Splunk Core Certified Power User Exam

Splunk SPLK-1002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 96

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

When should you use the transaction command instead of the stats command?

A. When you need to group on multiple values.

B. When duration is irrelevant in search results.

C. When you have over 1000 events in a transaction.

D. When you need to group based on start and end constraints.

ANSWER: A

Explanation:

Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/book-excerpt-when-to-use-transaction-and-when-to-use-stats.html

QUESTION NO: 2

When is a GET workflow action needed?

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: A

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaGETworkflowaction

QUESTION NO: 3

Which of the following statements describe the Common Information Model (CIM)? (Choose 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.

ANSWER: A B D

Explanation:

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

QUESTION NO: 4

Which of the following statements about data models and pivot are true? (Choose all that apply.)

A. They are both knowledge objects.

B. Data models are created out of datasets called pivots.

C. Pivot requires users to input SPL searches on data models.

D. Pivot allows the creation of data visualizations that present different aspects of a data model.

ANSWER: B D

QUESTION NO: 5

Which of the following statements about macros is true? (Choose all that apply.)

A. Arguments are defined at execution time.

B. Arguments are defined when the macro is created.

C. Argument values are used to resolve the search string at execution time.

D. Argument values are used to resolve the search string when the macro is created.

ANSWER: A C

QUESTION NO: 6

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.

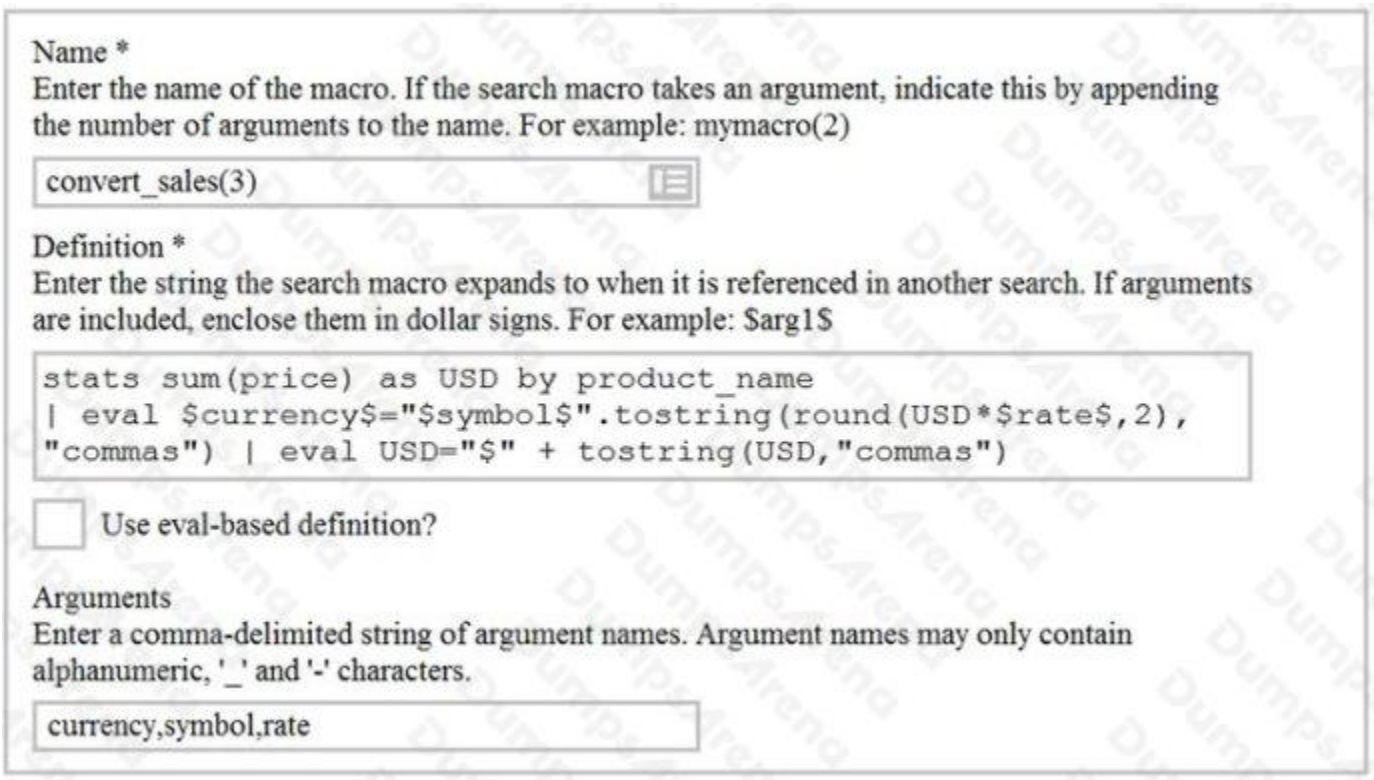
ANSWER: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions

QUESTION NO: 7

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($euro$,$€$,$.79$)"

D. 'convert_sales($euro$,$€$,$.79$)'

ANSWER: B

Explanation:

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

QUESTION NO: 8

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (Choose all that apply.)

A. Fast mode is enabled.

B. The dashboard is private.

C. The extraction is private.

D. The person in the organization running the report does not have access to the index.

ANSWER: C D

QUESTION NO: 9

Which of the following statements describe calculated fields? (Choose all that apply.)

A. Calculated fields can be used in the search bar.

B. Calculated fields can be based on an extracted field.

C. Calculated fields can only be applied to host and sourcetype.

D. Calculated fields are shortcuts for performing calculations using the eval command.

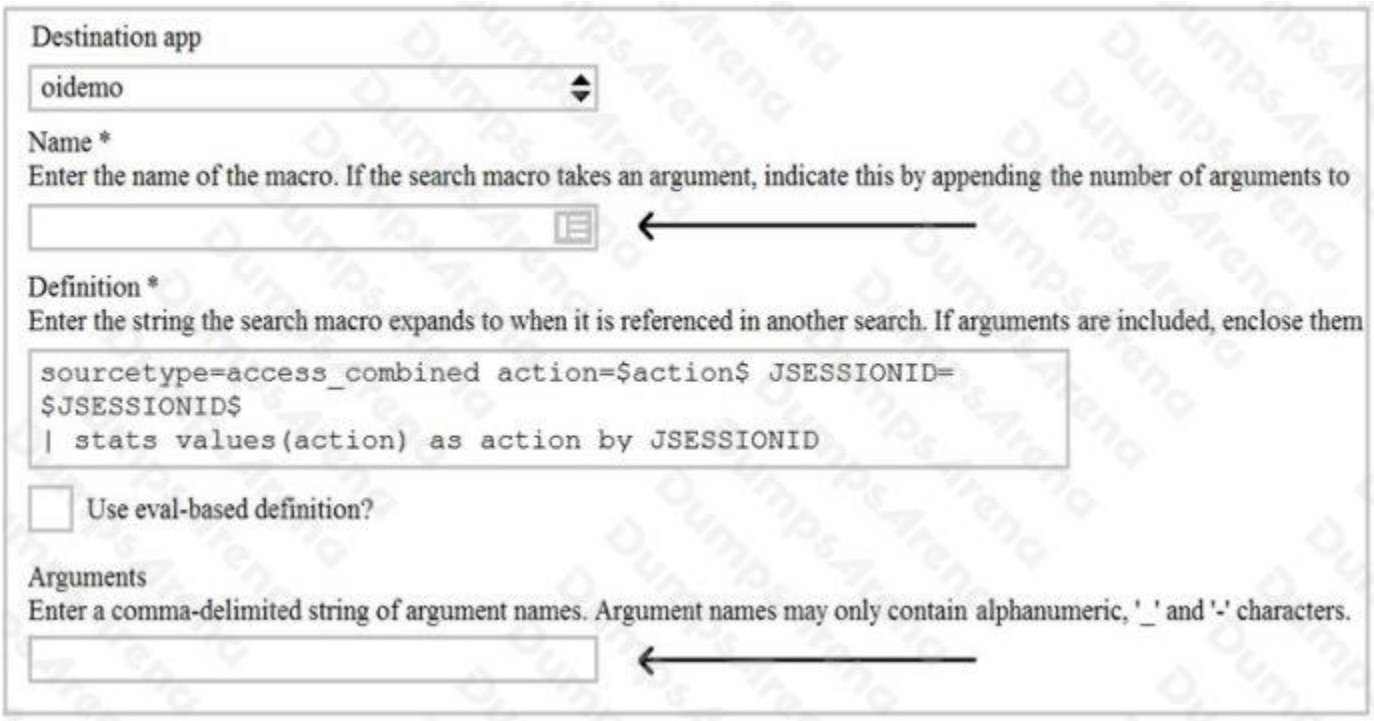
ANSWER: A B D

Explanation:

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

QUESTION NO: 10

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configure the macro?



A. The macro name is sessiontracker and the arguments are action, JESSIONID.

B. The macro name is sessiontracker(2) and the arguments are action, JESSIONID.

C. The macro name is sessiontracker and the arguments are $action$, $JESSIONID$.

D. The macro name is sessiontracker(2) and the Arguments are $action$, $JESSIONID$.

ANSWER: B

Explanation:

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