

## 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 Statements about macros is true? (select all that apply)

- A. Arguments are defined at execution time.
- B. Arguments are defined when the macro is created.
- C. Argument values are used to resolve the search string at execution time.
- D. Argument values are used to resolve the search string when the macro is created.

**Answer:** AC

#### NEW QUESTION 2

- (Exam Topic 1)

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

- A. Use the stats 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 3

- (Exam Topic 1)

Which of the following statements describes the command below (select all that apply) sourcetype-access\_combined | transaction JSESSIONID

- A. An additional field named maxspan is created.
- B. An additional field named duration is created.
- C. An additional field named eventcount is created.
- D. Events with the same JSESSIONID will be grouped together into a single event.

**Answer:** BCD

#### NEW QUESTION 4

- (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 5

- (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 6

- (Exam Topic 1)

A user wants to convert field values to string and also to sort on those value. Which command should be used first, the eval or the sort?

- A. It doesn't matter whether eval or sort is used first.
- B. Convert the numeric to a string with eval first, then sort.
- C. Use sort first, then convert the numeric to a string with eval.
- D. You cannot use the sort command and the eval command on the same field.

**Answer:** B

#### NEW QUESTION 7

- (Exam Topic 1)

Which of the following can be used with the eval command tostring function (select all that apply)

- A. "hex"
- B. "commas"
- C. "Decimal"
- D. "duration"

**Answer:** ABD

#### NEW QUESTION 8

- (Exam Topic 1)

Which of the following describes the Splunk Common Information Model (CIM) add-on?

- A. The CIM add-on uses machine learning to normalize data.
- B. The CIM add-on contains dashboards that show how to map data.
- C. The CIM add-on contains data models to help you normalize data.
- D. The CIM add-on is automatically installed in a Splunk environment.

**Answer:** C

#### NEW QUESTION 9

- (Exam Topic 1)

How does a user display a chart in stack mode?

- A. By using the stack command.
- B. By turning on the Use Trellis Layout option.
- C. By changing Stack Mode in the Format menu.
- D. You cannot display a chart in stack mode, only a timechart.

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

When should you use the transaction command instead of the scats command?

- A. When you need to group on multiple values.
- B. When duration is irrelevant in search result
- C. .
- D. When you have over 1000 events in a transaction.
- E. When you need to group based on start and end constraints.

**Answer:** C

#### NEW QUESTION 10

- (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 14

- (Exam Topic 1)

Which of the following statements describe the search below? (select all that apply) Index=main | transaction clientip host maxspan=30s maxpause=5s

- A. Events in the transaction occurred within 5 seconds.
- B. It groups events that share the same clientip and host.
- C. The first and last events are no more than 5 seconds apart.
- D. The first and last events are no more than 30 seconds apart.

**Answer:** B

#### NEW QUESTION 17

- (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 19

- (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 23**

- (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 24**

- (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 27**

- (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 28**

- (Exam Topic 2)

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Fast
- B. Smart
- C. Verbose

**Answer:** C

**NEW QUESTION 33**

- (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 34**

- (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 35**

- (Exam Topic 2)

Which is not a comparison operator in Splunk

- A. <=
- B. =
- C. !=
- D. >
- E. ?=

**Answer:** E

#### NEW QUESTION 39

- (Exam Topic 2)

What will you learn from the results of the following search? sourcetype=cisco\_esa | transaction mid, dcid, icid | timechart avg(duration)

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

**Answer:** A

#### NEW QUESTION 42

.....

## 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