Splunk

Exam Questions SPLK-1002

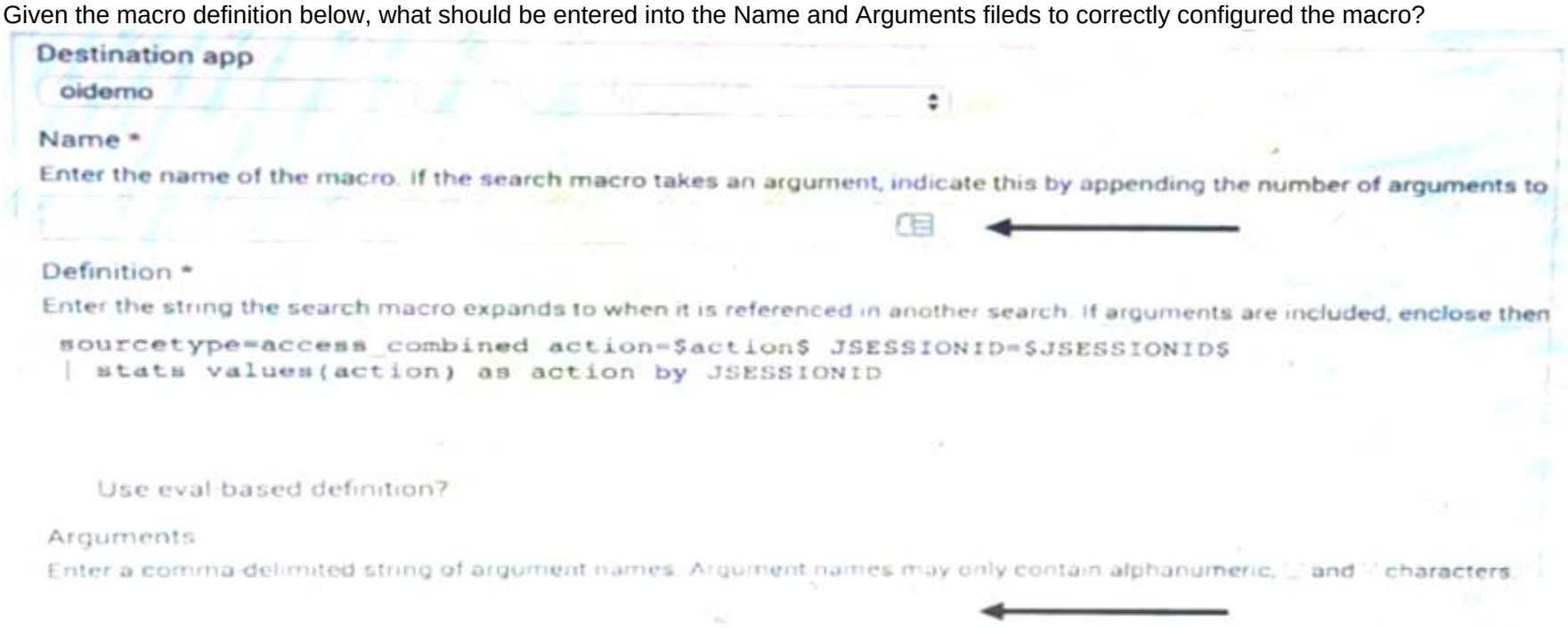
Splunk Core Certified Power User Exam

NEW QUESTION 1
- (Exam Topic 1)
Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

A. Alerts
B. Email
C. Database
D. User permissions

Answer: ABC

NEW QUESTION 2
- (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 3
- (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.

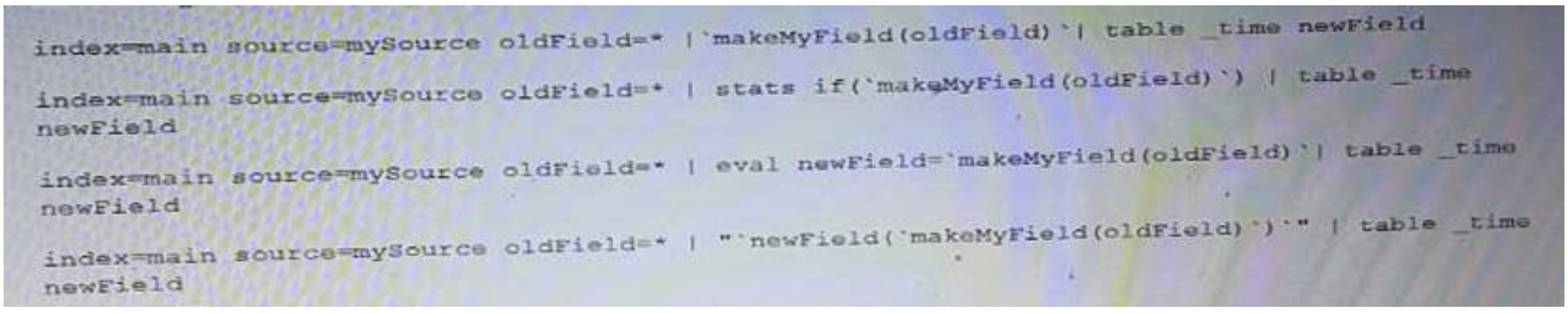
Answer: AC

NEW QUESTION 4
- (Exam Topic 1)
Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

A. | datamodel web search | filed web *
B. | Search datamodel web web | filed web*
C. | datamodel web web field | search web*
D. Datamodel=web | search web | filed web*

Answer: A

NEW QUESTION 5
- (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 6
- (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 7
- (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 8
- (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 9
- (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 10
- (Exam Topic 1)
When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

A. Rank
B. Weight
C. Priority
D. Precedence

Answer: C

NEW QUESTION 10
- (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 11
- (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 16
- (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 17
- (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 18
- (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 23
- (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 24
- (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 25
- (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 29
- (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 31
- (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 36
- (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 42
- (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 43
- (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 45
- (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 50
- (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 52
- (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 54
- (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 55
- (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 58
- (Exam Topic 2)
Which of the following search modes automatically returns all extracted fields in the fields sidebar?

A. Fast
B. Smart
C. Verbose

Answer: C

NEW QUESTION 62
- (Exam Topic 2)
Splunk alerts can be based on search that run _____. (Select all that apply.)

A. in real-time
B. on a regular schedule
C. and have no matching events

Answer: AB

NEW QUESTION 64
- (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 68
- (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 72
- (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 74
- (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 75
- (Exam Topic 2)
Which is not a comparison operator in Splunk

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

Answer: E

NEW QUESTION 76
.....

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