SPLK-1002$^{\text{Q\&As}}$

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

A. inputlookup

B. lookup

Correct Answer: B

QUESTION 2

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

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.

Correct Answer: ABC

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

The Common Information Model (CIM) is a methodology for normalizing data from different sources and making it easier to analyze and report on it3. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more3. One of the statements that describe the CIM is that it is a methodology for normalizing data, which means that it provides a standard way to name and structure data from different sources so that they can be compared and correlated3. Therefore, option A is correct. Another statement that describes the CIM is that it can correlate data from different sources, which means that it enables you to run searches and reports across data from different sources that share common fields and tags3. Therefore, option B is correct. Another statement that describes the CIM is that the Knowledge Manager uses the CIM to create knowledge objects, which means that the person who is responsible for creating and managing knowledge objects such as data models, field aliases, tags and event types can use the CIM as a guide to make their knowledge objects consistent and compatible with other apps and add-ons3. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.

QUESTION 3

The stats command will create a _____________ by default.

A. Table

B. Report

C. Pie chart

Correct Answer: A

QUESTION 4

Which of the following commands support the same set of functions?

A. stats, eval, table

B. search, where, eval

C. stats, chart, timechart

D. transaction, chart, timechart

Correct Answer: C

QUESTION 5

Which of the following statements about tags is true?

A. Tags are case insensitive.

B. Tags can make your data more understandable.

C. Tags are created at index time.

D. Tags are searched by using the syntax tag :: .

Correct Answer: B

Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .

Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or tag the value 404 as not_found .

QUESTION 6

A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, the eval or the sort?

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.

Correct Answer: C

Explanation: The eval command is used to create new fields or modify existing fields based on an expression2. The sort command is used to sort the results by one or more fields in ascending or descending order2. If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings2. This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 7

Which syntax will find events where the values for the 1 field match the values for the Renewal-MonthYear field?

A. | where 10yearAnnerversary=Renewal-MonthYear

B. | where `10yearAnnerversary=Renewal-MonthYear

C. | where 10yearAnnerversary=\\'Renewal-MonthYear\\'

D. | where `10yearAnnerversary\\'=\\'Renewal-MonthYear\\'

Correct Answer: A

Explanation: The correct answer is A. | where 10yearAnnerversary=Renewal-MonthYear.

The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions,

operators, and wildcards to create complex expressions1.

The syntax for the where command is:

| where

The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event. To compare two fields with the where command, you need to use the field names

without any quotation marks. For example, if you want to find events where the values for the 10yearAnnerversary field match the values for the Renewal-MonthYear field, you can use the following syntax:

| where 10yearAnnerversary=Renewal-MonthYear

This will return only the events where the two fields have the same value. The other options are not correct because they use quotation marks around the field names, which will cause the where command to interpret them as string values

instead of field names. For example, if you use:

| where `10yearAnnerversary\\'=`Renewal-MonthYear\\' This will return no events because there are no events where the string value `10yearAnnerversary\\' is equal to the string value `Renewal-MonthYear\\'.

References:

where command usage

QUESTION 8

What is the correct format for naming a macro with multiple arguments?

A. monthly_sales(argument 1, argument 2, argument 3)

B. monthly_sales(3)

C. monthly_sales[3]

D. monthly_sales[argument 1, argument 2, argument 3)

Correct Answer: C

Explanation: The correct format for naming a macro with multiple arguments is monthly_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as monthly_sales[region,salesperson,date].

QUESTION 9

What are the two parts of a root event dataset?

A. Fields and variables.

B. Fields and attributes.

C. Constraints and fields.

D. Constraints and lookups.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodel objects

A root event dataset is the base dataset for a data model that defines the source or sources of the data and the constraints and fields that apply to the data1. A root event dataset has two parts: constraints and fields1. Constraints are filters that limit the data to a specific index, source, sourcetype, host or search string1. Fields are the attributes that describe the data and can be extracted, calculated or looked up1. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 10

A user runs the following search:

index--X sourcetype=Y I chart count (domain) as count, sum (price) as sum by product, action usenull=f useother--f

Which of the following table headers match the order this command creates?

A. The chart command does not allow for multiple statistical functions.

B. Product, sum: addtocart, sum: remove, sum: purchase, count: addtocart, count: remove, count: purchase

C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase

D. Count: product, sum: product, count: action, sum: action

Correct Answer: C

The correct answer is C. Product, count: addtocart, count: remove, count: purchase, sum:

addtocart, sum: remove, sum: purchase1.

In Splunk, the chart command is used to create a table or a chart visualization from your data2. The chart command takes at least one function and one field, and optionally another field to group by2.

In the given search, the chart command is used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action). The usenull=f and useother=f options are used to exclude null values and

other values from the chart2. The chart command creates a table with headers that match the order of the fields and functions in the command1. The headers for the count function are prefixed with count:, and the headers for the sum

function are prefixed with sum:1. The values of the product and action fields are used as the suffixes for the headers1. Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase,

sum: addtocart, sum: remove, and sum: purchase1.

QUESTION 11

When creating a data model, which root dataset requires at least one constraint?

A. Root transaction dataset

B. Root event dataset

C. Root child dataset

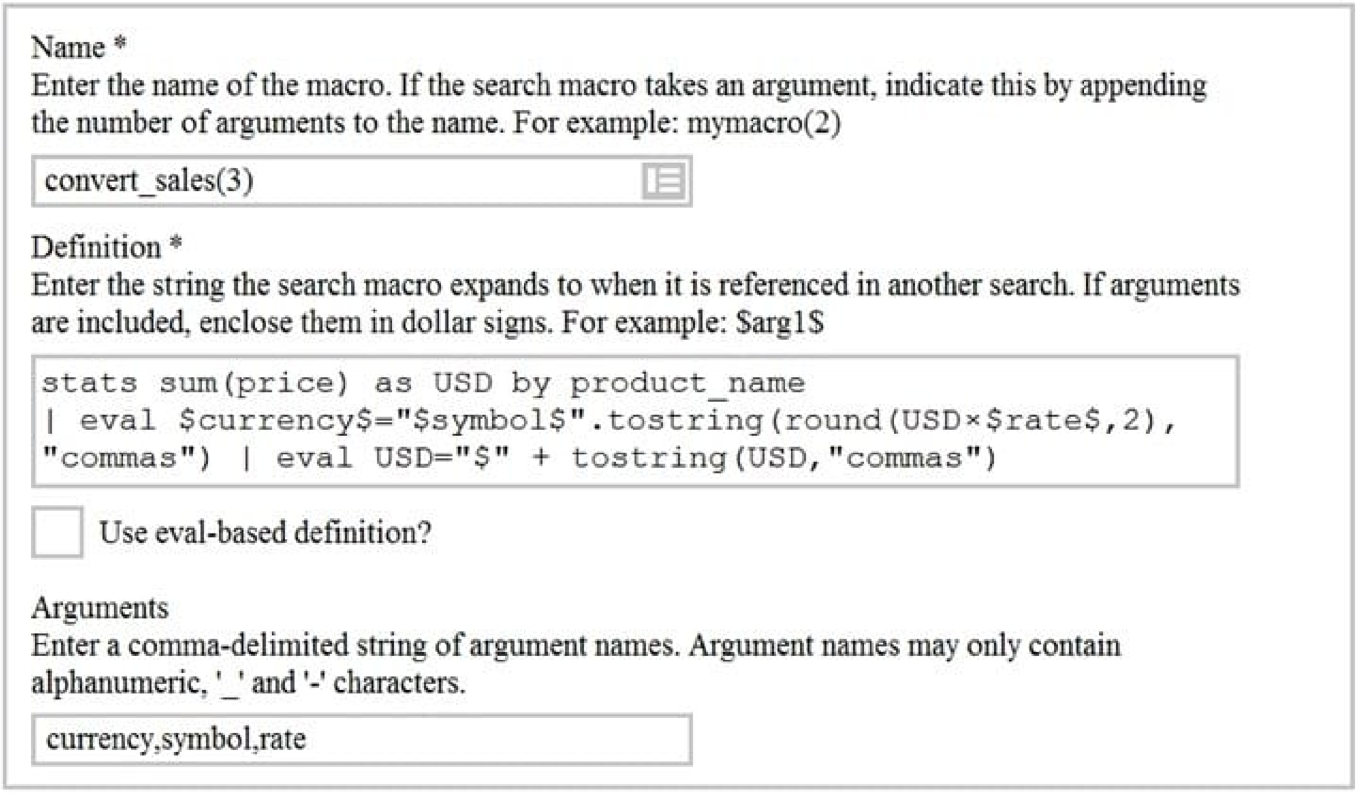
D. Root search dataset

Correct Answer: B

Explanation: The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation1. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

QUESTION 12

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD×$rate$,2),
"commas") | eval USD="$" + tostring(USD,"commas")
```

□ Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

A. Convert_sales (euro, , 79)"

B. Convert_sales (euro, , .79)

C. Convert_sales ($euro,$$,s79$

D. Convert_sales ($euro, $$,S,79$)

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros

The correct way to execute the macro in a search string is to use the format macro_name($arg1$, $arg2$, ...) where $arg1$, $arg2$, etc. are the arguments for the macro. In this case, the macro name is convert_sales and it takes three

arguments: currency, symbol, and rate. The arguments are enclosed in dollar signs and separated by commas. Therefore, the correct way to execute the macro is convert_sales($euro$, $$, .79).

QUESTION 13

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

A. Index-main | REJECT trans sessionid

B. Index-main | transaction sessionid | search REJECT

C. Index=main | transaction sessionid | whose transaction=reject

D. Index=main | transaction sessionid | where transaction=reject\\'\\'

Correct Answer: B

Explanation: The transaction command is used to group events that share a common value for one or more fields into transactions2. The transaction command assigns a transaction ID to each group of events and creates new fields such as duration, eventcount and eventlist for each transaction2. To identify all of the contributing events within a transaction that contains at least one REJECT event, you can use the following syntax: index=main | transaction sessionid | search REJECT2. This search will first group the events by sessionid, then filter out the transactions that do not contain REJECT in any of their events2. Therefore, option B is correct, while options A, C and D are incorrect because they do not follow the correct syntax for using the transaction command or the search command.

QUESTION 14

What is a limitation of searches generated by workflow actions?

A. Searches generated by workflow action cannot use macros.

B. Searches generated by workflow actions must be less than 256 characters long.

C. Searches generated by workflow action must run in the same app as the workflow action.

D. Searches generated by workflow action run with the same permissions as the user running them.

Correct Answer: D

QUESTION 15

Use the dedup command to _____.

A. Rename a field in the index

B. remove duplicate values

C. provide an additional alias for the field that can D.be used in the search criteria

Correct Answer: B