SPLK-1002$^{\text{Q\&As}}$

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

QUESTION 1

Which of these search strings is NOT valid:

A. index=web status=50* | chart count over host, status

B. index=web status=50* | chart count over host by status

C. index=web status=50* | chart count by host, status

Correct Answer: A

Explanation: This search string is not valid: index=web status=50* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

QUESTION 2

Which of the following searches will return all clientip addresses that start with 108?

A. ... | where like (clientip, "108.%)

B. ... | where (clientip, "108. %")

C. ... | where (clientip=108. %)

D. ... | search clientip=108

Correct Answer: A

QUESTION 3

Which of the following statements describes the use of the Filed Extractor (FX)?

A. The Field Extractor automatically extracts all field at search time.

B. The Field Extractor uses PERL to extract field from the raw events.

C. Field extracted using the Extracted persist as knowledge objects.

D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Correct Answer: C

Explanation: The Field Extractor (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 allows you to create field extractions that persist as knowledge objects, which are entities that you create to add knowledge to your data and make it easier to search and analyze2. Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. When you create a field extraction using the FX, you can save it as a knowledge object that applies to your data at search time2. You can also manage and share your field extractions with other users in your organization2. Therefore, option C is correct, while options A, B and D are incorrect because they do not describe the use of the FX.

QUESTION 4

Which are valid ways to create an event type? (select all that apply)

A. By using the searchtypes command in the search bar.

B. By editing the event_type stanza in the props.conf file.

C. By going to the Settings menu and clicking Event Types > New.

D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Correct Answer: CD

Explanation: Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error, success, login, logout, etc. Event types can also be used to create

transactions, alerts, reports, dashboards, etc. Event types can be created in two ways:

By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type.

By selecting an event in search results and clicking Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on

the selected event.

Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event_type stanza in the transforms.conf file, not the props.conf

file.

QUESTION 5

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