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

Splunk Core Certified Power User

QUESTION 1

Which of the following statements about data models and pivot are true? (select all that apply)

A. They are both knowledge objects.

B. Data models are created out of datasets called pivots.

C. Pivot requires users to input SPL searches on data models.

D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Correct Answer: D

Explanation: Data models and pivot are both knowledge objects in Splunk that allow you to analyze and visualize your data in different ways. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivot is a user interface that allows you to create data visualizations that present different aspects of a data model. Pivot does not require users to input SPL searches on data models, but rather lets them select options from menus and forms. Data models are not created out of datasets called pivots, but rather pivots are created from datasets in data models.

QUESTION 2

which of the following commands are used when creating visualizations(select all that apply.)

A. Geom

B. Choropleth

C. Geostats

D. iplocation

Correct Answer: ACD

The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are: geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions. geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters. iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

QUESTION 3

Which of the following examples would use a POST workflow action?

A. Perform an external IP lookup based on a domain value found in events.

B. Use the field values in an HTTP error event to create a new ticket in an external system.

C. Launch secondary Splunk searches that use one or more field values from selected events.

D. Open a web browser to look up an HTTP status code.

Correct Answer: B

The correct answer is B. Use the field values in an HTTP error event to create a new ticket in an external system.

A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create HTML links, generate HTTP POST requests, or launch secondary searches based

on field values1. There are three types of workflow actions that can be set up using Splunk Web: GET, POST, and Search2.

GET workflow actions create typical HTML links to do things like perform Google searches on specific values or run domain name queries against external WHOIS databases2.

POST workflow actions generate an HTTP POST request to a specified URI. This action type enables you to do things like creating entries in external issue management systems using a set of relevant field values2. Search workflow actions

launch secondary searches that use specific field values from an event, such as a search that looks for the occurrence of specific combinations of ipaddress and http_status field values in your index over a specific time range2.

Therefore, the example that would use a POST workflow action is B. Use the field values in an HTTP error event to create a new ticket in an external system. This example requires sending an HTTP POST request to the URI of the external

system with the field values from the event as arguments.

The other examples would use different types of workflow actions. These examples are:

A. Perform an external IP lookup based on a domain value found in events: This example would use a GET workflow action to create a link to an external IP lookup service with the domain value as a parameter.

C. Launch secondary Splunk searches that use one or more field values from selected events: This example would use a Search workflow action to run another Splunk search with the field values from the event as search terms. D. Open a web browser to look up an HTTP status code: This example would also use a GET workflow action to create a link to a web page that explains the meaning of the HTTP status code. References: Splexicon:Workflowaction About workflow actions in Splunk Web

QUESTION 4

The limit attribute will___________.

A. override default of 10

B. only work with top command

C. override default of 20

D. override default of 15

Correct Answer: A

QUESTION 5

If there are fields in the data with values that are " " or empty but not null, which of the following would add a value?

A. | eval notNULL = if(isnull (notNULL), "0" notNULL)

B. | eval notNULL = if(isnull (notNULL), "0"

C. | eval notNULL = "" | nullfill value=0 notNULL

D. | eval notNULL = "" fillnull value=0 notNULL

Correct Answer: D

The correct answer is D. | eval notNULL = "" fillnull value=0 notNULL

Option A is incorrect because it is missing a comma between the "0" and the notNULL in the if function. The correct syntax for the if function is if (condition, true_value, false_value).

Option B is incorrect because it is missing the false_value argument in the if function. The correct syntax for the if function is if (condition, true_value, false_value).

Option C is incorrect because it uses the nullfill command, which only replaces null values, not empty strings. The nullfill command is equivalent to fillnull value=null. Option D is correct because it uses the eval command to assign an empty

string to the notNULL field, and then uses the fillnull command to replace the empty string with a zero. The fillnull command can replace any value with a specified replacement, not just null values.

Latest SPLK-1002 Dumps SPLK-1002 PDF Dumps SPLK-1002 Braindumps