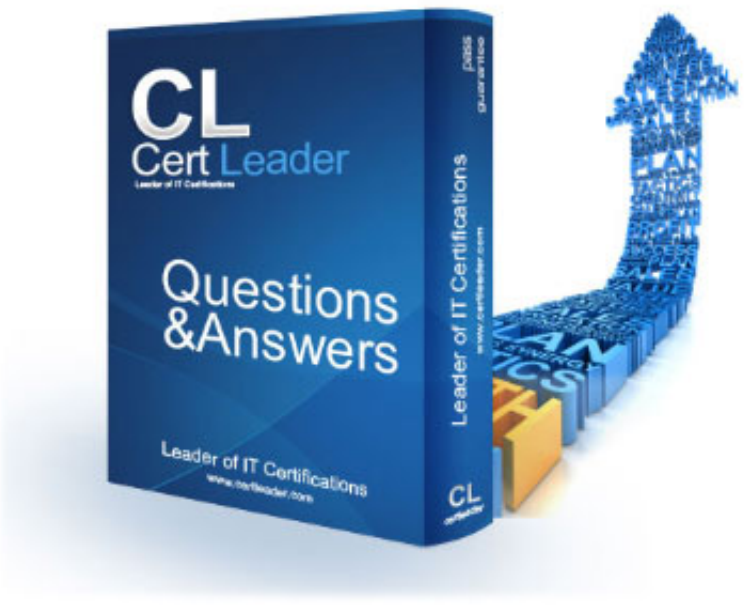
SPLK-1004 Dumps

Splunk Core Certified Advanced Power User

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



NEW QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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.

Answer: B

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.

NEW QUESTION 10
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 10
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 12
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 16
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 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

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 22
.....

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