

# Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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



### NEW QUESTION 1

- (Exam Topic 1)

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configured the macro?

- A. The macro name is sessiontracker and the argument are action, JSESSION.
- B. The macro name is sessiontracker (2) and the action JSESSIONID
- C. The macro name is sessiontracker and the argument are sectional , \$ JSESSIONIDS.
- D. The macro name is sessiontracker (2) and the argument are \$action , \$JSESSIONIDS.

Answer: B

### NEW QUESTION 2

- (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 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 describe the search string below?  
dacamodel Application\_State All\_Application\_State search

- A. Events will be returned from dataset named Application\_state.
- B. Events will be returned from the data model named Application\_State.
- C. Events will be returned from the data model named All\_Application\_state.
- D. No events will be returned because the pipe should occur after the datamodel command

**Answer:** C

#### NEW QUESTION 6

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (QM)? (select all that apply)

- A. CIM is a methodology for normalizing data.
- B. CIM can correlate data from different sources.
- C. The Knowledge Manager uses the CIM to create knowledge objects.
- D. CIM is an app that can coexist with other apps on a single Splunk deployment.

**Answer:** AC

#### NEW QUESTION 7

- (Exam Topic 1)

Which of the following statements describes field aliases?

- A. Field alias names replace the original field name.
- B. Field aliases can be used in lookup file definitions.
- C. Field aliases only normalize data across sources and sourcetypes.
- D. Field alias names are not case sensitive when used as part of a search.

**Answer:** A

#### NEW QUESTION 8

- (Exam Topic 1)

When creating a Search workflow action, which field is required?

- A. Search string
- B. Data model name
- C. Permission setting
- D. An eval statement

**Answer:** A

#### NEW QUESTION 9

- (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 10

- (Exam Topic 1)

Which of the following searches will return events contains a tag name Privileged?

- A. Tag= Priv
- B. Tag= Priv\*
- C. Tag= Priv\*
- D. Tag= Privileged

**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 12

- (Exam Topic 1)

What is the correct syntax to search for a tag associated with a value on a specific fields?

- A. Tag-<field?
- B. Tag<filed(tagname.)
- C. Tag=<filed>::<tagname>
- D. Tag::<filed>=<tagname>

**Answer:** D

#### NEW QUESTION 17

- (Exam Topic 1)

Which of the following statements describes macros?

- A. A macro is a reusable search string that must contain the full search.
- B. A macro is a reusable search string that must have a fixed time range.
- C. A macro is a reusable search string that may have a flexible time range.
- D. A macro is a reusable search string that must contain only a portion of the search.

**Answer:** C

#### NEW QUESTION 18

- (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 22

- (Exam Topic 1)

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

- A. Index-main | REJECT trans sessionid
- B. Index-main | transaction sessionid | search REJECT
- C. Index=main | transaction sessionid | whose transaction=reject
- D. Index=main | transaction sessionid | where transaction=reject"

**Answer:** D

#### NEW QUESTION 23

- (Exam Topic 1)

What does the fillnull command replace null values with, if the value argument is not specified?

- A. N/A
- B. NaN
- C. NULL

**Answer:** A

#### NEW QUESTION 25

- (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 26

- (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 29

- (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 31

- (Exam Topic 1)

Which of the following are required to create a POST workflow action?

- A. Label, URI, search string.
- B. XMI attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

**Answer:** B

#### NEW QUESTION 35

- (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 38

- (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 39

- (Exam Topic 1)

In what order are the following knowledge objects/configurations applied?

- A. Field Aliases, Field Extractions, Lookups
- B. Field Extractions, Field Aliases, Lookups
- C. Field Extractions, Lookups, Field Aliases
- D. Lookups, Field Aliases, Field Extractions

**Answer:** B

#### NEW QUESTION 41

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 45

- (Exam Topic 1)

Which of the following statements describe data model acceleration? (select all that apply)

- A. Root events cannot be accelerated.
- B. Accelerated data models cannot be edited.
- C. Private data models cannot be accelerated.
- D. You must have administrative permissions or the accelerate\_dacamodel capability to accelerate a data model.

**Answer:**



BCD

#### NEW QUESTION 47

- (Exam Topic 1)

In which of the following scenarios is an event type more effective than a saved search?

- A. When a search should always include the same time range.
- B. When a search needs to be added to other users' dashboards.
- C. When the search string needs to be used in future searches.
- D. When formatting needs to be included with the search string.

**Answer:** D

#### NEW QUESTION 49

- (Exam Topic 1)

What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

- A. Macros.
- B. Field aliases.
- C. The rename command.
- D. CIM does not work with different names for the same field.

**Answer:** B

#### NEW QUESTION 52

- (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 53

- (Exam Topic 2)

The eval command 'if' function requires the following three arguments (in order):

- A. Boolean expression, result if true, result if false
- B. Result if true, result if false, boolean expression
- C. Result if false, result if true, boolean expression
- D. Boolean expression, result if false, result if true

**Answer:** A

#### NEW QUESTION 55

- (Exam Topic 2)

Which of the following commands will show the maximum bytes?

- A. sourcetype=access\_\* | maximum totals by bytes
- B. sourcetype=access\_\* | avg (bytes)
- C. sourcetype=access\_\* | stats max(bytes)
- D. sourcetype=access\_\* | max(bytes)

**Answer:** C

#### NEW QUESTION 56

- (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 59

- (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 62

- (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 66

- (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 69

- (Exam Topic 2)

What is a limitation of searches generated by workflow actions?

- A. Searches generated by workflow action cannot use macros.
- B. Searches generated by workflow actions must be less than 256 characters long.
- C. Searches generated by workflow action must run in the same app as the workflow action.
- D. Searches generated by workflow action run with the same permissions as the user running them.

**Answer:** D

#### NEW QUESTION 73

- (Exam Topic 2)

Which of the following statements describes the use of the Filed Extractor (FX)?

- A. The Field Extractor automatically extracts all field at search time.
- B. The Field Extractor uses PERL to extract field from the raw events.
- C. Field extracted using the Extracted persist as knowledge objects.
- D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

**Answer:** C

#### NEW QUESTION 77

- (Exam Topic 2)

Clicking a SEGMENT on a chart, \_\_\_\_\_.

- A. drills down for that value
- B. highlights the field value across the chart
- C. adds the highlighted value to the search criteria

**Answer:** C

#### NEW QUESTION 82

- (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 85

- (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 86**

.....



## 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