

PRACTICE QUESTIONS

Splunk Core Certified Power User

SHARED BY [u/curiousbeacon1986](#) on aiexamcerts

EDITION	Free Set 1
---------	------------

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

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

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

Shared by [u/curiousbeacon1986](#) 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 search mode puts speed first by limiting field discovery to the fields the search needs?

- A Slow mode
- B Fast mode
- C Verbose mode
- D Smart mode

Answer: B

Fast mode skips most field discovery and returns results quickly. Verbose mode returns every event and field and is the slowest, while Smart mode is the default balance between the two. Slow mode is not a Splunk search mode, but it is a tempting name.

2. In `props.conf`, the setting prefix that defines a search-time field extraction is _____.

Answer: EXTRACT (also accepted: EXTRACT-)

EXTRACT- defines an inline regular expression that pulls a field out of events at search time, while REPORT- points to a transform for more complex work. TRANSFORMS works at index time, which makes it the tempting alternative.

3. What does the `dedup` command do when `host` is given as the field?

- A Adds a count of each host value
- B Sorts the events by host name
- C Removes the host field from every event in the results
- D Keeps the first event for each unique host value

Answer: D

`dedup` keeps the first event it sees for each value of the field, removing the repeats. Adding a count is a stats job, sorting is done by `sort`, and removing a field is done by the `fields` command, which makes the last option a tempting confusion.

4. A scheduled report cannot write its results to a summary index.

- A True
- B False

Answer: B (False)

A scheduled report can be configured with a summary indexing action, or a `collect` command in its search, so the statement is false. The tempting belief is that scheduled reports are read-only.

5. Which two statements about the lookup command are true? (Choose two.)

- A lookup adds fields from a lookup table to each matching event
- B lookup permanently changes the lookup file
- C The OUTPUT keyword names the fields to add to events
- D lookup works only on indexed fields
- E lookup requires a summary index to run

Answer: A, C

The lookup command matches event fields against a table and adds the fields named by OUTPUT or OUTPUTNEW. It does not change the lookup file, and it works on any extracted field, not only indexed ones, so the last two statements are tempting but false.

6. A dashboard needs a dropdown that changes the search for every panel on the page. Which feature provides it?

- A A dropdown input that sets a token
- B A lookup definition for the dropdown
- C A summary index
- D An acceleration summary

Answer: A

A dropdown input sets a token, and panel searches that reference that token update when the user picks a value. Lookup definitions enrich events and summary indexes store results, which makes them tempting wrong fits for an interactive control.

7. Which search returns events where status is 500 and host is web01?

- A `status==500 & host==web01`
- B `status=500 host=web01`
- C `status=500 OR host=web01`
- D `status=500 | host=web01`

Answer: B

Terms separated by a space are combined with AND, so both conditions must hold. OR returns events matching either condition, which is the tempting mistake. The pipe followed by a bare field comparison and the double-equals and ampersand forms are not valid search syntax.

8. A subsearch is enclosed in _____ brackets within the outer search.

Answer: square (also accepted: [], square brackets)

Square brackets mark a subsearch, which runs first and passes its results into the outer search. Parentheses group logical conditions, which makes them the tempting wrong choice.

9. Which eval function returns one value when a condition is true and another value when it is false?

- A len()
- B round()
- C if()
- D isnull()

Answer: C

if(condition, true_value, false_value) chooses between two results based on a condition. isnull tests for null, len counts characters and round rounds numbers, so each one is a tempting but different function.

10. Which knowledge object attaches a label to field values, such as marking a host as production?

- A Macro
- B Calculated field
- C Field alias
- D Tag

Answer: D

A tag attaches a label to a field-value pair, so a search can use tag=production. Macros are search fragments, calculated fields compute new values and field aliases rename fields, so each one is a tempting but different tool.