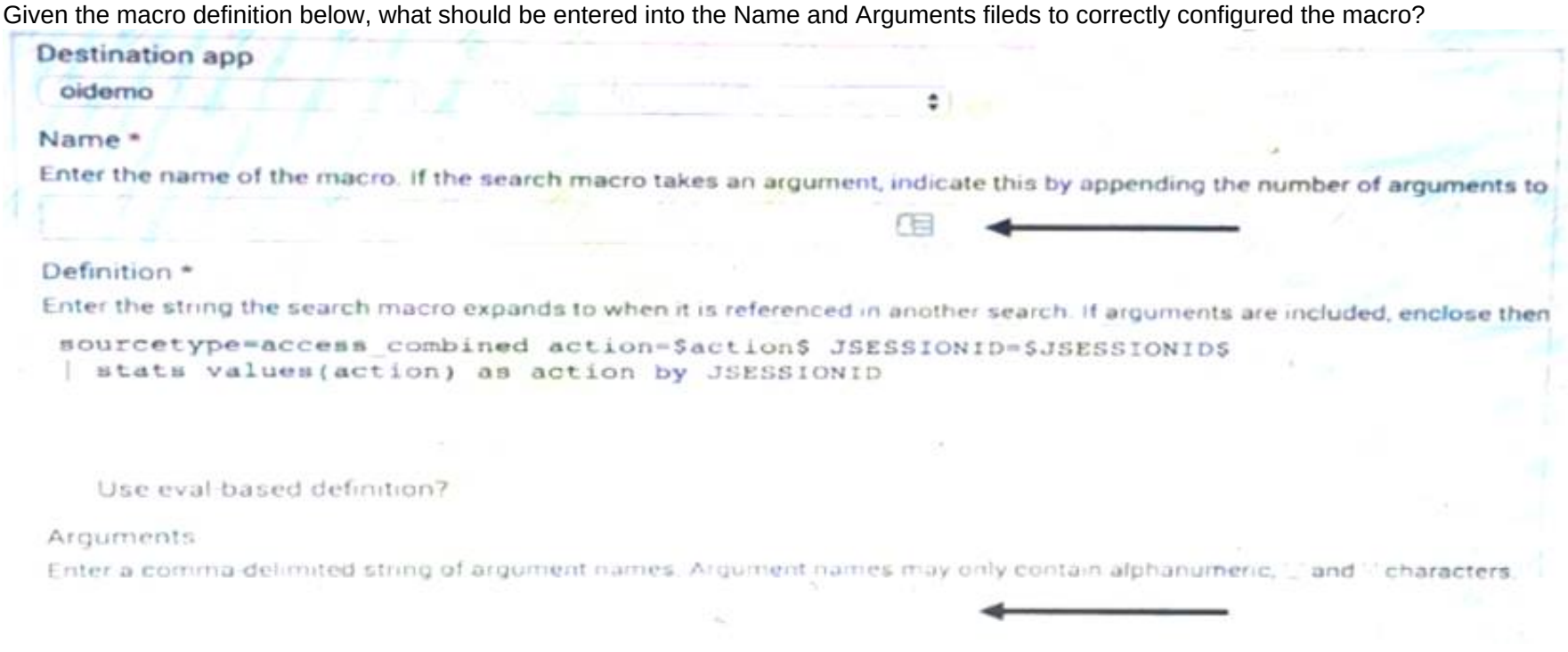
Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

NEW QUESTION 1
- (Exam Topic 1)
Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



A. The macro name is sessiontracker and the argument are action, JESSION.
B. The macro name is sessiontracker (2) and the action JESSIONID
C. The macro name is sessiontracker and the argument are sectional ,$ JESSIONIDS.
D. The macro name is sessiontracker (2) and the argument are $action ,$JESSIONIDS.

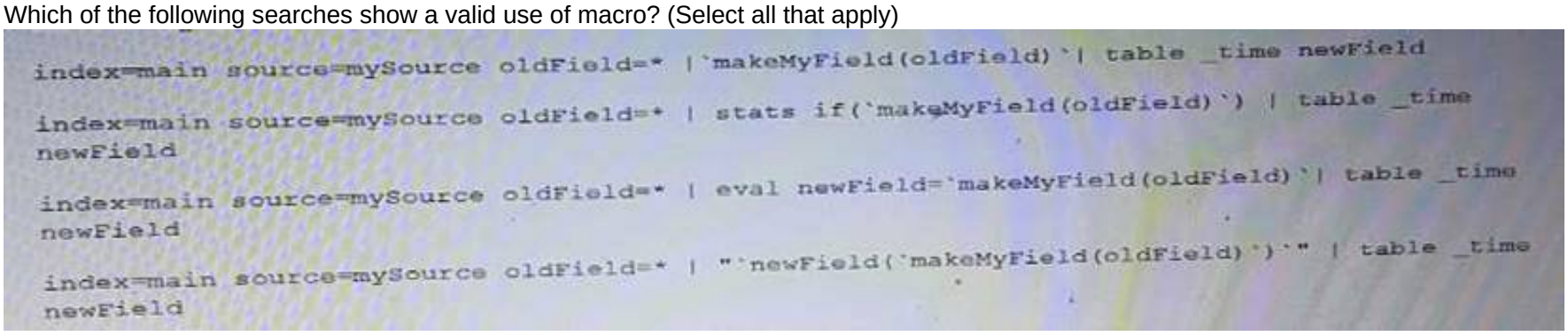
Answer: B

NEW QUESTION 2
- (Exam Topic 1)
Which of the following eval command function is valid?

A. Int ()
B. Count ( )
C. Print ()
D. Tostring ()

Answer: D

NEW QUESTION 3
- (Exam Topic 1)
Which of the following searches show a valid use of macro? (Select all that apply)



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 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 7
- (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 8
- (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 9
- (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 10
- (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 10
- (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 13
- (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 17
- (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 22
- (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 24
- (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 29
- (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 31
- (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 33
- (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 37
- (Exam Topic 1)
What does the fillnull command replace null values with, it the value argument is not specified?

A. N/A
B. NaN
C. NULL

Answer: A

NEW QUESTION 41
- (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 45
- (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 47
- (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 52
- (Exam Topic 1)
A space is an implied _____ in a search string.

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

Answer: B

NEW QUESTION 55
- (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 59
- (Exam Topic 1)
Which of the following statements describes this search? sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

A. This is a valid search and will display a timechart of the average duration, of each transaction event.
B. This is a valid search and will display a stats table showing the maximum pause among transactions.
C. No results will be returned because the transaction command must include the startswith and endswith options.
D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Answer: A

NEW QUESTION 62
- (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 66
- (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 70
- (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 74
- (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 78
- (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 79
- (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 82

- (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 86
- (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 91
- (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 93
- (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 97
- (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 99
- (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)
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 109

- (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 114
- (Exam Topic 2)
Which is not a comparison operator in Splunk

A. <=
B. =
C. !=
D. >
E. ?=

Answer: E

NEW QUESTION 115
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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