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

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

Answer: B

NEW QUESTION 5
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 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
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 8
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 9
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 10
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 10
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 15
Which events will be returned by the following search string?
host=www3 status=503

A. All events that either have a host of www3 or a status of 503.
B. All events with a host of www3 that also have a status of 503.
C. We need more information; we cannot tell without knowing the time range.
D. We need more information; a search cannot be run without specifying an index.

Answer: B

NEW QUESTION 17
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 22
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
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 24
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 28
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 30
Splunk shows data in _____ .

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

Answer: B

NEW QUESTION 31
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 36
Splunk index time process can be broken down into _____ phases.

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

Answer: A

NEW QUESTION 38
Where does Licensing meter happen?

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

Answer: A

NEW QUESTION 41
Matching search terms are highlighted.

A. Yes
B. No

Answer: A

NEW QUESTION 44

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

A. False
B. True

Answer: B

NEW QUESTION 48
Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 50
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 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 59
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 64
.....

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