

Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



NEW QUESTION 1

- (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 2

- (Exam Topic 1)

Which of the following eval command function is valid?

- A. Int ()
- B. Count ()
- C. Print ()
- D. ToString ()

Answer: D

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)

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 7

- (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 8

- (Exam Topic 1)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

After manually editing; a regular expression (regex), which of the following statements is true?

- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Answer: D

NEW QUESTION 10

- (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 10

- (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 12

- (Exam Topic 1)

Which one of the following statements about the search command is true?

- A. It does not allow the use of wildcards.
- B. It treats field values in a case-sensitive manner.
- C. It can only be used at the beginning of the search pipeline.
- D. It behaves exactly like search strings before the first pipe.

Answer: C

NEW QUESTION 16

- (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 20

- (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 21

- (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 22

- (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 23

- (Exam Topic 1)

Which of the following file formats can be extracted using a delimiter field extraction?

- A. CSV
- B. PDF
- C. XML
- D. JSON

Answer: A

NEW QUESTION 24

- (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 26

- (Exam Topic 1)

How does a user display a chart in stack mode?

- A. By using the stack command.
- B. By turning on the Use Trellis Layout option.
- C. By changing Stack Mode in the Format menu.
- D. You cannot display a chart in stack mode, only a timechart.

Answer: C

NEW QUESTION 29

- (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 33

- (Exam Topic 1)

In what order are 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 37

- (Exam Topic 1)

A space is an implied _____ in a search string.

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

Answer: B

NEW QUESTION 42

- (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 46

- (Exam Topic 1)

Which of the following statements describes Search workflow actions?

- A. By default
- 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 49

- (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 54

- (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 56

- (Exam Topic 1)

What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

- A. Creates a table of the total count of users and split by corndogs.
- B. Creates a table of the total count of mysterymeat corndogs split by user.
- C. Creates a table with the count of all types of corndogs eaten split by user.
- D. Creates a table that groups the total number of users by vegetarian corndogs.

Answer: A

NEW QUESTION 59

- (Exam Topic 1)

A calculated field may be 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 61

- (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 66

- (Exam Topic 2)

These users can create global knowledge objects. (Select all that apply.)

- A. users
- B. power users
- C. administrators

Answer: BC

NEW QUESTION 69

- (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 71

- (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 74

- (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 79

- (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 82

- (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 84

- (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 86

- (Exam Topic 2)

What will you learn from the results of the following search? sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

Answer: A

NEW QUESTION 90

.....

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](#)