# AZ-104 Module 11: Administer Monitoring – Learner Guide

## 1. Introduction to Azure Monitor

* Azure Monitor is a unified monitoring solution for Azure and on-premises environments.
* Supports monitoring across applications, infrastructure, and network layers.

### Key Capabilities

* Collects metrics, logs, traces, and changes from Azure and non-Azure resources.
* Offers dashboards, workbooks, and insights for performance and health monitoring.
* Enables proactive incident response through alerts and automated actions.
* Integrates with third-party tools like Grafana, ServiceNow, and Power BI.

### Core Components

* Application Monitoring via Application Insights.
* Guest OS Monitoring through Azure Monitor Agent.
* Resource Monitoring for VMs, storage, and networking.
* Subscription & Tenant Monitoring including activity logs and identity events.

## 2. Metrics and Logs

### Metrics

* Numerical data collected at regular intervals.
* Ideal for real-time monitoring and alerting.
* Stored in a time-series database.
* Examples: CPU usage, disk I/O.

### Logs

* Structured or unstructured records of events.
* Useful for deep analysis and troubleshooting.
* Stored in Log Analytics workspaces.
* Examples: Activity logs, diagnostic logs, application logs.

## 3. Activity Logs

* Provide insights into operations at the subscription level.
* Can be queried via portal, CLI, PowerShell, or REST API.
* Supports streaming to Event Hub, archiving to storage, and analysis in Power BI.
* Can be sent to Log Analytics for advanced querying.

## 4. Incident Response with Azure Alerts

### Alert Rules

* Combine resource, signal, and condition.
* Can be metric-based, log-based, or activity log-based.
* Support stateful (persistent until resolved) and stateless (triggered every time) modes.

### Action Groups

* Define who gets notified and what actions are taken.
* Support email, SMS, voice calls, push notifications, and automated actions.
* Up to five action groups can be attached to a single alert rule.

### Alert Processing Rules

* Modify alerts dynamically (e.g., suppress, reroute).
* Useful for scaling alert management.

## 5. Azure Monitor Logs and Log Analytics

### Log Analytics Workspace

* A container for log data.
* Supports multiple workspaces per subscription.
* Offers data isolation, geographic placement, and access control.

### Querying Logs

* Uses Kusto Query Language (KQL).
* Supports interactive analysis, alert creation, and data export.
* Can be visualized in charts, dashboards, and workbooks.

## 6. Kusto Query Language (KQL)

### Basics

* Tabular expression statements using pipes (|) to chain operations.
* Supports filtering, aggregation, sorting, and visualization.

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

### Advanced Features

* Time-series analysis
* Text parsing
* Geospatial queries
* Vector similarity searches

## 7. Best Practices for Monitoring

* Use recommended alert rules for common scenarios.
* Centralize logs in Log Analytics for cross-resource analysis.
* Automate responses using action groups and Logic Apps.
* Optimize costs by managing data retention and using diagnostic settings wisely.
* Use insights for curated monitoring experiences (e.g., VM Insights, Container Insights).