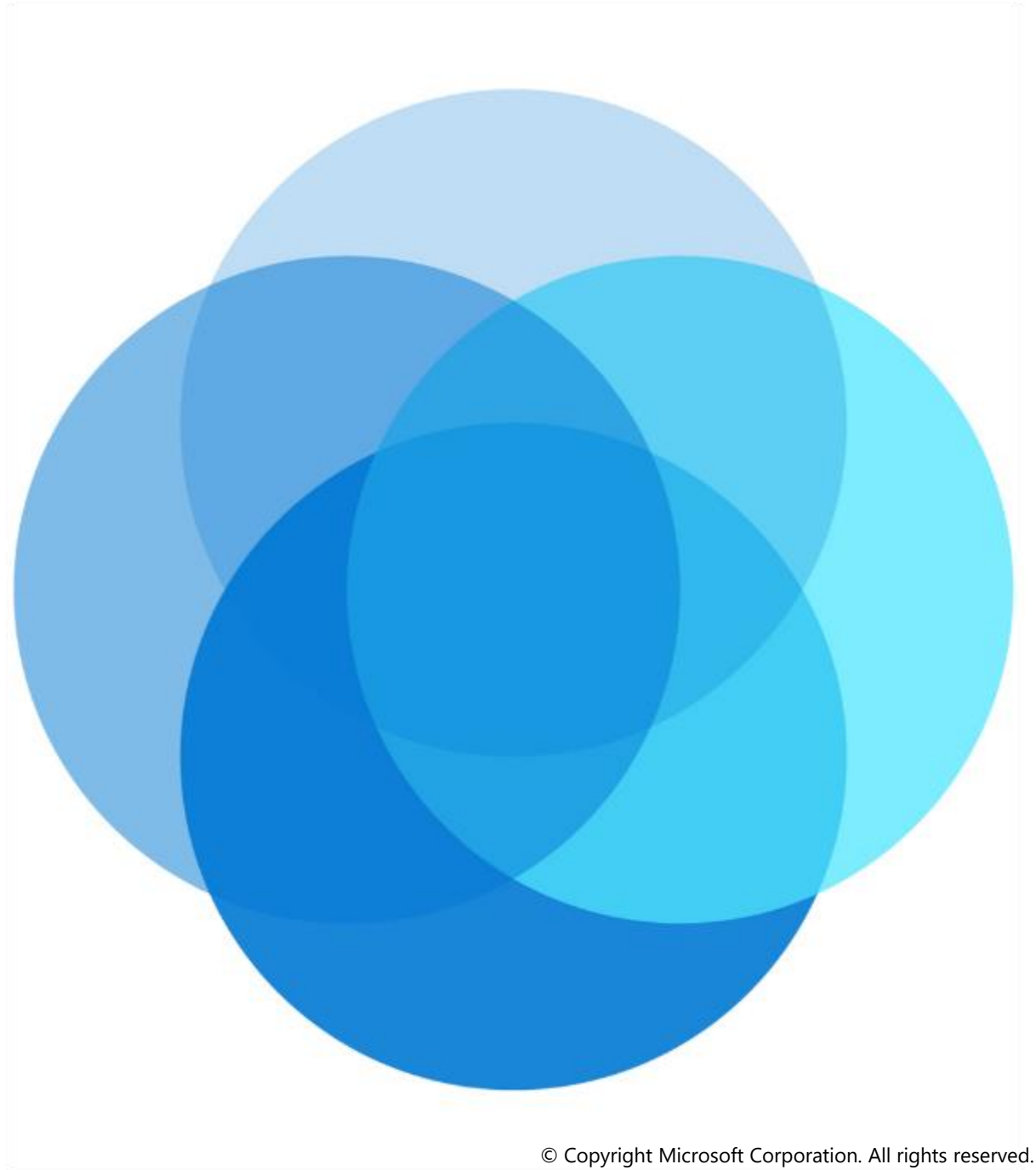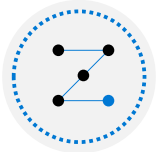Microsoft Azure

AZ-104

Administer Monitoring

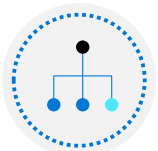# About this course: Course Outline

01: Administer Identity
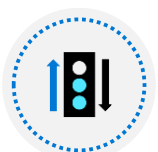
02: Administer Governance and Compliance

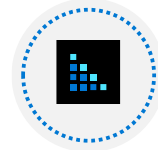03: Administer Azure Resources

04: Administer Virtual Networking

05: Administer Intersite Connectivity

06: Administer Network Traffic Management

07: Administer Azure Storage
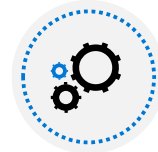
08: Administer Azure Virtual Machines

09: Administer PaaS Compute Options

10: Administer Data Protection
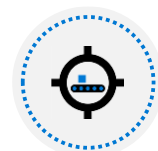
11: Administer Monitoring

Administer Monitoring Introduction
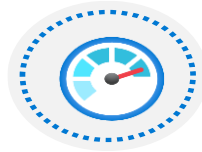
Configure Azure Monitor

Configure Azure Alerts

Configure Log Analytics

Lab 11 – Implement Monitoring
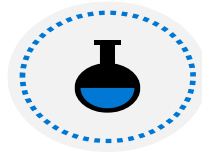
Handwritten annotations:
2%
Event
Action Group
Function
Logic App
Workspace
Kusto
KQL

Configure Azure Monitor

Configure Azure Monitor Introduction
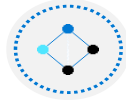
- Describe Azure Monitor Key Capabilities
- Describe Azure Monitor Components
- Define Metrics and Logs
- Identify Data Types
- Describe Activity Log Events
- Query the Activity Log
- Summary and Resources

Describe Azure Monitor 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

Understand Azure Monitor Components
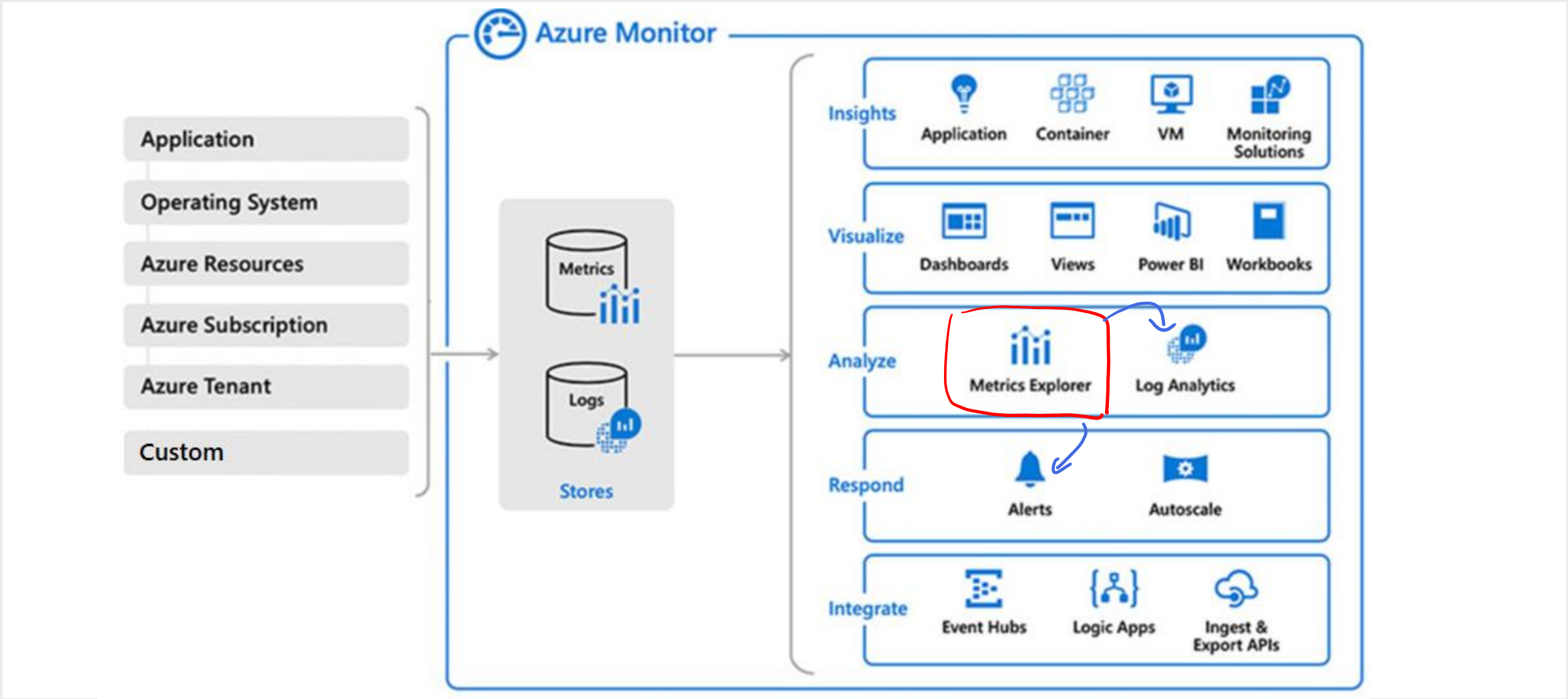
Define Metrics and Logs

Metrics → Metric Analytics

Logs → Log Analytics

- 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

Identify Data Types

→ App Insights

 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
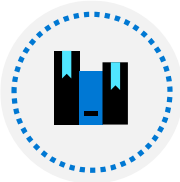
 Azure resource monitoring

 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

Describe Activity Log Events

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
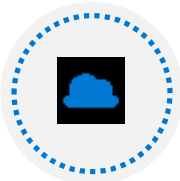
Analyze data with Power BI

Application

Application Logs

Diagnostic Logs

Guest OS

Host VM

Activity Logs

Azure Infrastructure

Compute resources only

Resource

Diagnostic Logs

Activity Logs

Azure Infrastructure

Non-Compute resources only

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

Summary and Resources – Configure Azure Monitor

Knowledge Check Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)

Monitor, diagnose, and troubleshoot your Azure storage (Sandbox)

- -

Analyze your Azure infrastructure by using Azure Monitor logs (Sandbox)

- -

Monitor and report on security events in Azure AD Docs

- -

Monitor the performance of virtual machines using Azure Monitor VM Insights (Sandbox)

A *sandbox* indicates a hands-on exercise.

Configure Azure Alerts

Configure Azure Alerts Overview

- Manage Azure Monitor Alerts
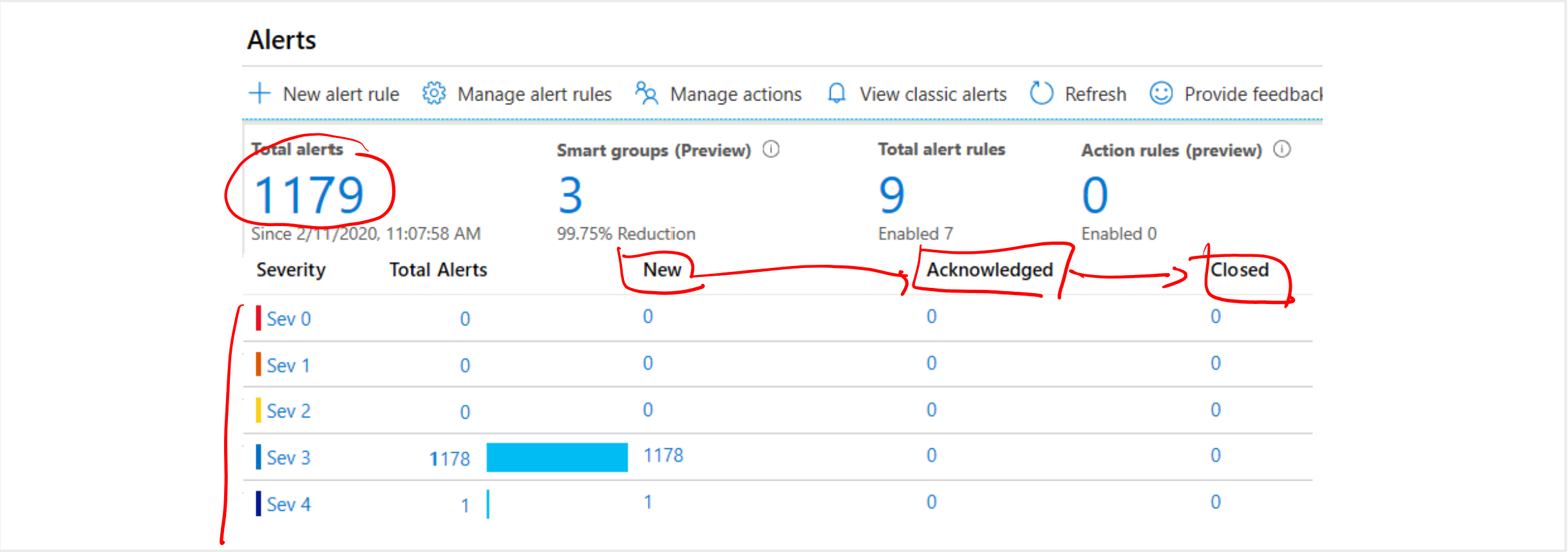- Create Alert Rules
- Create Action Groups
- Demonstration – Alerts
- Summary and Resources

Manage Azure Monitor Alerts

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

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

Demonstration – Alerts

Create an alert rule

Explore alert targets
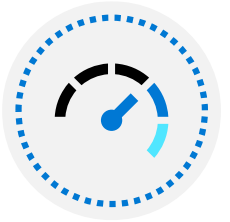
Explore alert conditions

Explore alert details

Summary and Resources – Configure Azure Alerts

Knowledge Check Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	[Improve incident response with alerting on Azure (Sandbox)](#)
	[Configure for alerts and detections in Microsoft Defender for Endpoint](#)
	[Manage alerts and incidents in Microsoft Defender for Endpoint](#)
	[Remediate security alerts using Microsoft Defender for Cloud](#)

A *sandbox* indicates a hands-on exercise.
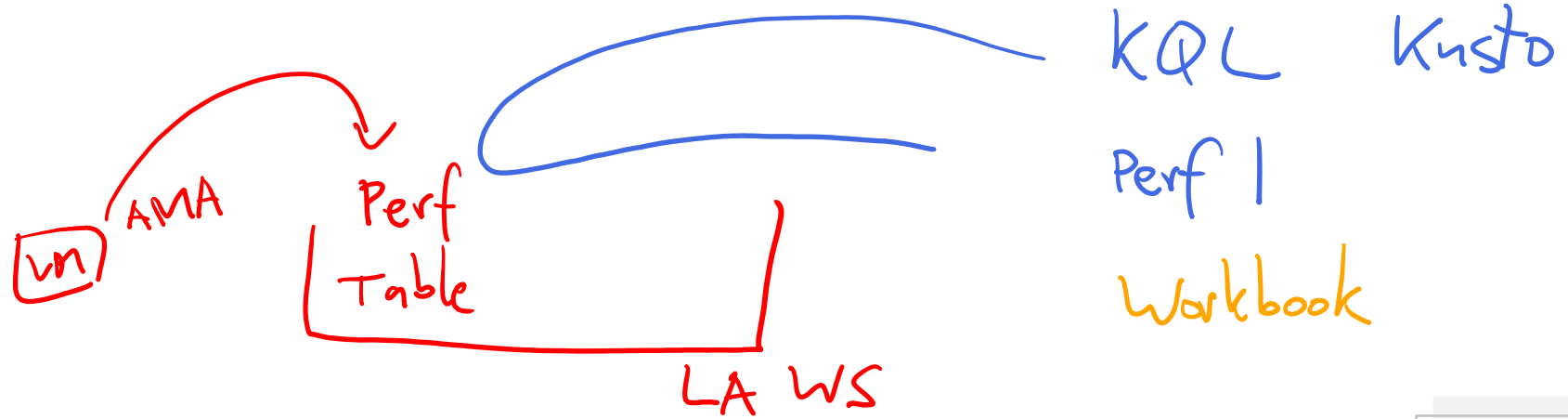
Configure Log Analytics

Configure Log Analytics Introduction

Determine Log Analytics Uses

Create a Workspace
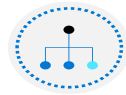
Query Log Analytics Data
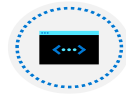
Structure Log Analytics Queries

Demonstration – Log Analytics

Summary and Resources

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

Home > Log Analytics workspaces >

Create Log Analytics workspace ...

Basics   Tags   Review + Create

ⓘ A Log Analytics workspace is the basic management unit of Azure Monitor Logs.
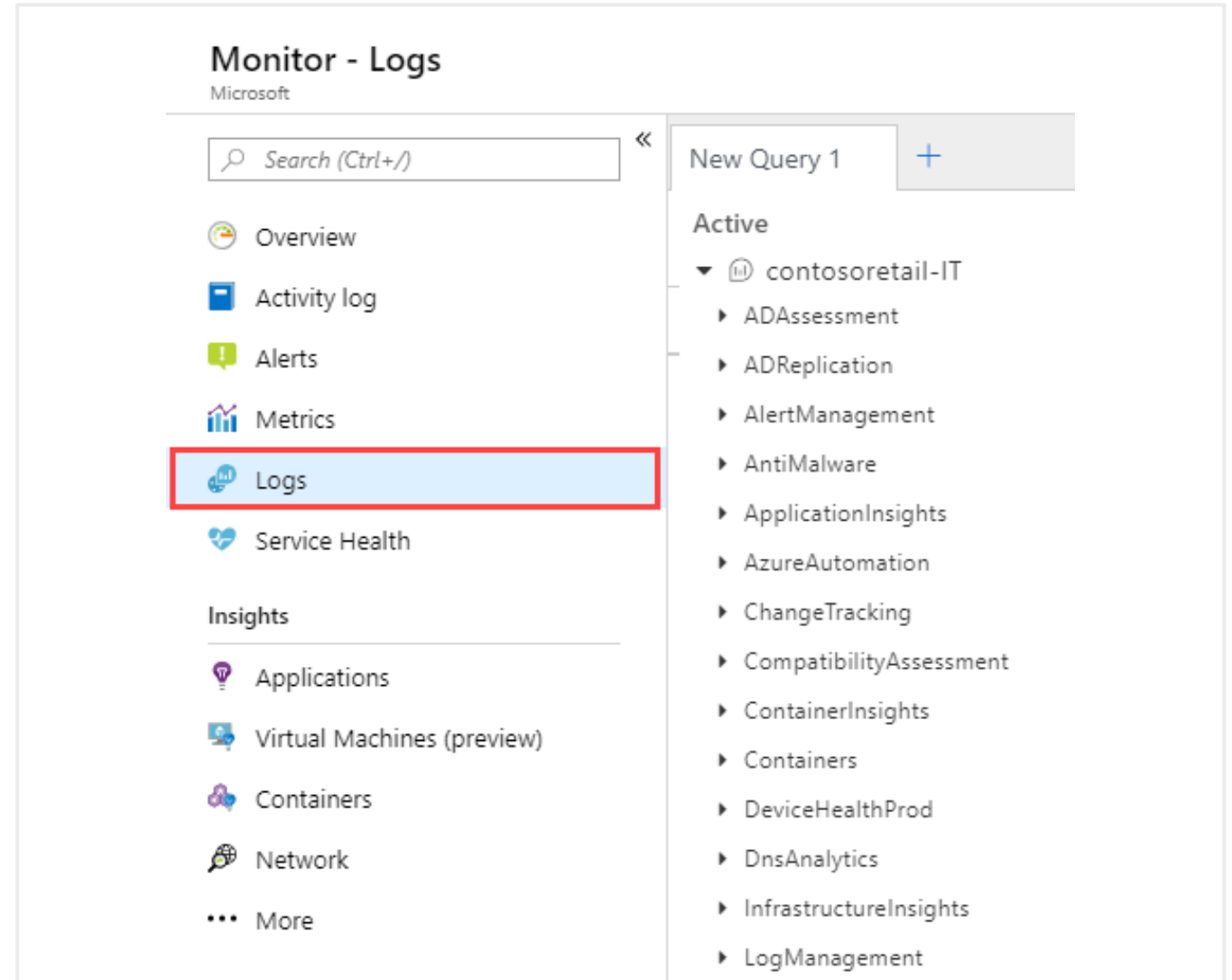There are specific considerations you should take when creating a new Log Analytics workspace.

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * ⓘ   ASC DEMO ▾

   Resource group * ⓘ   ▾

Create new

Instance details

Name * ⓘ

Region * ⓘ   East US 2 ▾

Query Log Analytics Data

Common queries and a query language for custom searches

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

Queries

Query packs: Select query packs

| Category | ∨ |

🔍 Search

Add filter

★ Favorites

All Queries

Applications

Audit

Azure Monitor

Azure Resources

Azure Virtual Deskt...

Containers

Databases

Desktop Analytics

IT & Management ...

APPLICATIONS

Response time trend

Chart request duration over the last 12 hours.

Run

Example query

Response time buckets

Show how many requests are in each performance-bucket.

Run

Example query

Structure Log Analytics Queries

KQL


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

Demonstration – Log Analytics

Access the demonstration environment

Use the Query Explorer

Summary and Resources – Configure Log Analytics

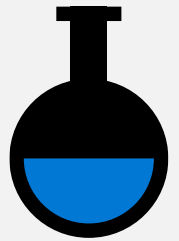| Knowledge Check Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	[Analyze your Azure infrastructure by using Azure Monitor logs (Sandbox)](#)
	[Monitor the performance of virtual machines using Azure Monitor VM Insights (Sandbox)](#)
	[Write your first query with Kusto Query Language](#)

A *sandbox* indicates a hands-on exercise.

Lab 11 – Implement Monitoring

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

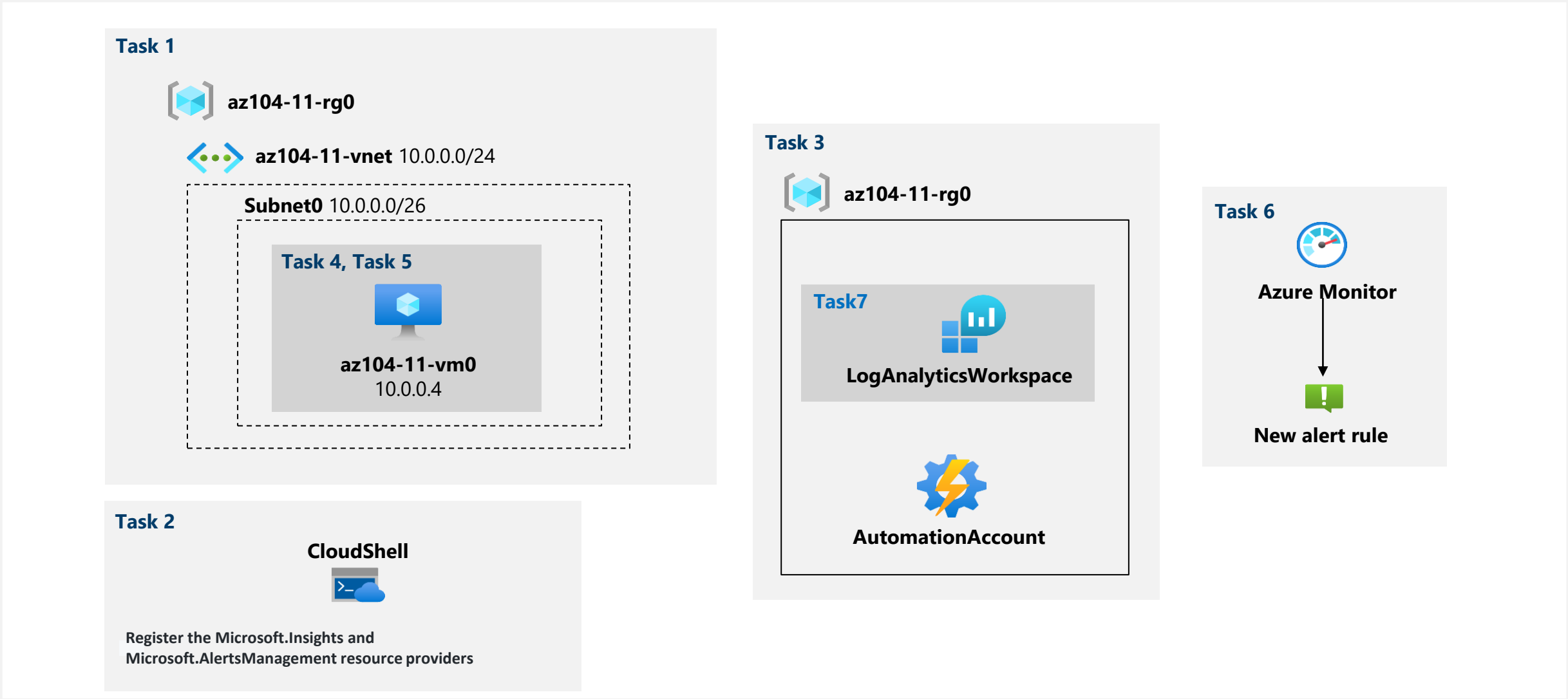| Task 1: Provision the lab environment	Task 2: Create and configure an Azure Log Analytics workspace and Azure Automation-based solutions	Task 3: Review default monitoring settings of Azure virtual machines
Task 4: Configure Azure virtual machine diagnostic settings	Task 5: Review Azure Monitor functionality	Task 6: Review Azure Log Analytics functionality

Next slide for an architecture diagram ⊖

Lab 11 – Architecture diagram

Task 1

az104-11-rg0

az104-11-vnet 10.0.0.0/24

Subnet0 10.0.0.0/26

Task 4, Task 5

az104-11-vm0
10.0.0.4

Task 2

CloudShell

Register the Microsoft.Insights and Microsoft.AlertsManagement resource providers

Task 3

az104-11-rg0

Task7

LogAnalyticsWorkspace

AutomationAccount

Task 6

Azure Monitor

New alert rule

End of presentation

Default Azure Active Directory Logs

Activity Reports

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Audit logs	Seven days	30 days	30 days
Sign-ins	Seven days	30 days	30 days
Azure AD MFA usage	30 days	30 days	30 days

Security Signals

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Risky users	No limit	No limit	No limit
Risky sign-ins	7 days	30 days	90 days

Features of Azure Monitor that are automatically enabled such as collection of standard metrics and activity logs are provided at **no cost**.

For more functionality such as longer retention, you should route the entries to another location based on your needs.

Entries in the Activity Log are system generated and cannot be changed or deleted.

Default Subscription Logs

ℹ️ Start Virtual Machine	Succeeded	a day ago	Thu Jun 09 2022 08:18:40...
ℹ️ Start Virtual Machine	Succeeded	a day ago	Thu Jun 09 2022 08:18:14...
ℹ️ Health Event Resolved	Resolved	a day ago	Thu Jun 09 2022 08:17:02...
ℹ️ Health Event Updated	Updated	a day ago	Thu Jun 09 2022 08:16:55...
ℹ️ Health Event Resolved	Resolved	a day ago	Thu Jun 09 2022 08:16:51...
ℹ️ Health Event Updated	Updated	a day ago	Thu Jun 09 2022 08:16:44...

Activity log events are retained in Azure for **90 days** and then deleted

There's **no charge** for entries during this time regardless of volume

For more functionality such as longer retention, you should route the entries to another location based on your needs

Default Metrics

Sum Server requests, Avg Server response time, and Sum Failed requests for tailspintoyswebapp

For most resources in Azure, platform metrics are stored for **93 days** at **no cost.** There are some exceptions.

You can only query (in the **Metrics** tile) for a maximum of **30 days** worth of data on any single chart.

You can send platform metrics for Azure Monitor resources to a Log Analytics workspace for long-term trending.