

# 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.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

Which of the following about reports is/are true?

- A. Reports are knowledge objects.
- B. Reports can be scheduled.
- C. Reports can run a script.
- D. All of the above.

Correct Answer: D

Explanation: A report is a way to save a search and its results in a format that you can reuse and share with others. A report is also a type of knowledge object, which is an entity that you create to add knowledge to your data and make it easier to search and analyze. Therefore, option A is correct. A report can be scheduled, which means that you can configure it to run at regular intervals and send the results to yourself or others via email or other methods. Therefore, option B is correct. A report can run a script, which means that you can specify a script file to execute when the report runs and use it to perform custom actions or integrations. Therefore, option C is correct. Therefore, option D is correct because all of the above statements are true for reports.

---

### QUESTION 2

Which of the following is NOT a stats function:

- A. sum
- B. addtotals
- C. count
- D. avg

Correct Answer: B

Explanation: The stats command is used to calculate summary statistics for your search results such as count, sum, avg, min, max and more. The stats command supports various functions that you can use to perform calculations on your fields. However, addtotals is not a stats function but a separate command that adds a row or column with the total of the values in each group. Therefore, option B is correct, while options A, C and D are incorrect because they are valid stats functions.

---

### QUESTION 3

Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

- A. Access
- B. Accounting

C. Authorization

D. Authentication

Correct Answer: D

---

#### QUESTION 4

Which of these search strings is NOT valid:

A. index=web status=50\* | chart count over host, status

B. index=web status=50\* | chart count over host by status

C. index=web status=50\* | chart count by host, status

Correct Answer: A

Explanation: This search string is not valid: index=web status=50\* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

---

#### QUESTION 5

When using a field value variable with a Workflow Action, which punctuation mark will escape the data

A. \*

B. !

C. ^

D. #

Correct Answer: B

Explanation: When using a field value variable with a Workflow Action, the exclamation mark (!) will escape the data. A Workflow Action is a custom action that performs a task when you click on a field value in your search results. A Workflow Action can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. A field value variable is a placeholder for the field value that will be used to replace the variable in the URL or post argument of the Workflow Action. A field value variable is written as fieldname, where field\_name is the name of the field whose value will be used. However, if the field value contains special characters that need to be escaped, such as spaces, commas, etc., you can use the exclamation mark (!) before and after the field value variable to escape the data. For example, if you have a field value variable host, you can write it as !\$host! to escape any special characters in the host field value. Therefore, option B is the correct answer.