DUMPSHQ

Free Questions for SPLK-1002 by dumpshq

Shared by Evans on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The macro weekly_sales (2) contains the search string:

index---games I eval Product Sales = $price$ $AmountS01d$

Which of the following will return results?

Options:

A- 'weekly_sales(3.99, 10) '

B- 'weekly_sales(3.99, 10)

C- 'weekly_sales (3.99, 10)

D- 'weekly_sales(3)

Answer:

C

Explanation:

The correct answer is C. 'weekly_sales (3.99, 10)'. This is because search macros accept arguments without quotation marks or dollar signs, and the number of arguments must match the number of parameters defined in the macro. The other options are incorrect because they either use quotation marks or dollar signs around the arguments, or they provide a different number of arguments than the macro expects. You can learn more about how to use search macros in searches from the Splunk documentation1.

Question 2

Question Type: MultipleChoice

Which search string would only return results for an event type called success ful_purchases?

Options:

A- tag=success ful_purchases

B- Event Type:: successful purchases

C- successful_purchases

D- event type---success ful_purchases

Answer:

C

Explanation:

This is because event types are added to events as a field named eventtype, and you can use this field as a search term to find events that match a specific event type. For example, eventtype=successful_purchases returns all events that have been categorized as successful purchases by the event type definition. The other options are incorrect because they either use a different field name (tag), a different syntax (Event Type:: or event type---), or have a typo (success ful_purchases).You can learn more about how to use event types in searches from the Splunk documentation1.

Question 3

Question Type: **MultipleChoice**

The macro weekly sales (2) contains the search string:

index=games | eval ProductSales = $Price$ * $AmountSold$

Which of the following will return results?

Options:

A- 'weekly sales (3)'

B- 'weekly_sales($3.995, $108)'

C- 'weekly_sales (3.99, 10)'

D- 'weekly sales (3.99, 10)'

Answer:

C

Explanation:

To use a search macro in a search string, you need to place a back tick character (`) before and after the macro name1. You also need to use the same number of arguments as defined in the macro2. The macro weekly sales (2) has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.

The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses spaces instead of commas to separate the argument values.

Question 4

Question Type: MultipleChoice

Which method in the Field Extractor would extract the port number from the following event? |

```
10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin
```

Options:

A- Delimiter

B- rex command

C- The Field Extractor tool cannot extract regular expressions.

D- Regular expression

Answer:

B

Explanation:

The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:

```
rex '\+\+\+\+port (?\d+)'
```

This will create a field called port with the value 54 for the event.

The delimiter method is not suitable for this event because there is no consistent delimiter between the fields. The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.

Question 5

Question Type: **MultipleChoice**

Calculated fields can be based on which of the following?

Options:

A- Tags

B- Extracted fields

C- Output fields for a lookup

D- Fields generated from a search string

Answer:

B

Explanation:

'Calculated fields can reference all types of field extractions and field aliasing, but they cannot reference lookups, event types, or tags.'

Question 6

Question Type: MultipleChoice

Which statement is true?

Options:

A- Pivot is used for creating datasets.

B- Data models are randomly structured datasets.

C- Pivot is used for creating reports and dashboards.

D- In most cases, each Splunk user will create their own data model.

Answer:

C

Explanation:

The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

Question 7

Question Type: MultipleChoice

A user wants to create a new field alias for a field that appears in two sourcetypes.

How many field aliases need to be created?

Options:

A- One.

B- Two.

C- It depends on whether the original fields have the same name.

D- It depends on whether the two sourcetypes are associated with the same index.

Answer:

B

Question 8

Question Type: **MultipleChoice**

Which command can include both an over and a by clause to divide results into sub-groupings?

Options:

A- chart

B- stats

C- xyseries

D- transaction

Answer:

A

Question 9

Question Type: **MultipleChoice**

When is a GET workflow action needed?

Options:

A- To send field values to an external resource.

B- To retrieve information from an external resource.

C- To use field values to perform a secondary search.

D- To define how events flow from forwarders to indexes.

Answer:

B

Question 10

Question Type: **MultipleChoice**

A data model can consist of what three types of datasets?

Options:

A- Pivot, searches, and events.

B- Pivot, events, and transactions.

C- Searches, transactions, and pivot.

D- Events, searches, and transactions.

Answer:

D

Question 11

Question Type: **MultipleChoice**

What information must be included when using the datamodel command?

Options:

A- status field

B- Multiple indexes

C- Data model field name.

D- Data model dataset name.

Answer:

D

Question 12

Question Type: **MultipleChoice**

Which of the following is a function of the Splunk Common Information Model (CIM)?

Options:

A- Normalizing data across a Splunk deployment.

B- Providing templates for reports and dashboards.

C- Algorithmically shifting events to other indexes.

D- Reingesting previously indexed data with new field names.

Answer:

A

20%
DISCOUNT