

SPLK-1002^{Q&As}

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/splk-1002.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

When creating a Search workflow action, which field is required?

- A. Search string
- B. Data model name
- C. Permission setting
- D. An eval statement

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction>

A workflow action is a link that appears when you click an event field value in your search results. A workflow action can open a web page or run another search based on the field value. There are two types of workflow actions: GET and POST. A GET workflow action appends the field value to the end of a URI and opens it in a web browser. A POST workflow action sends the field value as part of an HTTP request to a web server. When creating a Search workflow action, which is a type of GET workflow action that runs another search based on the field value, the only required field is the search string. The search string defines the search that will be run when the workflow action is clicked. Therefore, option A is correct, while options B, C and D are incorrect because they are not required fields for creating a Search workflow action.

QUESTION 2

When extracting fields, we may choose to use our own regular expressions

- A. True
- B. False

Correct Answer: A

QUESTION 3

A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, the eval or the sort?

- A. It doesn't matter whether eval or sort is used first.
- B. Convert the numeric to a string with eval first, then sort.
- C. Use sort first, then convert the numeric to a string with eval.
- D. You cannot use the sort command and the eval command on the same field.

Correct Answer: C

Explanation: The eval command is used to create new fields or modify existing fields based on an expression². The sort command is used to sort the results by one or more fields in ascending or descending order². If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings². This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 4

What is the correct syntax to search for a tag associated with a value on a specific fields?

A. Tag-