

SPLK-1002 Dumps

Splunk Core Certified Power User Exam

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



NEW QUESTION 1

- (Exam Topic 1)

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configure the macro?

Destination app
oidemo

Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in double quotes.
`sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONIDS | stats values(action) as action by JSESSIONID`

Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, _ and - characters.

- A. The macro name is sessiontracker and the argument are action, JSESSION.
- B. The macro name is sessiontracker (2) and the action JSESSIONID
- C. The macro name is sessiontracker and the argument are sectional , \$ JSESSIONIDS.
- D. The macro name is sessiontracker (2) and the argument are \$action , \$JSESSIONIDS.

Answer: B

NEW QUESTION 2

- (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 3

- (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 4

- (Exam Topic 1)

Which of the following statements is true, especially in large environments?

- A. Use the stats 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 5

- (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 URL link in the current window or in a new window

Answer: D

NEW QUESTION 6

- (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 7

- (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 8

- (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 9

- (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)

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 10

- (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 12

- (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 16

- (Exam Topic 1)

A space is an implied _____ in a search string.

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

Answer: B

NEW QUESTION 17

- (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 19

- (Exam Topic 1)

Which of the following statements describes this search? sourcetype=access_combined | 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 23

- (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 27

- (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 32

- (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 37

- (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 40

- (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 43

- (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 48

- (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 53

- (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 55

- (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 58

- (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 60

- (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 64

.....

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>