Free Questions for SPLK-1001 by actualtestdumps

Shared by Burton on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When is the pipe character, I, used in search strings?

Options:

A- Before clauses. For example: stats sum(bytes) | by host

B- Before commands. For example: | stats sum(bytes) by host

C- Before arguments. For example: stats sum| (bytes) by host

D- Before functions. For example: stats |sum(bytes) by host

Answer:

B

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/

Aboutsearchlanguagesyntax#Quotes_and_escaping_characters

Question 2

Question Type: MultipleChoice

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

Options:

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 3

Question Type: MultipleChoice

What are the two most efficient search filters?

Options:

A- _time and host

B- _time and index

C- host and sourcetype

D- index and sourcetype

Answer:

B

Question 4

Question Type: MultipleChoice

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

Options:

A- host

B- owner

C- bytes

D- action

Explanation:

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynamically

Answer:

A

Question 5

Question Type: **MultipleChoice**

In the Search and Reporting app, which tab displays timecharts and bar charts?

Options:

A- Events

B- Patterns

C- Statistics

D- Visualization

Explanation:

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Aboutreportingcommands

Answer:

D

Question 6

Question Type: **MultipleChoice**

Which of the following reports is available in the Fields window?

Options:

A- Top values by time

B- Rare values by time

C- Events with top value fields

D- Events with rare value fields

Answer:

C

Question 7

Question Type: **MultipleChoice**

Which search will return only events containing the word "error" and display the results as a table that includes

the fields named action, src, and dest?

Options:

A- error | table action, src, dest

B- error | tabular action, src, dest

C- error | stats table action, src, dest

D- error | table column=action column=src column=dest

Explanation:

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/search

Answer:

C