

SPLK-1001 Dumps

Splunk Core Certified User Exam

<https://www.certleader.com/SPLK-1001-dumps.html>



NEW QUESTION 1

After running a search, what effect does clicking and dragging across the timeline have?

- A. Executes a new search.
- B. Filters current search results.
- C. Moves to past or future events.
- D. Expands the time range of the search.

Answer: C

NEW QUESTION 2

In the fields sidebar, which character denotes alphanumeric field values?

- A. #
- B. %
- C. a
- D. a#

Answer: B

NEW QUESTION 3

What syntax is used to link key/value pairs in search strings?

- A. action+purchase
- B. action=purchase
- C. action | purchase
- D. action equal purchase

Answer: B

NEW QUESTION 4

Which of the following searches will return results where fail, 400, and error exist in every event?

- A. error AND (fail AND 400)
- B. error OR (fail and 400)
- C. error AND (fail OR 400)
- D. error OR fail OR 400

Answer: C

NEW 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 +

Answer: A

NEW QUESTION 6

Which of the following is a best practice when writing a search string?

- A. Include all formatting commands before any search terms.
- B. Include at least one function as this is a search requirement.
- C. Include the search terms at the beginning of the search string.
- D. Avoid using formatting clauses, as they add too much overhead.

Answer: D

NEW QUESTION 7

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.

Answer: A

NEW QUESTION 8

When a Splunk search generates calculated data that appears in the Statistics tab, in what formats can the results be exported?

- A. CSV, JSON, PDF
- B. CSV, XML, JSON
- C. Raw Events, XML, JSON
- D. Raw Events, CSV, XML, JSON

Answer: B

NEW QUESTION 9

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

Answer: B

NEW QUESTION 10

How can another user gain access to a saved report?

- A. The owner of the report can edit permissions from the Edit dropdown.
- B. Only users with an Admin or Power User role can access other users' reports.
- C. Anyone can access any reports marked as public within a shared Splunk deployment.
- D. The owner of the report must clone the original report and save it to their user account.

Answer: A

NEW QUESTION 10

What is the primary use for the rare command?

- A. To sort field values in descending order.
- B. To return only fields containing five or fewer values.
- C. To find the least common values of a field in a dataset.
- D. To find the fields with the fewest number of values across a dataset.

Answer: C

NEW QUESTION 15

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

- A. False
- B. True

Answer: B

NEW QUESTION 20

Splunk shows data in ____ .

- A. ASCII Character order.
- B. Reverse chronological order.
- C. Alphanumeric order.
- D. Chronological order.

Answer: B

NEW QUESTION 22

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

- A. False
- B. True

Answer: B

NEW QUESTION 27

Select the correct option that applies to Index time processing (Choose three.).

- A. Indexing
- B. Searching
- C. Parsing
- D. Settings
- E. Input

Answer: ACE

NEW QUESTION 30

Parsing of data can happen both in HF and UF.

- A. Yes
- B. No

Answer: B

NEW QUESTION 35

Upload option creates inputs.conf

- A. Yes
- B. No

Answer: B

NEW QUESTION 36

Splunk index time process can be broken down into _____ phases.

- A. 3
- B. 2
- C. 4
- D. 1

Answer: A

NEW QUESTION 40

Which symbol is used to snap the time?

- A. @
- B. &
- C. *
- D. #

Answer: A

NEW QUESTION 43

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1001 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-1001-dumps.html>