SPLK-1002 Dumps

Splunk Core Certified Power User Exam

https://www.certleader.com/SPLK-1002-dumps.html

NEW QUESTION 1
- (Exam Topic 1)
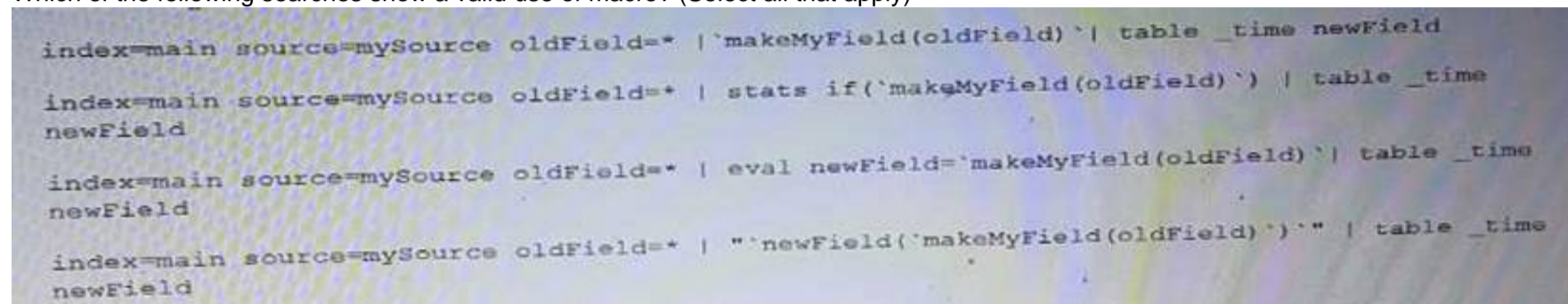Which of the following Statements about macros is true? (select all that apply)

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 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 describes the command below (select all that apply) sourcetype-access_combined | transaction JSESSIONID

A. An additional filed named maxspan is created.
B. An additional Held 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)
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 5
- (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 6
- (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 7
- (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: : <fieldneme>

Answer: C

NEW QUESTION 8
- (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 9
- (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 10
- (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 10
- (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 13
- (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 14
- (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 16
- (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 18
- (Exam Topic 1)
Which of the following are required to create a POST workflow action?

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

Answer: B

NEW QUESTION 20
- (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 25
- (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 28
- (Exam Topic 1)
What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. Creates a table of the total count of users and split by corndogs.
B. Creates a table of the total count of mysterymeat corndogs split by user.

C. Creates a table with the count of all types of corndogs eaten split by user.
D. Creates a table that groups the total number of users by vegetarian corndogs.

Answer: A

NEW QUESTION 29
- (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 30
- (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 31
- (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 35
- (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 39
- (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 41
- (Exam Topic 2)
These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Answer: BC

NEW QUESTION 42
- (Exam Topic 2)
We can use the rename command to _____ (Select all that apply.)

A. Change indexed fields

B. Exclude fields from our search results
C. Extract new fields from our data using regular expressions
D. Give a field a new name at search time

Answer: D

NEW QUESTION 45
- (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 49
- (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 51
- (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 55
- (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 58
......

Thank You for Trying Our Product

* 100% Pass or Money Back

　　All our products come with a 90-day Money Back Guarantee.

* One year free update

　　You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

　　We currently serve more than 30,000,000 customers.

* Shop Securely

　　All transactions are protected by VeriSign!

100% Pass Your SPLK-1002 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-1002-dumps.html