SPLK-1004Q&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.pass4itsure.com/splk-1004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Which statement about tsidx files is accurate?

A. Splunk updates tsidx files every 30 minutes.

B. Splunk removes outdated tsidx files every 5 minutes.

C. A tsidx file consists of a lexicon and a posting list.

D. Each bucket in each index may contain only one tsidx file.

Correct Answer: C

A tsidx file in Splunk is an index file that contains indexed data, and it consists of two main parts: alexicon and a posting list (Option C). The lexicon is a list of unique terms found in the data, and the posting list is a list of references to the occurrences of these terms in the indexed data. This structure allows Splunk to efficiently search and retrieve data based on search terms.

QUESTION 2

Which of the following Is valid syntax for the split function?

A. ...| eval split phoneNUmber by "_" as areaCodes.

B. ...| eval areaCodes = split (phonNumber, "_"

C. ...| eval phoneNumber split("-", 3, areaCodes)

D. ...| eval split (phone-Number, "_", areaCodes)

Correct Answer: B

The valid syntax for using the split function in Splunk is ... | eval areaCodes = split(phoneNumber, "_") (Option B). The split function divides a string into an array of substrings based on a specified delimiter, in this case, an underscore. The resulting array is stored in the new field areaCodes.

QUESTION 3

Which commands should be used in place of a subsearch if possible?

A. untable and/or xyseries

B. stats and/or eval

C. mvexpand and/or where

D. bin and/or where

Correct Answer: B

Using stats and/or eval commands in place of a subsearch is often recommended for performance optimization in Splunk searches. Subsearches can be resource-intensive and slow, especially when dealing with large datasets or complex search operations. The stats command is versatile and can be used for aggregation, summarization, and calculation of data, often achieving the same goals as a subsearch but more efficiently. The eval command is used for field calculations and conditional evaluations, allowing for the manipulation of search results without the need for a subsearch. These commands, when used effectively, can reduce the processing load and improve the speed of searches.

QUESTION 4

which function of the stats command creates a multivalue entry?

A. mvcombine

B. eval

C. makemv

D. list

Correct Answer: D

QUESTION 5

When would a distributable streaming command be executed on an Indexer?

A. If any of the preceding search commands are executed on the search head.

B. If all preceding search commands are executed on me indexer, and a streamstats command is used.

C. If all preceding search commands are executed on the Indexer.

D. If some of the preceding search commands are executed on the indexer, and a Timerchart command is used.

Correct Answer: C

A distributable streaming command would be executed on an indexer if all preceding search commands are executed on the indexer (Option C). Distributable streaming commands are designed to be executed where the data resides, reducing data transfer across the network and leveraging the processing capabilities of indexers. This enhances the overall efficiency and performance of Splunk searches, especially in distributed environments.