

# IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

**Exam : SPLK-1002**

**Title : Splunk Core Certified Power User**

**Version : DEMO**

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

**Explanation:**

A macro is a way to save a commonly used search string as a variable that you can reuse in other searches<sup>1</sup>. When you create a macro, you can define arguments that are placeholders for values that you specify at execution time<sup>1</sup>. The argument values are used to resolve the search string when the macro is invoked, not when it is created<sup>1</sup>. Therefore, statements B and C are true, while statements A and D are false.

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

**Explanation:**

To create a macro that accepts arguments, you must include the number of arguments in parentheses at the end of the macro name<sup>1</sup>. For example, my\_macro(3) is a macro that accepts three arguments. The number of arguments in the macro name must match the number of arguments in the definition<sup>1</sup>. Therefore, option A is correct, while options B, C and D are incorrect.

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

**Explanation:**

A workflow action is a link that appears when you click an event field value in your search results<sup>1</sup>. A workflow action can open a web page or run another search based on the field value<sup>1</sup>. There are two types of workflow actions: GET and POST<sup>1</sup>. A GET workflow action appends the field value to the end of a URI and opens it in a web browser<sup>1</sup>. A POST workflow action sends the field value as part of an HTTP request to a web server<sup>1</sup>. You can configure a workflow action to open a web page in either the same window or a new window<sup>1</sup>. Therefore, option D is correct, while options A, B and C are incorrect.

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

**Explanation:**

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

To use a macro in a search, you must enclose the macro name and any arguments in single quotation marks<sup>1</sup>. For example, 'my\_macro(arg1,arg2)' is a valid way to use a macro with two arguments. You can use macros anywhere in your search string where you would normally use a search command or expression<sup>1</sup>. Therefore, options A and C are valid searches that use macros, while options B and D are invalid because they do not enclose the macros in single quotation marks.

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

**Explanation:**

As mentioned before, there are two types of workflow actions: GET and POST<sup>1</sup>. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it<sup>1</sup>. Another type of workflow action is Search, which runs another search based on the field value<sup>1</sup>. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.