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.passapply.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 of the following searches would return a report of sales by product-name?

A. chart sales by product_name

B. chart sum(price) as sales by product_name

C. stats sum(price) as sales over product_name

D. timechart list(sales), values(product_name)

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Chart
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Stats

QUESTION 2

A space is an implied _____ in a search string.

A. OR

B. AND

C. ()

D. NOT

Correct Answer: B

A space is an implied AND in a search string, which means that it acts as a logical operator that returns events that match both terms on either side of the space2. For example, status=200 method=GET will return events that have both status=200 and method=GET2. Therefore, option B is correct, while options A, C and D are incorrect because they are not implied by a space in a search string.

QUESTION 3

Which of the following statements are true for this search? (Select all that apply.) SEARCH: sourcetype=access* |fields action productId status

A. is looking for all events that include the search terms: fields AND action AND productId AND status

B. users the table command to improve performance

C. limits the fields are extracted

D. returns a table with 3 columns

Correct Answer: C

QUESTION 4

Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

A. Field alias

B. Event types

C. Search workflow action

D. Tags

Correct Answer: A

The correct answer is A. Field alias123.

In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field3. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)12. The

CIM provides a methodology for normalizing values to a common field name1. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact2. By using field aliases, you can map vendor

fields to common fields that are the same for each data source in a given domain4. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention1.

QUESTION 5

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

A. Host

B. Sourcetype

C. Index

D. Source

Correct Answer: B