



SPLK-1004^{Q&As}

Splunk Core Certified Advanced Power User





Pass Splunk SPLK-1004 Exam with 100% Guarantee

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

<https://www.geekcert.com/splk-1004.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 stats function is used to return a sorted list of unique field values?

- A. values
- B. sum
- C. count
- D. list

Correct Answer: A

The values function in the stats command in Splunk is used to return a sorted list of unique field values (Option A). This function is particularly useful for summarizing data by listing all unique values of a specified field across the events returned by the search, which can provide insights into the diversity and distribution of the data associated with that field.

QUESTION 2

When possible, what is the best choice for summarizing data to improve search performance?

- A. Use the fieldsummary command.
- B. Data model acceleration
- C. Report acceleration
- D. Summary indexing

Correct Answer: D

QUESTION 3

What qualifies a report for acceleration?

- A. Fewer than 100k events in search results, with transforming commands used in the search string.
- B. More than 100k events in search results, with only a search command in the search string.
- C. More than 100k events in the search results, with a search and transforming command used in the search string.
- D. fewer than 100k events in search results, with only a search and transaction command used in the search string.

Correct Answer: A

A report qualifies for acceleration in Splunk if it involves fewer than 100,000 events in the search results and uses transforming commands in the search string (Option A). Transforming commands aggregate data, making it more suitable for acceleration by reducing the dataset's complexity and size, which in turn improves the speed and efficiency of report generation.



QUESTION 4

What is the value of base lisp in the Search Job Inspector for the search index-sales clientip-170.192.178.10?

- A. [index::sales 192 AND 10 AMD 178 AND 170]
- B. [index::sales AND 469 10 702 390]
- C. [192 AND 10 AND 178 AND 170 Index::sales]
- D. [AND 10 170 178 192 Index::sales]

Correct Answer: A

QUESTION 5

Which statement about the coalesce function is accurate?

- A. It can take only a single argument.
- B. It can take a maximum of two arguments.
- C. It can be used to create a new field in the results set.
- D. It can return null or non-null values.

Correct Answer: C

The coalesce function in Splunk is used to evaluate each argument in order and return the first non-null value. This function can be used within an eval expression to create a new field in the results set, which will contain the first non-null value from the list of fields provided as arguments to coalesce. This makes it particularly useful in situations where data may be missing or inconsistently populated across multiple fields, as it allows for a fallback mechanism to ensure that some value is always presented.

[SPLK-1004 VCE Dumps](#)

[SPLK-1004 Practice Test](#)

[SPLK-1004 Brindumps](#)