

# Exam Questions SPLK-1001

Splunk Core Certified User Exam

<https://www.2passeasy.com/dumps/SPLK-1001/>



#### NEW QUESTION 1

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 2

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 3

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 4

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

**Answer:** C

#### NEW QUESTION 5

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

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

**Answer:** B

#### NEW QUESTION 6

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 7

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 8

Which of the following is the most efficient filter for running searches in Splunk?

- A. Time
- B. Fast mode
- C. Sourcetype
- D. Selected Fields

**Answer:** C

#### NEW QUESTION 9

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 10

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 10

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 11

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

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

**Answer:** B

#### NEW QUESTION 15

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 18

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 20

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 24**

Three basic components of Splunk are (Choose three.):

- A. Forwarders
- B. Deployment Server
- C. Indexer
- D. Knowledge Objects
- E. Index
- F. Search Head

**Answer:** ACF

**NEW QUESTION 26**

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 29**

Splunk shows data in \_\_\_\_\_ .

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

**Answer:** B

**NEW QUESTION 33**

In monitor option you can select the following options in GUI.

- A. Only HTTP Event Collector (HEC) and TCP/UDP
- B. None of the above
- C. Only TCP/UDP
- D. Only Scripts
- E. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

**Answer:** E

**NEW QUESTION 36**

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

- A. False
- B. True

**Answer:** A

**NEW QUESTION 41**

Which symbol is used to snap the time?

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

**Answer:** A

**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 48**

Data summary button just below the search bar gives you the following (Choose three.):

- A. Hosts
- B. Sourcetypes
- C. Sources
- D. Indexes

**Answer:** ABC

**NEW QUESTION 51**

What options do you get after selecting timeline? (Choose four.)

- A. Zoom to selection
- B. Format Timeline
- C. Deselect
- D. Delete
- E. Zoom Out

**Answer:** ABCE

**NEW QUESTION 53**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1001 Product From:

<https://www.2passeasy.com/dumps/SPLK-1001/>

### Money Back Guarantee

#### **SPLK-1001 Practice Exam Features:**

- \* SPLK-1001 Questions and Answers Updated Frequently
- \* SPLK-1001 Practice Questions Verified by Expert Senior Certified Staff
- \* SPLK-1001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SPLK-1001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year