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.leads4pass.com/splk-1004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Which commands should be used in place of a subsearch if possible?

A. untable and/or xyseries

B. stats and/or eval

C. mvexpand and/or where

D. bin and/or where

Correct Answer: B

Using stats and/or eval commands in place of a subsearch is often recommended for performance optimization in Splunk searches. Subsearches can be resource-intensive and slow, especially when dealing with large datasets or complex search operations. The stats command is versatile and can be used for aggregation, summarization, and calculation of data, often achieving the same goals as a subsearch but more efficiently. The eval command is used for field calculations and conditional evaluations, allowing for the manipulation of search results without the need for a subsearch. These commands, when used effectively, can reduce the processing load and improve the speed of searches.

QUESTION 2

Which of the following best describes the process for tokenizing event data?

A. The event Cats is broken up by values in the punch field.

B. The event data is broken up by major breaker and then broken up further by minor breakers.

C. The event data is broken up by a series of user-defined regex patterns.

D. The event data has all punctuation stripped out and is then space delinked.

Correct Answer: B

The process for tokenizing event data in Splunk is best described as breaking the event data up by major breakers and then further breaking it up by minor breakers (Option B). Major breakers typically identify the boundaries of events, while minor breakers further segment the event data intofields. This hierarchical approach to tokenization allows Splunk to efficiently parse and structure the incoming data for analysis.

QUESTION 3

How can the inspect button be disabled on a dashboard panel?

A. Set inspect.link.disabled to 1

B. Set link.inspect .visible to 0

C. Set link.inspectSearch.visible too

D. Set link.search.disabled to 1

Correct Answer: B

To disable the inspect button on a dashboard panel in Splunk, you can set the link.inspect.visible attribute to 0 (Option B) in the panel\\'s source code. This attribute controls the visibility of the inspect button, and setting it to 0 hides the button, preventing users from accessing the search inspector for that panel.

QUESTION 4

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 5

What capability does a power user need to create a Log Event alert action?

A. edit_search_server

B. edit udp

C. edit_tcp

D. edit_alerts

Correct Answer: D

To create a Log Event alert action in Splunk, a power user needs the edit_alerts capability (Option D). This capability allows the user to configure and manage alert actions, including setting up alerts to log specific events based on predefined conditions within Splunk\\'s alerting framework.

QUESTION 6

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 7

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 8

Which of the following Is valid syntax for the split function?

A. ...| eval split phoneNUmber by "_" as areaCodes.

B. ...| eval areaCodes = split (phonNumber, "_"

C. ...| eval phoneNumber split("-", 3, areaCodes)

D. ...| eval split (phone-Number, "_", areaCodes)

Correct Answer: B

The valid syntax for using the split function in Splunk is ... | eval areaCodes = split(phoneNumber, "_") (Option B). The split function divides a string into an array of substrings based on a specified delimiter, in this case, an underscore. The resulting array is stored in the new field areaCodes.

QUESTION 9

What happens to panels with post-processing searches when their base search Is refreshed?

A. The parcels are deleted.

B. The panels are only refreshed If they have also been configured.

C. The panels are refreshed automatically.

D. Nothing happens to the panels.

Correct Answer: C

When the base search of a dashboard panel with post-processing searches is refreshed, the panels with these post-processing searches are refreshed automatically (Option C). Post-processing searches inherit the scope and results of the base search, and when the base search is updated or rerun, the post-processed results are recalculated to reflect the latest data.

QUESTION 10

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 11

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 12

What arguments are required when using the spath command?

A. input, output, index

B. input, output path

C. No arguments are required.

D. field, host, source

Correct Answer: B

QUESTION 13

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 14

Which stats function is used to return a sorted list of unique field values?

A. values

B. sum

C. count

D. list

Correct Answer: A

The values function in the stats command in Splunk is used to return a sorted list of unique field values (Option A). This function is particularly useful for summarizing data by listing all unique values of a specified field across the events returned by the search, which can provide insights into the diversity and distribution of the data associated with that field.

QUESTION 15

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.