Splunk

Exam Questions SPLK-1002

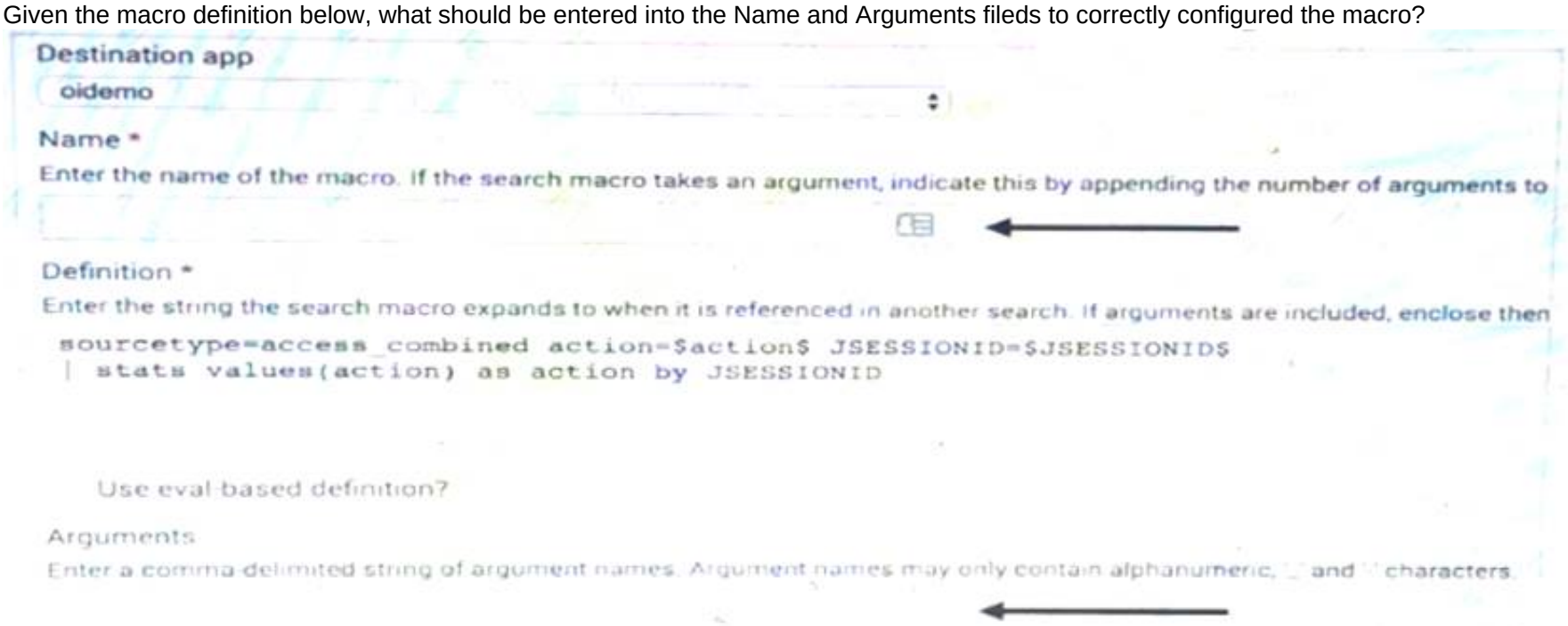
Splunk Core Certified Power User Exam

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 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 4
- (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 5
- (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 6
- (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 7
- (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 8
- (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 9
- (Exam Topic 1)
Which of the following statements describes POST workflow actions?

A. POST workflow actions are always encrypted.
B. POST workflow actions cannot use field values in their URI.
C. POST workflow actions cannot be created on custom sourcetypes.
D. POST workflow actions can open a web page in either the same window or a new .

Answer: D

NEW QUESTION 10
- (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 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 12
- (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 16
- (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 19
- (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 24
- (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 27
- (Exam Topic 1)
Selected fields are displayed _____ each event in the search results.
A. below
B. interesting fields
C. other fields
D. above

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
In what order arc 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 32
- (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 36
- (Exam Topic 1)
Which of the following statements describes Search workflow actions?

A. By defaul
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 37
- (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 40
- (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 43
- (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 46
- (Exam Topic 1)
What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

A. Macros.
B. Field aliases.
C. The rename command.
D. CIM does not work with different names for the same field.

Answer: B

NEW QUESTION 50
- (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 52
- (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 57
- (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 60
- (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 62
- (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 65
- (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 67
- (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 70
- (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 72
- (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 77
- (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 80
- (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 82
.....

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