SPLK-1002^{Q&As}

Splunk Core Certified Power User

QUESTION 1

Which of the following statements describe data model acceleration? (select all that apply)

A. Root events cannot be accelerated.

B. Accelerated data models cannot be edited.

C. Private data models cannot be accelerated.

D. You must have administrative permissions or the accelerate_dacamodel capability to accelerate a data model.

Correct Answer: BCD

Data model acceleration is a feature that speeds up searches on data models by creating and storing summaries of the data model datasets1. To enable data model acceleration, you must have administrative permissions or the accelerate_datamodel capability1. Therefore, option D is correct. Accelerated data models cannot be edited unless you disable the acceleration first1. Therefore, option B is correct. Private data models cannot be accelerated because they are not visible to other users1. Therefore, option C is correct. Root events can be accelerated as long as they are not based on a search string1. Therefore, option A is incorrect.

QUESTION 2

When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

A. OR

B. ( )

C. AND

D. NOT

Correct Answer: ABD

When you mouse over and click to add a search term from the Fields sidebar or from an event in your search results, Splunk automatically adds the term to your search string with an implied AND operator2. However, this does not apply to some Boolean operators such as OR, NOT and parentheses (). These operators are not implied when you add a search term and you have to type them manually if you want to use them in your search string2. Therefore, options A, B and D are correct, while option C is incorrect because AND is implied when you add a search term.

QUESTION 3

This is what Splunk uses to categorize the data that is being indexed.

A. sourcetype

B. index

C. source

D. host

Correct Answer: A

QUESTION 4

Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

A. maxpause

B. endswith

C. maxduration

D. maxspan

Correct Answer: D

The maxspan function of the transaction command allows you to set the maximum total time between the earliest and latest events returned. The maxspan function is an argument that can be used with the transaction command to specify the start and end constraints for the transactions. The maxspan function takes a time modifier as its value, such as 30s, 5m, 1h, etc. The maxspan function sets the maximum time span between the first and last events in a transaction. If the time span between the first and last events exceeds the maxspan value, the transaction will be split into multiple transactions.

QUESTION 5

When would transaction be used instead of stats?

A. To see results of a calculation.

B. To group events based on start/end values.

C. To have a faster and more efficient search.

D. To group events based on a single field value.

Correct Answer: B