

# Demo Questions

## SPLUNK SPLK-1002 Exam

Splunk Core Certified Power User

Thank you for downloading **SPLK-1002** Exam PDF

### Question #1 Topic 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.

**Correct Answer:** C

Reference:

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

### Question #2 Topic 1

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.

**Correct Answer:** A

### Question #3 Topic 1

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.

**Correct Answer: A**

### Question #4 Topic 1

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

**Correct Answer: ABC**

Reference:

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

### Question #5 Topic 1

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

**Correct Answer: D**

Reference:

<https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot>