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 must be done in order to use a lookup table in Splunk?

A. The lookup must be configured to run automatically.
B. The contents of the lookup file must be copied and pasted into the search bar.
C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Answer: C

NEW QUESTION 5
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 6
What is the purpose of using a by clause with the stats command?

A. To group the results by one or more fields.
B. To compute numerical statistics on each field.
C. To specify how the values in a list are delimited.
D. To partition the input data based on the split-by fields.

Answer: A

NEW QUESTION 7
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 8
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 9
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 10
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 10
When placed early in a search, which command is most effective at reducing search execution time?

A. dedup
B. rename
C. sort -
D. fields +

Answer: A

NEW QUESTION 15
Which search matches the events containing the terms “error” and “fail”?

A. index=security Error Fail
B. index=security error OR fail
C. index=security “error failure”
D. index=security NOT error NOT fail

Answer: B

NEW QUESTION 18
Which events will be returned by the following search string?
host=www3 status=503

A. All events that either have a host of www3 or a status of 503.
B. All events with a host of www3 that also have a status of 503.
C. We need more information; we cannot tell without knowing the time range.
D. We need more information; a search cannot be run without specifying an index.

Answer: B

NEW QUESTION 23
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 26
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 31
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 36
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 40
Parsing of data can happen both in HF and UF.

A. Yes
B. No

Answer: B

NEW QUESTION 42
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 43
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 44
Which of the statements are correct about HF? (Choose three.)

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

Answer: ABD

NEW QUESTION 45
The default host name used in Inputs general settings can not be changed.

A. False
B. True

Answer: A

NEW QUESTION 46
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 51

.....

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