



**Splunk**

## **Exam Questions SPLK-1001**

Splunk Core Certified User Exam

#### NEW QUESTION 1

When looking at a dashboard panel that is based on a report, which of the following is true?

- A. You can modify the search string in the panel, and you can change and configure the visualization.
- B. You can modify the search string in the panel, but you cannot change and configure the visualization.
- C. You cannot modify the search string in the panel, but you can change and configure the visualization.
- D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

**Answer:** C

#### NEW QUESTION 2

Which command is used to review the contents of a specified static lookup file?

- A. lookup
- B. csvlookup
- C. inputlookup
- D. outputlookup

**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

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

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 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

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 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

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.

**Answer:** C

#### 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

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 15

Which is the default app for Splunk Enterprise?

- A. Splunk Enterprise Security Suite
- B. Searching and Reporting
- C. Reporting and Searching
- D. Splunk apps for Security

**Answer:** B

#### NEW QUESTION 20

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

- A. False
- B. True

**Answer:** B

#### NEW QUESTION 24

You can on-board data to Splunk using following means (Choose four.):

- A. Props
- B. CLI
- C. Splunk Web
- D. savedsearches.conf
- E. Splunk apps and add-ons
- F. indexes.conf
- G. inputs.conf
- H. metadata.conf

**Answer:** BCEG

#### NEW QUESTION 25

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 30**

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

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

**Answer:** A

**NEW QUESTION 31**

Where does Licensing meter happen?

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

**Answer:** A

**NEW QUESTION 34**

Splunk Parses data into individual events, extracts time, and assigns metadata.

- A. False
- B. True

**Answer:** B

**NEW QUESTION 36**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SPLK-1001 Practice Test Here](#)**