

PRACTICE QUESTIONS

Splunk Core Certified Power User

SHARED BY [u/happy_heron_53](#) on aiexamcerts

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

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

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

EXAM	Splunk Core Certified Power User
------	----------------------------------

Shared by [u/happy_heron_53](#) on aiexamcerts

10 practice questions for the Splunk Core Certified Power 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-power-user. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. Which stats function counts only the unique values of a field?

- A `dc()`
- B `count()`
- C `values()`
- D `list()`

Answer: A

`dc` returns the distinct count of a field's values. `count` returns the number of events, which is the tempting wrong choice. `values` returns unique values themselves, while `list` returns every value including duplicates, so neither returns a number of distinct values.

2. Search-time field extractions are applied when a search runs, so changes take effect without reindexing the data.

- A True
- B False

Answer: A (True)

Search-time extractions run as each search executes, so a change takes effect without reindexing. The tempting confusion is with index-time fields, which are fixed when the data is written.

3. What does the `strftime` function do?

- A Rounds a number down to a whole value
- B Formats a time value as text using a format string
- C Converts a text value into a number so math can run
- D Returns the length of a string

Answer: B

`strftime` formats an epoch time value as text using a pattern such as `%Y-%m-%d`. `tonumber` converts text to a number, `len` returns string length and `round` handles numeric rounding, so each is a tempting but different function.

4. The command that keeps only the named fields as columns in a table-formatted result is _____.

Answer: table

table displays only the named fields as columns, in the order given. fields can also keep or remove fields for the rest of the pipeline, but it does not format a table, which makes it the tempting near-miss.

5. Which two statements about the index field are true? (Choose two.)

- A index=web restricts results to the web index
- B Events are stored in indexes on the indexers
- C The index field is always stored in the _time field
- D The tstats command cannot filter on the index field
- E The index is an optional knowledge object

Answer: A, B

index=web restricts a search to that index, and indexed events live on the indexers. The index is not stored in _time, tstats can filter on index, and the index is not a knowledge object, so those statements are tempting but false.

6. Which alert type evaluates its conditions continuously over a rolling window as events arrive?

- A Ad hoc search
- B Summary report
- C Real-time alert
- D Scheduled alert

Answer: C

A real-time alert evaluates a sliding window as events arrive, while a scheduled alert runs its search on a timetable. An ad hoc search is run by a user, and a summary report is not an alert, which makes both tempting but wrong.

7. Which command writes the results of a search into a lookup table?

- A inputlookup
- B lookup
- C collect index=lookup
- D outputlookup

Answer: D

outputlookup writes search results into a lookup file or KV store collection. inputlookup reads from a lookup, lookup enriches events and collect writes results into an index, which makes collect the tempting wrong destination.

8. Event types are stored as event data in the index alongside the raw events they describe.

- A True
- B False

Answer: B (False)

Event types are saved definitions held as configuration, not as data in the index. The tempting confusion is that a type sits with the events it matches.

9. A macro takes two arguments. Which form calls it correctly in a search?

- A ``mymacro(10, hour)``
- B `[mymacro 10 hour]`
- C `macro(mymacro, 10, hour)`
- D `$mymacro(10, hour)$`

Answer: A

Macros are called by wrapping the name and its arguments in backticks, with the arguments in parentheses. Square brackets start a subsearch, and the other two forms are token or function syntax that a search does not use for macros.

10. Which command groups events that share a session identifier into one result, using start and end conditions?

- A dedup
- B stats count
- C fillnull
- D transaction

Answer: D

transaction groups related events by fields such as `session_id` and can use `startswith` and `endswith` conditions to mark the boundaries. `dedup` removes duplicates and `stats count` summarizes events without forming sessions, which makes it the tempting choice. `fillnull` replaces null values.