

# ***KillTest***

Higher Quality, Better Service!



## **Q&A**

<http://www.killtest.com>

We offer free update service for one year.

**Exam : SPLK-1002**

**Title : Splunk Core Certified Power  
User**

**Version : DEMO**

1.Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event\_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

**Answer:** C,D

2.What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

- A. Creates a table of the total count of users and split by corndogs.
- B. Creates a table of the total count of mysterymeat corndogs split by user.
- C. Creates a table with the count of all types of corndogs eaten split by user.
- D. Creates a table that groups the total number of users by vegetarian corndogs.

**Answer:** B

3.Which of the following statements describes Search workflow actions?

- A. By default. Search workflow actions will run as a real-time search.
- B. Search workflow actions can be configured as scheduled searches,
- C. The user can define the time range of the search when created the workflow action.
- D. Search workflow actions cannot be configured with a search string that includes the transaction command

**Answer:** C

4.A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode.

Which field name appears in the results?

- A. Both will appear in the All Fields list, but only if the alias is specified in the search.
- B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
- C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
- D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

**Answer:** B

5.Data model are composed of one or more of which of the following datasets? (select all that apply.)

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

**Answer:** A,B,C

**Explanation:**

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