Welcome to Cert007 - Your Ultimate IT Certification Partner

- Real Exam Questions
- Free Updates
- Expert Support
- Instant Access
- Money-Back Guarantee

Visit us at **https://www.cert007.com/** for more information

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 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.
Reference: Splunk Documentation on Subsearches:
https://docs.splunk.com/Documentation/Splunk/latest/Search/Aboutsubsearches
Splunk Documentation on Search Syntax:
https://docs.splunk.com/Documentation/Splunk/latest/Search/Usefieldsinsearches

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.

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.

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:
In Splunk's processing model, commands are categorized based on how and where they execute within the search pipeline. Understanding these categories is crucial for optimizing search performance.
Distributable Streaming Commands:
Definition: These commands operate on each event individually and do not depend on the context of other events. Because of this independence, they can be executed on indexers, allowing the processing load to be distributed across multiple nodes.
Execution: When a search is run, distributable streaming commands can process events as they are retrieved from the indexers, reducing the amount of data sent to the search head and improving efficiency.
Examples: eval, rex, fields, rename
Other Command Types:
Dataset Processing Commands: These commands work on entire datasets and often require all events to be available before processing can begin. They typically run on the search head. Centralized Streaming Commands: These commands also operate on each event but require a centralized view of the data, meaning they usually run on the search head after data has been gathered from the indexers.
Transforming Commands: These commands, such as stats or chart, transform event data into statistical tables and generally run on the search head.
By leveraging distributable streaming commands, Splunk can efficiently process data closer to its source, optimizing resource utilization and search performance.
Reference: Splunk Documentation: Types of commands

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.