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

Which command is used to review the contents of a specified static lookup file?

A. lookup

B. csvlookup

C. inputlookup

D. outputlookup

Correct Answer: C

QUESTION 2

What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

A. the_questionnaire _pedia

B. the_questionnaire pedia

C. the_questionnaire_pedia

D. the_questionnaire Pedia

Correct Answer: C

QUESTION 3

How to make Interesting field into a selected field?

A. Click field in field sidebar -> click YES on the pop-up dialog on upper right side -> check now field should be visible in the list of selected fields.

B. Not possible.

C. Only CLI changes will enable it.

D. Click Settings -> Find field option -> Drop down select field -> enable selected field -> check now field should be visible in the list of selected fields.

Correct Answer: A

QUESTION 4

What kind of logs can Splunk Index?

A. Only A, B

B. Router and Switch Logs

C. Firewall and Web Server Logs

D. Only C

E. Database logs

F. All firewall, web server, database, router and switch logs

Correct Answer: F

QUESTION 5

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