[Mar-2025 Study resources for the Valid SPLK-1002 Braindumps! [Q48-Q63

[Mar-2025] Study resources for the Valid SPLK-1002 Braindumps!
Updated SPLK-1002 Tests Engine pdf - All Free Dumps Guaranteed!

QUESTION 48

To create a tag, which of the following conditions must be met by the user?
* Identify at least one field:value pair.
* Have the Power role at a minimum.
* Be able to edit the sourcetype the tag applies to.
* Must have the tag capability associated with their user role.

To create a tag, the user must have the tag capability associated with their user role. The tag capability allows

the user to create, edit, and delete tags. The user does not need to identify a field:value pair, have the Power

role, or be able to edit the sourcetype the tag applies to.ReferencesSee Define and manage tags in Settings and

[About capabilities] in the Splunk Documentation.

QUESTION 49

Which of the following is the correct way to use the datamodelcommand to search fields in the Webdata model within the Webdataset?
* | datamodel Web Web search | fields Web*
* | search datamodel Web Web | fields Web*
* | datamodel Web Web fields | search Web*
* datamodel=Web | search Web | fields Web*

QUESTION 50

Which of the following transforming commands can be used with transactions?

chart, timechart, stats, eventstats

chart, timechart, stats, diff

chart, timeehart, datamodel, pivot

chart, timecha:t, stats, pivot
* chart, timechart, stats, eventstats.
Transforming commands are commands that change the format of the search results into a table or a chart. They can be used to perform statistical calculations, create visualizations, or manipulate data in various ways1.

Transactions are groups of events that share some common values and are related in some way. Transactions can be defined by using the transaction command or by creating a transaction type in the transactiontypes.conf file2.

Some transforming commands can be used with transactions to create tables or charts based on the transaction fields. These commands include:

chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics3.

timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers4.

stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields5.

eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.

These commands can be applied to transactions by using the transaction fields as arguments. For example, if you have a transaction type named “login” that groups events based on the user field and has fields such as duration and eventcount, you can use the following commands with transactions:

| chart count by user : This command creates a table or a chart that shows how many transactions each user has.

| timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.

| stats sum(eventcount) as total_events by user : This command creates a table that shows the total number of events for each user across all transactions.

| eventstats avg(duration) as avg_duration : This command adds a new field named avg_duration to each transaction that shows the average duration of all transactions.

The other options are not valid because they include commands that are not transforming commands or cannot be used with transactions. These commands are:

diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.

datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.

pivot: This command creates a pivot report, which is a way to analyze data from a data model using a graphical interface. It is not a transforming command and it does not work with transactions.

Explanation:

The correct answer is

Reference:

About transforming commands

About transactions

chart command overview

timechart command overview

stats command overview

[eventstats command overview]

[diff command overview]

[datamodel command overview]

[pivot command overview]

QUESTION 51

Select this in the fields sidebar to automatically pipe you search results to the rare command
* events with this field
* rare values
* top values by time
* top values

QUESTION 52

Which of the following expressions could be used to create a calculated field called gigabytes?
* eval sc_bytes(1024/1024)
* | eval negabytes=sc_bytes(1024/1024)
* megabytes=sc_bytes(1024/1024)
* sc_bytas(1024/1024)

QUESTION 53

Which of these stats commands will show the total bytes for each unique combination of page and server?
* index=web | stats sum (bytes) BY page BY server
* index=web | stats sum (bytes) BY page server
* index=web | stats sum(bytes) BY page AND server
* index=web | stats sum(bytes) BY values (page) values (server)

The correct command to show the total bytes for each unique combination of page and server is index=web | stats sum (bytes) BY page server. In Splunk, the stats command is used to calculate aggregate statistics over the dataset, such as count, sum, avg, etc. When using the BY clause, it groups the results by the specified fields. The correct syntax does not include commas or the word ‘AND’ between the field names. Instead, it simply lists the field names separated by spaces within the BY clause.

Reference:

The usage of the stats command with the BY clause is confirmed by examples in the Splunk Community, where it’s explained that stats with a by foo bar will output one row for every unique combination of the by fields1.

QUESTION 54

What is the correct way to name a macro with two arguments?
* us_sales2
* us_sales(1,2)
* us_sale,2
* us_sales(2)

QUESTION 55

The fields sidebar does not show_____. (Select all that apply.)
* interesting fields
* selected fields
* all extracted fields

QUESTION 56

Complete the search, …. | _____ failure>successes
* Search
* Where
* If
* Any of the above

Explanation

The where command can be used to complete the search below.

… | where failure>successes

The where command is a search command that allows you to filter events based on complex or custom criteria.

The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.

The search string below does the following:

It uses … to represent any search criteria or commands before the where command.

It uses the where command to filter events based on a comparison between two fields: failure and successes.

It uses the greater than operator (>) to compare the values of failure and successes fields for each event.

It only keeps events where failure is greater than successes.

QUESTION 57

Which of the following statements describes the use of the Filed Extractor (FX)?
* The Field Extractor automatically extracts all field at search time.
* The Field Extractor uses PERL to extract field from the raw events.
* Field extracted using the Extracted persist as knowledge objects.
* Fields extracted using the Field Extractor do not persist and must be defined for each search.
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 58

Which workflow action method can be used the action type is set to link?
* GET
* PUT
* Search
* UPDATE
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction Define a GET workflow action Steps

* Navigate to Settings > Fields > Workflow Actions.

* Click New to open up a new workflow action form.

* Define a Label for the action.

The Label field enables you to define the text that is displayed in either the field or event workflow menu. Labels can be static or include the value of relevant fields.

* Determine whether the workflow action applies to specific fields or event types in your data.

Use Apply only to the following fields to identify one or more fields. When you identify fields, the workflow action only appears for events that have those fields, either in their event menu or field menus. If you leave it blank or enter an asterisk the action appears in menus for all fields.

Use Apply only to the following event types to identify one or more event types. If you identify an event type, the workflow action only appears in the event menus for events that belong to the event type.

* For Show action in determine whether you want the action to appear in the Event menu, the Fields menus, or Both.

* Set Action type to link.

* In URI provide a URI for the location of the external resource that you want to send your field values to.

Similar to the Label setting, when you declare the value of a field, you use the name of the field enclosed by dollar signs.

Variables passed in GET actions via URIs are automatically URL encoded during transmission. This means you can include values that have spaces between words or punctuation characters.

* Under Open link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.

* Set the Link method to get.

* Click Save to save your workflow action definition.

QUESTION 59

Which group of users would most likely use pivots?
* Users
* Architects
* Administrators
* Knowledge Managers

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

QUESTION 60

Which are valid ways to create an event type? (select all that apply)
* By using the searchtypes command in the search bar.
* By editing the event_type stanza in the props.conf file.
* By going to the Settings menu and clicking Event Types > New.
* By selecting an event in search results and clicking Event Actions > Build Event Type.

QUESTION 61

Which of the following statements about tags is true?
* Tags are case insensitive.
* Tags can make your data more understandable.
* Tags are created at index time.
* Tags are searched by using the syntax tag :: <fieldname>.

Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .

Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or tag the value 404 as not_found .

QUESTION 62

Which of the following statements describes field aliases?
* Field alias names replace the original field name.
* Field aliases can be used in lookup file definitions.
* Field aliases only normalize data across sources and sourcetypes.
* Field alias names are not case sensitive when used as part of a search.

Field aliases are alternative names for fields in Splunk. Field aliases can be used to normalize data across different sources and sourcetypes that have different field names for the same concept. For example, you can create a field alias for src_ip that maps to clientip, source_address, or any other field name that represents the source IP address in different sourcetypes. Field aliases can also be used in lookup file definitions to map fields in your data to fields in the lookup file. For example, you can use a field alias for src_ip to map it to ip_address in a lookup file that contains geolocation information for IP addresses. Field alias names do not replace the original field name, but rather create a copy of the field with a different name. Field alias names are case sensitive when used as part of a search, meaning that src_ip and SRC_IP are different fields.

QUESTION 63

Highlighted search terms indicate _____ search results in Splunk.
* Display as selected fields.
* Sorted
* Charted based on time
* Matching