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

QUESTION 1

Which commands can run on both search heads and indexers?

A. Transforming commands

B. Centralized streaming commands

C. Dataset processing commands

D. Distributable streaming commands

Correct Answer: D

Distributable streaming commands in Splunk can run on both search heads and indexers (Option D). These commands operate on each event independently and can be distributed across indexers for parallel execution, which enhances search efficiency and scalability. This category includes commands like search, where, eval, and many others that do not require the entire dataset to be available to produce their output.

QUESTION 2

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 3

How can the erex and rex commands be used in conjunction to extract fields?

A. The regex Generated by the erex command can be edited and used with the regex command in a subsequent search.

B. The regex generated by the rex command can be edited and used with the erex command in a subsequent search.

C. The regex generated by the erex command can be edited and used with the erex command in a subsequent search.

D. The erex and rex commands cannot be used in conjunction under any circumstances.

Correct Answer: A

The erex command in Splunk is used to generate regular expressions based on example data, and these generated regular expressions can then be edited and utilized with the rex command in subsequent searches (Option A). The erex command is helpful for users who may not be familiar with regular expression syntax, as it provides a starting point that can be refined and customized with rex for more precise field extraction.

QUESTION 4

What default Splunk role can use the Log Event alert action?

A. Power

B. User

C. can_delete

D. Admin

Correct Answer: D

In Splunk, the Admin role (Option D) has the capability to use the Log Event alert action among many other administrative privileges. The Log Event alert action allows Splunk to create an event in an index based on the triggering of an alert, providing a way to log and track alert occurrences over time. The Admin role typically encompasses a wide range of permissions, including the ability to configure and manage alert actions.

QUESTION 5

Which of these generates a summary index containing a count of events by productId?

A. | stats count by productId

B. | stats sum (productId)

C. | sistats count by productId

D. sistats summary_index by productid

Correct Answer: A

To generate a summary index containing a count of events by productId, the correct search command would be | stats count by productId (Option A). This command aggregates the events by productId, counting the number of events for each unique productId value. The stats command is a fundamental Splunk command used for aggregation and summarization, making it suitable for creating summary data like counts by specific fields.