Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam

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

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

Answer: B

NEW QUESTION 6
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 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
What can be included in the All Fields option in the sidebar?

A. Dashboards
B. Metadata only
C. Non-interesting fields
D. Field descriptions

Answer: D

NEW QUESTION 10
When viewing the results of a search, what is an Interesting Field?

A. A field that appears in any event.
B. A field that appears in every event.
C. A field that appears in the top 10 events.
D. A field that appears in at least 20% of the events.

Answer: D

NEW QUESTION 12
Which command is used to validate a lookup file?

A. | lookup products.csv
B. inputlookup products.csv
C. | inputlookup products.csv
D. | lookup_definition products.csv

Answer: C

NEW QUESTION 16
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 19
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 23
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Answer: A

NEW QUESTION 28
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 31
Which is the default app for Splunk Enterprise?

A. Splunk Enterprise Security Suite
B. Searching and Reporting
C. Reporting and Searching
D. Splunk apps for Security

Answer: B

NEW QUESTION 33
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 38
Splunk shows data in _____ .

A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.

Answer: B

NEW QUESTION 41
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Answer: B

NEW QUESTION 45
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 47
Which of the statements are correct about HF? (Choose three.)

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

Answer: ABD

NEW QUESTION 48
Matching search terms are highlighted.

A. Yes
B. No

Answer: A

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
Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

A. Open new search.
B. Exclude the item from search.
C. None of the above.
D. Add the item to search.

Answer: ABD

NEW QUESTION 57
You can view the search result in following format (Choose three.):

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

Answer: ABD

NEW QUESTION 61
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 66
What options do you get after selecting timeline? (Choose four.)

A. Zoom to selection
B. Format Timeline
C. Deselect
D. Delete
E. Zoom Out

Answer: ABCE

NEW QUESTION 67
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-1001 Practice Test Here