

Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam



NEW QUESTION 1

Which command is used to review the contents of a specified static lookup file?

- A. lookup
- B. csvlookup
- C. inputlookup
- D. outputlookup

Answer: C

NEW QUESTION 2

A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

- A. An app
- B. JSON
- C. A role
- D. An enhanced solution

Answer: A

NEW QUESTION 3

What is the purpose of using a by clause with the stats command?

- A. To group the results by one or more fields.
- B. To compute numerical statistics on each field.
- C. To specify how the values in a list are delimited.
- D. To partition the input data based on the split-by fields.

Answer: A

NEW QUESTION 4

What syntax is used to link key/value pairs in search strings?

- A. action+purchase
- B. action=purchase
- C. action | purchase
- D. action equal purchase

Answer: B

NEW QUESTION 5

What user interface component allows for time selection?

- A. Time summary
- B. Time range picker
- C. Search time picker
- D. Data source time statistics

Answer: B

NEW QUESTION 6

Which events will be returned by the following search string?
host=www3 status=503

- A. All events that either have a host of www3 or a status of 503.
- B. All events with a host of www3 that also have a status of 503.
- C. We need more information; we cannot tell without knowing the time range.
- D. We need more information; a search cannot be run without specifying an index.

Answer: B

NEW QUESTION 7

What can be configured using the Edit Job Settings menu?

- A. Export the result to CSV format.
- B. Add the Job results to a dashboard.
- C. Schedule the Job to re-run in 10 minutes.
- D. Change Job Lifetime from 10 minutes to 7 days.

Answer: B

NEW QUESTION 8

Which command is used to validate a lookup file?

- A. | lookup products.csv
- B. inputlookup products.csv
- C. | inputlookup products.csv
- D. | lookup_definition products.csv

Answer: C

NEW QUESTION 9

What happens when a field is added to the Selected Fields list in the fields sidebar?

- A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
- B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
- C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
- D. The selected field and its corresponding values will appear underneath the events in the search results.

Answer: D

NEW QUESTION 10

What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

- A. the_questionnaire _pedia
- B. the_questionnaire pedia
- C. the_questionnaire_pedia
- D. the_questionnaire Pedia

Answer: C

NEW QUESTION 10

Data sources being opened and read applies to:

- A. None of the above
- B. Indexing Phase
- C. Parsing Phase
- D. Input Phase
- E. License Metering

Answer: D

NEW QUESTION 15

Select the correct option that applies to Index time processing (Choose three.).

- A. Indexing
- B. Searching
- C. Parsing
- D. Settings
- E. Input

Answer: ACE

NEW QUESTION 16

Splunk index time process can be broken down into _____ phases.

- A. 3
- B. 2
- C. 4
- D. 1

Answer: A

NEW QUESTION 18

Where does Licensing meter happen?

- A. Indexer
- B. Parsing
- C. Heavy Forwarder
- D. Input

Answer: A

NEW QUESTION 19

You can view the search result in following format (Choose three.):

- A. Table
- B. Raw
- C. Pie Chart

D. List

Answer: ABD

NEW QUESTION 24

.....

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-1001 Practice Exam Features:

- * SPLK-1001 Questions and Answers Updated Frequently
- * SPLK-1001 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1001 Practice Test Here](#)