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.geekcert.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

When should you use the transaction command instead of the scats command?

A. When you need to group on multiple values.

B. When duration is irrelevant in search results. .

C. When you have over 1000 events in a transaction.

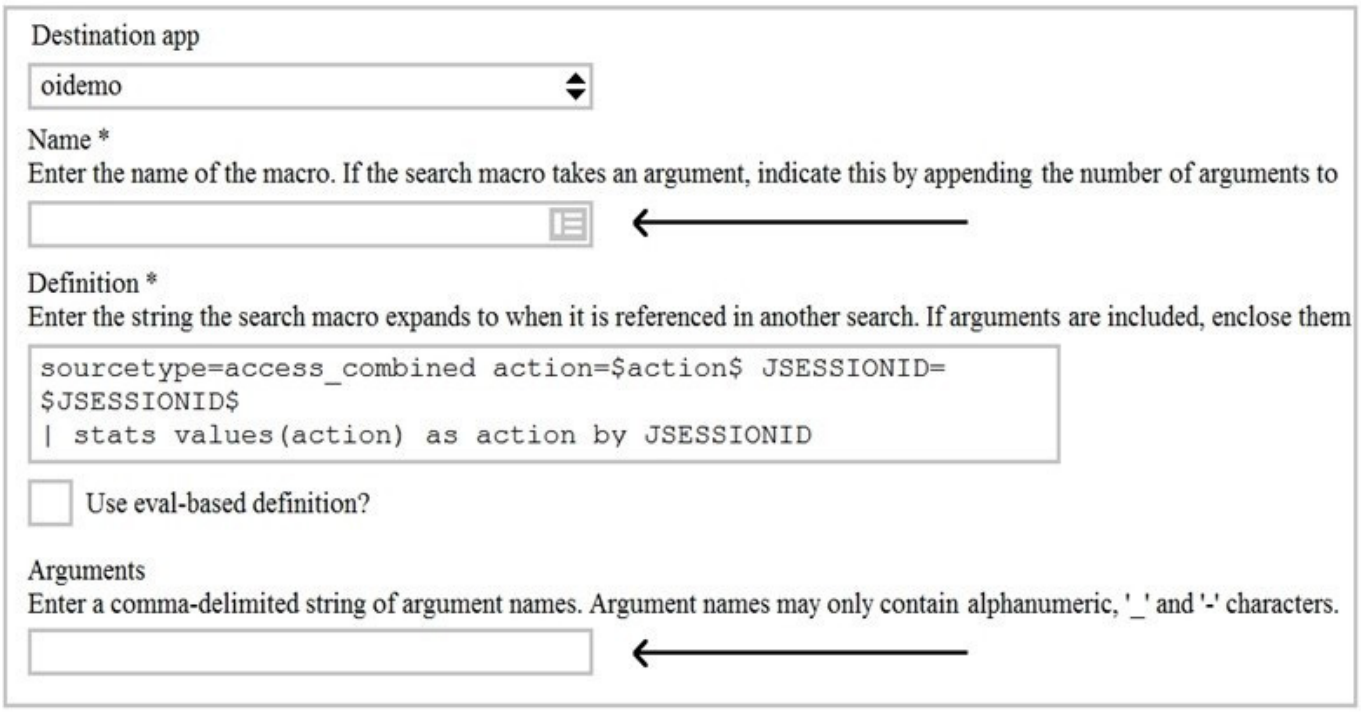
D. When you need to group based on start and end constraints.

Correct Answer: D

The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command can also specify start and end constraints for the transactions, such as a field value that indicates the beginning or the end of a transaction. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command cannot group events based on start and end constraints, but only on fields or time buckets. Therefore, the transaction command should be used instead of the stats command when you need to group events based on start and end constraints.

QUESTION 2

Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



A. The macro name is sessiontracker and the arguments are action, JESSIONID.

B. The macro name is sessiontracker(2) and the arguments are action, JESSIONID.

C. The macro name is sessiontracker and the arguments are $action$, $JESSIONID$.

D. The macro name is sessiontracker(2) and the Arguments are $action$, $JESSIONID$.

Correct Answer: B

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros

The macro definition below shows a macro that tracks user sessions based on two arguments: action and JSESSIONID.

sessiontracker(2)

The macro definition does the following:

It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string. It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when

it is executed.

It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them. In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.

Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.

QUESTION 3

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 4

Which workflow action type performs a secondary search?

A. POST

B. Drilldown

C. GET

D. Search

Correct Answer: D

The correct answer is D. Search.

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 workflow action type that performs a secondary search is Search. References: Splexicon:Workflowaction About workflow actions in Splunk Web

QUESTION 5

Which field extraction method should be selected for comma-separated data?

A. Regular expression

B. Delimiters

C. eval expression

D. table extraction

Correct Answer: B

The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation1. The other options are incorrect because they are not suitable for comma- separated data. The regular expression method works best with

unstructured event data, where you select and highlight one or more fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation23 .