Splunk.SPLK-1002.v2024-09-09.q118

Exam Code:	SPLK-1002
Exam Name:	Splunk Core Certified Power User Exam
Certification Provider:	Splunk
Free Question Number:	118
Version:	v2024-09-09
# of views:	2660
# of Questions views:	1180
https://www.freepdfdumps.com/Splunk.SPLK-1002.v2024-09-09.q118.html	

NEW QUESTION: 1

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

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: (SHOW ANSWER)

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 someuniqefield maxspan=1h In this search, the transaction command groups events that share the same someuniqefield 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: 2
Which workflow uses field values to perform a secondary search?
A. POST
B. Action
C. Search
D. Sub-Search
Answer: C (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb

NEW QUESTION: 3
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: 4
Which of the following statements about calculated fields in Splunk is true?
A. Calculated fields cannot be chained together to create more complex fields
B. Calculated fields can be chained together to create more complex fields.
C. Calculated fields can only be used in dashboards.
D. Calculated fields can only be used in saved reports.
Answer: B (LEAVE A REPLY)
The correct answer is B. Calculated fields can be chained together to create more complex fields. Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1.
Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as:
discount = total * 0.9
This will create a new field named discount that is equal to 90% of the total field value for each event2.
References:
* About calculated fields
* Chaining calculated fields

NEW QUESTION: 5
Which of the following file formats can be extracted using a delimiter field extraction?
A. CSV
B. PDF
C. XML
D. JSON
Answer: (SHOW ANSWER)
A delimiter field extraction is a method of extracting fields from data that uses a character or a string to separate fields in each event. A delimiter field extraction can be performed by using the Field Extractor (FX) tool or by editing the props.conf file. A delimiter field extraction can be applied to any file format that uses a delimiter to separate fields, such as CSV, TSV, PSV, etc. A CSV file is a comma-separated values file that uses commas as delimiters. Therefore, a CSV file can be extracted using a delimiter field extraction.

NEW QUESTION: 6

This function of the stats command allows you to identify the number of values a field has.
A. max
B. fields
C. count
D. distinct_count
Answer: (SHOW ANSWER)

NEW QUESTION: 7
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.ReferencesSee Define and manage tags in Settings and
[About capabilities] in the Splunk Documentation.

NEW QUESTION: 8
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)
"Calculated fields can reference all types of field extractions and field aliasing, but they cannot reference lookups, event types, or tags."

NEW QUESTION: 9
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: B (LEAVE A REPLY)
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: 10
Which of the following statements describes the command below (select all that apply)
Sourcetype=access_combined | transaction JSESSIONID
A. An additional filed named maxspan is created.
B. An additional field named duration is created.
C. An additional field named eventcount is created.
D. Events with the same JSESSIONID will be grouped together into a single event.
Answer: B,C,D (LEAVE A REPLY)
The command sourcetype=access_combined | transaction JSESSIONID does three things:
* It filters the events by the sourcetype access_combined, which is a predefined sourcetype for Apache web server logs.
* It groups the events by the field JSESSIONID, which is a unique identifier for each user session.
* It creates a single event from each group of events that share the same JSESSIONID value. This single event will have some additional fields created by the transaction command, such as duration, eventcount, and startime.
Therefore, the statements B, C, and D are true.

NEW QUESTION: 11
What is the correct syntax to find events associated with a tag?
A. tag:<field>=<value>
B. tags=<value>
C. tags:<field>=<value>
D. tag=<value>
Answer: (SHOW ANSWER)
The correct syntax to find events associated with a tag in Splunk is tag=<value>1. So, the correct answer is D.
tag=<value>. This syntax allows you to annotate specified fields in your search results with tags1. In Splunk, tags are a type of knowledge object that you can use to add meaningful aliases to field values in your data1. For example, if you have a field called status_code in your data, you might have different status codes like 200, 404, 500, etc. You can create tags for these status codes like success for 200, not_found for
404, and server_error for 500. Then, you can use the tag command in your searches to find events associated with these tags1.
Here is an example of how you can use the tag command in a search:
index=main sourcetype=access_combined | tag status_code
In this search, the tag command annotates the status_code field in the search results with the corresponding tags. If you have tagged the status code 200 with success, the status code 404 with not_found, and the status code 500 with server_error, the search results will include these tags1.
You can also use the tag command with a specific tag value to find events associated with that tag. For example, the following search finds all events where the status code is tagged with success:

index=main sourcetype=access_combined | tag status_code | search tag::status_code=success In this search, the tag command annotates the status_code field with the corresponding tags, and the search command filters the results to include only events where the status_code field is tagged with success1.

NEW QUESTION: 12
The macro weekly_sales (2) contains the search string:
index-games I eval Product Sales = $price$ $AmountS01d$
Which of the following will return results?
A. 'weekly_sales(3.99, 10) '
B. 'weekly_sales(3.99, 10)
C. 'weekly_sales (3.99, 10)
D. 'weekly_sales(3)
Answer: C (LEAVE A REPLY)
The correct answer is C. 'weekly_sales (3.99, 10)'. This is because search macros accept arguments without quotation marks or dollar signs, and the number of arguments must match the number of parameters defined in the macro. The other options are incorrect because they either use quotation marks or dollar signs around the arguments, or they provide a different number of arguments than the macro expects. You can learn more about how to use search macros in searches from the Splunk documentation1.

NEW QUESTION: 13
It is mandatory for the lookup file to have this for an automatic lookup to work.
A. Source type
B. At least five columns
C. Input filed
D. Timestamp
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
Consider the following search:
index=web sourcetype=access_combined
The log shows several events that share the same JSESSIONID value (SD470K92802F117). View the events as a group.
From the following list, which search groups events by JSESSIONID?
A. index=web sourcetype=access_combined | highlight JSESSIONID | search SD470K92802F117
B. index=web sourcetype=access_combined | transaction JSESSIONID | search SD470K92802F117
C. index=web sourcetype=access_combined SD470K92802F117 | table JSESSIONID
D. index=web sourcetype=access_combined JSESSIONID <SD470K92802F117>
Answer: B (LEAVE A REPLY)

To group events by JSESSIONID, the correct search is index=web sourcetype=access_combined | transaction JSESSIONID | search SD470K92802F117 (Option B). The transaction command groups events that share the same JSESSIONID value, allowing for the analysis of all events associated with a specific session as a single transaction. The subsequent search for SD470K92802F117 filters these grouped transactions to include only those related to the specified session ID.

NEW QUESTION: 15
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)
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: 16
Which of the following searches will return all clientip addresses that start with 108?
A. ... | where like (clientip, "108.%)
B. ... | search clientip=108
C. ... | where (clientip=108. %)
D. ... | where (clientip, "108. %")

Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
Use the dedup command to _____.
A. remove duplicate values
B. Rename a field in the index
C. provide an additional alias for the field that can D.be used in the search criteria
Answer: (SHOW ANSWER)

NEW QUESTION: 18
When creating a data model, which root dataset requires at least one constraint?
A. Root transaction dataset
B. Root event dataset
C. Root child dataset
D. Root search dataset
Answer: B (LEAVE A REPLY)
The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation1. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

NEW QUESTION: 19
Which of the following statements describes an event type?
A. A log level measurement: info, warn, error.
B. A knowledge object that is applied before fields are extracted.
C. A field for categorizing events based on a search string.
D. Either a log, a metric, or a trace.

Answer: C (LEAVE A REPLY)
This is because an event type is a knowledge object that assigns a user-defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards. You can learn more about event types from the Splunk documentation1. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

NEW QUESTION: 20
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: 21
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.
References
Search macro examples
Define search macros in Settings
Use search macros in searches

NEW QUESTION: 22
What does the transaction command do?
A. Groups a set of transactions based on time.
B. Creates a single event from a group of events.
C. Separates two events based on one or more values.
D. Returns the number of credit card transactions found in the event logs.
Answer: B (LEAVE A REPLY)
The transaction command is a search command that creates a single event from a group of events that share some common characteristics. The transaction command can group events based on fields, time, or both. The transaction command can also create some additional fields for each transaction, such as duration, eventcount, startime, etc. The transaction command does not group a set of transactions based on time, but rather groups a set of events into a transaction based on time.
The transaction command does not separate two events based on one or more values, but rather joins multiple events based on one or more values.
The transaction command does not return the number of credit card transactions found in the event logs, but rather creates transactions from the events that match the search criteria.

NEW QUESTION: 23
Which of the following statements about tags is true?
A. Tags are case insensitive.
B. Tags can make your data more understandable.
C. Tags are created at index time.
D. Tags are searched by using the syntax tag :: <fieldname>.
Answer: B (LEAVE A REPLY)
* Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .
* Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or tag the value 404 as not_found .

NEW QUESTION: 24
When extracting fields, we may choose to use our own regular expressions
A. True
B. False

Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")
A. The description field would contain no value.
B. The description field would contain the value 0.
C. The description field would contain the value "Internal Server Error".
D. This statement would produce an error in Splunk because it is incomplete.
Answer: A (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions

NEW QUESTION: 26
Which workflow action method can be used the action type is set to link?
A. GET
B. PUT
C. Search
D. UPDATE
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction Define a GET workflow action Steps
* Navigate to Settings > Fields > Workflow Actions.
* Click New to open up a new workflow action form.
* Define a Label for the action.
The Label field enables you to define the text that is displayed in either the field or event workflow menu.
Labels can be static or include the value of relevant fields.
* Determine whether the workflow action applies to specific fields or event types in your data.
Use Apply only to the following fields to identify one or more fields. When you identify fields, the workflow action only appears for events that have those fields, either in their event menu or field menus. If you leave it blank or enter an asterisk the action appears in menus for all fields.
Use Apply only to the following event types to identify one or more event types. If you identify an event type, the workflow action only appears in the event menus for events that belong to the event type.
* For Show action in determine whether you want the action to appear in the Event menu, the Fields menus, or Both.
* Set Action type to link.
* In URI provide a URI for the location of the external resource that you want to send your field values to.

Similar to the Label setting, when you declare the value of a field, you use the name of the field enclosed by dollar signs.
Variables passed in GET actions via URIs are automatically URL encoded during transmission. This means you can include values that have spaces between words or punctuation characters.
* Under Open link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.
* Set the Link method to get.
* Click Save to save your workflow action definition.

NEW QUESTION: 27
If a search returns _____ it can be viewed as a chart.
A. timestamps
B. statistics
C. events
D. keywords
Answer: B (LEAVE A REPLY)
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: 28
When using | timchart by host, which filed is representted in the x-axis?
A. date
B. host
C. -time
D. time
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following is true about the Splunk Common Information Model (CIM)?
A. The data models included in the CIM are configured with data model acceleration turned off.
B. The CIM contains 28 pre-configured datasets.
C. The CIM is an app that needs to run on the indexer.
D. The data models included in the CIM are configured with data model acceleration turned on.
Answer: D (LEAVE A REPLY)
The Splunk Common Information Model (CIM) is an app that contains a set of predefined data models that apply a common structure and naming convention to data from any source. The CIM enables you to use data from different sources in a consistent and coherent way. The CIM contains

28 pre-configured datasets that cover various domains such as authentication, network traffic, web, email, etc. The data models included in the CIM are configured with data model acceleration turned on by default, which means that they are optimized for faster searches and analysis. Data model acceleration creates and maintains summary data for the data models, which reduces the amount of raw data that needs to be scanned when you run a search using a data model.
Splunk Core Certified Power User Track, page 10. : Splunk Documentation, About the Splunk Common Information Model.

NEW QUESTION: 30
A user wants to create a new field alias for a field that appears in two sourcetypes.
How many field aliases need to be created?
A. It depends on whether the two sourcetypes are associated with the same index.
B. One.
C. It depends on whether the original fields have the same name.
D. Two.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
Why are tags useful in Splunk?
A. Tags look for less specific data.
B. Tags visualize data with graphs and charts.
C. Tags group related data together.
D. Tags add fields to the raw event data.
Answer: C (LEAVE A REPLY)
Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as router, and then search for tag=router to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values. For example, you can tag the field values error, fail, and critical as severity=high, and then search for severity=high to find all the events with high severity level2
1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION: 32
Which syntax will find events where the values for the 1 field match the values for the Renewal-MonthYear field?
A. | where 10yearAnnerversary=Renewal-MonthYear
B. | where '10yearAnnerversary=Renewal-MonthYear
C. | where 10yearAnnerversary='Renewal-MonthYear'
D. | where '10yearAnnerversary'='Renewal-MonthYear'
Answer: A (LEAVE A REPLY)
The correct answer is A. | where 10yearAnnerversary=Renewal-MonthYear.
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.
To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the 10yearAnnerversary field match the values for the Renewal-MonthYear field, you can use the following syntax:
| where 10yearAnnerversary=Renewal-MonthYear
This will return only the events where the two fields have the same value.
The other options are not correct because they use quotation marks around the field names, which will cause the where command to interpret them as string values instead of field names. For example, if you use:
| where '10yearAnnerversary'='Renewal-MonthYear'
This will return no events because there are no events where the string value '10yearAnnerversary' is equal to the string value 'Renewal-MonthYear'.
References:
* where command usage

NEW QUESTION: 33
Data models are composed of one or more of which of the following datasets? (select all that apply)
A. Transaction datasets
B. Events datasets
C. Search datasets
D. Any child of event, transaction, and search datasets

Answer: A,B,C (LEAVE A REPLY)
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: 34
A data model can consist of what three types of datasets?
A. Events, searches, and transactions.
B. Searches, transactions, and pivot.
C. Pivot, events, and transactions.
D. Pivot, searches, and events.
Answer: A (LEAVE A REPLY)

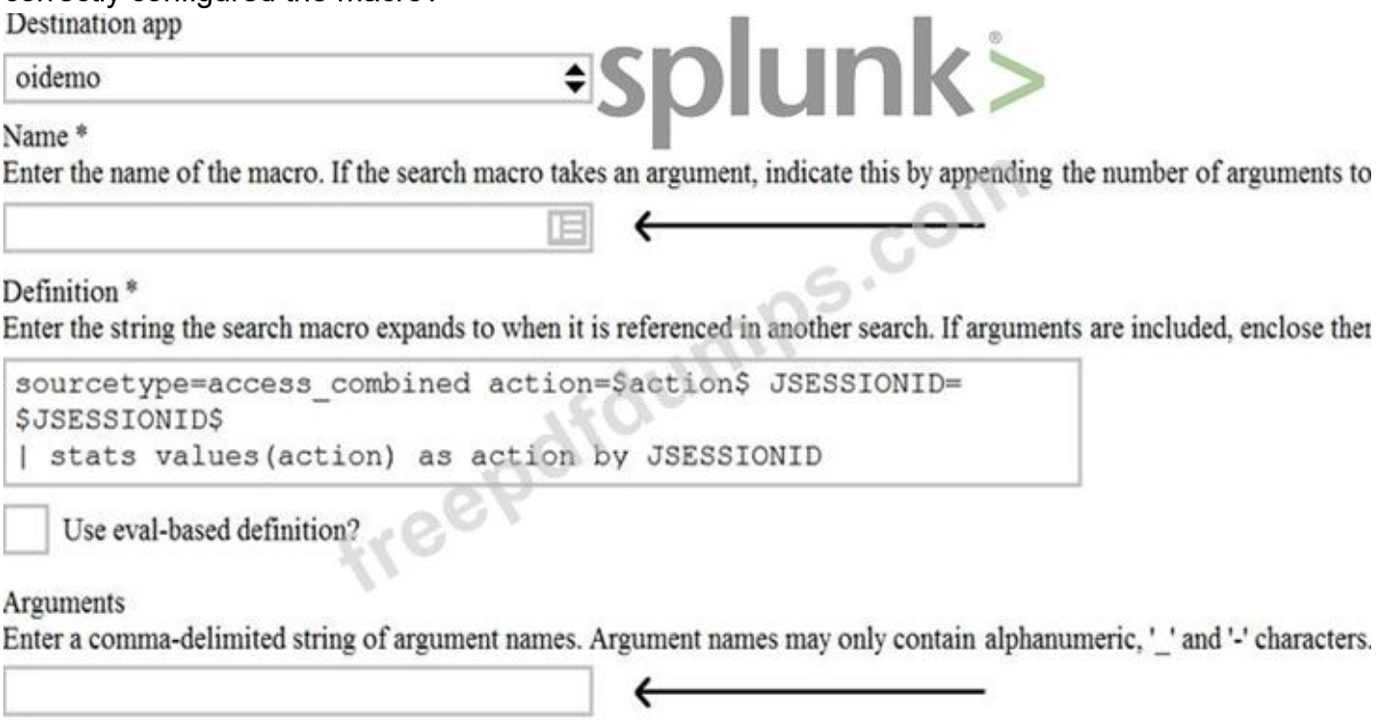
NEW QUESTION: 35
The timechart command buckets data in time intervals depending on:
A. the number of events returned
B. the selected time range
C. the type of visualization selected
Answer: B (LEAVE A REPLY)
The timechart command buckets data in time intervals depending on the selected time range2. The timechart command is similar to the chart command but it automatically groups events into time buckets based on the
_time field2. The size of the time buckets depends on the time range that you select for your search. For example, if you select Last 24 hours as your time range, Splunk will use 30-minute buckets for your timechart. If you select Last 7 days as your time range, Splunk will use 4-hour buckets for your timechart2.
Therefore, option B is correct, while options A and C are incorrect because they are not factors that affect the size of the time buckets.

NEW QUESTION: 36
Which search string would only return results for an event type called success ful_purchases?
A. tag=success ful_purchases
B. Event Type:: successful purchases
C. successful_purchases
D. event type-success ful_purchases
Answer: C (LEAVE A REPLY)
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 (success ful_purchases). You can learn more about how to use event types in searches from the Splunk documentation1.

NEW QUESTION: 37

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



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

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

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

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

Answer: (SHOW ANSWER)

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

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

sessiontracker(2)

The macro definition does the following:

It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string.

It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when it is executed.

It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action= $action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as

search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them.
In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.
Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.

NEW QUESTION: 38
We can use the rename command to _____ (Select all that apply.)
A. Give a field a new name at search time
B. Change indexed fields
C. Exclude fields from our search results
D. Extract new fields from our data using regular expressions
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)
A. Auto-Extracted fields can be hidden in Pivot.
B. Auto-Extracted fields can have their data type changed.
C. Auto-Extracted fields can be given a friendly name for use in Pivot.
D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.
Answer: (SHOW ANSWER)
Data model fields are fields that describe the attributes of a dataset in a data model2. Data model fields can be added using various methods such as Auto-Extracted, Evaluated or Lookup2. Auto-Extracted fields are fields that are automatically extracted from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. Auto-Extracted fields can be hidden in Pivot, which means that you can choose whether to display them or not in the Pivot interface2. Therefore, option A is correct. Auto-Extracted fields can have their data type changed, which means that you can specify whether they are strings, numbers, booleans or timestamps2. Therefore, option B is correct. Auto-Extracted fields can be given a friendly name for use in Pivot, which means that you can assign an alternative name to them that is more descriptive or user-friendly than the original field name2. Therefore, option C is correct. Auto-Extracted fields can be added if they already exist in the dataset with constraints, which means that you can include them in your data model even if they are already extracted from your raw data by applying filters or constraints to limit the scope of your dataset2. Therefore, option D is correct.

NEW QUESTION: 40
These users can create global knowledge objects. (Select all that apply.)
A. power users

B. users
C. administrators
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 41
A calculated field is a shortcut for performing repetitive, long, or complex transformations using which of the following commands?
A. transaction
B. lookup
C. stats
D. eval
Answer: D (LEAVE A REPLY)
The correct answer is D. eval.
A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1.
A calculated field is a shortcut for performing repetitive, long, or complex transformations using the eval command. The eval command is used to create or modify fields by using expressions. The eval command can perform mathematical, string, date and time, comparison, logical, and other operations on fields or values2.
For example, if you want to create a new field named total that is the sum of two fields named price and tax, you can use the eval command as follows:
| eval total=price+tax
However, if you want to use this new field in multiple searches, reports, or dashboards, you can create a calculated field instead of writing the eval command every time. To create a calculated field with Splunk Web, you need to go to Settings > Fields > Calculated Fields and enter the name of the new field (total), the name of the sourcetype (sales), and the eval expression (price+tax). This will create a calculated field named total that will be added to all events with the sourcetype sales at search time. You can then use the total field like any other extracted field without writing the eval expression1.
The other options are not correct because they are not related to calculated fields. These options are:
* A. transaction: This command is used to group events that share some common values into a single record, called a transaction. A transaction can span multiple events and multiple sources, and can be useful for correlating events that are related but not contiguous3.
* B. lookup: This command is used to enrich events with additional fields from an external source, such as a CSV file or a database. A lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field.
* C. stats: This command is used to calculate 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 fields.

References:
* About calculated fields
* eval command overview
* transaction command overview
* [lookup command overview]
* [stats command overview]

NEW QUESTION: 42
Which of the following is a feature of the Pivot tool?
A. Creates lookups without using SPL.
B. Data Models are not required.
C. Creates reports without using SPL
D. Datasets are not required.
Answer: C (LEAVE A REPLY)
The correct answer is C. Creates reports without using SPL. This is because the Pivot tool is a feature of Splunk that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL). You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations. You can learn more about the Pivot tool from the Splunk documentation1 or watch a video tutorial2. The other options are incorrect because they do not describe the features of the Pivot tool. The Pivot tool requires data models and datasets to define the data that you want to work with. Data models and datasets are designed by the knowledge managers in your organization. You can learn more about data models and datasets from the Splunk documentation3. The Pivot tool does not create lookups, which are tables that match field values to other field values. You can create lookups using SPL or the Lookup Editor. You can learn more about lookups from the Splunk documentation.

NEW QUESTION: 43
Splunk alerts can be based on search that run_____. (Select all that apply.)
A. in real-time
B. on a regular schedule
C. and have no matching events
Answer: A,B (LEAVE A REPLY)
Splunk alerts can be based on searches that run in real-time or on a regular schedule3. An alert is a way to monitor your data and get notified when certain conditions are met3. You can create an alert by specifying a search and a triggering condition3. You can also specify how often you want to run the search and how you want to receive the alert notifications3. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk3. Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day3. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

NEW QUESTION: 44
Which delimiters can the Field Extractor (FX) detect? (select all that apply)
A. Tabs
B. Pipes
C. Spaces
D. Commas
Answer: B,C,D (LEAVE A REPLY)
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.

NEW QUESTION: 45
Which of the following statements describe the search string below?
| datamodel Application_State All_Application_State search
A. Evenrches would return a report of sales by state.
B. Events will be returned from the data model named Application_State.
C. Events will be returned from the data model named All_Application_state.
D. No events will be returned because the pipe should occur after the datamodel command
Answer: (SHOW ANSWER)
The search string below returns events from the data model named Application_State.
| datamodel Application_State All_Application_State search
The search string does the following:
* It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.
* It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications.
* It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from all child datasets.
* It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.
Therefore, the search string returns events from the data model named Application_State.

NEW QUESTION: 46
Which of the following is true about data model attributes?
A. They cannot be created within the data model.
B. They can only be added into a root search dataset.
C. They cannot be edited if inherited from a parent dataset.

D. They can be added to a dataset from search time field extractions.

Answer: D (LEAVE A REPLY)

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.ReferencesSee About data models, [Define data model attributes], and [Edit data model datasets] in the Splunk Documentation.

NEW QUESTION: 47

Given the following eval statement:

...| eval fieldl - if(isnotnull(fieldl),fieldl,0), field2 = if(isnull<field2>, "NO-VALUE", fieid2) Which of the following is the equivalent using f ilinull?

A. There is no equivalent expression using f ilinull

B. ... t filinull values=(0,"NO-VALUE") fields=(fieldl,field2)

C. ... I filinull value=0 fieldl I fillnull fields

D. ... I fillnull fieldl I filinull value="NO-VALUE" field2

Answer: (SHOW ANSWER)

The fillnull command replaces null values in one or more fields with a specified value. The values option allows you to specify a comma-separated list of values to fill the null values in the corresponding fields. The fields option allows you to specify a comma-separated list of fields to apply the fillnull command to. The eval statement in the question uses the if and isnull functions to check if field1 and field2 have null values and replace them with 0 and "NO-VALUE" respectively. The equivalent expression using fillnull is to use the values option to specify 0 and "NO-VALUE" and the fields option to specify field1 and field22

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, fillnull command.

NEW QUESTION: 48

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.

NEW QUESTION: 49

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

A. The Field Extractor automatically extracts all fields at search time.

B. The Field Extractor uses PERL to extract fields from the raw events.

C. Fields extracted using the Field Extractor 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 statement that fields extracted using the Field Extractor persist as knowledge objects is true. The Field Extractor (FX) is a graphical tool that allows you to extract fields from raw events using regular expressions or delimiters. The fields extracted by the FX are saved as knowledge objects that can be used in future searches or shared with other users.

NEW QUESTION: 50

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: (SHOW ANSWER)

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: 51
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)
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: 52
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 Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:
Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.
Search datasets: These are derived datasets that represent the results of a search on events or other datasets.
Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.
Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

NEW QUESTION: 53
Which search would limit an "alert" tag to the "host" field?
A. tag=alert
B. host::tag::alert
C. tag==alert
D. tag::host=alert
Answer: D (LEAVE A REPLY)
The search below would limit an "alert" tag to the "host" field.
tag::host=alert
The search does the following:
* It uses tag syntax to filter events by tags. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data.
* It specifies tag::host=alert as the tag filter. This means that it will only return events that have an "alert" tag applied to their host field or host field value.
* It uses an equal sign (=) to indicate an exact match between the tag and the field or field value.

NEW QUESTION: 54
What information must be included when using the datamodel command?
A. Data model dataset name.
B. Data model field name.
C. Multiple indexes

D. status field
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which field will be used to populate the field if the productName and product:d fields have values for a given event?
| eval productINFO=coalesco(productName,productid)
A. Both field values will be used and the product INFO field will become a multivalue field for the given event.
B. The value for the productName field because it appears first.
C. Neither field value will be used and the field will be assigned a NULL value for the given event.
D. The value for the field because it appears second.
Answer: B (LEAVE A REPLY)
The correct answer is B. The value for the productName field because it appears first.
The coalesce function is an eval function that takes an arbitrary number of arguments and returns the first value that is not null. A null value means that the field has no value at all, while an empty value means that the field has a value, but it is "" or zero-length1.
The coalesce function can be used to combine fields that have different names but represent the same data, such as IP address or user name. The coalesce function can also be used to rename fields for clarity or convenience2.
The syntax for the coalesce function is:
coalesce(<field1>,<field2>,...)
The coalesce function will return the value of the first field that is not null in the argument list. If all fields are null, the coalesce function will return null.
For example, if you have a set of events where the IP address is extracted to either clientip or ipaddress, you can use the coalesce function to define a new field called ip, that takes the value of either clientip or ipaddress, depending on which is not null:
| eval ip=coalesce(clientip,ipaddress)
In your example, you have a set of events where the product name is extracted to either productName or productid, and you use the coalesce function to define a new field called productINFO, that takes the value of either productName or productid, depending on which is not null:
| eval productINFO=coalesce(productName,productid)
If both productName and productid fields have values for a given event, the coalesce function will return the value of the productName field because it appears first in the argument list. The productid field will be ignored by the coalesce function.
Therefore, the value for the productName field will be used to populate the productINFO field if both fields have values for a given event.
References:
* Search Command> Coalesce
* USAGE OF SPLUNK EVAL FUNCTION : COALESCE

NEW QUESTION: 56
Which of the following statements describes field aliases?
A. Field alias names replace the original field name.
B. Field aliases can be used in lookup file definitions.
C. Field aliases only normalize data across sources and sourcetypes.
D. Field alias names are not case sensitive when used as part of a search.
Answer: B (LEAVE A REPLY)
Field aliases are alternative names for fields in Splunk. Field aliases can be used to normalize data across different sources and sourcetypes that have different field names for the same concept. For example, you can create a field alias for src_ip that maps to clientip, source_address, or any other field name that represents the source IP address in different sourcetypes. Field aliases can also be used in lookup file definitions to map fields in your data to fields in the lookup file. For example, you can use a field alias for src_ip to map it to ip_address in a lookup file that contains geolocation information for IP addresses. Field alias names do not replace the original field name, but rather create a copy of the field with a different name. Field alias names are case sensitive when used as part of a search, meaning that src_ip and SRC_IP are different fields.

NEW QUESTION: 57
Which method in the Field Extractor would extract the port number from the following event? | 10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin <web error>
A. Delimiter
B. rex command
C. The Field Extractor tool cannot extract regular expressions.
D. Regular expression
Answer: B (LEAVE A REPLY)
The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:
rex "\+\+\+\+port (?<port>\d+)"
This will create a field called port with the value 54 for the event.
The delimiter method is not suitable for this event because there is no consistent delimiter between the fields.
The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.
Reference: 1 Splunk Core Certified Power User | Splunk

NEW QUESTION: 58
When should transaction be used?
A. When event grouping is based on start/end values.
B. When grouping events results in over 1000 events in each group.

C. When calculating results from one or more fields.
D. Only in a large distributed Splunk environment.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
Which command can include both an over and a by clause to divide results into sub-groupings?
A. chart
B. xyseries
C. stats
D. transaction
Answer: (SHOW ANSWER)

NEW QUESTION: 60
What will you learn from the results of the following search?
sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)
A. The average time elapsed during each transaction for all transactions
B. The average time between each transaction
C. The average time for each event within each transaction
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
When would a user select delimited field extractions using the Field Extractor (FX)?
A. When a log file has values that are separated by the same character, for example, commas.
B. When a log file contains empty lines or comments.
C. With structured files such as JSON or XML.
D. When the file has a header that might provide information about its structure or format.
Answer: A (LEAVE A REPLY)
The correct answer is A. When a log file has values that are separated by the same character, for example, commas.
The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions1.
The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them1.
The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds1.

Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions.
The other options are not correct because they are not suitable for the delimited field extraction method. These options are:
* B. When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or include some unwanted values.
* C. With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions2. The delimited method might not work well with this type of data, as it might not recognize the nested structure or the special characters.
* D. When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data, as it might not be able to identify the fields based on the header information.
References:
* Build field extractions with the field extractor
* Configure indexed field extraction

NEW QUESTION: 62
What is the correct syntax to search for a tag associated with a value on a specific fields?
A. Tag-<field?
B. Tag<filed(tagname.)
C. Tag=<filed>::<tagname>
D. Tag::<filed>=<tagname>
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/TagandaliasfieldvaluesinSplunkWeb
A tag is a descriptive label that you can apply to one or more fields or field values in your events2. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags2. To search for a tag associated with a value on a specific field, you can use

the following syntax: tag::<field>=<tagname>2. For example, tag::status=error will search for events where the status field has a tag named error. Therefore, option D is correct, while options A, B and C are incorrect because they do not follow the correct syntax for searching tags.

NEW QUESTION: 63

_____ datasets can be added to root dataset to narrow down the search

A. parent

B. extracted

C. event

D. child

Answer: D (LEAVE A REPLY)

Child datasets can be added to root datasets to narrow down the search. Datasets are collections of events that represent your data in a structured and hierarchical way. Datasets can be created by using commands such as datamodel or pivot. Datasets can have different types, such as events, search, transaction, etc. Datasets can also have different levels, such as root or child. Root datasets are base datasets that contain all events from a data model or an index. Child datasets are derived datasets that contain a subset of events from a parent dataset based on some constraints, such as search terms, fields, time range, etc. Child datasets can be added to root datasets to narrow down the search and filter out irrelevant events.

NEW QUESTION: 64

What fields does the transaction command add to the raw events? (select all that apply)

A. count

B. duration

C. eventcount

D. transaction id

Answer: B,D (LEAVE A REPLY)

Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies. The correct answers are B. duration and D. transaction id.

The explanation is as follows:

* The transaction command is a Splunk command that finds transactions based on events that meet various constraints12.
* Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member12.
* The transaction command adds some fields to the raw events that are part of the transaction123. These fields are:
* duration: The difference, in seconds, between the timestamps for the first and last events in the transaction123.
* eventcount: The number of events in the transaction123.
* transaction_id: A unique identifier for each transaction3. This field is useful for filtering or joining transactions3.

* Therefore, the fields that the transaction command adds to the raw events are duration and transaction_id, which are options B and D in your question.

NEW QUESTION: 65
Which is not a comparison operator in Splunk
A. <=
B. =
C. !=
D. >
E. ?=
Answer: E (LEAVE A REPLY)
A comparison operator is a symbol that compares two values and returns a Boolean result (true or false)2. Splunk supports various comparison operators such as <, >, =, !=, <=, >=, IN and LIKE2. However,
?= is not a valid comparison operator in Splunk and will cause a syntax error if used in a search string2.
Therefore, option E is correct, while options A, B, C and D are incorrect because they are valid comparison operators in Splunk

NEW QUESTION: 66
Using the Field Extractor (FX) tool, a value is highlighted to extract and give a name to a new field. Splunk has not successfully extracted that value from all appropriate events. What steps can be taken so Splunk successfully extracts the value from all appropriate events? (select all that apply)
A. Select an additional sample event with the Field Extractor (FX) and highlight the missing value in the event.
B. Re-ingest the data and attempt to extract from a new dataset.
C. Click on the event where the field was not extracted and choose "Change to Delimited".
D. Edit the regular expression manually.
Answer: A,D (LEAVE A REPLY)
When using the Field Extractor (FX) tool in Splunk and the tool fails to extract a value from all appropriate events, there are specific steps you can take to improve the extraction process. These steps involve interacting with the FX tool and possibly adjusting the extraction method:
A: Select an additional sample event with the Field Extractor (FX) and highlight the missing value in the event. This approach allows Splunk to understand the pattern better by providing more examples. By highlighting the value in another event where it wasn't extracted, you help the FX tool to learn the variability in the data format or structure, improving the accuracy of the field extraction.
D: Edit the regular expression manually. Sometimes the FX tool might not generate the most accurate regular expression for the field extraction, especially when dealing with complex log formats or subtle nuances in the data. In such cases, manually editing the regular expression can significantly improve the extraction process. This involves understanding regular expression syntax

and how Splunk extracts fields, allowing for a more tailored approach to field extraction that accounts for variations in the data that the automatic process might miss.
Options B and C are not typically related to improving field extraction within the Field Extractor tool. Re-ingesting data (B) does not directly impact the extraction process, and changing to a delimited extraction method (C) is not always applicable, as it depends on the specific data format and might not resolve the issue of missing values across events.

NEW QUESTION: 67
Which statement is true?
A. Pivot is used for creating datasets.
B. Data model 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: (SHOW ANSWER)
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot Pivot is used for creating reports and dashboards. Pivot is a tool that allows you to create reports and dashboards from your data models without writing any SPL commands. Pivot can help you visualize and analyze your data using various options, such as filters, rows, columns, cells, charts, tables, maps, etc. Pivot can also help you accelerate your reports and dashboards by using summary data from your accelerated data models.
Pivot is not used for creating datasets or data models. Datasets are collections of events that represent your data in a structured and hierarchical way. Data models are predefined datasets for various domains, such as network traffic, web activity, authentication, etc. Datasets and data models can be created by using commands such as datamodel or pivot.

NEW QUESTION: 68
Which of the following statements describes this search?
sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)
A. This is a valid search and will display a timechart of the average duration, of each transaction event.
B. This is a valid search and will display a stats table showing the maximum pause among transactions.
C. No results will be returned because the transaction command must include the startswith and endswith options.
D. No results will be returned because the transaction command must be the last command used in the search pipeline.
Answer: (SHOW ANSWER)
This search uses the transaction command to group events that share a common value for JSESSIONID into transactions1. The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction1. The search then uses the timechart command to create a time-series chart of the

average duration of each transaction1. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field. Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction1. Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search1.

NEW QUESTION: 69
This clause is used to group the output of a stats command by a specific name.
A. As
B. By
C. Rex
D. List
Answer: (SHOW ANSWER)

NEW QUESTION: 70
The time range specified for a historical search defines the _____ .------questionable on ans
A. Amount of data fetched from index matching that time range
B. Amount of data shown on the timeline as data streams in
C. Time range for the static results
Answer: (SHOW ANSWER)
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: 71
Which of the following transforming commands can be used with transactions?
A. chart, timechart, stats, eventstats
B. chart, timechart, stats, diff
C. chart, timeehart, datamodel, pivot
D. chart, timecha:t, stats, pivot
Answer: A (LEAVE A REPLY)
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: 72
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)
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: 73
Selected fields are displayed _____each event in the search results.
A. below
B. interesting fields
C. other fields
D. above
Answer: A (LEAVE A REPLY)
Selected fields are fields that you choose to display in your search results by clicking on them in the Fields sidebar or by using the fields command2. Selected fields are displayed below each event in the search results, along with their values2. Therefore, option A is correct, while options B, C and D are incorrect because they are not places where selected fields are displayed.

NEW QUESTION: 74
Which of the following statements best describes a macro?
A. A macro is a method of categorizing events based on a search.
B. A macro is a way to associate an additional (new) name with an existing field name.
C. A macro is a portion of a search that can be reused in multiple place
D. A macro is a knowledge object that enables you to schedule searches for specific events.
Answer: C (LEAVE A REPLY)
The correct answer is C. A macro is a portion of a search that can be reused in multiple places.

A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.
To create a macro, you need to define its name, definition, arguments, and description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments if any1.
For example, if you have a macro named my_macro that takes one argument named object and has the following definition:
search sourcetype= object
You can use it in a search by writing:
my_macro(web)
This will expand the macro and run the following SPL code:
search sourcetype=web
The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.
The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:
* A. An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports2.
* B. A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.
* D. An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4.
References:
* About event types
* About field aliases
* About alerts
* Define search macros in Settings
* Use search macros in searches

NEW QUESTION: 75
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 are equal to values of field B.

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

Answer: C (LEAVE A REPLY)

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.

To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the field A match the values for the field B, you can use the following syntax:

| where A=B

This will return only the events where the two fields have the same value.

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

* A. Events that contain the string value where A=B: This option uses the string value where 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 "where A=B" in them.
* 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.

* D. Events where field A contains the string value B: This option uses quotation marks around the value B, which is not valid syntax for comparing fields with the where command. Quotation marks are used to enclose phrases or exact matches in a search2. This option will return events where the field A contains the string value "B".

References:

* where command usage
* Search command cheatsheet

NEW QUESTION: 76

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

A. Index-main | REJECT trans sessionid

B. Index=main | transaction sessionid | whose transaction=reject

C. Index-main | transaction sessionid | search REJECT

D. Index=main | transaction sessionid | where transaction=reject"

Answer: C (LEAVE A REPLY)

NEW QUESTION: 77
A user wants to create a workflow action that will retrieve a specific field value from an event and run a search in a new browser window in the user's Splunk instance. What kind of workflow action should they create?
A. A Run workflow action, because the user is running a new search with a specific field value from an event returned in the user's search.
B. A Search workflow action, because the user is running a new search with a specific field value from an event returned in the user's search.
C. A POST workflow action, because the search is being sent to the user's current Splunk instance.
D. A GET workflow action, because a field value needs to be retrieved from the events returned in the user's search.
Answer: (SHOW ANSWER)
A Search workflow action is the appropriate choice when a user wants to retrieve a specific field value from an event and run a search in a new browser window within their Splunk instance (Option B). This type of workflow action allows users to define a search that utilizes field values from selected events as parameters, enabling more detailed investigation or context-specific analysis based on the original search results.

NEW QUESTION: 78
How is a Search Workflow Action configured to run at the same time range as the original search?
A. Set the earliest time to match the original search.
B. Select the same time range from the time-range picker.
C. Select the "Use the same time range as the search that created the field listing" checkbox.
D. Select the "Overwrite time range with the original search" checkbox.
Answer: C (LEAVE A REPLY)
To configure a Search Workflow Action to run at the same time range as the original search, you need to select the "Use the same time range as the search that created the field listing" checkbox. This will ensure that the workflow action search uses the same earliest and latest time parameters as the original search.

NEW QUESTION: 79

What is the correct format for naming a macro with multiple arguments?
A. monthly_sales(argument 1, argument 2, argument 3)
B. monthly_sales(3)
C. monthly_sales[3]
D. monthly_sales[argument 1, argument 2, argument 3)
Answer: C (LEAVE A REPLY)
The correct format for naming a macro with multiple arguments is monthly_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as monthly_sales[region,salesperson,date].

NEW QUESTION: 80
By default search results are not returned in _____ order.
A. Reverser chronological
B. Alphabetical
C. ASCIE
D. Chronological
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following about reports is/are true?
A. Reports are knowledge objects.
B. Reports can be scheduled.
C. Reports can run a script.
D. All of the above.
Answer: (SHOW ANSWER)
A report is a way to save a search and its results in a format that you can reuse and share with others2. A report is also a type of knowledge object, which is an entity that you create to add knowledge to your data and make it easier to search and analyze2. Therefore, option A is correct. A report can be scheduled, which means that you can configure it to run at regular intervals and send the results to yourself or others via email or other methods2. Therefore, option B is correct. A report can run a script, which means that you can specify a script file to execute when the report runs and use it to perform custom actions or integrations2. Therefore, option C is correct. Therefore, option D is correct because all of the above statements are true for reports.

NEW QUESTION: 82
A field alias is created where field1-fieid2 and the Overwrite Field Values checkbox is selected. What happens if an event only contains values for fieid1?
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: (SHOW ANSWER)

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: 83

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

A. It does not allow the use of wildcards.

B. It treats field values in a case-sensitive manner.

C. It can only be used at the beginning of the search pipeline.

D. It behaves exactly like search strings before the first pipe.

Answer: (SHOW ANSWER)

Reference:

https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand The search command is used to filter or refine your search results based on a search string that matches the events2. The search command behaves exactly like search strings before the first pipe, which means that you can use the same syntax and operators as you would use in the initial part of your

search2. Therefore, option D is correct, while options A, B and C are incorrect because they are not true statements about the search command.

NEW QUESTION: 84
Which of these is NOT a field that is automatically created with the transaction command?
A. maxcount
B. duration
C. eventcount
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
How is a macro referenced in a search?
A. By using the macroname command.
B. By using the macro command.
C. By enclosing the macro name in backtick characters (').
D. By enclosing the macro name in single-quote characters (').
Answer: C (LEAVE A REPLY)
The correct answer is C. By enclosing the macro name in backtick characters (`).
A macro is a way to reuse a piece of SPL code in different searches. A macro can take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.
To reference a macro in a search, you need to enclose the macro name in backtick characters ().
For example, if you have a macro named my_macro` that takes one argument, you can reference it in a search by using the following syntax:
| my_macro(argument) | ...
This will replace the macro name and argument with the SPL code contained in the macro definition.
For example, if the macro definition is:
[my_macro(argument)] search sourcetype=$argument$
And you reference it in a search with:
index=main | my_macro(web) | stats count by host
This will expand the macro and run the following SPL code:
index=main | search sourcetype=web | stats count by host
References:
* Use search macros in searches

NEW QUESTION: 86
Which of the following searches would return a report of sales by product-name?
A. chart sales by product_name
B. chart sum(price) as sales by product_name
C. stats sum(price) as sales over product_name
D. timechart list(sales), values(product_name)

Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Chart
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Stats

NEW QUESTION: 87
How could the following syntax for the chart command be rewritten to remove the OTHER category? (select all that apply)

A. | chart count over CurrentStanding by Action useother=f
B. | chart count over CurrentStanding by Action usenull-f useother-t
C. | chart count over CurrentStanding by Action limit=10 useother=f
D. | chart count over CurrentStanding by Action limit-10
Answer: A,C (LEAVE A REPLY)
In Splunk, when using the chart command, the useother parameter can be set to false (f) to remove the
'OTHER' category, which is a bucket that Splunk uses to aggregate low-cardinality groups into a single group to simplify visualization. Here's how the options break down:
A: | chart count over CurrentStanding by Action useother=fThis command correctly sets the useother parameter to false, which would prevent the 'OTHER' category from being displayed in the resulting visualization.
B: | chart count over CurrentStanding by Action usenull=f useother=tThis command has useother set to true (t), which means the 'OTHER' category would still be included, so this is not a correct option.
C: | chart count over CurrentStanding by Action limit=10 useother=fSimilar to option A, this command also sets useother to false, additionally imposing a limit to the top 10 results, which is a way to control the granularity of the chart but also to remove the 'OTHER' category.

D: | chart count over CurrentStanding by Action limit-10This command has a syntax error (limit-10 should be limit=10) and does not include the useother=f clause. Therefore, it would not remove the 'OTHER' category, making it incorrect.
The correct answers to rewrite the syntax to remove the 'OTHER' category are options A and C, which explicitly set useother=f.

NEW QUESTION: 88
What type of command is eval?
A. Streaming in some modes
B. Report generating
C. Distributable streaming
D. Centralized streaming
Answer: (SHOW ANSWER)
The correct answer is C. Distributable streaming. This is because the eval command is a type of command that can run on the indexers before the results are sent to the search head. This reduces the amount of data that needs to be transferred and improves the search performance. Distributable streaming commands can operate on each event or result individually, without depending on other events or results. You can learn more about the types of commands and how they affect search performance from the Splunk documentation1.

NEW QUESTION: 89
Which of the following searches will return events contains a tag name Privileged?
A. Tag= Priv
B. Tag= Pri*
C. Tag= Priv*
D. Tag= Privileged
Answer: (SHOW ANSWER)
Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity A tag is a descriptive label that you can apply to one or more fields or field values in your events1. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags1. To search for events that contain a tag name, you can use the tag keyword followed by an equal sign and the tag name1. You can also use wildcards (*) to match partial tag names1. Therefore, option B is correct because it will return events that contain a tag name that starts with Pri. Options A and D are incorrect because they will only return events that contain an exact tag name match. Option C is incorrect because it will return events that contain a tag name that starts with Priv, not Privileged.

NEW QUESTION: 90
Which of the following statements would help a user choose between the transaction and stats commands?
A. state can only group events using IP addresses.

B. The transaction command is faster and more efficient.
C. There is a 1000 event limitation with the transaction command.
D. Use state when the events need to be viewed as a single event.
Answer: C (LEAVE A REPLY)
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction One of the statements that would help a user choose between the transaction and stats commands is that there is a 1000 event limitation with the transaction command3.
The transaction command is used to group events that share a common value for one or more fields into transactions3. The transaction command has a default limit of 1000 events per transaction, which means that it will not group more than 1000 events into a single transaction3. This limit can be changed by using the maxevents parameter, but it can affect the performance and memory usage of Splunk3. Therefore, option C is correct, while options A, B and D are incorrect because they are not statements that would help a user choose between the transaction and stats commands.

NEW QUESTION: 91
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)
Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups.
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

NEW QUESTION: 92
Which of the following is a function of the Splunk Common Information Model (CIM)?
A. Reingesting previously indexed data with new field names.
B. Algorithmically shifting events to other indexes.
C. Normalizing data across a Splunk deployment.
D. Providing templates for reports and dashboards.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
The limit attribute will_____.
A. override default of 15
B. only work with top command
C. override default of 20
D. override default of 10
Answer: (SHOW ANSWER)

NEW QUESTION: 94
What are search macros?
A. Lookup definitions in lookup tables.
B. Reusable pieces of search processing language.
C. A method to normalize fields.
D. Categories of search results.
Answer: B (LEAVE A REPLY)
The correct answer is B. Reusable pieces of search processing language.
The explanation is as follows:
* Search macros are knowledge objects that allow you to insert chunks of SPL into other searches12.
* Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command12.
* You can also specify whether the macro field takes any arguments and define validation expressions for them12.
* Search macros can help you make your SPL searches shorter and easier to understand3.
* To use a search macro in a search string, you need to put a backtick character () before and after the macro name[^1^][1]. For example, mymacro`.

NEW QUESTION: 95
Which of the following describes the I transaction command?
A. It is an SPL command that groups at least two events together based on shared values in selected fields.
B. It allows an exchange of data from one Splunk index to another Splunk index.
C. It is an SPL command that groups events together with shared values in selected fields.
D. It allows an exchange of data from one Splunk system to another Splunk system.
Answer: (SHOW ANSWER)
* The transaction command is a Splunk command that finds transactions based on events that meet various constraints .
* Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member .

* The transaction command groups events together by matching one or more fields that have the same value across the events . For example, | transaction clientip will group events that have the same value in the clientip field.

NEW QUESTION: 96
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: A (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction A workflow action is a link that appears when you click an event field value in your search results2. A workflow action can open a web page or run another search based on the field value2. There are two types of workflow actions: GET and POST2. A GET workflow action appends the field value to the end of a URI and opens it in a web browser2. A POST workflow action sends the field value as part of an HTTP request to a web server2. When creating a Search workflow action, which is a type of GET workflow action that runs another search based on the field value, the only required field is the search string2. The search string defines the search that will be run when the workflow action is clicked2. Therefore, option A is correct, while options B, C and D are incorrect because they are not required fields for creating a Search workflow action.

NEW QUESTION: 97
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: (SHOW ANSWER)
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: 98

What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

A. The user is unable to return to the automatic field extraction workflow.

B. There is a limit to the number of fields that can be extracted.

C. The extraction is added at index time.

D. The user is unable to preview the extractions.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 99

Which of the following statements describe data model acceleration? (select 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_dacamodel capability to accelerate a data model.

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

Data model acceleration is a feature that speeds up searches on data models by creating and storing summaries of the data model datasets1. To enable data model acceleration, you must have administrative permissions or the accelerate_datamodel capability1. Therefore, option D is correct. Accelerated data models cannot be edited unless you disable the acceleration first1. Therefore, option B is correct. Private data models cannot be accelerated because they are not visible to other users1. Therefore, option C is correct. Root events can be accelerated as long as they are not based on a search string1. Therefore, option A is incorrect.

NEW QUESTION: 100

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

A. maxpause

B. endswith

C. maxduration

D. maxspan

Answer: D (LEAVE A REPLY)

The maxspan function of the transaction command allows you to set the maximum total time between the earliest and latest events returned. The maxspan function is an argument that can be used with the transaction command to specify the start and end constraints for the transactions. The maxspan function takes a time modifier as its value, such as 30s, 5m, 1h, etc. The maxspan function sets the maximum time span between the first and last events in a transaction. If the time span between the first and last events exceeds the maxspan value, the transaction will be split into multiple transactions.

NEW QUESTION: 101

The macro weekly_sales (2) contains the search string:
index=games | eval ProductSales = $Price$ * $AmountSold$
Which of the following will return results?
A. 'weekly sales (3)'
B. 'weekly_sales($3.995, $108)'
C. 'weekly_sales (3.99, 10)'
D. 'weekly sales (3.99, 10)'
Answer: C (LEAVE A REPLY)
To use a search macro in a search string, you need to place a back tick character (`) before and after the macro name1. You also need to use the same number of arguments as defined in the macro2. The macro weekly sales (2) has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.
The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses spaces instead of commas to separate the argument values.
Reference: 1 Use search macros in searches - Splunk Documentation 2 Define search macros in Settings - Splunk Documentation

NEW QUESTION: 102
Consider the the following search run over a time range of last 7 days:
index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane Which option is used to change the default time span so that results are grouped into 12 hour intervals?
A. span=12h
B. timespan=12h
C. span=12
D. timespan=12
Answer: (SHOW ANSWER)
The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals. The timespan option is not a valid option for the timechart command2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, timechart command.

NEW QUESTION: 103
What commands can be used to group events from one or more data sources?
A. eval, coalesce
B. transaction, stats
C. stats, format
D. top, rare
Answer: B (LEAVE A REPLY)

The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of a subsearch, not to group events. The top and rare commands are used to rank the most or least common values of a field, not to group events23 1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command. 3:
Splunk Documentation, stats command.

NEW QUESTION: 104
When would transaction be used instead of stats?
A. To group events based on a single field value.
B. To see results of a calculation.
C. To have a faster and more efficient search.
D. To group events based on start/end values.
Answer: D (LEAVE A REPLY)
The transaction command is used to group events that are related by some common fields or conditions, such as start/end values, time span, or pauses. The stats command is used to calculate statistics on a group of events by a common field value.
References
Splunk Community
Splunk Transaction - Exact Details You Need

NEW QUESTION: 105
When using | timechart by host, which field is represented in the x-axis?
A. date
B. host
C. time
D. _time
Answer: D (LEAVE A REPLY)
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart

NEW QUESTION: 106
How is an event type created from the search window? (select all that apply)
A. In the top right corner, click Save As > Event Type.
B. In an event's detail dropdown, click Event Actions > Build Event Type.
C. Edit eventtypes.conf and add a new stanza.
D. Add | eventtype to the SPL and execute the search.
Answer: A,C (LEAVE A REPLY)

In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type1. This opens the Save as Event Type dialog, where you can provide the event type name and optionally apply tags to it1.
You can also create an event type by editing the eventtypes.conf file and adding a new stanza1. Each stanza in the eventtypes.conf file represents an event type1. The stanza name is the name of the event type, and the search attribute specifies the search string that defines the event type1.
It's important to note that while you can use the eventtype command in a search to find events associated with a specific event type, adding | eventtype to the SPL and executing the search does not create a new event type1. Similarly, clicking Event Actions > Build Event Type in an event's detail dropdown does not create a new event type1.

NEW QUESTION: 107
Which of the following search control will not re-rerun the search? (Select all that apply.)
A. zoom out
B. selecting a bar on the timeline
C. deselect
D. selecting a range of bars on the timelines
Answer: B,C,D (LEAVE A REPLY)
The timeline is a graphical representation of your search results that shows the distribution of events over time2. You can use the timeline to zoom in or out of a specific time range or to select one or more bars on the timeline to filter your results by that time range2. However, these actions will not re-run the search, but rather refine the existing results based on the selected time range2.
Therefore, options B, C and D are correct, while option A is incorrect because zooming out will re-run the search with a broader time range.

NEW QUESTION: 108
Highlighted search terms indicate _____ search results in Splunk.
A. Display as selected fields.
B. Sorted
C. Charted based on time
D. Matching
Answer: D (LEAVE A REPLY)

Highlighted search terms indicate matching search results in Splunk, which means that they show which parts of your events match your search string2. For example, if you search for error OR fail, Splunk will highlight error or fail in your events to show which events match your search string2. Therefore, option D is correct, while options A, B and C are incorrect because they are not indicated by highlighted search terms.

NEW QUESTION: 109
Which of the following options will define the first event in a transaction?
A. startswith
B. with
C. startingwith
D. firstevent
Answer: A (LEAVE A REPLY)
The explanation is as follows:
* The transaction command is used to find transactions based on events that meet various constraints12.
* Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member1.
* The startswith option is used to define the first event in a transaction by specifying a search term or an expression that matches the event13.
* For example, | transaction clientip JSESSIONID startswith="view" will create transactions based on the clientip and JSESSIONID fields, and the first event in each transaction will contain the term "view" in the _raw field2.

NEW QUESTION: 110
Which of the following commands support the same set of functions?
A. stats, chart, timechart
B. search, where, eval
C. stats, eval, table
D. transaction, chart, timechart
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which of the following statements describe calculated fields? (select 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 eval command.
Answer: A,B,D (LEAVE A REPLY)
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields
Calculated fields are fields that are created by performing calculations on existing fields using the

eval command. Calculated fields can be used in the search bar to filter and transform events based on the calculated values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for performing calculations using the eval command, but rather results of performing calculations using the eval command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype.
Therefore, statements A, B, and D are true about calculated fields.

NEW QUESTION: 112
Which of the following expressions could be used to create a calculated field called gigabytes?
A. sc_bytas(1024/1024)
B. megabytes=sc_bytes(1024/1024)
C. | eval negabytes=sc_bytes(1024/1024)
D. eval sc_bytes(1024/1024)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
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)
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: 114
When a search returns _____, you can view the results as a list.
A. statistical values
B. transactions
C. a list of events
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
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)
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: 116
When defining a macro, what are the required elements?
A. Name and arguments.
B. Name and a validation error message.
C. Name and definition.
D. Definition and arguments.
Answer: C (LEAVE A REPLY)
When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced. The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Define search macros in Settings.

NEW QUESTION: 117
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: (SHOW ANSWER)
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: 118
Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

A. POST
B. Search
C. GET
D. Format
Answer: (SHOW ANSWER)
The type of workflow action that sends field values to an external resource (e.g. a ticketing system) is POST.
A POST workflow action allows you to send a POST request to a URI location with field values or static values as arguments. For example, you can use a POST workflow action to create a ticket in an external system with information from an event.