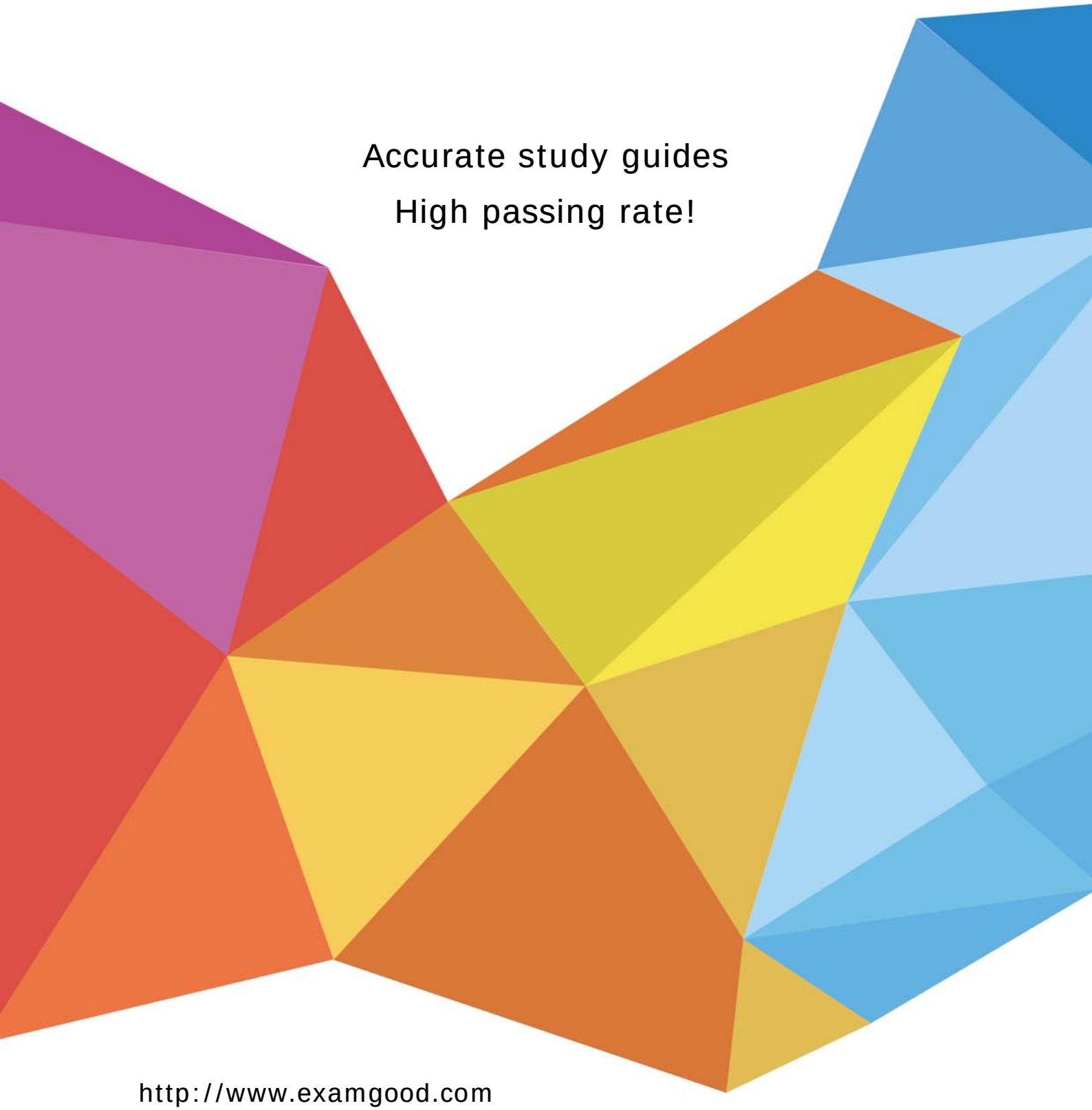
EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!



Accurate study guides

High passing rate!

Exam : **SPLK-1004**

Title : Splunk Core Certified Advanced Power User Exam

Version : DEMO

1.If a search contains a subsearch, what is the order of execution?
A. The order of execution depends on whether either search uses a stats command.
B. The inner search executes first.
C. The otter search executes first.
D. The two searches are executed in parallel.
Answer: B
Explanation:
In a Splunk search containing a subsearch, the inner subsearch executes first (Option B). The result of the subsearch is then passed to the outer search. This is because the outer search often depends on the results of the inner subsearch to complete its execution. For example, a subsearch might be used to identify a list of relevant terms or values which are then used by the outer search to filter or manipulate the main dataset.

2.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.
Answer: A
Explanation:
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.

3.What command is used la compute find write summary statistic, to a new field in the event results?
A. tstats
B. stats
C. eventstats
D. transaction
Answer: C
Explanation:
The eventstats command in Splunk is used to compute and add summary statistics to all events in the search results, similar to the stats command, but without grouping the results into a single event (Option C). This command adds the computed summary statistics as new fields to each event, allowing those fields to be used in subsequent search operations or for display purposes. Unlike the transaction command, which groups events into transactions, eventstats retains individual events while enriching them with statistical information.

4.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
Answer: D
Explanation:
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.

5.What is returned when Splunk finds fewer than the minimum matches for each lookup value?
A. The default value NULL until the minimum match threshold is reached.
B. The default match value until the minimum match threshold Is reached.
C. The first match unless the time_field attribute is specified.
D. Only the first match.
Answer: A
Explanation:
When Splunk's lookup feature finds fewer than the minimum matches specified for each lookup value, it returns the default value NULL for those unmatched entries until the minimum match threshold is reached (Option A). This behavior ensures that lookups return consistent and expected results, even when the available data does not meet the specified criteria for a minimum number of matches.