

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 fields to correctly configure the macro?

- 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 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 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 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 5

- (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 6

- (Exam Topic 1)

Which of the following statements describes the command below (select all that apply) sourcetype-access_combined | transaction JSESSIONID

- A. An additional field named maxspan is created.
- B. An additional field 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 7

- (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 8

- (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 9

- (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 10

- (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 10

- (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 15

- (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 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 20

- (Exam Topic 1)

Which of the following statements describes macros?

- A. A macro is a reusable search string that must contain the full search.
- B. A macro is a reusable search string that must have a fixed time range.
- C. A macro Is a reusable search string that may have a flexible time range.
- D. A macro Is a reusable search string that must contain only a portion of the search.

Answer: C

NEW QUESTION 24

- (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 28

- (Exam Topic 1)

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

- A. Index-main | REJECT trans sessionid
- B. Index-main | transaction sessionid | search REJECT
- C. Index=main | transaction sessionid | whose transaction=reject
- D. Index=main | transaction sessionid | where transaction=reject"

Answer: D

NEW QUESTION 30

- (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 34

- (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 36

- (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 40

- (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)

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 50

- (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 52

- (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 56

- (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 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 62

- (Exam Topic 2)

Which of the following searches will show the number of categoryId used by each host?

- A. Sourcetype=access_* |sum bytes by host
- B. Sourcetype=access_* |stats sum(categoryId) by host
- C. by host
- D. Sourcetype=access_* |sum(bytes) by host
- E. Sourcetype=access_* |stats sum by host

Answer: B

NEW QUESTION 66

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1002 Practice Test Here](#)