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.geekcert.com/splk-1002.html

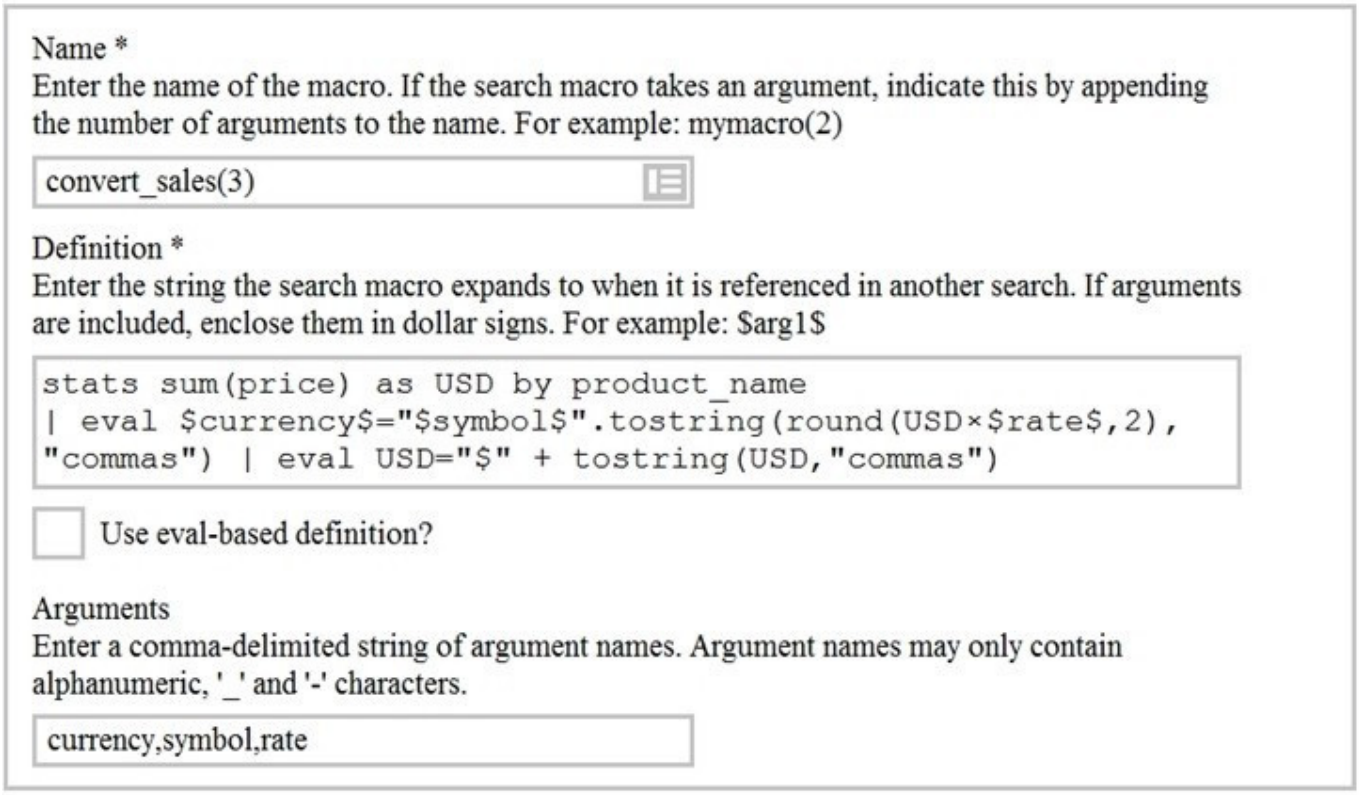
100% Passing Guarantee
100% Money Back Assurance

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

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).

QUESTION 2

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 3

Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

A. Events in the transaction occurred within 5 seconds.

B. It groups events that share the same clientip and host.

C. The first and last events are no more than 5 seconds apart.

D. The first and last events are no more than 30 seconds apart.

Correct Answer: ABD

The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction. index=main | transaction clientip host maxspan=30s maxpause=5s The search does the following: It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes. It uses the transaction command to group events into transactions based on two fields: clientip and host. The transaction command creates new events from groups of events that share the same clientip and host values. It specifies the start and end constraints for the transactions using the maxspan and maxpause arguments. The maxspan argument sets the maximum time span between the first and last events in a transaction. The maxpause argument sets the maximum time span between any two consecutive events in a transaction. In this case, the maxspan is 30 seconds and the maxpause is 5 seconds, meaning that any transaction that has a longer time span or pause will be split into multiple transactions. It creates some additional fields for each transaction, such as duration, eventcount, startime, etc. The duration field shows the time span between the first and last events in a transaction.

QUESTION 4

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

A. Auto-Extracted fields can be hidden in Pivot.

B. Auto-Extracted fields can have their data type changed.

C. Auto-Extracted fields can be given a friendly name for use in Pivot.

D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Correct Answer: ACD

Auto-Extracted fields in Splunk Data Models are derived directly from the indexed data based on the existing fields within the events. These fields are identified and extracted by Splunk automatically, without the need for explicit field extractions configured by the user. Understanding the characteristics of Auto-Extracted fields is crucial for effectively managing Data Models and utilizing them in Pivot tables for analysis. A. Auto-Extracted fields can be hidden in Pivot. This is true. When building a Data Model, you have the option to hide certain fields from appearing in Pivot, making the Pivot table cleaner and more focused on the fields that are most relevant for analysis. This helps in reducing clutter and focusing on the data that matters most to the users. B. Auto-Extracted fields can have their data type changed. This statement is not typically accurate for Auto-Extracted fields. The data type of an Auto-Extracted field is determined by Splunk based on the field\\'s content in the indexed data. While you can assign a type to a field when you manually create a field in a data model, the inherent data type of Auto-Extracted fields is not something that is changed within the Data Model itself. C. Auto-Extracted fields can be given a friendly name for use in Pivot. This is correct. Within Data Models, you can assign a more user-friendly, descriptive name to an Auto- Extracted field. This feature is particularly useful in making Data Models more intuitive and easier to use for those who may not be familiar with the original field names or when the original field names are not descriptive or user-friendly. D. Auto-Extracted fields can be added if they already exist in the dataset with constraints. This is true. Auto-Extracted fields are based on fields that already exist in the data. When you define a dataset within a Data Model, you can apply constraints to narrow down the events that the dataset includes. The Auto-Extracted fields are then identified from this constrained dataset. This means that the fields must already be present in the data that meets the dataset\\'s constraints to be available for auto-extraction. In summary, Auto-Extracted fields in Splunk Data Models offer a flexible and efficient way to utilize existing data fields within Pivot tables, with options to rename them for clarity and hide unnecessary fields to streamline data analysis.

QUESTION 5

Which of the following statements describes calculated fields?

A. Calculated fields are only used on fields added by lookups.

B. Calculated fields are a shortcut for repetitive and complex eval commands.

C. Calculated fields are a shortcut for repetitive and complex calc commands.

D. Calculated fields automatically calculate the simple moving average for indexed fields.

Correct Answer: B