



# SPLK-1002<sup>Q&As</sup>

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.geekcert.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

Which type of visualization shows relationships between discrete values in three dimensions?

- A. Pie chart
- B. Line chart
- C. Bubble chart
- D. Scatter chart

Correct Answer: C

<https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub>

---

### QUESTION 2

Highlighted search terms indicate \_\_\_\_\_ search results in Splunk.

- A. Display as selected fields.
- B. Sorted
- C. Charted based on time
- D. Matching

Correct Answer: D

Highlighted search terms indicate matching search results in Splunk, which means that they show which parts of your events match your search string. For example, if you search for error OR fail, Splunk will highlight error or fail in your events to show which events match your search string. Therefore, option D is correct, while options A, B and C are incorrect because they are not indicated by highlighted search terms.

---

### QUESTION 3

Which of the following are required to create a POST workflow action?

- A. Label, URI, search string.
- B. XML attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Correct Answer: C

POST workflow actions are custom actions that send a POST request to a web server when you click on a field value in your search results. POST workflow actions can be configured with various options, such as label name, base URL, URI



parameters, post arguments, app context, etc. One of the options that are required to create a POST workflow action is post arguments. Post arguments are key-value pairs that are sent in the body of the POST request to provide additional information to the web server. Post arguments can include field values from your data by using dollar signs around the field names.

#### QUESTION 4

A user runs the following search:

```
index--X sourcetype=Y | chart count (domain) as count, sum (price) as sum by product, action usenull=f useother--f
```

Which of the following table headers match the order this command creates?

- A. The chart command does not allow for multiple statistical functions.
- B. Product, sum: addtocart, sum: remove, sum: purchase, count: addtocart, count: remove, count: purchase
- C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase
- D. Count: product, sum: product, count: action, sum: action

Correct Answer: C

The correct answer is C. Product, count: addtocart, count: remove, count: purchase, sum:

addtocart, sum: remove, sum: purchase1.

In Splunk, the chart command is used to create a table or a chart visualization from your data2. The chart command takes at least one function and one field, and optionally another field to group by2. In the given search, the chart command is

used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action). The usenull=f and useother=f options are used to exclude null values and other values from the chart2. The chart

command creates a table with headers that match the order of the fields and functions in the command1. The headers for the count function are prefixed with count:, and the headers for the sum function are prefixed with sum:1. The values of

the product and action fields are used as the suffixes for the headers1. Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, and sum: purchase1.

#### QUESTION 5

A data model consists of which three types of datasets?

- A. Constraint, field, value.
- B. Events, searches, transactions.
- C. Field extraction, regex, delimited.
- D. Transaction, session ID, metadata.



Correct Answer: B

The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole. Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

<https://docs.splunk.com/Splexicon:Datamodeldataset>

[Latest SPLK-1002 Dumps](#)

[SPLK-1002 Practice Test](#)

[SPLK-1002 Braindumps](#)