Vendor: Splunk

Exam Code:SPLK-1002

Exam Name: Splunk Core Certified Power User

Version: Demo

QUESTION 1

In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")

A. The description field would contain no value.

B. The description field would contain the value 0.

C. The description field would contain the value "Internal Server Error".

D. This statement would produce an error in Splunk because it is incomplete.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctio ns

---

QUESTION 2

For the following search, which field populates the x-axis?

index=security sourcetype=linux secure | timechart count by action

A. action

B. source type

C. _time

D. time

Correct Answer: C

Explanation: The correct answer is C. _time.

The timechart command creates a time series chart with corresponding table of statistics, with time used as the X-axis1. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart1. In this case,

the split-by field is action, which means that the chart will have different lines for different actions, such as accept, reject, or fail2. The count function will calculate the number of events for each action in each time bin1.

For example, the following image shows a timechart of the count by action for a similar search3:

As you can see, the x-axis is populated by the _time field, which represents the time range of the search. The y-axis is populated by the count function, which represents the number of events for each action. The legend shows the different

values of the action field, which are used to split the chart into different series.

Reference:

2: Timechart Command In Splunk With Example - Mindmajix 1: timechart - Splunk Documentation 3: timechart command examples - Splunk Documentation

---

QUESTION 3

Which of the following commands support the same set of functions?

A. stats, eval, table

B. search, where, eval

C. stats, chart, timechart

D. transaction, chart, timechart

Correct Answer: C

QUESTION 4

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

A. chart, timechart, stats, eventstats

B. chart, timechart, stats, diff

C. chart, timeehart, datamodel, pivot

D. chart, timecha:t, stats, pivot

Correct Answer: A

The correct answer is A. 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.

References:

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 5

What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. Creates a table of the total count of users and split by corndogs.

B. Creates a table of the total count of mysterymeat corndogs split by user.

C. Creates a table with the count of all types of corndogs eaten split by user.

D. Creates a table that groups the total number of users by vegetarian corndogs.

Correct Answer: B

Explanation: The search string below creates a table of the total count of mysterymeat corndogs split by user.

| stats count by user | where corndog=mysterymeat The search string does the following:

It uses the stats command to calculate the count of events for each value of the user field. The stats command creates a table with two columns: user and count. It uses the where command to filter the results by the value of the corndog field.

The where command only keeps the rows where corndog equals mysterymeat. Therefore, the search string creates a table of the total count of mysterymeat corndogs split by user.

QUESTION 6

A user runs the following search:

index--X sourcetype=Y I chart count (domain) as count, sum (price) as sum by product, action usenull=f useother--f

Which of the following table headers match the order this command creates?

A. The chart command does not allow for multiple statistical functions.

B. Product, sum: addtocart, sum: remove, sum: purchase, count: addtocart, count: remove, count: purchase

C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase

D. Count: product, sum: product, count: action, sum: action

Correct Answer: C

The correct answer is C. Product, count: addtocart, count: remove, count: purchase, sum:

addtocart, sum: remove, sum: purchase1.

In Splunk, the chart command is used to create a table or a chart visualization from your data2. The chart command takes at least one function and one field, and optionally another field to group by2.

In the given search, the chart command is used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action). The usenull=f and useother=f options are used to exclude null values and

other values from the chart2. The chart command creates a table with headers that match the order of the fields and functions in the command1. The headers for the count function are prefixed with count:, and the headers for the sum

function are prefixed with sum:1. The values of the product and action fields are used as the suffixes for the headers1. Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase,

sum: addtocart, sum: remove, and sum: purchase1.

QUESTION 7

Which of the following statements about event types is true? (select all that apply)

A. Event types can be tagged.

B. Event types must include a time range,

C. Event types categorize events based on a search.

D. Event types can be a useful method for capturing and sharing knowledge.

Correct Answer: ACD

Reference: https://www.edureka.co/blog/splunk-events-event-types-and-tags/

As mentioned before, an event type is a way to categorize events based on a search string that matches the events2. Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches2. Therefore, option A is correct. Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type2. Therefore, option C is correct. Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization2. Therefore, option D is correct. Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events2. Therefore, option B is incorrect.

QUESTION 8

Which of the following workflow actions can be executed from search results? (select all that apply)

A. GET

B. POST

C. LOOKUP

D. Search

Correct Answer: ABD

Explanation: As mentioned before, there are two types of workflow actions: GET and POST1. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it1. Another type of workflow action is Search, which runs another search based on the field value1. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

QUESTION 9

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

A. Both will appear in the All Fields list, but only if the alias is specified in the search.

B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.

C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.

D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Correct Answer: B

Explanation: A field alias is a way to assign an alternative name to an existing field without changing the original field name or value2. You can use field aliases to make your field names more consistent or descriptive across different sources or sourcetypes2. When you run a search without any transforming commands in Smart Mode, Splunk automatically identifies and displays interesting fields in your results2. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. If you have created a field alias based on an original field, both the original field name and the alias name will appear in the Interesting Fields list if they meet these criteria2. However, only one of them will appear in each event depending on which one you have specified in your search string2. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 10

Which of the following statements best describes a macro?

A. A macro is a method of categorizing events based on a search.

B. A macro is a way to associate an additional (new) name with an existing field name.

C. A macro is a portion of a search that can be reused in multiple place

D. A macro is a knowledge object that enables you to schedule searches for specific events.

Correct Answer: C

The correct answer is C. A macro is a portion of a search that can be reused in multiple places.

A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which

are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1. To create a macro, you need to define its name, definition, arguments, and

description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments

if any1. For example, if you have a macro named my_macro that takes one argument named object and has the following definition:

search sourcetype= object

You can use it in a search by writing:

my_macro(web)

This will expand the macro and run the following SPL code:

search sourcetype=web

The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.

The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:

A. An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports2. B. A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.

D. An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4. References: About event types About field aliases About alerts Define search macros in Settings Use search macros in searches

---

QUESTION 11

Which of the following is NOT a stats function:

A. sum

B. addtotals

C. count

D. avg

Correct Answer: B

Explanation: The stats command is used to calculate summary statistics for your search results such as count, sum, avg, min, max and more2. The stats command supports various functions that you can use to perform calculations on your fields2. However, addtotals is not a stats function but a separate command that adds a row or column with the total of the values in each group2. Therefore, option B is correct, while options A, C and D are incorrect because they are valid stats functions.

QUESTION 12

Which of the following are required to create a POST workflow action?

A. Label, URI, search string.

B. XMI attributes, URI, name.

C. Label, URI, post arguments.

D. URI, search string, time range picker.

Correct Answer: C

Explanation: POST workflow actions are custom actions that send a POST request to a web server when you click on a field value in your search results. POST workflow actions can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. One of the options that are required to create a POST workflow action is post arguments. Post arguments are key-value pairs that are sent in the body of the POST request to provide additional information to the web server. Post arguments can include field values from your data by using dollar signs around the field names.