Exam Questions SPLK-1001

Splunk Core Certified User Exam

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

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
What is a primary function of a scheduled report?

A. Auto-detect changes in performance.
B. Auto-generated PDF reports of overall data trends.
C. Regularly scheduled archiving to keep disk space use low.
D. Triggering an alert in your Splunk instance when certain conditions are met.

Answer: D

NEW QUESTION 3
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 4
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 5
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 6
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 7
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 8
What is the primary use for the rare command?

A. To sort field values in descending order.
B. To return only fields containing five of 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 9
Which component of Splunk let us write SPL query to find the required data?

A. Forwarders
B. Indexer
C. Heavy Forwarders
D. Search head

Answer: D

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 11
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Answer: B

NEW QUESTION 12
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 14
Select the correct option that applies to Index time processing (Choose three.).

A. Indexing
B. Searching
C. Parsing
D. Settings
E. Input

Answer: ACE

NEW QUESTION 17
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. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Answer: E

NEW QUESTION 20
Where does Licensing meter happen?

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

Answer: A

NEW QUESTION 25
Splunk Parses data into individual events, extracts time, and assigns metadata.

A. False
B. True

Answer: B

NEW QUESTION 28
You can view the search result in following format (Choose three.):

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

Answer: ABD

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