Splunk

Exam SPLK-1001

Splunk Core Certified User

Version: 12.0

[Total Questions: 229]

Question No : 1

Which of the following is the best way to create a report that shows the last 24 hours of events?

A. Use earliest=-1d@d latest=@d
B. Set a real-time search over a 24-hour window
C. Use the time range picket to select “Yesterday”
D. Use the time range picker to select “Last 24 hours”

Answer: D

Question No : 2

Put query into separate lines where | (Pipes) are used by selecting following options.

A. CTRL + Enter
B. Shift + Enter
C. Space + Enter
D. ALT + Enter

Answer: B

Question No : 3

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: D

Question No : 4

Which of the following searches will show the number of categoryId used by each host?

A. Sourcetype=access_* |sum bytes by host

B. Sourcetype=access_* |stats sum(categorylD) by host
C. Sourcetype=access_* |sum(bytes) by host
D. Sourcetype=access_* |stats sum by host

Answer: B

Question No : 5

Which of the statements are correct? (Choose three.)

A. Zoom to selection: Narrows the time range and re-executes the search.
B. Zoom to selection: Narrows the time range and doesn't re-executes the search.
C. Format Timeline: Hides or shows the timeline in different views.
D. Zoom-Out: Expands the time focus and doesn't re-executes the search.
E. Zoom-out: Expands the time focus and re-executes the search.

Answer: A,C,E

Question No : 6

Lookups allow you to overwrite your raw event.

A. True
B. False

Answer: A

Question No : 7

Which of the following is a metadata field assigned to every event in Splunk?

A. host
B. owner
C. bytes
D. action

Answer: A
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynami

cally

Question No : 8

Which command is used to review the contents of a specified static lookup file?

A. lookup
B. csvlookup
C. inputlookup
D. outputlookup

Answer: C

Question No : 9

By default, how long does Splunk retain a search job?

A. 10 Minutes
B. 15 Minutes
C. 1 Day
D. 7 Days

Answer: A

Question No : 10

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

A. inputlookup
B. lookup

Answer: B

Question No : 11

This is what Splunk uses to categorize the data that is being indexed.

A. Host
B. Sourcetype
C. Index
D. Source

Answer: B

Question No : 12

By default search results are not returned in _____ order.

A. Chronological
B. Reverser chronological
C. ASCIE
D. Alphabetical

Answer: A,D

Question No : 13

Which symbol is used to snap the time?

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

Answer: A

Question No : 14

The command shown here does witch of the following: Command: |outputlookup products.csv

A. Writes search results to a file named products.csv
B. Returns the contents of a file named products.csv

Answer: A

Question No : 15

Which of the following searches would return events with failure in index netfw or warn or critical in index netops?

A. (index=netfw failure) AND index=netops warn OR critical
B. (index=netfw failure) OR (index=netops (warn OR critical))
C. (index=netfw failure) AND (index=netops (warn OR critical))
D. (index=netfw failure) OR index=netops OR (warn OR critical)

Answer: B

Question No : 16

Which of the following fields is stored with the events in the index?

A. user
B. source
C. location
D. sourcelp

Answer: B

Question No : 17

Splunk automatically determines the source type for major data types.

A. False
B. True

Answer: B

Question No : 18

Which of the following are functions of the stats command?

A. count, sum, add
B. count, sum, less
C. sum, avg, values
D. sum, values, table

Answer: C

Question No : 19

Which of the following are Splunk premium enhanced solutions? (Choose three.)

A. Splunk User Behavior Analytics (UBA)
B. Splunk IT Service Intelligence (ITSI)
C. Splunk Enterprise Security (ES)
D. Splunk Analytics Security (AS)

Answer: A,B,C

Question No : 20

Which search will return the 15 least common field values for the dest_ip field?

A. sourcetype=firewall | rare num=15 dest_ip
B. sourcetype=firewall | rare last=15 dest_ip
C. sourcetype=firewall | rare count=15 dest_ip
D. sourcetype=firewall | rare limit=15 dest_ip

Answer: C
Reference: https://answers.splunk.com/answers/41928/add-a-lookup-csv-colum-information-to-the-results-ofa-inputlookup-search.html

Question No : 21

What is the correct way to use a time range specifier in the search bar so that the search looks back 2 hours?

A. latest=-2h
B. earliest=-2h
C. latest=-2hour@d
D. earliest=-2hour@d

Answer: B
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Specifytimemodifiersinyoursearch

Question No : 22

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: D

Question No : 23

Can you stop or pause the searching?

A. No
B. Yes

Answer: B

Question No : 24

Splunk indexes the data on the basis of timestamps.

A. True
B. False

Answer: A

Question No : 25

Which of the following commands will show the maximum bytes?

A. sourcetype=access_* | maximum totals by bytes
B. sourcetype=access_* | avg (bytes)
C. sourcetype=access_* | stats max(bytes)
D. sourcetype=access_* | max(bytes)

Answer: C

Question No : 26

At the time of searching the start time is 03:35:08.

Will it look back to 03:00:00 if we use -30m@h in searching?

A. Yes
B. No

Answer: A

Question No : 27

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

Question No : 28

Which Boolean operator is always implied between two search terms, unless otherwise specified?

A. OR
B. NOT
C. AND
D. XOR

Answer: C

Question No : 29

Which time range picker configuration would return real-time events for the past 30 seconds?

A. Preset - Relative: 30-seconds ago
B. Relative - Earliest: 30-seconds ago, Latest: Now
C. Real-time - Earliest: 30-seconds ago, Latest: Now
D. Advanced - Earliest: 30-seconds ago, Latest: Now

Answer: C

Question No : 30

Which of the following are not true about lookups? (Select all that apply.)

A. Lookups can be time based
B. Search results can be used to populate a lookup table
C. Splunk DB Connect can be used to populate a lookup table from relational databases
D. Output from a script can be used to populate a lookup table
E. Lookup have a 10mg maximum size limit

Answer: E