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 Boolean operator is always implied between two search terms, unless otherwise specified?

A. OR

B. NOT

C. AND

D. XOR

Correct Answer: C

QUESTION 2

Which of the following is a correct way to limit search results to display the 5 most common values of a field?

A. | rare top=5

B. | top rare=5

C. | top limit=5

D. | rare limit=5

Correct Answer: C

QUESTION 3

Documentations for Splunk can be found at docs.splunk.com

A. True

B. False

Correct Answer: A

QUESTION 4

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 5

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

A. limit

B. useperc

C. addtotals

D. fieldcount

Correct Answer: A

QUESTION 6

Which search string only returns events from hostWWW3?

A. host=*

B. host=WWW3

C. host=WWW*

D. Host=WWW3

Correct Answer: B

QUESTION 7

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 8

!= and NOT are same arguments.

A. True

B. False

Correct Answer: B

QUESTION 9

What are the three main Splunk components?

A. Search head, GPU, streamer

B. Search head, indexer, forwarder

C. Search head, SQL database, forwarder

D. Search head, SSD, heavy weight agent

Correct Answer: B

Reference: https://www.edureka.co/blog/splunk-architecture/

QUESTION 10

Following are the time selection option while making search: (Choose all that apply.)

A. Date and Time Range

B. Advanced

C. Date Range

D. Presets

E. Relative

Correct Answer: B

QUESTION 11

This search will return 20 results. SEARCH: error | top host limit = 20

A. True

B. False

Correct Answer: A

QUESTION 12

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

QUESTION 13

Data sources being opened and read applies to:

A. None of the above

B. Indexing Phase

C. Parsing Phase

D. Input Phase

E. License Metering

Correct Answer: D

QUESTION 14

Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

A. Save the search as a report and use it in multiple dashboards as needed

B. Save the search as a dashboard panel for each dashboard that needs the data

C. Save the search as a scheduled alert and use it in multiple dashboards as needed

D. Export the results of the search to an XML file and use the file as the basis of the dashboards

Correct Answer: A

QUESTION 15

What does the following specified time range do? earliest=-72h@h latest=@d

A. Look back 3 days ago and prior

B. Look back 72 hours up to one day ago

C. Look back 72 hours, up to the end of today

D. Look back from 3 days ago up to the beginning of today

Correct Answer: D