Exam Questions SPLK-1004

Splunk Core Certified Advanced Power User

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

NEW QUESTION 1
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 2
A report named "Linux logins" populates a summary index with the search string sourcetype=linux_secure| sitop src_ip user. Which of the following correctly searches against the summary index for this data?

A. index=summary sourcetype="linux_secure" | top src_ip user
B. index=summary search_name="Linux logins" | top src_ip user
C. index=summary search_name="Linux logins" | stats count by src_ip user
D. index=summary sourcetype="linux_secure" | stats count by src_ip user

Answer: B

Explanation:
When searching against summary data in Splunk, it's common to reference the name of the saved search or report that populated the summary index. The correct search syntax to retrieve data from the summary index populated by a report named "Linux logins" is index=summary search_name="Linux logins" | top src_ip user (Option B). This syntax uses the search_name field, which holds the name of the saved search or report that generated the summary data, allowing for precise retrieval of the intended summary data.

NEW QUESTION 3
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 4
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 5
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 6
When running a search, which Splunk component retrieves the individual results?

A. Indexer
B. Search head
C. Universal forwarder
D. Master node

Answer: B

Explanation:
The Search head (Option B) in Splunk architecture is responsible for initiating and coordinating search activities across a distributed environment. When a search is run, the search head parses the search query, distributes the search tasks to the appropriate indexers (which hold the actual data), and then consolidates the results retrieved by the indexers. The search head is the component that interacts with the user, presenting the final search results

NEW QUESTION 7
What is the recommended way to create a field extraction that is both persistent and precise?

A. Use the rex command.
B. Use the Field Extractor and manually edit the generated regular expression.
C. Use the Field Extractor and let it automatically generate a regular expression.
D. Use the erex command.

Answer: B

NEW QUESTION 8
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 9
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 10
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 10
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

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 andscripts.

NEW QUESTION 11
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 16
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: C

Explanation:
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 19
Which predefined drilldown token passes a clicked value from a table row?

A. $rowclic
B. <fieldname>$
C. $tableclick .< fieldname>$
D. $ro
E. <fieldname>$
F. $table .< fieldname>$

Answer: A

Explanation:
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 23
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 27
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 31
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 35
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 38
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]

Answer: A

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.

NEW QUESTION 40
Which of the following can be used to access external lookups?

A. Perl and Python
B. Python and Ruby
C. Perl and binary executable
D. Python and binary executable

Answer: D

Explanation:
Splunk supports the use of external lookups, which can be scripts or binary executables that enrich search results with external data. These external lookups can be written in various scripting languages or compiled as binary executables. Among the options given, Python and binary executables (Option D) are commonly used for creating external lookups in Splunk. Python is a widely used programming language that can easily interact with Splunk's API and data structures, and binary executables can be used for more complex or performance-critical lookup operations. Perl and Ruby (Options A and B) are less commonly used in this context, and Perl combined with binary executables (Option C) is not as standard for Splunk external lookups as Python.

NEW QUESTION 45
......