Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

https://www.2passeasy.com/dumps/SPLK-1002/

NEW QUESTION 1
- (Exam Topic 1)
When should you use the transaction command instead of the scats command?

A. When you need to group on multiple values.
B. When duration is irrelevant in search result
C. .
D. When you have over 1000 events in a transaction.
E. When you need to group based on start and end constraints.

Answer: D

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

NEW QUESTION 2
- (Exam Topic 1)
What does the fillnull command replace null values with, it the value argument is not specified?

A. N/A
B. NaN
C. NULL

Answer: A

Explanation:
Reference: https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specfying-a-field.html The fillnull command is a search command that replaces null values with a specified value or 0 if no value is
specified. Null values are values that are missing, empty, or undefined in Splunk. The fillnull command can replace null values for all fields or for specific fields. The fillnull command can take an optional argument called value that specifies the value to replace null values with. If no value argument is specified, the fillnull command will replace null values with 0 by default.

NEW QUESTION 3
- (Exam Topic 1)
Which of the following actions can the eval command perform?

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

Answer: B

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

NEW QUESTION 4
- (Exam Topic 1)
In which of the following scenarios is an event type more effective than a saved search?

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

Answer: C

Explanation:
Reference: https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html
An event type is a way to categorize events based on a search string that matches the events2. You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names2. An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again2. Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.

NEW QUESTION 5
- (Exam Topic 1)
Which of the following statements describes macros?

A. A macro is a reusable search string that must contain the full search.

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

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros
A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

NEW QUESTION 6
- (Exam Topic 1)
Which of the following statements describes POST workflow actions?

A. POST workflow actions are always encrypted.
B. POST workflow actions cannot use field values in their URI.
C. POST workflow actions cannot be created on custom sourcetypes.
D. POST workflow actions can open a web page in either the same window or a new .

Answer: D

Explanation:
A workflow action is a link that appears when you click an event field value in your search results1. A workflow action can open a web page or run another search based on the field value1. There are two types of workflow actions: GET and POST1. A GET workflow action appends the field value to the end of a URI and opens it in a web browser1. A POST workflow action sends the field value as part of an HTTP request to a web server1. You can configure a workflow action to open a web page in either the same window or a new window1. Therefore, option D is correct, while options A, B and C are incorrect.

NEW QUESTION 7
- (Exam Topic 1)
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: BCD

Explanation:
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 8
- (Exam Topic 1)
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

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

NEW QUESTION 9
- (Exam Topic 1)
Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

A. Alerts
B. Email
C. Database
D. User permissions

Answer: ABC

Explanation:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview
The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it3. The CIM add-on includes several data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, options A, B and C are correct because they are names of some of the data models included in the CIM add-on. Option D is incorrect because User permissions is not a name of a data model in the CIM add-on.

NEW QUESTION 10
- (Exam Topic 1)
Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

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

Answer: ABD

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

- It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.
- It uses the transaction command to group events into transactions based on two fields: clientip and host.

The transaction command creates new events from groups of events that share the same clientip and host values.

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

NEW QUESTION 10
- (Exam Topic 1)
What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

A. Custom visualizations
B. Pre-configured data models
C. Fields and event category tags
D. Automatic data model acceleration

Answer: BC

Explanation:
The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it3. The CIM add-on includes pre-configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, option B is correct. The CIM add-on also includes fields and event category tags that define the common attributes and labels for the data models3. Therefore, option C is correct. The CIM add-on does not include custom visualizations or automatic data model acceleration. Therefore, options A and D are incorrect.

NEW QUESTION 15
- (Exam Topic 2)
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: D

Explanation:
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 18
- (Exam Topic 2)
When using the transaction command, how are evicted transactions identified?

A. Closed_txn field is set to o, or false.
B. Max_txn field is set to O, or false.
C. Txn_field is set to 1, or true.
D. open_txn field is set to 1, or true.

Answer: A

Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints1.
- 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 transaction command adds some fields to the raw events that are part of the transaction12. These fields are:
- duration: The difference, in seconds, between the timestamps for the first and last events in the transaction12.
- eventcount: The number of events in the transaction12.
- closed_txn: A Boolean field that indicates whether the transaction is closed or evicted2. A transaction is closed if it meets one of the following conditions: maxevents, maxpause, maxsp or startswith2. A transaction is evicted if it does not meet any of these conditions and exceeds th memory limit specified by maxopentxn or maxopenevents23.
- Therefore, evicted transactions can be distinguished from non-evicted transactions by checking the value of the closed_txn field. The closed_txn field is set to 0, or false, for evicted transactions and 1 for non-evicted, or closed, transactions23.

NEW QUESTION 21
- (Exam Topic 2)
The eval command 'if' function requires the following three arguments (in order):

A. Boolean expression, result if true, result if false
B. Result if true, result if false, boolean expression
C. Result if false, result if true, boolean expression
D. Boolean expression, result if false, result if true

Answer: A

Explanation:
The eval command ‘if’ function requires the following three arguments (in order): boolean expression, result if true, result if false. The eval command is a search command that allows you to create new fields or modify existing fields by performing calculations or transformations on them. The eval command can use various functions to perform different operations on fields. The ‘if’ function is one of the functions that can be used with the eval command to perform conditional evaluations on fields. The ‘if’ function takes three arguments: a boolean expression that evaluates to true or false, a result that will be returned if the boolean expression is true, and a result that will be returned if the boolean expression is false. The ‘if’ function returns one of the two results based on the evaluation of the boolean expression.

NEW QUESTION 25
- (Exam Topic 2)
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: BCD

Explanation:
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 26
- (Exam Topic 2)
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: D

Explanation:
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 27
- (Exam Topic 2)
Which syntax is used to represent an argument in a macro definition?

A. "argument"
B. %argument%
C. ‘argument’
D. $argument$

Answer: D

Explanation:
The correct answer is D.
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 macro1.
To represent an argument in a macro definition, you need to use the dollar sign ($) character to enclose the argument name. For example, if you want to create a search macro that takes one argument named “object”, you can use the following syntax:
[my_macro(object)] search sourcetype= object
This will create a search macro named my_macro that takes one argument named object. When you call the macro in a search, you need to provide a value for the object argument, such as:
my_macro(web)
This will replace the object argument with the value web and run the following SPL code: search sourcetype=web
The other options are not correct because they use quotation marks (’ or ") or percentage signs (%) to represent arguments, which are not valid syntax for macro arguments. These characters will be interpreted as literal values instead of variables.
References:
- Use search macros in searches

NEW QUESTION 28
- (Exam Topic 2)
The transaction command allows you to ________ events across multiple sources

A. duplicate
B. correlate
C. persist
D. tag

Answer: B

Explanation:
The transaction command allows you to correlate events across multiple sources. The transaction command is a search command that allows you to group events into transactions based on some common characteristics, such as fields, time, or both. A transaction is a group of events that share one or more fields that relate them to each other. A transaction can span across multiple sources or sourcetypes that have different formats or structures of data. The transaction command can help you correlate events across multiple sources by using the common fields as the basis for grouping. The transaction command can also create some additional fields for each transaction, such as duration, eventcount, startime, etc.

NEW QUESTION 32
- (Exam Topic 2)
A data model can consist of what three types of datasets?

A. Pivot, searches, and events.
B. Pivot, events, and transactions.
C. Searches, transactions, and pivot.
D. Events, searches, and transactions.

Answer: D

NEW QUESTION 33
- (Exam Topic 2)
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: ABC

Explanation:
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 35
- (Exam Topic 2)
The Splunk Common Information Model (CIM) is a collection of what type of knowledge object?

A. KV Store
B. Lookups

C. Saved searches
D. Data models

Answer: D

Explanation:
The Splunk Common Information Model (CIM) is a collection of data models that apply a common structure and naming convention to data from any source. A data model is a type of knowledge object that defines the structure and relationships of fields in a dataset. A data model can have one or more datasets, which are subsets of the data model that represent different aspects of the data. For example, the Network Traffic data model has datasets such as All Traffic, DNS, HTTP, etc. The CIM contains 28 pre-configured data models that cover various domains such as authentication, network traffic, web, email, etc. The CIM is implemented as an add-on that contains the JSON files for the data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time23
1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, Overview of the Splunk Common Information Model 1. 3: Splunkbase, Splunk Common Information Model (CIM) 2.

NEW QUESTION 38
- (Exam Topic 2)
Which workflow action method can be used the action type is set to link?

A. GET
B. PUT
C. Search
D. UPDATE

Answer: A

Explanation:

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 40
- (Exam Topic 2)
Which of these search strings is NOT valid:

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

Answer: A

Explanation:
This search string is not valid: index=web status=50* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

NEW QUESTION 43
- (Exam Topic 2)
Which of the following statements describes the use of the Filed Extractor (FX)?

A. The Field Extractor automatically extracts all field at search time.
B. The Field Extractor uses PERL to extract field from the raw events.
C. Field extracted using the Extracted persist as knowledge objects.

D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Answer: C

Explanation:
The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface or by manually editing the regular expression2. The FX allows you to create field extractions that persist as knowledge objects, which are entities that you create to add knowledge to your data and make it easier to search and analyze2. Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. When you create a field extraction using the FX, you can save it as a knowledge object that applies to your data at search time2. You can also manage and share your field extractions with other users in your organization2. Therefore, option C is correct, while options A, B and D are incorrect because they do not describe the use of the FX.

NEW QUESTION 45
- (Exam Topic 2)
These allow you to categorize events based on search terms. Select your answer.

A. Groups
B. Event Types
C. Macros
D. Tags

Answer: B

NEW QUESTION 50
- (Exam Topic 2)
Complete the search, …. | _______ failure>successes

A. Search
B. Where
C. If
D. Any of the above

Answer: B

Explanation:
The where command can be used to complete the search below.
… | where failure>successes
The where command is a search command that allows you to filter events based on complex or custom criteria. The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.
The search string below does the following:

- It uses … to represent any search criteria or commands before the where command.
- It uses the where command to filter events based on a comparison between two fields: failure and successes.
- It uses the greater than operator (>) to compare the values of failure and successes fields for each event.
- It only keeps events where failure is greater than successes.

NEW QUESTION 54
- (Exam Topic 2)
When using | timechart by host, which field is represented in the x-axis?

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

Answer: D

Explanation:

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

NEW QUESTION 57
- (Exam Topic 2)
In which Settings section are macros defined?

A. Fields
B. Tokens
C. Advanced Search
D. Searches, Reports, Alerts

Answer: C

NEW QUESTION 62
- (Exam Topic 2)
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

Explanation:
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 64
- (Exam Topic 2)
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

Explanation:
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 65
- (Exam Topic 2)
This function of the stats command allows you to return the sample standard deviation of a field.

A. stdev
B. dev
C. count deviation
D. by standarddev

Answer: A

NEW QUESTION 66
- (Exam Topic 2)
Tags can reference which of the following knowledge objects?

A. Lookups and event types only.
B. Extracted fields, field aliases, calculated fields, lookups, and event types.
C. Tags cannot reference any of these knowledge objects because tags are the last knowledge objects generated in the search-time operation sequence.
D. Extracted fields, calculated fields, and field aliases only.

Answer: B

Explanation:
Tags are a type of knowledge object that enable you to assign descriptive keywords to events. Tags can reference any of the following knowledge objects: extracted fields, field aliases, calculated fields, lookups, and event types. Tags cannot reference other tags or search macros. Tags are applied to events at search time based on the values of the fields that they reference2
1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION 70
- (Exam Topic 2)
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

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

NEW QUESTION 72
- (Exam Topic 2)
By default search results are not returned in _______ order.

A. Chronological
B. Reverser chronological
C. ASCIE
D. Alphabetical

Answer: AD

NEW QUESTION 74
- (Exam Topic 2)
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

Explanation:
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 76
- (Exam Topic 2)
What does the fillnull command replace null values with, if the value argument is not specified?

A. N/A
B. NaN
C. NULL

Answer: A

Explanation:
The fillnull command replaces null values with 0 by default, if the value argument is not specified. You can use the value argument to specify a different value to replace null values with, such as N/A or NULL.

NEW QUESTION 79
- (Exam Topic 2)
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. One.
B. Two.
C. It depends on whether the original fields have the same name.
D. It depends on whether the two sourcetypes are associated with the same index.

Answer: B

NEW QUESTION 84
- (Exam Topic 2)
Which tool uses data models to generate reports and dashboard panels without using SPL?

A. Visualization tab
B. Pivot
C. Datasets
D. splunk CIM

Answer: B

Explanation:
The correct answer is B. Pivot1.
In Splunk, Pivot is a tool that uses data models to generate reports and dashboard panels without the need for users to write or understand Splunk’s Search Processing Language (SPL)1. Data models enable users of Pivot to create compelling reports and dashboards1. When a Pivot user designs a pivot report, they select the data model that represents the category of event data that they want to work with1. Then they select a dataset within that data model that represents the specific dataset on which they want to report1. This makes Pivot a powerful tool for users who need to create visualizations but do not have a deep understanding of SPL1.

NEW QUESTION 87
- (Exam Topic 2)
When used with the timechart command, which value of the limit argument returns all values?

A. limit=*
B. limit=all
C. limit=none
D. limit=0

Answer: D

Explanation:
The correct answer is D. limit=0. This is because the limit argument specifies the maximum number of series to display in the chart. If you set limit=0, no series filtering occurs and all values are returned. You can learn more about the limit argument and how it works with the agg argument from the Splunk documentation1. The other options are incorrect because they are not valid values for the limit argument. The limit argument expects an integer value, not a string or a wildcard. You can learn more about the syntax and usage of the timechart command from the Splunk documentation23.

NEW QUESTION 88
- (Exam Topic 2)
Which of these is NOT a field that is automatically created with the transaction command?

A. maxcount
B. duration
C. eventcount

Answer: A

NEW QUESTION 93
- (Exam Topic 2)
Which of the following searches will return events containing a tag named Privileged?

A. tag=Priv
B. tag=Priv*
C. tag=priv*
D. tag=privileged

Answer: B

Explanation:
The tag=Priv* search will return events containing a tag named Privileged, as well as any other tag that starts with Priv. The asterisk (*) is a wildcard character that matches zero or more characters. The other searches will not match the exact tag name.

NEW QUESTION 96
- (Exam Topic 2)
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

Explanation:
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 98
- (Exam Topic 2)
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

Explanation:
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 100
- (Exam Topic 2)
Which of the following expressions could be used to create a calculated field called gigabytes?

A. eval sc_bytes(1024/1024)
B. | eval negabytes=sc_bytes(1024/1024)
C. megabytes=sc_bytes(1024/1024)
D. sc_bytas(1024/1024)

Answer: B

NEW QUESTION 101
- (Exam Topic 2)
For choropleth maps,splunk ships with the following KMZ files (select all that apply)

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

Answer: AD

Explanation:
Splunk ships with the following KMZ files for choropleth maps: States of the United States and Countries of the World. A KMZ file is a compressed file that contains a KML file and other resources. A KML file is an XML file that defines geographic features and their properties. A KMZ file can be used to create choropleth maps in Splunk by using the geom command. A choropleth map is a type of map that shows geographic regions with different colors based on some metric. Splunk ships with two KMZ files that define the geographic regions for choropleth maps:

- States of the United States: This KMZ file defines the 50 states of the United States and their boundaries. The name of this KMZ file is us_states.kmz and it is located in the
$SPLUNK_HOME/etc/apps/maps/appserver/static/geo directory.
- Countries of the World: This KMZ file defines the countries of the world and their boundaries. The name of this KMZ file is world_countries.kmz and it is located in the
$SPLUNK_HOME/etc/apps/maps/appserver/static/geo directory.

Splunk does not ship with KMZ files for States and provinces of the United States and Canada or Countries of the European Union. However, you can create your own KMZ files or download them from external sources and use them in Splunk.

NEW QUESTION 103
- (Exam Topic 2)
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

Explanation:
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 105
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1002 Product From:

https://www.2passeasy.com/dumps/SPLK-1002/

Money Back Guarantee

SPLK-1002 Practice Exam Features:

* SPLK-1002 Questions and Answers Updated Frequently

* SPLK-1002 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year