Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam

NEW QUESTION 1
Which of the following is a Splunk search best practice?
Splunk Core Certified User

A. Filter as early as possible.
B. Never specify more than one index.
C. Include as few search terms as possible.
D. Use wildcards to return more search results.

Answer: A

NEW QUESTION 2
After running a search, what effect does clicking and dragging across the timeline have?

A. Executes a new search.
B. Filters current search results.
C. Moves to past or future events.
D. Expands the time range of the search.

Answer: C

NEW QUESTION 3
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 4
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 5
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 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
Which command is used to validate a lookup file?

A. | lookup products.csv
B. inputlookup products.csv
C. | inputlookup products.csv
D. | lookup_definition products.csv

Answer: C

NEW QUESTION 9
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 10
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 10
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 12
Parsing of data can happen both in HF and UF.

A. Yes
B. No

Answer: B

NEW QUESTION 17
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 19
.....

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