SPLK-1002 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.passapply.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following statements describe GET workflow actions?

A. GET workflow actions must be configured with POST arguments.

B. Configuration of GET workflow actions includes choosing a sourcetype.

C. Label names for GET workflow actions must include a field name surrounded by dollar signs.

D. GET workflow actions can be configured to open the URT link in the current window or in a new window

Correct Answer: D

GET workflow actions are custom actions that open a URL link when you click on a field value in your search results. GET workflow actions can be configured with various options, such as label name, base URL, URI parameters, app context, etc. One of the options is to choose whether to open the URL link in the current window or in a new window. GET workflow actions do not have to be configured with POST arguments, as they use GET method to send requests to web servers. Configuration of GET workflow actions does not include choosing a sourcetype, as they do not generate any data in Splunk. Label names for GET workflow actions must include a field name surrounded by dollar signs, as this indicates the field value that will be used to replace the variable in the URL link.

QUESTION 2

How can an existing accelerated data model be edited?

A. An accelerated data model can be edited once its .tsidx file has expired.

B. An accelerated data model can be edited from the Pivot tool.

C. The data model must be de-accelerated before edits can be made to its structure.

D. It cannot be edited. A new data model would need to be created.

Correct Answer: C

An existing accelerated data model can be edited, but the data model must be de- accelerated before any structural edits can be made (Option C). This is because the acceleration process involves pre-computing and storing data, and changes to the data model\\'s structure could invalidate or conflict with the pre-computed data. Once the data model is de-accelerated and edits are completed, it can be re-accelerated to optimize performance.

QUESTION 3

In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")

A. The description field would contain no value.

B. The description field would contain the value 0.

C. The description field would contain the value "Internal Server Error".

D. This statement would produce an error in Splunk because it is incomplete.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctio ns

QUESTION 4

When should the regular expression mode of Field Extractor (FX) be used? (select all that apply)

A. For data cleanly separated by a space, a comma, or a pipe character.

B. For data in a CSV (comma-separated value) file.

C. For data with multiple, different characters separating fields.

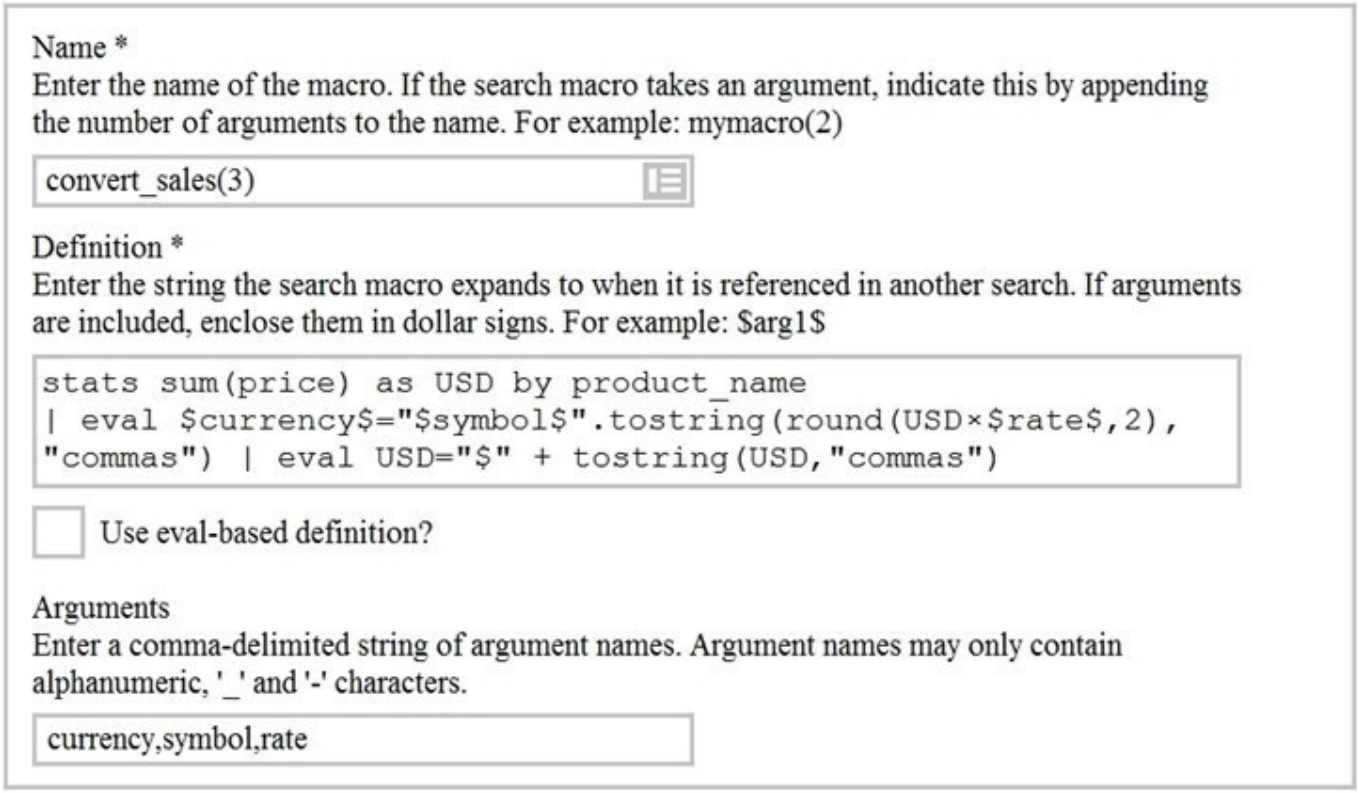
D. For unstructured data.

Correct Answer: CD

The regular expression mode of Field Extractor (FX) should be used for data with multiple, different characters separating fields or for unstructured data. The regular expression mode allows you to select a sample event and highlight the fields that you want to extract, and the field extractor generates a regular expression that matches similar events and extracts the fields from them.ReferencesSee Build field extractions with the field extractor - Splunk Documentation and Field Extractor: Select Method step - Splunk Documentation.

QUESTION 5

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



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).