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

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 2

What does using the tstats command with summariesonly=false do?

A. Returns results from only non-summarized data.

B. Returns results from both summarized and non-summarized data.

C. Prevents use of wildcard characters in aggregate functions.

D. Returns no results.

Correct Answer: B

Using the tstats command with summariesonly=false instructs Splunk to return results from both summarized (accelerated) data and non-summarized (raw) data. This can be useful when you need a comprehensive view of the data that includes both the high-performance summaries provided by data model acceleration and the detailed granularity of raw data.

QUESTION 3

What is a performance improvement technique unique to dashboards?

A. Using stats instead of transaction

B. Using global searches

C. Using report acceleration

D. Using datamodel acceleration

Correct Answer: C

Using report acceleration (Option C) is a performance improvement technique unique to dashboards in Splunk. Report acceleration involves pre-computing the results of a report (which can be a saved search or a dashboard panel) and storing these results in a summary index, allowing dashboards to load faster by retrieving the pre-computed data instead of running the full search each time. This technique is especially useful for dashboards that rely on complex searches or searches over large datasets.

QUESTION 4

Repeating JSON data structures within one event will be extracted as what type of fields?

A. Single value

B. Lexicographical

C. Multivalue

D. Mvindex

Correct Answer: C

Repeating JSON data structures within a single event in Splunk are extracted as multivalue fields (Option C). Multivalue fields allow a single field to contain multiple distinct values, which is common with JSON data structures that include arrays or repeated elements. Splunk\\'s field extraction capabilities automatically recognize and parse these structures, allowing users to work with each value within the multivalue field for analysis and reporting

QUESTION 5

Where does the output of an append command appear in the search results?

A. Added as a column to the right of the search results.

B. Added as a column to the left of the search results.

C. Added to the beginning of the search results.

D. Added to the end of the search results.

Correct Answer: D

The output of an append command in Splunk search results is added to the end of the search results (Option D). The append command is used to concatenate the results of a subsearch to the end of the current search results, effectively extending the result set with additional data. This can be particularly useful for combining related datasets or adding contextual information to the existing search results.