

Oracle 1Z0-1111-26

Oracle Cloud Infrastructure 2026 Observability Professional

**Thank You for Downloading 1Z0-1111-26 Updated Exam
Questions**

<https://certs4sale.com/oracle/1z0-1111-26-pdf-exam-dumps>

Oracle 1Z0-1111-26

Oracle Cloud Infrastructure Observability Professional

ORACLE CLOUD
PRACTICE ASSESSMENT

TARGET CERTIFICATION

Oracle Cloud Infrastructure Observability Professional

EXAM CODE

1Z0-1111-26

DOCUMENT PURPOSE

Practice Questions & Detailed Explanations

CORE FOCUS AREAS

Metrics, Logging, APM, Events & Monitoring

Question 1

SINGLE CHOICE

Your organization is deploying a multi-tier application across OCI and needs to establish a comprehensive observability strategy. You are tasked with explaining the core principles to the team. Which of the following best represents the three pillars of OCI Observability?

- A. Metrics, Logs, and Traces
- B. Monitoring, Analytics, and Alerting
- C. Events, Dashboards, and Connectors
- D. Instrumentation, Collection, and Storage
- E. Performance, Availability, and Reliability

Correct Answer: A

Explanation:

The three pillars of OCI Observability are Metrics, Logs, and Traces. Metrics provide quantitative measurements of system behavior; Logs capture detailed event data; and Traces track requests across distributed systems. Options B, C, D, and E describe components or outcomes of observability but not the foundational pillars themselves. Understanding these three pillars is essential for designing a complete observability strategy in OCI.

Question 2**MULTIPLE CHOICE**

You are configuring alarms in OCI Monitoring to track CPU utilization across your compute instances. The alarm should trigger when CPU exceeds 80% for more than 2 minutes to avoid false positives from brief spikes. Which alarm configuration best practices should you apply? (Choose two.)

- A. Set the statistic to 'Mean' and the evaluation periods to 2 consecutive periods of 1 minute each
- B. Use a notification rule that escalates to multiple channels only after the alarm fires three consecutive times
- C. Set the threshold to 80 and configure the trigger rule with 'Trigger after 2 consecutive breaches' or equivalent duration-based condition
- D. Configure the alarm to suppress notifications during business hours to reduce noise
- E. Set the statistic to 'Maximum' to ensure the alarm catches all spike events regardless of duration

Correct Answer: A, C**Explanation:**

Best practices for alarm configuration include: (1) using appropriate statistics like 'Mean' combined with evaluation periods to filter out brief spikes, and (2) setting clear threshold values with explicit duration-based trigger conditions (such as 'trigger after 2 consecutive breaches'). Option A correctly describes using Mean over 2 one-minute periods to achieve a 2-minute evaluation window. Option C correctly describes setting the threshold and using a duration-based trigger rule. Option B is incorrect because escalation is not a built-in alarm feature—notifications are sent immediately when conditions are met. Option D suggests suppressing during business hours, which contradicts monitoring best practices. Option E is wrong because Maximum statistics would trigger on every spike, not just sustained high CPU, defeating the purpose of filtering false positives.

Question 3**SINGLE CHOICE**

Your development team has deployed an e-commerce application on OCI and wants to respond to resource scaling events in real-time. When a compute instance is terminated unexpectedly, the system should automatically trigger a notification and potentially initiate a remediation workflow. Which OCI service and configuration should you use, and what is the correct event structure?

- A.** Use OCI Events Service to detect 'Compute Instance - Terminate' event type and create a rule that routes the event to a notification topic via an integration with Functions or other targets
- B.** Use OCI Monitoring Service to set an alarm based on instance count metrics and trigger a webhook to an external system
- C.** Use OCI Logging Service to search log entries for termination events and configure Log Connectors to send alerts
- D.** Use OCI Stack Monitoring to discover instance relationships and automatically restart terminated instances without external notification
- E.** Use OCI Application Performance Monitoring to track instance lifecycle events and correlate with application performance degradation

Correct Answer: A**Explanation:**

The OCI Events Service is the correct choice for responding to cloud resource changes in real-time. The Events Service captures system-generated events (such as 'Compute Instance - Terminate') and allows you to create rules that route these events to targets like notification topics, Functions, or other OCI services. The event structure includes metadata about the resource, the action performed, and the timestamp. Option B is incorrect because Monitoring primarily tracks metrics, not discrete events. Option C confuses Logging Service with Events Service—Logging captures application and system logs, not system events. Option D describes Stack Monitoring, which focuses on monitoring topology and metrics, not real-time event response. Option E describes APM, which is designed for application performance, not infrastructure event handling.

Question 4**SINGLE CHOICE**

Your organization has multiple applications and databases generating logs across OCI. You need to centrally collect, manage, and search logs from all sources while maintaining the ability to rapidly identify issues. Currently, logs are stored in different OCI services. Which approach best addresses your requirement?

- A.** Use OCI Logging to enable log collection from all OCI resources and services, aggregate them into a central Log Group, and use the Logs Search capability to query across the entire log estate
- B.** Use OCI Logging Analytics to ingest raw logs and immediately apply machine learning models to detect anomalies without performing manual searches
- C.** Export all logs to Object Storage and use Spark to run batch analytics every hour to identify patterns
- D.** Use separate Logging dashboards for each application and configure email alerts whenever error-level logs are detected
- E.** Archive all logs in OCI Data Lake and query them using SQL only when a specific issue is reported

Correct Answer: A**Explanation:**

OCI Logging is the core service for centrally managing and visualizing log data across your entire OCI environment. It enables unified log collection from multiple sources into centralized Log Groups and provides powerful search and filtering capabilities to query across the entire log estate. This is the foundational layer for log management. Option B confuses Logging with Logging Analytics—while Logging Analytics builds on Logging and provides advanced analytics, the basic requirement of central collection and search is addressed by OCI Logging itself. Option C describes a batch approach that is not suitable for rapid issue identification. Option D fragments logs across multiple dashboards, defeating the purpose of centralized management. Option E introduces unnecessary complexity with data lakes and SQL-only querying, which is not optimal for real-time log search.

Question 5**MULTIPLE CHOICE**

Your team is ingesting large volumes of application and infrastructure logs into OCI Logging Analytics for pattern identification and troubleshooting. You need to identify the root cause of intermittent performance degradation across your microservices. Which capabilities of Logging Analytics should you leverage? (Choose two.)

- A.** Use log pattern recognition and correlation features to automatically identify recurring error sequences and anomalies in log data
- B.** Create custom visualizations and dashboards that display log trends over time to support visual pattern analysis
- C.** Configure log collection directly from databases using Logging Analytics agents without requiring OCI Logging as an intermediate layer
- D.** Export logs to Data Catalog and use metadata tagging to classify logs by severity before analysis
- E.** Run real-time SQL queries on raw logs stored in Object Storage to identify performance anomalies

Correct Answer: A, B**Explanation:**

Logging Analytics provides advanced pattern recognition and correlation features that automatically identify recurring patterns and anomalies in logs, making it ideal for root cause analysis. Additionally, Logging Analytics supports creating custom visualizations and dashboards that help visualize log trends and support troubleshooting efforts. These are core analytics capabilities. Option C is incorrect because Logging Analytics typically works with logs from OCI Logging as a source. Option D confuses Logging Analytics with Data Catalog, which is a metadata management service. Option E suggests a manual SQL approach on Object Storage, which bypasses Logging Analytics' advanced analytics features and is not aligned with the service's design.

End of Assessment Demo

You have completed the preview module for **Oracle 1Z0-1111-26: OCI Observability Professional**.

THANK YOU FOR DOWNLOADING 1Z0-1111-26 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our 1Z0-1111-26 Exam Product

Visit Our Site to Purchase the Full Set of Actual 1Z0-1111-26 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/oracle/1z0-1111-26-pdf-exam-dumps>