

PRACTICE QUESTIONS

Elastic Certified Observability Engineer

SHARED BY [u/Crisp-Crane-3759](#) on aiexamcerts

EDITION	Free Set 2
---------	------------

QUESTIONS	10
-----------	----

SHARED	October 15, 2026
--------	------------------

EXAM	Elastic Certified Observability Engineer
------	--

Shared by [u/Crisp-Crane-3759](#) on aiexamcerts

10 practice questions for the Elastic Certified Observability Engineer exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/elastic/elastic-certified-observability-engineer. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. In Elastic Common Schema, which field holds the main text of a log entry?

- A event.original
- B log.body
- C text.content
- D message

Answer: D

ECS stores the primary log text in message, while event.original keeps the raw source before any parsing. event.original is the tempting distractor because it is the unparsed text, but it is a preservation field rather than the main text field.

2. Elasticsearch can place indices on tiers such as hot, warm, cold and frozen by assigning data tier node roles such as data_hot and data_frozen.

- A True
- B False

Answer: A (True)

Data tier node roles let lifecycle policies and data stream settings move indices between storage tiers. Assigning the role is enough, so there is no separate tier database to create.

3. Which APM feature measures page load timing from real visitors' browsers?

- A Real User Monitoring (RUM) agent
- B Heartbeat HTTP monitor
- C Universal Profiling agent
- D Synthetics browser journey

Answer: A

The RUM agent runs in the visitor's browser and reports real session timing. A Synthetics browser journey is the tempting distractor because it also measures page loads, but it runs scripted checks from a fixed location instead of real sessions.

4. Enrolled Elastic Agents receive policy updates from the Fleet _____ when they check in.

Answer: Server

Fleet Server is the component agents check in with to fetch their policy and report status. The Fleet screens in Kibana are the tempting distractor, since that is where policies are edited, but they do not serve agent check-ins.

5. Which two statements about ingest pipelines are correct? (Choose two.)
- A Pipelines run in Kibana before the data reaches Elasticsearch
 - B A pipeline must be attached to a data stream by editing its mappings
 - C A pipeline can be tested against sample documents with the simulate API before it is used
 - D A reindex request always runs the pipeline named in the source index
 - E A failure processor can route a document to an error handler when a processor fails

Answer: C, E

The simulate API runs documents through a pipeline without indexing them, and `on_failure` handlers catch processor errors. Pipelines execute inside Elasticsearch, not in Kibana, and a pipeline is referenced through settings rather than mappings, which makes those options wrong.

6. Which capability lets OpenTelemetry SDK data reach Elastic without the Elastic APM agent?
- A Translation performed only by the Java agent
 - B OTLP trace, metric and log ingestion over gRPC or HTTP
 - C Jaeger Thrift over UDP only
 - D Forwarding through Filebeat only

Answer: B

Elastic accepts OTLP natively, so OpenTelemetry SDKs and collectors can export directly. The Java agent is the tempting distractor because it is Elastic's own instrumentation, but it is not required for OpenTelemetry data.

7. Which Elastic deployment option removes node sizing, upgrades and capacity planning from your team's work?
- A Self-managed cluster on your own virtual machines
 - B Elastic Cloud Hosted deployment with chosen node sizes
 - C Elastic Cloud Serverless project
 - D Elastic Cloud on Kubernetes with manually sized node pools

Answer: C

A serverless project is fully managed and scales without you choosing node counts. Elastic Cloud Hosted is the tempting distractor because Elastic runs it too, but you still pick node sizes and tiers yourself.

8. A Lens visualization can combine layers that query different data views, so one panel can show data from several data streams.
- A True
 - B False

Answer: A (True)

Lens supports multiple layers with different data views, so one panel can show more than one stream. The common assumption that every panel is locked to one index is the tempting but incorrect view.

9. Which rule type fires when a field aggregated over a time window crosses a set value?

- A Anomaly detection job
- B Synthetics private location
- C Ingest pipeline failure handler
- D Index threshold rule

Answer: D

The index threshold rule aggregates a field over a window and compares it to a fixed value. The anomaly detection job is the tempting distractor because it also spots metric changes, but it learns a baseline rather than checking a fixed threshold.

10. Which SLO indicator type counts good and total events by supplying two KQL queries?

- A Custom KQL indicator
- B APM latency indicator, based on transaction duration
- C Histogram indicator, based on bucketed field values
- D Timeslice metric indicator, based on per-slice thresholds

Answer: A

A custom KQL indicator takes an explicit good query and total query over the data. The APM latency indicator is the tempting distractor because it also measures good and bad events, but it uses transaction durations rather than arbitrary KQL.