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.leads4pass.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 statements about calculated fields in Splunk is true?

A. Calculated fields cannot be chained together to create more complex fields

B. Calculated fields can be chained together to create more complex fields.

C. Calculated fields can only be used in dashboards.

D. Calculated fields can only be used in saved reports.

Correct Answer: B

The correct answer is B. Calculated fields can be chained together to create more complex fields.

Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1. Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as: discount = total * 0.9 This will create a new field named discount that is equal to 90% of the total field value for each event2. References: About calculated fields Chaining calculated fields

---

QUESTION 2

A space is an implied _____ in a search string.

A. OR

B. AND

C. ()

D. NOT

Correct Answer: B

Explanation: 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

How does a user display a chart in stack mode?

A. By using the stack command.

B. By turning on the Use Trellis Layout option.

C. By changing Stack Mode in the Format menu.

D. You cannot display a chart in stack mode, only a timechart.

Correct Answer: C

Explanation: A chart is a graphical representation of your search results that shows the relationship between two or more fields2. You can display a chart in stack mode by changing the Stack Mode option in the Format menu2. Stack mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series2. Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

QUESTION 4

Which type of visualization shows relationships between discrete values in three dimensions?

A. Pie chart

B. Line chart

C. Bubble chart

D. Scatter chart

Correct Answer: C

https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub

QUESTION 5

Data model are composed of one or more of which of the following datasets? (select all that apply.)

A. Events datasets

B. Search datasets

C. Transaction datasets

D. Any child of event, transaction, and search datasets

Correct Answer: ABC

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:

Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.

Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.

Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.