Exam Questions SPLK-1004

Splunk Core Certified Advanced Power User

https://www.2passeasy.com/dumps/SPLK-1004/

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 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 4
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 5
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 6
What is an example of the simple XML syntax for a base search and its post-srooess search?

A. <search id="myBaseSearch">, <search base="myBaseSearch">
B. <search globalsearch="myBaseSearch">, <search globalsearch>
C. <panel id="myBaseSearch">, <panel base="myBaseSearch">
D. <search id="myGlobalSearch">, <search base="myBaseSearch">

Answer: A

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
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 9
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 10
Which of the following has a schema or structure embedded in the data itself?

A. Dark data
B. Unstructured data
C. Embedded data
D. Self-describing data

Answer: D

Explanation:
Self-describing data (Option D) refers to data that includes information about its own structure or schema within the data itself. This characteristic makes it easier to understand and process the data because the structure and meaning of the data are embedded with the data, reducing the need for external definitions or mappings. Examples of self- describing data formats include JSON and XML, where elements and attributes describe the data they contain.

NEW QUESTION 10
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 15
What qualifies a report for acceleration?

A. Fewer than 100k events in search results, with transforming commands used in the search string.
B. More than 100k events in search results, with only a search command in the search string.
C. More than 100k events in the search results, with a search and transforming command used in the search string.
D. fewer than 100k events in search results, with only a search and transaction command used in the search string.

Answer: A

Explanation:
A report qualifies for acceleration in Splunk if it involves fewer than 100,000 events in the search results and uses transforming commands in the search string (Option A). Transforming commands aggregate data, making it more suitable for acceleration by reducing the dataset's complexity and size, which in turn improves the speed and efficiency of report generation.

NEW QUESTION 20
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 23
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 26
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 30
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 34
How can the erex and rex commands be used in conjunction to extract fields?

A. The regex Generated by the erex command can be edited and used with the regex command in a subsequent search.
B. The regex generated by the rex command can be edited and used with the erex command in a subsequent search.
C. The regex generated by the erex command can be edited and used with the erex command in a subsequent search.
D. The erex and rex commands cannot be used in conjunction under any circumstances.

Answer: A

Explanation:
The erex command in Splunk is used to generate regular expressions based on example data, and these generated regular expressions can then be edited and utilized with the rex command in subsequent searches (Option A). The erex command is helpful for users who may not be familiar with regular expression syntax, as it provides a starting point that can be refined and customized with rex for more precise field extraction.

NEW QUESTION 37
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: C

Explanation:
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 38
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 39
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 43
which function of the stats command creates a multivalue entry?

A. mvcombine
B. eval
C. makemv
D. list

Answer: D

NEW QUESTION 48
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 53
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 55
What is returned when Splunk finds fewer than the minimum matches for each lookup value?

A. The default value NULL until the minimum match threshold is reached.
B. The default match value until the minimum match threshold Is reached.
C. The first match unless the time_field attribute is specified.
D. Only the first match.

Answer: A

Explanation:
When Splunk's lookup feature finds fewer than the minimum matches specified for each lookup value, it returns the default value NULL for those unmatched entries until the minimum match threshold is reached (Option A). This behavior ensures that lookups return consistent and expected results, even when the available data does not meet the specified criteria for a minimum number of matches.

NEW QUESTION 59
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 60
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 64
Which syntax is used when referencing multiple CSS files in a view?

A. <dashboard stylesheet="custom.css, userapps.css">
B. <dashboard style="custom.css, userapps.css">
C. <dashboard stylesheet=custom.css stylesheet=userapps.css>
D. <dashboard stylesheet="custom.css | userapps.css">

Answer: C

Explanation:
When referencing multiple CSS files in a Splunk dashboard view (within Simple XML), the correct approach is to include separate stylesheet attributes for each CSS file. The syntax for this would be similar to <dashboard stylesheet="custom.css" stylesheet="userapps.css"> (Option C). This method allows the dashboard to load and apply the styles from both CSS files, enhancing the dashboard's visual appearance and user interface design.

NEW QUESTION 69
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: C

Explanation:
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 73
Which of the following is accurate about cascading inputs?

A. They can be reset by an event handler.
B. The final input has no impact on previous inputs.
C. Only the final input of the sequence can supply a token to searches.
D. Inputs added to panels can not participate.

Answer: A

Explanation:
Cascading inputs in Splunk dashboards allow the selection in one input (like a dropdown, radio button, etc.) to determine the available options in the subsequent input, creating a dependent relationship between them. An event handler can be configured to reset subsequent inputs based on the selection made in a preceding input (Option A), ensuring that only relevant options are presented to the user as they make selections. This approach enhances the dashboard's usability by guiding the user through a logical flow of choices, where each selection refines the scope of the following options.

NEW QUESTION 78
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

Explanation:
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 80
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

Explanation:
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 82
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 83
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<5
B. earliest=-2h@h AND latest=-5h@h
C. time_hour>-2 AND time_hour>-5
D. earliest=2h@ AND latest=5h3h

Answer: B

Explanation:
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.

NEW QUESTION 86
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1004 Product From:

https://www.2passeasy.com/dumps/SPLK-1004/

Money Back Guarantee

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