

Tag 3

Azure Implement & Manage (Applied Skills)

Guten Morgen!



Azure - Implement & Manage (Applied Skills)

AZ-1002

Configure secure access to your workloads using Azure virtual
networking

AZ-1003

Secure storage for Azure Files and Azure Blob Storage

AZ-1004

Deploy and configure Azure Monitor

AZ-1007

Deploy and administer Linux virtual machines on Azure

Assessment retired!

Go Deploy Lab

Assessment

0 €
72h wachten

AZ-1004

Deploy and configure
Azure Monitor

Introduction to the course scenario – business group requirements

serverless
Computing

Logic App
Functions

Implement monitoring infrastructure

- Need Log Analytics workspaces to be configured for appropriate access, and data retention and archival.
- Also ensure notifications of any workspace health degradation.

Application monitoring
App Insights

- Provide performance and availability monitoring for apps and services in cloud environments, or on-premises.
- Collect telemetry generated from running company applications.

Monitor compute resources
VM ACI

- Monitor performance of a fleet of heterogeneous IaaS VMs deployed in Azure.
- Ensure that virtual machine performance is tracked and visible in the Azure Portal.

Network monitoring

- Monitor the health of the Azure IaaS resources in the network environment.
- Deploy Azure Network Watcher tools to view metrics and diagnose network traffic issues.

Alerting system

- Need a system of alerts to proactively manage issue notifications
- Need to stay informed of issues affecting applications and infrastructure before they occur.

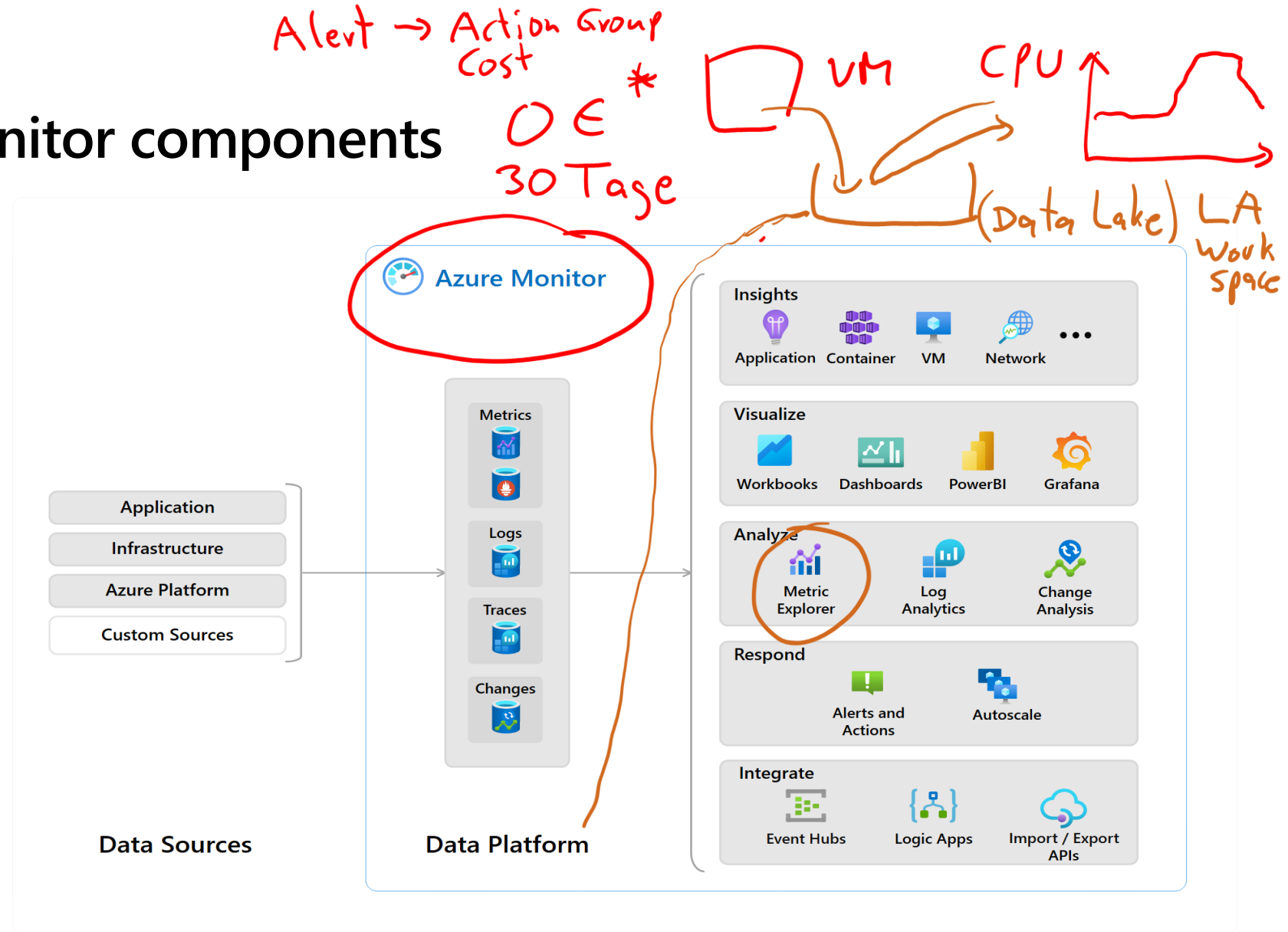
Network Watcher

*Action Group
→ Ticket*

Understand Azure Monitor components

- Application monitoring data
- Guest OS monitoring
- Azure resource monitoring
- Azure subscription monitoring
- Azure tenant monitoring

YLB



Create and configure a Log Analytics workspace

LA

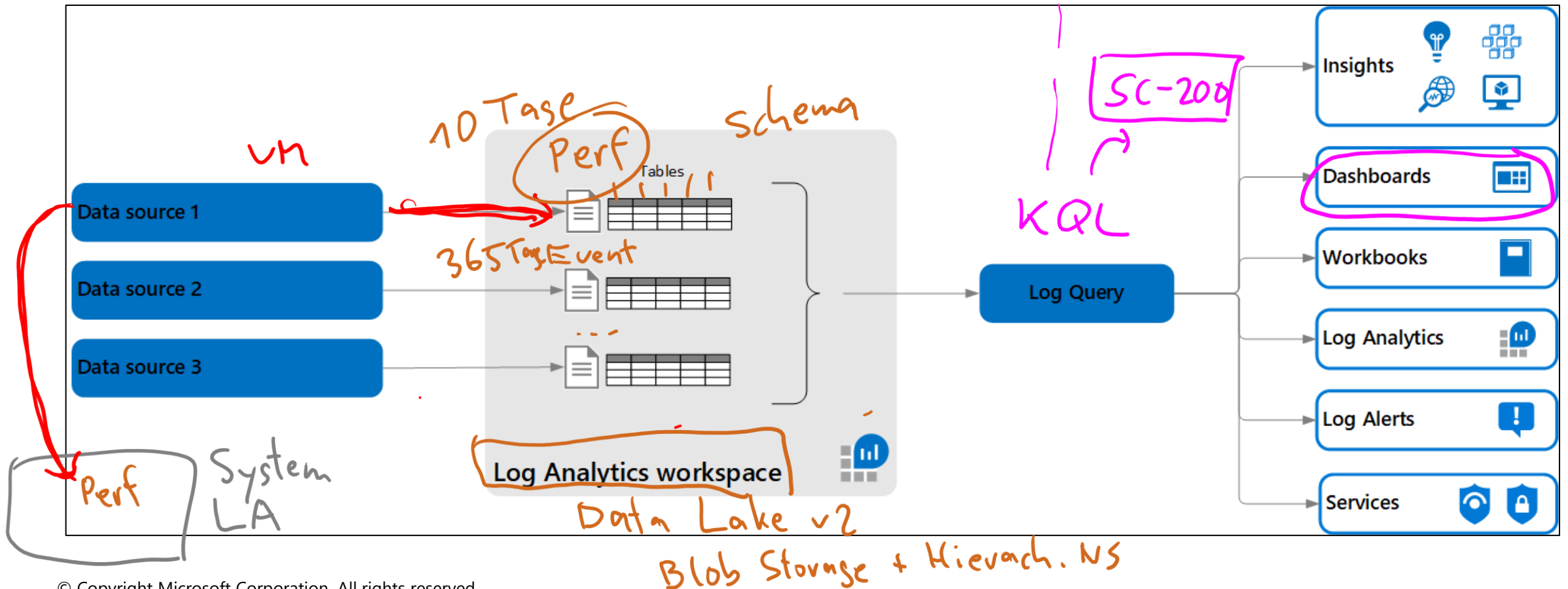


What is a Log Analytics workspace?

Log Analytics workspace is a unique environment for log data from Azure Monitor and other Azure services

Sentinel (SIEM)

3rd Party
Prometheus
Grafana



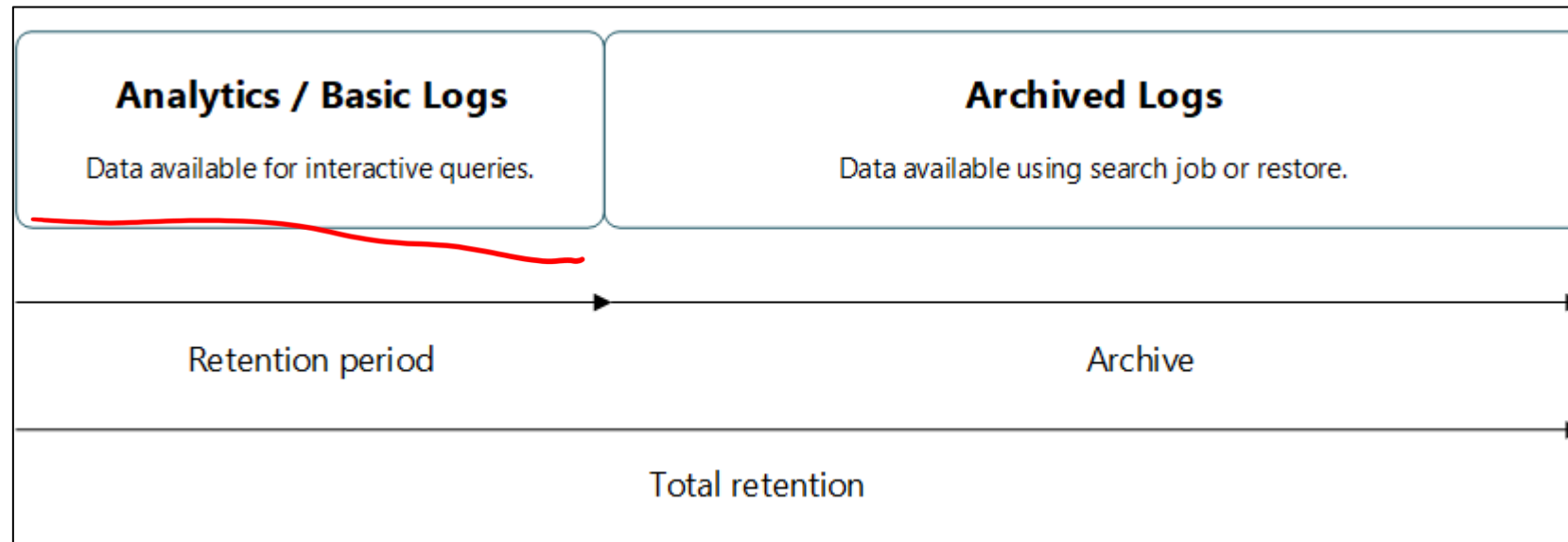
Configure Log Analytics data retention

Interactive retention

- Interactive retention: retain logs for monitoring, troubleshooting, and analytics

Archive

- Archive: store logs for compliance or occasional reference (saves costs)



KQL examples

- Log Analytics offers *Simple mode* and *KQL mode* for analyzing data
- Use KQL mode if you need to derive deeper insights from your logs

Limit query results on a security event, filtering by conditions of **Level** and **Event ID**.


Kusto

```
SecurityEvent  
| where Level == 8 and EventID == 4672
```

Calculate the average **CounterValue** for each combination of computer and specific performance counter

Kusto

```
Perf  
| where TimeGenerated > ago(1h)  
| summarize avg(CounterValue) by Computer, CounterName
```



Configure Log Analytics health status alerts

Log Analytics workspaces can provide data for query and analysis

- Data based on available latency

Set up health status alerts to proactively monitor workspace health

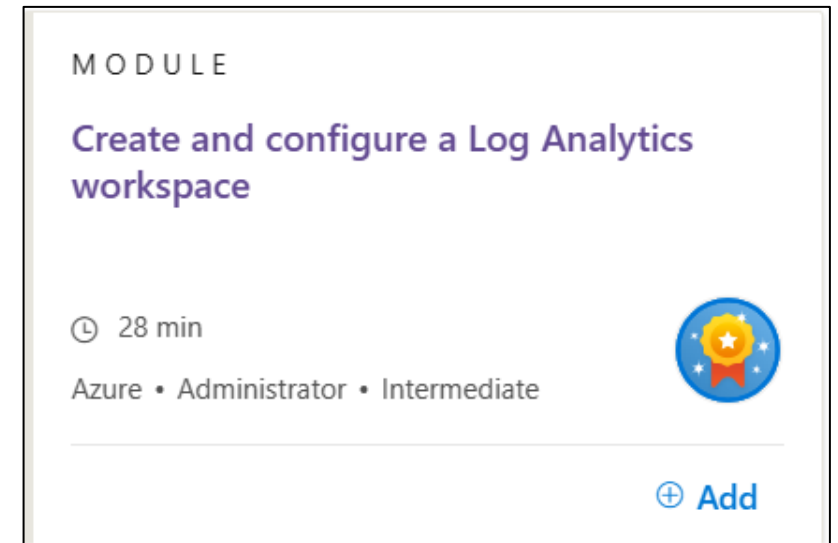
Get notification when an issue is detected and take timely corrective action

- Enable recommended alert rules.
- Create a new alert rule

The screenshot shows the 'Create an alert rule' interface in Log Analytics. The breadcrumb navigation is 'Home > Log Analytics workspaces > my-workspace | Resource health >'. The main heading is 'Create an alert rule' with a three-dot menu. Below this are tabs for 'Scope', 'Condition' (which is selected and underlined), 'Actions', 'Details', 'Tags', and 'Review + create'. A sub-header reads: 'Configure when the alert rule should trigger by selecting a signal and defining its logic.' Under the 'Condition' tab, there is a section titled 'Resource Health' which is highlighted with a red rectangle. Below this section are four configuration items, each with a dropdown menu: 'Event status' (4 selected), 'Current resource status' (3 selected), 'Previous resource status' (4 selected), and 'Reason type' (3 selected). At the bottom of the form are three buttons: 'Review + create' (in blue), 'Previous', and 'Next: Actions >'.

Review questions and reference module – Log Analytics workspace

1. List some of the monitored resources from which Log Analytics allows you to collect data?
2. Your organization wants to configure Azure diagnostics on all Azure resources in a specific workspace. What must you do to enable this?
3. How can your organization ensure access to data in a Log Analytics workspace when it's no longer needed for monitoring, troubleshooting, or analysis?
4. What is the time between data being created on a monitored system and the data being ingested as log data referred to as?



Configure monitoring for applications



What is Azure Monitor Application Insights?



Application Insights is an extension of Azure Monitor

Proactive: gain insights into how an application is performing

Provides Application Performance Monitoring (APM) features

Reactive: review application execution data to determine cause of an incident

Monitor applications from development, through test, and into production

Collect and store application trace logging data

Application Insights capabilities

Visibility

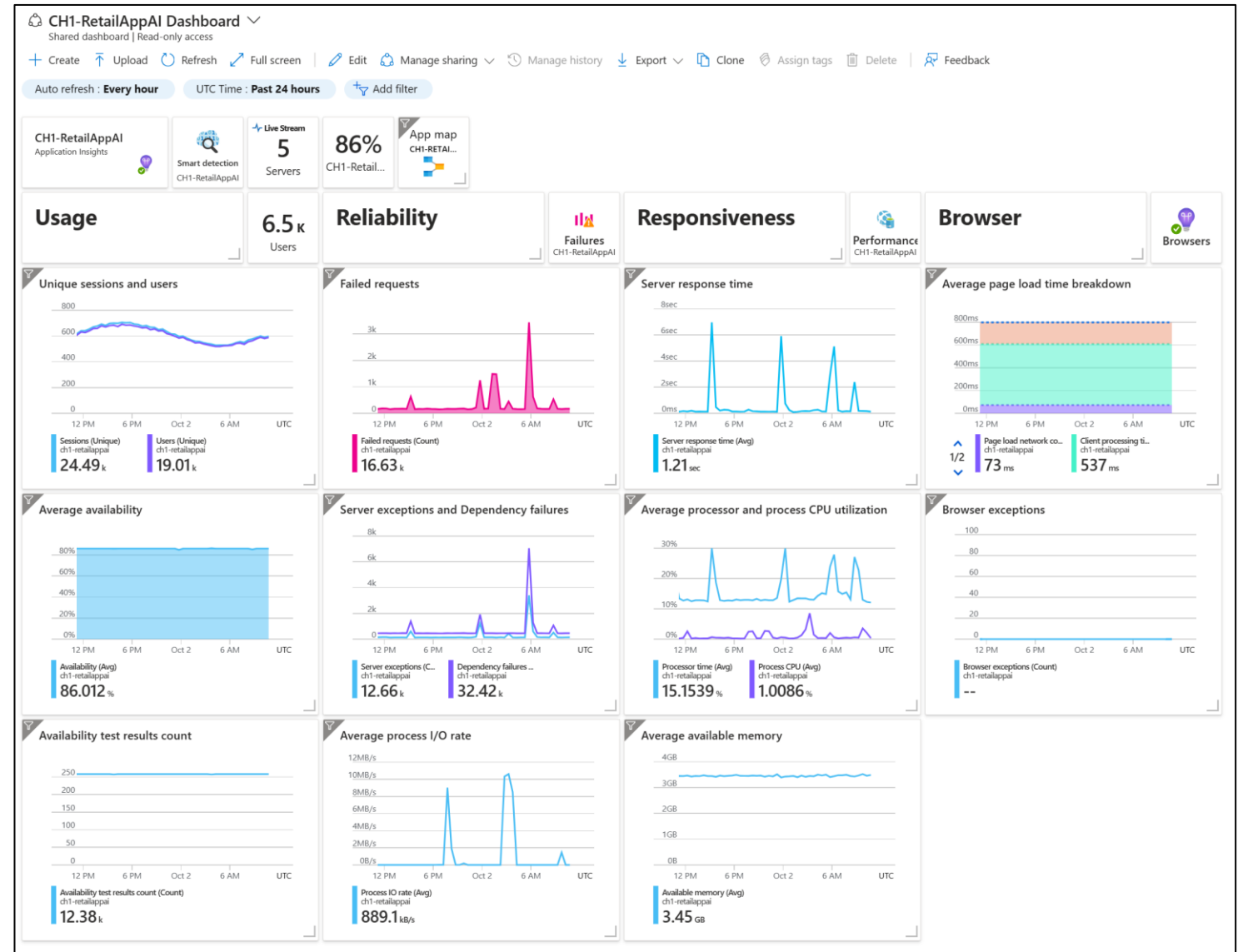
- Near real-time alerts & notifications
- Multi-dimensional metrics
- Health & availability monitoring
- Azure dashboards

Insights – find and fix problems

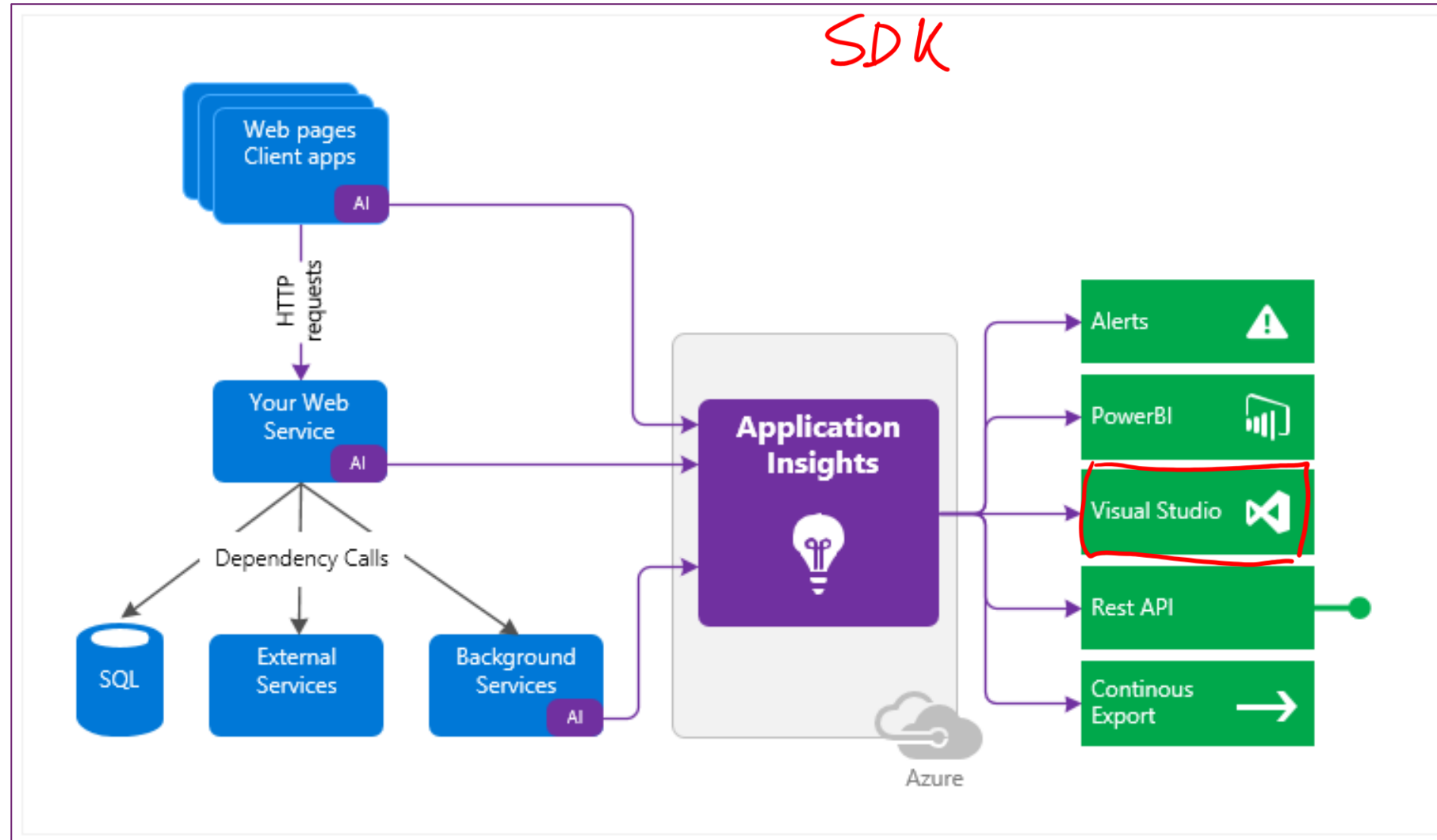
- Detect, diagnose & debug failures
- Distributed maps & transaction tracing
- Advanced analytics with ML
- Automated actions & remediations

Optimization

- Performance optimization & profiling
- User behavior & customer insights
- Impact correlation
- Integration with Dev/DevOps tools



Application Insights components



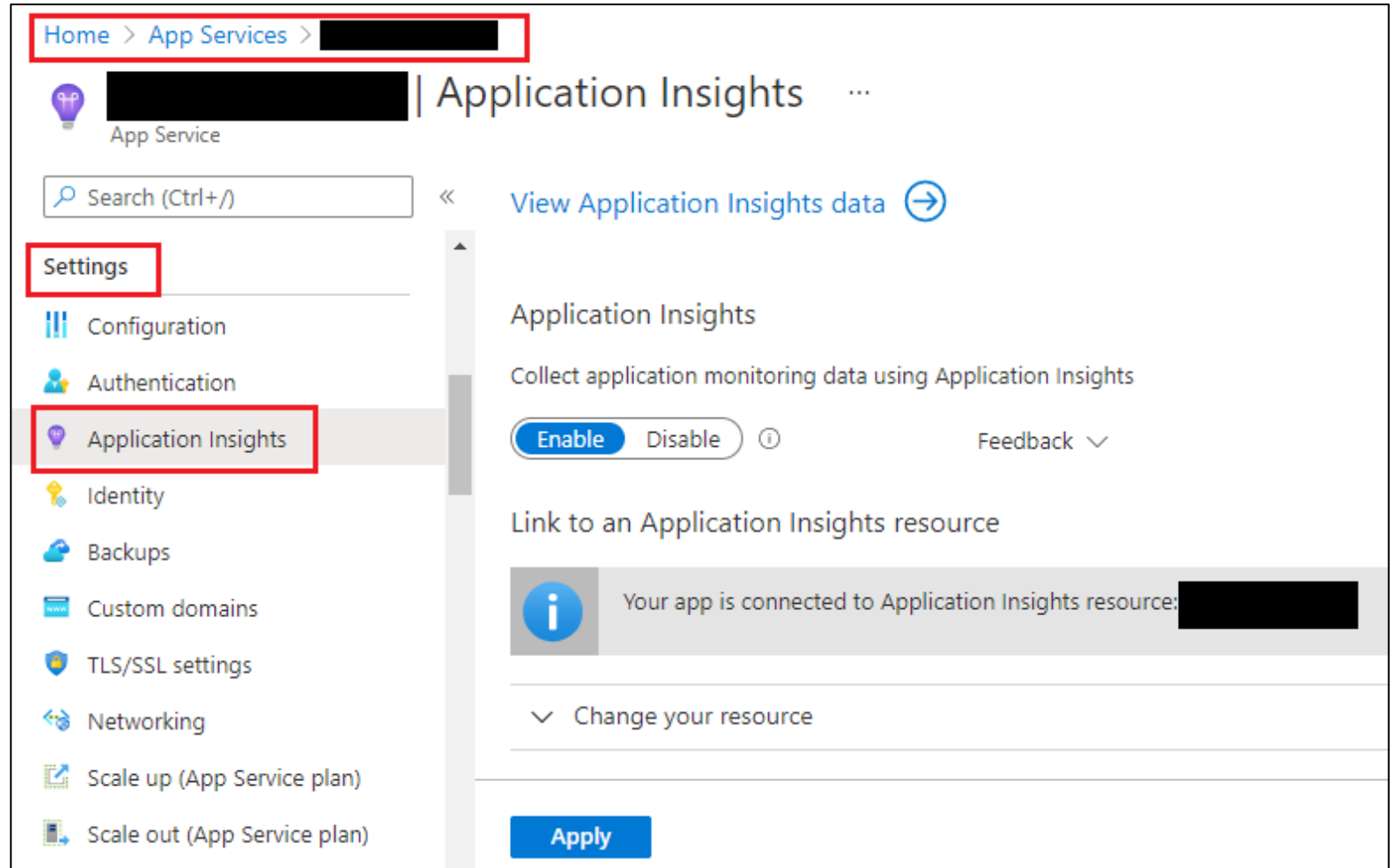
Enabling Application Insights

Codeless monitoring

- Easiest to enable, no advanced configuration is required
- Often referred to as "runtime" monitoring"
- Monitors web apps that are already running – No code changes.

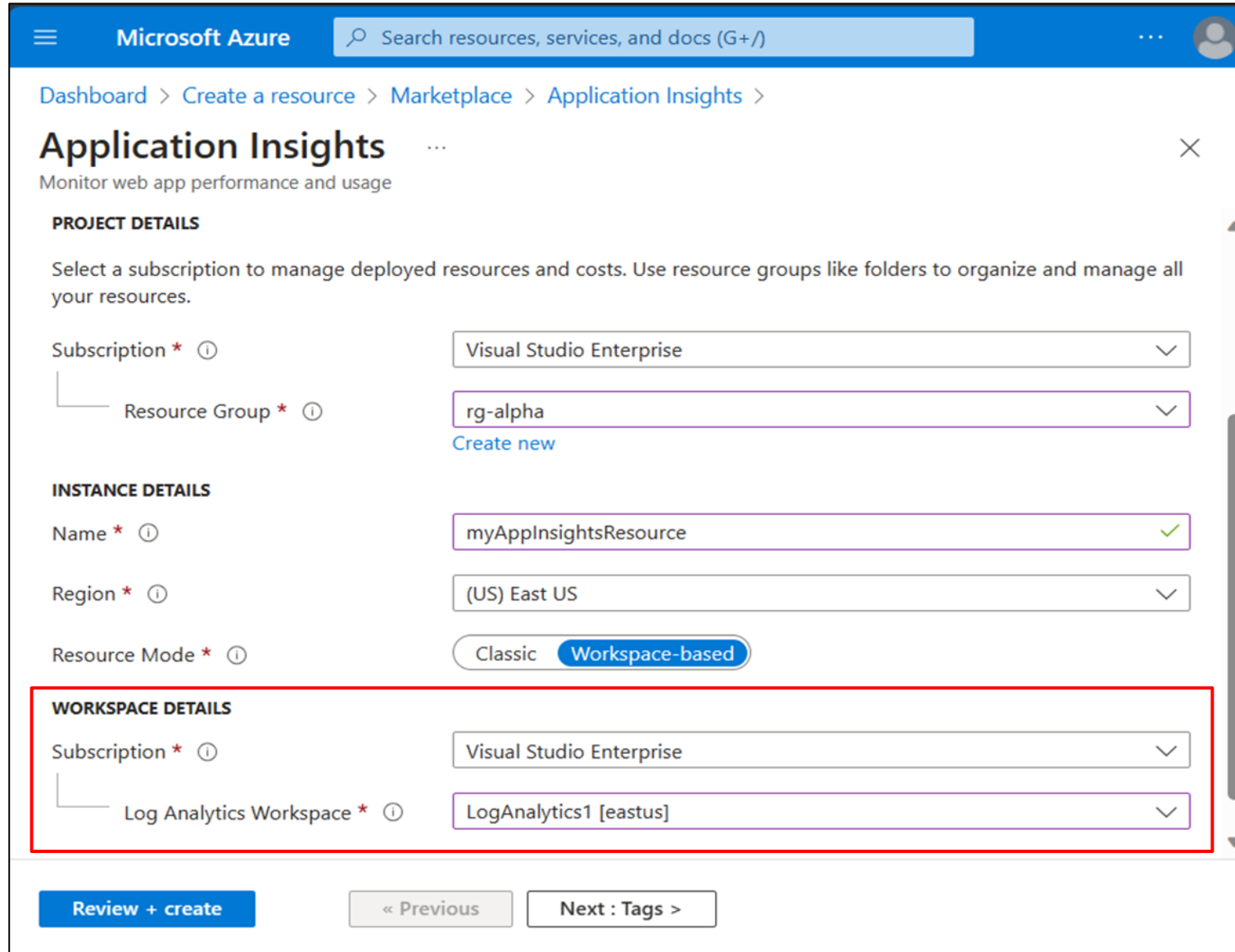
Code-based monitoring

- Requires adding Application Insights SDK
- This approach is much more customizable



Workspace-based Application Insights resources

- You can now send Application Insights telemetry to a Log Analytics Workspace.
- Use a common workspace for application, infrastructure, and platform logs without the need for cross-app/workspace queries.



Microsoft Azure

Search resources, services, and docs (G+ /)

Dashboard > Create a resource > Marketplace > Application Insights >

Application Insights

Monitor web app performance and usage

PROJECT DETAILS

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Visual Studio Enterprise

Resource Group * ⓘ rg-alpha
[Create new](#)

INSTANCE DETAILS

Name * ⓘ myAppInsightsResource ✓

Region * ⓘ (US) East US

Resource Mode * ⓘ Classic **Workspace-based**

WORKSPACE DETAILS

Subscription * ⓘ Visual Studio Enterprise

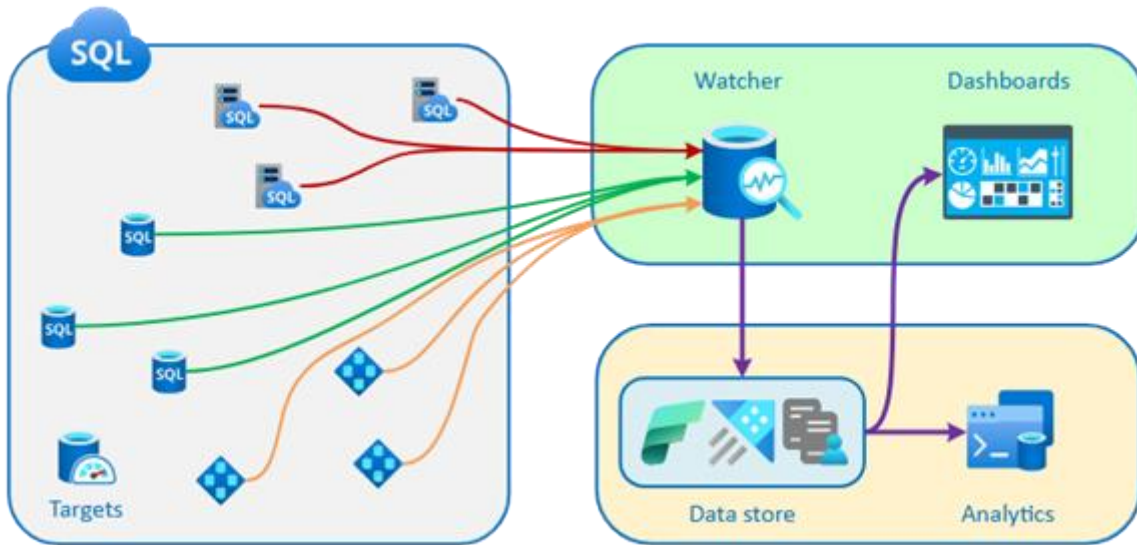
Log Analytics Workspace * ⓘ LogAnalytics1 [eastus]

[Review + create](#) [« Previous](#) [Next : Tags >](#)

Monitoring SQL workloads with database watcher (preview)

Database watcher is a managed monitoring solution for Azure SQL database services

- Collects workload monitoring data
- Provides detailed view of database performance, configuration, and health



Configure a **watcher** resource in your Azure subscription

Monitoring data stored in a central **data store**

Dashboards display detailed view of **SQL targets**, including:

- Databases
- Elastic pools
- SQL managed instances

Powered by Azure Data Explorer

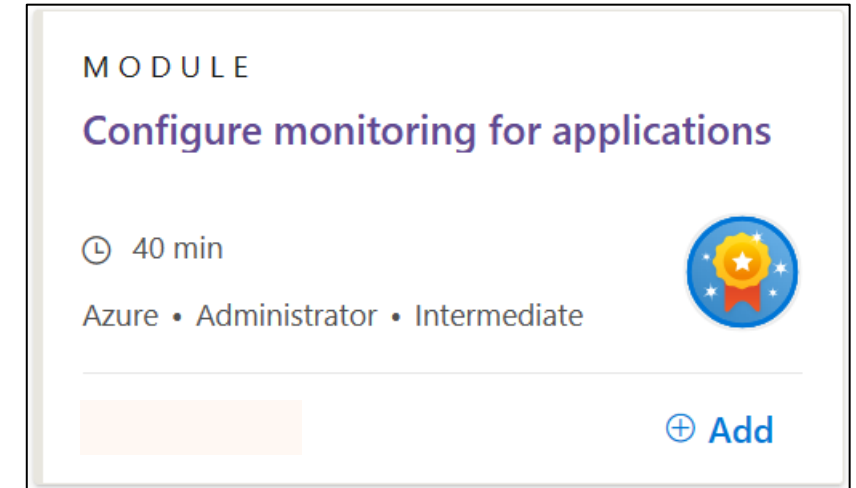
- Managed, highly scalable data service
- Fast, real-time data ingestion for analytics
- On-demand data analysis using KQL or T-SQL

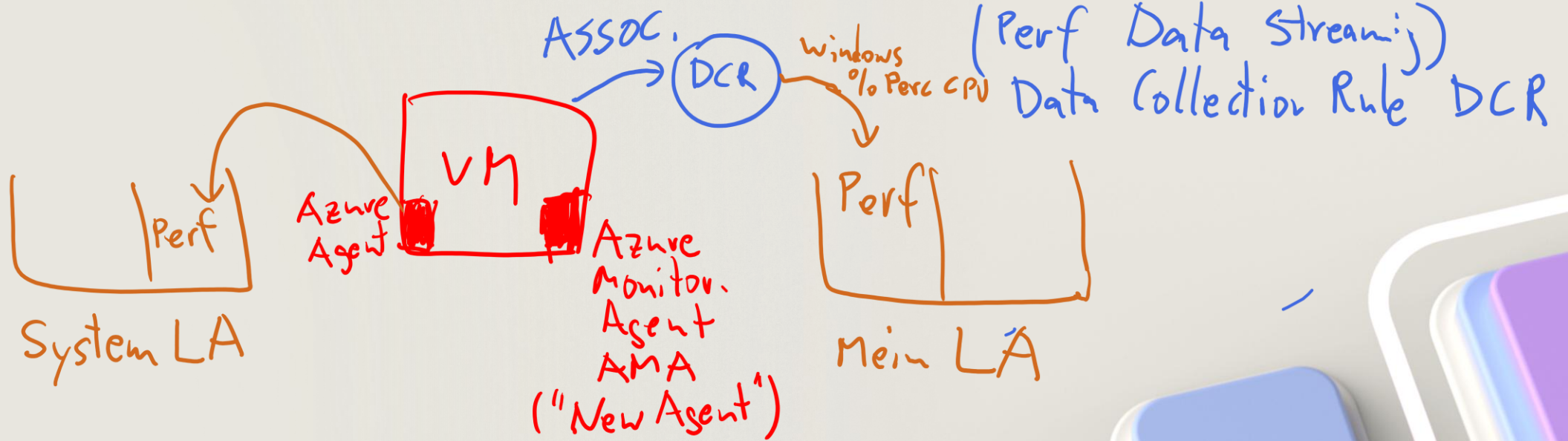
Query insights in Microsoft Fabric data

- When a SQL query runs in Microsoft Fabric, the query insights feature collects and consolidates its execution data, providing you with valuable information.
- Helps in making informed decisions to optimize the performance of Fabric Warehouse or SQL Analytics endpoint.
- Useful in the following scenarios:
 - Query performance analysis
 - Query optimization and tuning
 - User activity monitoring
- Provides a central location for history query data and actionable insights for 30 days.
- Roles - Administrator, Member, and Contributor can view complete query text.

Review questions and reference module – Configure monitoring for web apps

1. How can you monitor rates, response, times, and failure rates for web pages?
2. How can you reduce throttling when using Application Insights to monitor applications?
3. What can you use to dynamically collect resource logs based on predefined groupings instead of individually?
4. What are the two solutions that database watcher can use to store and analyze SQL monitoring data?





Configure monitoring for virtual machines

What does Azure Monitor Agent do?

"New"

Pre-Azure Monitor Agent ✗

Historically, multiple monitoring agents exist for different monitoring needs

Multiple agents required just to gain visibility into different systems

Difficult to centrally manage and obtain information at a granular level

Azure Monitor Agent solves this

Azure Monitor Agent (AMA) functions as one agent to send data to Azure Monitor

AMA works with **data collection rules** (DCRs) to configure data collection for Azure Monitor

Zero configuration required to install the agent as its just a VM extension

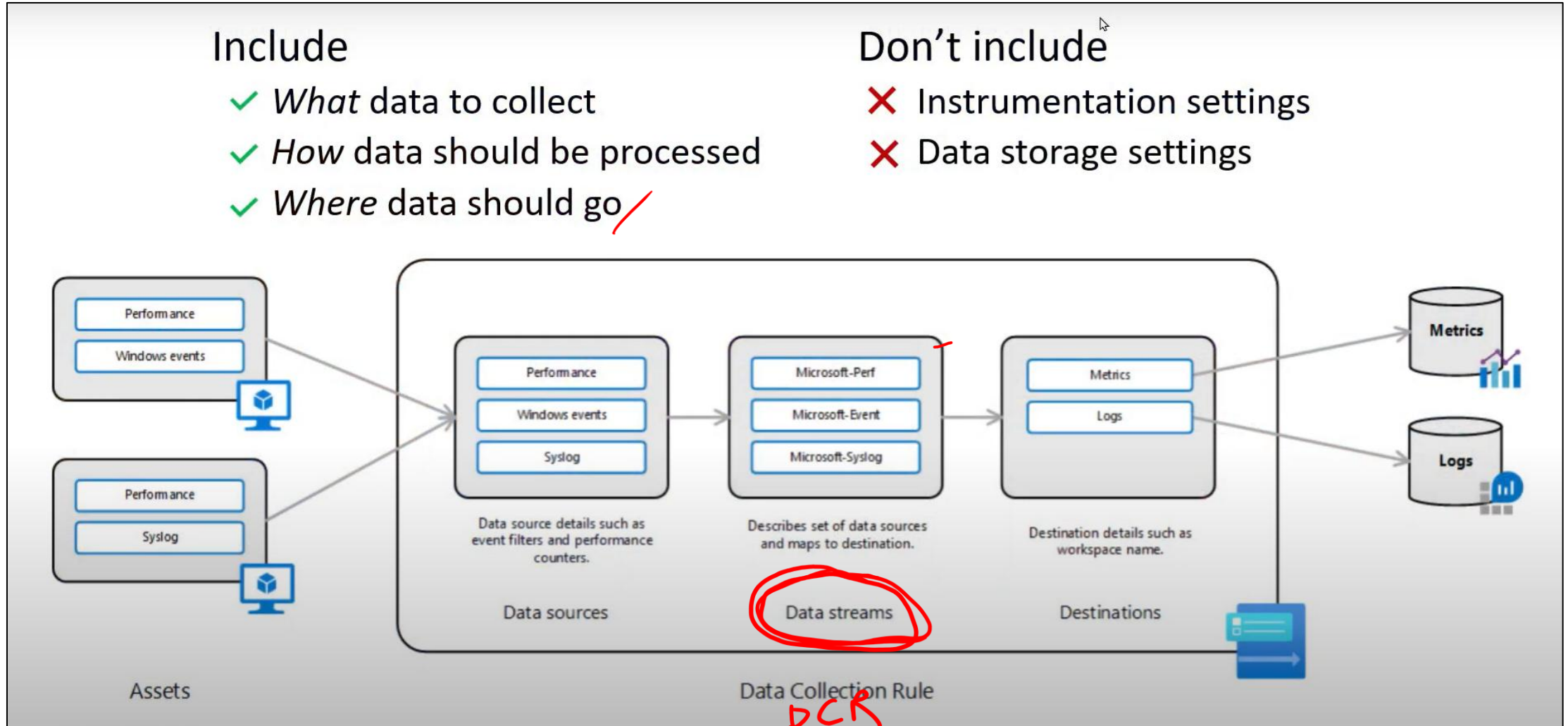
Data collection rules

Include

- ✓ *What* data to collect
- ✓ *How* data should be processed
- ✓ *Where* data should go ✓

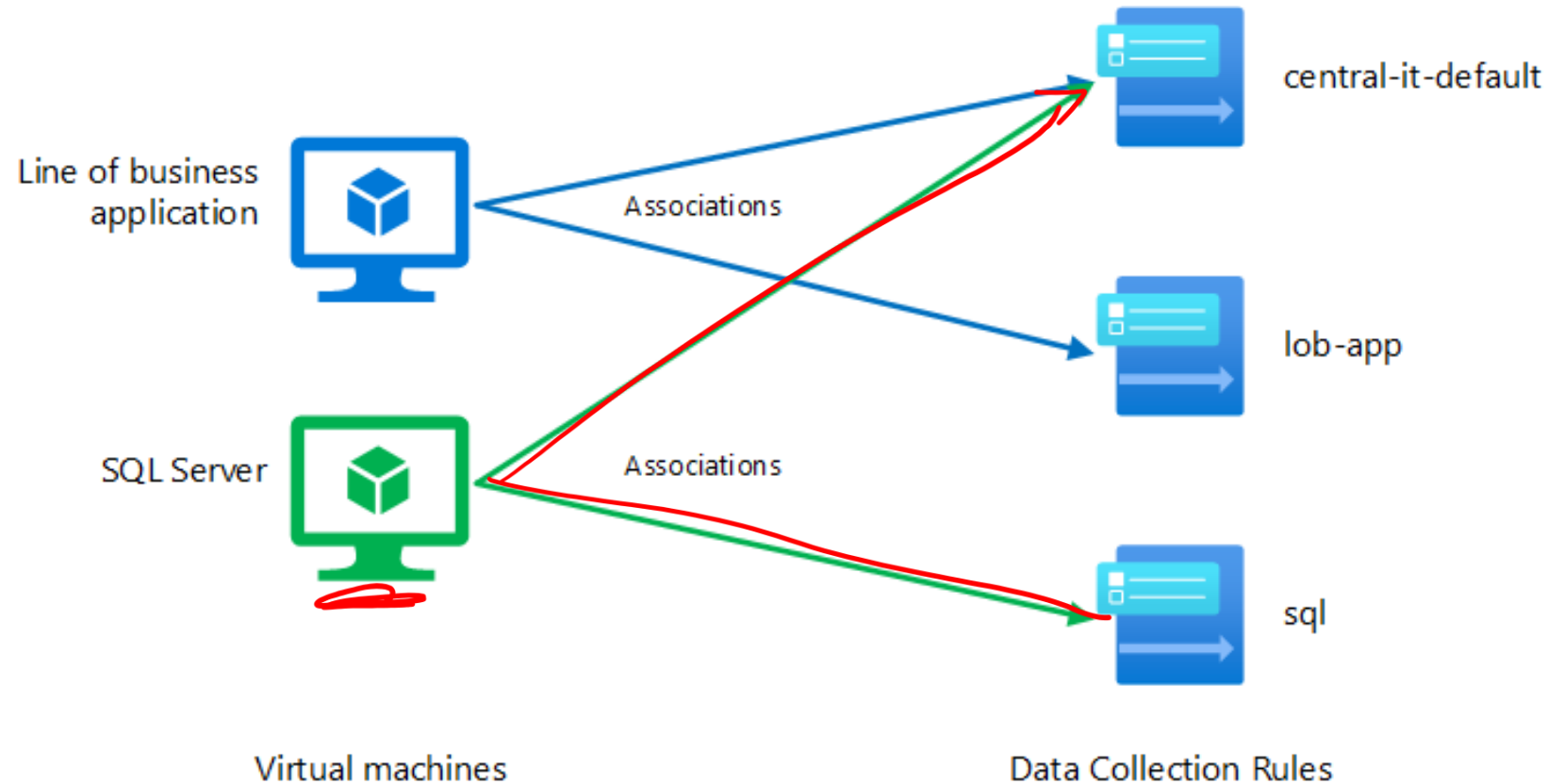
Don't include

- ✗ Instrumentation settings
- ✗ Data storage settings



Azure Monitor Agent and data collection rule associations

- Once installed, agents must be associated with data collection rules to function.
- Creating a DCR through the portal automatically deploys AMA on an IaaS VM (if not already deployed). ✓
- Managed identity must be enabled on Azure VMs.

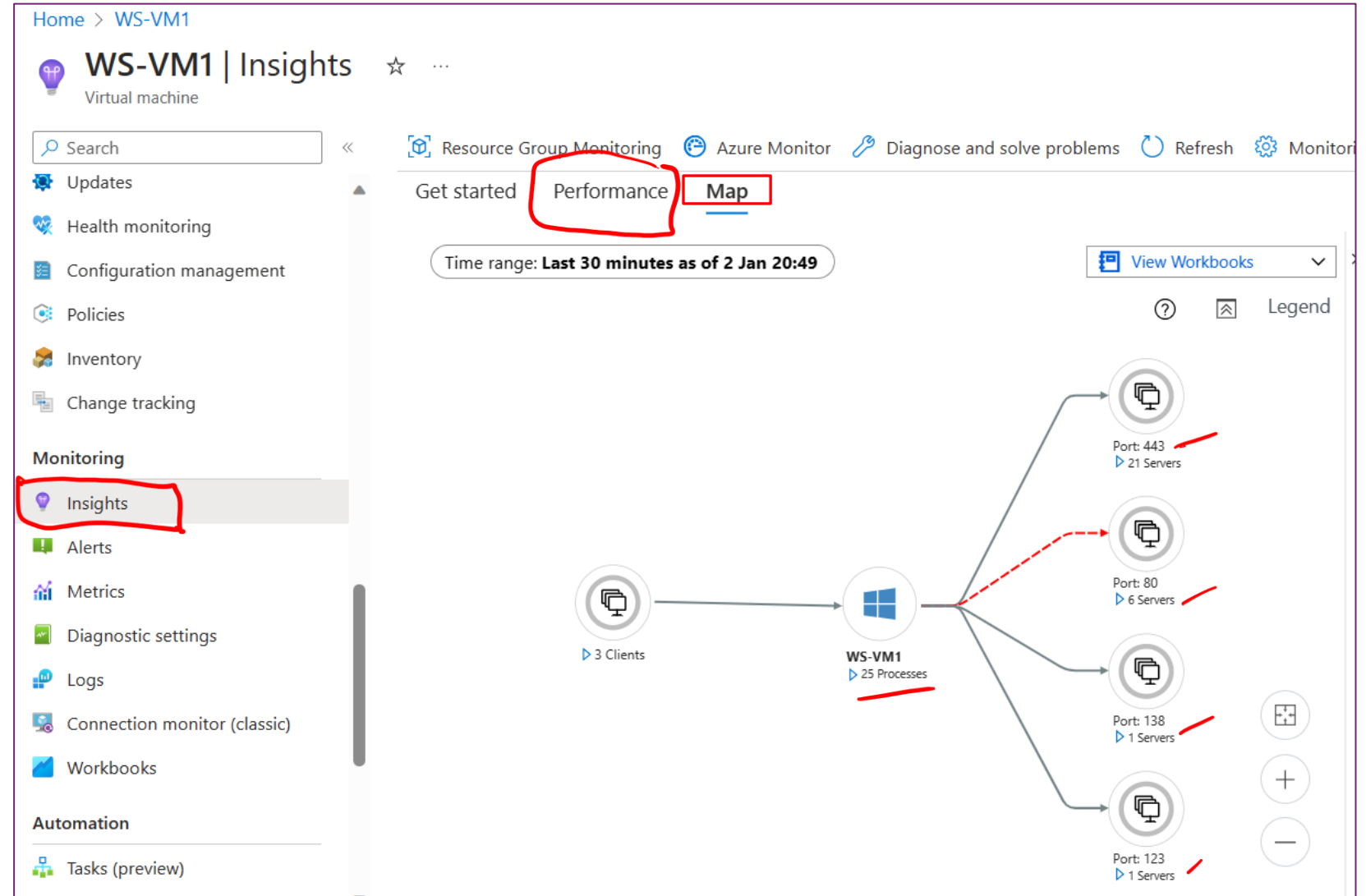


Viewing dependencies in VM insights

Use the Map feature in VM insights to view VM dependencies

Map discovers running processes that have:

- Active network connections between servers
- Inbound and outbound connection latency
- Ports across TCP-connected architecture



Review questions and reference module – Configure monitoring for VMs

1. Which agent requires Azure Monitor Agent to be installed on the same machine?
2. When using Map to view virtual machine dependencies, when would you use Azure Monitor over VM Insights?
3. When configuring a syslog collection using data collection rules, what data source should you specify?
4. When you enable VM insights, what does the default data collection rule not include?

MODULE

Configure monitoring for virtual machines

🕒 36 min

Azure • Administrator • Intermediate



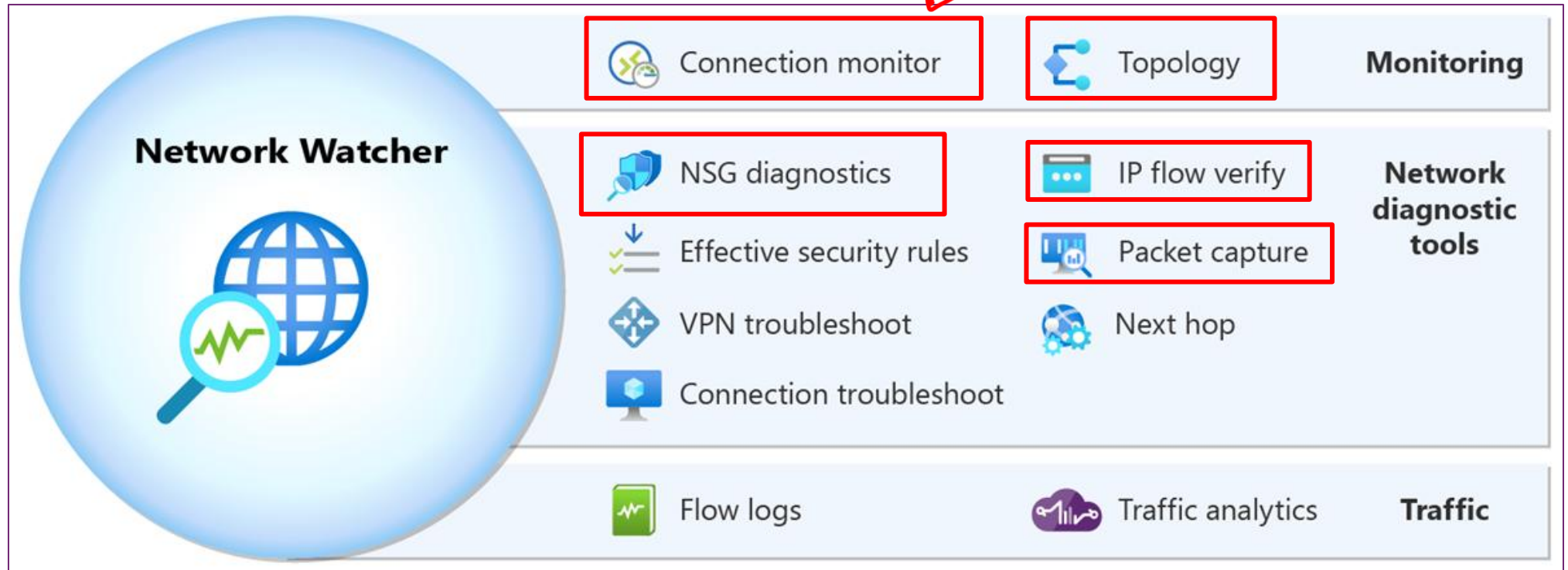
⊕ Add

Configure monitoring for virtual networks



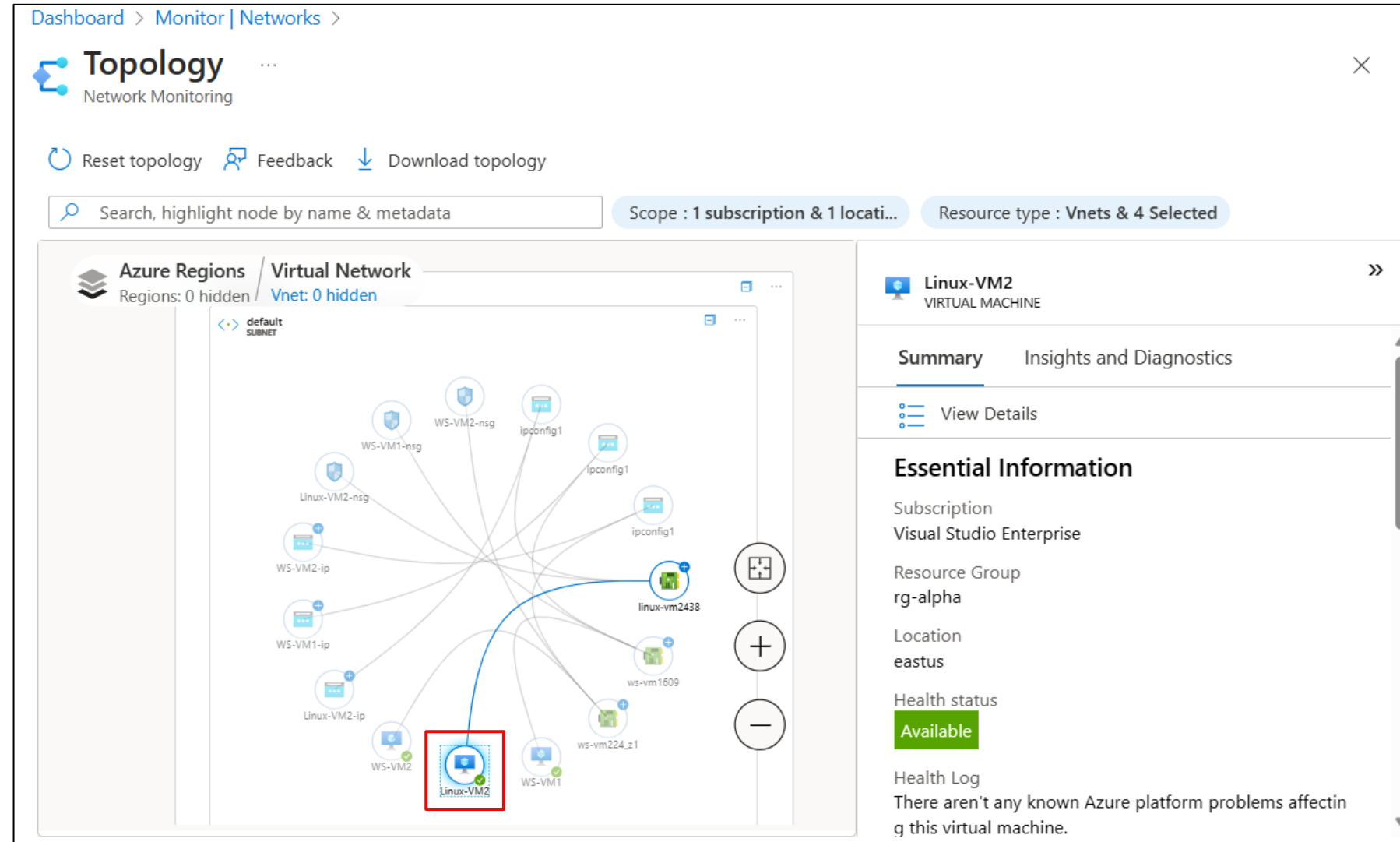
Overview of Azure Network Watcher

Suite of tools to monitor, diagnose, view metrics, enable/disable logs, and repair the network health of IaaS resources



View the topology of an Azure virtual network

- Visualize entire network configuration
- Provides interactive view of resources and their relationships in Azure
- Drill down to individual resources for component-level visualization



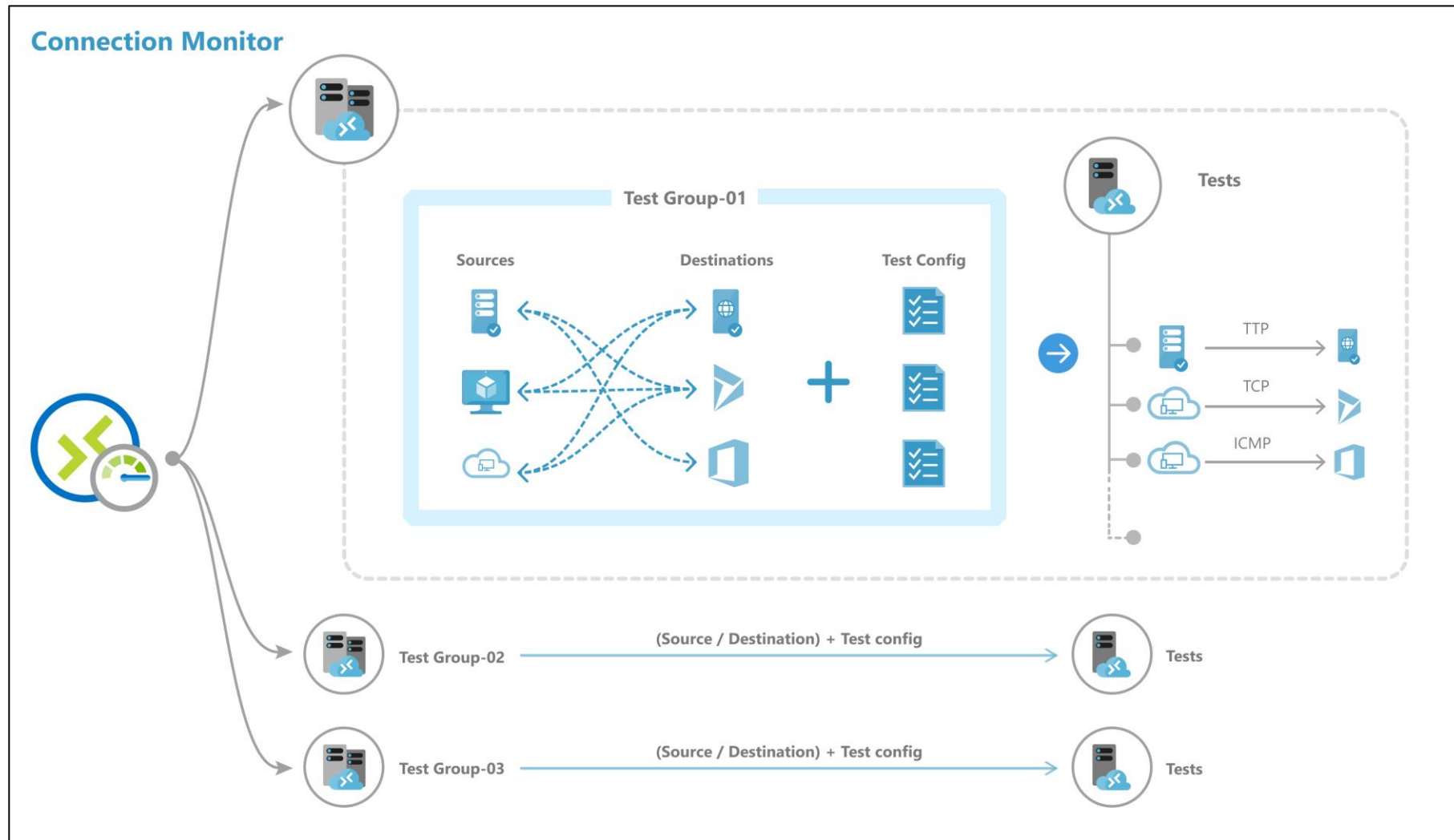
Connection Monitor

Multi-agent solution

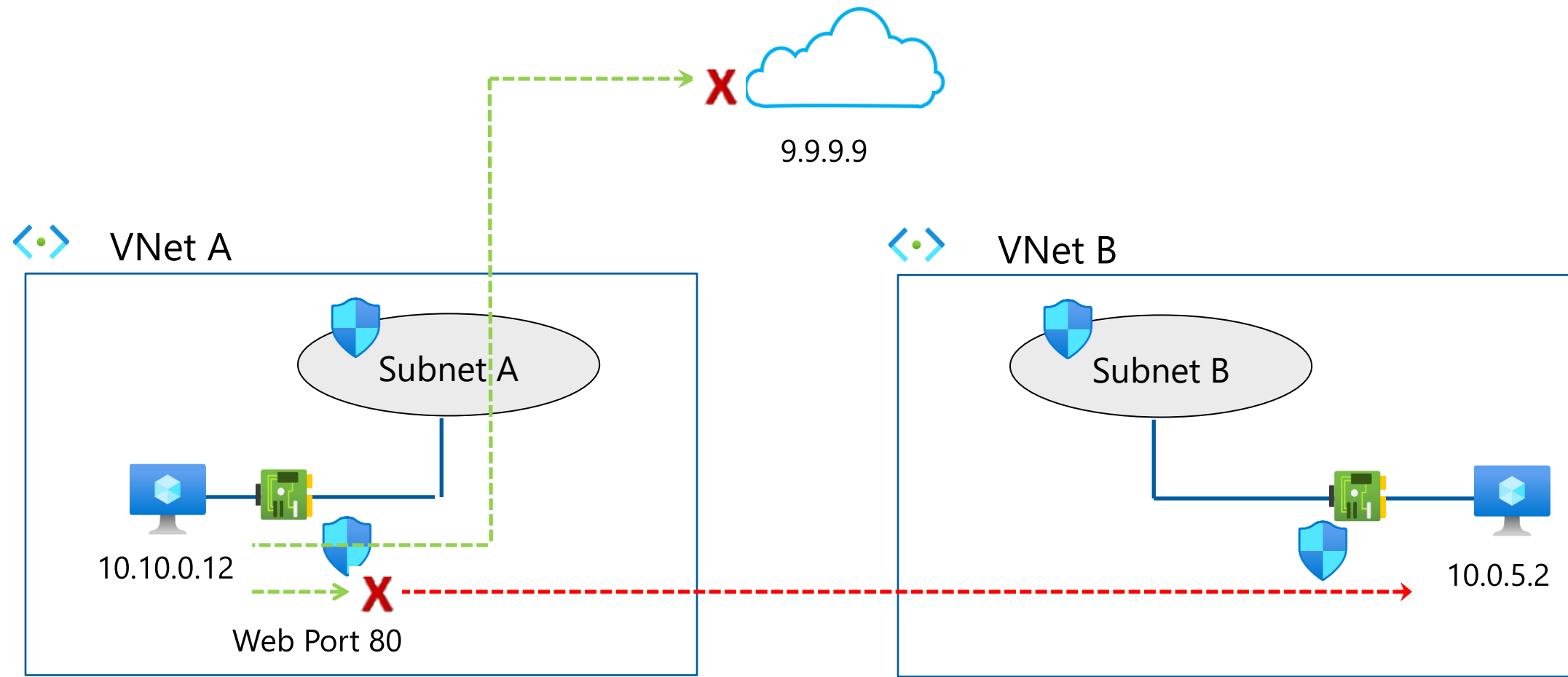
Monitors connectivity
at regular intervals
across Azure and
Hybrid endpoints

Provides aggregated
data for:

- Packet loss
- Latency
- Status codes over TCP, ICMP, and HTTP(s) pings



IP flow verify



NSG diagnostics

NSG diagnostics tool can simulate a given flow based on the source and destination provided.

Returns whether flow is allowed or denied with detailed information about the security rule allowing or denying flow.

Network Watcher | NSG diagnostics

Microsoft

Search

Overview

Get started

Monitoring

Topology

Connection monitor (classic)

Connection monitor

Network Performance Monitor

Network diagnostic tools

IP flow verify

NSG diagnostics

Next hop

Effective security rules

VPN troubleshoot

Packet capture

Connection troubleshoot

Metrics

Usage + quotas

The Network Security Group Diagnostics tool provides detailed information to understand and debug the security configuration of your network. For a given source-destination pair, network security group diagnostics returns all network security groups that will be traversed, the rules that will be applied in each network security group, and the final allow/deny status for the flow. [Learn more.](#)

Target resource

Target resource type *
Virtual machine

Virtual machine *
myVM
[Select virtual machine](#)

Traffic details

Protocol
TCP

Direction
☒ Inbound
☐ Outbound

Source type *
IPv4 address/CIDR

IPv4 address/CIDR *
10.0.1.0/26

Destination IP address *
10.0.0.4

Destination port *
*

Run NSG diagnostic

Results

Traffic will be allowed if all NSGs allow it.

Traffic status: ⛔ Denied

NSG name	Applied to	Applied action	Additional info
GlobalRules	myVNet	✅ Allow	View details
mySubnet-nsg	mySubnet	✅ Allow	View details
myVM-nsg	myvm36	⛔ Deny	View details

Packet Capture

Advanced filtering options and fine-tuned controls

The capture can be stored in Azure Storage, on the VM's disk, or both

Analyze the capture file using several standard network capture analysis tools

Home > Network Watcher

Network Watcher | Packet capture

Microsoft

Search

+ Add Refresh

Subscription ⓘ

Filter by name or target All subscriptions

Name	Target	Status	Start time
WS-VM1_1	WS-VM1	Stopped	1/9/2024, 6:10:54 PM

Network diagnostic tools

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

Review questions and reference module – Configure monitoring for VNets

1. What tool should you use to compare latencies for branch office sites for Microsoft 365 URLs?
2. When using Next Hop what route table is returned in the case where a route is not defined using a user-defined route?
3. What do you need to create for all regions in which you plan to run IP flow verify?
4. Where is Packet Capture data stored?

MODULE

Configure monitoring for virtual networks

🕒 35 min

Azure • Administrator • Intermediate



⊕ Add

Configure alerts and responses



Manage Azure Monitor alerts

Alerts

[+ New alert rule](#) [⚙ Manage alert rules](#) [👤 Manage actions](#) [🔔 View classic alerts](#) [🔄 Refresh](#) [😊 Provide feedback](#)

Total alerts
1179
Since 2/11/2020, 11:07:58 AM

Smart groups (Preview) ⓘ
3
99.75% Reduction

Total alert rules
9
Enabled 7

Action rules (preview) ⓘ
0
Enabled 0

Severity	Total Alerts	New	Acknowledged	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0
Sev 2	0	0	0	0
Sev 3	1178	1178	0	0
Sev 4	1	1	0	0

Unified authoring experience

Displayed by severity

Categorized by New, Acknowledged, and Closed

Create Alert Rules

Scope: Target selection, Alert criteria, and Alert logic

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

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

[Home](#) > [Alerts](#) >

Create alert rule

Rules management

Create an alert rule to identify and address issues when important conditions are found in your monitoring data. When defining the alert rule, check that your inputs do not contain any sensitive content.

Scope

Select the target resource you wish to monitor.

Resource

No resource selected yet

[Select resource](#)

Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name

No condition selected yet

Action group

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group

Action group name

No action group selected yet

Create 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

Notifications

Configure the method in which users will be notified when the action group triggers. Select notification types, provide receiver details and add a unique description. This step is optional.

Notification type ⓘ	Name ⓘ	Selected ⓘ
<div><div></div><div>Email Azure Resource Manager Role</div><div>Email/SMS message/Push/Voice</div></div>	<div></div>	

Actions

Configure the method in which actions are performed when the action group triggers. Select action types, fill out associated details, and add a unique description. This step is optional.

Action type ⓘ	Name ⓘ	Selected ⓘ
<div><div></div><div>Automation Runbook</div><div>Azure Function</div><div>ITSM</div><div>Logic App</div><div>Secure Webhook</div><div>Webhook</div></div>	<div></div>	

Review questions and reference module – Configure alerts and responses

1. Which built-in Azure roles have the required permissions to access alerts information and create alerts?
2. Which region option should you choose to ensure that the processing of your action group is performed within a specific geographic boundary?
3. What elements are required to define alert actions?
4. What should you do if you want to suppress alert notifications during planned maintenance?

MODULE

Configure alerts and responses

🕒 24 min

Azure • Administrator • Intermediate

⊕ Add



End of presentation

