Splunk Core Certified Power User

Splunk SPLK-1002 Dumps Available Here at:

https://www.certification-questions.com/splunk-exam/splk-1002-dumps.html

Enrolling now you will get access to 181 questions in a unique set of SPLK-1002 dumps

Which of the following Statements about macros is true? (select all that apply)

Question 1

Which of the following Statements about macros is true? (select all that apply)

Options:

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: B, C

What is required for a macro to accept three arguments?

Question 2

What is required for a macro to accept three arguments?

Options:

A. The macro's name ends with (3).

B. The macro's name starts with (3).

C. The macro's argument count setting is 3 or more.

D. Nothing, all macros can accept any number of arguments.

Answer: A

Which of the following statements describes POST workflow actions?

Question 3

Which of the following statements describes POST workflow actions?

Options:

A. POST workflow actions are always encrypted.

B. POST workflow actions cannot use field values in their URI.

C. POST workflow actions cannot be created on custom sourcetypes.

D. POST workflow actions can open a web page in either the same window or a new .

Answer: D

Which of the following searches show a valid use of macro? (Select all that apply)

Question 4

Which of the following searches show a valid use of macro? (Select all that apply)

Options:

A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField

B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time

newField

C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time

newField

D. index=main source=mySource oldField=* | "'newField('makeMyField(oldField)')'" | table _time

newField

Answer: A, C

Explanation:
tps://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html
Explanation:

Which of the following workflow actions can be executed from search results? (select all that apply)

Question 5

Which of the following workflow actions can be executed from search results? (select all that apply)

Options:

A. GET

B. POST

C. LOOKUP

D. Search

Answer: A, B, D

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

Question 6

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

Options:

A. | datamodel web search | filed web *

B. | Search datamodel web web | filed web*

C. | datamodel web web field | search web*

D. Datamodel=web | search web | filed web*

Answer: A

Which of the following searches will return events contains a tag name Privileged?

Question 7

Which of the following searches will return events contains a tag name Privileged?

Options:

A. Tag= Priv

B. Tag= Pri*

C. Tag= Priv*

D. Tag= Privileged

Answer: B

Explanation:
tps://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity
Explanation:

Which of the following statements describes this search?

sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

Question 8

Which of the following statements describes this search?

sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

Options:

A. This is a valid search and will display a timechart of the average duration, of each transaction

event.

B. This is a valid search and will display a stats table showing the maximum pause among

transactions.

C. No results will be returned because the transaction command must include the startswith and

endswith options.

D. No results will be returned because the transaction command must be the last command used in

the search pipeline.

Answer: A

Calculated fields can be based on which of the following?

Question 9

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:

tps://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

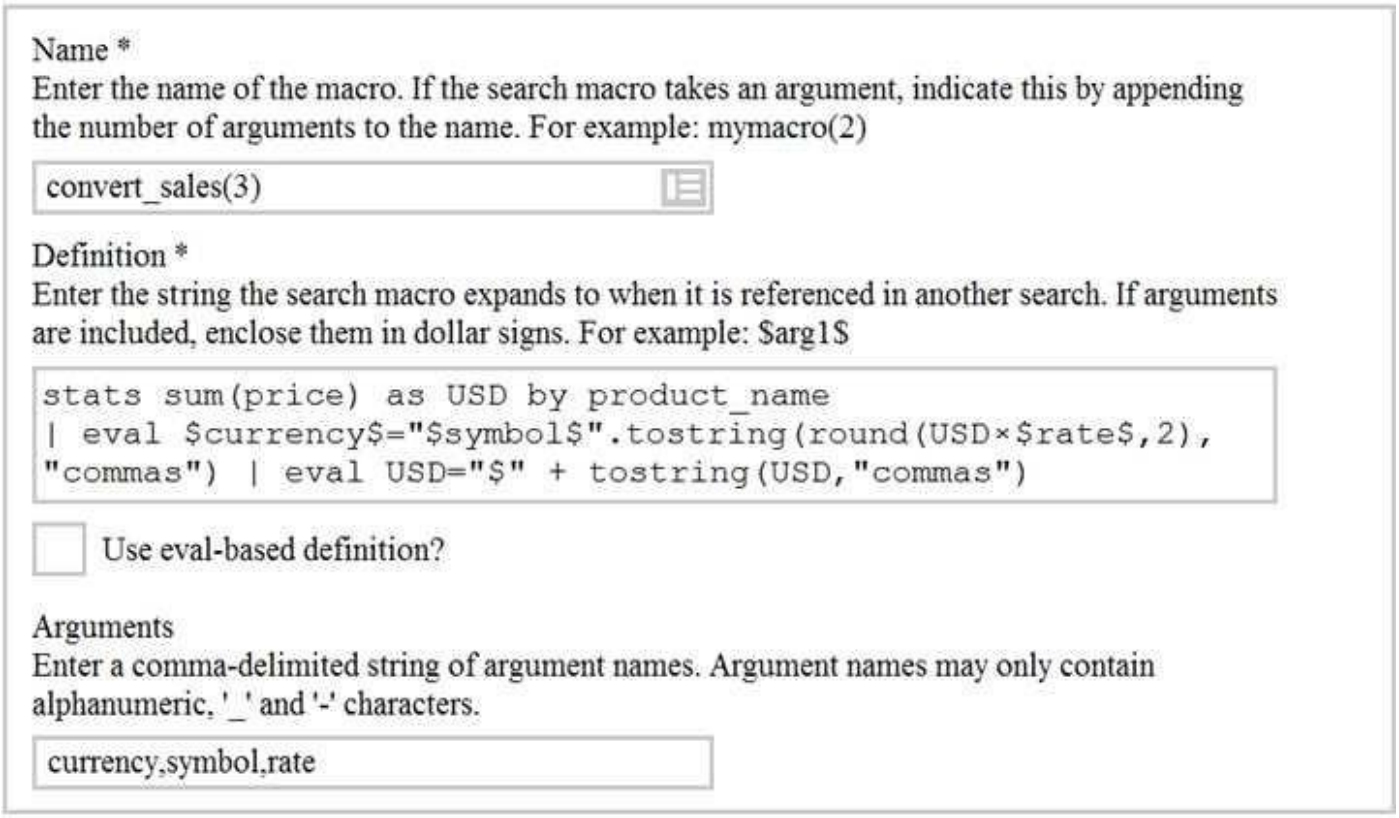
Explanation:

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

[PIC-2-2127357525]

Question 10

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



Options:

A. Convert_sales (euro, €, 79)”

B. Convert_sales (euro, €, .79)

C. Convert_sales ($euro,$€$,s79$

D. Convert_sales ($euro, $€$,S,79$)

Answer: B

Explanation:

tps://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros

Explanation: