Splunk

Exam Questions SPLK-1004

Splunk Core Certified Advanced Power User

NEW QUESTION 1
How is a cascading input used?

A. As part of a dashboard, but not in a form.
B. Without notation in the underlyin
C. XML.
D. As a way to filter other input selections.
E. As a default way to delete a user role.

Answer: C

Explanation:
A cascading input is used as a way to filter other input selections within a dashboard or form (Option C). It enables a dynamic user interface where the selection made in one input (e.g., a dropdown menu) determines the available options in another input. This setup allows for more intuitive and relevant user interactions, as each choice narrows down the subsequent options to ensure they are contextually appropriate.

NEW QUESTION 2
Which element attribute is required for event annotation?

A. <search type="event_annotation">
B. <search style="annotation">
C. <search type=$annotation$>
D. <search type="annotation">

Answer: D

Explanation:
In Splunk dashboards, event annotations are used to add informative overlays on timeline visualizations to mark significant events. The required element attribute to define an event annotation within a dashboard panel is <search type="annotation"> (Option D). This attribute specifies that the search within this element is intended to generate annotations, which are then overlaid on the timeline based on the time and information provided by the search results.

NEW QUESTION 3
Which of the following fields are provided by the fieldsummary command? (select all that apply)

A. count
B. stdev
C. mean
D. dc

Answer: AD

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.

NEW QUESTION 4
What default Splunk role can use the Log Event alert action?

A. Power
B. User
C. can_delete
D. Admin

Answer: D

Explanation:
In Splunk, the Admin role (Option D) has the capability to use the Log Event alert action among many other administrative privileges. The Log Event alert action allows Splunk to create an event in an index based on the triggering of an alert, providing a way to log and track alert occurrences over time. The Admin role typically encompasses a wide range of permissions, including the ability to configure and manage alert actions.

NEW QUESTION 5
What order of incoming events must be supplied to the transaction command to ensure correct results?

A. Reverse lexicographical order
B. Ascending lexicographical order
C. Ascending chronological order
D. Reverse chronological order

Answer: C

Explanation:
The transaction command in Splunk groups events into transactions based on common fields or characteristics. For the transaction command to function correctly and group events into meaningful transactions, the incoming events must be supplied in ascending chronological order (Option C). This ensures that related events are sequenced correctly according to their occurrence over time, allowing for accurate transaction grouping and analysis

NEW QUESTION 6
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: B

Explanation:
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 7
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 8
Which of the following statements is accurate regarding the append command?

A. It is used with a subsearch and only accesses real-lime searches.
B. It is used with a subsearch and oily accesses historical data.
C. It cannot be used with a subsearch and only accesses historical data.
D. It cannot be used with a subsearch and only accesses real-time searches.

Answer: B

Explanation:
The append command in Splunk is often used with a subsearch to add additional data to the end of the primary search results, and it can access historical data (Option B). This capability is useful for combining datasets from different time ranges or sources, enriching the primary search results with supplementary information.

NEW QUESTION 9
What is one way to troubleshoot dashboards?

A. Run the | previous_searches command to troubleshoot your SPL queries.
B. Go to the Troubleshooting dashboard of me Searching and Reporting app.
C. Delete the dashboard and start over.
D. Create an HTML panel using tokens to verify that they are being set.

Answer: B

Explanation:
To troubleshoot dashboards in Splunk, one effective approach is to go to the Troubleshooting dashboard of the Search & Reporting app (Option B). This dashboard provides insights into the performance and potential issues of other dashboards and searches, offering a centralized place to diagnose and address problems. This method allows for a structured approach to troubleshooting, leveraging built-in tools and reports to identify and resolve issues.

NEW QUESTION 10
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

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.

NEW QUESTION 10
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

Answer: B

Explanation:
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.

NEW QUESTION 13
Where can wildcards be used in the tstats command?

A. No wildcards can be used with
B. In the where to clause.
C. In the from clause.
D. In the by clause.

Answer: C

Explanation:
Wildcards can be used in the from clause of the tstats command in Splunk (Option C). The from clause specifies the data model or dataset from which to retrieve the statistics, and using wildcards here allows users to query across multiple data models or datasets that share a common naming pattern, making the search more flexible and encompassing.

NEW QUESTION 16
Which commands can run on both search heads and indexers?

A. Transforming commands
B. Centralized streaming commands
C. Dataset processing commands
D. Distributable streaming commands

Answer: D

Explanation:
Distributable streaming commands in Splunk can run on both search heads and indexers (Option D). These commands operate on each event independently and can be distributed across indexers for parallel execution, which enhances search efficiency and scalability. This category includes commands like search, where, eval, and many others that do not require the entire dataset to be available to produce their output.

NEW QUESTION 19
When using the bin command, which argument sets the bin size?

A. mazDataSizeMB
B. max
C. volume
D. span

Answer: D

Explanation:
When using the bin command in Splunk, the span argument is used to set the size of each bin (Option D). The span argument determines the granularity or width of each bin when segmenting data over a time range or numerical field, which is essential for time series analysis, histogram generation, or other aggregated data visualizations.

NEW QUESTION 23
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: D

Explanation:
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 26
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 28
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 32
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 33
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 34
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

Explanation:
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 37
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 streamstatscommand 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

Explanation:
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 39
How is a muitlvalue Add treated from product-"a, b, c, d"?

A. . . . | makemv delim{product, “,”}
B. . . . | eval mvexpand{makemv{product, “,”})
C. . . . | mvexpand product
D. . . . | makemv delim=”,” product

Answer: D

Explanation:
To treat a multivalue field product="a, b, c, d" in Splunk, the correct command is ...| makemv delim="," product (Option D).The makemv command with the delim argument specifies the delimiter (in this case, a comma) to split the field values into a multivalue field. This allows for easier manipulation and analysis of each value within the product field as separate entities.

NEW QUESTION 43
What is the correct hierarchy of XML elements in a dashboard panel?

A. <panel><dashboard><row>
B. <dashboard><row><panel>
C. <dashboard><panel><row>
D. <panel><row><dashboard>

Answer: B

Explanation:
In a Splunk dashboard, the correct hierarchy of XML elements for a dashboard panel is
<dashboard><row><panel> (Option B). A Splunk dashboard is defined within the
<dashboard> element. Within this, <row> elements are used to organize the layout into rows, and each <panel> 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.

NEW QUESTION 47
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-1004 Practice Exam Features:

* SPLK-1004 Questions and Answers Updated Frequently

* SPLK-1004 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year