# 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 is the most efficient search?

A. index=* "failed password"

B. "failed password" index=*

C. (index=* OR index=security) "failed password"

D. index=security "failed password"

Correct Answer: A

**QUESTION 2**

Which statement is true about Splunk alerts?

A. Alerts are based on searches that are either run on a scheduled interval or in real-time.

B. Alerts are based on searches and when triggered will only send an email notification.

C. Alerts are based on searches and require cron to run on scheduled interval.

D. Alerts are based on searches that are run exclusively as real-time.

Correct Answer: A

**QUESTION 3**

What type of search can be saved as a report?

A. Any search can be saved as a report

B. Only searches that generate visualizations

C. Only searches containing a transforming command

D. Only searches that generate statistics or visualizations

Correct Answer: D

**QUESTION 4**

Which of the following are common constraints of the top command?

A. limit, count

B. limit, showpercent

C. limits, countfield

D. showperc, countfield

Correct Answer: A

**QUESTION 5**

Monitor option in Add Data provides _____.

A. Only continuous monitoring.

B. Only One-time monitoring.

C. None of the above.

D. Both One-time and continuous monitoring

Correct Answer: D