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.geekcert.com/splk-1004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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-2 AND time_hour>-5

D. earliest=2h@ AND latest=5h3h

Correct Answer: B

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 2

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

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 3

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

Correct Answer: C

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.

QUESTION 4

Where can wildcards be used in the tstats command?

A. No wildcards can be used with

B. In the where to clause.

C. In the from clause.

D. In the by clause.

Correct Answer: C

Wildcards can be used in the from clause of the tstats command in Splunk (Option C). The from clause specifies the data model or dataset from which to retrieve the statistics, and using wildcards here allows users to query across multiple data models or datasets that share a common naming pattern, making the search more flexible and encompassing.

QUESTION 5

What does the query | makeresults generate?

A. A timestamp

B. A results field

C. An error message

D. The results of the previously run search.

Correct Answer: B

The | makeresults command in Splunk generates a single event containing default fields, with theprimary purpose of creating sample data or a placeholder event for testing and development purposes. The most notable field it generates is _time, but it does not create a specific \\'results\\' field per se. However, it\\'s commonly used to create a base event for further manipulation with eval or other commands in search queries for demonstration, testing, or constructing specific scenarios.