SPLK-1004$^{Q\&As}$

Splunk Core Certified Advanced Power User

Pass Splunk SPLK-1004 Exam with 100% Guarantee

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

QUESTION 1

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 2

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.

Correct Answer: A

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.

QUESTION 3

Where does the output of an append command appear in the search results?

A. Added as a column to the right of the search results.

B. Added as a column to the left of the search results.

C. Added to the beginning of the search results.

D. Added to the end of the search results.

Correct Answer: D

The output of an append command in Splunk search results is added to the end of the search results (Option D). The append command is used to concatenate the results of a subsearch to the end of the current search results, effectively extending the result set with additional data. This can be particularly useful for combining related datasets or adding contextual information to the existing search results.

QUESTION 4

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

Correct Answer: B

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.

QUESTION 5

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

Correct Answer: D

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.