

Splunk.SPLK-1002.v2026-09-13.q139

□□□□:	SPLK-1002
□□□□:	Splunk Core Certified Power User Exam
□□□:	Splunk
□□ □□ □□□:	139
□□:	v2026-09-13
# □□ □:	188
# □□ □□□:	1390
https://www.krdump.com/Splunk.SPLK-1002.v2026-09-13.q139.html	

NEW QUESTION: 1

Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

- A. maxspan
- B. maxduration
- C. maxpause
- D. endswith

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

Which of the following statements describes the command below (select all that apply) Sourcetype=access_combined | transaction JSESSIONID

- A. An additional field named duration is created.
- B. Events with the same JSESSIONID will be grouped together into a single event.
- C. An additional field named maxspan is created.
- D. An additional field named eventcount is created.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 3

Which of the following statements is true about the root dataset of a data model?

- A. It must contain the transaction command if it is a root transaction dataset.
- B. It can contain transforming commands as long as it is a root search dataset.
- C. It will automatically contain knowledge objects associated with the base search.
- D. It can only contain a base search with no transforming commands.

Answer: C ([LEAVE A REPLY](#))

In Splunk, a data model's root dataset is the foundational element upon which the rest of the data model is built. The root dataset can be of various types, including search, transaction, or event-based datasets. One of the key features of the root dataset is that

it automatically inherits the knowledge objects associated with its base search. These knowledge objects include field extractions, lookups, aliases, and calculated fields that are defined for the base search, ensuring that the root dataset has all necessary contextual information from the outset. This allows users to build upon this dataset with additional child datasets and objects without having to redefine the base search's knowledge objects.

NEW QUESTION: 4

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

- A. Data models are created out of datasets called pivots.
- B. Pivot allows the creation of data visualizations that present different aspects of a data model.
- C. They are both knowledge objects.
- D. Pivot requires users to input SPL searches on data models.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 5

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

- A. Choropleth
- B. Geom
- C. Geostats
- D. iplocation

Answer: B,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 6

When can a pipe follow a macro?

- A. The current user must own the macro.
- B. A pipe may always follow a macro.
- C. The macro must be defined in the current app.
- D. Only when sharing is set to global for the macro.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 7

A macro has another macro nested within it, and this inner macro requires an argument. How can the user pass this argument into the SPL?

- A. An argument can be passed through the outer macro.
- B. An argument can be passed to the outer macro by nesting parentheses.
- C. There is no way to pass an argument to the inner macro.
- D. An argument can be passed to the inner macro by nesting parentheses.

Answer: D ([LEAVE A REPLY](#))

Explanation

The correct answer is D. An argument can be passed to the inner macro by nesting parentheses.

A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain another search

macro within it, which is called a nested macro. A nested macro can also take arguments, which can be passed from the outer macro or directly from the search string.

To pass an argument to the inner macro, you need to use parentheses to enclose the argument value and separate it from the outer macro argument. For example, if you have a search macro named `outer_macro` (1) that contains another search macro named `inner_macro` (2), and both macros take one argument each, you can pass an argument to the inner macro by using the following syntax:

```
outer_macro (argument1, inner_macro (argument2))
```

This will replace the `argument1` and `argument2` with the values you provide in the search string. For example, if you want to pass "foo" as the `argument1` and "bar" as the `argument2`, you can write:

```
outer_macro ("foo", inner_macro ("bar"))
```

This will expand the macros with the corresponding arguments and run the SPL code contained in them.

References:

Search macro examples

Use search macros in searches

NEW QUESTION: 8

Which of the following is true about a datamodel that has been accelerated?

- A. They can be used with Pivot, the `| tstats` command, or the `| datamodel` command.
- B. They can still be used in the Pivot tool but only with the `accelerate_pivot` capability.
- C. They can no longer be used in the Pivot tool.
- D. They can be used with the `| tstats` command, but will only return that data which has been accelerated.

Answer: A ([LEAVE A REPLY](#))

A data model that has been accelerated can be used with Pivot, the `| tstats` command, or the `| datamodel` command (Option A). Acceleration pre-computes and stores results for quicker access, enhancing the performance of searches and analyses that utilize the data model, especially for large datasets. This makes accelerated data models highly efficient for use in various analytical tools and commands within Splunk.

NEW QUESTION: 9

Which of the following statements describes field aliases?

- A. Field alias names replace the original field name.
- B. Field aliases only normalize data across sources and sourcetypes.
- C. Field aliases can be used in lookup file definitions.
- D. Field alias names are not case sensitive when used as part of a search.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 10

To create a tag, which of the following conditions must be met by the user?

- A. Identify at least one field:value pair.
- B. Have the Power role at a minimum.
- C. Be able to edit the sourcetype the tag applies to.
- D. Must have the tag capability associated with their user role.

Answer: D ([LEAVE A REPLY](#))

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. [References](#) See Define and manage tags in Settings and [About capabilities] in the Splunk Documentation.

NEW QUESTION: 11

Using the export function, you can export a maximum of 2000 results.

- A. True
- B. False

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 12

Which command can include both an over and a by clause to divide results into sub-groupings?

- A. chart
- B. stats
- C. xyseries
- D. transaction

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/search-commands-stats-chart-and-timechart.html

NEW QUESTION: 13

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

- A. Search string
- B. Data model name
- C. Permission setting
- D. An eval statement

Answer: ([SHOW ANSWER](#))

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction>

NEW QUESTION: 14

A user runs the following search:

```
index=X sourcetype=Y | chart count (domain) as count, sum (price) as sum by product, action use null=f use other=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

Answer: ([SHOW ANSWER](#))

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

In Splunk, the `chart` command is used to create a table or a chart visualization from your data. The `chart` command takes at least one function and one field, and optionally another field to group by. 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=false` and `useOther=false` options are used to exclude null values and other values from the chart.

Therefore, the table headers created by this command are `Product,count: addtocart,count: remove,count: purchase,sum: addtocart,sum: remove, andsum: purchase1`.

Which of the following eval command functions is valid?

- Answer: ([SHOW ANSWER](#))**

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions> The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns "3.14". The other functions are not valid eval command functions.

Which search would limit an "alert" tag to the "host" field?

- Answer: B (LEAVE A REPLY)**

NEW QUESTION: 17

How can an existing accelerated data model be edited?

- A. An accelerated data model can be edited once its .tsidx file has expired.
- B. An accelerated data model can be edited from the Pivot tool.
- C. The data model must be de-accelerated before edits can be made to its structure.
- D. It cannot be edited. A new data model would need to be created.

Answer: C ([LEAVE A REPLY](#))

An existing accelerated data model can be edited, but the data model must be de-accelerated before any structural edits can be made (Option C). This is because the acceleration process involves pre-computing and storing data, and changes to the data model's structure could invalidate or conflict with the pre-computed data. Once the data model is de-accelerated and edits are completed, it can be re-accelerated to optimize performance.

NEW QUESTION: 18

When using | timechart by host, which field is represented in the x-axis?

- A. host
- B. _time
- C. time
- D. date

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 19

Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. Configuration of GET workflow actions includes choosing a sourcetype.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. GET workflow actions can be configured to open the URT link in the current window or in a new window

Answer: D ([LEAVE A REPLY](#))

GET workflow actions are custom actions that open a URL link when you click on a field value in your search results. GET workflow actions can be configured with various options, such as label name, base URL, URI parameters, app context, etc. One of the options is to choose whether to open the URL link in the current window or in a new window. GET workflow actions do not have to be configured with POST arguments, as they use GET method to send requests to web servers. Configuration of GET workflow actions does not include choosing a sourcetype, as they do not generate any data in Splunk. Label names for GET workflow actions must include a field name surrounded by dollar signs, as this indicates the field value that will be used to replace the variable in the URL link.

NEW QUESTION: 20

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

- A. | Search datamodel web web | filed web*
- B. Datamodel=web | search web | filed web*
- C. | datamodel web web field | search web*
- D. | datamodel web search | filed web *

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 21

For the following search, which command would further filter for only IP addresses present more than five times?

- A. index=games | stats count as IP_count by IP B. | where IP_count > 5
- B. index=games | search IP_Count > 5
- C. index=games | where IP > 5
- D. index=games | search IP > 5

Answer: A ([LEAVE A REPLY](#))

To filter for only IP addresses that appear more than five times in the search results for index=games, you can use a combination of the stats and where commands. The stats command counts the occurrences of each IP address and assigns the count to IP_count. The where command then filters the results to include only those IP addresses with a count greater than five.

Here is how the complete search would look:

```
index=games | stats count as IP_count by IP | where IP_count > 5
```

References:

- * Splunk Docs: stats command
- * Splunk Docs: where command
- * Splunk Answers: Filtering results using stats and where commands

NEW QUESTION: 22

Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

- A. Authentication
- B. Authorization
- C. Access
- D. Accounting

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 23

Which of the following statements describe calculated fields? (Choose all that apply.)

- A. Calculated fields can be used in the search bar.
- B. Calculated fields can be based on an extracted field.
- C. Calculated fields can only be applied to host and sourcetype.
- D. Calculated fields are shortcuts for performing calculations using the evalcommand.

Answer: (SHOW ANSWER)

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields>

NEW QUESTION: 24

This function of the stats command allows you to identify the number of values a field has.

- A. distinct_count
- B. fields

- C. max
- D. count

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 25

A calculated field maybe based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

Answer: B ([LEAVE A REPLY](#))

Explanation

As mentioned before, a calculated field is a field that you create based on the value of another field or fields². A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

NEW QUESTION: 26

A Splunk app is configured to extract domain names in web service logs and specify them as a field named domain. What workflow action would return an external IP lookup for the field named domain?

- A. POST
- B. PUT
- C. GET
- D. Search

Answer: C ([LEAVE A REPLY](#))

In Splunk, a workflow action that returns an external IP lookup for a field named domain would typically use the GET method. This HTTP method is used to retrieve data from a specified resource, which is appropriate for looking up information based on the domain field.

Reference:

Splunk Docs: Define workflow actions

Splunk Answers: Workflow actions for external lookups

NEW QUESTION: 27

Where are the results of eval commands stored?

- A. In a field.
- B. In an index.
- C. In a KV Store.
- D. In a database.

Answer: A ([LEAVE A REPLY](#))

Explanation

<https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval> The eval command calculates an expression and puts the resulting value into a search results field.

* If the field name that you specify does not match a field in the output, a new field is added to the search results.

* If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION: 28

In this search, _____ will appear on the y-axis. SEARCH: sourcetype=access_combined status!=200 | chart count over host

A. status

B. host

C. count

Answer: ([SHOW ANSWER](#))

In this search, count will appear on the y-axis². This search uses the chart command to create a chart of the count of events over host for events that have status not equal to 2002. The chart command creates a table with one column for each value of the field after the over clause and one row for each value of the field after the by clause (if any)². The values in the table are calculated by applying the function before the over clause to the events in each group². In this case, the chart command creates a table with one column for each host and one row for the count of events for each host. The y-axis of the chart shows the values of the count function applied to each host. Therefore, option C is correct, while options A and B are incorrect because they appear on the x-axis or as labels of the chart.

NEW QUESTION: 29

When creating a POST workflow action, what can a user define as the POST arguments?

A. Static text only

B. A combination of static text and field value pairs

C. A combination of field value pairs and the search query

D. Field value pairs only

Answer: ([SHOW ANSWER](#))

POST workflow actions allow parameters to contain both fixed values and values substituted from event fields.

Extract: "POST arguments can include static text, field value substitutions, or a combination of both."

NEW QUESTION: 30

Which of the following statements about tags is true? (select all that apply.)

A. Tags are designed to make data more understandable.

B. Tags are based on field/value pairs.

C. Tags are case-insensitive.

D. Tags categorize events based on a search.

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 31

What are the two parts of a root event dataset?

- A. Fields and variables.
- B. Fields and attributes.
- C. Constraints and fields.
- D. Constraints and lookups.

Answer: C (LEAVE A REPLY)

Explanation/Reference: <https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects>

SPLK-1002                            

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

The line of SPL used to join the tables is: | join employeeNumber type=outer How many rows are returned in the new table?

- A. Zero
- B. Five
- C. Eight
- D. Three

Answer: C ([LEAVE A REPLY](#))

When performing an outer join in Splunk using the | join employeeNumber type=outer command, it combines the rows from both tables based on the employeeNumber field. An outer join returns all rows from both tables, with matching rows from both sides where available. If there is no match, the result is NULL on the side of the join where there is no match.

In the provided tables, there are five rows in the first table and three in the second. Since it's an outer join, all rows from both tables will be returned. This means the new table will have a total of eight rows, combining the matched rows and the unmatched rows from both tables.

References:

Splunk Documentation on the join command.

Splunk Community discussions on the usage of join and types of joins.

NEW QUESTION: 35

Which of the following data models are included in the Splunk Common Information Model (CIM) add-on?

(select all that apply)

- A. User permissions
- B. Alerts
- C. Databases

D. Email

Answer: B,C,D ([LEAVE A REPLY](#))

The Splunk Common Information Model (CIM) add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and `__raw__` `__raw__` `__raw__`. CIM `__raw__` `__raw__` `__raw__` `__raw__`.
`__raw__`, `__raw__`, `__raw__` `__raw__` 22 `__raw__` `__raw__` `__raw__` `__raw__`. `__raw__` `__raw__` `__raw__` `__raw__`.
CIM `__raw__`.`__raw__` `__raw__`: Splunk `__raw__` `__raw__` `__raw__` `__raw__` `__raw__` Splunk `__raw__`
`__raw__` `__raw__` `__raw__` - `__raw__` `__raw__` `__raw__` `__raw__` `__raw__`.

NEW QUESTION: 36

For choropleth maps,splunk ships with the following KMZ files (select all that apply)

- A. Countries of the World
- B. States of the United States
- C. States and provinces of the united states and Canada
- D. Countries of the European Union

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 37

What does the fillnull command replace null values with, if the value argument is not specified?

- A. 0
- B. N/A
- C. NaN
- D. NULL

Answer: A ([LEAVE A REPLY](#))

Reference:<https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specifying-a-field.html>

The fillnull command is a search command that replaces null values with a specified value or 0 if no value is specified. Null values are values that are missing, empty, or undefined in Splunk. The fillnull command can replace null values for all fields or for specific fields. The fillnull command can take an optional argument called value that specifies the value to replace null values with. If no value argument is specified, the fillnull command will replace null values with 0 by default.

NEW QUESTION: 38

In which of the following scenarios is an event type more effective than a saved search?

- A. When a search should always include the same time range.
- B. When a search needs to be added to other users' dashboards.
- C. When the search string needs to be used in future searches.
- D. When formatting needs to be included with the search string.

Answer: D ([LEAVE A REPLY](#))

Reference:<https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html>

NEW QUESTION: 39

Which statement is true?

- A. Pivot is used for creating datasets.
- B. Data models are randomly structured datasets.
- C. Pivot is used for creating reports and dashboards.
- D. In most cases, each Splunk user will create their own data model.

Answer: C ([LEAVE A REPLY](#))

Explanation

The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

NEW QUESTION: 40

Which of the following statements describe the search below? (select all that apply) Index=main | transaction clientip host maxspan=30s maxpause=5s

- A. Events in the transaction occurred within 5 seconds.
- B. It groups events that share the same clientip and host.
- C. The first and last events are no more than 5 seconds apart.
- D. The first and last events are no more than 30 seconds apart.

Answer: (SHOW ANSWER)

The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction.

index=main | transaction clientip host maxspan=30s maxpause=5s

The search does the following:

It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.

It uses the transaction command to group events into transactions based on two fields: clientip and host. The transaction command creates new events from groups of events that share the same clientip and host values.

It specifies the start and end constraints for the transactions using the maxspan and maxpause arguments. The maxspan argument sets the maximum time span between the first and last events in a transaction. The maxpause argument sets the maximum time span between any two consecutive events in a transaction. In this case, the maxspan is 30 seconds and the maxpause is 5 seconds, meaning that any transaction that has a longer time span or pause will be split into multiple transactions. It creates some additional fields for each transaction, such as duration, eventcount, starttime, etc. The duration field shows the time span between the first and last events in a transaction.

NEW QUESTION: 41

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

- A. lookup
- B. inputlookup

Answer: (SHOW ANSWER)

NEW QUESTION: 42

A field alias is created where field1-field2 and the Overwrite Field Values checkbox is selected.

What happens if an event only contains values for field1?

- A. field2 values are removed from the events.
- B. field1 and field2 values are merged.
- C. field2 values are unchanged.
- D. field2 values are replaced with the value of the field1.

Answer: D ([LEAVE A REPLY](#))

The correct answer is D. field2 values are replaced with the value of the field1.

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 convenience¹.

When you create a field alias in Splunk Web, you can select the Overwrite Field Values option to change the behavior of the field alias. This option affects how the Splunk software handles situations where the original field has no value or does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field².

If you select the Overwrite Field Values option, the following rules apply:

If the original field does not exist or has no value in an event, the alias field is removed from that event.

If the original field and the alias field both exist in an event, the value of the alias field is replaced with the value of the original field.

If you do not select the Overwrite Field Values option, the following rules apply:

If the original field does not exist or has no value in an event, the alias field is unchanged in that event.

If the original field and the alias field both exist in an event, both fields are retained with their respective values.

Therefore, if you create a field alias where field1=field2 and select the Overwrite Field Values option, and an event only contains values for field1, then the value of field2 will be replaced with the value of field1.

References:

About calculated fields

About field aliases

Create field aliases in Splunk Web

NEW QUESTION: 43

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

- A. chart, timechart, stats, eventstats
- B. chart, timechart, stats, diff
- C. chart, timechart, datamodel, pivot
- D. chart, timechart, stats, pivot

Answer: A ([LEAVE A REPLY](#))

Explanation

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](#)

[\[eventstats command overview\]](#)

[\[diff command overview\]](#)

[\[datamodel command overview\]](#)

[\[pivot command overview\]](#)

NEW QUESTION: 44

A POST workflow action will pass which types of arguments to an external website?

- A.** Clear text only.
- B.** A mix of clear text strings and variables.
- C.** It can only send raw event data.
- D.** Variables only.

Answer: B (LEAVE A REPLY)

A POST workflow action in Splunk is designed to send data to an external web service by using HTTP POST requests. This type of workflow action can pass a combination of clear text strings and variables derived from the search results or event data. The clear text strings might include static text or predefined values, while the variables are dynamic elements that represent specific fields or values extracted from the Splunk events. This flexibility allows for constructing detailed and context-specific requests to external systems, enabling various integration and automation scenarios. The POST request can include both types of data, making it versatile for different use cases.

NEW QUESTION: 45

When a search returns _____, you can view the results as a list.

- A. transactions
- B. a list of events
- C. statistical values

Answer: C (LEAVE A REPLY)

NEW QUESTION: 46

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

- A.** Tabs
B. Pipes
C. Spaces
D. Commas

Answer: (SHOW ANSWER)

Reference:<https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep>

The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. The FX can detect some common delimiters automatically, such as pipes (|), spaces (), commas (,), semicolons (;), etc. The FX cannot detect tabs (t) as delimiters automatically, but you can specify them manually in the FX interface.

SPLK-1002      DumpTop    SPLK-1002 ! DumpTop   **SPLK-1002**     
    , DumpTop SPLK-1002               
  DumpTop SPLK-1002   . <https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (315 Q&As
Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 47

Which of the following statements describes the use of the Field Extractor (FX)?

- A. The Field Extractor automatically extracts all field at search time.
- B. The Field Extractor uses PERL to extract field from the raw events.
- C. Field extracted using the Extracted persist as knowledge objects.
- D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Answer: C ([LEAVE A REPLY](#))

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.

NEW QUESTION: 48

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 49

When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

- A. Tabs
- B. Pipes
- C. Colons
- D. Spaces

Answer: A,B,D ([LEAVE A REPLY](#))

Reference:

<https://community.splunk.com/t5/Splunk-Search/Field-Extraction-Separate-on-Colon/m-p/29751>

NEW QUESTION: 50

When using a field value variable with a Workflow Action, which punctuation mark will escape the data

- A. *
- B. !
- C. ^
- D. #

Answer: B ([LEAVE A REPLY](#))

When using a field value variable with a Workflow Action, the exclamation mark (!) will escape the data. A Workflow Action is a custom action that performs a task when you click on a field value in your search results. A Workflow Action can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. A field value variable is a placeholder for the field value that will be used to replace the variable in the URL or post argument of the Workflow Action. A field value variable is written as fieldname, where field_name is the name of the field whose value will be used. However, if the field value contains special characters that need to be escaped, such as spaces, commas, etc., you can use the exclamation mark (!) before and after the field value variable to escape the data. For example, if you have a field value variable host, you can write it as !\$host! to escape any special characters in the host field value. Therefore, option B is the correct answer.

NEW QUESTION: 51

Which of the following commands will show the maximum bytes?

- A. sourcetype=access_* | stats max(bytes)
- B. sourcetype=access_* | maximum totals by bytes
- C. sourcetype=access_* | avg (bytes)
- D. sourcetype=access_* | max(bytes)

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 52

Select this in the fields sidebar to automatically pipe you search results to the rare command

- A. rare values
- B. events with this field
- C. top values
- D. top values by time

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 53

Which search string would only return results for an event type called successful_purchases?

- A. tag=successful_purchases
- B. Event Type:: successful purchases
- C. successful_purchases
- D. event type-successful_purchases

Answer: C ([LEAVE A REPLY](#))

Explanation

This is because event types are added to events as a field named eventtype, and you can use this field as a search term to find events that match a specific event type. For example, eventtype=successful_purchases returns all events that have been categorized as successful purchases by the event type definition. The other options are incorrect because they either use a different field name (tag), a different syntax (Event Type:: or event type-), or have a typo (successful_purchases). You can learn more about how to use event types in searches from the Splunk documentation¹.

NEW QUESTION: 54

Which of the following statements describes macros?

- A. A macro is a reusable search string that must contain the full search.
- B. A macro is a reusable search string that must have a fixed time range.
- C. A macro is a reusable search string that may have a flexible time range.
- D. A macro is a reusable search string that must contain only a portion of the search.

Answer: ([SHOW ANSWER](#))

Explanation

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros>

NEW QUESTION: 55

A space is an implied _____ in a search string.

- A. OR
- B. AND
- C. ()
- D. NOT

Answer: B ([LEAVE A REPLY](#))

Explanation

A space is an implied AND in a search string, which means that it acts as a logical operator that returns events that match both terms on either side of the space². For example, status=200 method=GET will return events that have both status=200 and method=GET². Therefore, option B is correct, while options A, C and D are incorrect because they are not implied by a space in a search string.

NEW QUESTION: 56

Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

- A. Field alias
- B. Event types
- C. Search workflow action
- D. Tags

Answer: ([SHOW ANSWER](#))

The correct answer is A. Field alias¹²³.

In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field³. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)¹².

The CIM provides a methodology for normalizing values to a common field name¹. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact². By using field aliases, you can map vendor fields to common fields that are the same for each data source in a given domain⁴. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention¹.

NEW QUESTION: 57

Which Knowledge Object does the Splunk Common Information Model (CIM) use to normalize data, in addition to field aliases, event types, and tags?

- A. Macros
- B. Lookups
- C. Workflow actions
- D. Field extractions

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime>

NEW QUESTION: 58

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

Destination app
oidemo

Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

```
sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONID$  
| stats values(action) as action by JSESSIONID
```

☐ Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

- A. The macro name is sessiontracker and the arguments are \$action\$, \$JSESSIONID\$.
- B. The macro name is sessiontracker(2) and the Arguments are \$action\$, \$JSESSIONID\$.
- C. The macro name is sessiontracker and the arguments are action, JSESSIONID.
- D. The macro name is sessiontracker(2) and the arguments are action, JSESSIONID.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 59

Data model are composed of one or more of which of the following datasets? (select all that apply.)

- A. Events datasets
- B. Search datasets
- C. Transaction datasets
- D. Any child of event, transaction, and search datasets

Answer: A,B,C ([LEAVE A REPLY](#))

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels>

NEW QUESTION: 60

Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

- A. CIM is a methodology for normalizing data.
- B. CIM can correlate data from different sources.
- C. The Knowledge Manager uses the CIM to create knowledge objects.
- D. CIM is an app that can coexist with other apps on a single Splunk deployment.

Answer: A,B,C ([LEAVE A REPLY](#))

Reference: <https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview> The Common Information Model (CIM) is a methodology for normalizing data from different sources and making it easier to analyze and report on it³. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more³. One of the statements that describe the CIM is that it is a methodology for normalizing data, which means that it provides a standard way to name and structure data from different sources so that they can be compared and correlated³.

Therefore, option A is correct. Another statement that describes the CIM is that it can correlate data from different sources, which means that it enables you to run searches and reports across data from different sources that share common fields and tags³.

Therefore, option B is correct. Another statement that describes the CIM is that the Knowledge Manager uses the CIM to create knowledge objects, which means that the person who is responsible for creating and managing knowledge objects such as data models, field aliases, tags and event types can use the CIM as a guide to make their knowledge objects consistent and compatible with other apps and add-ons³. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.

NEW QUESTION: 61

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

Destination app

oidemo

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

```
sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONID$ | stats values(action) as action by JSESSIONID
```

☐ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

- A.** The macro name is sessiontracker and the arguments are action, JSESSIONID.
- B.** The macro name is sessiontracker(2) and the arguments are action, JSESSIONID.
- C.** The macro name is sessiontracker and the arguments are \$action\$, \$JSESSIONID\$.
- D.** The macro name is sessiontracker(2) and the Arguments are \$action\$, \$JSESSIONID\$.

Answer: B (LEAVE A REPLY)

Reference:

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

SPLK-1002         DumpTop     SPLK-1002  ! DumpTop   **SPLK-1002**       

NEW QUESTION: 62

When using the Field Extractor (FX) to perform a field extraction, which delimiter can be used?

- A.** A period or comma.
- B.** A comma.
- C.** A tab or space.
- D.** Any consistent character.

Answer: D ([LEAVE A REPLY](#))

When using the Field Extractor (FX) in Splunk to perform field extraction, any consistent character can be used as a delimiter. The Field Extractor allows users to define how fields are separated in the raw event data, and as long as the delimiter is consistent, the FX tool can parse and extract the fields correctly.

Reference:

Splunk Docs: Field Extractor

Splunk Answers: Field extraction delimiters

NEW QUESTION: 63

Using the export function, you can export search results as _____. (Select all that apply)

- A.** Xml
B. Json
C. Html
D. A php file

Answer: A,B (LEAVE A REPLY)

Using the export function, you can export search results as XML or JSON2. The export function allows you to save your search results in a structured format that can be used by other applications or tools2. You can use the output_mode parameter to specify whether you want to export your results as XML or JSON2. Therefore, options A and B are correct, while options C and D are incorrect because they are not formats that you can export your search results as.

NEW QUESTION: 64

Which of the following statements about tags is true? (select all that apply.)

- A. Tags are case-insensitive.
- B. Tags are based on field/value pairs.
- C. Tags categorize events based on a search.
- D. Tags are designed to make data more understandable.

Answer: ([SHOW ANSWER](#))

Explanation

The following statements about tags are true: tags are based on field/value pairs and tags categorize events based on a search. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. Tags can be used to filter or analyze your data based on common concepts or themes. Tags can be created by using various methods, such as search commands, configuration files, user interfaces, etc. Some of the characteristics of tags are:

Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called "alert" for the field name "status" and the field value "critical". This means that only events that have status=critical will have the "alert" tag applied to them.

Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called "web" for the search string sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the "web" tag applied to them.

The following statements about tags are false: tags are case-insensitive and tags are designed to make data more understandable. Tags are case-sensitive and tags are designed to make data more searchable. Tags are case-sensitive: This means that tags must match the exact case of the field name and field value that they are associated with. For example, if you create a tag called "alert" for the field name "status" and the field value "critical", it will not apply to events that have status=CRITICAL or Status=critical. Tags are designed to make data more searchable: This means that tags can help you find relevant events or patterns in your data by using common concepts or themes. For example, if you create a tag called "web" for the search string sourcetype=access_combined, you can use tag=web to find all events related to web activity.

NEW QUESTION: 65

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.

Answer: B ([LEAVE A REPLY](#))

Explanation

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>

NEW QUESTION: 66

This is what Splunk uses to categorize the data that is being indexed.

- A. Index
- B. Host
- C. Sourcetype
- D. Source

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 67

A search contains example(100,200). What is the name of the macro?

- A. example(2)
- B. example(var1,var2)
- C. example(\$,\$)
- D. example[2]

Answer: B ([LEAVE A REPLY](#))

In Splunk, macros that accept arguments are defined with placeholders for those arguments in the format example(var1, var2). In the search example(100,200), "100" and "200" are the values passed for var1 and var2 respectively.

References:

Splunk Docs - Macros

NEW QUESTION: 68

When can a pipe follow a macro?

- A. A pipe may always follow a macro.
- B. The current user must own the macro.
- C. The macro must be defined in the current app.
- D. Only when sharing is set to global for the macro.

Answer: A ([LEAVE A REPLY](#))

Explanation

A macro is a way to save a segment of a search string as a variable and reuse it in other searches². A macro can be followed by a pipe, which is a symbol that separates commands in a search pipeline². A pipe may always follow a macro, regardless of who owns the macro, where the macro is defined or how the macro is shared². For example, if you have a macro called us_sales that returns events from the US region, you can use it in a search like this: us_sales | stats sum(price) by product². This search will use the macro to filter the events and then calculate the total price for each product². Therefore, option A is correct, while options B, C and D are incorrect because they are not conditions that affect whether a pipe can follow a macro.

NEW QUESTION: 69

Which of the following actions can the eval command perform?

- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

Answer: B (LEAVE A REPLY)

The eval command is used to create new fields or modify existing fields based on an expression2. The eval command can perform various actions such as calculations, conversions, string manipulations and more2. One of the actions that the eval command can perform is to create or replace an existing field with a new value based on an expression2. For example, | eval status=if(status="200","OK","ERROR") will create or replace the status field with either OK or ERROR depending on the original value of status2. Therefore, option B is correct, while options A, C and D are incorrect because they are not actions that the eval command can perform.

NEW QUESTION: 70

Which one of the following statements about the search command is true?

- A. It behaves exactly like search strings before the first pipe.
- B. It can only be used at the beginning of the search pipeline.
- C. It does not allow the use of wildcards.
- D. It treats field values in a case-sensitive manner.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 71

Two separate results tables are being combined using the |join command. The outer table has the following values:
Refer to following Tables

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

The line of SPL used to join the tables is: | join employeeNumber type=outer How many rows are returned in the new table?

- A. Zero

- B. Five
- C. Eight
- D. Three

Answer: C ([LEAVE A REPLY](#))

When performing an outer join in Splunk using the `| join employeeNumber type=outer` command, it combines the rows from both tables based on the `employeeNumber` field. An outer join returns all rows from both tables, with matching rows from both sides where available. If there is no match, the result is NULL on the side of the join where there is no match.

In the provided tables, there are five rows in the first table and three in the second. Since it's an outer join, all rows from both tables will be returned. This means the new table will have a total of eight rows, combining the matched rows and the unmatched rows from both tables.

References:

- * Splunk Documentation on the join command.
- * Splunk Community discussions on the usage of join and types of joins.

NEW QUESTION: 72

When using a split series on a chart, the series MUST be displayed using the STACKED option.

- A. True
- B. False

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 73

Which of the following describes the Splunk Common Information Model (CIM) add-on?

- A. The CIM add-on uses machine learning to normalize data.
- B. The CIM add-on contains dashboards that show how to map data.
- C. The CIM add-on contains data models to help you normalize data.
- D. The CIM add-on is automatically installed in a Splunk environment.

Answer: C ([LEAVE A REPLY](#))

The Splunk Common Information Model (CIM) add-on is a Splunk app that contains data models to help you normalize data from different sources and formats. The CIM add-on defines a common and consistent way of naming and categorizing fields and events in Splunk. This makes it easier to correlate and analyze data across different domains, such as network, security, web, etc. The CIM add-on does not use machine learning to normalize data, but rather relies on predefined field names and values. The CIM add-on does not contain dashboards that show how to map data, but rather provides documentation and examples on how to use the data models. The CIM add-on is not automatically installed in a Splunk environment, but rather needs to be downloaded and installed from Splunkbase.

NEW QUESTION: 74

Which workflow action type performs a secondary search?

- A. Search
- B. Drilldown
- C. GET

D. POST

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 75

Which of the following can be saved as an event type?

A. index=server_472 sourcetype=BETA_494 code=488 [! inputlookup append=t servercode.csv]

B. index=server_472 sourcetype=BETA_494 code=488

C. index-server_472 sourcetype-BETA_494 code=488 | stats count by code

D. index=server_472 sourcetype=BETA_494 code=488 | stats where code > 200

Answer: B ([LEAVE A REPLY](#))

Event types in Splunk are saved searches that categorize data, making it easier to search for specific patterns or criteria within your data. When saving an event type, the search must essentially filter events based on criteria without performing operations that transform or aggregate the data. Here's a breakdown of the options:

A). The search index=server_472 sourcetype=BETA_494 code=488 | stats count by code performs an aggregation operation (stats count by code), which makes it unsuitable for saving as an event type. Event types are meant to categorize data without aggregating or transforming it.

B). The search index=server_472 sourcetype=BETA_494 code=488 [| inputlookup append=t servercode.csv] includes a subsearch and input lookup, which is typically used to enrich or filter events based on external data.

This complexity goes beyond simple event categorization.

C). The search index=server_472 sourcetype=BETA_494 code=488 | stats where code > 200 includes a filtering condition within a transforming command (stats), which again, is not suitable for defining an event type due to the transformation of data.

D). The search index=server_472 sourcetype=BETA_494 code=488 is the correct answer as it purely filters events based on index, sourcetype, and a code field condition without transforming or aggregating the data.

This is what makes it suitable for saving as an event type, as it categorizes data based on specific criteria without altering the event structure or content.

NEW QUESTION: 76

What are the expected results for a search that contains the command | where A=B?

A. Events that contain the string value where A=B.

B. Events that contain the string value A=B.

C. Events where values of field A are equal to values of field B.

D. Events where field A contains the string value B.

Answer: ([SHOW ANSWER](#))

The correct answer is C. Events where values of field A are equal to values of field B.

The where command is used to filter the search results based on an expression that evaluates to true or false.

The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions¹.

The syntax for the where command is:

| where <expression>

The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.

| where $A=B$

The other options are not correct because they use different syntax or fields that are not related to the where command. These options are:

B). Events that contain the string value A=B: This option uses the string value A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text "A=B" in them.

References:

Search command cheatsheet

NEW QUESTION: 77

A. constantly running in the background

Answer: A ([LEAVE A REPLY](#))

Which of the following statements describes macros?

B. A macro is a reusable search string that may have a flexible time range.

D. A macro is a reusable search string that must contain only a portion of the search.

Answer: ([SHOW ANSWER](#))

A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that

can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

NEW QUESTION: 79

Which of the following statements describe data model acceleration? (Choose all that apply.)

- A. Root events cannot be accelerated.
- B. Accelerated data models cannot be edited.
- C. Private data models cannot be accelerated.
- D. You must have administrative permissions or the accelerate_datamodelcapability to accelerate a data model.

Answer: B,D ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 80

Which of the following searches show a valid use of a macro? (Choose all that apply.)

- A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField
- B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField
- C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
- D. index=main source=mySource oldField=* | ""newField('makeMyField(oldField)')"" | table _time newField

Answer: (SHOW ANSWER)

Explanation

The searches A and C show a valid use of a macro. A macro is a reusable piece of SPL code that can be called by using single quotes ("). A macro can take arguments, which are passed inside parentheses after the macro name. For example, 'makeMyField(oldField)' calls a macro named makeMyField with an argument oldField. The searches B and D are not valid because they use double quotes ("") instead of single quotes (").

NEW QUESTION: 81

Two separate results tables are being combined using the join command. The outer table has the following values:

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

The line of SPL used to join the tables is: join employeeNumber type=outer How many rows are returned in the new table?

- A. Three
- B. Eight
- C. Five
- D. Zero

Answer: C ([LEAVE A REPLY](#))

In this case, the outer join is applied, which means that all rows from the outer (left) table will be included, even if there are no matching rows in the inner (right) table. The result will include all five rows from the outer table, with the matched data from the inner table where employeeNumber matches. Rows without matching employeeNumber values will have null values for the fields from the inner table.

References:

Splunk Documentation - Join Command

NEW QUESTION: 82

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

- A. Regular expression
- B. Delimiters
- C. eval expression
- D. table extraction

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 83

Which SPL query will group results that occur within 15 seconds of each other by user and host?

- A. index=firewall | transaction user host span=15s
- B. index=firewall | stats count by _time host user maxspan=15s
- C. index=firewall | stats count by _time host user span=15s
- D. index=firewall | transaction user host maxspan=15s

Answer: D ([LEAVE A REPLY](#))

The transaction command groups related events based on shared field values. The maxspan argument specifies the maximum time span allowed between the earliest and latest events in a transaction.

Extract: "Use the maxspan argument to specify the maximum duration of a transaction. Events that exceed this time span are not grouped into the same transaction." Therefore, transaction user host maxspan=15s groups events by user and host only when they occur within 15 seconds of each other.

NEW QUESTION: 84

In which of the following scenarios is an event type more effective than a saved search?

- A. When the search string needs to be used in future searches.
- B. When a search needs to be added to other users' dashboards.

- C. When formatting needs to be included with the search string.
- D. When a search should always include the same time range.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 85

This role is required to install the CIM Add-on.

Select your answer.

- A. USER
- B. ADMIN
- C. POWER

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 86

What do events in a transaction have in common?

- A. All events in a transaction must have the same timestamp.
- B. All events in a transaction must have the same sourcetype.
- C. All events in a transaction must have the exact same set of fields.
- D. All events in a transaction must be related by one or more fields.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions>

NEW QUESTION: 87

Which search retrieves events with the event type web_errors?

- A. tag=web_errors
- B. eventtype=web_errors
- C. eventtype "web errors"
- D. eventtype (web_errors)

Answer: B ([LEAVE A REPLY](#))

Explanation

The correct answer is B. eventtype=web_errors.

An event type is a way to categorize 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 reports¹.

To search for events that have a specific event type, you need to use the eventtype field with the name of the event type as the value. The syntax for this is:

eventtype=<event_type_name>

For example, if you want to search for events that have the event type web_errors, you can use the following syntax:

eventtype=web_errors

This will return only the events that match the search criteria defined by the web_errors event type.

The other options are not correct because they use different syntax or fields that are not related to event types.

These options are:

A: tag=web_errors: This option uses the tag field, which is a way to add descriptive keywords to events based on field values. Tags are different from event types, although they can be used together. Tags can be used to filter and group events by common characteristics².

C: eventtype "web errors": This option uses quotation marks around the event type name, which is not valid syntax for the eventtype field. Quotation marks are used to enclose phrases or exact matches in a search³.

D: eventtype (web_errors): This option uses parentheses around the event type name, which is also not valid syntax for the eventtype field. Parentheses are used to group expressions or terms in a search³.

References:

About event types

About tags

Search command cheatsheet

NEW QUESTION: 88

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

- A. Label, URI, search string.
- B. XML attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 89

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

- A. Spaces
- B. Commas
- C. Tabs
- D. Pipes

Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 90

Where are the results of eval commands stored?

- A. In a field.
- B. In an index.
- C. In a KV Store.
- D. In a database.

Answer: A (LEAVE A REPLY)

<https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval>

The eval command calculates an expression and puts the resulting value into a search results field. If the field name that you specify does not match a field in the output, a new field is added to the search results.

If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION: 91

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

- A. Geom
- B. Choropleth
- C. Geostats
- D. iplocation

Answer: A,C,D (LEAVE A REPLY)

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.

SPLK-1002                         

NEW QUESTION: 92

After manually editing a regular expression (regex), which of the following statements is true?

- A.** Changes made manually can be reverted in the Field Extractor (FX) UI.
- B.** It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C.** It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.

D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Answer: ([SHOW ANSWER](#))

Explanation

NEW QUESTION: 93

These kinds of charts represent a series in a single bar with multiple sections

- A.** Multi-Series
- B.** Split-Series
- C.** Omit nulls
- D.** Stacked

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 94

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

- A.** Weight
- B.** Priority
- C.** Rank
- D.** Precedence

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 95

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

- A.** GET
- B.** POST
- C.** LOOKUP
- D.** Search

Answer: A,B,D ([LEAVE A REPLY](#))

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.

NEW QUESTION: 96

Which of the following is included with the Common Information Model (CIM) add-on?

- A.** Search macros
- B.** Event category tags
- C.** Workflow actions
- D.** tsidx files

Answer: B ([LEAVE A REPLY](#))

The correct answer is B. Event category tags. This is because the CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest.

Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category. You can learn more about event category tags from the Splunk documentation¹². The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

NEW QUESTION: 97

Which two file formats are supported by the Splunk Maps app? (Choose two.)

- A. GeoJSON
- B. KML and KMZ
- C. JSON and XML
- D. CSV and XLS

Answer: A,D (LEAVE A REPLY)

The Splunk Maps app is a web-based application that allows you to visualize data from Splunk searches. It supports two file formats for map data: GeoJSON and KML/KMZ. GeoJSON is a standard format for encoding geographic data structures. KML (Keyhole Markup Language) is an XML-based format for describing geographic data. KMZ (Keyhole Markup Language ZIP) is a compressed version of KML files. The Splunk Maps app can load and display data from both GeoJSON and KML/KMZ files. It also provides a user interface for interacting with the data, such as zooming, panning, and filtering.

Example 1: To load a KMZ file into the Splunk Maps app, you can use the following command in the Splunk Search bar:

```
search us_states.kmz
```

Example 2: To load a GeoJSON file into the Splunk Maps app, you can use the following command in the Splunk Search bar:

```
search world_countries.geojson
```

The Splunk Maps app also supports loading data from external sources, such as web services and databases. It provides a user interface for configuring these data sources and for interacting with the data. For more information about the Splunk Maps app, see the Splunk documentation.

NEW QUESTION: 98

What are the two parts of a root event dataset?

- A. Fields and variables.
- B. Fields and attributes.
- C. Constraints and fields.
- D. Constraints and lookups.

Answer: (SHOW ANSWER)

Reference: <https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects> A root event dataset is the base dataset for a data model that defines the source or sources of the data and the constraints and fields that apply to the data¹. A root event dataset has two parts: constraints and fields¹. Constraints are filters that limit the data to a specific index, source, sourcetype, host or search string¹. Fields are the attributes that describe the data and can be extracted, calculated or looked up¹.

Therefore, option C is correct, while options A, B and D are incorrect.

NEW QUESTION: 99

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

- A. | datamodel web search | filed web *
- B. | Search datamodel web web | filed web*
- C. | datamodel web web field | search web*
- D. Datamodel=web | search web | filed web*

Answer: A ([LEAVE A REPLY](#))

The data model command allows you to run searches on data models that have been accelerated¹. The syntax for using the data model command is | datamodel <model_name> <dataset_name> [search <search_string>]¹.

Therefore, option A is the correct way to use the data model command to search fields in the data model within the web dataset.

Options B and C are incorrect because they do not follow the syntax for the data model command. Option D is incorrect because it does not use the data model command at all.

NEW QUESTION: 100

Which of these search strings is NOT valid:

- A. index=web status=50* | chart count by host, status
- B. index=web status=50* | chart count over host, status
- C. index=web status=50* | chart count over host by status

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 101

If a search returns _____ it can be viewed as a chart.

- A. timestamps
- B. statistics
- C. events
- D. keywords

Answer: (SHOW ANSWER)

If a search returns statistics, it can be viewed as a chart². Statistics are tabular data that show the relationship between two or more fields². You can create statistics by using commands such as stats, chart or timechart². You can view statistics as a chart by selecting the Visualization tab in the Search app and choosing a chart type such as column, line or pie². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of data that can be viewed as a chart.

NEW QUESTION: 102

Which type of visualization shows relationships between discrete values in three dimensions?

- A. Pie chart
- B. Line chart
- C. Bubble chart
- D. Scatter chart

Answer: C ([LEAVE A REPLY](#))

<https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub>

NEW QUESTION: 103

Which of the following is the correct way to use the datamodelcommand to search fields in the Webdata model within the Webdataset?

- A. datamodel=Web | search Web | fields Web*
- B. | search datamodel Web Web | fields Web*
- C. | datamodel Web Web fields | search Web*
- D. | datamodel Web Web search | fields Web*

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 104

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2),
"commas") | eval USD="$" + tostring(USD, "commas")
```

☐ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

A. Convert_sales (euro, €, 79)"

- D. Convert_sales (\$euro, \$€\$, \$,79\$)**

Answer: B (LEAVE A REPLY)

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros> The correct way to execute the macro in a search string is to use the format `macro_name($arg1$, $arg2$, ...)` where `$arg1$`, `$arg2$`, etc. are the arguments for the macro. In this case, the macro name is `convert_sales` and it takes three arguments: currency, symbol, and rate. The arguments are enclosed in dollar signs and separated by commas. Therefore, the correct way to execute the macro is `convert_sales($euro$, $€$, .79)`.

NEW QUESTION: 105

How does a user display a chart in stack mode?

- A.** By using the stack command.
- B.** By turning on the Use Trellis Layout option.
- C.** By changing Stack Mode in the Format menu.
- D.** You cannot display a chart in stack mode, only a timechart.

Answer: ([SHOW ANSWER](#))

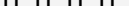
A chart is a graphical representation of your search results that shows the relationship between two or more fields². You can display a chart in stack mode by changing the Stack Mode option in the Format menu². Stack mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series². Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

NEW QUESTION: 106

Which of the following searches will return all clientip addresses that start with 108?

- A.** ... | where like (clientip, "108.% ")
- B.** ... | where (clientip, "108. %")
- C.** ... | where (clientip=108. %)
- D.** ... | search clientip=108

Answer: A (LEAVE A REPLY)

SPLK-1002  DumpTop  SPLK-1002 ! DumpTop  **SPLK-1002** 
 , DumpTop SPLK-1002   .   
  DumpTop SPLK-1002  . <https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (315 Q&As
Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 107

What are the expected search results from executing the following SPL command?

index=network NOT StatusCode=200

- A.** Every event in the network index that does not have a value in this field.
- B.** Every event in the network index that does not contain a StatusCode of 200 and excluding events that do not have a value in this field.
- C.** Every event in the network index that does not contain a StatusCode of 200, including events that do not have a value in this field.
- D.** No results as the syntax is incorrect, the != field expression needs to be used instead of the NOT operator.

Answer: C ([LEAVE A REPLY](#))

In Splunk, the NOT operator is used to exclude events from your search results. The search index=network NOT StatusCode=200 will return all events in the 'network' index where the StatusCode is not 200. This includes events where the StatusCode field is present and has a value other than 200, as well as events where the StatusCode field is not present at all. Reference:

The use of the NOT operator in SPL (Search Processing Language) is consistent with the information provided in the Splunk documentation and resources, which describe how to generate efficient searches and make the most of Splunk's capabilities

NEW QUESTION: 108

To which of the following can a field alias be applied?

- A.** Data found in a lookup table.
- B.** Either a calculated field or an extracted field.
- C.** Only one single field in a dataset.
- D.** A given host, source, or sourcetype.

Answer: B ([LEAVE A REPLY](#))

In Splunk, a field alias is used to create an alternative name for an existing field, making it easier to refer to data in a consistent manner across different searches and reports. Field aliases can be applied to both calculated fields and extracted fields. Calculated fields are those that are created using eval expressions, while extracted fields are typically those parsed from the raw data at index time or search time. This flexibility allows users to streamline their searches by using more intuitive field names without altering the underlying data. Field aliases cannot be applied to data in a lookup table, specific individual fields within a dataset, or directly to a host, source, or sourcetype.

NEW QUESTION: 109

Which of the following statements describes macros?

- A.** A macro is a reusable search string that must contain the full search.
- B.** A macro is a reusable search string that must have a fixed time range.
- C.** A macro is a reusable search string that may have a flexible time range.
- D.** A macro is a reusable search string that must contain only a portion of the search.

Answer: (SHOW ANSWER)

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros>

NEW QUESTION: 110

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A.** Fast

C. C. Verbose

Explanation

NEW QUESTION: 111

A. Custom visualizations

C. Fields and event category tags

Answer: B,C (LEAVE A REPLY)

Explanation

NEW QUESTION: 112

A. index=main source=mySource oldField=* |'makeMyField(oldField)' ☐☐☐ ☐☐ newField

```
C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)' | table _time
newField
```

D. `index=main source=mySource oldField=* | "newField('makeMyField(oldField))'" | table time newField`

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 113

When using| timechart by host, which field is represented in the x-axis?

- A. date
- B. host
- C. time
- D. _time

Answer: C ([LEAVE A REPLY](#))

Reference:<https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart>

NEW QUESTION: 114

Which of the following eval command functions is valid?

- A. int()
- B. count()
- C. print()
- D. tostring()

Answer: D ([LEAVE A REPLY](#))

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions> The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns "3.14". The other functions are not valid eval command functions.

NEW QUESTION: 115

What field must be present in order to use the timechart command?

- A. _raw
- B. rime
- C. _time
- D. index

Answer: C ([LEAVE A REPLY](#))

The timechart command in Splunk requires the _time field to be present in the dataset because it uses time as the primary axis for charting data. The _time field represents the time of events and is essential for commands that generate visualizations based on time, such as timechart. This command groups the events into time intervals and performs statistical functions on those time intervals. Without the _time field, the timechart command will not function properly.

Reference:

Splunk Docs - timechart command

NEW QUESTION: 116

The time range specified for a historical search defines the _____.-----questionable on ans

- A. Amount of data shown on the timeline as data streams in
- B. Amount of data fetched from index matching that time range
- C. Time range for the static results

Answer: (SHOW ANSWER)

Explanation

The time range specified for a historical search defines the amount of data fetched from the index matching that time range². A historical search is a search that runs over a fixed period of time in the past². When you run a historical search, Splunk searches

the index for events that match your search string and fall within the specified time range². Therefore, option B is correct, while options A and C are incorrect because they are not what the time range defines for a historical search.

NEW QUESTION: 117

What does the following search do?

index=condlog type=mysterymeat action=eaten | stats count as cornlog_count by us:

- A. Creates a table of the total count of users and split by corndogs.
- B. Creates a table with the count of all types of corndogs eaten split by user.
- C. Creates a table that groups the total number of users by vegetarian corndogs.
- D. Creates a table of the total count of mysterymeat corndogs split by user.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 118

□□□ □□ □□:

□□□ □□□ □□□ □□□ _____ □□□ □□□.

- A. □□
- B. □□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 119

What other syntax will produce exactly the same results as | chart count over vendor_action by user?

- A. | chart count by vendor_action, user
- B. | chart count over vendor_action, user
- C. | chart count by vendor_action over user
- D. | chart count over user by vendor_action

Answer: A ([LEAVE A REPLY](#))

<https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Chart>

NEW QUESTION: 120

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B ([LEAVE A REPLY](#))

Reference:

A calculated field is a field that you create based on the value of another field or fields¹. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format¹. Calculated fields can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters, or key-value pairs¹. Therefore, option B is correct, while options A, C and D are incorrect because tags, output fields for a lookup, and fields generated from a search string are not types of extracted fields.

Data model attributes are fields that are added to a dataset from search time field extractions, calculated fields, lookups, or aliases. They can be created within the data model editor or inherited from a parent dataset. They can be edited or removed unless they are required by the data model. They can be added to any type of dataset, not just root search datasets. References See About data models, [Define data model attributes], and [Edit data model datasets] in the Splunk Documentation.

NEW QUESTION: 124

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

- A. Label, URI, search string.
- B. XML attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaPOSTworkflowaction>

NEW QUESTION: 125

What happens to the original field name when a field alias is created?

- A. The original field name is not affected by the creation of a field alias.
- B. The original field name is replaced by the field alias within the index.
- C. The original field name is italicized to indicate that it is not an alias.
- D. The original field name still exists in the index but is not visible to the user at search time.

Answer: A ([LEAVE A REPLY](#))

Creating a field alias in Splunk does not modify or remove the original field. Instead, the alias allows the same data to be accessed using a different field name without affecting the original field.

References:

Splunk Docs - Field aliases

NEW QUESTION: 126

Which statement is true?

- A. In most cases, each Splunk user will create their own data model.
- B. Data model are randomly structured datasets.
- C. Pivot is used for creating datasets.
- D. Pivot is used for creating reports and dashboards.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 127

A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being_____.

- A. skipped or deferred
- B. automatically accelerated
- C. deleted
- D. all of the above

Answer: A ([LEAVE A REPLY](#))

A report that is scheduled to run every 15 minutes but takes 17 minutes to complete is in danger of being skipped or deferred². This means that Splunk may skip some scheduled runs of the report if they overlap with previous runs that are still in progress or defer them until the previous runs are finished². This can affect the accuracy and timeliness of the report results and notifications². Therefore, option A is correct, while options B, C and D are incorrect because they are not consequences of a report taking longer than its schedule interval.

NEW QUESTION: 128

How are event types different from saved reports?

- A.** Event types cannot be used to organize data into categories.
- B.** Event types include formatting of the search results.
- C.** Event types can be shared with Splunk users and added to dashboards.
- D.** Event types do not include a time range.

Answer: D ([LEAVE A REPLY](#))

Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies.

The correct answer is D. Event types do not include a time range.

The explanation is as follows:

Event types are a categorization system that help you make sense of your data by matching events with the same search string¹.

Event types are applied to events at search time and can be used as search terms or filters¹².

Saved reports are results saved from a search action that can show statistics and visualizations of events³.

Saved reports can be run anytime, and they fetch fresh results each time they are run³⁴. Saved reports can be shared with other users and added to dashboards⁴.

The main difference between event types and saved reports is that event types do not include a time range, while saved reports do¹⁴. This means that event types can match events from any time period, while saved reports are limited by the time range specified when they are created or run¹⁴.

NEW QUESTION: 129

A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, the eval or the sort?

- A.** It doesn't matter whether eval or sort is used first.
- B.** Convert the numeric to a string with eval first, then sort.
- C.** Use sort first, then convert the numeric to a string with eval.
- D.** You cannot use the sort command and the eval command on the same field.

Answer: C ([LEAVE A REPLY](#))

The eval command is used to create new fields or modify existing fields based on an expression². The sort command is used to sort the results by one or more fields in ascending or descending order². If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings².

This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

NEW QUESTION: 130

Which of the following statements is true, especially in large environments?

- A. Use the transaction command when you want to see the results of a calculation.
- B. Use the stats command when you next to group events by two or more fields.
- C. The transaction command is faster and more efficient than the stats command.
- D. The stats command is faster and more efficient than the transaction command

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 131

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization.

If another person in the organization runs the shared report and no results are returned, why might this be?

(Choose all that apply.)

- A. The person in the organization running the report does not have access to the index.
- B. The extraction is private.
- C. Fast mode is enabled.
- D. The dashboard is private.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 132

How are arguments defined within the macro search string?

- A. \$arg\$
- B. 'arg'
- C. %arg%
- D. "arg"

Answer: A ([LEAVE A REPLY](#))

Arguments are defined within the macro search string by using dollar signs on either side of the argument name, such as arg1 or fragment.

Reference

Search macro examples

Define search macros in Settings

Use search macros in searches

NEW QUESTION: 133

Why would the following search produce multiple transactions instead of one?

```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| state list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

Events (641) Patterns Statistics (147) Visualization

20 Per Page ▾ / Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src	num_events	total_events
107.3.146.207	1000 1000 1000 405	3405
108.65.113.83	1000 120	1120
109.169.32.135	1000 1000 79	2079
11.17.160.129	1000 1000 238	2238

- A. The maxspan option is not included.
- B. The transaction command has a limit of 1000 events per transaction.
- C. The transaction and commands cannot be used together.
- D. The stats list () function is used.

Answer: A (LEAVE A REPLY)

In Splunk, the transaction command is used to group events that share common characteristics into a single transaction¹. By default, the transaction command groups all matching events into a single transaction¹.

However, you can use the maxspan option to limit the time span of the transactions¹. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction¹.

Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value¹.

Here is an example of how you can use the maxspan option in a search:

index=main sourcetype=access_combined | transaction someuniquefield maxspan=1h In this search, the transaction command groups events that share the same someuniquefield value into a single transaction, but only if the time span between the first and last event in the transaction does not exceed 1 hour¹. If the time span exceeds 1 hour, the transaction command will start a new transaction¹.

NEW QUESTION: 134

Which of the following knowledge objects represents the output of an eval expression?

- A. Field extractions

- B. Eval fields**
C. Calculated fields
D. Calculated lookups

Answer: C (LEAVE A REPLY)

NEW QUESTION: 135

☐☐ ☐ ☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐☐☐

- A. ☐ ☐
- B. ☐ ☐ ☐ ☐ ☐
- C. ☐ ☐
- D. ☐ ☐

Answer: B (LEAVE A REPLY)

11

```
`stats` □□□□ □□ □□□ □□ □□, □□, □□, □□□, □□□ □□ □□ □□ □□□ □□□□ □ □□□□□.2
`stats` □□□□ □□□ □□ □□□ □□□□ □ □□□ □ □□ □□□ □□□ □□□□□.2 □□□ `addtotals` □
`stats` □□□ □□□ □ □□□ □ □□□ □ □□ □□ □□□□ □□□ □□□□□□.2 □□□ □□ B□ □□□□,
□□ A, C, D□ □□□ `stats` □□□□□ □□□□ □□□□.
```

NEW QUESTION: 136

These are the default selected fields.

- A.** source, sourcetype, index
B. source, sourcetype, host
C. source, sourcetype, timestamp
D. host, source, raw

Answer: (SHOW ANSWER)

SPLK-1002        DumpTop        **SPLK-1002**  
       , DumpTop SPLK-1002        .       
  DumpTop SPLK-1002        . <https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (315 Q&As
Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 137

After manually editing; a regular expression (regex), which of the following statements is true?

- A.** It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- B.** It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C.** Changes made manually can be reverted in the Field Extractor (FX) UI.
- D.** The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 138

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. The extraction is private-
- B. The person in the organization running the report does not have access to the index.
- C. The dashboard is private.
- D. Fast mode is enabled.

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 139

Given the event below, how can the value in the Zip_Code field be used to retrieve the weather from an external resource?

25/Oct/2023:20:29:43

151.162.101.143, v2.003, Zip_Code: 75510, DataCenter: DC1

- A. Create a GET workflow action
- B. Create a workflow action
- C. Create a PUT workflow action
- D. Create a Search workflow action

Answer: A ([LEAVE A REPLY](#))

Workflow actions allow interaction with external resources.

Extract: "GET workflow actions create an HTTP link using field values. Clicking the link performs an HTTP GET request." Thus, creating a GET workflow action retrieves weather data using Zip_Code.

SPLK-1002       DumpTop     SPLK-1002 ! DumpTop   **SPLK-1002** 

Dumps, **30%OFF** Special Discount: **KrDump**)