

KillTest

質量更高 服務更好



學習資料

<http://www.killtest.net>

一年免費更新服務

Exam : **SPLK-1002**

Title : Splunk Core Certified Power
User

Version : DEMO

1.Which one of the following statements about the search command is true?

- A. It does not allow the use of wildcards.
- B. It treats field values in a case-sensitive manner.
- C. It can only be used at the beginning of the search pipeline.
- D. It behaves exactly like search strings before the first pipe.

Answer: C

Explanation:

Reference:

<https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usetheseearchcommand>

2.Which of the following actions can the eval command perform?

- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

Answer: A

3.When can a pipe follow a macro?

- A. A pipe may always follow a macro.
- B. The current user must own the macro.
- C. The macro must be defined in the current app.
- D. Only when sharing is set to global for the macro.

Answer: A

4.Data models are composed of one or more of which of the following datasets? (Choose all that apply.)

- A. Events datasets
- B. Search datasets
- C. Transaction datasets
- D. Any child of event, transaction, and search datasets

Answer: ABC

Explanation:

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

5.When using the Field Extractor (FX), which of the following delimiters will work? (Choose all that apply.)

- A. Tabs
- B. Pipes
- C. Colons
- D. Spaces

Answer: BD

Explanation:

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