

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 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 3

- (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 4

- (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 5

- (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 6

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (CIM)? (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)

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 8

- (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 9

- (Exam Topic 1)

Which of the following actions can the eval command perform?

- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

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

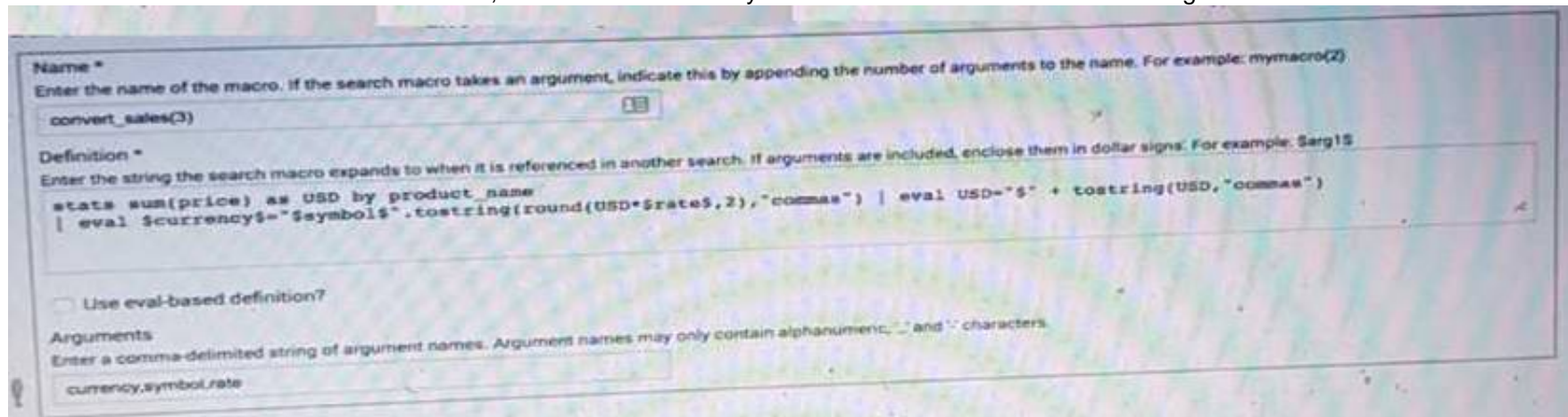
- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field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

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



- A. Convert_sales (euro, €, 79)"
- B. Convert_sales (euro, €, .79)
- C. Convert_sales (\$euro,\$€\$,s79\$
- D. Convert_sales (\$euro, \$€\$,S,79\$)

Answer: B

NEW QUESTION 12

- (Exam Topic 1)

Which of the following statements about tags is true?

- A. Tags are case insensitive.
- B. Tags are created at index time.
- C. Tags can make your data more understandable.
- D. Tags are searched by using the syntax tag: : <fieldname>

Answer: C

NEW QUESTION 15

- (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)

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)

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 21

- (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 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 28

- (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 30

- (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 31

- (Exam Topic 1)

What is required for a macro to accept three arguments?

- A. The macro's name ends with (3).
- B. The macro's name starts with (3).
- C. The macro's argument count setting is 3 or more.
- D. Nothing, all macros can accept any number of arguments.

Answer: A

NEW QUESTION 34

- (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 36

- (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 40

- (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 41

- (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 45

- (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 47

- (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 51

- (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 54

- (Exam Topic 2)

These allow you to categorize events based on search terms. Select your answer.

- A. Groups
- B. Event Types
- C. Macros
- D. Tags

Answer: B

NEW QUESTION 56

.....

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