Free Questions for SPLK-1002 by go4braindumps

Shared by Phillips on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which search would limit an "alert" tag to the "host" field?

Options:

A) tag=alert

B) host::tag::alert

C) tag==alert

D) tag::host=alert

Answer:

D

Question 2

Question Type: MultipleChoice

Which of the following statements describe the Common Information Model (QM)? (select all that apply)

Options:

A) CIM is a methodology for normalizing data.

B) CIM can correlate data from different sources.

C) The Knowledge Manager uses the CIM to create knowledge objects.

D) CIM is an app that can coexist with other apps on a single Splunk deployment.

Answer:

A, B, C

Explanation:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

Question 3

Question Type: MultipleChoice

Which of the following knowledge objects represents the output of an oval expression?

Options:

A) Eval fields

B) Calculated fields

C) Field extractions

D) Calculated lookups

Answer:

B

Explanation:

https://docs.splunk.com/Splexicon:Calculatedfield

Question 4

Question Type: MultipleChoice

Data model are composed of one or more of which of the fo-owing datasets? (select all that apply.)

Options:

A) Events datasets

B) Search datasets

C) Transaction datasets

D) Any child of event, transaction, and search datasets

Answer:

A, B, C

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

Question 5

Question Type: **MultipleChoice**

Which of the following statements describe the search string below?

dacamodel Application_State All_Application_State search

Options:

A) Events will be returned from dataset named Application_state.

B) Events will be returned from the data model named Application_State.

C) Events will be returned from the data model named All_Application_state.

D) No events will be returned because the pipe should occur after the datamodel command

Answer:

C

Question 6

Question Type: **MultipleChoice**

When using timechart, how many fields can be listed after a by clause? (Choose Two)

Options:

A) because timechart doesn't support using a by clause.

B) because _time is already implied as the x-axis.

C) because one field would represent the x-axis and the other would represent the y-axis.

D) There is no limit specific to timechart.

Answer:

B, D

Question 7

Question Type: **MultipleChoice**

A user wants to convert field values to string and also to sort on those value. Which command should be used first, the eval or the sort?

Options:

A) It doesn't matter whether eval or sort is used first.

B) Convert the numeric to a string with eval first, then sort.

C) Use sort first, then convert the numeric to a string with eval.

D) You cannot use the sort command and the eval command on the same field.

Answer:

B

Question 8

Question Type: MultipleChoice

Which of the following actions can the aval command perform?

Options:

A) Remove fields from results.

B) Create or replace an existing field.

C) Group transactions by one or more fields.

D) Save SPL commands to be reused in other searches.

Answer:

B

Question 9

Question Type: MultipleChoice

Which of the following statements is true, especially in largo environments?

Options:

A) Use the scats command when you next to group events by two or more fields.

B) The scats command is faster and more efficient than the transaction command

C) The transaction command is faster and more efficient than the stats command.

D) Use the transaction command when you want to see the results of a calculation.

Answer:

C

Question 10

Question Type: MultipleChoice

What does the following search do?

index=condlog type=mysterymeat action=eaten I scats count as cornlog_count by us:

Options:

A) Creates a table of the total count of users and split by corndogs.

B) Creates a table of the total count of mysterymeat corndogs split by user.

C) Creates a table with the count of all types of corndogs eaten split by user.

D) Creates a table that groups the total number of users by vegetarian corndogs.

Answer:

A