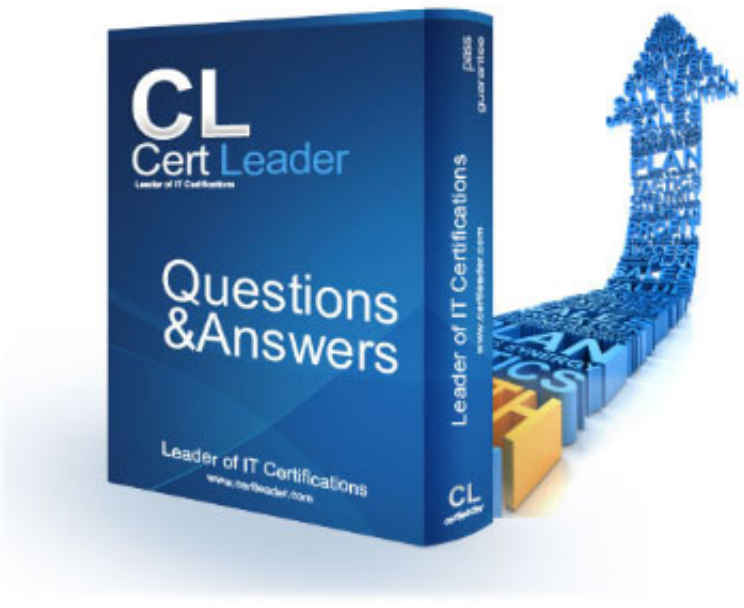
SPLK-1001 Dumps

Splunk Core Certified User Exam

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



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
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 3
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 4
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 5
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 6
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 7
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 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 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
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 10
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 12
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 15
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 18
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 19
What can be configured using the Edit Job Settings menu?

A. Export the result to CSV format.
B. Add the Job results to a dashboard.
C. Schedule the Job to re-run in 10 minutes.
D. Change Job Lifetime from 10 minutes to 7 days.

Answer: B

NEW QUESTION 22
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
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 29
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Answer: A

NEW QUESTION 31
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 34
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 38
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 40

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

A. False
B. True

Answer: B

NEW QUESTION 41
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 45
Which of the statements are correct about HF? (Choose three.)

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

Answer: ABD

NEW QUESTION 46
Where does Licensing meter happen?

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

Answer: A

NEW QUESTION 48
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 51
Splunk Parses data into individual events, extracts time, and assigns metadata.

A. False
B. True

Answer: B

NEW QUESTION 54
Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 55
You can view the search result in following format (Choose three.):

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

Answer: ABD

NEW QUESTION 56

.....

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