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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

When running a search, which Splunk component retrieves the individual results?

A. Indexer

B. Search head

C. Universal forwarder

D. Master node

Correct Answer: B

The Search head (Option B) in Splunk architecture is responsible for initiating and coordinating search activities across a distributed environment. When a search is run, the search head parses the search query, distributes the search tasks to the appropriate indexers (which hold the actual data), and then consolidates the results retrieved by the indexers. The search head is the component that interacts with the user, presenting the final search results

QUESTION 2

What does the query | makeresults generate?

A. A timestamp

B. A results field

C. An error message

D. The results of the previously run search.

Correct Answer: B

The | makeresults command in Splunk generates a single event containing default fields, with theprimary purpose of creating sample data or a placeholder event for testing and development purposes. The most notable field it generates is _time, but it does not create a specific \\'results\\' field per se. However, it\\'s commonly used to create a base event for further manipulation with eval or other commands in search queries for demonstration, testing, or constructing specific scenarios.

QUESTION 3

If a nested macro expands to a search string that begins with a generating command, what additional syntax is needed?

A. Double tick marks around the nested macro.

B. A comma before the nested macro.

C. Square brackets around the nested macro.

D. A pipe character before the nested macro.

Correct Answer: C

When a nested macro in Splunk expands to a search string that begins with a generating command, square brackets (Option C) are needed around the nested macro. This syntax ensures that the expanded macro is correctly interpreted as part of the overall search command structure. Generating commands in Splunk are those that can start a search pipeline and do not require input from a preceding command, such as search, inputlookup, and datamodel. Encapsulating the nested macro in square brackets allows Splunk to process it as an independent subsearch or command within the larger search query. The other options, including double tick marks, a comma, and a pipe character, do not provide the correct syntax for this purpose.

QUESTION 4

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.

QUESTION 5

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

Correct Answer: C

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.