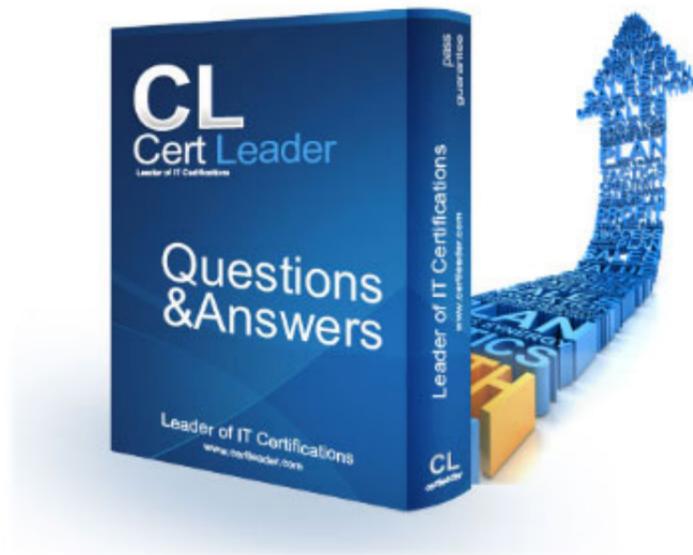


## SPLK-1001 Dumps

### Splunk Core Certified User Exam

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



**NEW QUESTION 1**

Which of the following is a Splunk search best practice?  
Splunk Core Certified User

- A. Filter as early as possible.
- B. Never specify more than one index.
- C. Include as few search terms as possible.
- D. Use wildcards to return more search results.

**Answer: A**

**NEW QUESTION 2**

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 3**

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 4**

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 5**

Which statement is true about Splunk alerts?

- A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
- B. Alerts are based on searches and when triggered will only send an email notification.
- C. Alerts are based on searches and require cron to run on scheduled interval.
- D. Alerts are based on searches that are run exclusively as real-time.

**Answer: A**

**NEW QUESTION 6**

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 7**

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

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

**Answer: B**

**NEW QUESTION 8**

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 9**

What user interface component allows for time selection?

- A. Time summary
- B. Time range picker
- C. Search time picker
- D. Data source time statistics

**Answer: B**

**NEW QUESTION 10**

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 10**

How does Splunk determine which fields to extract from data?

- A. Splunk only extracts the most interesting data from the last 24 hours.
- B. Splunk only extracts fields users have manually specified in their data.
- C. Splunk automatically extracts any fields that generate interesting visualizations.
- D. Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data.

**Answer: D**

**NEW QUESTION 14**

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 18**

When viewing the results of a search, what is an Interesting Field?

- A. A field that appears in any event.
- B. A field that appears in every event.
- C. A field that appears in the top 10 events.
- D. A field that appears in at least 20% of the events.

**Answer: D**

**NEW QUESTION 22**

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 26**

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 30**

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 35**

Which events will be returned by the following search string?

host=www3 status=503

- A. All events that either have a host of www3 or a status of 503.
- B. All events with a host of www3 that also have a status of 503.
- C. We need more information; we cannot tell without knowing the time range.
- D. We need more information; a search cannot be run without specifying an index.

**Answer: B**

**NEW QUESTION 36**

What does the stats command do?

- A. Automatically correlates related fields.
- B. Converts field values into numerical values.
- C. Calculates statistics on data that matches the search criteria.
- D. Analyzes numerical fields for their ability to predict another discrete field.

**Answer: C**

**NEW QUESTION 40**

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 45**

What can be configured using the Edit Job Settings menu?

- A. Export the result to CSV format.
- B. Add the Job results to a dashboard.
- C. Schedule the Job to re-run in 10 minutes.
- D. Change Job Lifetime from 10 minutes to 7 days.

**Answer: B**

**NEW QUESTION 48**

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 52**

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 55**

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

- A. True
- B. False

**Answer:** A

**NEW QUESTION 56**

Which component of Splunk let us write SPL query to find the required data?

- A. Forwarders
- B. Indexer
- C. Heavy Forwarders
- D. Search head

**Answer:** D

**NEW QUESTION 59**

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

- A. False
- B. True

**Answer:** B

**NEW QUESTION 62**

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

- A. False
- B. True

**Answer:** B

**NEW QUESTION 67**

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

**Answer:** D

**NEW QUESTION 71**

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 76**

Upload option creates inputs.conf

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 80**

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

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

**Answer:** A

**NEW QUESTION 85**

Which of the statements are correct about HF? (Choose three.)

- A. Parsing
- B. Masking
- C. Searching
- D. Forwarding

**Answer:** ABD

**NEW QUESTION 88**

Where does Licensing meter happen?

- A. Indexer
- B. Parsing
- C. Heavy Forwarder
- D. Input

**Answer:** A

**NEW QUESTION 92**

The default host name used in Inputs general settings can not be changed.

- A. False
- B. True

**Answer:** A

**NEW QUESTION 94**

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

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

**Answer:** BCD

**NEW QUESTION 96**

.....

## 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>