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 file types is an option for exporting Splunk search results?

A. PDF

B. JSON

C. XLS

D. RTF

Correct Answer: B

QUESTION 2

Which of the following searches would return events with failure in index netfw or warn or critical in index netops?

A. (index=netfw failure) AND index=netops warn OR critical

B. (index=netfw failure) OR (index=netops (warn OR critical))

C. (index=netfw failure) AND (index=netops (warn OR critical))

D. (index=netfw failure) OR index=netops OR (warn OR critical)

Correct Answer: B

QUESTION 3

Which search matches the events containing the terms "error" and "fail"?

A. index=security Error Fail

B. index=security error OR fail

C. index=security "error failure"

D. index=security NOT error NOT fail

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Search

QUESTION 4

@ Symbol can be used in advanced time unit option.

A. No

B. Yes

Correct Answer: B

QUESTION 5

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