Vendor: Splunk

Exam Code:SPLK-1004

Exam Name: Splunk Core Certified Advanced Power User

Version: Demo

QUESTION 1

What does using the tstats command with summariesonly=false do?

A. Returns results from only non-summarized data.

B. Returns results from both summarized and non-summarized data.

C. Prevents use of wildcard characters in aggregate functions.

D. Returns no results.

Correct Answer: B

Using the tstats command with summariesonly=false instructs Splunk to return results from both summarized (accelerated) data and non-summarized (raw) data. This can be useful when you need a comprehensive view of the data that includes both the high-performance summaries provided by data model acceleration and the detailed granularity of raw data.

QUESTION 2

What order of incoming events must be supplied to the transaction command to ensure correct results?

A. Reverse lexicographical order

B. Ascending lexicographical order

C. Ascending chronological order

D. Reverse chronological order

Correct Answer: C

The transaction command in Splunk groups events into transactions based on common fields or characteristics. For the transaction command to function correctly and group events into meaningful transactions, the incoming events must be supplied in ascending chronological order (Option C). This ensures that related events are sequenced correctly according to their occurrence over time, allowing for accurate transaction grouping and analysis

---

QUESTION 3

Which of the following is an event handler action?

A. Run an eval statement based on a user clicking a value on a form.

B. Set a token to select a value from the time range picker.

C. Pass a token from a drilldown to modify index settings.

D. Cancel all jobs based on the number of search job results captured.

Correct Answer: A

An event handler action in Splunk is an action that is triggered based on user interaction with dashboard elements. Running an eval statement based on a user clicking a value on a form (Option A) is an example of an event handler action. This capability allows dashboards to be interactive and dynamic, responding to user inputs or actions to modify displayed data, visuals, or other elements in real-time.

QUESTION 4

Which command processes a template for a set of related fields?

A. bin

B. xyseries

C. foreach

D. untable

Correct Answer: C

The foreach command in Splunk is used to apply a processing step to each field in a set of related fields, making it ideal for performing repetitive tasks across multiple fields without having to specify each field individually. This command can process a template of commands or functions to apply to each specified field, thereby streamlining operations that need to be applied uniformly across multiple data points.

QUESTION 5

Which of the following functions\\' primary purpose is to convert epoch time to a string format?

A. tostring

B. strptime

C. tonumber

D. strftime

Correct Answer: D

The strftime function in Splunk is used to convert epoch time (also known as POSIX time or Unix time, which is a system for describing points in time as the number of seconds elapsed since January 1, 1970) into a human-readable string format. This function is particularly useful when formatting timestamps in search results or when creating more readable time representations in dashboards and reports. The strftime function takes an epoch time value and a format string asarguments and returns the formatted time as a string according to the specified format. The other options (tostring, strptime, and tonumber) serve different purposes: tostring converts values to strings, strptime converts string representations of time into epoch format, and tonumber converts values to numbers.

QUESTION 6

Where does the output of an append command appear in the search results?

A. Added as a column to the right of the search results.

B. Added as a column to the left of the search results.

C. Added to the beginning of the search results.

D. Added to the end of the search results.

Correct Answer: D

The output of an append command in Splunk search results is added to the end of the search results (Option D). The append command is used to concatenate the results of a subsearch to the end of the current search results, effectively extending the result set with additional data. This can be particularly useful for combining related datasets or adding contextual information to the existing search results.

QUESTION 7

How can form inputs impact dashboard panels using inline searches?

A. Panels powered by an inline search require a minimum of one form input.

B. Form inputs can not impact panels using inline searches.

C. Adding a form input to a dashboard converts all panels to prebuilt panels.

D. A token in a search can be replaced by a form input value.

Correct Answer: D

Form inputs in Splunk dashboards can dynamically impact the panels using inline searches by allowing a token in the search to be replaced by a form input value (Option D). This capability enables dashboard panels to update their content based on user interaction with the form elements. When a user makes a selection or enters data into a form input, the corresponding token in the search string of a dashboard panel is replaced with this value, effectively customizing the search based on user input. This feature makes dashboards more interactive and adaptable to different user needs or questions.

QUESTION 8

What type of drilldown passes a value from a user click into another dashboard or external page?

A. Visualization

B. Event

C. Dynamic

D. Contextual

Correct Answer: D

Contextual drilldown (Option D) is the type of drilldown that allows passing a value from a user click (e.g., from a table row or chart element) into another dashboard or an external page. This feature enables the creation of interactive dashboards where clicking on a specific element dynamically updates another part of the dashboard or navigates to a different page with relevant information, using the clicked value as a context for the subsequent view.

QUESTION 9

When possible, what is the best choice for summarizing data to improve search performance?

A. Us the fieldsummary command.

B. Data model acceleration

C. Report acceleration

D. Summary indexing

Correct Answer: D

QUESTION 10

What is the value of base lispy in the Search Job Inspector for the search index-sales clientip-170.192.178.10?

A. [index::sales 192 AND 10 AMD 178 AND 170]

B. [index::sales AND 469 10 702 390]

C. [192 AND 10 AND 178 AND 170 Index::sales]

D. [AND 10 170 178 192 Index::sales]

Correct Answer: A

QUESTION 11

How can a lookup be referenced in an alert?

A. Use the lookup dropdown in the alert configuration window.

B. Follow a lookup with an alert command in the search bar.

C. Run a search that uses a lookup and save as an alert.

D. Upload a lookup file directly to the alert.

Correct Answer: C

To reference a lookup in an alert in Splunk, you would run a search that uses a lookup and then save that search as an alert (Option C). This method integrates the lookup within the search logic, and when the search conditions meet the alert\\'s trigger conditions, the alert is activated. This approach allows the alert to leverage the enriched data provided by the lookup for more accurate and informative alerting.

QUESTION 12

Which of the following statements is accurate regarding the append command?

A. It is used with a subsearch and only accesses real-lime searches.

B. It is used with a subsearch and oily accesses historical data.

C. It cannot be used with a subsearch and only accesses historical data.

D. It cannot be used with a subsearch and only accesses real-time searches.

Correct Answer: B

The append command in Splunk is often used with a subsearch to add additional data to the end of the primary search results, and it can access historical data (Option B). This capability is useful for combining datasets from different time ranges or sources, enriching the primary search results with supplementary information.