Splunk

SPLK-1004 Exam

Splunk Core Certified Advanced Power User

[Questions & Answers Demo]

Version: 4.1

Question: 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 outer 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. The result of the subsearch is then passed to the outer search, which often depends on the results of the inner subsearch to complete its execution.

Question: 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 rex 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 generates regular expressions based on example data. These generated regular expressions can then be edited and utilized with the rex command in subsequent searches.

Question: 3

What command is used to compute and write summary statistics 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 stats, but without grouping the results into a single event.

Question: 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 operate on each event independently and can be distributed across indexers for parallel execution, improving search efficiency and scalability.

Question: 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 for each lookup value, it returns the default value NULL for unmatched entries until the minimum match threshold is reached.