

PRACTICE QUESTIONS

# Splunk Core Certified Advanced Power User

SHARED BY [u/noblellama1979](#) on aiexamcerts

---

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

|           |    |
|-----------|----|
| QUESTIONS | 10 |
|-----------|----|

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

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

---

Shared by [u/noblellama1979](#) 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](http://www.aiexamcerts.com/splunk/splunk-core-certified-advanced-power-user). Spotted a mistake? Email [support@aiexamcerts.com](mailto:support@aiexamcerts.com) with the exam name and the question number.

1. Which props.conf setting masks sensitive digits in stored events using a regex substitution at index time?

- A FIELDALIAS-
- B EVAL-
- C SEDCMD-
- D EXTRACT-

**Answer: C**

SEDCMD- applies a sed-style substitution to the raw event at index time, so the stored text is masked. EXTRACT and EVAL work at search time, and FIELDALIAS only renames fields, which makes them tempting but unable to mask data already stored.

2. In transforms.conf, index-time routing to a different index uses DEST\_KEY set to \_\_\_\_\_.

**Answer: \_MetaData:Index** (also accepted: MetaData:Index)

DEST\_KEY = \_MetaData:Index with a FORMAT naming the target index changes which index an event is written to. DEST\_KEY set to queue with nullQueue discards events instead, which makes it the tempting different routing.

3. A dashboard token holds user input that goes into a search, and quotes in the input must not break the query. Which token form escapes it?

- A \$token|s\$
- B \$token\$
- C [token] in double brackets
- D %token%

**Answer: A**

The |s modifier escapes the value for use inside a search string. Plain \$token\$ inserts the value unchanged, which is the tempting but risky default. Double brackets and percent signs are not Splunk token syntax.

4. Dashboard Studio dashboards are defined in JSON.

- A True
- B False

**Answer: A (True)**

Dashboard Studio stores dashboard definitions as JSON, and the source view can be edited directly. The tempting misconception is that Simple XML is the only dashboard source format.

5. Which two statements about data model acceleration are true? (Choose two.)

- A Acceleration builds its summaries in the background
- B Acceleration deletes raw events from the index after summarizing them
- C Summary range sets how far back the summaries are kept
- D Accelerated objects are hidden from pivot
- E tstats cannot use a by clause

**Answer: A, C**

Acceleration builds summaries in the background, and summary range controls how far back those summaries cover. Acceleration does not delete raw events, and accelerated objects remain usable in pivot, so the second and fourth statements are tempting but false.

6. Which command reports statistics over data stored in a summary index?

- A outputlookup
- B sistats
- C tstats
- D fillnull

**Answer: B**

sistats computes statistics over summary index data in the same way stats works on raw events, and it is built for stored partial results. tstats is for indexed fields and data model summaries, which makes it the tempting alternative. fillnull and outputlookup do not report statistics from summaries.

7. A CIM Authentication data model is needed to find failed logins. Which add-on provides the CIM data models?

- A Splunk Deployment Server
- B Splunk Monitoring Console
- C Splunk Common Information Model add-on
- D Splunk Universal Forwarder on each host

**Answer: C**

The Common Information Model add-on provides standard data models such as Authentication, Web and Network Traffic. The forwarder delivers data, the deployment server manages configuration and the monitoring console checks health, so each of those is a tempting but different component.

8. The tstats argument that adds the results of an earlier tstats search to the current output is named \_\_\_\_\_.

**Answer: append** (also accepted: append=true)

append=true adds the results of a preceding tstats search to the current output. prestats prepares partial results for a later stats command, which makes it the tempting confusion.

9. Which command runs a search once for each row of the results it receives?

- A dedup
- B eventstats
- C fields
- D map

**Answer: D**

map runs a search for each input row, which is powerful but often slow and resource heavy. dedup, eventstats and fields do not run a search per row, which makes them tempting but different commands.

---

10. Which command turns x and y fields into a wide table, with the y values becoming columns?

- A xyseries
- B untable
- C eventstats
- D mvexpand

**Answer: A**

xyseries pivots rows into a wide table, using the x field as rows and the y field values as columns. untable does the reverse, which makes it the tempting wrong answer, and mvexpand splits multivalue fields into rows.