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

At the time of searching the start time is 03:35:08. Will it look back to 03:00:00 if we use -30m@h in searching?

A. Yes

B. No

Correct Answer: A

QUESTION 2

Which of the following statements describes a search job?

A. Once a search job begins, it cannot be stopped

B. A search job can only be paused when less than 50% of events are returned

C. A search job can only be stopped when less than 50% of events are returned

D. Once a search job begins, it can be stopped or paused at any point in time

Correct Answer: D

Reference: https://answers.splunk.com/answers/329699/why-does-my-search-head-cluster-captain-start-dele- 1.html

QUESTION 3

Which search string matches only events with the status_code of 4:4?

A. status_code !=404

B. status_code>=400

C. status_code403 status_code