SPLK-1001 Dumps

Splunk Core Certified User Exam

https://www.certleader.com/SPLK-1001-dumps.html

NEW QUESTION 1
Which of the following is true about user account settings and preferences?

A. Search & Reporting is the only app that can be set as the default application.
B. Full names can only be changed by accounts with a Power User or Admin role.
C. Time zones are automatically updated based on the setting of the computer accessing Splunk.
D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Answer: B

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
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 4
What does the values function of the stats command do?

A. Lists all values of a given field.
B. Lists unique values of a given field.
C. Returns a count of unique values for a given field.
D. Returns the number of events that match the search.

Answer: C

NEW QUESTION 5
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 6
In the fields sidebar, which character denotes alphanumeric field values?

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

Answer: B

NEW QUESTION 7
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 8
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 9
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 10
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
What type of search can be saved as a report?

A. Any search can be saved as a report.
B. Only searches that generate visualizations.
C. Only searches containing a transforming command.
D. Only searches that generate statistics or visualizations.

Answer: A

NEW QUESTION 13
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 16
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 21
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 24
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 28
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 32
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 37
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 41
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Answer: A

NEW QUESTION 43
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 46
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 50
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 55
The default host name used in Inputs general settings can not be changed.

A. False
B. True

Answer: A

NEW QUESTION 56
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 60
Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts
B. Sourcetypes
C. Sources
D. Indexes

Answer: ABC

NEW QUESTION 65
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your SPLK-1001 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-1001-dumps.html