




AZ-104

Administer Monitoring

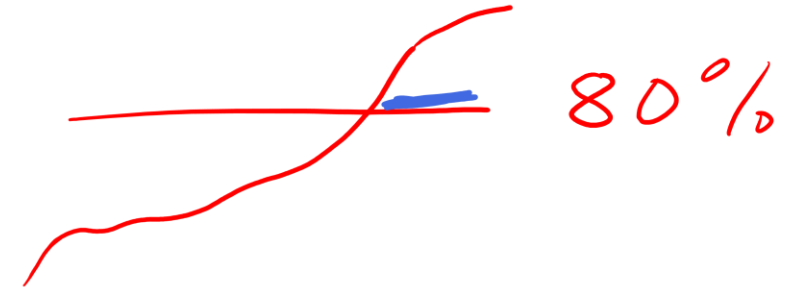
AZ-104 Course Outline

- 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 

Learning Objectives - Administer Monitoring

- Configure Azure Monitor
- Improve incident response with alerting on Azure
- Configure Log Analytics
- Lab 11 – Implement Monitoring

LAW
KQL



Configure Azure Monitor



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](#)

Core monitoring for Azure services



Query & Analyze Logs

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

[Search Logs](#)

Collects metrics, activity logs, and diagnostic logs



Setup Alert & Actions

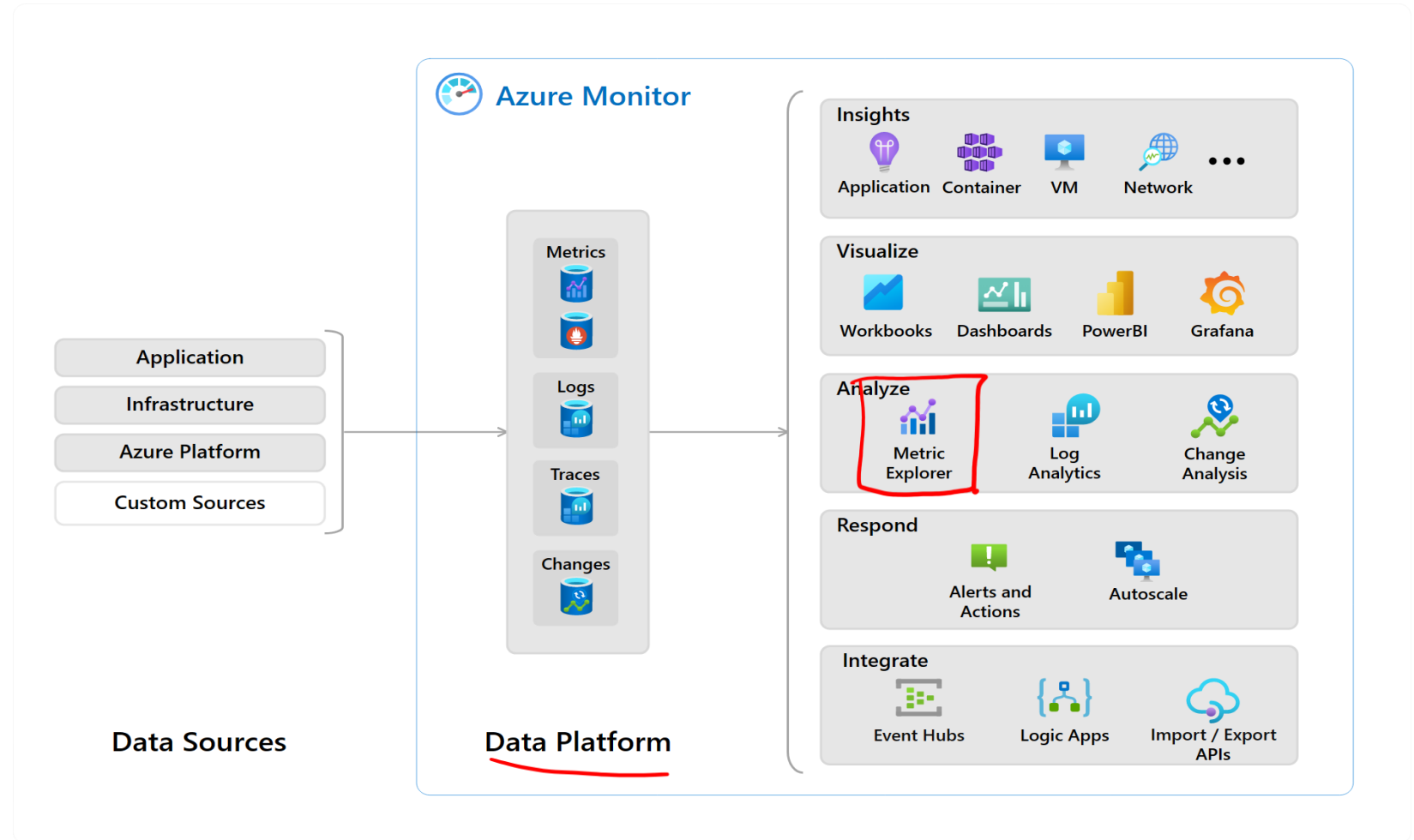
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

[Create Alert](#)

Use for time critical alerts and notifications

Understand Azure Monitor Components

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



Define Metrics and Logs



- 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

Describe Activity Log Events

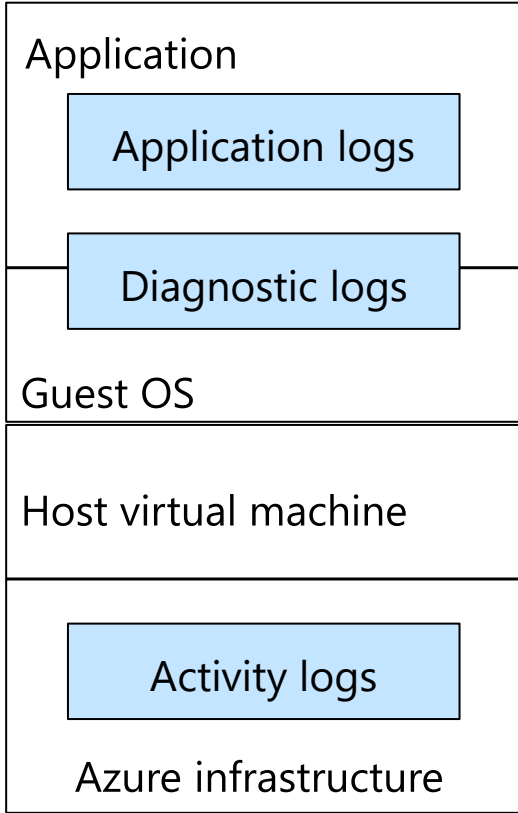
Send data to Log Analytics for advanced search and alerts

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

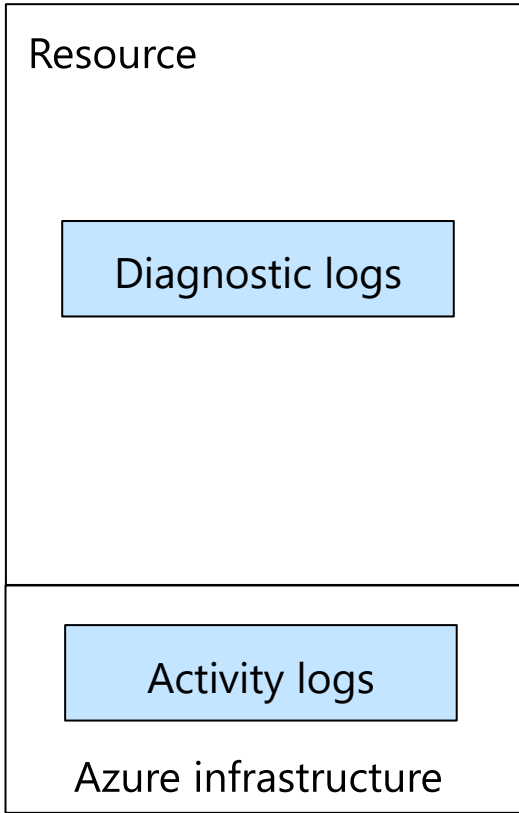
Stream information to Event Hub

Archive data to a storage account

Analyze data with Power BI



Compute
resources only



Non-compute
resources only

Query the Activity Log




Activity log

 Edit columns  Refresh  Diagnostics settings  Download as CSV  Logs |  Pin current filters

 Search

 Quick Insights  Add Filter

Management Group : **None** Subscription : **2 selected** Timespan : **Last 6 hours** Event severity : **All**

Operation name	Status	Time	Time stamp	Subscription
>  Create or Update Virtual Network Subnet	Failed	a minute ago	Thu Mar 12 ...	ASC DEMO
>  Write GuestConfigurationAssignments	Succeeded	17 minutes ...	Thu Mar 12 ...	ASC DEMO
>  Gets workflow recommend operation groups	Succeeded	29 minutes ...	Thu Mar 12 ...	ASC DEMO

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

Learning Recap – Configure Azure Monitor



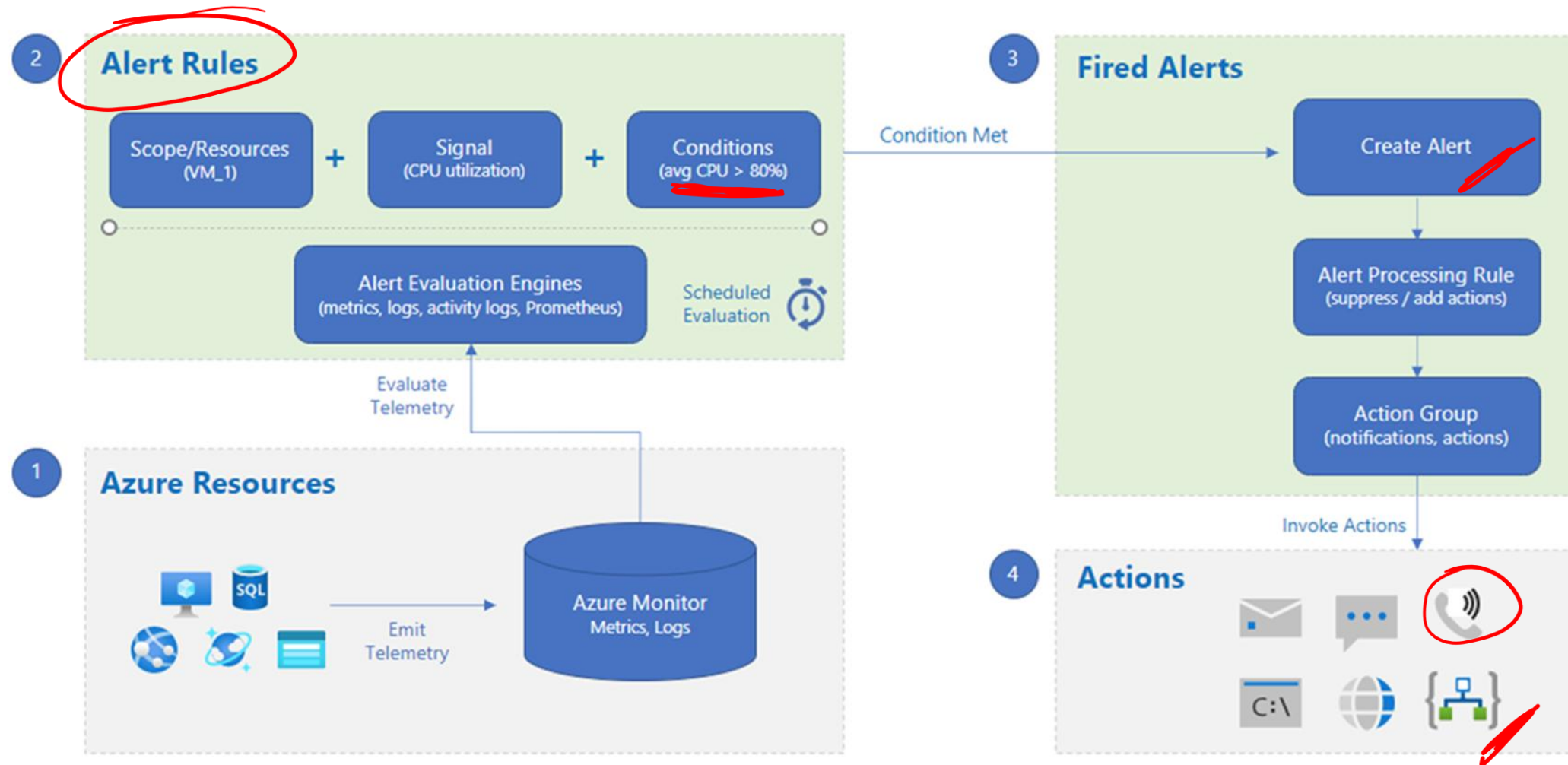
**Check your
knowledge
questions and
additional
study**

- Analyze your Azure infrastructure by using Azure Monitor logs
- Monitor your Azure virtual machines with Azure Monitor
- Monitor, diagnose, and troubleshoot your Azure storage

Improve incident response with alerting on Azure



Manage Azure Monitor Alerts



Create Alert Rules

Home > Monitor | Alerts >

Alert rules ...

Name ↑↓	Condition	Severity ↑↓	Target scope	Target resource type	Signal type ↑↓	Status ↑↓
<input type="checkbox"/> AzureSecurityCenter	Table rows > 1	4 - Verbose	export2LogA	Log Analytics workspace	Log search	✔ Enabled
<input type="checkbox"/> CPU Usage Percentage	node_cpu_usage_percentage > 80	3 - Informational	Demo	Kubernetes service	Metrics	✔ Enabled
<input type="checkbox"/> Failure Anomalies - HumanResources	Failure Anomalies detected	3 - Informational	humanresources	Application Insights	Smart detector	✔ Enabled

- Alert rules combine the resources to be monitored, the signal or data from the resource, and the conditions.
- You can enable recommended out-of-the-box alert rules in the Azure portal.

Create Action Groups

Defines a set of notifications and/or actions when an alert is triggered

You can add up to five action groups to an alert rule. Multiple alert rules can use the same action group.

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 ⓘ
---------------------	--------	------------

<input type="text"/>	<input type="text"/>	
Email Azure Resource Manager Role		
Email/SMS message/Push/Voice		

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 ⓘ
---------------	--------	------------

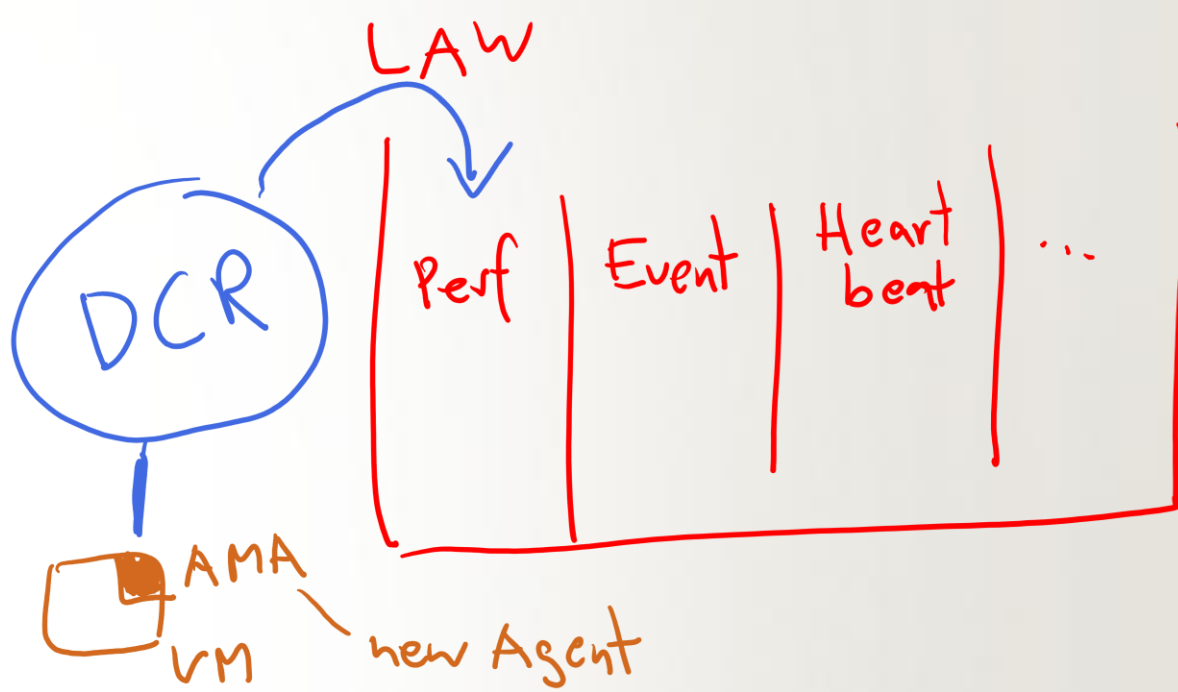
<input type="text"/>	<input type="text"/>	
Automation Runbook		
Azure Function		
Event Hub		
ITSM		
Logic App		
Secure Webhook		
Webhook		

Learning Recap – Configure Azure Alerts



**Check your
knowledge
questions and
additional
study**

- Improve incident response with alerting on Azure
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Remediate security alerts using Microsoft Defender for Cloud



DCR
Data Coll. Rule

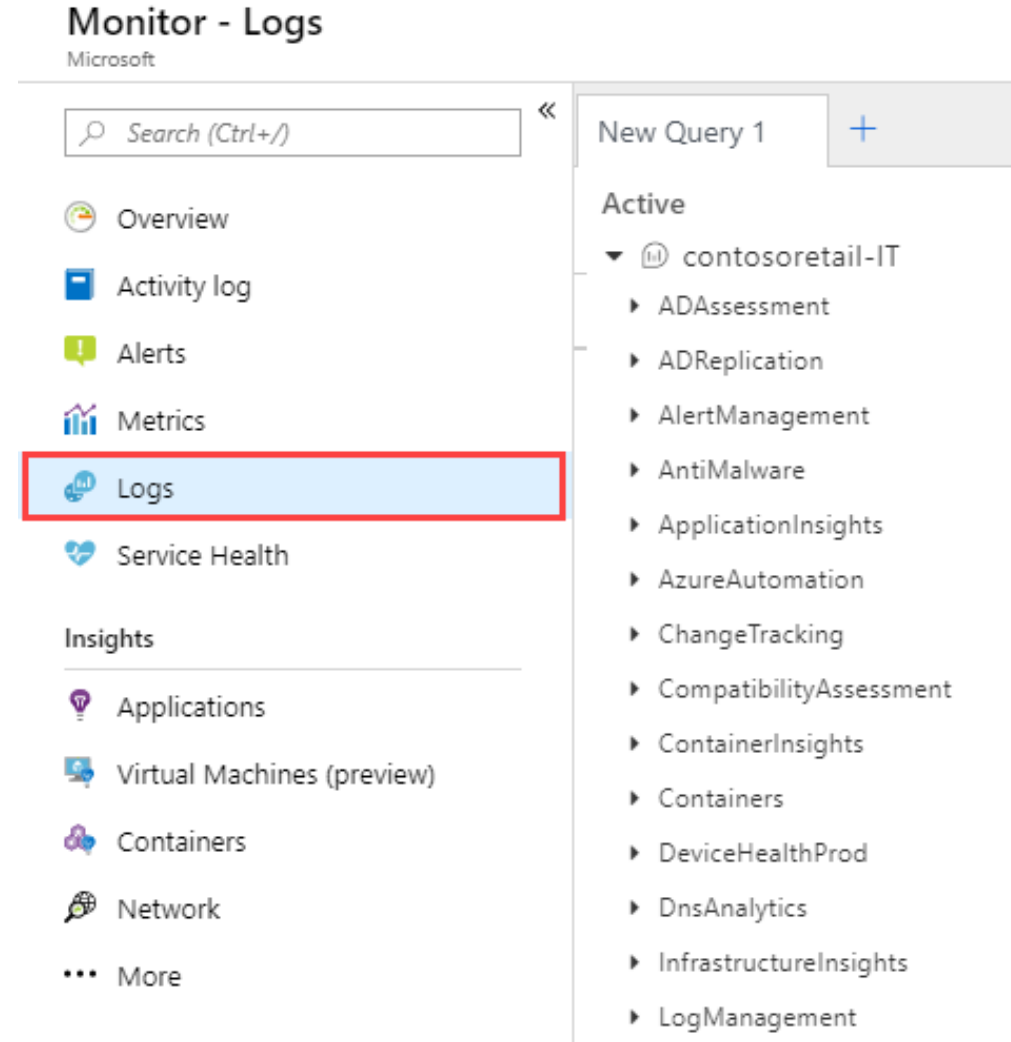
Configure Log Analytics

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 **KQL**

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



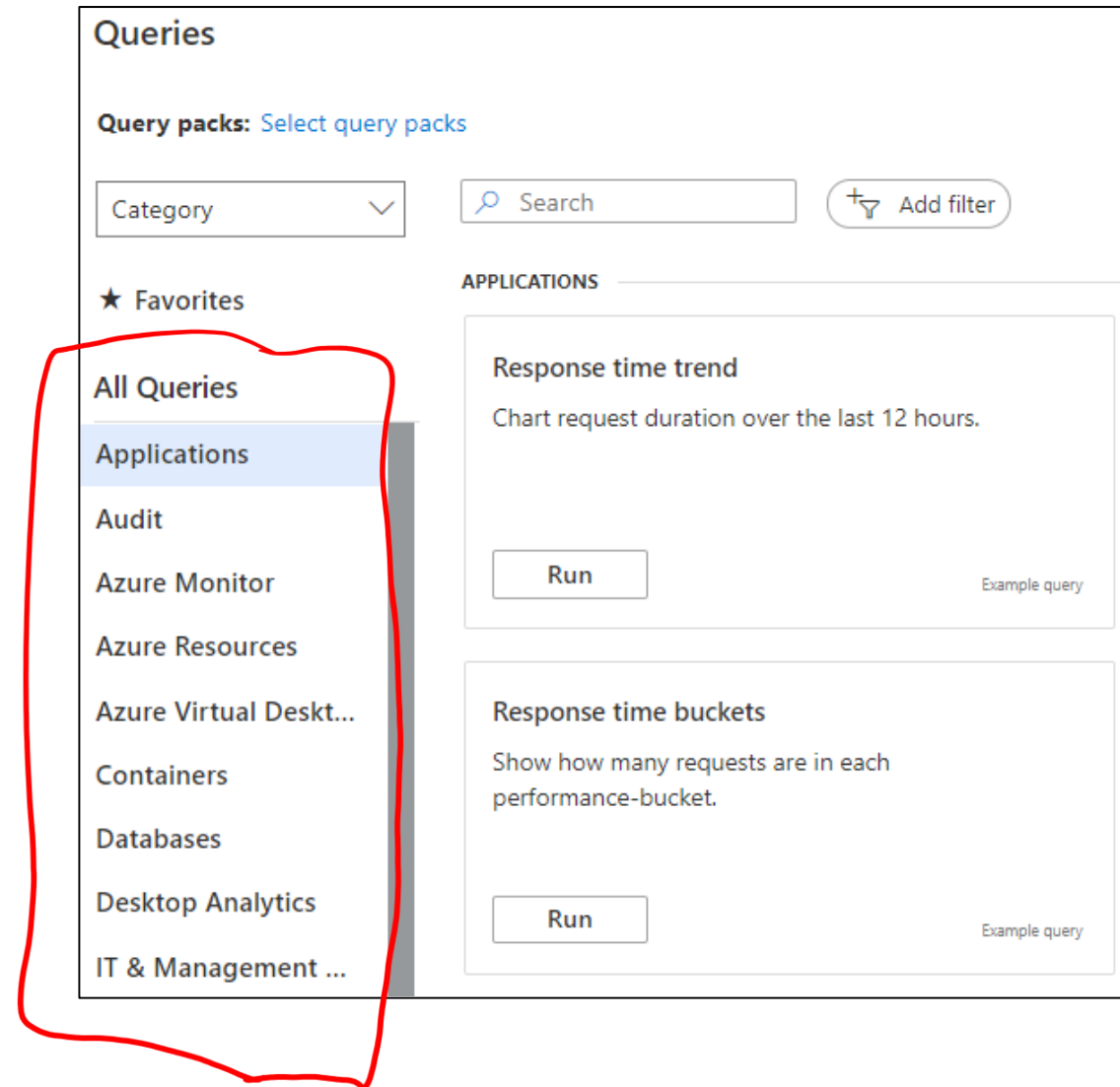
Query Log Analytics Data

Common queries and a query language (KQL) for custom searches

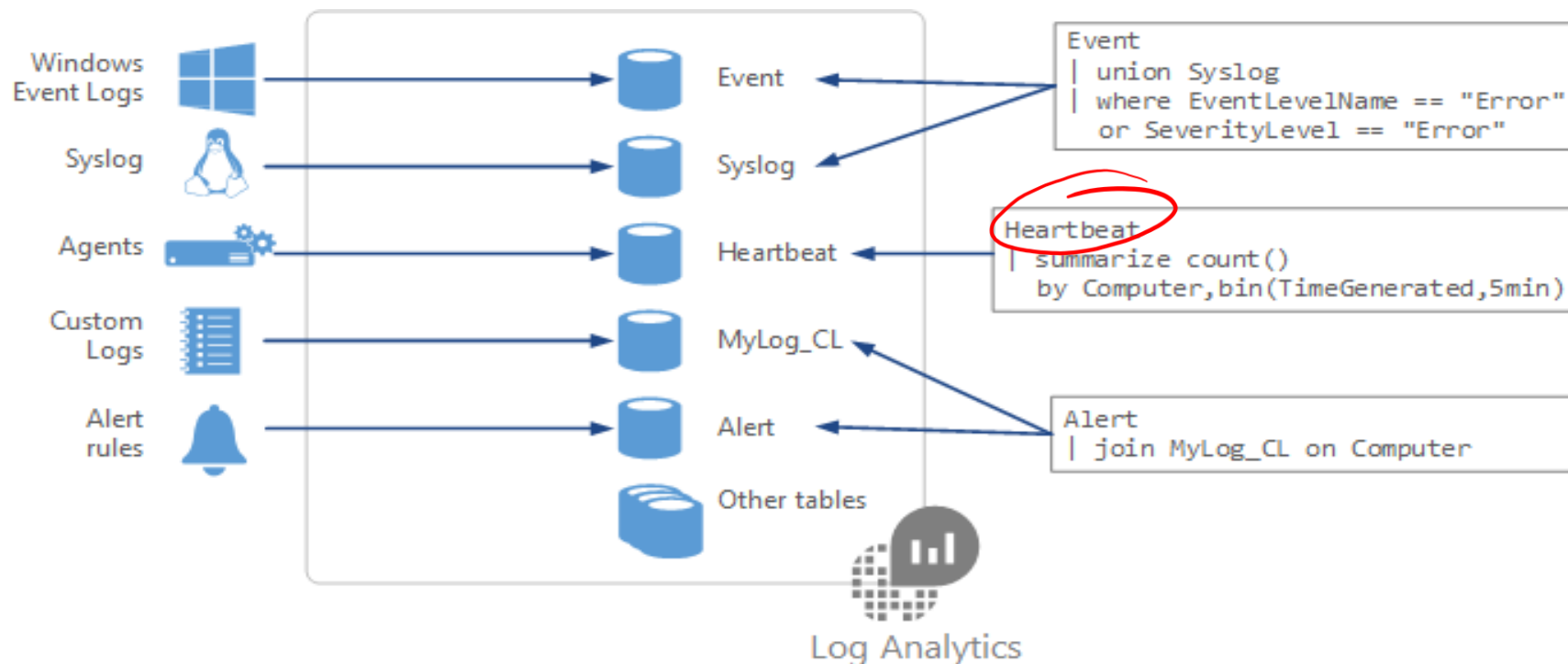
Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

Export the data to Power BI or Excel



Structure Log Analytics Queries



AZ-104
SC-200

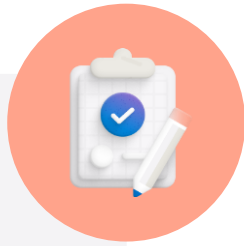
Event

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

Kusto QL

SCCM
Sentinel SIEM

Learning Recap – Configure Log Analytics



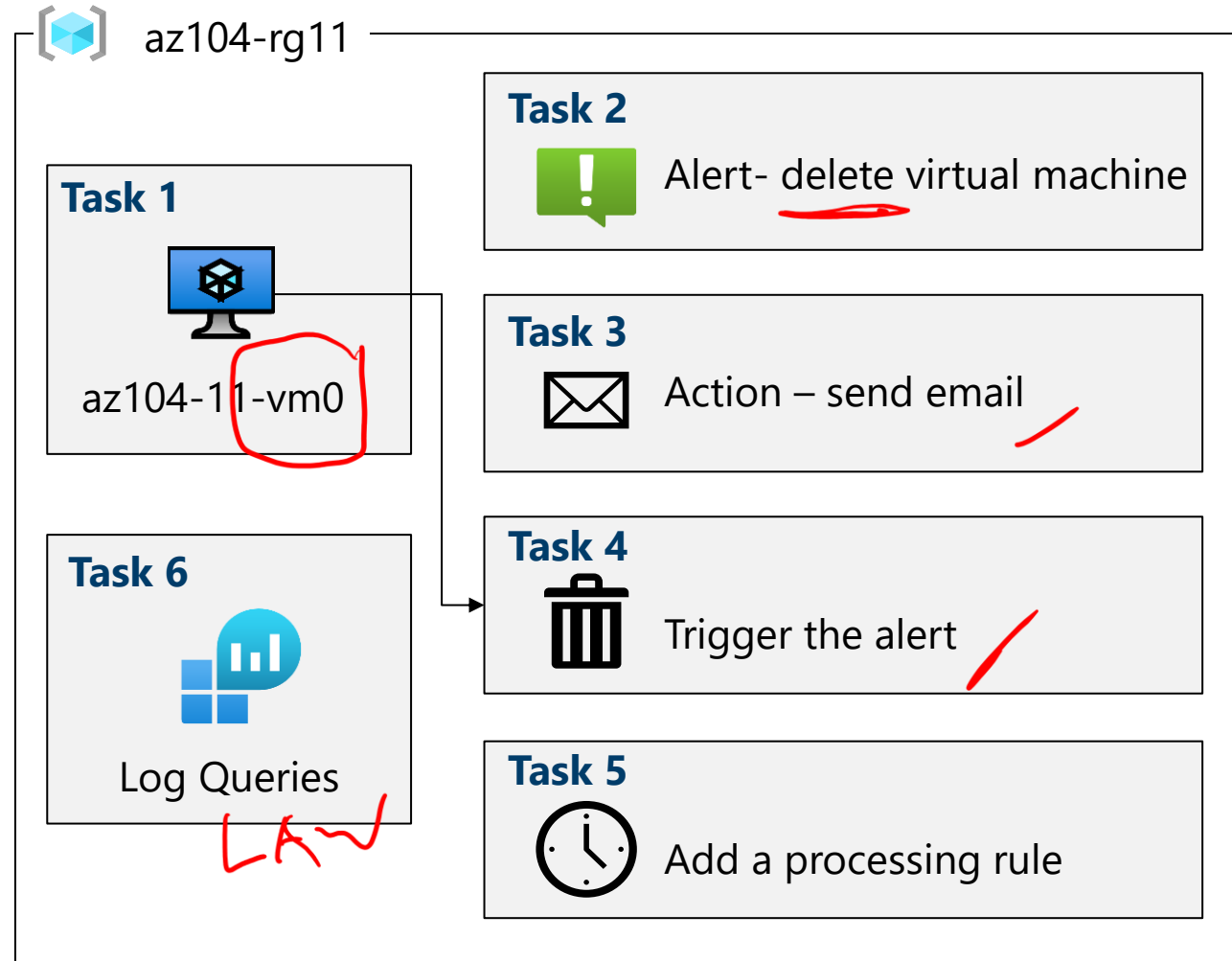
Check your
knowledge
questions and
additional
study

- Write your first query with Kusto Query Language

Lab – Implement Monitoring



Lab 11 – Architecture diagram



End of presentation

