1-1-1: Achieving Cloud Observability Using Logging and Monitoring

After completing this episode, you should be able to:

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

Description: In this episode, the learner will examine logs, logging, and logging activities, such as aggregation and retention. We will explore the benefits of implementing logging to achieve cloud observability.

- Describe what is observability in the cloud
    - The ability to gain insights into system behavior through data collection and analysis.
- Describe some of the benefits to achieving obeservability in the cloud?
    - Ability to gain insights into system behavior
    - Helps understand system operations and troubleshoot issues
    - Aids in monitoring performance
    - Leads to improved system reliability and user experience
    - Relies on data collection and analysis
    - Uses metrics, logs, traces, and events
- Describe logging and monitoring
    - Logging (demo - Entra ID activity logs)
        - Records of events or activities generated by software, hardware, or infrastructure, detailing what occurred, when it happened, and sometimes why it happened
    - Monitoring (demo - Azure Monitor [metrics, logs, events])
        - Continuously observing and analyzing system metrics, performance indicators, and behaviors to detect anomalies, identify trends, and ensure optimal performance.
- Describe common log sources (demo - show resource group)
    - Server logs (demo - show VM)
        - Record activities on servers, including system errors, user activities, and application events
    - Application logs (demo App Service)
        - Capture information specific to applications, such as user interactions, errors, and performance metrics
    - Infrastructure logs (demo - show container, VM or service health)
        - Provide insights into the health and performance of infrastructure components like virtual machines, storage, and networking devices.
    - Database logs
        - Log database activities, such as queries, transactions, and changes to database structures
    - Security logs
        - Document security-related events like login attempts, unauthorized access, and system breaches
- Describe log aggregation and the benefit to observability (Demo - show log analysis)
    - The process of collecting and centralizing logs from multiple sources into a single repository or system for easier analysis and management.
    - Benefits to observability in the cloud
        - Simplified monitoring - centralizing logs allows cloud teams to monitor distributed applications more effectively, obtaining a unified view of system events.
        - Enhanced troubleshooting - With logs aggregated in one location, identifying and resolving issues becomes faster and more straightforward.
        - Improved compliance - log aggregation helps to facilitate consistent retention policies and auditing processes, aiding in compliance with regulatory requirements.
        - Efficient incident response - Centralized logs allow for quicker analysis during incidents, enabling faster response times.
        - Scalability - Log aggregation systems in the cloud can scale with increased data volumes, ensuring that observability remains effective even as cloud environments grow. Implementing larger systems such as Security Information and Event Management systems or SIEMs and eXtended Detection Response or XDR solutions

- Describe a real-world application of using logging for observability
    - Example
        - Activity logs on an Azure Resource Group will display all resource activities within that cloud solution

Additional Resources

- OpenTelemetry: https://opentelemetry.io/
- OpenTelemetry - Observability: https://opentelemetry.io/docs/concepts/observability-primer/#what-is-observability
- Event
    - An observable occurrence, change or circumstance in a system that are captured with specific details like timestamp, source, and context
- Metric
    - Quantitative measurements representing the state, behavior, or performance of a system or component, typically collected at regular intervals to track trends, diagnose issues, and make informed decisions.