SPLK-1004 Q&As

Splunk Core Certified Advanced Power User

Pass Splunk SPLK-1004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-1004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

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 2

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

A. mazDataSizeMB

B. max

C. volume

D. span

Correct Answer: D

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 3

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

A. ,

B. ,

C. ,

D. ,

Correct Answer: A

QUESTION 4

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: AD

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 5

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

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.