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

Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms

B. Include at least one function as this is a search requirement

C. Include the search terms at the beginning of the search string

D. Avoid using formatting clauses as they add too much overhead

Correct Answer: A

QUESTION 2

Which of the following is the most efficient filter for running searches in Splunk?

A. Time

B. Fast mode

C. Sourcetype

D. Selected Fields

Correct Answer: A

QUESTION 3

Field names are case sensitive and field value are not.

A. True

B. False

Correct Answer: A

QUESTION 4

Which of the following is true about user account settings and preferences?

A. Search and Reporting is the only app that can be set as the default application.

B. Full names can only be changed by accounts with a Power User or Admin role.

C. Time zones are automatically updated based on the setting of the computer accessing Splunk.

D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Correct Answer: D

QUESTION 5

Which search string only returns events from hostWWW3?

A. host=*

B. host=WWW3

C. host=WWW*

D. Host=WWW3

Correct Answer: B