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.pass4itsure.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following commands will show the maximum bytes?

A. sourcetype=access_* | maximum totals by bytes

B. sourcetype=access_* | avg (bytes)

C. sourcetype=access_* | stats max(bytes)

D. sourcetype=access_* | max(bytes)

Correct Answer: C

QUESTION 2

A user runs the following search:

index--X sourcetype=Y I chart count (domain) as count, sum (price) as sum by product, action usenull=f useother--f

Which of the following table headers match the order this command creates?

A. The chart command does not allow for multiple statistical functions.

B. Product, sum: addtocart, sum: remove, sum: purchase, count: addtocart, count: remove, count: purchase

C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase

D. Count: product, sum: product, count: action, sum: action

Correct Answer: C

The correct answer is C. Product, count: addtocart, count: remove, count: purchase, sum:

addtocart, sum: remove, sum: purchase1.

In Splunk, the chart command is used to create a table or a chart visualization from your data2. The chart command takes at least one function and one field, and optionally another field to group by2. In the given search, the chart command is

used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action). The usenull=f and useother=f options are used to exclude null values and other values from the chart2. The chart

command creates a table with headers that match the order of the fields and functions in the command1. The headers for the count function are prefixed with count:, and the headers for the sum function are prefixed with sum:1. The values of

the product and action fields are used as the suffixes for the headers1. Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, and sum: purchase1.

QUESTION 3

Which is not a comparison operator in Splunk

A.

E. ?=

Correct Answer: E

A comparison operator is a symbol that compares two values and returns a Boolean result (true or false)2. Splunk supports various comparison operators such as , =, !=, =, IN and LIKE2. However, ?= is not a valid comparison operator in Splunk and will cause a syntax error if used in a search string2. Therefore, option E is correct, while options A, B, C and D are incorrect because they are valid comparison operators in Splunk

QUESTION 4

Which of the following statements describes an event type?

A. A log level measurement: info, warn, error.

B. A knowledge object that is applied before fields are extracted.

C. A field for categorizing events based on a search string.

D. Either a log, a metric, or a trace.

Correct Answer: C

This is because an event type is a knowledge object that assigns a user- defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards. You can learn more about event types from the Splunk documentation1. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

QUESTION 5

Which of the following is a function of the Splunk Common Information Model (CIM)?

A. Normalizing data across a Splunk deployment.

B. Providing templates for reports and dashboards.

C. Algorithmically shifting events to other indexes.

D. Reingesting previously indexed data with new field names.

Correct Answer: A

Latest SPLK-1002 Dumps SPLK-1002 Study Guide SPLK-1002 Exam Questions