



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

Forward Option gather and forward data to indexers over a receiving port from remote machines.

- A. False
- B. True

Correct Answer: B

QUESTION 2

Splunk apps are used for following (Choose three.):

- A. Designed to cater numerous use cases and empower Splunk.
- B. We can not install Splunk App.
- C. Allows multiple workspaces for different use cases/user roles.
- D. It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

Correct Answer: ACD

QUESTION 3

Portal for Splunk apps can be accessed through www.splunkbase.com

- A. False
- B. True

Correct Answer: B

QUESTION 4

Which of the following constraints can be used with the top command?

- A. limit
- B. useperc
- C. addtotals
- D. fieldcount

Correct Answer: A



QUESTION 5

Which of the following is the best way to create a report that shows the last 24 hours of events?

- A. Use earliest=-1d@d latest=@d
- B. Set a real-time search over a 24-hour window
- C. Use the time range picket to select "Yesterday"
- D. Use the time range picker to select "Last 24 hours"

Correct Answer: D

[SPLK-1001 VCE Dumps](#)

[SPLK-1001 Study Guide](#)

[SPLK-1001 Braindumps](#)