SPLK-1004$^{\text{Q\&As}}$

Splunk Core Certified Advanced Power User

QUESTION 1

What is the correct hierarchy of XML elements in a dashboard panel?

A.

B.

C.

D.

Correct Answer: B

In a Splunk dashboard, the correct hierarchy of XML elements for a dashboard panel is (Option B). A Splunk dashboard is defined within the element. Within this, elements are used to organize the layout into rows, and each element within a row defines an individual panel that can contain visualizations, searches, or other content. This hierarchical structure allows for organized and customizable layouts of dashboard elements, facilitating clear presentation of data and analyses. The other options provided do not represent the correct hierarchical order for defining dashboard panels in Splunk\\'s XML dashboard syntax.

QUESTION 2

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 3

Which search generates a field with a value of "hello"?

A. | Makeresults field-`\\'hello\\'\\'

B. | Makeresults | fields`\\'hello\\'\\'

C. | Makeresults | eval field-`\\'hello\\'\\'

D. | Makeresults | eval field =make{\\'\\'hello\\'\\'}

Correct Answer: C

To generate a field with a value of "hello" using the makeresults command in Splunk, the correct syntax is | makeresults | eval field="hello" (Option C). The makeresults command creates a single event, and the eval command is used to add a new field (named "field" in this case) with the specified value ("hello"). This is a common method for creating sample data or for demonstration purposes within Splunk searches.

QUESTION 4

Assuming a standard time zone across the environment, what syntax will always return ewnts from between 2:00am and 5:00am?

A. datehour>-2 AND date_hour-2 AND time_hour>-5

D. earliest=2h@ AND latest=5h3h

Correct Answer: B

To always return events from between 2:00 AM and 5:00 AM, assuming a standard time zone across the environment, the correct Splunk search syntax is earliest=-2h@h AND latest=-5h@h (Option B). This syntax uses relative time modifiers to specify a range starting 2 hours ago from the current hour (-2h@h) and ending 5 hours ago from the current hour (-5h@h), effectively capturing the desired time window.

QUESTION 5

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 6

When using a nested search macro, how can an argument value be passed to the inner macro?

A. The argument value may be passed to the outer macro.

B. An argument cannot be used with an inner nested macro.

C. An argument cannot be used with an outer nested macro.

D. The argument value must be specified in the outer macro.

Correct Answer: A

When using a nested search macro in Splunk, an argument value can be passed to the inner macro by specifying the argument in the outer macro\\'s invocation (Option A). This allows the outer macro to accept arguments from the user or another search command and then pass those arguments into the inner macro, enabling dynamic and flexible macro compositions that can adapt based on input parameters.

QUESTION 7

Which of the following is accurate regarding predefined drilldown tokens?

A. They capture data from a form Input.

B. They vary by visualization type

C. There are eight categories of predefined drilldown tokens.

D. They are defined by a panel\\'s base search.

Correct Answer: B

Predefined drilldown tokens in Splunk vary by visualization type (Option B). These tokens are placeholders that capture dynamic values based on user interactions with dashboard elements, such as clicking on a chart segment or table row. The specific tokens available and their meanings can differ depending on the type of visualization, as each visualization type may present and interact with data differently.

QUESTION 8

Which of the following is not a common default time field?

A. date_zone

B. date minute

C. date_year

D. date_day

Correct Answer: A

In Splunk, common default time fields include date_minute, date_year, and date_day, which represent the minute, year, and day parts of event timestamps, respectively. date_zone (Option A) is not recognized as a common default time field in Splunk. The platform typically uses fields like _time and various date_* fields for time-related information but does not use date_zone as a standard time field.

QUESTION 9

What is an example of the simple XML syntax for a base search and its post-srooess search?

A. ,

B. ,

C. ,

D. ,

Correct Answer: A

QUESTION 10

A report named "Linux logins" populates a summary index with the search string sourcetype=linux_secure| sitop src_ip user. Which of the following correctly searches against the summary index for this data?

A. index=summary sourcetype="linux_secure" | top src_ip user

B. index=summary search_name="Linux logins" | top src_ip user

C. index=summary search_name="Linux logins" | stats count by src_ip user

D. index=summary sourcetype="linux_secure" | stats count by src_ip user

Correct Answer: B

When searching against summary data in Splunk, it\\'s common to reference the name of the saved search or report that populated the summary index. The correct search syntax to retrieve data from the summary index populated by a report named "Linux logins" is index=summary search_name="Linux logins" | top src_ip user (Option B). This syntax uses the search_name field, which holds the name of the saved search or report that generated the summary data, allowing for precise retrieval of the intended summary data.

QUESTION 11

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 12

Why is the transaction command slow in large splunk deployments?

A. It forces the search to run in fast mode.

B. transaction or runs on each Indexer in parallel.

C. It forces all event data to be returned to the search head.

D. transaction runs a hidden eval to format fields.

Correct Answer: C

The transaction command can be slow in large Splunk deployments because it requires all event data relevant to the transaction to be returned to the search head (Option C). This process can be resource-intensive, especially for transactions that span a large volume of data or time, as it involves aggregating and sorting events across potentially many indexers before the transaction logic can be applied.

QUESTION 13

What are the four types of event actions?

A. stats, target, set, and unset

B. stats, target, change, and clear

C. eval, link, change, and clear

D. eval, link, set, and unset

Correct Answer: C

The four types of event actions in Splunk are eval, link, change, and clear (Option C). These actions can be used in dashboard panel configurations to dynamically interact with or manipulate event data based on user inputs or other criteria. Eval is used for calculating fields, link for creating hyperlinks, change for modifying field values, and clear for removing field values or other data elements.

QUESTION 14

what is the result of the xyseries command?

A. To transform single series output into a multi-series output

B. To transform a stats-like output into chart-like output.

C. To transform a multi-series output into single series output.

D. To transform a chart-like output into a stats-like output.

Correct Answer: B

The result of the xyseries command in Splunk is to transform a stats-like output into chart- like output (Option B). The xyseries command restructures the search results so that each row represents a unique combination of x and y values, suitable for plotting in a chart, making it easier to visualize complex relationships between multiple data points.

QUESTION 15

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.