

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](#)
- [Configure Azure Alerts](#)
- [Configure Log Analytics](#)
- [Lab 11 – Implement Monitoring](#)

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

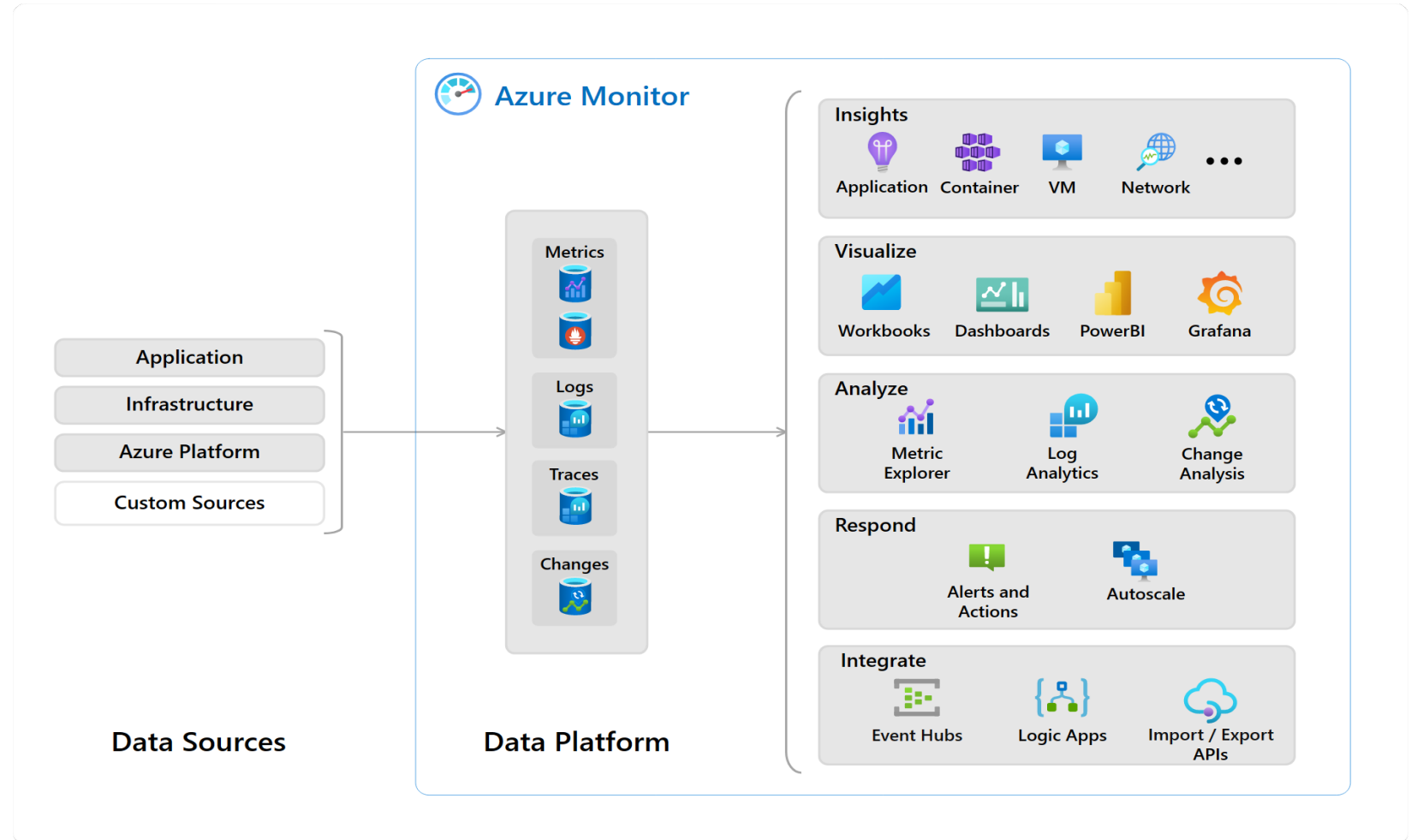
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

[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

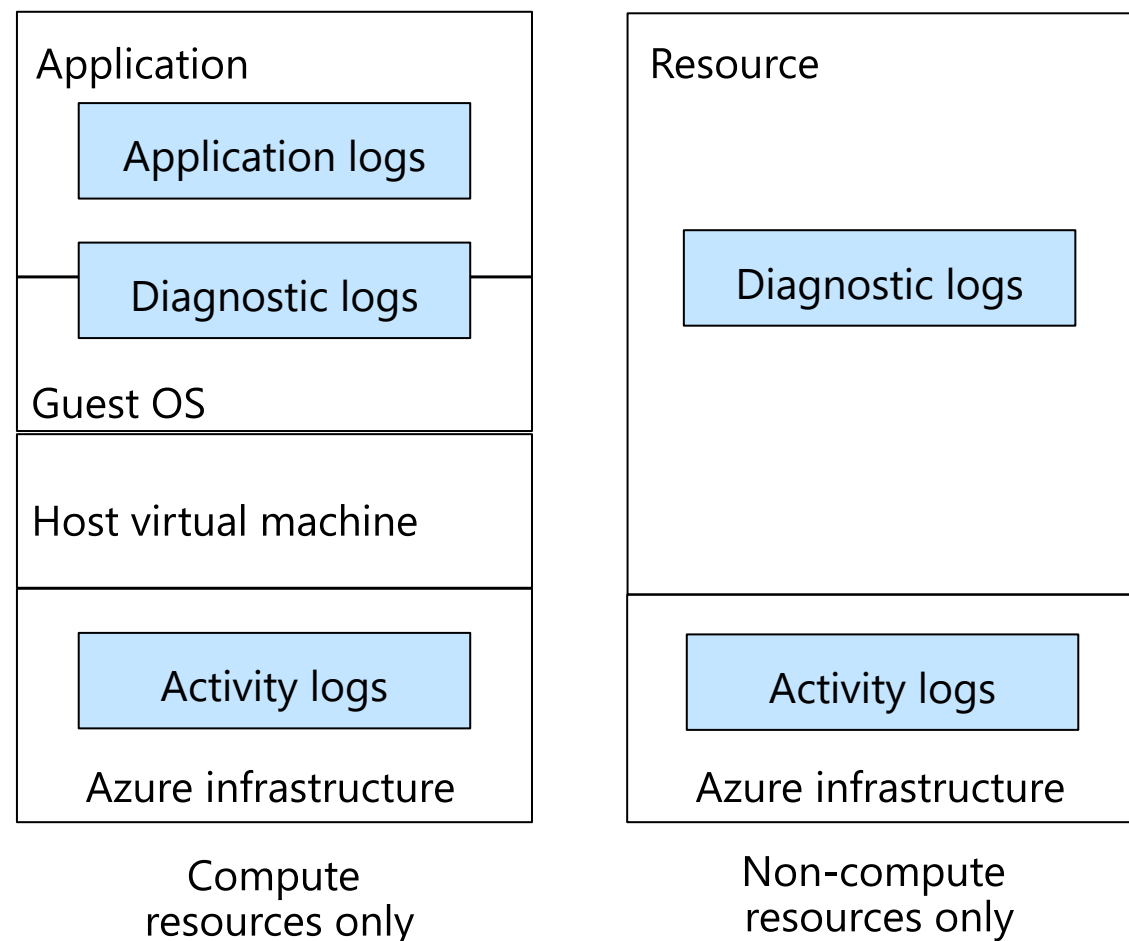
Send data to Log Analytics for advanced search and alerts

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



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

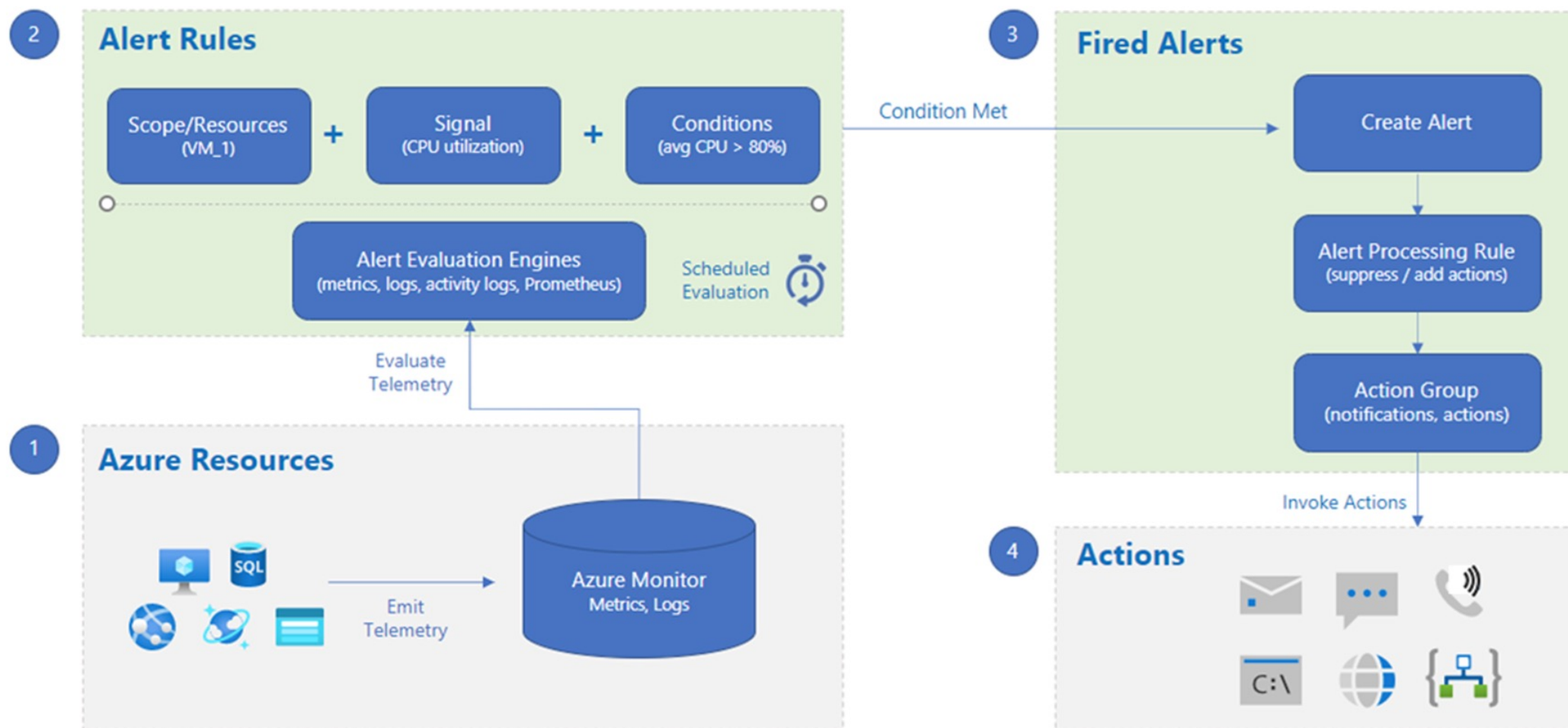
Add a filter, like Event Category
(Security, Recommendations,
Alerts)

Pin current filters and download
as CSV

Configure Azure Alerts



Manage Azure Monitor Alerts



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 ⓘ

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 ⓘ

Automation Runbook

Azure Function

ITSM

Logic App

Secure Webhook

Webhook

Configure Log Analytics

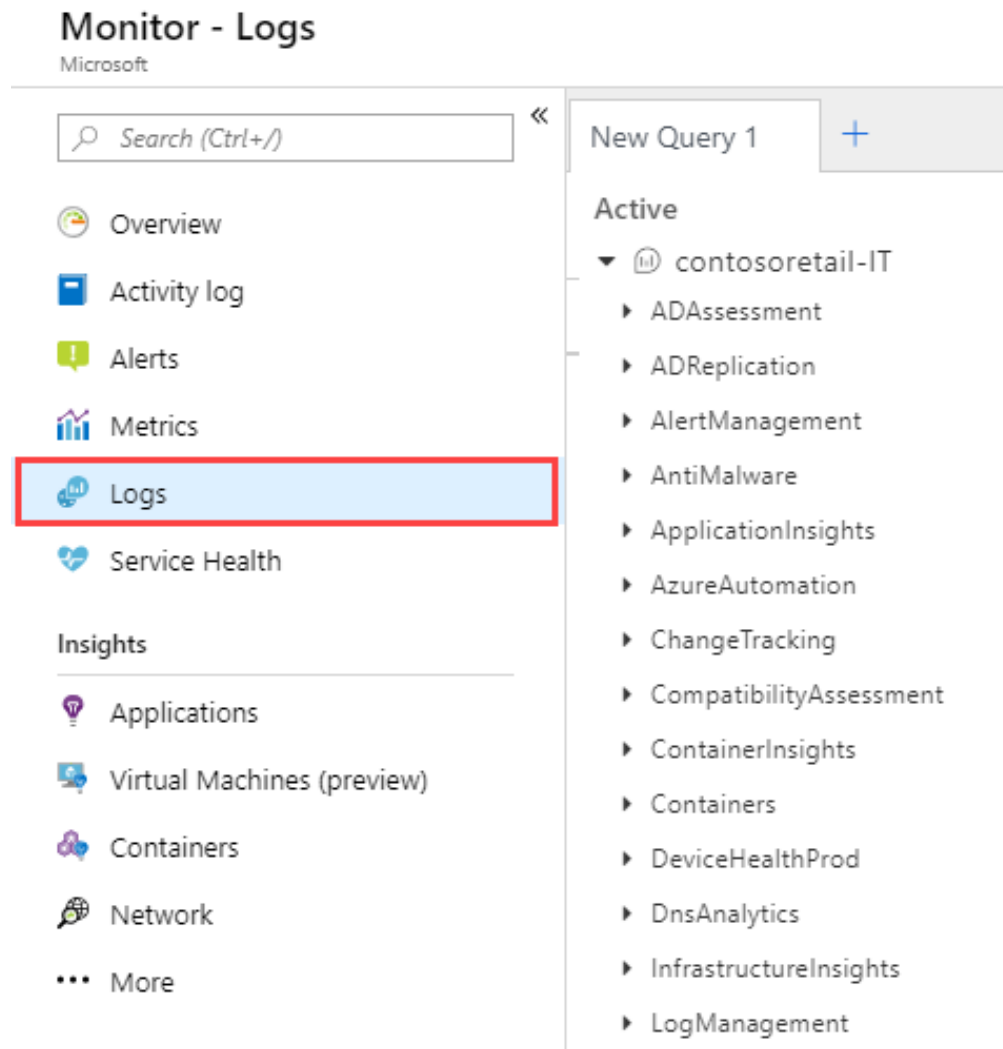


Determine Log Analytics Uses

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

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



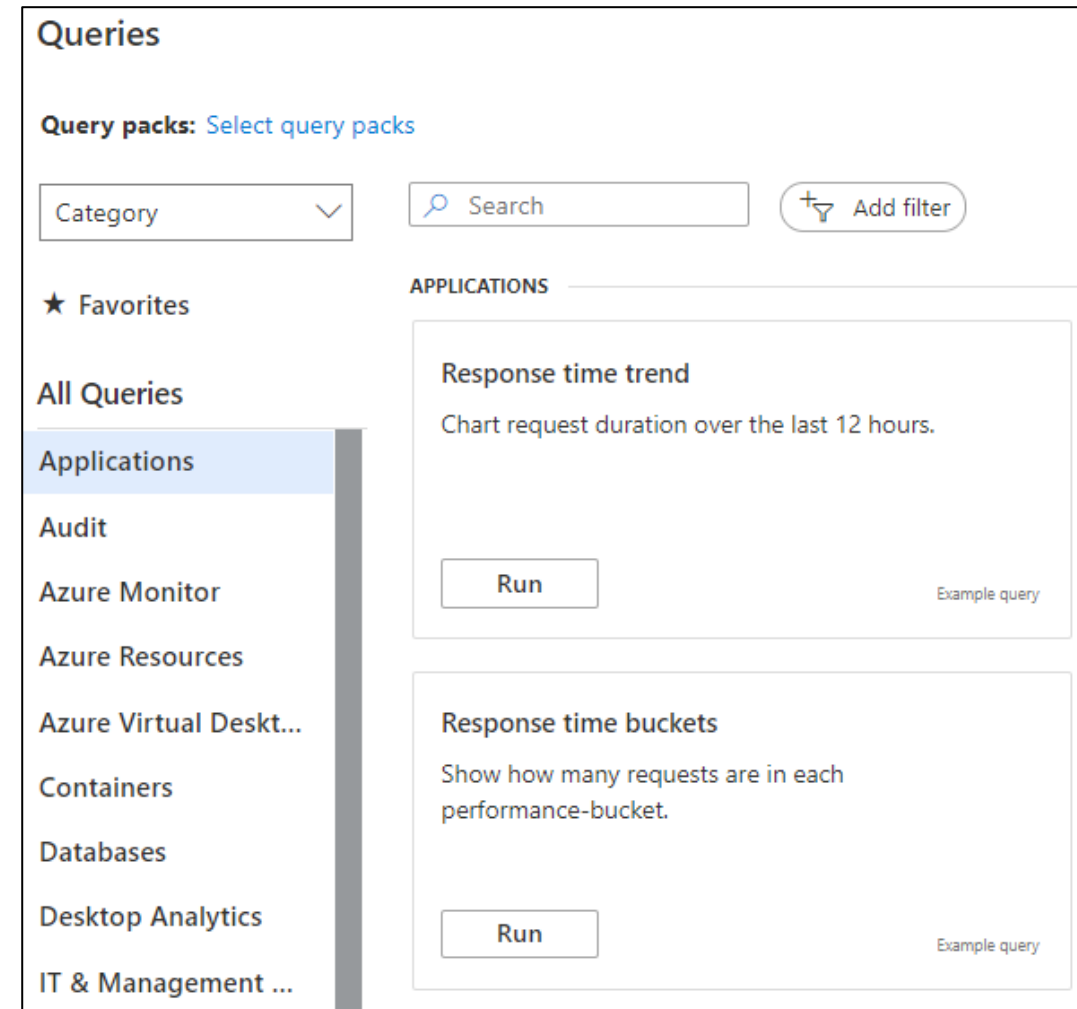
Query Log Analytics Data

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

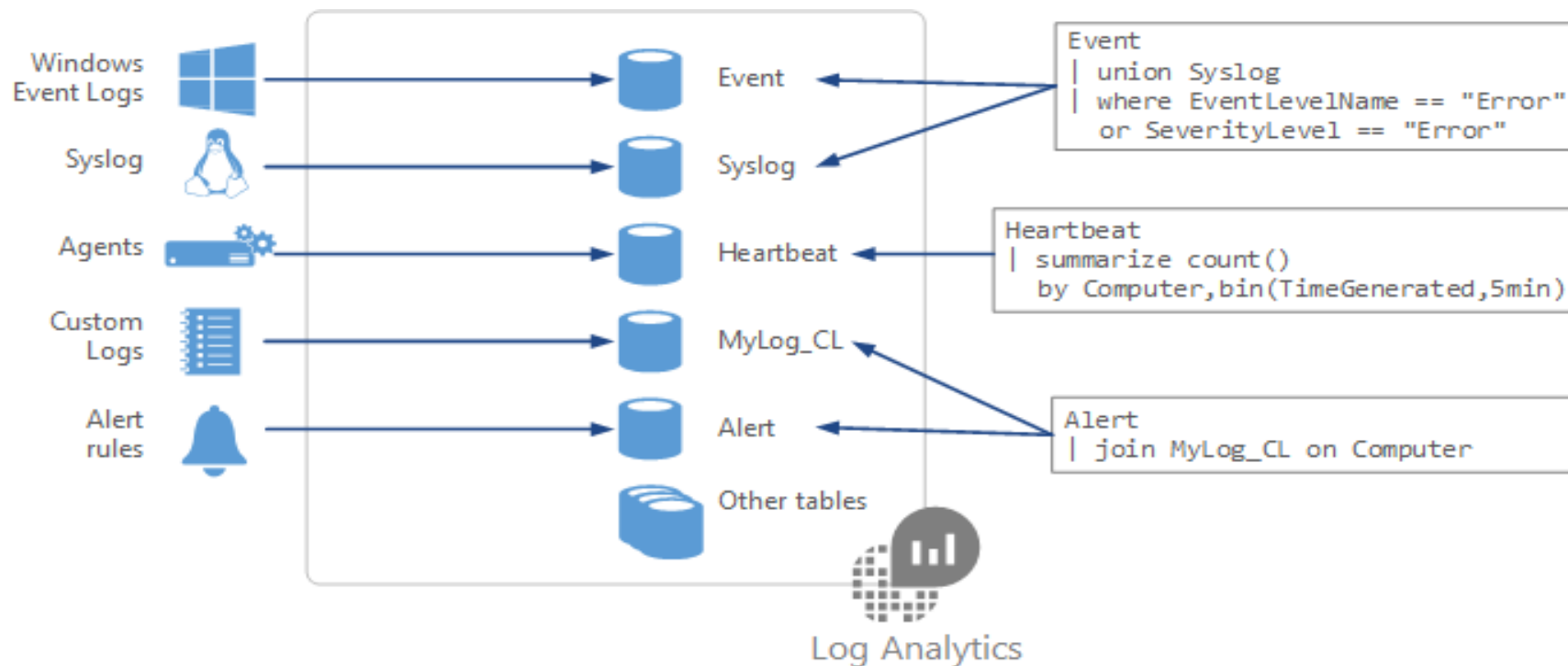
Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

Export the data to Power BI or Excel



Structure Log Analytics Queries



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

Lab 11 – Implement Monitoring



Lab 11 – Implement monitoring



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

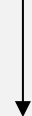


AutomationAccount

Task 6



Azure Monitor



New alert rule

End of presentation

