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
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
Which statement is true about Splunk alerts?

A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
B. Alerts are based on searches and when triggered will only send an email notification.
C. Alerts are based on searches and require cron to run on scheduled interval.
D. Alerts are based on searches that are run exclusively as real-time.

Answer: A

NEW QUESTION 4
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 5
In the fields sidebar, which character denotes alphanumeric field values?

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

Answer: B

NEW QUESTION 6
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 7
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 8
Which of the following is the most efficient filter for running searches in Splunk?

A. Time
B. Fast mode
C. Sourcetype
D. Selected Fields

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
Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms.
B. Include at least one function as this is a search requirement.
C. Include the search terms at the beginning of the search string.
D. Avoid using formatting clauses, as they add too much overhead.

Answer: D

NEW QUESTION 10
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 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
What does the following specified time range do?
earliest=-72h@h latest=@d

A. Look back 3 days ago and prior.
B. Look back 72 hours, up to one day ago.
C. Look back 72 hours, up to the end of today.
D. Look back from 3 days ago, up to the beginning of today.

Answer: C

NEW QUESTION 19
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 24
What happens when a field is added to the Selected Fields list in the fields sidebar?

A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
D. The selected field and its corresponding values will appear underneath the events in the search results.

Answer: D

NEW QUESTION 27
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 28
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 33
All components are installed and administered in Splunk Enterprise on-premise.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Explanation/Reference:
B. False
Answer:

NEW QUESTION 35
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 40
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 44
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 47
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 51
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 52
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 53
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 54
Splunk index time process can be broken down into _____ phases.

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

Answer: A

NEW QUESTION 58
Where does Licensing meter happen?

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

Answer: A

NEW QUESTION 60
Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 64
You can view the search result in following format (Choose three.):

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

Answer: ABD

NEW QUESTION 67

.....

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