Splunk.SPLK-1004.by.Athort.32q

Number: SPLK-1004
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: SPLK-1004

Exam Name: Splunk Core Certified Advanced Power User

Exam A

QUESTION 1
Which of the following would exclude all entries contained in the lookup file baditems. csv from search results?

A. NOT [inputlookup baditems.csv]

B. NOT (lookup baditems.csv OUTPUT item)

C. WHERE item NOT IN (baditems.csv)

D. [NOT inputlookup baditems.csv]

Correct Answer: A
Section:
Explanation:
The correct syntax to exclude all entries contained in the lookup file baditems.csv from search results is NOT [inputlookup baditems.csv]. This syntax uses a subsearch with the inputlookup command to retrieve the contents of the baditems.csv lookup file and then uses the NOT operator to exclude those results from the main search. This approach is efficient for filtering out unwanted data based on a predefined list of criteria stored in a lookup file.

QUESTION 2
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

Correct Answer: C
Section:
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

QUESTION 3
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

Correct Answer: D
Section:
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.

QUESTION 4
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.

Correct Answer: B
Section:
Explanation:
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.

QUESTION 5
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.

Correct Answer: A
Section:
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.

QUESTION 6
What are the four types of event actions?

A. stats, target, set, and unset
B. stats, target, change, and clear
C. eval, link, change, and clear
D. eval, link, set, and unset

Correct Answer: C
Section:
Explanation:
The four types of event actions in Splunk are eval, link, change, and clear (Option C). These actions can be used in dashboard panel configurations to dynamically interact with or manipulate event data based on user inputs or other criteria. Eval is used for calculating fields, link for creating hyperlinks, change for modifying field values, and clear for removing field values or other data elements.

QUESTION 7
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.

Correct Answer: D
Section:
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.

QUESTION 8
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

Correct Answer: D
Section:
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.

QUESTION 9
Which of the following fields are provided by the fieldsummary command? (select all that apply)

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

Correct Answer: A, D
Section:
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.

QUESTION 10
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.

Correct Answer: A
Section:
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.

QUESTION 11
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'>

Correct Answer: D
Section:
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.

QUESTION 12
What is the correct hierarchy of XML elements in a dashboard panel?

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

Correct Answer: B
Section:
Explanation:
In a Splunk dashboard, the correct hierarchy of XML elements for a dashboard panel is <dashboard><row> (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 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.

QUESTION 13
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.

Correct Answer: B
Section:
Explanation:

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.

QUESTION 14
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
Section:
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.

QUESTION 15
When using the bin command, which argument sets the bin size?

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

Correct Answer: D
Section:
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.

QUESTION 16
How is a cascading input used?

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

Correct Answer: C
Section:
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.

QUESTION 17
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.

Correct Answer: B
Section:
Explanation:
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.

QUESTION 18
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.

Correct Answer: B
Section:
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.

QUESTION 19
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
Section:
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.

QUESTION 20
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
Section:
Explanation:
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 21
Which field Is requited for an event annotation?

A. annotation_category
B. _time
C. eventype
D. annotation_label

Correct Answer: B
Section:
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.

QUESTION 22
How is regex passed to the makemv command?

A. makemv be preceded by the erex command.
B. It is specified by the delim argument.
C. It Is specified by the tokenizer argument.
D. Makemv must be preceded by the rex command.

Correct Answer: B
Section:
Explanation:
The regex is passed to the makemv command in Splunk using the delim argument (Option B). This argument specifies the delimiter used to split a single string field into multiple values, effectively creating a multivalue field from a field that contains delimited data.

QUESTION 23
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

Section:
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 into fields. This hierarchical approach to tokenization allows Splunk to efficiently parse and structure the incoming data for analysis.

QUESTION 24
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.

Correct Answer: A
Section:
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.

QUESTION 25
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

Correct Answer: B
Section:
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.

QUESTION 26
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
Section:
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.

QUESTION 27

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. ,
D. <search id='myGlobalSearch'>, <search base='myBaseSearch'>

Correct Answer: A
Section:

QUESTION 28
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
Section:
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.

QUESTION 29
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

Correct Answer: C
Section:
Explanation:
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 and scripts.

QUESTION 30
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

Section:
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.

QUESTION 31
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.

Correct Answer: B
Section:
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.

QUESTION 32
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

Correct Answer: D
Section:
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.