



**Splunk**

**Exam Questions SPLK-1002**

Splunk Core Certified Power User Exam

### NEW QUESTION 1

- (Exam Topic 1)

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

- A. | datamodel web search | filed web \*
- B. | Search datamodel web web | filed web\*
- C. | datamodel web web field | search web\*
- D. Datamodel=web | search web | filed web\*

**Answer: A**

### NEW QUESTION 2

- (Exam Topic 1)

Which of the following searches show a valid use of macro? (Select all that apply)

```
index=main source=mySource oldField=* | `makeMyField(oldField)` | table _time newField
index=main source=mySource oldField=* | stats if(`makeMyField(oldField)`) | table _time newField
index=main source=mySource oldField=* | eval newField=`makeMyField(oldField)` | table _time newField
index=main source=mySource oldField=* | "`newField(`makeMyField(oldField)`)" | table _time newField
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: AC**

### NEW QUESTION 3

- (Exam Topic 1)

Which of the following statements about event types is true? (select all that apply)

- A. Event types can be tagged.
- B. Event types must include a time range,
- C. Event types categorize events based on a search.
- D. Event types can be a useful method for capturing and sharing knowledge.

**Answer: AC**

### NEW QUESTION 4

- (Exam Topic 1)

Which of the following statements describe calculated fields? (select all that apply)

- A. Calculated fields can be used in the search bar.
- B. Calculated fields can be based on an extracted field.
- C. Calculated fields can only be applied to host and sourcetype.
- D. Calculated fields are shortcuts for performing calculations using the eval command.

**Answer: BD**

### NEW QUESTION 5

- (Exam Topic 1)

Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. Configuration of GET workflow actions includes choosing a sourcetype.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. GET workflow actions can be configured to open the URT link in the current window or in a new window

**Answer: D**

### NEW QUESTION 6

- (Exam Topic 1)

Which of the following statements describes POST workflow actions?

- A. POST workflow actions are always encrypted.
- B. POST workflow actions cannot use field values in their URI.
- C. POST workflow actions cannot be created on custom sourcetypes.
- D. POST workflow actions can open a web page in either the same window or a new .

**Answer: D**

#### NEW QUESTION 7

- (Exam Topic 1)

After manually editing a regular expression (regex), which of the following statements is true?

- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

**Answer: D**

#### NEW QUESTION 8

- (Exam Topic 1)

Which of the following knowledge objects represents the output of an oval expression?

- A. Eval fields
- B. Calculated fields
- C. Field extractions
- D. Calculated lookups

**Answer: C**

#### NEW QUESTION 9

- (Exam Topic 1)

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

- A. Both will appear in the All Fields list, but only if the alias is specified in the search.
- B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
- C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
- D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event\_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

**Answer: CD**

#### NEW QUESTION 10

- (Exam Topic 1)

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. Fast mode is enabled.
- B. The dashboard is private.
- C. The extraction is private
- D. The person in the organization running the report does not have access to the index.

**Answer: BD**

#### NEW QUESTION 13

- (Exam Topic 1)

Which of the following workflow actions can be executed from search results? (select all that apply)

- A. GET
- B. POST
- C. LOOKUP
- D. Search

**Answer: ABD**

#### NEW QUESTION 14

- (Exam Topic 1)

Selected fields are displayed \_\_\_\_\_ each event in the search results.

- A. below
- B. interesting fields
- C. other fields
- D. above

**Answer:** A

**NEW QUESTION 19**

- (Exam Topic 1)

A space is an implied \_\_\_\_\_ in a search string.

- A. OR
- B. AND
- C. ()
- D. NOT

**Answer:** B

**NEW QUESTION 23**

- (Exam Topic 1)

What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

- A. Creates a table of the total count of users and split by corndogs.
- B. Creates a table of the total count of mysterymeat corndogs split by user.
- C. Creates a table with the count of all types of corndogs eaten split by user.
- D. Creates a table that groups the total number of users by vegetarian corndogs.

**Answer:** A

**NEW QUESTION 26**

- (Exam Topic 1)

What does the transaction command do?

- A. Groups a set of transactions based on time.
- B. Creates a single event from a group of events.
- C. Separates two events based on one or more values.
- D. Returns the number of credit card transactions found in the event logs.

**Answer:** B

**NEW QUESTION 31**

- (Exam Topic 2)

Which workflow uses field values to perform a secondary search?

- A. POST
- B. Action
- C. Search
- D. Sub-Search

**Answer:** C

**Explanation:**

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb>

**NEW QUESTION 33**

- (Exam Topic 2)

The gauge command:

- A. creates a single-value visualization
- B. allows you to set colored ranges for a single-value visualization
- C. creates a radial gauge visualization

**Answer:** B

**NEW QUESTION 36**

- (Exam Topic 2)

We can use the rename command to \_\_\_\_\_ (Select all that apply.)

- A. Change indexed fields
- B. Exclude fields from our search results
- C. Extract new fields from our data using regular expressions
- D. Give a field a new name at search time

**Answer:** D

**NEW QUESTION 38**

- (Exam Topic 2)

Using the export function, you can export search results as \_\_\_\_\_.( Select all that apply)

- A. Xml
- B. Json
- C. Html
- D. A php file

**Answer:** AB

#### **NEW QUESTION 43**

- (Exam Topic 2)

When using the transaction command, what does the argument maxspan do?

- A. Sets the maximum total time between events in a transaction.
- B. Sets the maximum length of all events within a transaction.
- C. Sets the maximum total time between the earliest and latest events in a transaction.
- D. Sets the maximum length that any single event can reach to be included in the transaction.

**Answer:** B

#### **NEW QUESTION 45**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SPLK-1002 Practice Exam Features:

- \* SPLK-1002 Questions and Answers Updated Frequently
- \* SPLK-1002 Practice Questions Verified by Expert Senior Certified Staff
- \* SPLK-1002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SPLK-1002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The SPLK-1002 Practice Test Here](#)