Splunk

SPLK-1002 Exam

Splunk Core Certified Power User Exam

Questions & Answers
(Demo Version – Limited Content)

Thank you for Downloading SPLK-1002 exam PDF Demo

Version: 10.0

Question: 1

Which of the following Statements about macros is true? (select 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: 2

What is required for a macro to accept three arguments?

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

Question: 3

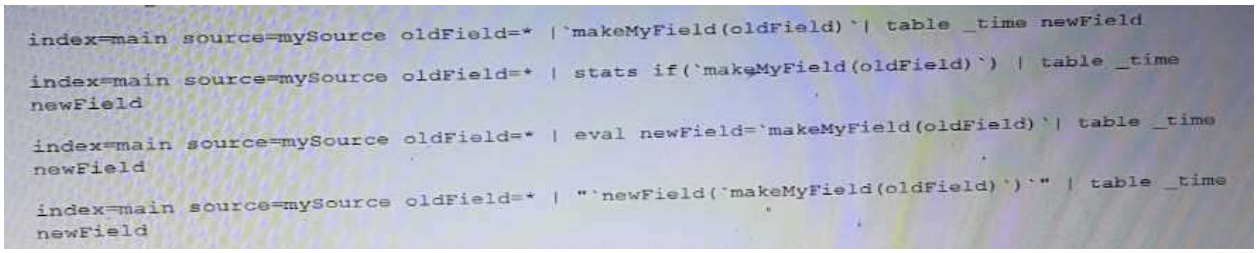
Which of the following statements describes POST workflow actions?

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

Question: 4

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



A. Option A
B. Option B
C. Option C
D. Option D

Answer: A, C

Question: 5

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

A. GET
B. POST
C. LOOKUP
D. Search

Answer: A, B, D

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?

A. | datamodel web search | filed web *
B. | Search datamodel web web | filedweb*
C. | datamodel web web field | searchweb*
D. Datamodel=web | search web | filed web*

Answer: A

Question: 7

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

A. Tag= Priv

B. Tag= Priv*
C. Tag= Priv*
D. Tag= Privileged

Answer: D

Question: 8

Which of the following statements describes this search?
sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

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

Question: 9

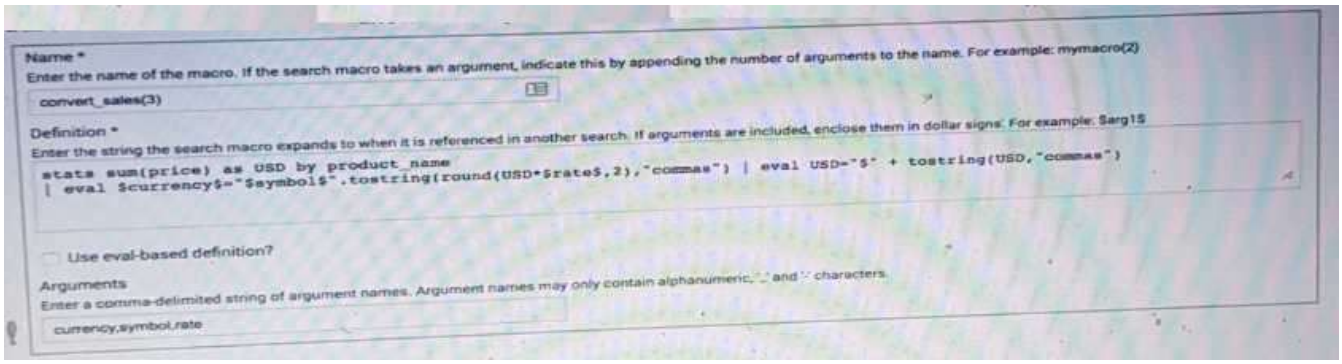
Calculated fields can be based on which of the following?

A. Tags
B. Extracted fields
C. Output fields for a lookup
D. Fields generated from a search string

Answer: B

Question: 10

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$)

Answer: B

Thank You for trying SPLK-1002 PDF Demo