

## SPLK-1001 Dumps

### Splunk Core Certified User Exam

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



**NEW QUESTION 1**

What is a primary function of a scheduled report?

- A. Auto-detect changes in performance.
- B. Auto-generated PDF reports of overall data trends.
- C. Regularly scheduled archiving to keep disk space use low.
- D. Triggering an alert in your Splunk instance when certain conditions are met.

**Answer:** D

**NEW QUESTION 2**

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 3**

Which stats command function provides a count of how many unique values exist for a given field in the result set?

- A. dc(field)
- B. count(field)
- C. count-by(field)
- D. distinct-count(field)

**Answer:** A

**NEW QUESTION 4**

What is the purpose of using a by clause with the stats command?

- A. To group the results by one or more fields.
- B. To compute numerical statistics on each field.
- C. To specify how the values in a list are delimited.
- D. To partition the input data based on the split-by fields.

**Answer:** A

**NEW QUESTION 5**

What is the main requirement for creating visualizations using the Splunk UI?

- A. Your search must transform event data into Excel file format first.
- B. Your search must transform event data into XML formatted data first.
- C. Your search must transform event data into statistical data tables first.
- D. Your search must transform event data into JSON formatted data first.

**Answer:** B

**NEW QUESTION 6**

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 7**

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 8**

Which of the following fields is stored with the events in the index?

- A. user
- B. source
- C. location
- D. sourcecp

**Answer:** B

**NEW QUESTION 9**

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.

**Answer:** D

**NEW QUESTION 10**

Which is primary function of the timeline located under the search bar?

- A. To differentiate between structured and unstructured events in the data.
- B. To sort the events returned by the search command in chronological order.
- C. To zoom in and zoom out, although this does not change the scale of the chart.
- D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.

**Answer:** D

**NEW QUESTION 10**

Which command is used to validate a lookup file?

- A. | lookup products.csv
- B. inputlookup products.csv
- C. | inputlookup products.csv
- D. | lookup\_definition products.csv

**Answer:** C

**NEW QUESTION 14**

What happens when a field is added to the Selected Fields list in the fields sidebar?

- A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
- B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
- C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
- D. The selected field and its corresponding values will appear underneath the events in the search results.

**Answer:** D

**NEW QUESTION 18**

What is Splunk?

- A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
- B. Database management tool.
- C. Security Information and Event Management (SIEM).
- D. Cloud based application that help in analyzing logs.

**Answer:** A

**NEW QUESTION 20**

Splunk Enterprise is used as a Scalable service in Splunk Cloud.

- A. True
- B. False

**Answer:** A

**NEW QUESTION 22**

All components are installed and administered in Splunk Enterprise on-premise.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Explanation/Reference:

B. False

Answer:

**NEW QUESTION 26**

Log filtering/parsing can be done from \_\_\_\_\_.

- A. Index Forwarders (IF)
- B. Universal Forwarders (UF)
- C. Super Forwarder (SF)
- D. Heavy Forwarders (HF)

**Answer:** D

**NEW QUESTION 27**

Portal for Splunk apps can be accessed through [www.splunkbase.com](http://www.splunkbase.com)

- A. False
- B. True

**Answer:** B

**NEW QUESTION 31**

Parsing of data can happen both in HF and UF.

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 35**

Splunk index time process can be broken down into \_\_\_\_\_ phases.

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

**Answer:** A

**NEW QUESTION 37**

Matching search terms are highlighted.

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 39**

There are three different search modes in Splunk (Choose three.):

- A. Automatic
- B. Smart
- C. Fast
- D. Verbose

**Answer:** BCD

**NEW QUESTION 42**

Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

- A. Open new search.
- B. Exclude the item from search.
- C. None of the above.
- D. Add the item to search.

**Answer:** ABD

**NEW QUESTION 43**

You can view the search result in following format (Choose three.):

- A. Table
- B. Raw
- C. Pie Chart
- D. List

**Answer:** ABD

**NEW QUESTION 47**

.....

## 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>