SPLK-1002Q&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.pass2lead.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

How many ways are there to access the Field Extractor Utility?

A. 3

B. 4

C. 1

D. 5

Correct Answer: A

QUESTION 2

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.

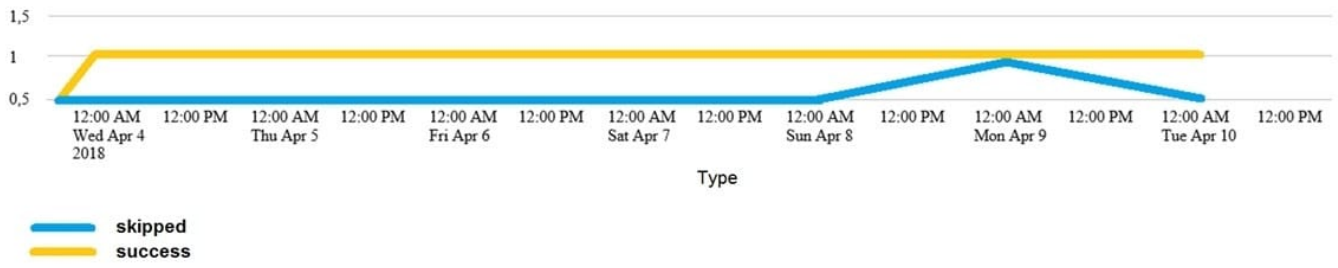
D. Only when sharing is set to global for the macro.

Correct Answer: A

Explanation: 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.

QUESTION 3

Which of the following searches would create a graph similar to the one below?



A. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states

B. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time

C. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status

D. None of these searches would generate a similart graph.

Correct Answer: C

Explanation: The following search would create a graph similar to the one below:

index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status

The search does the following:

It uses index_internal to specify the internal index that contains Splunk logs and metrics.

It uses sourcetype=Savesplunker to filter events by the sourcetype that indicates the Splunk Enterprise Security app.

It uses fields sourcetype, status to keep only the sourcetype and status fields in the events.

It uses transaction status maxspan=1d to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction.

It uses timechart count by status to create a time-based chart that shows the count of transactions for each status value over time.

The graph shows the following:

It is a line graph with two lines, one yellow and one blue. The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018. The y-axis is labeled with numbers from 0 to 15. The yellow line represents "shipped" and the blue line

represents "success". The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.

The graph is titled "Type".

Therefore, option C is the correct answer.

QUESTION 4

When would a user select delimited field extractions using the Field Extractor (FX)?

A. When a log file has values that are separated by the same character, for example, commas.

B. When a log file contains empty lines or comments.

C. With structured files such as JSON or XML.

D. When the file has a header that might provide information about its structure or format.

Correct Answer: A

The correct answer is A. When a log file has values that are separated by the same character, for example, commas.

The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions1. The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them1. The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds1. Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions. The other options are not correct because they are not suitable for the delimited field extraction method. These options are:

B. When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or

include some unwanted values.

C. With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions2. The delimited

method might not work well with this type of data, as it might not recognize the nested structure or the special characters.

D. When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data,

as it might not be able to identify the fields based on the header information.

References:

Build field extractions with the field extractor Configure indexed field extraction

QUESTION 5

What is the correct format for naming a macro with multiple arguments?

A. monthly_sales(argument 1, argument 2, argument 3)

B. monthly_sales(3)

C. monthly_sales[3]

D. monthly_sales[argument 1, argument 2, argument 3)

Correct Answer: C

Explanation: The correct format for naming a macro with multiple arguments is monthly_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are

separated by commas when calling the macro, such as monthly_sales[region,salesperson,date].