

# Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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



### NEW QUESTION 1

- (Exam Topic 1)

What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

- A. Custom visualizations
- B. Pre-configured data models
- C. Fields and event category tags
- D. Automatic data model acceleration

**Answer:** AC

### 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 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 5

- (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 6

- (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 7

- (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 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)

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 10

- (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 13

- (Exam Topic 1)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

**Answer:** B

#### NEW QUESTION 14

- (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 15

- (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 20

- (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 25

- (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 28

- (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 33

- (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 38

- (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 39

- (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 44

- (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 47

- (Exam Topic 1)

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

- A. Auto-Extracted fields can be hidden in Pivot.
- B. Auto-Extracted fields can have their data type changed.
- C. Auto-Extracted fields can be given a friendly name for use in Pivot.
- D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

**Answer:** B

#### NEW QUESTION 51

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 54

- (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 57

- (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 58

- (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 61



- (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 66

- (Exam Topic 1)

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

- A. The regex can no longer be edited.
- B. The field being extracted will be required for all future events.
- C. The events without the required field will not display in searches.
- D. Only events with the required string will be included in the extraction.

**Answer:** D

#### NEW QUESTION 70

- (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 71

- (Exam Topic 1)

A calculated field may be 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 74

- (Exam Topic 1)

When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

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

**Answer:** ABD

#### NEW QUESTION 77

- (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 79

- (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 82

- (Exam Topic 2)

which of the following are valid options with the chart command

- A. useother
- B. usenull
- C. fillfield
- D. usefiled

**Answer:** AB

#### NEW QUESTION 85

- (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 90

- (Exam Topic 2)

This tab shows you the event patterns in the results of a specific search.

- A. statistics
- B. visualization
- C. patterns

**Answer:** C

#### NEW QUESTION 91

- (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 94

- (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 99

- (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 101

- (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 103**

- (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 104**

- (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 107**

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

**Answer:** B

**NEW QUESTION 110**

- (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 114**

.....



## 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