SPLK-1001 Q&As

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/splk-1001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the main requirement for creating visualizations using the Splunk UI?

A. Your search must transform event data into Excel file format first.

B. Your search must transform event data into XML formatted data first.

C. Your search must transform event data into statistical data tables first.

D. Your search must transform event data into JSON formatted data first.

Correct Answer: C

QUESTION 2

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

A. Indexing

B. Searching

C. Parsing

D. Settings

E. Input

Correct Answer: ACE

QUESTION 3

Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts

B. Sourcetypes

C. Sources

D. Indexes

Correct Answer: ABD

QUESTION 4

When using the top command in the following search, which of the following will be true about the results?

index="main" sourcetype="access_*" action="purchase" | top 3 statusCode by user showperc=f

countfield=status_code_count

A. The search will fail. The proper top command format is top limit=3 instead of top 3.

B. The top three most common values in statusCode will be displayed for each user.

C. Only the top three overall most common values in statusCode will be displayed.

D. The percentage field will be displayed in the results.

Correct Answer: B

The top command returns the most common values of a field and their count. By using the by clause, you can group the results by another field. In this case, the top command will return the top three most common values in statusCode for each user. The showperc=f option will suppress the percentage column in the output. The countfield option will rename the count column to status_code_count2.

QUESTION 5

Which of the statements is correct regarding click and drag option in timeline?

A. The new result after selecting the range by dragging filters the events and displays the most recent first.

B. There is no functionality like click and drag in Splunk\\'s timeline.

C. Using this option executes a new query.

D. This doesn\\'t execute a new query

Correct Answer: A