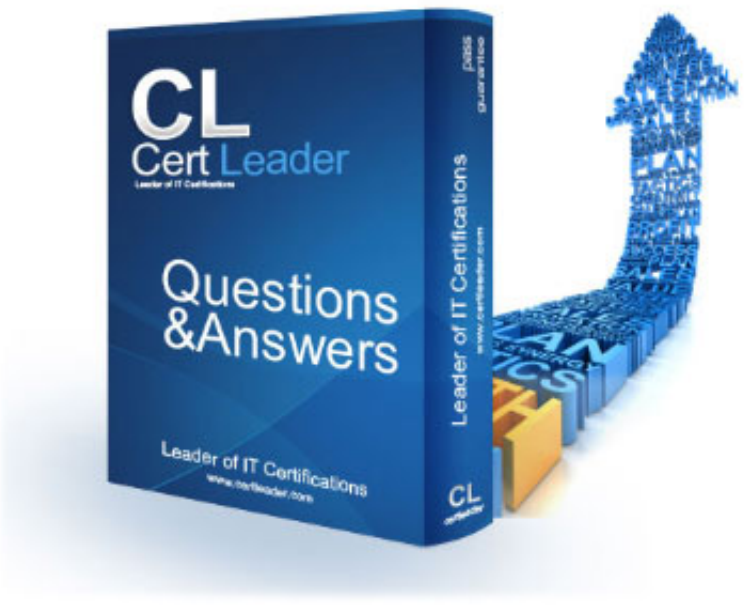
SPLK-1004 Dumps

Splunk Core Certified Advanced Power User

https://www.certleader.com/SPLK-1004-dumps.html



NEW QUESTION 1
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

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.

NEW QUESTION 2
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]

Answer: A

NEW QUESTION 3
Which is a regex best practice?

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.

NEW QUESTION 4
Which of the following is not a common default time field?

A. date_zone
B. date minute
C. date_year
D. date_day

Answer: A

Explanation:
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.

NEW QUESTION 5
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.

Answer: C

Explanation:
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.

NEW QUESTION 6
Which field Is requited for an event annotation?

A. annotation_category
B. _time

C. eventype
D. annotation_label

Answer: B

Explanation:
For an event annotation in Splunk, the required field is time (Option B). The time field specifies the point or range in time that the annotation should be applied to in timeline visualizations, making it essential for correlating the annotation with the correct temporal context within the data.

NEW QUESTION 7
Which statement about tsidx files is accurate?

A. Splunk updates tsidx files every 30 minutes.
B. Splunk removes outdated tsidx files every 5 minutes.
C. A tsidx file consists of a lexicon and a posting list.
D. Each bucket in each index may contain only one tsidx file.

Answer: C

Explanation:
A tsidx file in Splunk is an index file that contains indexed data, and it consists of two main parts: alexicon and a posting list (Option C). The lexicon is a list of unique terms found in the data, and the posting list is a list of references to the occurrences of these terms in the indexed data. This structure allows Splunk to efficiently search and retrieve data based on search terms.

NEW QUESTION 8
Repeating JSON data structures within one event will be extracted as what type of fields?

A. Single value
B. Lexicographical
C. Multivalue
D. Mvindex

Answer: C

Explanation:
Repeating JSON data structures within a single event in Splunk are extracted as multivalue fields (Option C). Multivalue fields allow a single field to contain multiple distinct values, which is common with JSON data structures that include arrays or repeated elements. Splunk's field extraction capabilities automatically recognize and parse these structures, allowing users to work with each value within the multivalue field for analysis and reporting

NEW QUESTION 9
What is a performance improvement technique unique to dashboards?

A. Using stats instead of transaction
B. Using global searches
C. Using report acceleration
D. Using datamodel acceleration

Answer: C

Explanation:
Using report acceleration (Option C) is a performance improvement technique unique to dashboards in Splunk. Report acceleration involves pre-computing the results of a report (which can be a saved search or a dashboard panel) and storing these results in a summary index, allowing dashboards to load faster by retrieving the pre-computed data instead of running the full search each time. This technique is especially useful for dashboards that rely on complex searches or searches over large datasets.

NEW QUESTION 10
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.

Answer: C

Explanation:
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.

NEW QUESTION 10
Which command processes a template for a set of related fields?

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.

NEW QUESTION 13
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.

Answer: D

Explanation:
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.

NEW QUESTION 15
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.

Answer: B

Explanation:
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.

NEW QUESTION 20
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.

Answer: B

Explanation:
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.

NEW QUESTION 23
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

Explanation:
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 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: 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.

NEW QUESTION 30
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

Answer: D

Explanation:
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.

NEW QUESTION 31
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

Explanation:
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 36
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1004 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-1004-dumps.html