



# SPLK-1001<sup>Q&As</sup>

Splunk Core Certified User

## Pass Splunk SPLK-1001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/splk-1001.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

Universal forwarder is recommended for forwarding the logs to indexers.

- A. False
- B. True

Correct Answer: B

---

### QUESTION 2

How can another user gain access to a saved report?

- A. The owner of the report can edit permissions from the Edit dropdown
- B. Only users with an Admin or Power User role can access other users\' reports
- C. Anyone can access any reports marked as public within a shared Splunk deployment
- D. The owner of the report must clone the original report and save it to their user account

Correct Answer: A

---

### QUESTION 3

Which of the following is a best practice when writing a search string?

- A. Include all formatting commands before any search terms
- B. Include at least one function as this is a search requirement
- C. Include the search terms at the beginning of the search string
- D. Avoid using formatting clauses as they add too much overhead

Correct Answer: C

A best practice when writing a search string is to include the search terms at the beginning of the search string. This helps Splunk narrow down the events that match your search criteria and improve the search performance. Formatting commands and functions can be added later in the search pipeline to manipulate and display the results. References: Splunk Core User Certification Exam Study Guide, page 13.

---

### QUESTION 4

What is the primary use for the rare command?

- A. To sort field values in descending order



- B. To return only fields containing five or fewer values
- C. To find the least common values of a field in a dataset
- D. To find the fields with the fewest number of values across a dataset

Correct Answer: C

---

#### QUESTION 5

When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?

- A. |
- B. \$
- C. !
- D. ,

Correct Answer: D

[SPLK-1001 PDF Dumps](#)

[SPLK-1001 Study Guide](#)

[SPLK-1001 Exam  
Questions](#)