

PRACTICE QUESTIONS

Splunk Core Certified Advanced Power User

SHARED BY [u/Breezy-Moose-1805](#) on aiexamcerts

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

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

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

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

Shared by [u/Breezy-Moose-1805](#) on aiexamcerts

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

1. Which rex option replaces matched text in a field using a sed-style expression?

- A field=_raw only
- B erex
- C max_match=0
- D mode=sed

Answer: D

rex mode=sed performs substitutions on the named field during the search. max_match controls how many matches are captured, and erex builds a regex from example values. Field selection alone does not substitute text, which makes it a tempting but incomplete option.

2. Report acceleration stores a copy of the raw events in a summary index.

- A True
- B False

Answer: B (False)

Report acceleration keeps summaries of a report's results, not copies of the raw events. The tempting mix-up is with summary indexes, which an admin fills deliberately with collect.

3. An alert has throttling set to 30 minutes. What does throttling do during that window?

- A It forces the search to run in real time
- B It suppresses repeat alert actions for matching results
- C It deletes the older results from the search cache and the index
- D It increases the search frequency

Answer: B

Throttling suppresses repeated alert actions for matching results during the window. It does not delete results or change how often the search runs, which makes the search-frequency option a tempting misreading.

4. In a data model, the top-level object that child objects inherit their base constraints from is the _____ object.

Answer: root

A root object defines the base constraints and fields, and child objects narrow it further. Child objects are the tempting term, because they are the ones built on top of the root.

5. Which two statements about stats and tstats are correct? (Choose two.)
- A stats runs over the events returned by a search
 - B tstats can only read indexed fields and accelerated data model summaries
 - C tstats is always slower than stats on raw events
 - D stats can read accelerated summaries directly without a data model
 - E tstats cannot use a by clause

Answer: A, B

stats aggregates the events a search returns, and tstats is limited to indexed fields and accelerated summaries. tstats is usually faster than stats on raw events, and stats does not read summaries without a data model, so the last three statements are tempting but wrong.

6. Which workflow action type opens a web address built from field values, such as \$host\$?
- A Dashboard input
 - B Summary index action
 - C Link workflow action
 - D Search workflow action

Answer: C

A link workflow action builds a URL from field values and opens it. A search workflow action runs a new search instead, which makes it the tempting alternative. Dashboard inputs and summary index actions do not open web addresses.

7. Which props.conf setting extracts JSON keys into fields at search time without a regex?
- A SEDCMD-json
 - B TRANSFORMS-json
 - C FIELDALIAS-json
 - D KV_MODE = json

Answer: D

KV_MODE = json tells search-time extraction to parse JSON keys into fields. SEDCMD changes raw text at index time, TRANSFORMS is an index-time setting with a regex, and FIELDALIAS only renames existing fields, so those are tempting but wrong for this purpose.

8. Summary range controls how far back a data model's acceleration summaries cover.
- A True
 - B False

Answer: A (True)

Summary range sets the period that acceleration summarizes, so data older than the range is not covered by summaries. The tempting misconception is that summary range sets how long raw events are retained.

9. A subsearch must return one row to be used in an outer comparison. Which command keeps only the first row?
- A head 1
 - B tail 1
 - C dedup
 - D fillnull

Answer: A

head 1 keeps only the first row, so the outer search receives one value. tail 1 keeps the last row, which is a tempting but different result, and dedup and fillnull do not limit the number of rows.

10. Which eval expression tests whether a field has a value before a comparison?
- A tostring()
 - B isnotnull()
 - C len()
 - D round()

Answer: B

isnotnull returns true when the field has a value, so a search can filter out empty results before comparing. len counts characters, round rounds numbers and tostring converts a value to text, so each one is a tempting but different function.