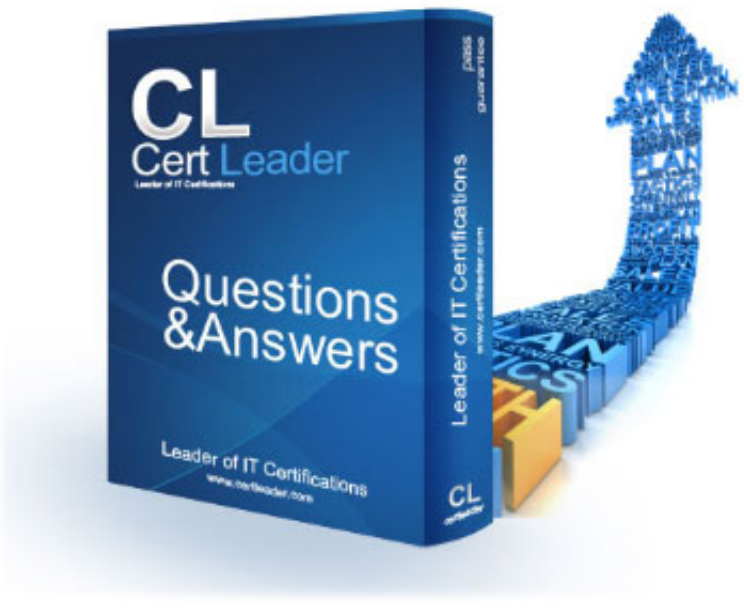
SPLK-1001 Dumps

Splunk Core Certified User Exam

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



NEW QUESTION 1
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 2
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 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
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 6
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 7
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 8
What is Splunk?

A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
B. Database management tool.
C. Security Information and Event Management (SIEM).
D. Cloud based application that help in analyzing logs.

Answer: A

NEW QUESTION 9
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Answer: A

NEW QUESTION 10
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 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 13
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Answer: B

NEW QUESTION 14
Which of the statements are correct about HF? (Choose three.)

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

Answer: ABD

NEW QUESTION 18
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 20
Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 22

.....

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