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 statement is true?

A. Pivot is used for creating datasets.

B. Data models are randomly structured datasets.

C. Pivot is used for creating reports and dashboards.

D. In most cases, each Splunk user will create their own data model.

Correct Answer: C

The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

QUESTION 2

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 3

Which one of the following statements about the search command is true?

A. It does not allow the use of wildcards.

B. It treats field values in a case-sensitive manner.

C. It can only be used at the beginning of the search pipeline.

D. It behaves exactly like search strings before the first pipe.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcomm and

The search command is used to filter or refine your search results based on a search string that matches the events2. The search command behaves exactly like search strings before the first pipe, which means that you can use the same syntax and operators as you would use in the initial part of your search2. Therefore, option D is correct, while options A, B and C are incorrect because they are not true statements about the search command.

QUESTION 4

Field aliases are used to _____ data

A. clean

B. transform

C. calculate

D. normalize

Correct Answer: D

QUESTION 5

When can a pipe follow a macro?

A. A pipe may always follow a macro.

B. The current user must own the macro.

C. The macro must be defined in the current app.

D. Only when sharing is set to global for the macro.

Correct Answer: A

A macro is a way to save a segment of a search string as a variable and reuse it in other searches2. A macro can be followed by a pipe, which is a symbol that separates commands in a search pipeline2. A pipe may always follow a macro, regardless of who owns the macro, where the macro is defined or how the macro is shared2. For example, if you have a macro called us_sales that returns events from the US region, you can use it in a search like this: us_sales | stats sum (price) by product2. This search will use the macro to filter the events and then calculate the total price for each product2. Therefore, option A is correct, while options B, C and D are incorrect because they are not conditions that affect whether a pipe can follow a macro.