

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.leads4pass.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 are Splunk premium enhanced solutions? (Choose three.)

- A. Splunk User Behavior Analytics (UBA)
- B. Splunk IT Service Intelligence (ITSI)
- C. Splunk Enterprise Security (ES)
- D. Splunk Analytics Security (AS)

Correct Answer: ABC

QUESTION 2

Field names are case sensitive.

- A. True
- B. False

Correct Answer: A

QUESTION 3

You are able to create new Index in Data Input settings.

- A. No
- B. Yes

Correct Answer: B

QUESTION 4

What happens when a field is added to the Selected Fields list in the fields sidebar\`?

- A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field
- B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
- C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time
- D. The selected field and its corresponding values will appear underneath the events in the search results

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

[SPLK-1001 PDF Dumps](#)

[SPLK-1001 VCE Dumps](#)

[SPLK-1001 Braindumps](#)