SPLK-1002^Q&As

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

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

https://www.pass2lead.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

Explanation: 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 2

What is the correct syntax to search for a tag associated with a value on a specific fields?

A. Tag-