Free Questions for SPLK-1004 by certscare

Shared by Snyder on 26-02-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When and where do search debug messages appear to help with troubleshooting views?

Options:

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.

Question 2

Question Type: MultipleChoice

Which of these generates a summary index containing a count of events by productId?

Options:

A- | stats count by productId

B- | stats sum (productId)

C- | sistats count by productId

D- sistats summary_index by productid

Answer:

A

Explanation:

To generate a summary index containing a count of events by productId, the correct search command would be | stats count by productId (Option A). This command aggregates the events by productId, counting the number of events for each unique productId value. The stats command is a fundamental Splunk command used for aggregation and summarization, making it suitable for creating summary data like counts by specific fields.

Question 3

Question Type: MultipleChoice

What is a performance improvement technique unique to dashboards?

Options:

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.

Question 4

Question Type: MultipleChoice

Which of the following is not a common default time field?

Options:

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.

Question 5

Question Type: MultipleChoice

Which statement about tsidx files is accurate?

Options:

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: a lexicon 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.

Question 6

Question Type: MultipleChoice

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?

Options:

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.

Question 7

Question Type: MultipleChoice

Repeating JSON data structures within one event will be extracted as what type of fields?

Options:

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

Question 8

Question Type: **MultipleChoice**

Which element attribute is required for event annotation?

Options:

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.