Splunk

SPLK-1002 Exam

Splunk Core Certified Power User

**Questions & Answers
Demo**

Version: 14.0

Topic 1, Questions Set 1

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: B, 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. 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

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

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