

PRACTICE QUESTIONS

Elastic Certified Observability Engineer

SHARED BY [u/Glad-Cache-3342](#) on aiexamcerts

EDITION	Free Set 1
---------	------------

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

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

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

Shared by [u/Glad-Cache-3342](#) 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. Which index setting controls how many replica copies of each primary shard are kept for redundancy?

- A `index.number_of_shards`
- B `index.number_of_replicas`
- C `index.refresh_interval`
- D `index.routing.allocation.total_shards_per_node`

Answer: B

The replica count is set with `index.number_of_replicas` and can be changed on a live index. The primary shard count is fixed at creation, which makes `index.number_of_shards` the tempting distractor.

2. Metrics from the System integration for CPU are written to the data stream `metrics-system._____`-default.

Answer: cpu

The System integration names its CPU stream `metrics-system.cpu`, so the blank is `cpu`. Memory, filesystem and network streams follow the same `type-dataset-namespace` pattern with different dataset names.

3. Which Elasticsearch component collects and forwards host data without requiring Logstash?

- A Heartbeat, which only runs uptime checks
- B Kibana Canvas, which only renders workpads
- C Elastic Agent
- D Snapshot repository, which only stores backups

Answer: C

Elastic Agent ships logs, metrics and other data straight to Elasticsearch under Fleet policy. Heartbeat is the tempting distractor because it also sends data, but it only runs availability checks and does not collect host logs or metrics.

4. The grok processor is faster than dissect, so it is the better choice for log lines with fixed delimiters.
- A True
 - B False

Answer: B (False)

Dissect is faster when the format is a fixed delimiter pattern because it does no regular expression matching. Grok is more flexible but slower, which makes it the wrong pick for simple delimited logs even though it is the tempting option for many developers.

5. Which two components are needed for a trace that crosses two services instrumented with Elastic APM agents? (Choose two.)
- A A Synthetics private location in each region
 - B Agents in both services that propagate the W3C traceparent header
 - C A Logstash grok filter that parses the trace id
 - D An APM Server or the APM integration that receives and indexes the spans
 - E A Canvas workpad that charts response times

Answer: B, D

Trace context must travel from one service to the next in the traceparent header, and something must receive and index the spans. A Synthetics private location is the tempting distractor because it runs remote checks, but it does not link service-to-service requests.

6. Which Fleet object bundles the integrations and settings that enrolled agents apply?
- A Agent policy
 - B Enrollment token
 - C Index template
 - D Ingest pipeline

Answer: A

An agent policy groups integrations and their settings and is assigned to agents. An enrollment token only authorizes an agent to join, so it is the tempting distractor, but it holds no configuration.

7. A log line is a JSON document inside the message field. Which ingest processor parses it into separate fields at index time?
- A dissect processor, which splits on fixed delimiters
 - B rename processor, which only renames existing fields
 - C json processor
 - D convert processor, which only changes field data types

Answer: C

The json processor decodes a JSON string into structured fields. The dissect processor is the tempting distractor because it also parses text, but it relies on fixed delimiter patterns rather than JSON structure.

8. In APM, a unit of timed work inside a transaction, such as a database query, is called a _____.

Answer: span

A span records one timed operation inside a transaction, such as a SQL query or an outgoing HTTP call. A transaction is the top-level unit for a request or job, which makes it the tempting answer.

9. Which Kibana app shows hosts and containers with their key metrics in one inventory view?
- A Stack Monitoring
 - B Infrastructure Inventory
 - C Dev Tools console
 - D Maps

Answer: B

Infrastructure Inventory lists hosts and containers with their metrics and drill-down views. Stack Monitoring is the tempting distractor because it also charts metrics, but it reports on the health of Elastic Stack components themselves.

10. A team must roll out the same integrations to 400 hosts. What is the most efficient approach?
- A Create one agent policy and enroll all hosts with it through Fleet
 - B Edit each host's elastic-agent.yml by hand
 - C Create a separate Kibana space for every host
 - D Route every host through one shared Logstash relay

Answer: A

A shared agent policy applies one configuration to every enrolled host, so changes are made once. Hand-editing each host is the tempting distractor because standalone configuration also works, but it does not scale and drifts over time.