

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 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 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 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 5

- (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 6

- (Exam Topic 1)

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?

Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

```
stats sum(price) as USD by product_name  
| eval $currency$=\"$symbol$\".tostring(round(USD*$rate$,2),\"comma\") | eval USD=\"$\" + tostring(USD,\"comma\")
```

☐ Use eval-based definition?

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

currency,symbol,rate

- 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)

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 8

- (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 9

- (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 10

- (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 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)

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

Answer: D

NEW QUESTION 20

- (Exam Topic 1)

Which of the following statements describe the search below? (select all that apply) Index=main | transaction clientip host maxspan=30s maxpause=5s

- A. Events in the transaction occurred within 5 seconds.
- B. It groups events that share the same clientip and host.
- C. The first and last events are no more than 5 seconds apart.
- D. The first and last events are no more than 30 seconds apart.

Answer: B

NEW QUESTION 22

- (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 27

- (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 28

- (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 31

- (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 35

- (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 40

- (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 42

.....

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>