

PRACTICE QUESTIONS

Elastic Certified Analyst

SHARED BY [u/Daring-Beacon-6815](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Elastic Certified Analyst

Shared by [u/Daring-Beacon-6815](#) 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. Which Discover feature keeps a query, its filters and its selected columns so that the analyst can reopen the same view later?
 - A Pinned filter that stays across apps
 - B Saved search
 - C Rollup job that summarizes older data
 - D Field formatter for numeric display values

Answer: B

A saved search stores the query text, filters, columns and sort order, and it can be reopened from the Discover list. A pinned filter only persists across applications within the same session and is not a stored view. Rollup jobs and field formatters serve data summarization and display, so neither saves a Discover view.

2. A data view uses the _____ field to apply the time picker range, and the usual field name is @timestamp.

Answer: @timestamp (also accepted: timestamp)

Data views use a timestamp field for the time picker, and Elastic data usually stores it as @timestamp. Without a time field, time-based filtering is not applied to the data view. Naming the field correctly is part of making Discover time filters work.

3. An analyst wants documents whose message field contains the exact phrase connection refused. Which query does this?
 - A message:connection AND refused
 - B message IS connection refused
 - C message:"connection refused"
 - D message=connection refused

Answer: C

Quoting the words in KQL requires them to appear as a phrase, in order, in the field. Connecting the terms with AND matches documents that contain both words anywhere, and the other two forms are not valid KQL. The quoted phrase form is what the analyst needs.

4. KQL supports regular expressions, so a pattern such as `/err.*/` matches any text field value.
- A True
 - B False

Answer: B (False)

KQL does not support regular expressions, so `/err.*/` is not a KQL pattern. Patterns between forward slashes are a Lucene feature that Kibana accepts when Lucene mode is selected. In KQL the supported way to match a text pattern is the asterisk wildcard.

5. Which two statements about bucket and metric aggregations in visualizations are correct? (Choose two.)
- A Metric aggregations such as Sum and Average are calculated within each bucket
 - B Bucket aggregations such as Terms and Date histogram define the rows or slices
 - C Metric aggregations must be placed above bucket aggregations in every chart
 - D Bucket aggregations always return the average of their documents
 - E Only pie charts can use bucket aggregations

Answer: A, B

Buckets define the groups, such as hosts or time intervals, and metrics calculate a value for each group. Metrics do not need to come before buckets, and buckets do not average their documents. Many chart types, not only pie charts, use buckets.

6. A dashboard must show the number of distinct users per day. Which metric fits?
- A Unique count (cardinality) of user.id per day
 - B Sum of the user.id values per day
 - C Maximum of the event timestamp
 - D Count of the index names in the cluster

Answer: A

A cardinality metric estimates the number of distinct values, and it is accurate enough for dashboards on large data. Summing an identifier produces a meaningless total, and the maximum timestamp gives the latest event. Counting index names does not measure users.

7. Which dashboard feature opens another dashboard or URL when a user clicks an element of a chart?
- A Drilldown
 - B Panel border style
 - C Saved search export
 - D Runtime field script

Answer: A

A drilldown links a chart element to another dashboard, Discover or a URL, and it can pass the clicked value along. Panel borders only change appearance. Saved search exports and runtime fields do not respond to clicks.

8. Clicking a chart element to open another dashboard or Discover with values passed along is a _____.

Answer: drilldown (also accepted: drill-down, drill down)

A drilldown links a chart element to another dashboard, Discover or a URL, and it can carry the clicked value into the target. Dashboard settings name this feature drilldowns. Filter controls are different because they apply to every panel rather than to one click.

9. Which Maps layer shows the boundary of a region as a filled area?
- A Polygon layer built from a geo_shape field
 - B Heat map of point counts across the city
 - C Timeline chart of events by day
 - D Tag cloud of region names sized by document count

Answer: A

A polygon layer draws geo_shape areas, such as district boundaries, as filled regions. A heat map shows density of points, a timeline shows events over time, and a tag cloud is a word chart. Areas need geo_shape data and a polygon layer.

10. An analyst's point layer draws nothing even though the index has documents. Which check should come first?
- A Increase the number of primary shards in the index
 - B Confirm the field is mapped as geo_point and that the time range contains documents
 - C Rename the map title to a shorter name
 - D Disable TLS on the Elasticsearch cluster

Answer: B

An empty layer usually means the field is not a geo_point or the time range excludes the documents, so those are the first checks. Adding primary shards, renaming the map and disabling TLS do not address the layer's data source. Checking the mapping and the time range is the efficient diagnosis.