SPLK-1002 Q&As

Splunk Core Certified Power User

QUESTION 1

What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

A. There is a limit to the number of fields that can be extracted.

B. The user is unable to preview the extractions.

C. The extraction is added at index time.

D. The user is unable to return to the automatic field extraction workflow.

Correct Answer: A

QUESTION 2

Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search

A. Evenrches would return a report of sales by state.

B. Events will be returned from the data model named Application_State.

C. Events will be returned from the data model named All_Application_state.

D. No events will be returned because the pipe should occur after the datamodel command

Correct Answer: B

The search string below returns events from the data model named Application_State.

| datamodel Application_State All_Application_State search The search string does the following:

It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model. It specifies the name of the data model as

Application_State. This is a predefined data model in Splunk that contains information about web applications. It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from

all child datasets. It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.

QUESTION 3

When creating a Search workflow action, which field is required?

A. Search string

B. Data model name

C. Permission setting

D. An eval statement

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowacti on

A workflow action is a link that appears when you click an event field value in your search results2. A workflow action can open a web page or run another search based on the field value2. There are two types of workflow actions: GET and POST2. A GET workflow action appends the field value to the end of a URI and opens it in a web browser2. A POST workflow action sends the field value as part of an HTTP request to a web server2. When creating a Search workflow action, which is a type of GET workflow action that runs another search based on the field value, the only required field is the search string2. The search string defines the search that will be run when the workflow action is clicked2. Therefore, option A is correct, while options B, C and D are incorrect because they are not required fields for creating a Search workflow action.

QUESTION 4

Which of the following statements describes the command below (select all that apply)

Sourcetype=access_combined | transaction JSESSIONID

A. An additional filed named maxspan is created.

B. An additional field named duration is created.

C. An additional field named eventcount is created.

D. Events with the same JSESSIONID will be grouped together into a single event.

Correct Answer: BCD

The command sourcetype=access_combined | transaction JSESSIONID does three things:

It filters the events by the sourcetype access_combined, which is a predefined sourcetype for Apache web server logs.

It groups the events by the field JSESSIONID, which is a unique identifier for each user session.

It creates a single event from each group of events that share the same JSESSIONID value. This single event will have some additional fields created by the transaction command, such as duration, eventcount, and startime.

Therefore, the statements B, C, and D are true.

QUESTION 5

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

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