Splunk.SPLK-1004.v2024-07-10.q26

Exam Code:	SPLK-1004
Exam Name:	Splunk Core Certified Advanced Power User
Certification Provider:	Splunk
Free Question Number:	26
Version:	v2024-07-10
# of views:	1045
# of Questions views:	260
https://www.freepdfdumps.com/Splunk.SPLK-1004.v2024-07-10.q26.html	

NEW QUESTION: 1
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.
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 2
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
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 3
Which of the following are potential string results returned by the type of function?

A. True, False, Unknown
B. Number, Siring, Bool
C. Number, String, Null
D. Field, Value, Lookup
Answer: C (LEAVE A REPLY)
The typeof function in Splunk returns a string that represents the data type of the evaluated expression. The potential string results include "Number", "String", and "Null" (Option C). These indicate whether the evaluated expression is a numerical value, a string, or a null value, respectively, helping users understand the data types they are working with in their searches andscripts.

NEW QUESTION: 4
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.
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 5
What file types does Splunk use to define geospatial lookups?
A. GPX or GML files
B. TXT files
C. KMZ or KML files
D. CSV files
Answer: (SHOW ANSWER)
For defining geospatial lookups, Splunk uses KMZ or KML files (Option C). KML (Keyhole Markup Language) is an XML notation for expressing geographic annotation and visualization within Internet-based maps and Earth browsers like Google Earth. KMZ is a compressed version of KML files. These file types allow Splunk to map data points to geographic locations, enabling the creation of geospatial visualizations and analyses. GPX or GML files (Option A), TXT files (Option B), and CSV files (Option D) are not specifically used for geospatial lookups in Splunk, although CSV files are commonly used for other types of lookups.

NEW 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.
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 7
What is the recommended way to create a field extraction that is both persistent and precise?
A. Use the Field Extractor and manually edit the generated regular expression.
B. Use the rex command.
C. Use the erex command.
D. Use the Field Extractor and let it automatically generate a regular expression.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Which statement about the coalesce function is accurate?
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 (LEAVE A REPLY)
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.

NEW QUESTION: 9
If a search contains a subsearch, what is the order of execution?
A. The order of execution depends on whether either search uses a stats command.
B. The inner search executes first.

C. The otter search executes first.
D. The two searches are executed in parallel.
Answer: B (LEAVE A REPLY)
In a Splunk search containing a subsearch, the inner subsearch executes first (Option B). The result of the subsearch is then passed to the outer search. This is because the outer search often depends on the results of the inner subsearch to complete its execution. For example, a subsearch might be used to identify a list of relevant terms or values which are then used by the outer search to filter or manipulate the main dataset.

NEW QUESTION: 10
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.
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 11
Why use the tstats command?
A. As an alternative to the summary command.
B. To generate statistics on indexed fields.
C. To generate an accelerated datamodel.
D. To generate statistics on search-time fields.
Answer: B (LEAVE A REPLY)
The tstats command in Splunk is used to generate statistics on indexed fields, particularly from data models that have been accelerated (Option B). This command is highly efficient for summarizing large volumes of data because it operates on indexed-time summarizations rather than raw data, enabling faster search performance and reduced processing time. The tstats command is especially useful in scenarios where quick aggregation and analysis of indexed data are required, making it a powerful tool for exploring and reporting on data model information. While tstats can be seen as an alternative to some uses of the summary command (Option A), its primary utility is in its ability to leverage data model accelerations and indexed field statistics, rather than creating or referring to summary indexes. It does not specifically generate statistics on search-time fields (Option D) or create an accelerated data model (Option C), but rather it queries against existing accelerated data models.

NEW QUESTION: 12
What XML element is used to pass multiple fields into another dashboard using a dynamic drilldown?
A. <drilldown field_"sources_Field_name">
B. <condition field_"sources_Field_name">
C. <pas_token field_"sources_field_name">
D. <link field_"sources_field_name">
Answer: D (LEAVE A REPLY)
In Splunk Simple XML for dashboards, dynamic drilldowns are configured within the<drilldown>element, not<link>,<condition>, or<pass_token>. To pass multiple fields to another dashboard, you would use a combination of<set>tokens within the<drilldown>element. Each<set>token specifies a field or value to be passed. The correct configuration might look something like this within the<drilldown>element:
<drilldown>
<set token="token1">$row.field1$</set>
<set token="token2">$row.field2$</set>
<link target="_blank">/app/search/new_dashboard</link>
</drilldown>
In this configuration,$row.field1$and$row.field2$are placeholders for the field values from the clicked event, which are assigned to tokenstoken1andtoken2. These tokens can then be used in the target dashboard to receive the values. The<link>element specifiesthe target dashboard. Note that the exact syntax can vary based on the specific requirements of the drilldown and the dashboard configuration.

NEW QUESTION: 13
When possible, what is the best choice for summarizing data to improve search performance?
A. Us the fieldsummary command.
B. Data model acceleration
C. Summary indexing
D. Report acceleration
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
Which stats function is used to return a sorted list of unique field values?
A. values
B. sum
C. count
D. list
Answer: A (LEAVE A REPLY)

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.

NEW QUESTION: 15
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.
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 16
Which of the following functions' primary purpose is to convert epoch time to a string format?
A. tostring
B. strptime
C. tonumber
D. strftime
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 17
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 18
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
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 19
When and where do search debug messages appear to help with troubleshooting views?

A. In the Dashboard Editor, while the search is running.
B. In the Search Job Inspector, after the search completes.
C. In the Search Job Inspector, while the search is running.
D. In the Dashboard Editor, after the search completes.
Answer: (SHOW ANSWER)
Search debug messages in Splunk appear in the Search Job Inspector while the search is running (Option C).
The Search Job Inspector provides detailed information about a search job, including performance statistics, search job properties, and any messages or warnings generated during the search execution. This tool is invaluable for troubleshooting and optimizing searches, as it offers real-time insights into the search process and potential issues.

NEW QUESTION: 20
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"}
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 21
When would a distributable streaming command be executed on an Indexer?
A. If any of the preceding search commands are executed on the search head.
B. If all preceding search commands are executed on me indexer, and a streamstats command is used.
C. If all preceding search commands are executed on the Indexer.
D. If some of the preceding search commands are executed on the indexer, and a Timerchart command is used.
Answer: C (LEAVE A REPLY)
A distributable streaming command would be executed on an indexer if all preceding search commands are executed on the indexer (Option C). Distributable streaming commands are designed to be executed where the data resides, reducing data transfer across the network and leveraging the processing capabilities of indexers.
This enhances the overall efficiency and performance of Splunk searches, especially in distributed environments.

NEW QUESTION: 22
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.
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 23
Which command processes a template for a set of related fields?
A. bin
B. xyseries
C. foreach
D. untable
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 24
Which predefined drilldown token passes a clicked value from a table row?
A. $rowclick. <fieldname>$
B. $tableclick .< fieldname>$
C. $row. <fieldname>$
D. $table .< fieldname>$
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 25
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
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 26
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.
Answer: (SHOW ANSWER)
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.