

PRACTICE QUESTIONS

Splunk Core Certified User

SHARED BY [u/bravehawk1997](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Splunk Core Certified User

Shared by [u/bravehawk1997](#) on aiexamcerts

10 practice questions for the Splunk Core Certified User exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/splunk/splunk-core-certified-user. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. An analyst needs to see only the first 10 events of a search result. Which command should be added to the search?

- A head 10
- B tail 10
- C top 10
- D dedup 10

Answer: A

The head command returns the first N results in the current sort order, so head 10 keeps ten events. tail returns the last events instead, and top summarizes the most common values rather than returning raw events. dedup 10 keeps up to ten copies of each duplicate value, so it does not limit the result to ten events.

2. Adjacent search terms with no operator between them are combined with an implicit OR.

- A True
- B False

Answer: B (False)

Splunk combines adjacent terms with an implicit AND, so error timeout returns only events that contain both words. An explicit OR is needed when either term is acceptable, and the implicit operator is not OR.

3. Which command removes the fields source and sourcetype from the search results?

- A fields + source sourcetype
- B table source sourcetype
- C rename source sourcetype
- D fields - source sourcetype

Answer: D

fields with a minus sign removes the listed fields from the results. fields with a plus sign keeps only the listed fields, which is the opposite effect. table displays the listed fields as columns, and rename changes field names rather than removing them.

4. The stats command groups its results with the _____ clause, as in stats count by host.

Answer: by

The by keyword names the fields to group on and is written after the aggregation functions. Without by, stats returns one row covering all events. Adding by host produces one row per host.

5. Which two searches calculate the total bytes for each host? (Choose two.)

- A stats sum(bytes) by host
- B chart sum(bytes) over host
- C top bytes by host
- D rare host bytes
- E sort -bytes by host

Answer: A, B

stats and chart both aggregate bytes with sum() and group the results by host. top and rare count how often values appear rather than summing a numeric field, and sort only reorders results.

6. Which command renames the field src_ip to source_address in the search results?

- A fields src_ip AS source_address
- B replace src_ip with source_address
- C alias src_ip source_address
- D rename src_ip as source_address

Answer: D

rename uses the form rename oldname as newname to change a field name in the results while keeping its values. fields only selects or removes fields, replace changes field values rather than names, and alias is not a search command.

7. Which file format is the standard choice for a Splunk lookup table uploaded through the web interface?

- A XML
- B CSV
- C PDF
- D Parquet

Answer: B

CSV is the standard lookup table format and is uploaded through Settings or a lookup definition. XML and PDF are not lookup table formats, and Parquet is not a standard format for Splunk lookup tables.

8. A saved report can be scheduled only by the Splunk administrator, and its results cannot be shared with other users.

- A True
- B False

Answer: B (False)

Saved reports can be scheduled by users with the right permissions, and their results can be shared with roles or users. The schedule is set in the saved search settings, and sharing is controlled by permissions.

9. Which search command reads the rows of a lookup table as its results?

- A outputlookup
- B lookup
- C inputlookup
- D readlookup

Answer: C

inputlookup returns the rows of a lookup table as results and can be placed at the start of a search. outputlookup writes search results to a lookup file, lookup enriches existing events with lookup fields, and readlookup is not a Splunk search command.

10. Which index holds Splunk's own internal operational logs?

- A _internal
- B main
- C summary
- D _audit

Answer: A

_internal holds Splunk's operational logs, such as splunkd and metrics data. main is the default index for user data, summary holds saved summary results, and _audit records audit trail activity such as searches run by users.