

# Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

<https://www.2passeasy.com/dumps/SPLK-1002/>



**NEW QUESTION 1**

- (Exam Topic 1)

Which of the following eval command function is valid?

- A. Int ()
- B. Count ()
- C. Print ()
- D. ToString ()

**Answer: D**

**NEW QUESTION 2**

- (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 3**

- (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 4**

- (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 5**

- (Exam Topic 1)

Which of the following statements is true, especially in large environments?

- A. Use the scats command when you next to group events by two or more fields.
- B. The stats command is faster and more efficient than the transaction command
- C. The transaction command is faster and more efficient than the stats command.
- D. Use the transaction command when you want to see the results of a calculation.

**Answer: B**

**NEW QUESTION 6**

- (Exam Topic 1)

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

- A. Rank
- B. Weight
- C. Priority
- D. Precedence

**Answer: C**

#### NEW QUESTION 7

- (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 8

- (Exam Topic 1)

What is the relationship between data models and pivots?

- A. Data models provide the datasets for pivots.
- B. Pivots and data models have no relationship.
- C. Pivots and data models are the same thing.
- D. Pivots provide the datasets for data models.

**Answer: D**

#### NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 1)

Which of the following file formats can be extracted using a delimiter field extraction?

- A. CSV
- B. PDF
- C. XML
- D. JSON

**Answer: A**

#### NEW QUESTION 14

- (Exam Topic 1)

What do events in a transaction have in common?

- A. All events in a transaction must have the same timestamp.
- B. All events in a transaction must have the same sourcetype.
- C. All events in a transaction must have the exact same set of fields.
- D. All events in a transaction must be related by one or more fields.

**Answer: B**

#### NEW QUESTION 17

- (Exam Topic 1)

What are the two parts of a root event dataset?

- A. Fields and variables.
- B. Fields and attributes.
- C. Constraints and fields.
- D. Constraints and lookups.

**Answer:**

C

**NEW QUESTION 20**

- (Exam Topic 1)

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

**Answer: D****NEW QUESTION 21**

- (Exam Topic 1)

When using timechart, how many fields can be listed after a by clause? ( Choose Two )

- A. because timechart doesn't support using a by clause.
- B. because `_time` is already implied as the x-axis.
- C. because one field would represent the x-axis and the other would represent the y-axis.
- D. There is no limit specific to timechart.

**Answer: BD****NEW QUESTION 22**

- (Exam Topic 1)

Which of the following statements describes Search workflow actions?

- A. By default
- B. Search workflow actions will run as a real-time search.
- C. Search workflow actions can be configured as scheduled searches,
- D. The user can define the time range of the search when created the workflow action.
- E. Search workflow actions cannot be configured with a search string that includes the transaction command

**Answer: C****NEW QUESTION 24**

- (Exam Topic 1)

Which of the following statements describes this search? `sourcetype=access_combined | transaction JSESSIONID | timechart avg (duration)`

- A. This is a valid search and will display a timechart of the average duration, of each transaction event.
- B. This is a valid search and will display a stats table showing the maximum pause among transactions.
- C. No results will be returned because the transaction command must include the `startswith` and `endswith` options.
- D. No results will be returned because the transaction command must be the last command used in the search pipeline.

**Answer: A****NEW QUESTION 25**

- (Exam Topic 1)

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

- A. Tabs
- B. Pipes
- C. Spaces
- D. Commas

**Answer: ABCD****NEW QUESTION 29**

- (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 32**

- (Exam Topic 1)

A calculated field maybe based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

**Answer:** B

**NEW QUESTION 34**

- (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 35**

- (Exam Topic 2)

The transaction command allows you to \_\_\_\_\_ events across multiple sources

- A. duplicate
- B. correlate
- C. persist
- D. tag

**Answer:** B

**NEW QUESTION 37**

- (Exam Topic 2)

Which of the following are valid options to speed up reports? (Select all the apply.)

- A. Edit permissions
- B. Edit description
- C. Edit acceleration
- D. Edit schedule

**Answer:** C

**NEW QUESTION 42**

- (Exam Topic 2)

Splunk alerts can be based on search that run \_\_\_\_\_. (Select all that apply.)

- A. in real-time
- B. on a regular schedule
- C. and have no matching events

**Answer:** AB

**NEW QUESTION 46**

- (Exam Topic 2)

By default search results are not returned in \_\_\_\_\_ order.

- A. Chronological
- B. Reverser chronological
- C. ASCIE
- D. Alphabetical

**Answer:** AD

**NEW QUESTION 49**

- (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 50**

- (Exam Topic 2)

Which of the following searches will show the number of categoryId used by each host?

- A. Sourcetype=access\_\* |sum bytes by host
- B. Sourcetype=access\_\* |stats sum(category|
- C. by host
- D. Sourcetype=access\_\* |sum(bytes) by host
- E. Sourcetype=access\_\* |stats sum by host

**Answer: B**

**NEW QUESTION 52**

- (Exam Topic 2)

Which search would limit an "alert" tag to the "host" field?

- A. tag=alert
- B. host::tag::alert
- C. tag==alert
- D. tag::host=alert

**Answer: D**

**NEW QUESTION 55**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1002 Product From:

<https://www.2passeasy.com/dumps/SPLK-1002/>

## Money Back Guarantee

### **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