Free Questions for SPLK-1001 by go4braindumps

Shared by Shelton on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is a quick, comprehensive way to learn what data is present in a Splunk deployment?

Options:

A- Review Splunk reports

B- Run ./splunk show

C- Click Data Summary in Splunk Web

D- Search index=* sourcetype=* host=*

Explanation:

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/InheritedDeployment/Yourdata

Answer:

C

Question 2

Question Type: MultipleChoice

When viewing results of a search job from the Activity menu, which of the following is displayed?

Options:

A- New events based on the current time range picker

B- The same events based on the current time range picker

C- The same events from when the original search was executed

D- New events in addition to the same events from the original search

Answer:

C

Question 3

Question Type: MultipleChoice

Which of the following is a correct way to limit search results to display the 5 most common values of a field?

Options:

A- | rare top=5

B- | top rare=5

C- | top limit=5

D- | rare limit=5

Answer:

C

Question 4

Question Type: **MultipleChoice**

Which of the following is the most efficient search?

Options:

A- index=* "failed password"

B- "failed password" index=*

C- (index=* OR index=security) "failed password"

D- index=security "failed password"

Answer:

A

Question 5

Question Type: MultipleChoice

Which command will rename action to Customer Action?

Options:

A- | rename action = CustomerAction

B- | rename Action as "Customer Action"

C- | rename Action to "Customer Action"

D- | rename action as "Customer Action"

Explanation:

Reference:
https://answers.splunk.com/answers/610038/understanding-command-in-search.html

Answer:

D

Question 6

Question Type: MultipleChoice

Which of the following is a Splunk internal field?

Options:

A- _raw

B- host

C- _host

D- index

Answer:

A

Question 7

Question Type: MultipleChoice

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

Options:

A- latest=-2h

B- earliest=-2h

C- latest=-2hour@d

D- earliest=-2hour@d

Explanation:

Reference:

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

Answer:

B

Question 8

Question Type: MultipleChoice

What will always appear in the Selected Fields list?

Options:

A- index

B- action

C- clientip

D- sourcetype

Answer:

D