

# Exam Questions SPLK-1001

Splunk Core Certified User Exam

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



#### NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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

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

**Answer:** B

#### NEW QUESTION 15

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

- A. False
- B. True

**Answer:** B

#### NEW QUESTION 20

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 21

Parsing of data can happen both in HF and UF.

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 25

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

- A. False
- B. True

**Answer:** B

**NEW QUESTION 30**

Which symbol is used to snap the time?

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

**Answer:** A

**NEW QUESTION 33**

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

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

**Answer:** BCD

**NEW QUESTION 34**

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 37**

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

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

**Answer:** ABD

**NEW QUESTION 39**

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 42**

.....

## 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