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.pass2lead.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

This is what Splunk uses to categorize the data that is being indexed.

A. sourcetype

B. index

C. source

D. host

Correct Answer: A

QUESTION 2

In the Fields sidebar, what does the number directly to the right of the field name indicate?

A. The value of the field

B. The number of values for the field

C. The number of unique values for the field

D. The numeric non-unique values of the field

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchTutorial/Usefieldstosearch

QUESTION 3

Which search string is the most efficient?

A. "failed password"

B. \\'\\'failed password"*

C. index=* "failed password"

D. index=security "failed password"

Correct Answer: D

QUESTION 4

Which command is used to validate a lookup file?

A. | lookup products.csv

B. inputlookup products.csv

C. I inputlookup products.csv

D. | lookup definition products.csv

Correct Answer: C

QUESTION 5

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

A. 3

B. 2

C. 4

D. 1

Correct Answer: A