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

The eval command \\'if\\' function requires the following three arguments (in order):

A. Boolean expression, result if true, result if false

B. Result if true, result if false, boolean expression

C. Result if false, result if true, boolean expression

D. Boolean expression, result if false, result if true

Correct Answer: A

Explanation: The eval command `if\\' function requires the following three arguments (in order): boolean expression, result if true, result if false. The eval command is a search command that allows you to create new fields or modify existing fields by performing calculations or transformations on them. The eval command can use various functions to perform different operations on fields. The `if\\' function is one of the functions that can be used with the eval command to perform conditional evaluations on fields. The `if\\' function takes three arguments: a boolean expression that evaluates to true or false, a result that will be returned if the boolean expression is true, and a result that will be returned if the boolean expression is false. The `if\\' function returns one of the two results based on the evaluation of the boolean expression.

QUESTION 2

In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

A. Selected-Fields

B. Non-Matches

C. Non-Extractions

D. Matches

Correct Answer: B

Explanation: The Field Extractor Utility (FX) is a tool that helps you extract fields from your events using a graphical interface or by manually editing the regular expression2. The FX has a button that displays events that do not contain extracted fields, which is the Non- Matches button2. The Non-Matches button shows you the events that do not match the regular expression that you have defined for your field extraction2. This way, you can check if your field extraction is accurate and complete2. Therefore, option B is correct, while options A, C and D are incorrect because they are not buttons that display events that do not contain extracted fields.

QUESTION 3

A field alias is created where field1--fieid2 and the Overwrite Field Values checkbox is selected.

What happens if an event only contains values for fieid1?

A. field2 values are removed from the events.

B. field1 and field2 values are merged.

C. field2 values are unchanged.

D. field2 values are replaced with the value of the field1.

Correct Answer: D

The correct answer is D. field2 values are replaced with the value of the field1.

A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used

to rename fields for clarity or convenience1.

When you create a field alias in Splunk Web, you can select the Overwrite Field Values option to change the behavior of the field alias. This option affects how the Splunk software handles situations where the original field has no value or

does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field2.

If you select the Overwrite Field Values option, the following rules apply:

If the original field does not exist or has no value in an event, the alias field is removed from that event.

If the original field and the alias field both exist in an event, the value of the alias field is replaced with the value of the original field. If you do not select the Overwrite Field Values option, the following rules apply:

If the original field does not exist or has no value in an event, the alias field is unchanged in that event.

If the original field and the alias field both exist in an event, both fields are retained with their respective values.

Therefore, if you create a field alias where field1--field2 and select the Overwrite Field Values option, and an event only contains values for field1, then the value of field2 will be replaced with the value of field1.

References:

About calculated fields

About field aliases Create field aliases in Splunk Web

QUESTION 4

Which of the following statements about tags is true?

A. Tags are case insensitive.

B. Tags are created at index time.

C. Tags can make your data more understandable.

D. Tags are searched by using the syntax tag: :

Correct Answer: C

Explanation: Tags are aliases or alternative names for field values in Splunk. They can make your data more understandable by using common or descriptive terms instead of cryptic or technical terms. For example, you can tag a field value such as "200" with "OK" or "success" to indicate that it is a HTTP status code for a successful request. Tags are case sensitive, meaning that "OK" and "ok" are different tags. Tags are created at search time, meaning that they are applied when you run a search on your data. Tags are searched by using the syntax tag::, where is the name of the tag you want to search for.

QUESTION 5

When using the timechart command, how can a user group the events into buckets based on time?

A. Using the span argument.

B. Using the duration argument.

C. Using the interval argument.

D. Adjusting the fieldformat options.

Correct Answer: A