

Exam Questions SPLK-1001

Splunk Core Certified User Exam

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



NEW QUESTION 1

Which of the following is true about user account settings and preferences?

- A. Search & Reporting is the only app that can be set as the default application.
- B. Full names can only be changed by accounts with a Power User or Admin role.
- C. Time zones are automatically updated based on the setting of the computer accessing Splunk.
- D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Answer: B

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

What does the values function of the stats command do?

- A. Lists all values of a given field.
- B. Lists unique values of a given field.
- C. Returns a count of unique values for a given field.
- D. Returns the number of events that match the search.

Answer: C

NEW QUESTION 4

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

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

Answer: B

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 syntax is used to link key/value pairs in search strings?

- A. action+purchase
- B. action=purchase
- C. action | purchase
- D. action equal purchase

Answer: B

NEW QUESTION 7

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 8

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 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

What can be included in the All Fields option in the sidebar?

- A. Dashboards
- B. Metadata only
- C. Non-interesting fields
- D. Field descriptions

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 12

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 13

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 18

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 22

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 23

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

- A. True
- B. False

Answer: A

NEW QUESTION 24

Splunk shows data in _____ .

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

Answer: B

NEW QUESTION 29

What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

- A. the_questionnaire _pedia
- B. the_questionnaire pedia
- C. the_questionnaire_pedia
- D. the_questionnaire Pedia

Answer: C

NEW QUESTION 34

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 36

Splunk index time process can be broken down into _____ phases.

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

Answer: A

NEW QUESTION 37

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. Files & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Answer: E

NEW QUESTION 38

Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 41

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 44

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 50

.....

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