

Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



NEW QUESTION 1

- (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 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 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 4

- (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 5

- (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 6

- (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 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)

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)

Data model are composed of one or more of which of the fo-owing datasets? (select all that apply.)

- A. Events datasets
- B. Search datasets
- C. Transaction datasets
- D. Any child of event, transaction, and search datasets

Answer: ABC

NEW QUESTION 10

- (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 15

- (Exam Topic 1)

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

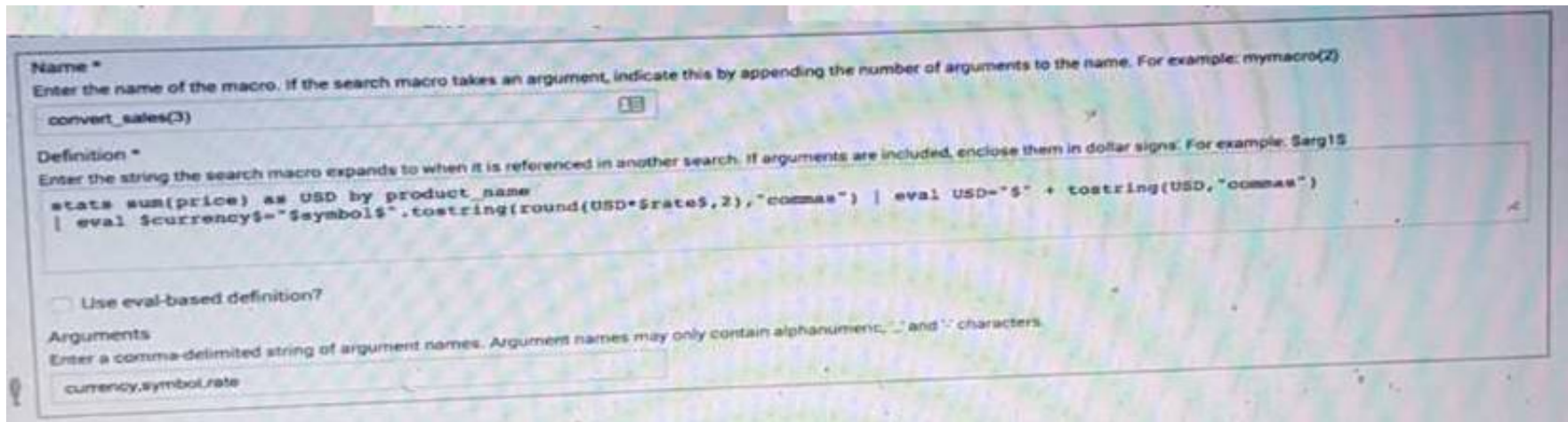
- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field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

Answer: D

NEW QUESTION 20

- (Exam Topic 1)

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



The screenshot shows the 'Macro Definition' form in Splunk. The 'Name' field is 'convert_sales(3)'. The 'Definition' field contains the following code: `stats sum(price) as USD by product_name | eval $currency$="$symbol$".tostring(round(USD*$rate$,2),"comma") | eval USD="$" + tostring(USD,"comma")`. The 'Arguments' field is 'currency,symbol,rate'. There is a checkbox for 'Use eval-based definition?' which is unchecked.

- 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 24

- (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 28

- (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 33

- (Exam Topic 1)

Which one of the following statements about the search command is true?

- A. It does not allow the use of wildcards.
- B. It treats field values in a case-sensitive manner.
- C. It can only be used at the beginning of the search pipeline.
- D. It behaves exactly like search strings before the first pipe.

Answer: C

NEW QUESTION 36

- (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 39

- (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 44

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Answer: CD

NEW QUESTION 48

- (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 49

- (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 51

- (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 56

- (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 57

- (Exam Topic 1)

Which of the following statements about data models and pivot are true? (select all that apply)

- A. They are both knowledge objects.
- B. Data models are created out of datasets called pivots.
- C. Pivot requires users to input SPL searches on data models.
- D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Answer: BD

NEW QUESTION 62

- (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 64

- (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 67

- (Exam Topic 1)

A space is an implied _____ in a search string.

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

Answer: B

NEW QUESTION 71

- (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 72

- (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 74

- (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 78

- (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 82

- (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 83

- (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 84

- (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 87

- (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 91

- (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 93

- (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 98

- (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 100

- (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 104

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1002 Practice Test Here](#)