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.passapply.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 default lifetime of every Splunk search job?

A. All search jobs are saved for 10 days

B. All search jobs are saved for 10 hours

C. All search jobs are saved for 10 weeks D. All search jobs are saved for 10 minutes

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Extendjoblifetimes

QUESTION 2

How are events displayed after a search is executed?

A. In chronological order.

B. Randomly by default.

C. In reverse chronological order.

D. Alphabetically according to field name.

Correct Answer: C

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

The better way of writing search query for index is:

A. index=a index=b

B. (index=a OR index=b)

C. index=(a and b)

D. index = a, b

Correct Answer: B

QUESTION 5

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

A. sourcetype

B. index

C. source

D. host

Correct Answer: A