

PRACTICE QUESTIONS

Elastic Certified Analyst

SHARED BY [u/Witty-Lantern-4081](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Elastic Certified Analyst

Shared by [u/Witty-Lantern-4081](#) on aiexamcerts

10 practice questions for the Elastic Certified Analyst exam, each followed by its answer and a short explanation. More free sets and the full practice exam: www.aiexamcerts.com/elastic/elastic-certified-analyst. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. An analyst clicks a field name in the Discover sidebar. What does Discover show for that field?
 - A The field mapping as stored in the index template
 - B A histogram of the field across all indices in the cluster
 - C The top values among the documents currently matched, with their counts
 - D A Painless script that computes the field's value for each document

Answer: C

Clicking a field in the Discover sidebar shows its most common values among the documents in the current result, with counts and percentages. The mapping is visible in data view management rather than the sidebar. A cluster-wide histogram and a Painless script are not what the sidebar displays.

2. Clicking Visualize on a field in Discover can only open a dashboard panel, never a Lens visualization.
 - A True
 - B False

Answer: B (False)

Visualize on a Discover field opens a Lens visualization with that field already placed, so the statement is false. Lens then lets the analyst choose the chart type and change the metric. The shortcut does not create dashboard panels directly.

3. An analyst needs response_time values of 2000 or more. Which KQL clause is correct?
 - A response_time:[2000 TO *]
 - B response_time GTE 2000
 - C response_time => 2000
 - D response_time >= 2000

Answer: D

KQL supports comparison operators such as greater than or equal to on numeric fields, so response_time >= 2000 is valid. The bracket range with TO is Lucene syntax that KQL does not use, and GTE and the arrow form are not KQL operators.

4. The aggregation that counts distinct values, which is approximate for large sets, is called _____.

Answer: cardinality

The Cardinality aggregation returns an approximate count of distinct values, which is why it suits large datasets. A plain row count is a Count metric, and Terms lists the distinct values themselves. Dashboards often label this metric Unique count.

5. Which two statements about KQL and Lucene query modes in Kibana are correct? (Choose two.)

- A KQL is the default query language in the Kibana query bar
- B Lucene mode supports regular expressions and fuzzy matching
- C KQL requires every search term to be quoted
- D Lucene mode cannot search keyword fields
- E KQL can run aggregations directly from the query bar

Answer: A, B

KQL is the default language for the query bar, and Lucene mode adds regular expressions and fuzzy matching. KQL does not require quotes for simple terms, and Lucene can search keyword fields. Aggregations are built in visualizations rather than typed as KQL queries.

6. Which aggregation groups documents by the most frequent values of a keyword field such as host.name?

- A Date range with fixed boundaries
- B Terms
- C Histogram with a numeric interval
- D Significant terms ranked by unusual frequency

Answer: B

Terms creates one bucket for each distinct value and orders the buckets by count by default. Date range uses boundaries you define in time, and histogram uses numeric intervals. Significant terms ranks values by how unusual they are, so it answers a different question.

7. Which format does Kibana Reporting produce for a scheduled dashboard report that is emailed?

- A CSV of the raw documents behind the dashboard
- B PDF or PNG
- C Ingest pipeline definition in JSON form
- D Snapshot restore log in plain text

Answer: B

Kibana Reporting renders dashboards to PDF or PNG for scheduled and emailed reports. CSV is an export of Discover results rather than a dashboard image. Ingest pipeline definitions and restore logs are not report formats.

8. The ES|QL command KEEP removes the listed columns from the result, and DROP keeps only the listed columns.
- A True
 - B False

Answer: B (False)

KEEP keeps only the columns that are named, and DROP removes the columns that are named. The statement swaps the two commands, so it is false. Choosing the right command matters before a dashboard reads the result columns.

9. A group should view a dashboard but must not edit it or change alerts. Which access setup is least privileged?
- A A cluster superuser role shared with the group
 - B The delete_index privilege on every index in the cluster
 - C A Kibana role with read-only dashboard access in the space that holds it
 - D A shared administrator account for the whole team

Answer: C

A read-only role limited to the space gives viewing rights without any editing or alert management. A superuser role or a shared administrator account exceeds the requirement, and delete_index is a destructive index privilege. Least privilege means granting only the access needed.

10. What does a geo_distance query select?
- A Documents whose text contains a distance unit
 - B Documents that share the same host name
 - C Documents within a given radius of a point
 - D Documents sorted by their timestamp value

Answer: C

A geo_distance query returns documents whose location falls within a chosen distance from a point. Text with a unit, host matches and timestamp sorting are unrelated to distance from a location. The query needs a geo_point field to work.