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.pass2lead.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 index searches would provide the most efficient search performance?

A. index=*

B. index=web OR index=s*

C. (index=web OR index=sales)

D. *index=sales AND index=web*

Correct Answer: C

QUESTION 2

What is the correct way to use a time range specifier in the search bar so that the search looks back 2 hours?

A. latest=-2h

B. earliest=-2h

C. latest=-2hour@d

D. earliest=-2hour@d

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Specifytimemodifiersinyoursearch

QUESTION 3

How do you add or remove fields from search results?

A. Use field +to add and field -to remove.

B. Use table +to add and table -to remove.

C. Use fields +to add and fields o remove.

D. Use fields Plus to add and fields Minus to remove.

Correct Answer: C

QUESTION 4

In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?

A. No events will be returned.

B. Splunk will prompt you to specify an index.

C. All non-indexed events to which the user has access will be returned.

D. Events from every index searched by default to which the user has access will be returned.

Correct Answer: D

QUESTION 5

When placed early in a search, which command is most effective at reducing search execution time?

A. dedup

B. rename

C. sort

D. fields +

Correct Answer: A