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.geekcert.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

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

Explanation: 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 2

What is the relationship between data models and pivots?

A. Data models provide the datasets for pivots.

B. Pivots and data models have no relationship.

C. Pivots and data models are the same thing.

D. Pivots provide the datasets for data models.

Correct Answer: A

Explanation: The relationship between data models and pivots is that data models provide the datasets for pivots. 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. Pivots are user interfaces that allow you to create data visualizations that present different aspects of a data model. Pivots let you select options from menus and forms to create charts, tables,

maps, etc., without writing any SPL code. Pivots use datasets from data models as their source of data. Pivots and data models are not the same thing, as pivots are tools for visualizing data models. Pivots do not provide datasets for data

models, but rather use them as inputs.

Therefore, only statement A is true about the relationship between data models and pivots.

QUESTION 3

A data model consists of which three types of datasets?

A. Constraint, field, value.

B. Events, searches, transactions.

C. Field extraction, regex, delimited.

D. Transaction, session ID, metadata.

Correct Answer: B

Explanation: The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole. Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

https://docs.splunk.com/Splexicon:Datamodeldataset

QUESTION 4

In most large Splunk environments, what is the most efficient command that can be used to group events by fields/

A. join

B. stats

C. streamstats

D. transaction

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Abouttransactions In other cases, it\\'s usually better to use the stats command, which performs more efficiently, especially in a distributed environment. Often there is a unique ID in the events and stats can be used.

QUESTION 5

What will you learn from the results of the following search?

sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

A. The average time elapsed during each transaction for all transactions

B. The average time for each event within each transaction

C. The average time between each transaction

Correct Answer: A

SPLK-1002 VCE Dumps | SPLK-1002 Study Guide | SPLK-1002 Exam Questions