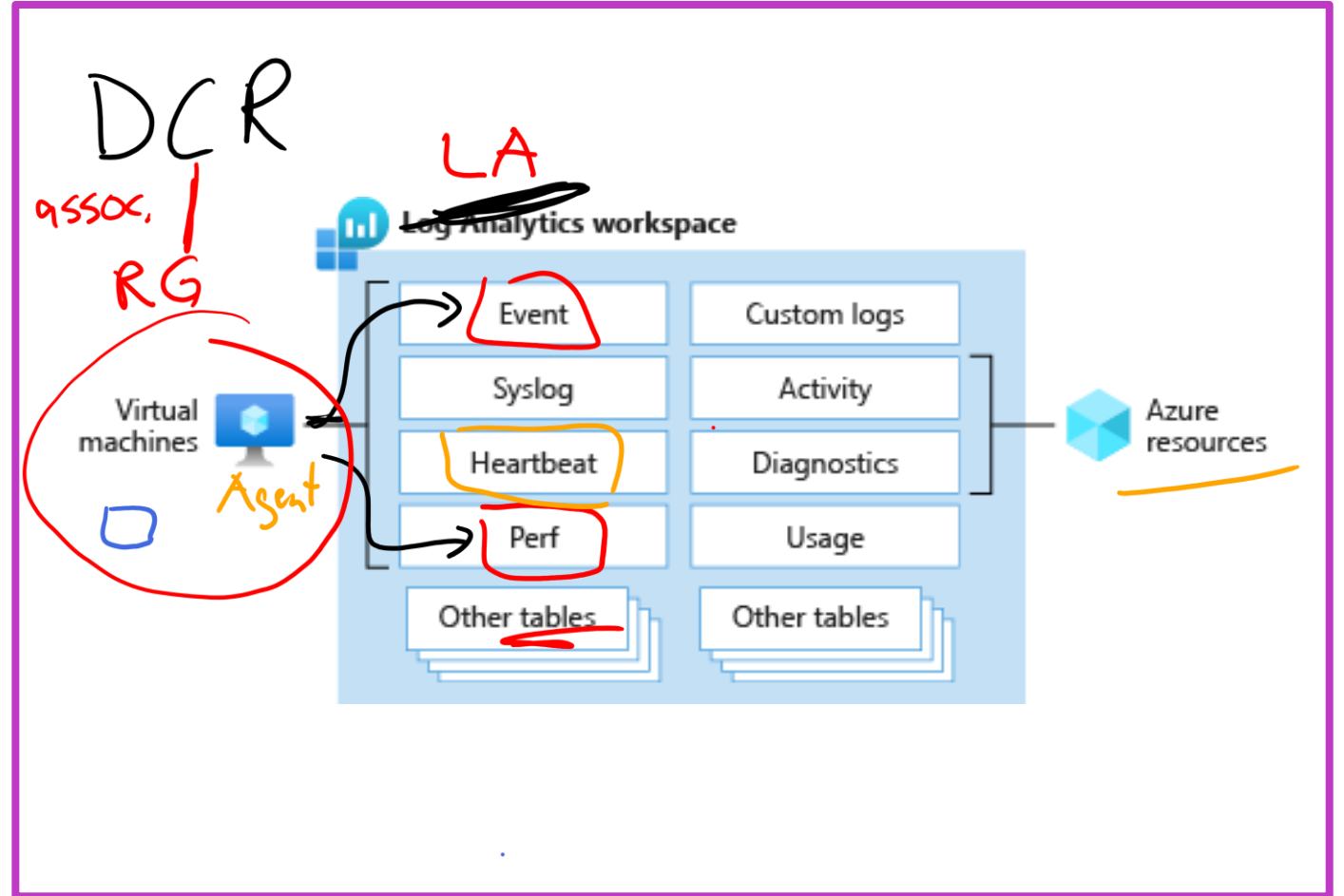
Demonstration – Monitor VMs with Azure Monitor

Enable Azure Monitor for VMs

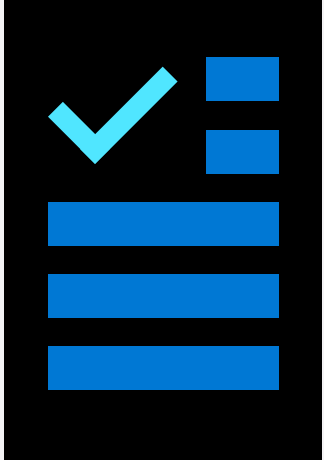**Configure a Log Analytics workspace**
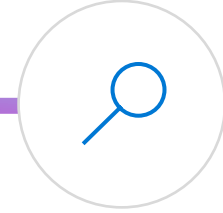
View collected data

Learning recap – Monitor Windows Server Virtual Machines and hybrid instances

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Monitor Windows Server Virtual Machines and hybrid instances

# Monitor your Azure virtual machines with Azure Monitor

Learning Objectives – Monitor your Azure virtual machines with Azure Monitor

- Monitor the health of the virtual machine

- Set up a VM with boot diagnostics

- View VM metrics

- Diagnostic data case studies

- Using diagnostic data

- Build log queries by using the Kusto Query Language

- Learning recap

Monitor the health of the virtual machine

- Basic metrics for Azure VMs

- View metrics

- Collect guest OS metrics

- Get boot diagnostics
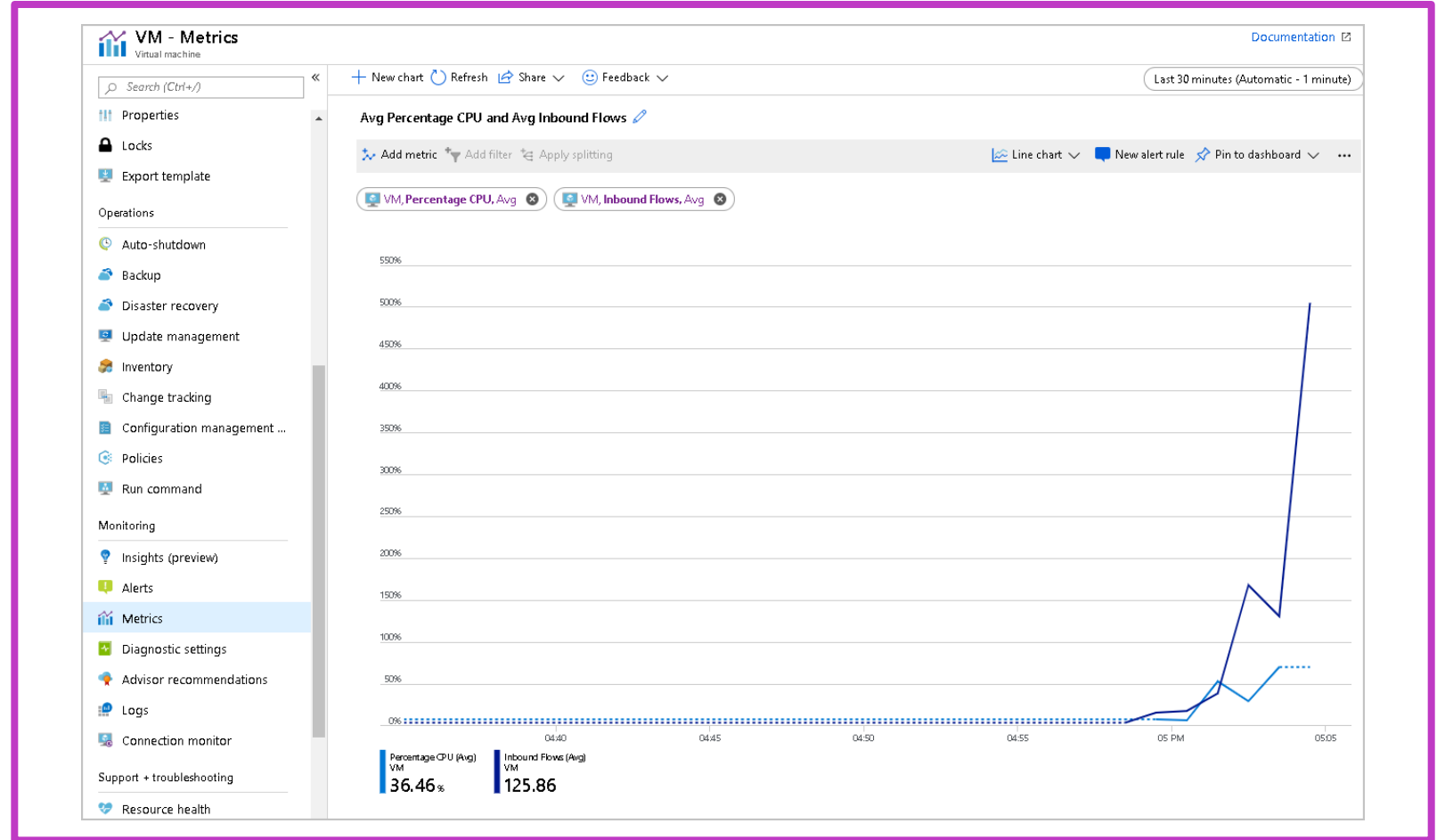
Demonstration - Set up a VM with boot diagnostics
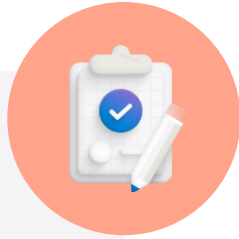
Task 1: Create a VM and enable recommended alerts
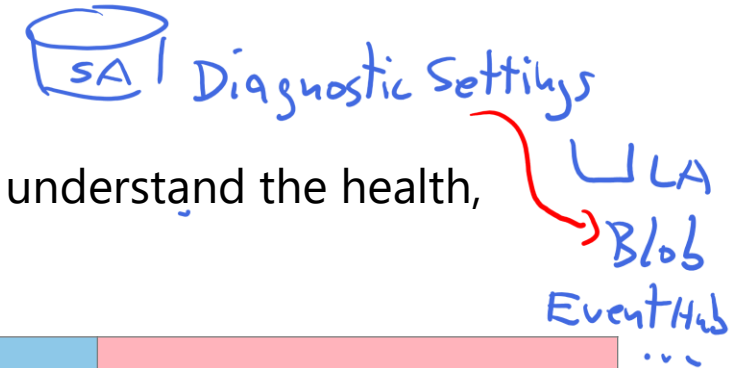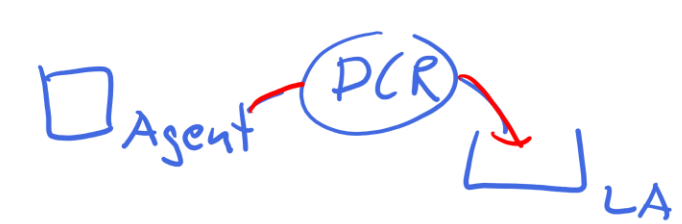
Task 2: View built-in metrics graphs

Task 3: View boot diagnostics

Metrics

Azure metrics are numerical values available from the Azure portal that help you understand the health, operation, and performance of your VMs.

Kind	CPU	OS Disk	Data Disk	Network
Metric	• CPU Credits Consumed [or Remaining] • Percentage CPU	• OS Disk Queue Depth • OS Disk Read [or Write] Bytes/Sec • OS Disk Read [or Write] Operations/Sec • Premium OS Disk Cache Read Hit [or Miss]	• Data Disk Queue Depth • Data Disk Read [or Write] Bytes/Sec • Data Disk Read [or Write] Operations/Sec • Premium Data Disk Cache Read Hit [or Miss]	• Inbound [or Outbound] Flows • Network In [or Out] Total

View VM metrics (2 of 3)

Overview graphs

- The Azure portal displays four graphs for your VM on the **Monitoring** tab of the **Overview** page.

- On the **Overview** page, you can also change the range of all the graphs.
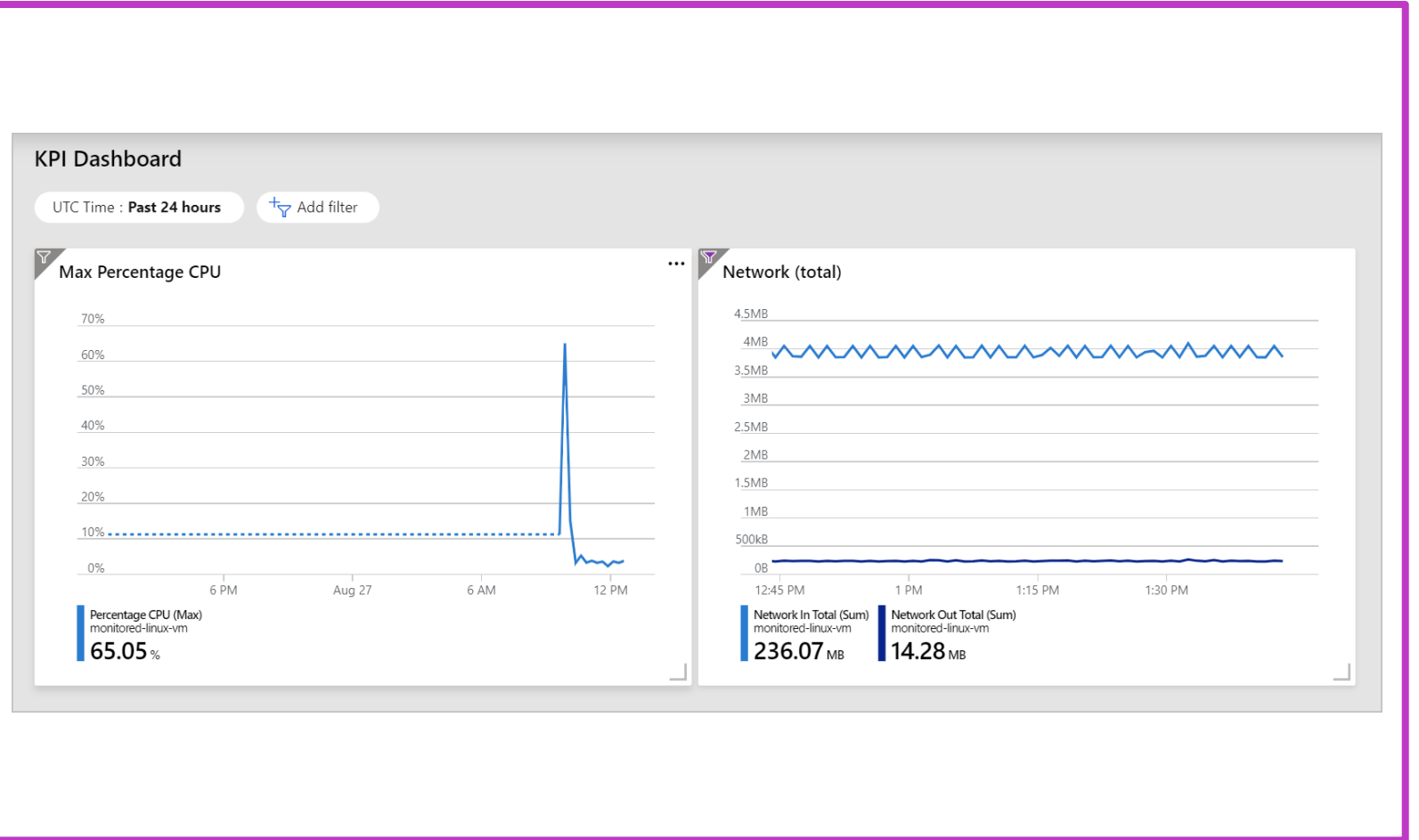
View VM metrics (3 of 3)

KPI dashboard

You can have greater control, with more options, by creating a custom key performance indicator (KPI) dashboard for your VM.

Two questions that you want to answer with graphs are:

- How hot is the VM or how much CPU is being used?
- How busy is the VM or how much network traffic is the VM processing?

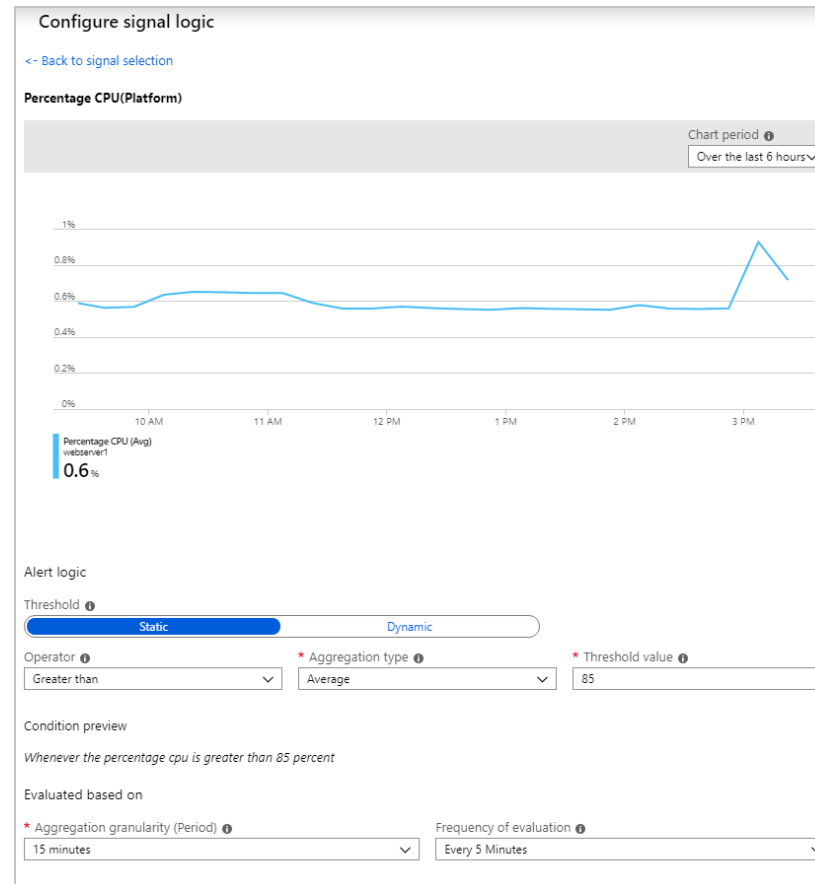# Diagnostic data case studies (1 of 3)

DDoS attack

1. To create a chart or alert for a DDoS attack, in the Azure portal, you go to **Monitor > Metrics.**

2. You then specify your public IP address as the resource to monitor and add DDoS metrics, including **Under DDoS attack or not.**

3. You then add an alert to be notified of an attack.
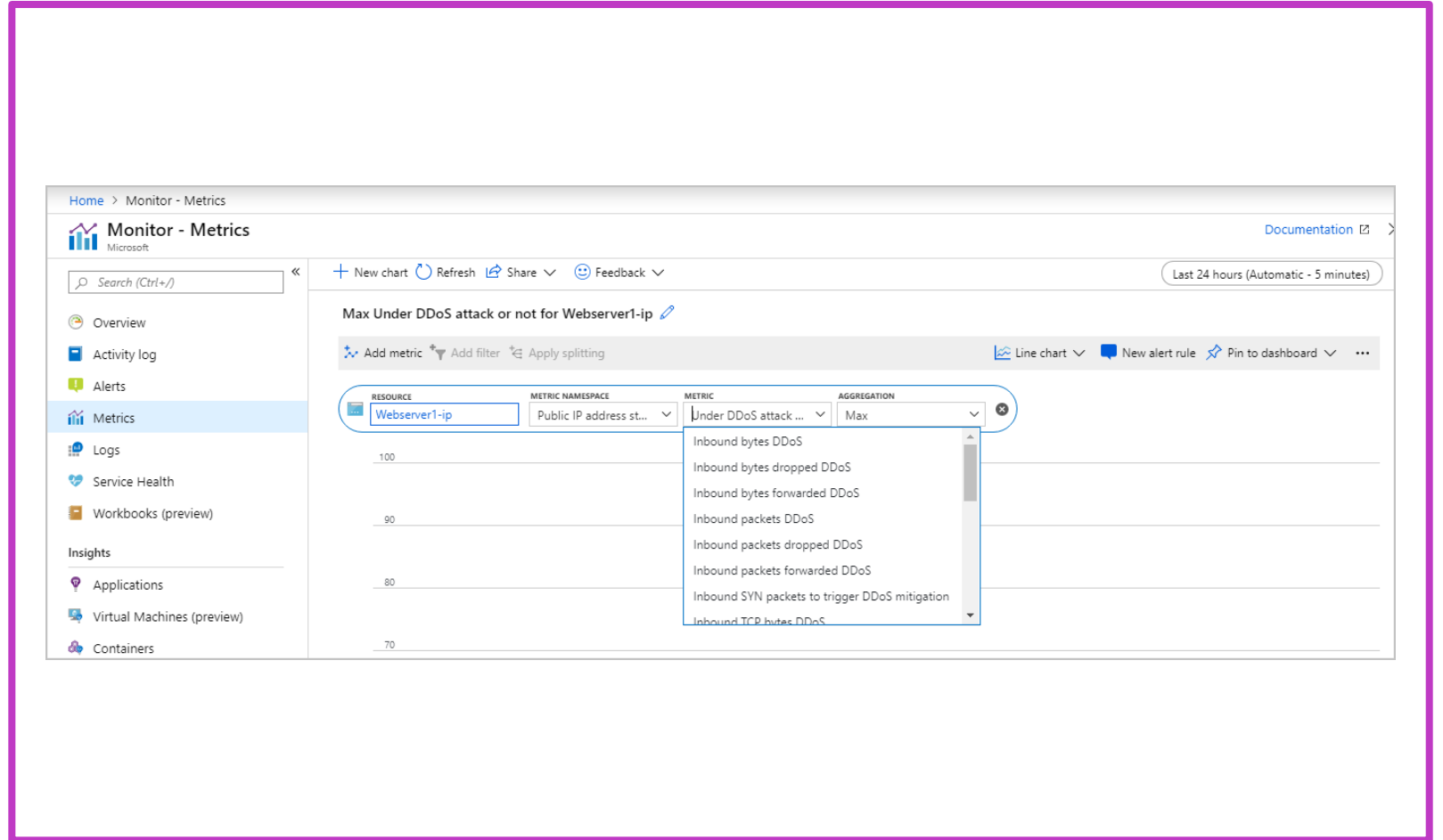
Diagnostic data case studies (2 of 3)

Increased CPU load

- Monitor CPU activity and memory availability to see if you need to scale up your web server.

- To respond to a high load, you can create an alert rule for the virtual machine with a condition for the CPU metric.

Diagnostic data case studies (3 of 3)

Action Groups allow for consolidated:

- Notifications:
  - Email/SMS/Push/Voice

- Action Types:
  - Automation Runbook
  - Azure Function
  - ITSM
  - Logic App
  - Webhook
  - Event Hub

Add action group

* Action group name ⓘ	Scale Up VM
* Short name ⓘ	Scaleup
* Subscription ⓘ	CM Azure Subscription
* Resource group ⓘ	Learn

Actions

ACTION NAME	ACTION TYPE
Email	Email Azure Resource Manager Role
ScaleUp_VM ✓	Automation Runbook ⌄

Build log queries by using the Kusto Query Language

Kusto syntax and operators

- At its core, a Kusto query is a read-only request.
- A query consists of references to actual tables and one or more query operators applied in sequence.
- Tabular operators will predominantly be the way you interact with and query monitoring data.

Understand the schema and schema pane

- The schema is a series of tables logically grouped together. The schema allows for an easy understanding behind how Log Analytics stores data

Write a new query

- Start with a table name is the right way to configure log queries.
- The KQL is case sensitive.

Basic query understanding

- One of the tables captured by Azure Monitor is the Heartbeat table. This table contains a number of useful columns. Run a query with only Heartbeat to see what makes up this table.

Troubleshoot Windows Server Virtual Machines in Azure

Learning Objectives – Troubleshoot Windows Server Virtual Machines in Azure

- Troubleshoot VM deployment

- Troubleshoot VM startup

- Troubleshoot VM connectivity

- Optimize VM network connectivity security with Azure Bastion

- Troubleshoot VM performance

- Troubleshoot VM storage

- Learning recap

Troubleshoot VM deployment

Understand provisioning failures

- Resolve upload errors

  To resolve errors in Windows generalized & Windows specialized that result during upload,

  - Use Add-AzVhd to upload the original VHD

- Resolve capture errors

  To resolve errors in Windows generalized & Windows specialized that result during capture:

  - Delete the current image from the portal.

  - Recapture it from the current VHDs with the same setting as that for the operating system (generalized/specialized).

Understand allocation failures

- Resolve VM size allocation failures error

- Resolve VM resource allocation failures error

Troubleshoot VM startup

Tools that can be used to identify the causes

- Boot diagnostics
  - Very useful in determining the specific cause of a startup problem in your Windows Server VM

- Azure Serial Console
  - Your VM must have been configured to use the option **Enable with custom storage account** for the Boot diagnostics setting

Common boot errors

- BitLocker errors

- Blue screen errors

- CRITICAL SERVICE FAILED errors
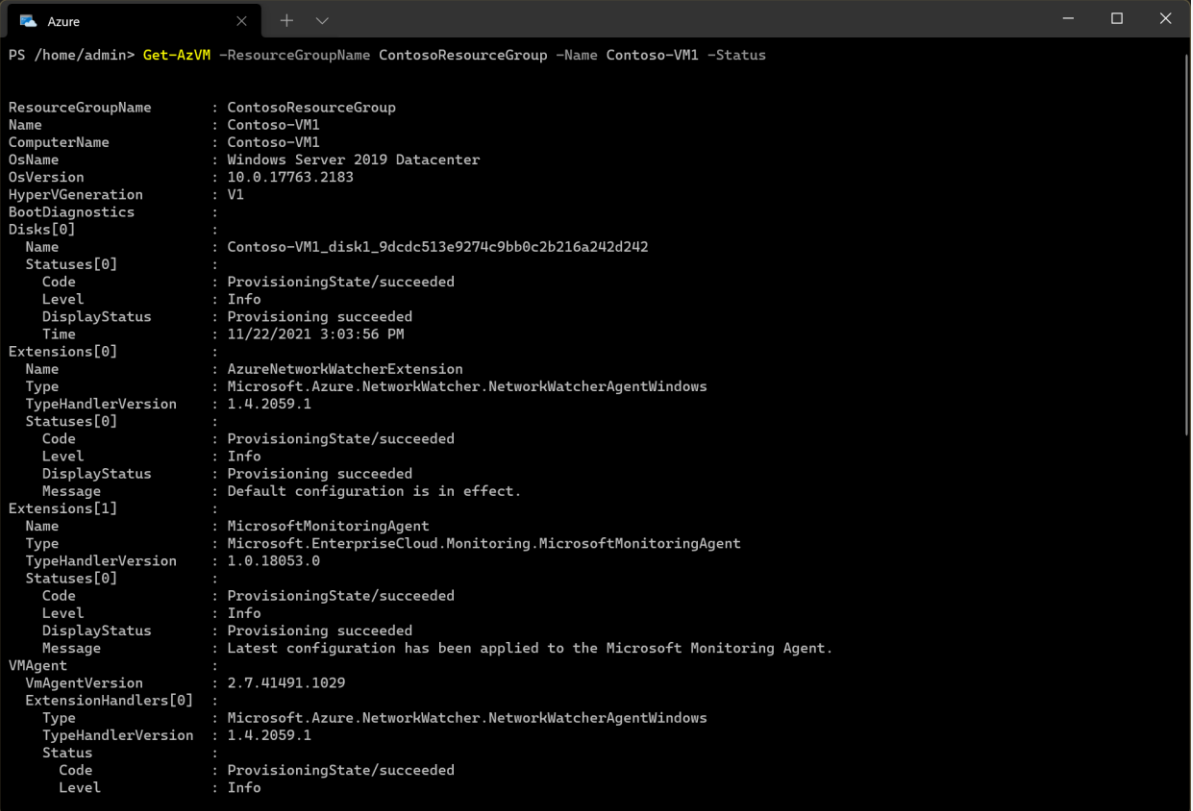
- Stuck at Windows Update

Troubleshoot VM extensions

Review extension status

- You can check the VM Agent status and the status of any installed extensions by using the `get-AzVM PowerShell cmdlet`

- You can get specific details about a particular extension by using the following PowerShell command: `Get-AzVMExtension -ResourceGroupName $RGName -VMName $vmName -Name $ExtensionName`

Review extension logs

- Extension logs reside in the C:\WindowsAzure\Logs\Plugins folder.

- Extension settings and status files reside in the C:\Packages\Plugins folder.


```
Azure

PS /home/admin> Get-AzVM -ResourceGroupName ContosoResourceGroup -Name Contoso-VM1 -Status

ResourceGroupName       : ContosoResourceGroup
Name                    : Contoso-VM1
ComputerName            : Contoso-VM1
OsName                  : Windows Server 2019 Datacenter
OsVersion               : 10.0.17763.2183
HyperVGeneration        : V1
BootDiagnostics         :
Disks[0]                :
  Name                  : Contoso-VM1_disk1_9dcdc513e9274c9bb0c2b216a242d242
  Statuses[0]           :
    Code                : ProvisioningState/succeeded
    Level               : Info
    DisplayStatus       : Provisioning succeeded
    Time                : 11/22/2021 3:03:56 PM
Extensions[0]           :
  Name                  : AzureNetworkWatcherExtension
  Type                  : Microsoft.Azure.NetworkWatcher.NetworkWatcherAgentWindows
  TypeHandlerVersion    : 1.4.2059.1
  Statuses[0]           :
    Code                : ProvisioningState/succeeded
    Level               : Info
    DisplayStatus       : Provisioning succeeded
    Message             : Default configuration is in effect.
Extensions[1]           :
  Name                  : MicrosoftMonitoringAgent
  Type                  : Microsoft.EnterpriseCloud.Monitoring.MicrosoftMonitoringAgent
  TypeHandlerVersion    : 1.0.18053.0
  Statuses[0]           :
    Code                : ProvisioningState/succeeded
    Level               : Info
    DisplayStatus       : Provisioning succeeded
    Message             : Latest configuration has been applied to the Microsoft Monitoring Agent.
VMAgent                 :
  VmAgentVersion        : 2.7.41491.1029
  ExtensionHandlers[0]  :
    Type                : Microsoft.Azure.NetworkWatcher.NetworkWatcherAgentWindows
    TypeHandlerVersion  : 1.4.2059.1
    Status              :
      Code              : ProvisioningState/succeeded
      Level             : Info
```

Troubleshoot VM connectivity

Test connectivity

If you're experiencing connection issues, test the connection. Open the Azure portal and use the following procedure:

1. Navigate to the VM you want to connect to.

2. Select Connect in the Settings section of the navigation pane.

3. Review, and if necessary, update the settings for RDP.

4. Select the Test your connection link.

5. Select RDP in the Service list, and then select Test connection.

Validate network/network security

If this basic connectivity test is successful, then attempt to reconnect using the recorded details. If you're unsuccessful, then consider the following:

- Verify that RDP is a supported connection type for this VM. Should you be using Azure Bastion, for example?

- Check any Network Security Group rules to ensure that they're not blocking the RDP traffic:

- If traffic is permitted, then consider resetting the virtual machine's NIC.

- If that doesn't resolve the issue, if possible, restart the VM itself.

Optimize VM network connectivity security with Azure Bastion

Consider implementing Azure Bastion

- Securely connect to your Azure VMs remotely, without needing to expose remote administrative ports to the internet

- Bastion host servers:
  - Are designed and configured to withstand attacks.
  - Provide RDP and SSH connectivity to your Azure workloads behind the bastion.

The following diagram displays the architecture of a typical Azure Bastion deployment

- The bastion host is deployed in the Azure virtual network.

- A user connects to the Azure portal using any HTML5 browser over TLS.

- The user selects the VM to connect to.

- The Bastion host establishes the RDP/SSH connection to the target VM.
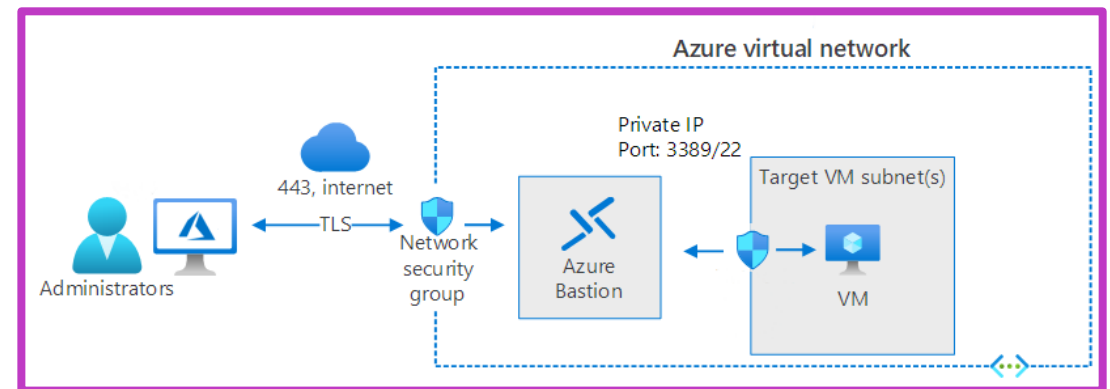
Troubleshoot VM performance

What resources should you monitor?

- Memory

- Processor

- Disk

- Network

What tools are available for performance monitoring?

- Performance Monitor

- Windows Admin Center

- System Insights

- VM diagnostics

- VM performance diagnostics.

Troubleshoot VM storage (1 of 2)

Differences between Premium Storage and Standard Storage

- Premium Storage offers superior performance, equivalent to what SSD technology provides.

- Standard Storage provides performance similar to commodity magnetic disks, referred to typically as hard disk drives (HDD).

- All Azure VM sizes support Standard Storage. Many Azure VM sizes also support Premium Storage.
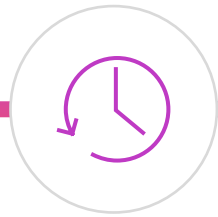
Unmanaged and managed disks

- The use of **unmanaged disks** involves potentially significant administrative overhead.

- You can eliminate this administrative overhead by using **managed disks.**

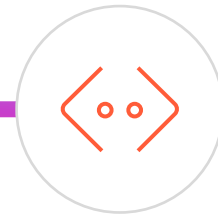# Troubleshoot VM storage (2 of 2)
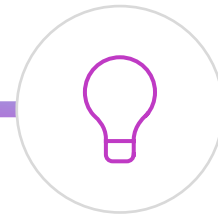
Common storage issues include:
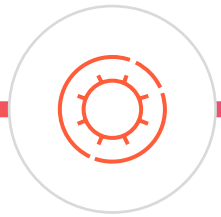
Cannot extend an encrypted OS volume in Windows

Errors when deleting storage resources

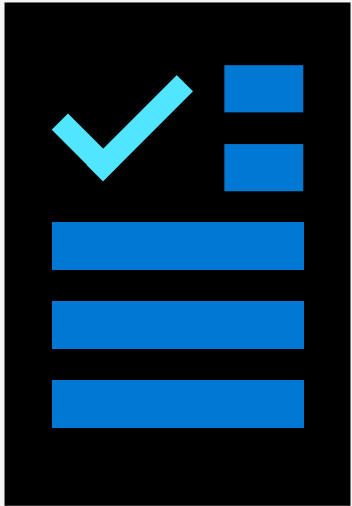Your VHD is not supported when you create a VM in Azure

Azure disk encryption issues

Learning recap – Troubleshoot Windows Server Virtual Machines in Azure

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Troubleshoot Windows Server Virtual Machines in Azure

Troubleshoot on-premises and hybrid networking

Learning Objectives – Troubleshoot on-premises and hybrid networking

- Diagnose DHCP problems

- Diagnose DNS problems

- Diagnose IP configuration issues

- Diagnose routing problems

- Use Packet Monitor to help diagnose network problems

- Use Azure Network Watcher to help diagnose network problems

- Learning recap

Diagnose DHCP problems

Vint Cerf 2^{32} Public IP

vNet
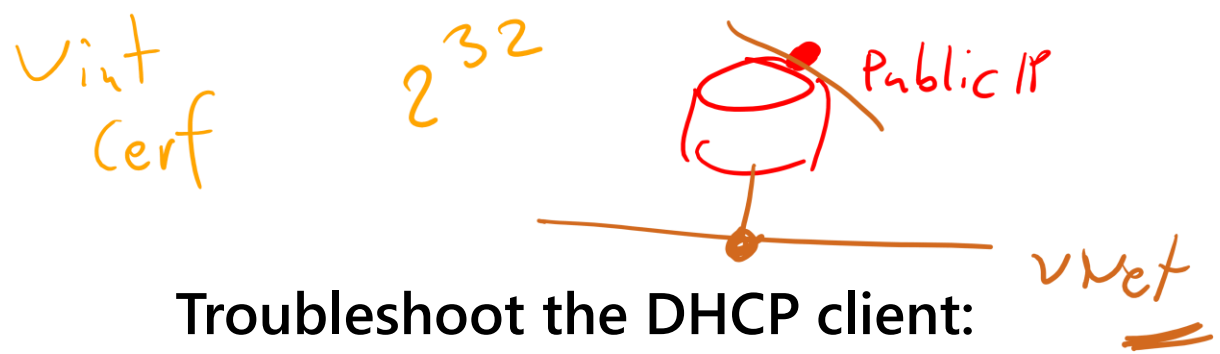
Troubleshoot the DHCP server role:

If you're experiencing problems that you think relate to DHCP, you should:

- The administration of identity systems
- Ensure that the DHCP server is authorized in AD DS
- Verify that the DHCP server service is running
- Check that there are addresses available in the DHCP server scope for the appropriate subnet
- Ensure that there are no devices with static IP addresses that haven't been excluded from your scopes
- Check that any required DHCP relays are operational for subnets without a DHCP server
- Ensure that no other services are listening on UDP 67 and 68.
- Review any DHCP policies and filters
- Examine DHCP-related logs

Troubleshoot the DHCP client:

If you think the issue lies with the client, then you should:

- Dedicated hardware
- Verify cabling
- Check that the network adapter is not disabled
- Consider updating the NIC driver, or, if recently updated, consider rolling back the driver
- Ensure that the DHCP Client service is running
- Verify that no firewall is blocking UDP ports 67 and 68

Diagnose DNS problems (1 of 2)

Check the fundamentals

- Cmdlets are the fundamental components of commands.
- Verify that the DNS server service is running.
- Check the event logs for errors recorded that relate to DNS.
- Determine whether an incorrect response is from an authoritative server.
- If the server is not authoritative, then the problem might be caused by synchronization (zone transfer) problems from the configured master.

Review DNS server logs

- By default, DNS maintains a DNS server log, which you can view in the Event Viewer.

Configure DNS logging

- For more verbose logging, you can enable debug logging.

Diagnose DNS problems (2 of 2)

What are the tools and techniques for troubleshooting name resolution?

Tools:

- Nslookup
- DNSCmd
- DNSlint
- IPConfig

Cmdlets that you can use for DNS client and server management:

- Clear-DNSClientCache
- Get-DNSClient
- Get-DNSClientCache
- Register-DNSClient
- Resolve-DNSName
- Set-DNSClient
- Test-DNSServer

DNSSec

Diagnose IP configuration issues

What are the stages of an IP troubleshooting methodology?

- Identify the scope of the problem.
- Take a logical approach to analyze problems.
- Determine which tools you will need to use to resolve the issue in a timely fashion.

What are the tools and techniques for troubleshooting IP configuration?

- Tools and cmdlets
  - Resource Monitor.
  - Network Diagnostics
  - Event Viewer.

- IPConfig
- Ping
- Tracert
- Pathping
- Route
- Telnet
- Netstat
- Get-NetIPv4Protocol
- Get-NetIPAddress
- Get-NetRoute
- Get-NetConnectionProfile
- Test-Connection
- Test-NetConnection

Diagnose routing problems

What do routers do?

When a router receives traffic destined for an endpoint outside of the local network, it checks to determine whether it has a route to the destination network. Then:

1. If the route exists, the router forwards the packet to the destination network router address.

2. If a route does not exist, the router sends the traffic to the router's default gateway or default route.

What are routing tables?

Routing tables contain the following information about a route for a specific interface:

1. Network destination.

2. Netmask.

3. Gateway.

4. Interface.

5. Metric.

Several ways to review and modify routing tables

- Use Windows PowerShell

- Use the route command

Get - Net Route

Use Packet Monitor to help diagnose network problems

wireshark

What is Packet Monitor?

- Packet Monitor can intercept network packets at various points in the network stack.

Capabilities of Packet Monitor :

- Packet monitoring and counting at multiple locations within the network stack

- Detection of packets drop throughout various levels in the stack

- Flexible runtime packet filtering with encapsulation support

- General logging and tracing support

- TXT log analysis based on TcpDump packet parsing

- Multiple logging modes, including: real-time, high volume in-memory, multi-file, circular

- Support for ethernet, Wi-Fi, and mobile broadband media types

Use the following procedure to capture and analyze packets with Pktmon.exe:

- Choose the types of packets you want to capture. Select by IP address, ports, protocols and so on.

- Apply capture filters based on your requirements: pktmon filter add <filters>

- Start the capture and enable packet logging: pktmon start –c

- Reproduce the network-related problem you're having.

- Check the counters to verify presence of required traffic: pktmon counters

- Stop the capture: `pktmon stop'.

- Retrieve the logs in a suitable format: pktmon etl2txt <filename>

Use Azure Network Watcher to help diagnose network problems

What is Azure Network Watcher?

- Azure Network Watcher provides tools to monitor, view, diagnose, review metrics, and enable or disable logs for resources in an Azure virtual network

## Diagnostics capabilities of Network Watcher:

- Diagnose network traffic filtering problems
- Diagnose network routing problems
- Diagnose outbound connections from a VM
- Capture packets
- Diagnose problems with an Azure Virtual network gateway and connections
- Determine relative latencies
- View security rules
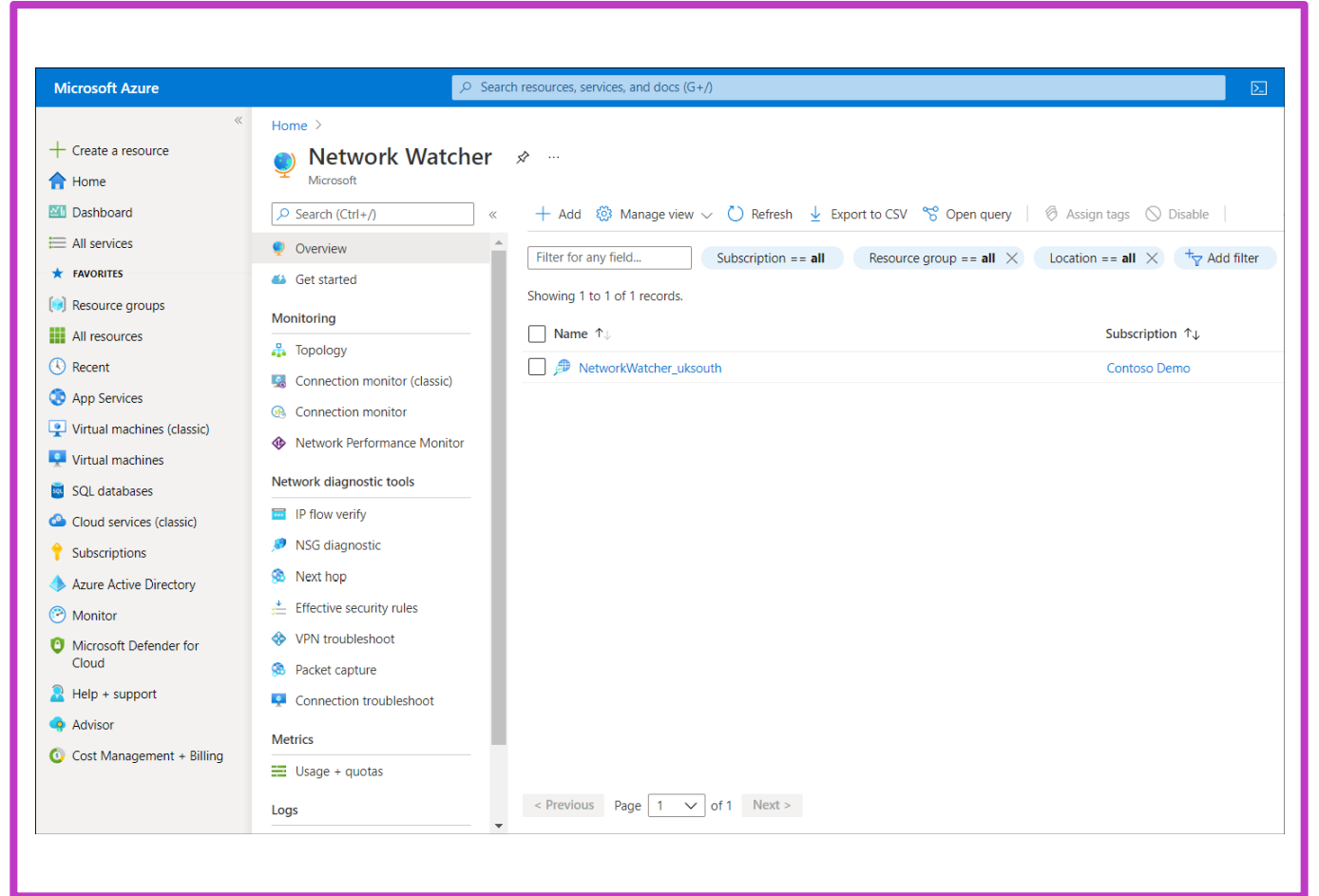
Learning recap – Troubleshoot on-premises and hybrid networking

Knowledge Check
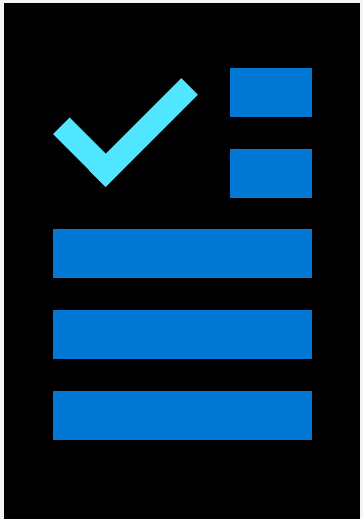
Microsoft Learn Modules (learn.microsoft.com/)

Troubleshoot on-premises and hybrid networking

Lab 09: Implementing operational monitoring in hybrid scenarios

Lab 09 – Implementing operational monitoring in hybrid scenarios

Lab scenario

You need to evaluate Microsoft Azure functionality that would provide insight into the performance and configuration of Azure resources, focusing in particular on Azure virtual machines (VMs). To accomplish this, you intend to examine the capabilities of Azure Monitor, including Log Analytics.

Objectives

- Prepare a monitoring environment
- Configure monitoring of on-premises servers
- Configure monitoring of Azure VMs
- Evaluate monitoring services

End of presentation