Free Questions for SPLK-1004 by certsinside

Shared by Mcclure on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is accurate about cascading inputs?

Options:

A- They can be reset by an event handler.

B- The final input has no impact on previous inputs.

C- Only the final input of the sequence can supply a token to searches.

D- Inputs added to panels can not participate.

Answer:

A

Explanation:

Cascading inputs in Splunk dashboards allow the selection in one input (like a dropdown, radio button, etc.) to determine the available options in the subsequent input, creating a dependent relationship between them. An event handler can be configured to reset subsequent inputs based on the selection made in a preceding input (Option A), ensuring that only relevant options are presented to the

user as they make selections. This approach enhances the dashboard's usability by guiding the user through a logical flow of choices, where each selection refines the scope of the following options.

Question 2

Question Type: MultipleChoice

Which of the following fields are provided by the fieldsummary command? (select all that apply)

Options:

A- count

B- stdev

C- mean

D- dc

Answer:

A, D

Explanation:

The fieldsummary command in Splunk generates statistical summaries of fields in the search results, including the count of events that contain the field (count) and the distinct count of field values (dc). These summaries provide insights into the prevalence and distribution of fields within the dataset, which can be valuable for understanding the data's structure and content. Standard deviation (stdev) and mean (mean) are not directly provided by fieldsummary but can be calculated using other commands like stats for fields that contain numerical data.

Question 3

Question Type: MultipleChoice

Which of the following is an event handler action?

Options:

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.

Answer:

A

Explanation:

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

Question Type: MultipleChoice

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

Options:

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.

Answer:

B

Explanation:

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 5

Question Type: MultipleChoice

Which is a regex best practice?

Options:

A- Use complex expressions rather than simple ones.

B- Avoid backtracking.

C- Use greedy operators (. *) instead of non-greedy operators (. *?).

D- Use * rather than +.

Answer:

B

Explanation:

In regex (regular expressions), one of the best practices is to avoid backtracking when possible. Backtracking occurs when the regex engine revisits previous parts of the input string to attempt different permutations of the pattern, which can significantly degrade performance, especially with complex patterns on large inputs. Designing regex patterns to minimize or avoid backtracking can lead to more efficient and faster evaluations.

Question 6

Question Type: MultipleChoice

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

Options:

A- bin

B- xyseries

C- foreach

D- untable

Answer:

C

Explanation:

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 7

Question Type: MultipleChoice

Which statement about the coalesce function is accurate?

Options:

A- It can take only a single argument.

B- It can take a maximum of two arguments.

C- It can be used to create a new field in the results set.

D- It can return null or non-null values.

Answer:

C

Explanation:

The coalesce function in Splunk is used to evaluate each argument in order and return the first non-null value. This function can be used within an eval expression to create a new field in the results set, which will contain the first non-null value from the list of fields provided as arguments to coalesce. This makes it particularly useful in situations where data may be missing or inconsistently populated across

multiple fields, as it allows for a fallback mechanism to ensure that some value is always presented.

Question 8

Question Type: MultipleChoice

Which predefined drilldown token passes a clicked value from a table row?

Options:

A- $rowclick. <fieldname>$

B- $tableclick .< fieldname>$

C- $row. <fieldname>$

D- $table .< fieldname>$

Answer:

A

Explanation:

The predefined drilldown token that passes a clicked value from a table row in Splunk dashboards is $row.<fieldname>$ (Option A). This token syntax is used within the drilldown configuration of a dashboard panel to capture the value of a specific field from a row where the user clicks. This value can then be passed to another dashboard panel or used within the same panel to dynamically update the content based on the user's interaction, enhancing the interactivity and relevance of dashboard data presentations.