

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

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 3

A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

- A. An app
- B. JSON
- C. A role
- D. An enhanced solution

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

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 6

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 7

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 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

What is the primary use for the rare command?

- A. To sort field values in descending order.
- B. To return only fields containing five or fewer values.
- C. To find the least common values of a field in a dataset.
- D. To find the fields with the fewest number of values across a dataset.

Answer: C

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

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 12

Portal for Splunk apps can be accessed through www.splunkbase.com

- A. False
- B. True

Answer: B

NEW QUESTION 13

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

- A. False
- B. True

Answer: B

NEW QUESTION 16

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

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

Answer: ABD

NEW QUESTION 20

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

- A. False
- B. True

Answer: B

NEW QUESTION 25

Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 30

.....

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