



# 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.passapply.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

What is the correct format for naming a macro with multiple arguments?

- A. `monthly_sales(argument 1, argument 2, argument 3)`
- B. `monthly_sales(3)`
- C. `monthly_sales[3]`
- D. `monthly_sales[argument 1, argument 2, argument 3]`

Correct Answer: C

Explanation: The correct format for naming a macro with multiple arguments is `monthly_sales3`. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as `monthly_sales[region,salesperson,date]`.

---

### QUESTION 2

Which of the following eval command function is valid?

- A. `Int ()`
- B. `Count ()`
- C. `Print ()`
- D. `Tostring ()`

Correct Answer: D

Explanation: The eval command supports a number of functions that you can use in your expressions to perform calculations, conversions, string manipulations and more<sup>2</sup>. One of the eval command functions is `tostring()`, which converts a numeric value to a string value<sup>2</sup>. Therefore, option D is correct, while options A, B and C are incorrect because they are not valid eval command functions.

---

### QUESTION 3

When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

- A. OR
- B. ( )
- C. AND
- D. NOT

Correct Answer: ABD



Explanation: When you mouse over and click to add a search term from the Fields sidebar or from an event in your search results, Splunk automatically adds the term to your search string with an implied AND operator<sup>2</sup>. However, this does not apply to some Boolean operators such as OR, NOT and parentheses (). These operators are not implied when you add a search term and you have to type them manually if you want to use them in your search string<sup>2</sup>. Therefore, options A, B and D are correct, while option C is incorrect because AND is implied when you add a search term.

---

#### QUESTION 4

When using | timchart by host, which field is represented in the x-axis?

- A. date
- B. host
- C. time
- D. -time

Correct Answer: A

---

#### QUESTION 5

Which of the following is a function of the Splunk Common Information Model (CIM)?

- A. Normalizing data across a Splunk deployment.
- B. Providing templates for reports and dashboards.
- C. Algorithmically shifting events to other indexes.
- D. Reingesting previously indexed data with new field names.

Correct Answer: A

[Latest SPLK-1002 Dumps](#)

[SPLK-1002 VCE Dumps](#)

[SPLK-1002 Exam Questions](#)