



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

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 Splunk components typically resides on the machines where data originates?

- A. Indexer
- B. Forwarder
- C. Search head
- D. Deployment server

Correct Answer: B

QUESTION 3

Splunk index time process can be broken down into _____ phases.

- A. 3
- B. 2
- C. 4
- D. 1

Correct Answer: A

QUESTION 4

Universal forwarder is recommended for forwarding the logs to indexers.

- A. False
- B. True



Correct Answer: B

QUESTION 5

What user interface component allows for time selection?

- A. Time summary
- B. Time range picker
- C. Search time picker
- D. Data source time statistics

Correct Answer: B

[Latest SPLK-1001 Dumps](#)

[SPLK-1001 VCE Dumps](#)

[SPLK-1001 Exam
Questions](#)