Microsoft Azure

AZ-104T00A Module 11: Monitoring

Module Overview

Lesson 01: Azure Monitor

Lesson 02: Azure Alerts

Lesson 03: Log Analytics

Lesson 04: Network Watcher

Lesson 05: Module 11 Lab and Review

Lesson 01: Azure Monitor

Azure Monitor Overview

- Azure Monitor Service
- Key Capabilities
- Monitoring Data Platform
- Log Data
- Data Types
- Activity Log
- Query the Activity Log

Key Capabilities

Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

Explore Metrics

Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

Search Logs

Setup Alert & Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

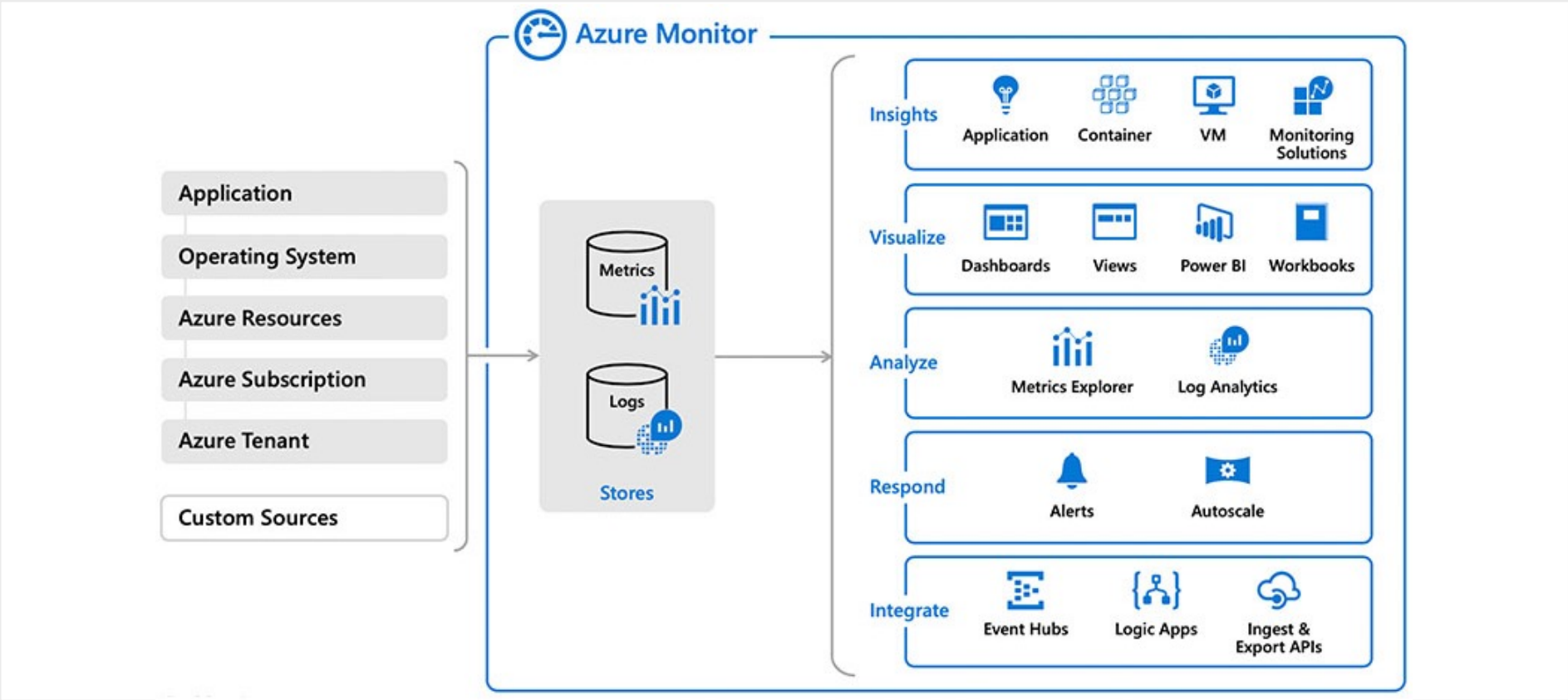
Create Alert

Core monitoring for Azure services

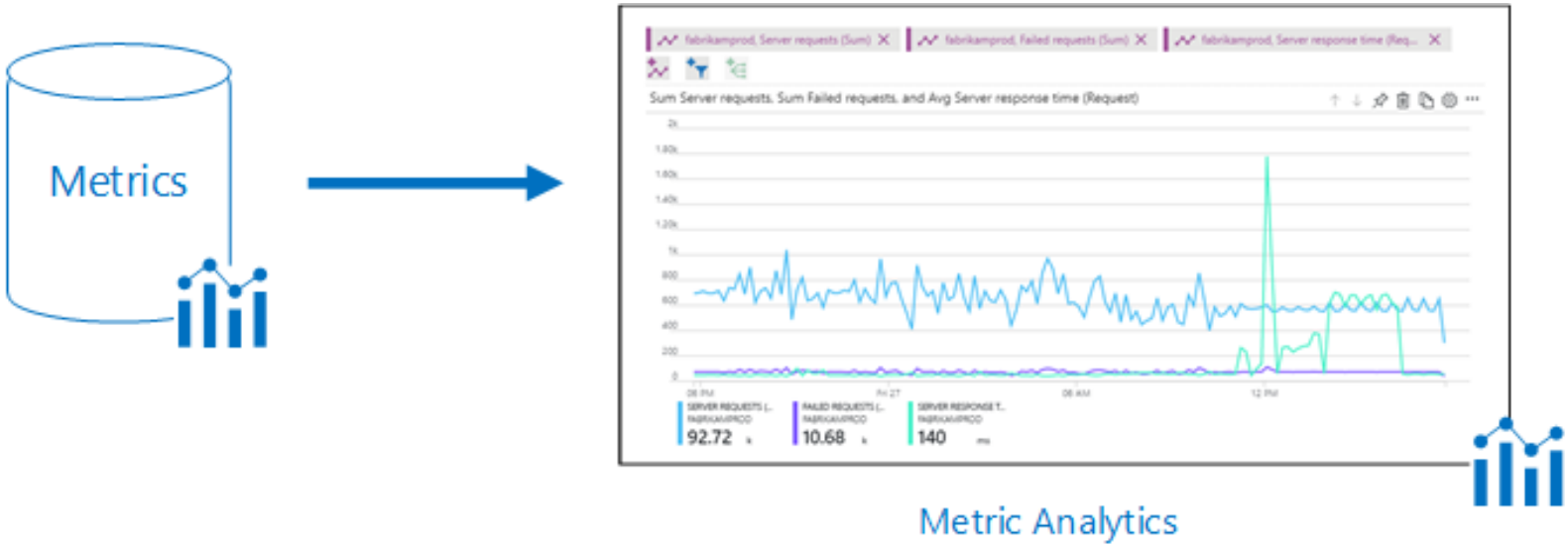
Collects metrics, activity logs, and diagnostic logs

Use for time critical alerts and notifications

Azure Monitor Service



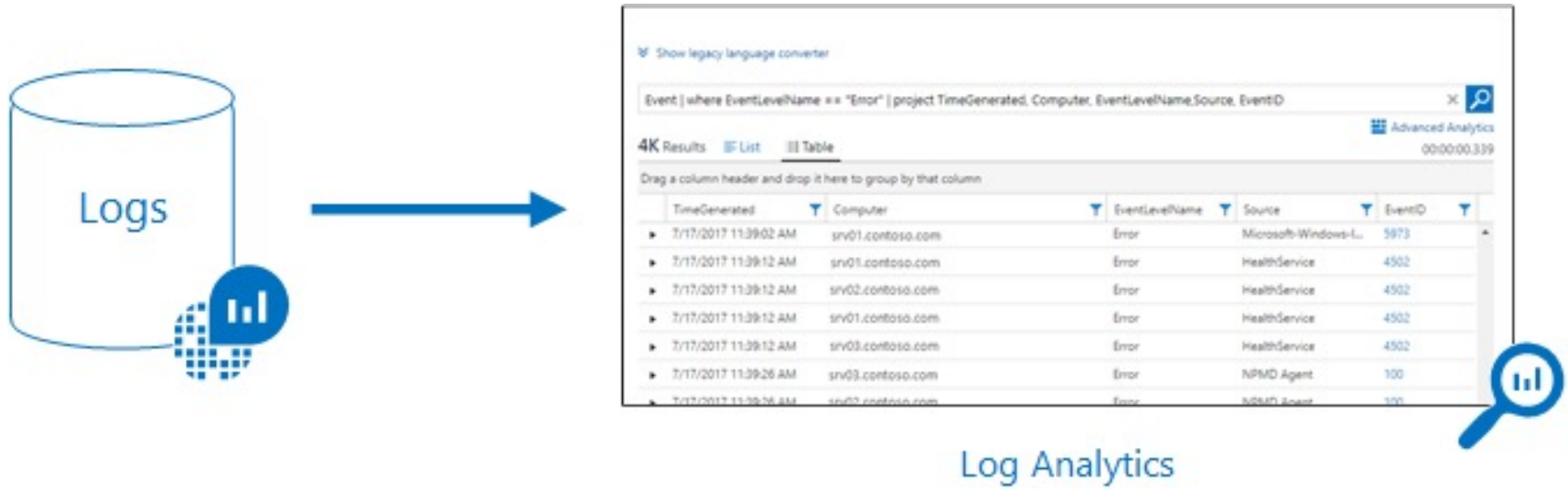
Monitoring Data Platform



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 such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis

Log Data



Log data is stored in Log Analytics which includes a rich query language to quickly retrieve, consolidate, and analyze collected data

The Data Explorer query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics

Data Types

Application monitoring data – Performance and functionality of the code you have written, regardless of its platform

Guest OS monitoring – Azure, another cloud, or on-premises

Azure resource monitoring

Azure subscription monitoring – Operation and management of an Azure subscription, as well as data about the health and operation of Azure itself

Azure tenant monitoring – Operation of tenant-level Azure services, such as Azure Active Directory

Activity Log

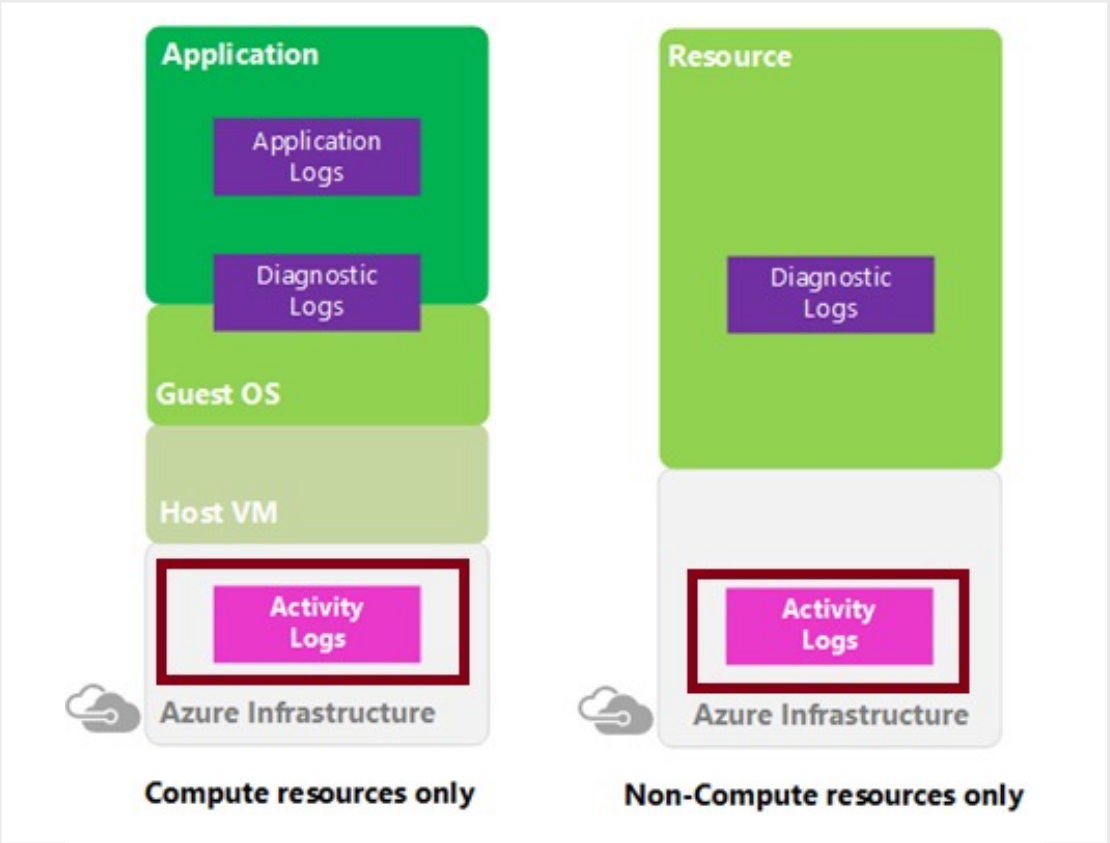
Send data to Log Analytics for advanced search and alerts

Query or manage events in the Portal, PowerShell, CLI, and REST API

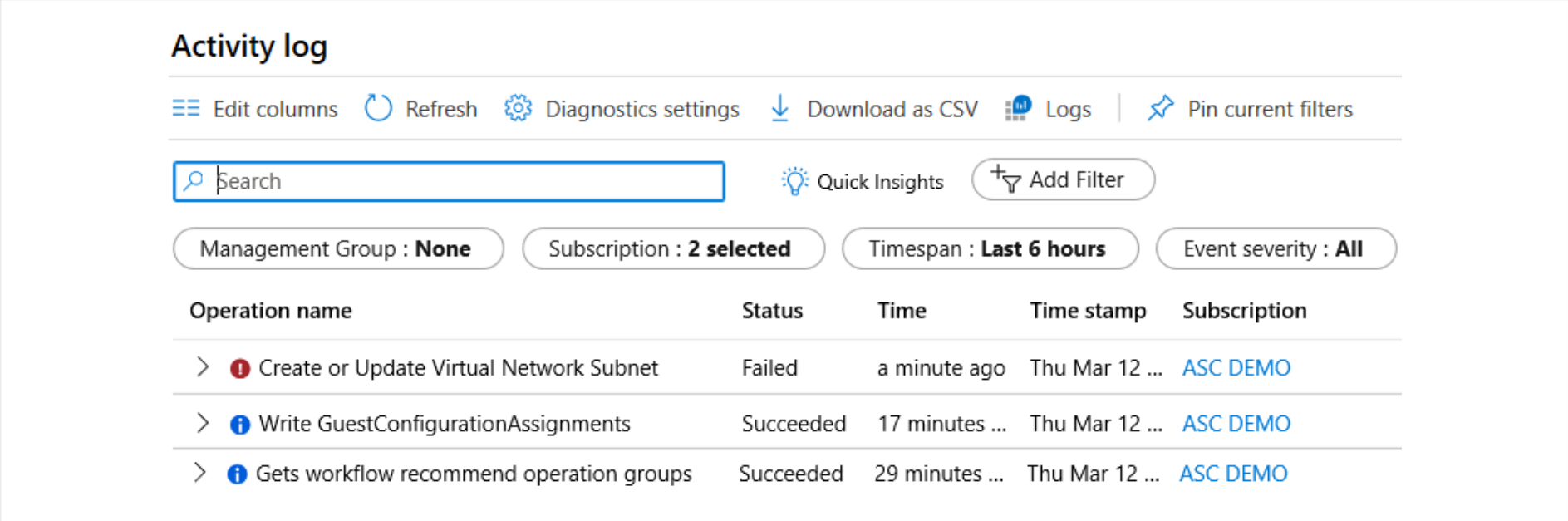
Stream information to Event Hub

Archive data to a storage account

Analyze data with Power BI



Query the Activity Log

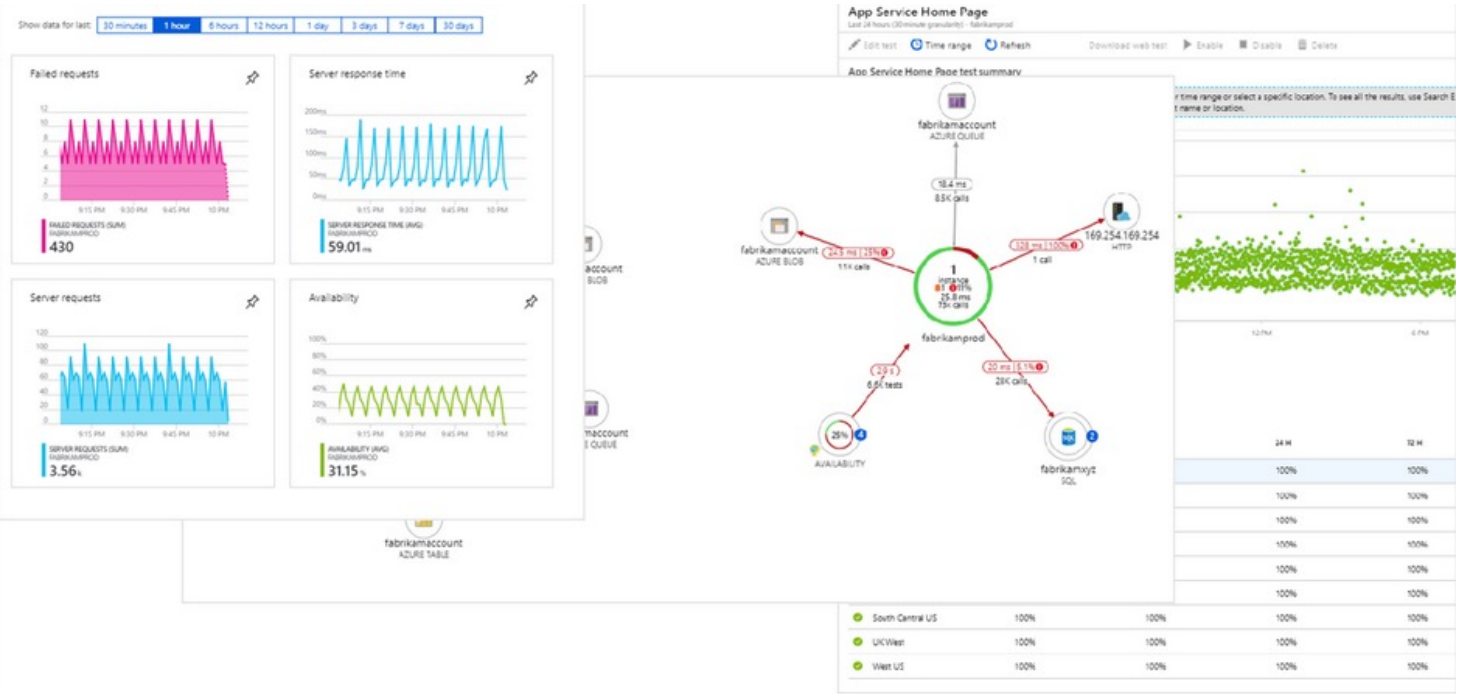


Filter by Management group, Subscription, Timespan, and Event Severity

Add a filter, like Event Category (Security, Recommendations, Alerts)

Pin current filters and download as CSV

Application Insights



Lesson 02: Azure Alerts

Azure Alerts Overview

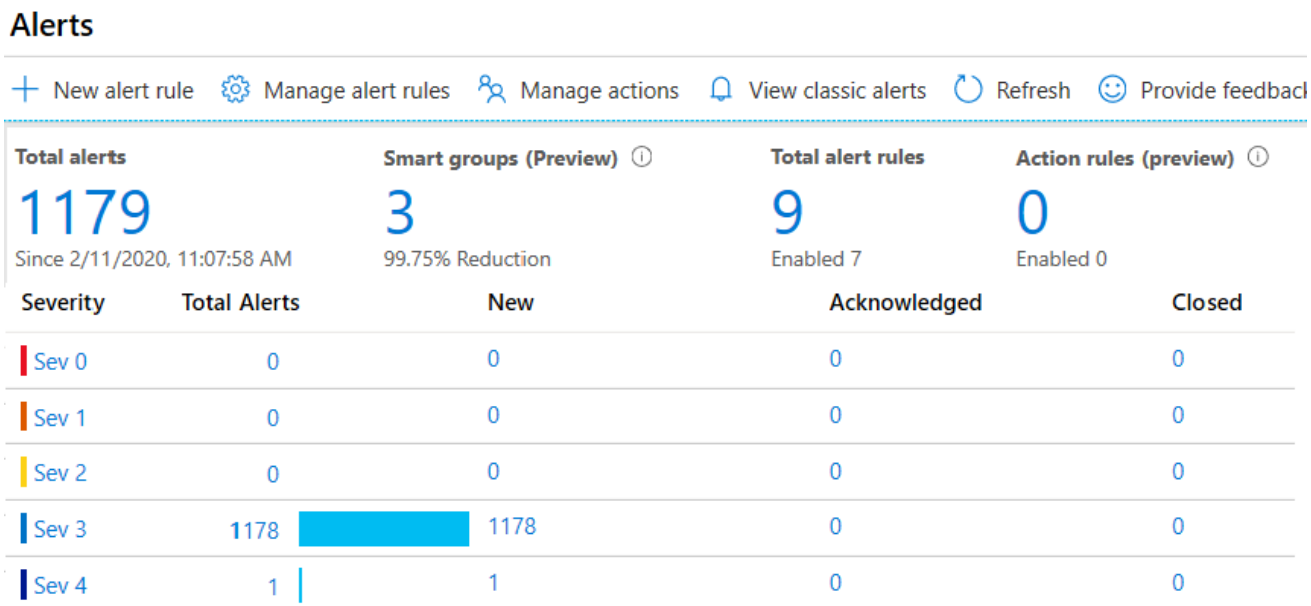
Azure Monitor Alerts

Creating Alert Rules

Action Groups

Demonstration – Alerts

Azure Monitor Alerts



Unified authoring experience

Displayed by severity

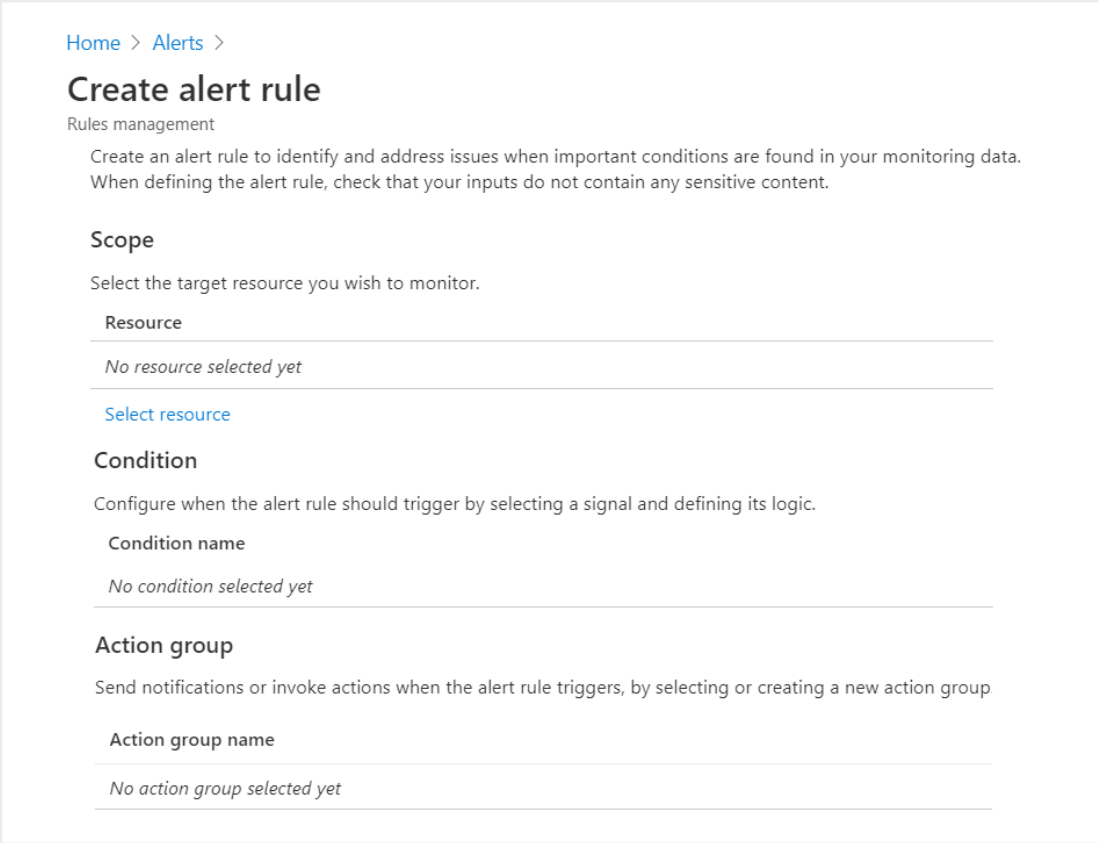
Categorized by New, Acknowledged, and Closed

Creating Alert Rules

Scope: Target selection, Alert criteria, and Alert logic

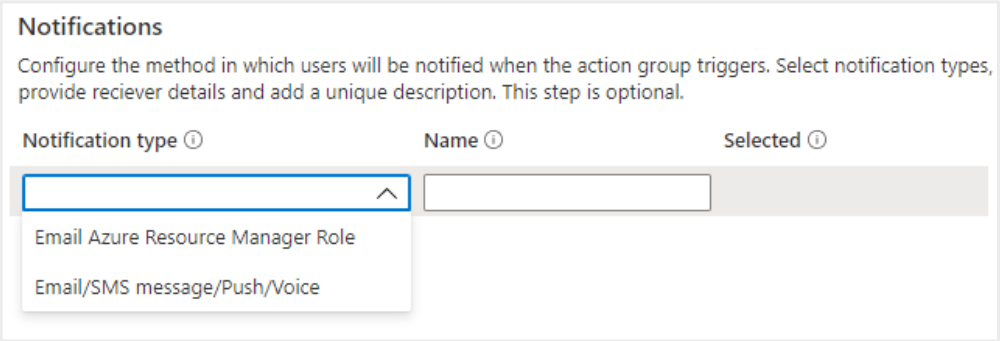
Alert rule details: Alert rule name, description, and severity (0 to 4)

Action group: Notify your team via email and text messages or automate actions using webhooks and runbooks

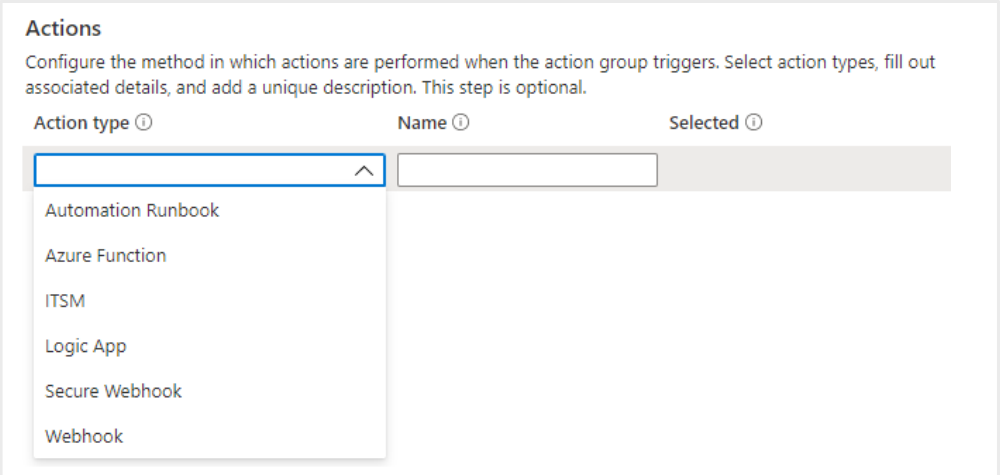


Action Groups

Configure the method in which users will be notified when the action group triggers



Configure the method in which actions are performed when the action group triggers



Lesson 03: Configure Log Analytics

Log Analytics Overview

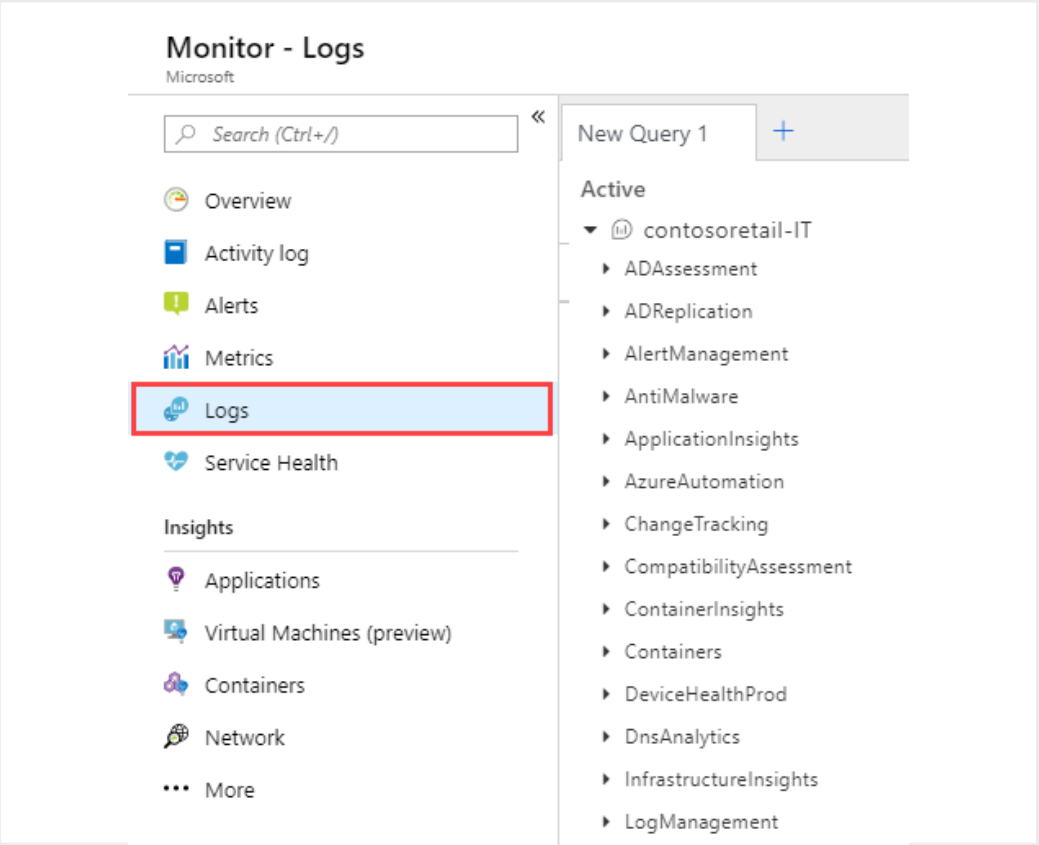
- Log Analytics
- Create a Workspace
- Connected Sources
- Data Sources
- Log Analytics Querying
- Query Language Syntax
- Demonstration – Log Analytics

Determine Log Analytics Uses

A service that helps you collect and analyze data generated by resources in your cloud and on-premises environments

Write log queries and interactively analyze their results

Examples include assessing system updates and troubleshooting operational incidents

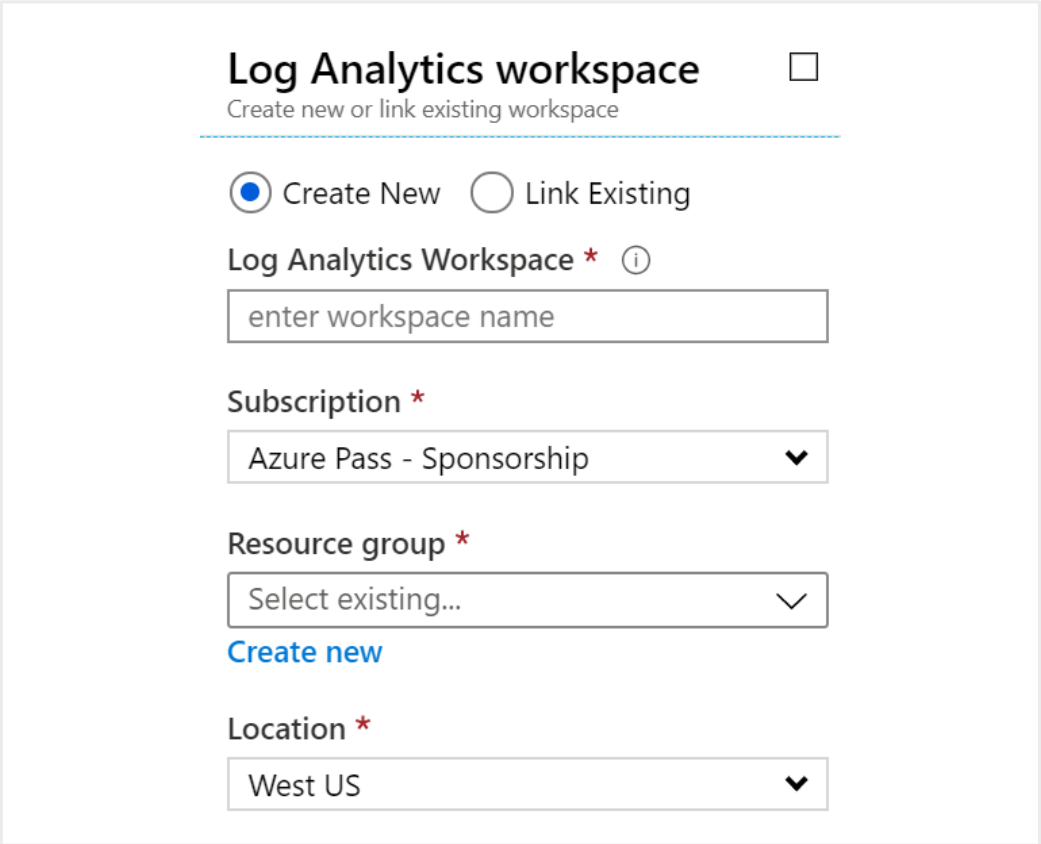


Create a Workspace

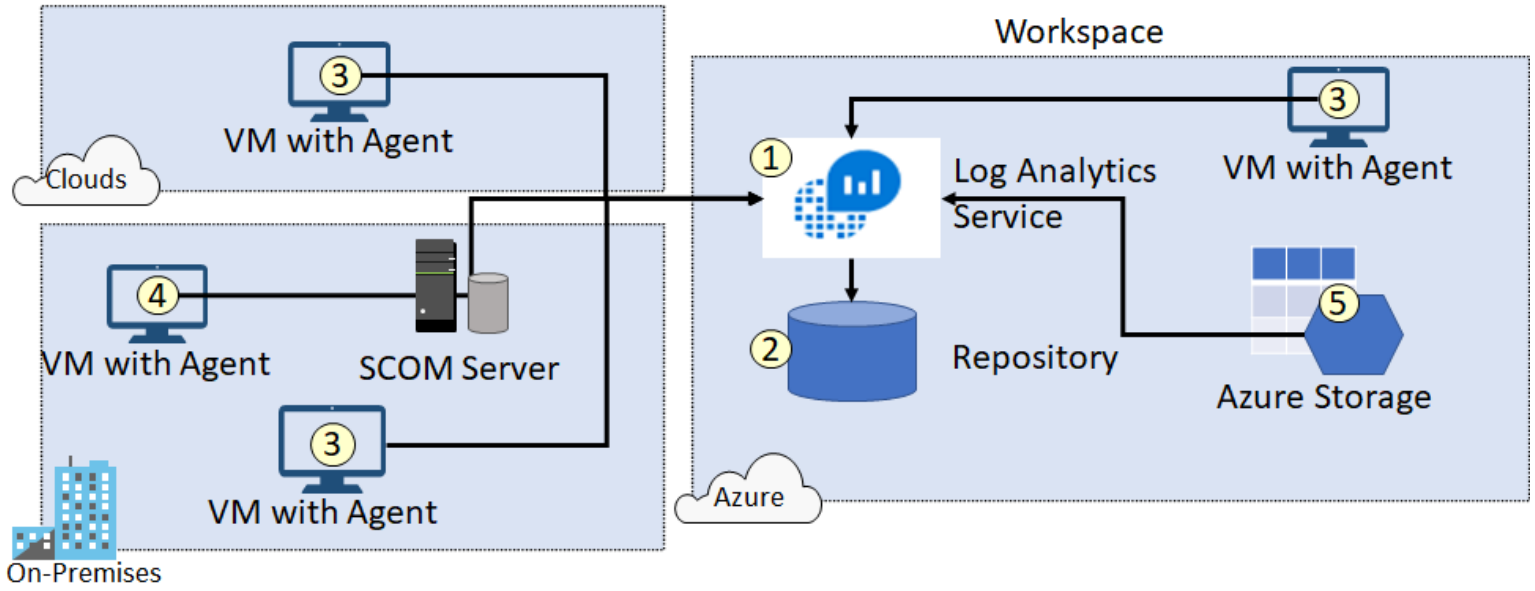
A workspace is an Azure resource and is a container where data is collected, aggregated, analyzed, and presented

You can have multiple workspaces per Azure subscription, and you can have access to more than one workspace

A workspace provides a geographic location, data isolation, and scope



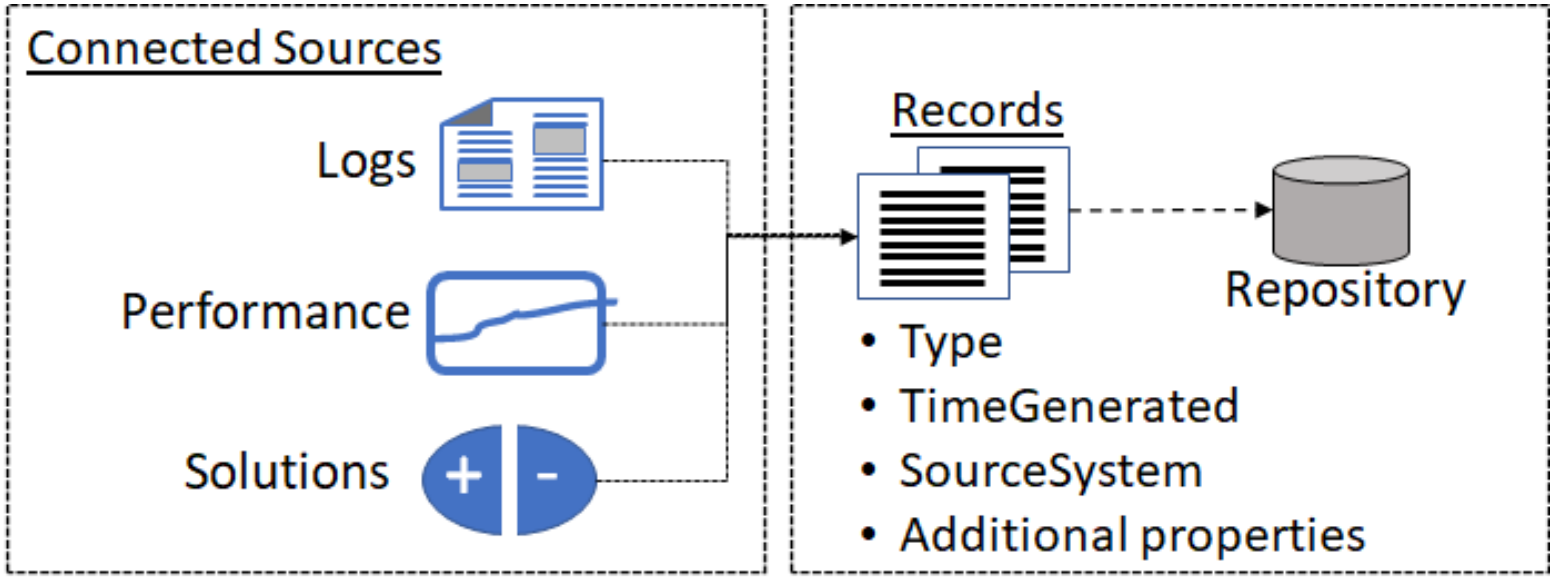
Create Connected Sources



Connected Sources generate data

Data can be collected from Windows, Linux, SCOM and Azure Storage

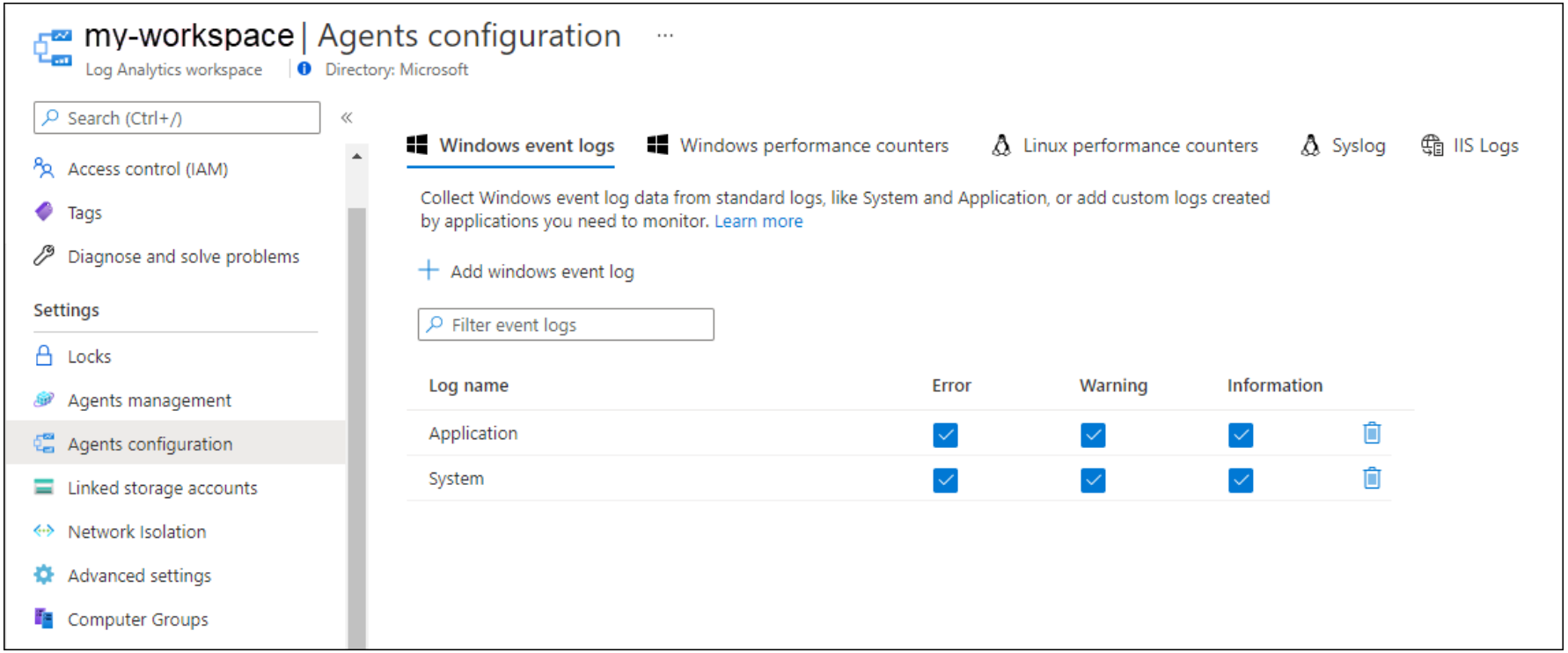
Define Data Sources



Data sources include Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog

Each data source has additional configuration options

Configuring data sources



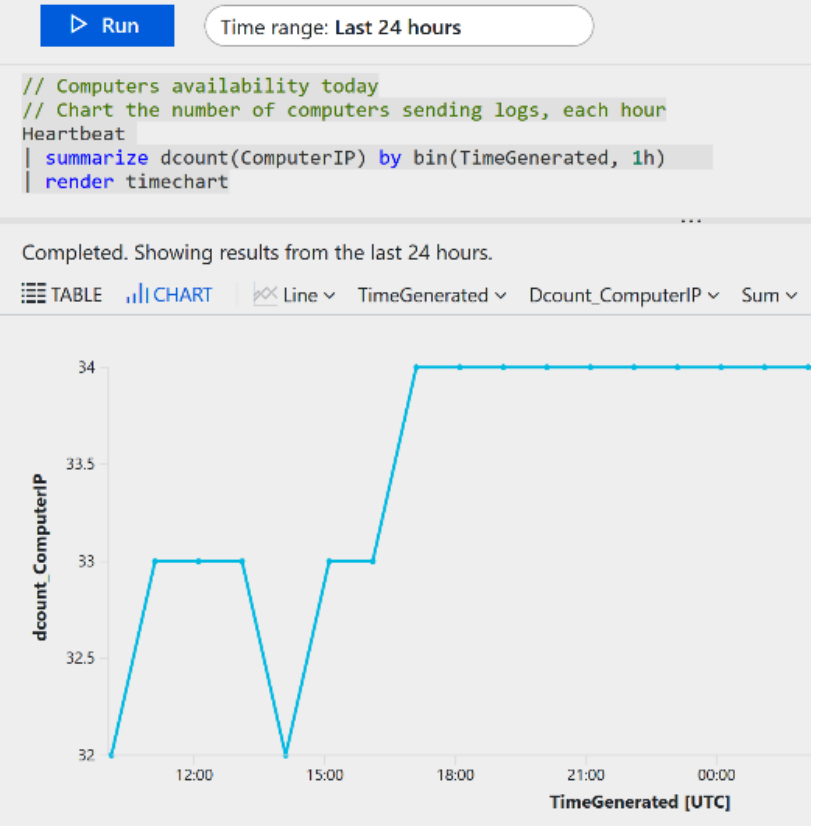
Visualize Log Analytics Data

Log Analytics provides a query syntax

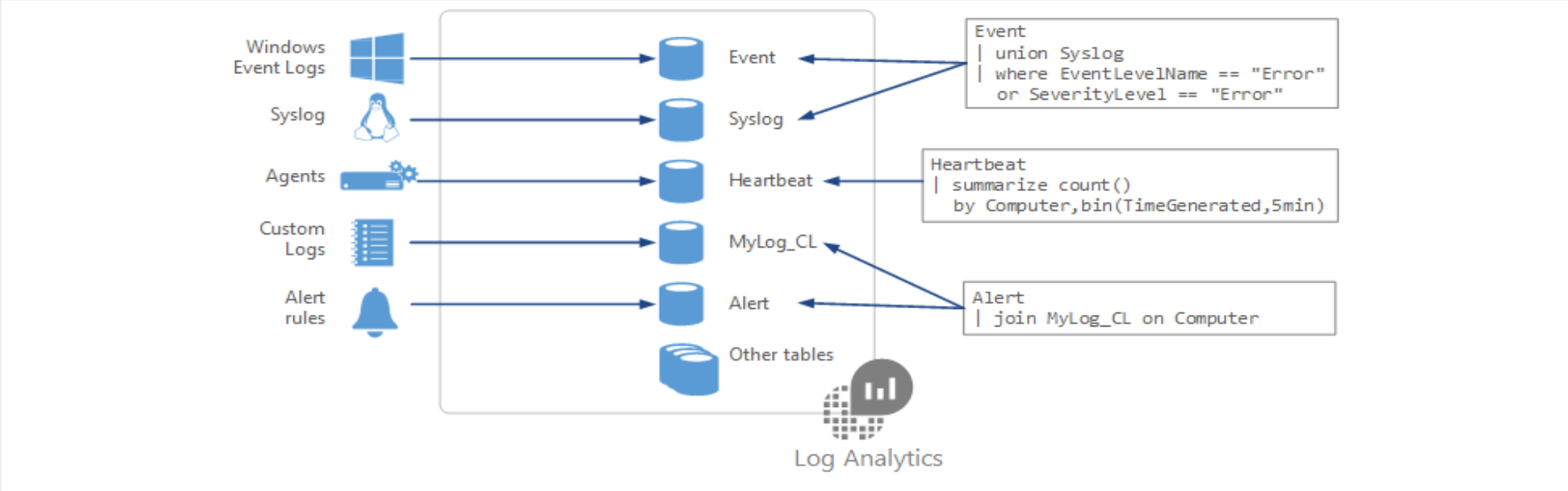
Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

Export the data to Power BI or Excel



Structure Log Analytics Queries




```
Event
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCount = count() by Computer
| top 10 by ErrorCount desc
```

Summary and Resources – Configure Log Analytics

Knowledge Check Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Analyze your Azure infrastructure by using Azure Monitor logs
	Monitor performance of virtual machines by using Azure Monitor for VMs

Lesson 04: Configure Network Watcher

Configure Network Watcher Introduction

- Describe Network Watcher Features
- Review IP Flow Verify Diagnostics
- Review Next Hop Diagnostics
- Visualize the Network Topology
- Summary and Resources

Describe Network Watcher Features

A **regional service** that provides various network diagnostic and monitoring tools

IP Flow Verify diagnoses connectivity issues

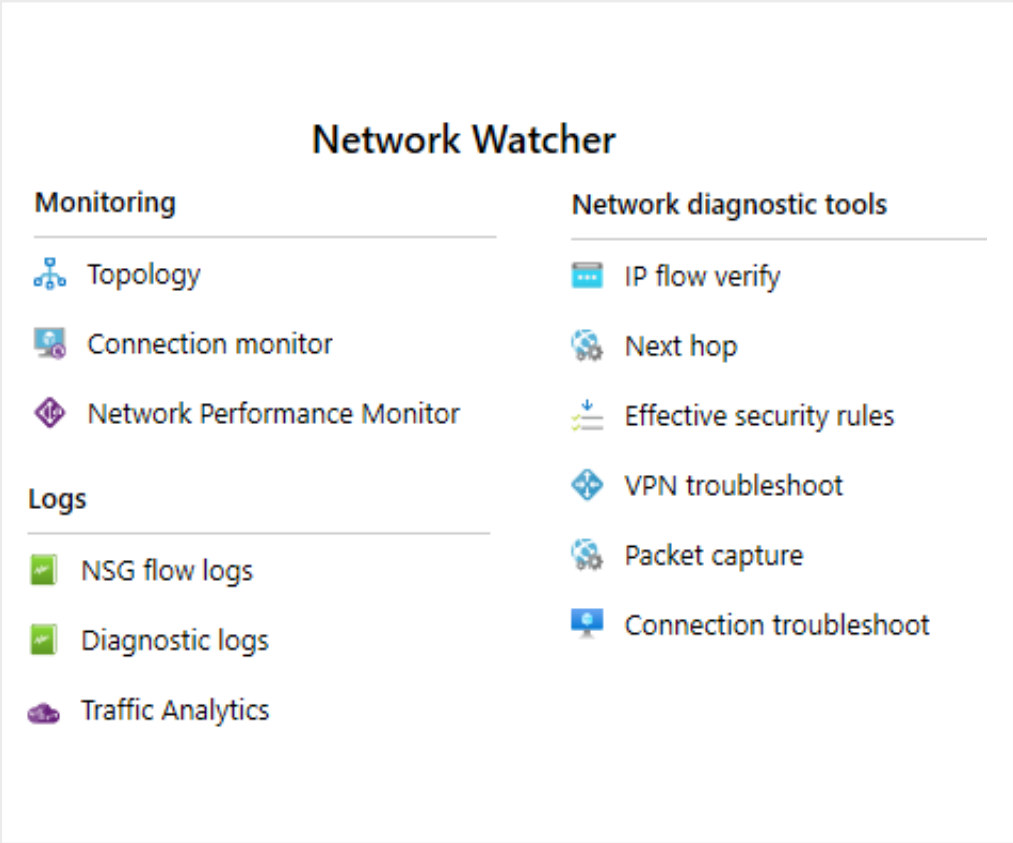
Next Hop determines if traffic is being correctly routed

VPN Diagnostics troubleshoots gateways and connections

NSG Flow Logs maps IP traffic through a network security group

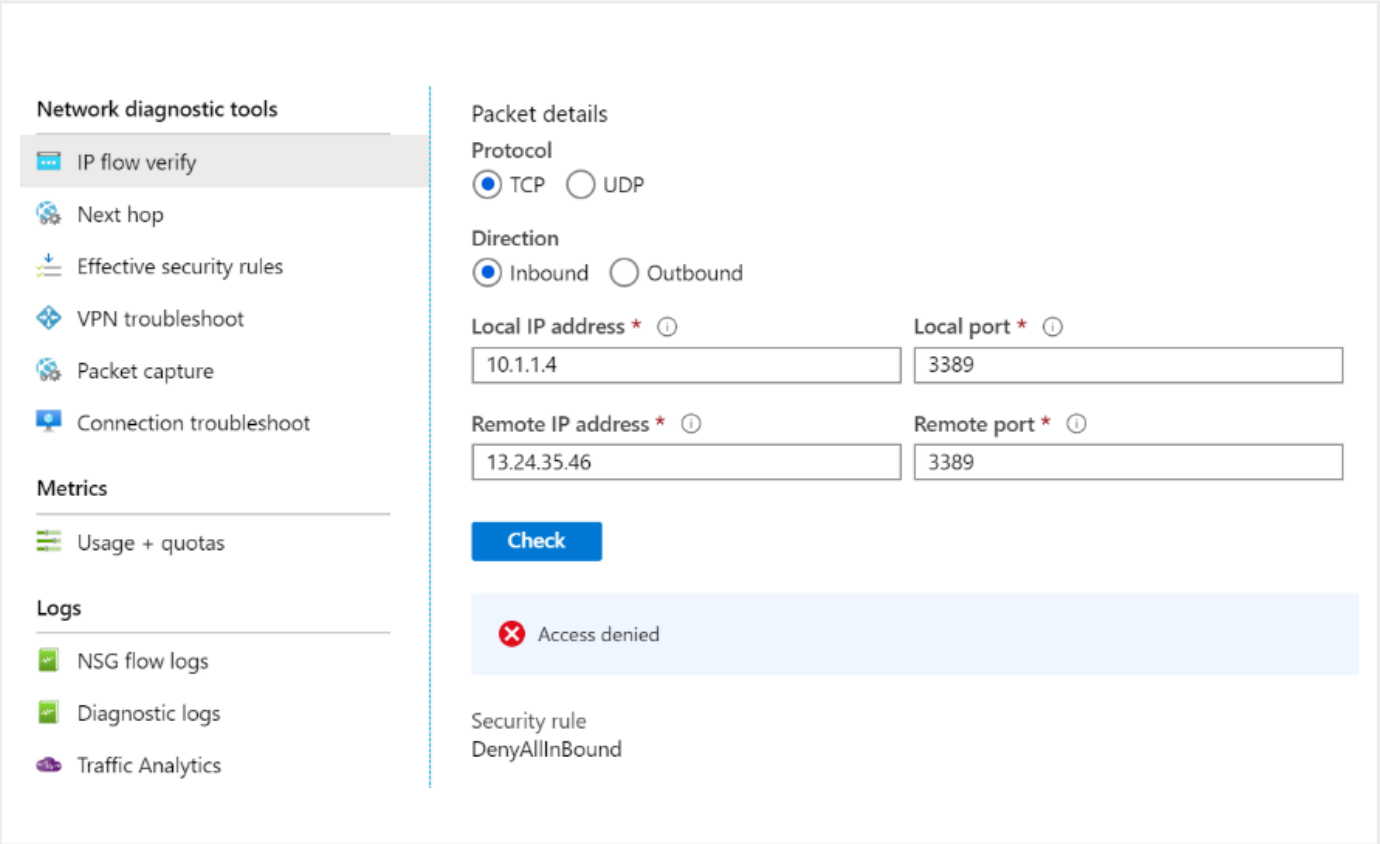
Connection troubleshoot shows connectivity between source VM and destination

Topology generates a visual diagram of resources



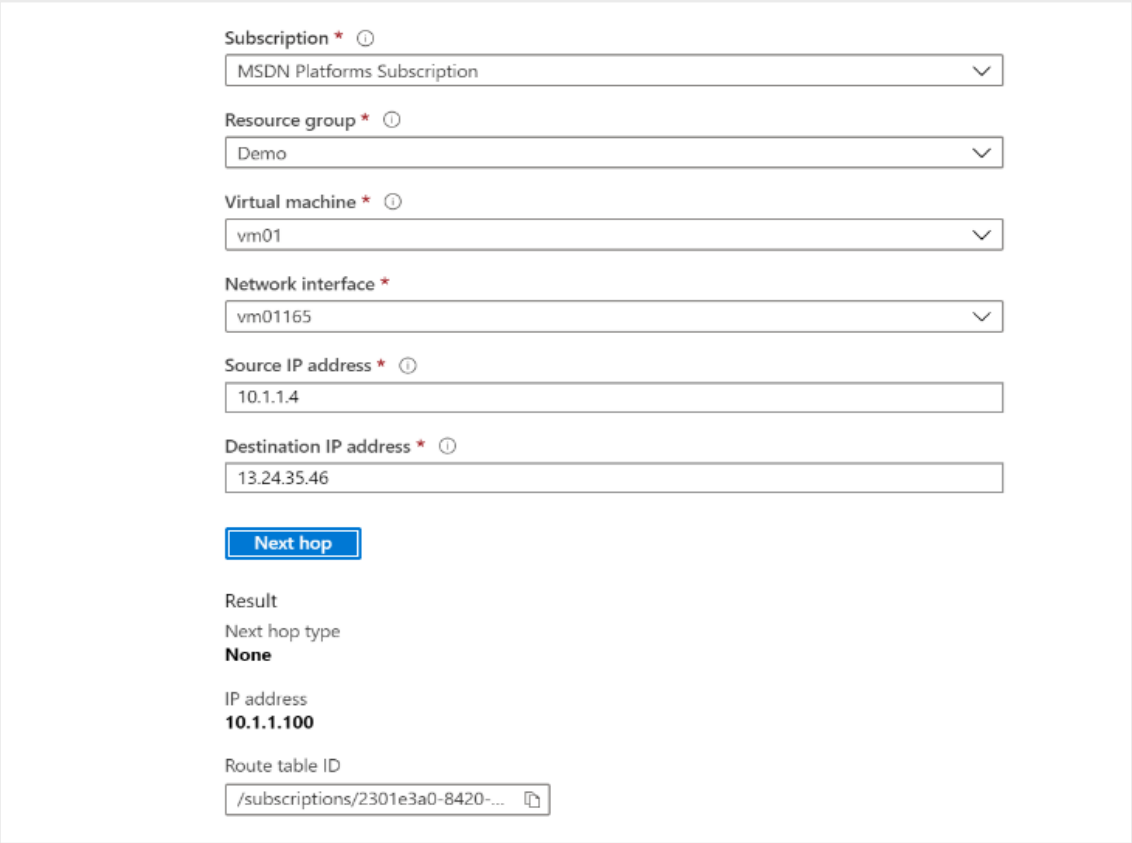
Review IP Flow Verify Diagnostics

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



Review Next Hop Diagnostics

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



Diagnostics – Effective Security Rules

nsg01

Inbound rules

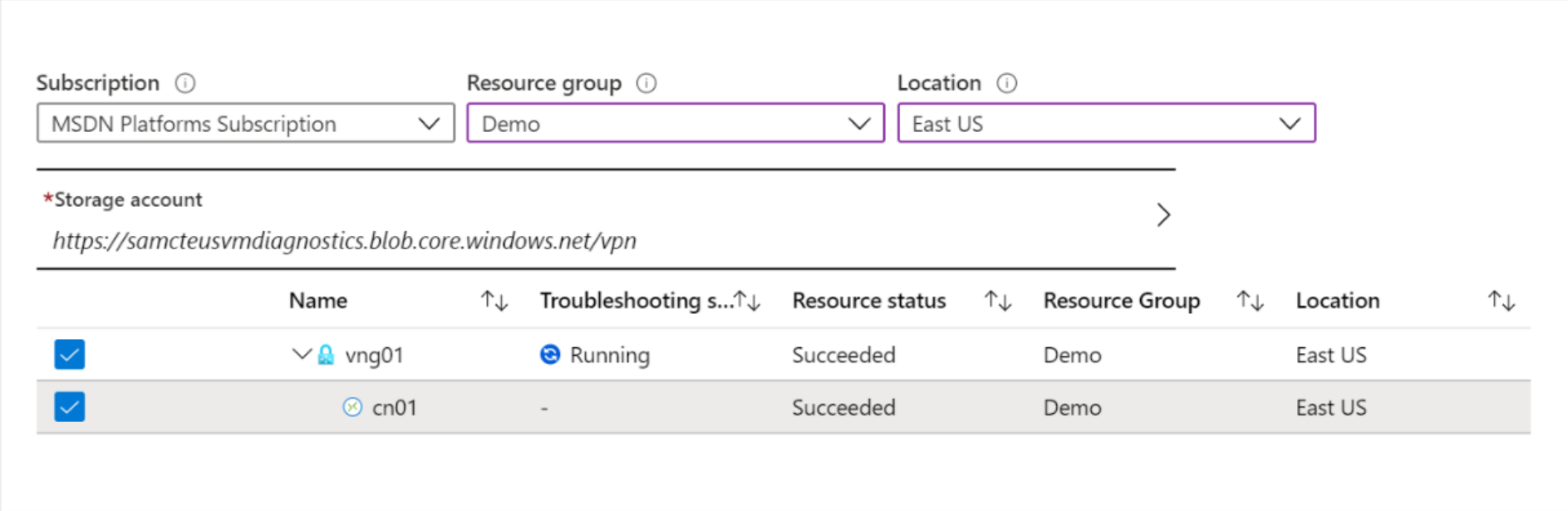
Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
RDP_Inbound	100	13.23.34.45/32	0-65535	0.0.0.0/0	3389-3389	TCP	Allow
AllowVnetInBound	65000	Virtual network (1 prefixes)	0-65535	Virtual network (1 prefixes)	0-65535	All	Allow
AllowAzureLoadBalancerInBound	65001	Azure load 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

Diagnostics – VPN Troubleshoot



Helps you troubleshoot gateways and connections

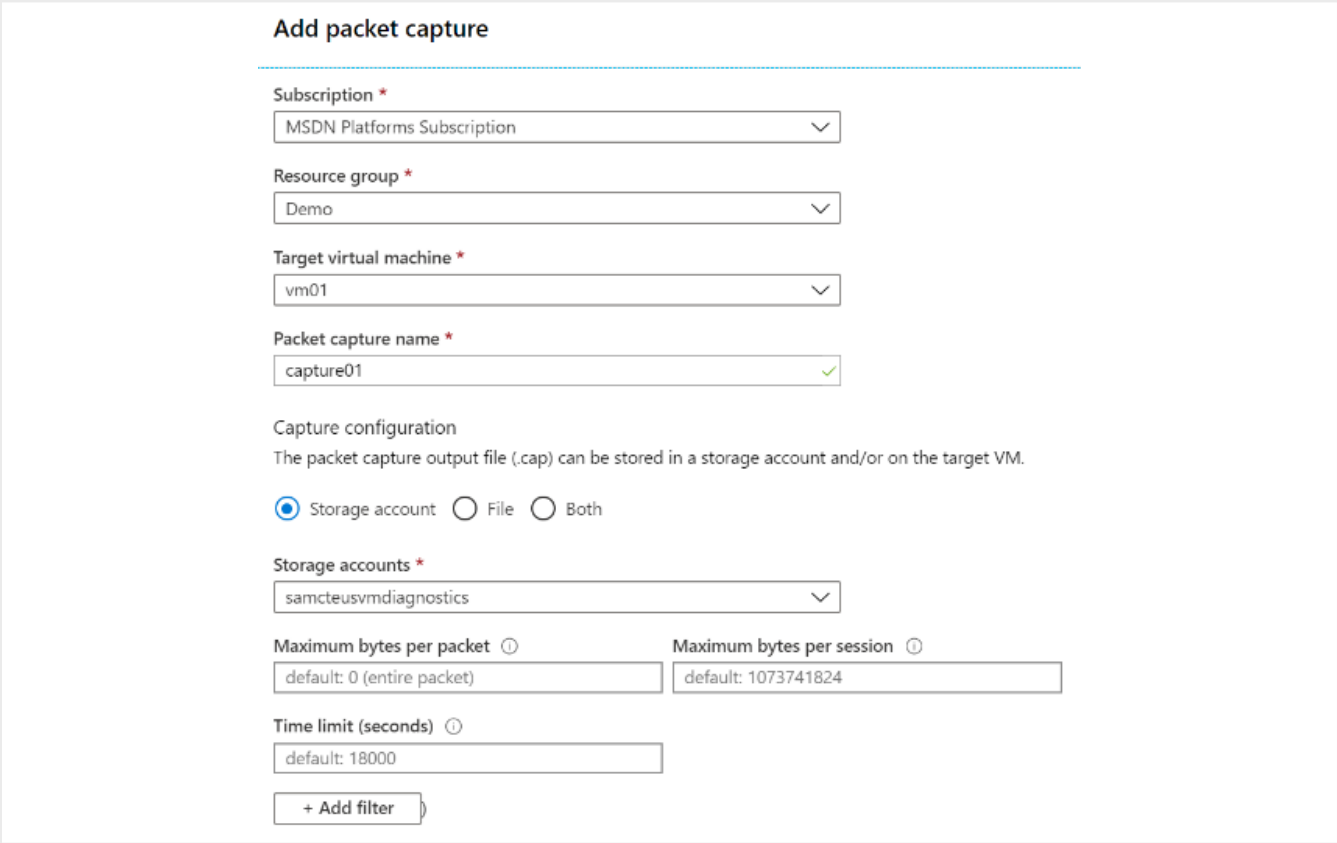
Provides summary information and detailed information

Can troubleshoot multiple gateways or connections simultaneously

Diagnostics – Packet Capture

Captures inbound and outbound traffic from a Virtual Machine

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



Diagnostics – Connection Troubleshoot

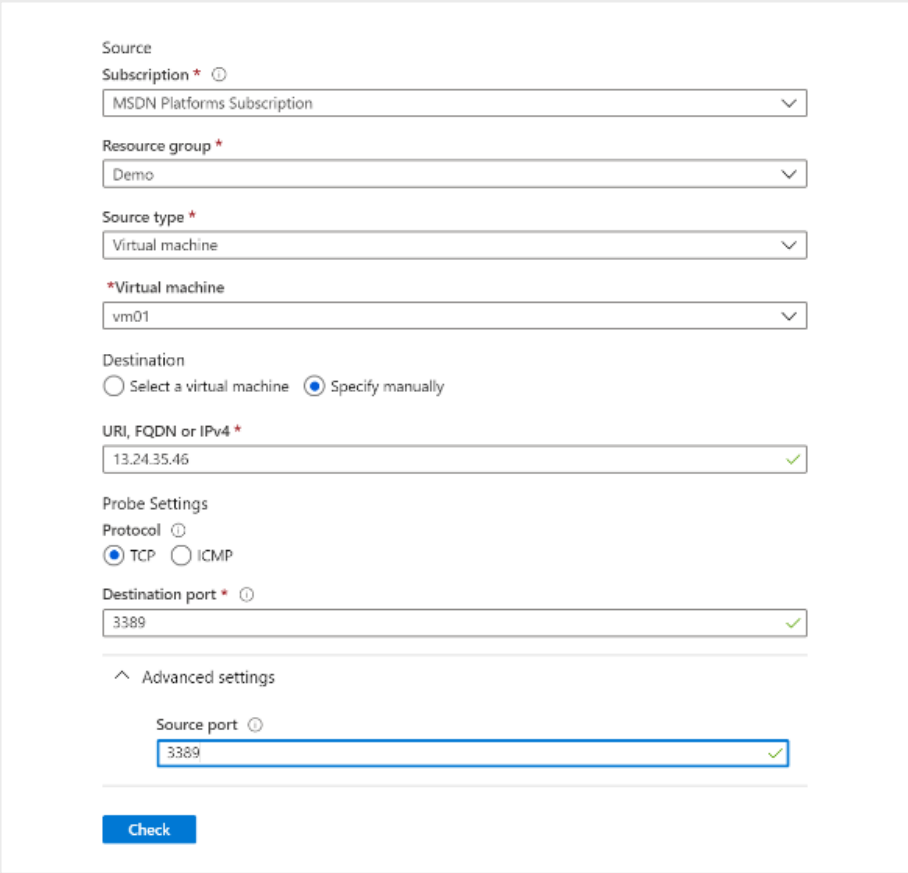
Check connectivity between source VM and destination

Identify configuration issues that are impacting reachability

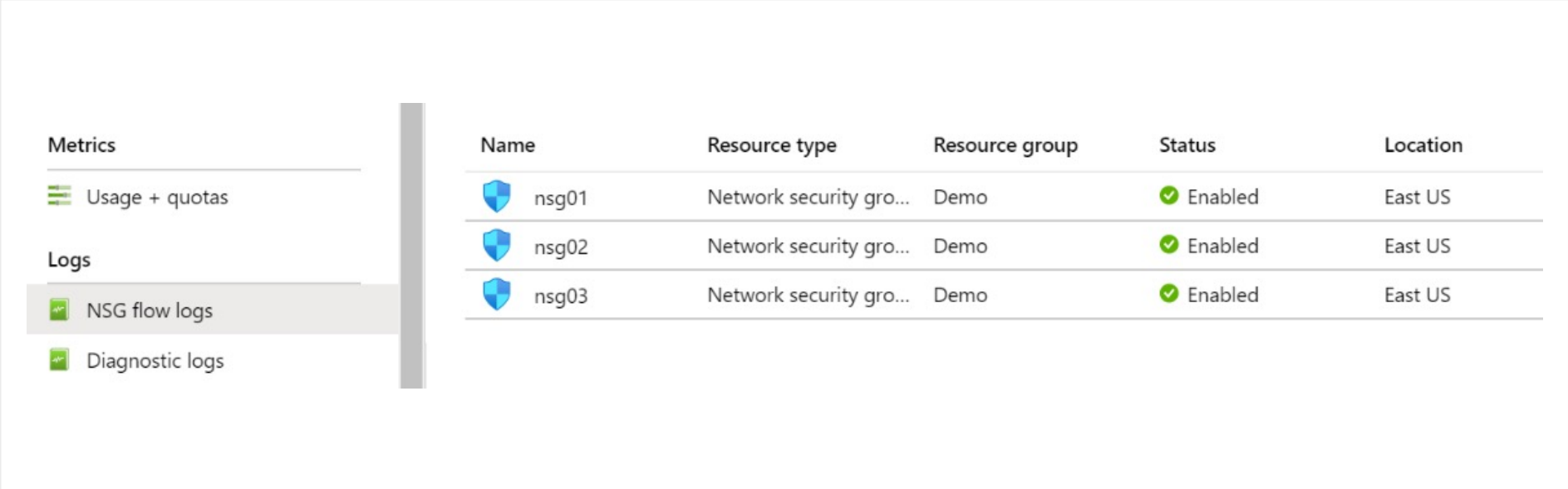
Provide all possible hop by hop paths from the source to destination

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

View a graphical topology from your source to destination



Logs – NSG Flow Logs

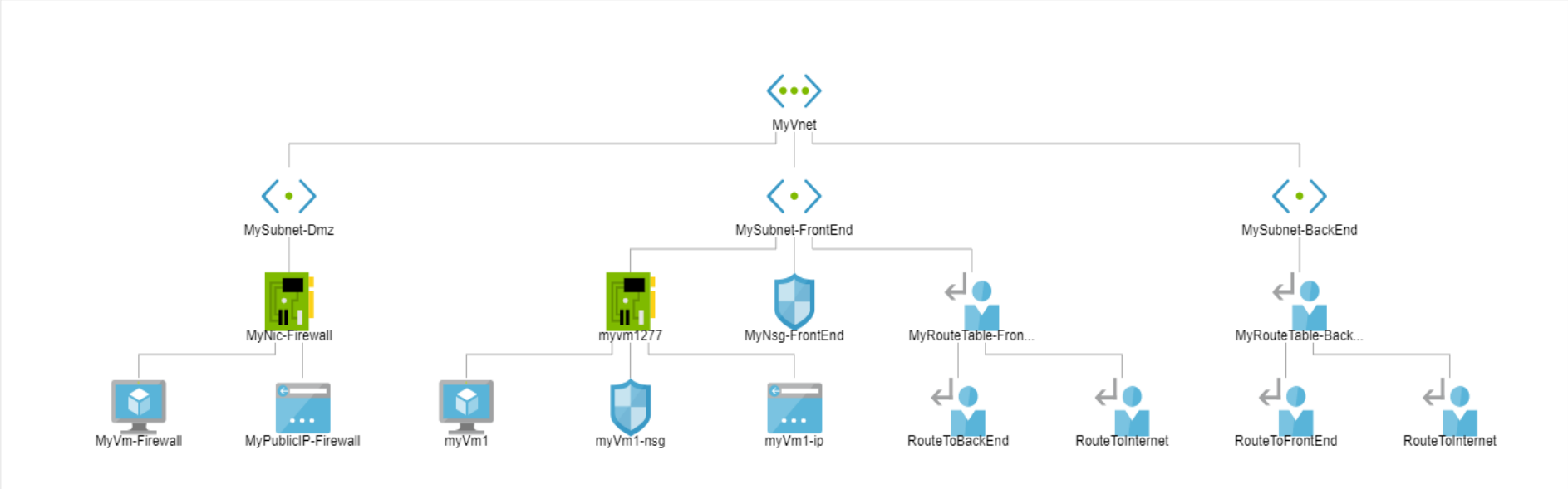


View information about ingress and egress IP traffic through an NSG

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

Visualize the Network Topology



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 in the same region as the virtual network

Summary and Resources – Configure Network Watcher

Knowledge Check Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools

Lesson 05: Module 11 Lab

Lab 11 – Implement monitoring

Lab scenario

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

Objectives

Task 1:
Provision the lab environment

Task 2:
Create and configure an Azure Log Analytics workspace and Azure Automation-based solutions

Task 3:
Review default monitoring settings of Azure virtual machines

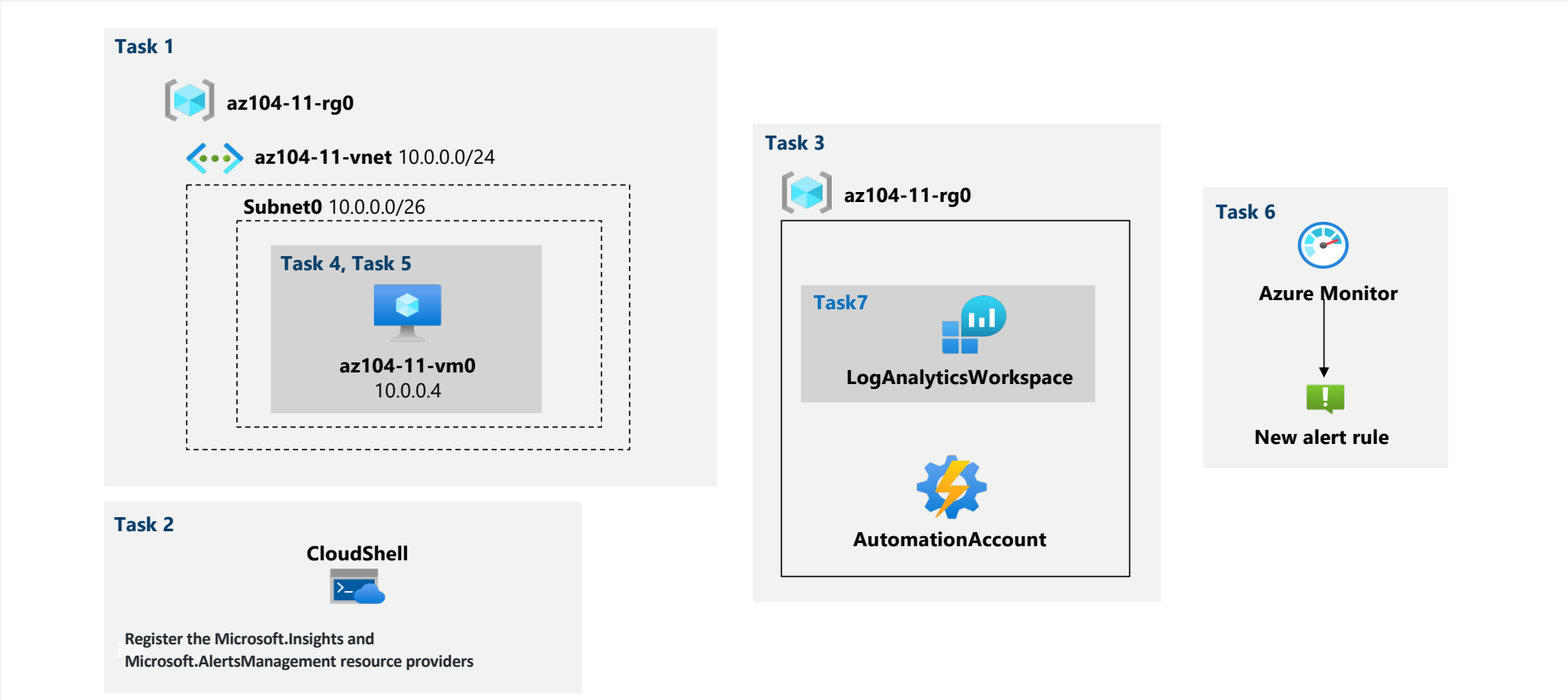
Task 4:
Configure Azure virtual machine diagnostic settings

Task 5:
Review Azure Monitor functionality

Task 6:
Review Azure Log Analytics functionality

Next slide for an architecture diagram

Lab 11 – Architecture diagram



Module Review

Module Review Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Analyze your Azure infrastructure by using Azure Monitor logs
	Improve incident response with alerting on Azure
	Monitor the health of your Azure virtual machine by collecting and analyzing diagnostic data
	Monitor, diagnose, and troubleshoot your Azure storage
	Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools
	Design a holistic monitoring strategy on Azure
	Monitor performance of virtual machines by using Azure Monitor for VMs

End of presentation