



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

There are three different search modes in Splunk (Choose three.):

- A. Automatic
- B. Smart
- C. Fast
- D. Verbose

Correct Answer: BCD

QUESTION 2

Which command is used to validate a lookup file?

- A. | lookup products.csv
- B. inputlookup products.csv
- C. | inputlookup products.csv
- D. | lookup definition products.csv

Correct Answer: C

QUESTION 3

Data sources being opened and read applies to:

- A. None of the above
- B. Indexing Phase
- C. Parsing Phase
- D. Input Phase
- E. License Metering

Correct Answer: D

QUESTION 4

What is the purpose of using a by clause with the stats command?

- A. To group the results by one or more fields.



- B. To compute numerical statistics on each field.
- C. To specify how the values in a list are delimited.
- D. To partition the input data based on the split-by fields.

Correct Answer: A

QUESTION 5

In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?

- A. No events will be returned.
- B. Splunk will prompt you to specify an index.
- C. All non-indexed events to which the user has access will be returned.
- D. Events from every index searched by default to which the user has access will be returned.

Correct Answer: D

[SPLK-1001 PDF Dumps](#)

[SPLK-1001 VCE Dumps](#)

[SPLK-1001 Study Guide](#)