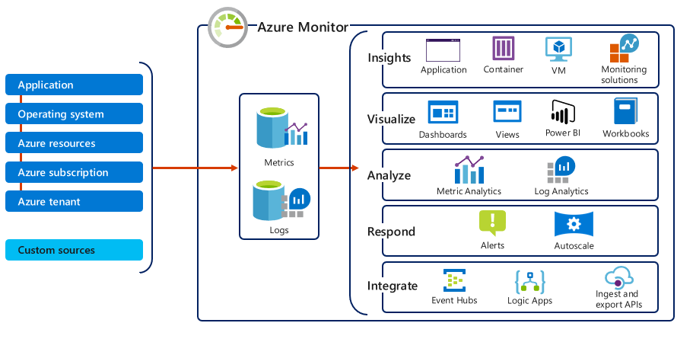
Module 8: Design and implement network monitoring

# Chapter 2: Monitor your networks using Azure monitor

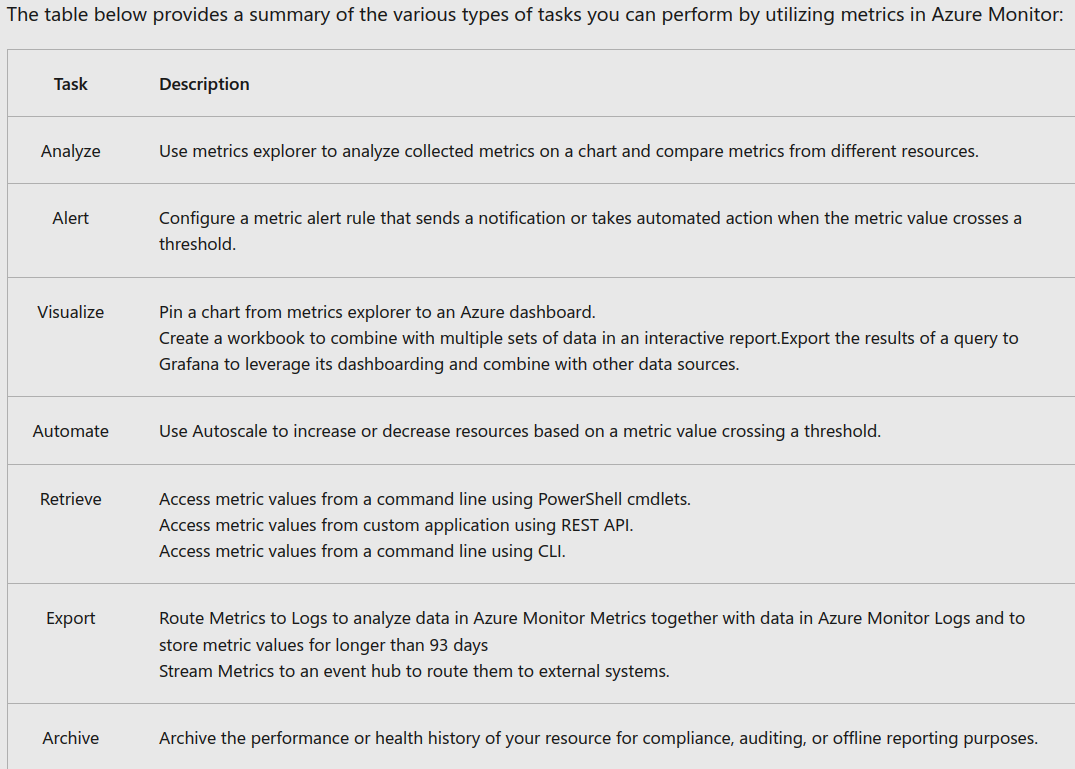
## Azure Monitor

* Maximizes availability/performance of Azure apps and services by providing a comprehensive solution for collecting, analyzing, and acting on telemetric data.
  + 

### Monitor data types in Azure Monitor

* 2 types of data:
  + **Metrics**
    - Numerical values describing parts of system at specific time
  + **Logs** 
    - Data organized into records with different sets of properties for each type.
      * **Ex**. Telemetry (**ex**. events and traces) are stored as logs

### Azure Monitor metrics

* Numeric data from monitored resources into a time series database.
  + 

#### 3 Sources of Metrics collected by Azure Monitor:

* **Azure resources** 
  + Platform metrics created by Azure resources (health and performance).
* **Apps** 
  + Metrics created by App Insights (tracks performance)
* **VM agents** 
  + Collected from guest OS of VM.
* **Custom metrics** 
  + **You** define custom metrics in app monitored by App Insights
  + Or use custom metrics API to create custom metrics

## Monitor network resources with Azure Monitor Network Insights

* Structured around (tabs):
  + Network health & metrics
  + Connectivity & Traffic
  + Diagnostic Toolkit
    - Provides access to ALL diagnostic features for troubleshooting networks and components.
    - Following network monitoring features:
      * Capture packets on virtual machines w/ Network Watcher **packet capture** tool
      * Troubleshoot VPN w/ Network Watcher **VPN Troubleshoot** tool
      * Troubleshoot connectivity w/ Network Watcher **Connection Troubleshoot** tool
      * Identify next hops w/ Network Watcher **Next hop** tool
      * Diagnose traffic filtering issues w/ Network Watcher **IP flow verify** tool

# Chapter 4: Monitor your networks using Azure network watcher

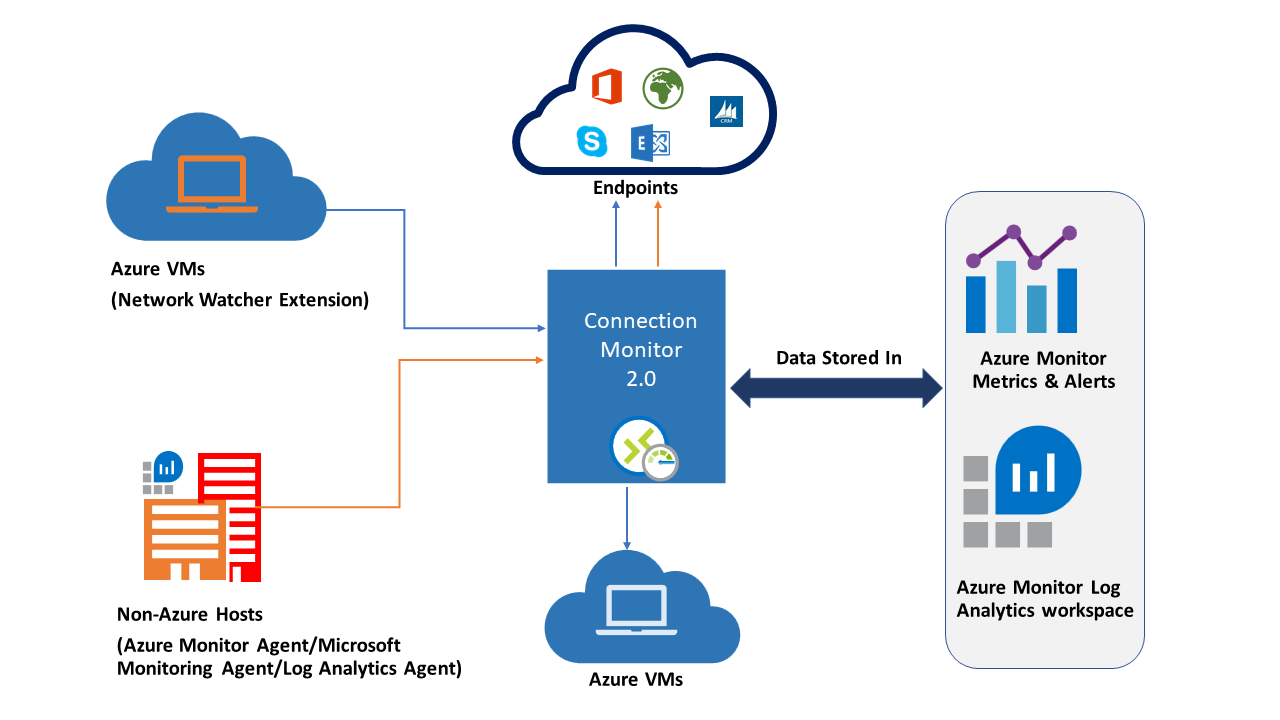
## Azure Network Watcher

* Regional service which enables monitoring/diagnosing of conditions at network level in Azure
  + Enables you to diagnose problems at an end-to-end network level view
  + Create a Network Watcher resource, which is designed to monitor/repair network health of IaaS products (**ex**. VMs, VNETS, App Gateways, and LBs.
    - Features/Use Cases:
      * *Automate remote network monitoring with packet capture*
      * *Gain insight into your network traffic using flow logs*
      * *Diagnose VPN connectivity issues*
* **Network Watcher Tools**
  + *Network Topology*
    - Visual relationship diagram of resources in VNET.
  + *Verify IP Flow*
  + *Next Hop*
    - Determine if traffic is being directed to the intended destination by showing the next hop.
  + *Effective security rules*
    - Check NSGs associated at subnet/NIC level.
  + *VPN Diagnostics for troubleshooting gateways and connections*
  + *Packet Capture*
    - Track traffic to and from a VM
  + *Connection Troubleshoot*
  + *NSG Flow Logs*

## Configure NSG Flow Logs

* Allows you to log information about IP traffic flowing through an NSG
* Use cases for NSG flow logs:
  + *Network Monitoring*
    - Id unknown or undesired traffic
    - Monitor traffic levels/bandwidth consumption
  + *Usage monitoring and optimization*
  + *Compliance* - verify network isolation/compliance
  + Network forensics and security analysis

## Connection Monitor

* Provides unified end-to-end connection monitoring in Azure Network Watcher (NW).
  + 
* Use cases for Connection Monitor:
  + Check network connectivity between the two VMs
    - **Ex**. Front-end web server VM communicates with a database server VM
  + Compare cross-region network latencies of VMs in USEA to VMs in USCN
  + Compare latencies between Seattle and Ashburn (sites).
  + Compare latencies of on-premises site to the latencies of the Azure application
  + Check connectivity between on-premises setups and Azure VMs
* Benefits:
  + Unified
  + Cross-region
  + Higher probing frequencies (better visibility into network performance)
  + Faster alerting
  + Support for connectivity checks that are based on HTTP, TCP, and ICMP
  + Metrics and Log Analytics support

#### **Link on how to set up Connection Monitor**:

* https://learn.microsoft.com/en-us/training/modules/design-implement-network-monitoring/4-monitor-networks-using-azure-network-watcher

## Traffic Analytics

* Provides visibility into user/app activity in Azure VNET
  + Features:
    - Visualize network activity across Azure subscriptions.
    - Identify security threats to secure VNET
    - Understand traffic flow patterns across Azure regions
    - Pinpoint network misconfigurations leading to failed connections in VNET.

### How Traffic Analytics works

* Examines raw NSG flow logs/captures and aggregates common flows among the same source/destination IP, destination port, and protocol
  + Key components of Traffic Analytics:
    - NSG
    - NSG flow logs – logs about ingress and egress IP traffic through NSG
    - Log Analytics – monitoring data and stores the data in a central repository
    - Log Analytics workspace (LGA) – stores data for an Azure account
    - Network Watcher – regional service that monitor/diagnose network