Free Questions for SPLK-1002 by certsinside

Shared by Holmes on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following eval command functions is valid?

Options:

A- int()

B- count()

C- print()

D- tostring()

https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions

Answer:

D

Question 2

Question Type: MultipleChoice

What is the Splunk Common Information Model (CIM)?

Options:

A- The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.

B- The CIM provides a methodology to normalize data from different sources and source types.

C- The CIM defines an ecosystem of apps that can be fully supported by Splunk.

D- The CIM is a data exchange initiative between software vendors.

Answer:

B

Question 3

Question Type: **MultipleChoice**

How is a Search Workflow Action configured to run at the same time range as the original search?

Options:

A- Set the earliest time to match the original search.

B- Select the same time range from the time-range picker.

C- Select the 'Use the same time range as the search that created the field listing' checkbox.

D- Select the 'Overwrite time range with the original search' checkbox.

Answer:

C

Question 4

Question Type: **MultipleChoice**

What does the fillnull command replace null values with, if the value argument is not specified?

Options:

A- 0

B- N/A

C- NaN

D- NULL

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which of the following searches will return events containing a tag named Privileged?

Options:

A- tag=Priv

B- tag=Priv*

C- tag=priv*

D- tag=privileged

Answer:

B

Question 6

Question Type: MultipleChoice

Data models are composed of one or more of which of the following datasets? (select all that apply)

Options:

A- Transaction datasets

B- Events datasets

C- Search datasets

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

Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

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

Answer:

A, B, C

Question 7

Question Type: **MultipleChoice**

Consider the following search:

Index=web sourcetype=access_combined

The log shows several events that share the same JSESSIONID value (SD404K289O2F151). View the events as a group. From the following list, which search groups events by JSESSIONID?

Options:

A- index=web sourcetype=access_combined SD404K289O2F151 I table JSESSIONID

B- index=web sourcetype=access_combined JSESSIONID <SD404K289O2F151>

C- index=web sourcetype=access_combined I highlight JSESSIONID I search SD404K289O2F151

D- index-web sourcetype=access_combined I transaction JSESSIONID I search SD404K289O2F151

Answer:

B