1-2-1: Achieving Cloud Observability Using Alerting

After completing this episode, you should be able to:

- Identify and explain the importance of alerting to cloud observability, given a scenario.

Description: In this episode, the learner will examine alerts, alerting, and alerting activities, such as alert triage and response. We will explore the benefits of implementing alerting to achieve cloud observability.

- Describe alerting and the significance of cloud observability
    - Alerting
        - The process of notifying relevant parties when predefined conditions or thresholds are met in the monitored system.
        - It involves setting up triggers based on metrics, logs, or events and sending notifications to appropriate stakeholders or systems when these triggers are activated. (demo - show Azure Monitor Alerts - aci-cloud-demo-alert-01, administrative operations awareness)
- Describe alert triage and the significance of observability in the cloud
    - Alert triage - involves prioritizing and categorizing alerts generated by monitoring systems based on their urgency, severity, and impact on business operations. (demo - show Azure Monitor Alerts severity attributes)
    - Benefits
        - Efficient resource allocation
            - Teams can allocate resources effectively, focusing on critical issues that require immediate attention while deprioritizing less urgent alerts.
        - Reduced noise
            - Helps to filter out noise by identifying false positives or non-actionable alerts, preventing alert fatigue among monitoring teams.
        - Improved incident response time
            - Enables teams to respond faster to critical incidents, reducing mean time to resolution (MTTR) and minimizing potential business impact.
- Describe alert response and the significance of observability in the cloud
    - Response - refers to actions taken to address and resolve issues triggered by alerts, such as restarting services or escalating to the appropriate team.
- Describe a real-world scenario for alerting in the cloud
    - Example
        - Use the Resource Visualizer interface - allowing observability across an entire solution contained within a specific resource group
        - Using the Alert feature in Azure Monitor to proactively implement monitoring and notifications systems for cloud resources in Azure
        - Purpose
            - Set up alerts
            - Define thresholds
            - Select notification channels (SMS, email, workspace)
            - Create and customize alerting logic
            - Monitor and respond
            - Review and optimize
            - Wash, rinse, repeat

Additional Resources

- Metric - a quantitative measurement used to track specific aspects of a cloud system, such as CPU usage, memory consumption, or network traffic.
- Log - a record of system activity, typically capturing detailed information about events, operations, and error messages.
- Event - an occurrence or action within a cloud system, like a user request, a change in configuration, or a system warning.
- Load - the demand placed on a cloud system, typically measured by the number of requests, processing tasks, or resource usage.
- Trigger - a condition or Event that initiates a specific action or response in a cloud system, such as scaling, alerting, or automated workflows.