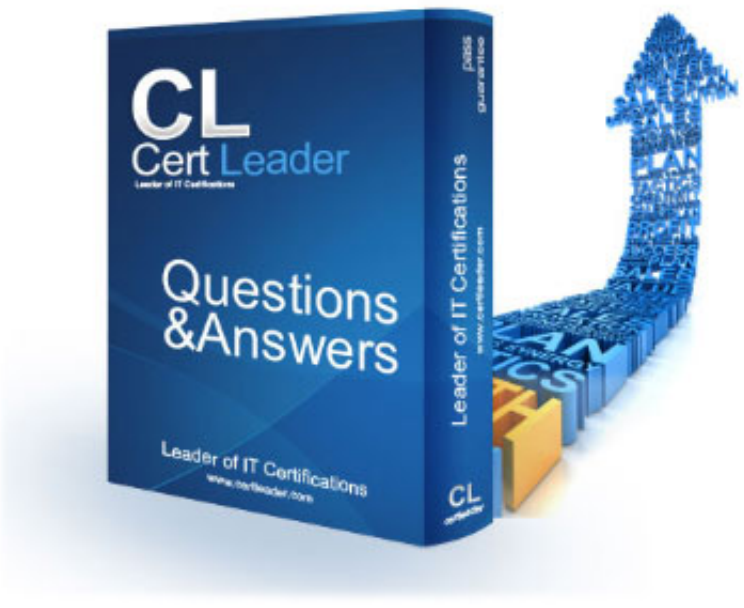
SPLK-1002 Dumps

Splunk Core Certified Power User Exam

https://www.certleader.com/SPLK-1002-dumps.html



NEW QUESTION 1
- (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 2
- (Exam Topic 1)
The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

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

Answer: CD

Explanation:
The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical
interface2. You can create a report using a custom field extracted by the FX and share it with other users in your organization2. However, if another user runs the shared report and no results are returned, there could be two possible reasons. One reason is that the extraction is private, which means that only you can see and use the extracted field2. To make the extraction available to other users, you need to make it global or app-level2. Therefore, option C is correct. Another reason is that the other user does not have access to the index where the events are stored2. To fix this issue, you need to grant the appropriate permissions to the other user for the index2. Therefore, option D is correct. Options A and B are incorrect because they are not related to the field extraction or the report.

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
Which of the following statements describe GET workflow actions?

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

Answer: D

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

NEW QUESTION 5
- (Exam Topic 1)

How does a user display a chart in stack mode?

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

Answer: C

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

NEW QUESTION 6
- (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.

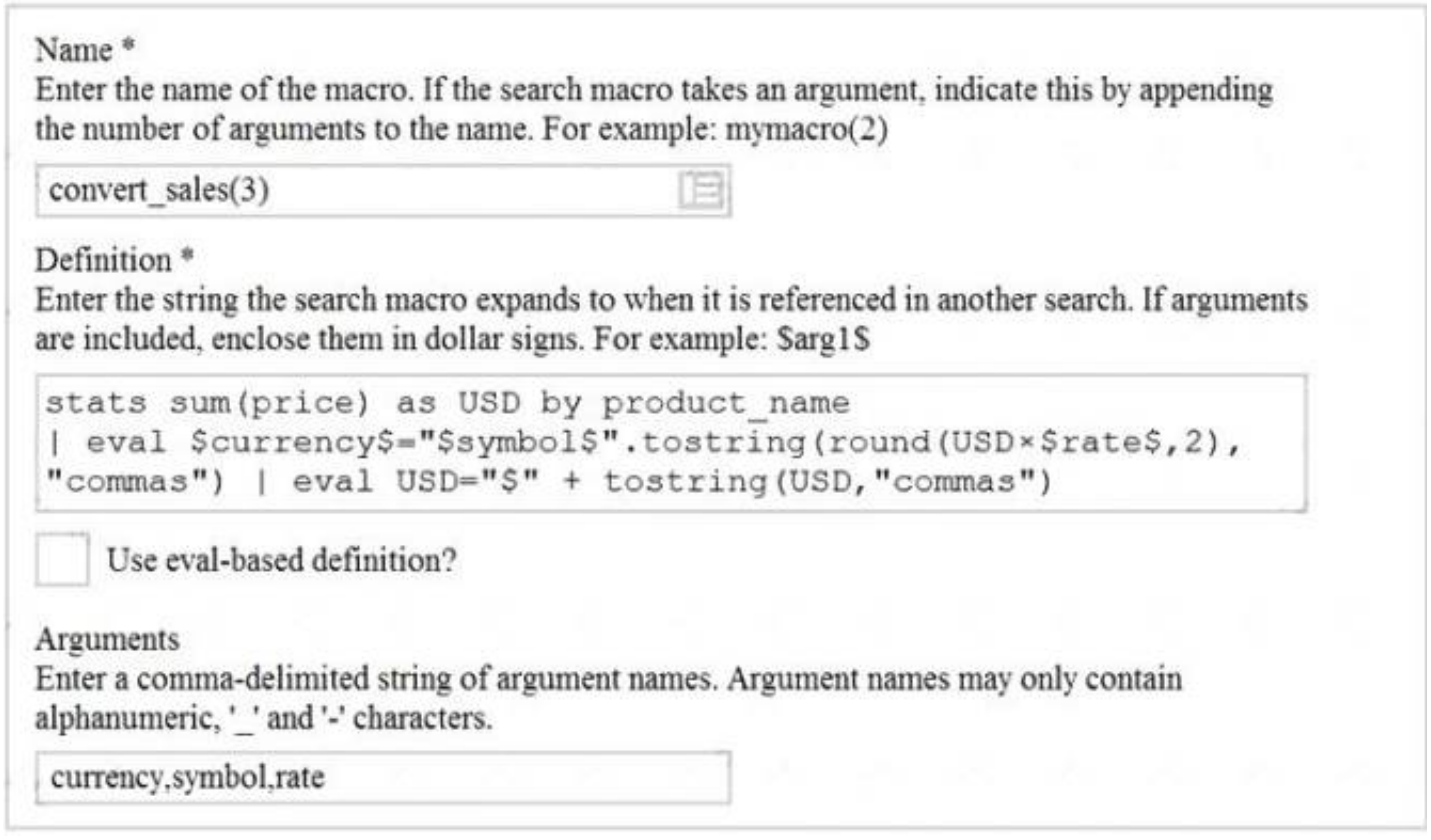
NEW QUESTION 7
- (Exam Topic 1)
Selected fields are displayed _____ each event in the search results.

A. below
B. interesting fields
C. other fields
D. above

Answer: A

Explanation:
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 8
- (Exam Topic 1)
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



A. Convert_sales (euro, €, 79)”
B. Convert_sales (euro, €, .79)
C. Convert_sales ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)

Answer: B

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

NEW QUESTION 9
- (Exam Topic 1)
When using timechart, how many fields can be listed after a by clause?

A. because timechart doesn't support using a by clause.
B. because _time is already implied as the x-axis.
C. because one field would represent the x-axis and the other would represent the y-axis.
D. There is no limit specific to timechart.

Answer: B

Explanation:
The timechart command is used to create a time-series chart of statistical values based on your search results2. You can use the timechart command with a by clause to split the results by one or more fields and create multiple series in the chart2. However, you can only list one field after the by clause when using the timechart command because _time is already implied as the x-axis of the chart2. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 10
- (Exam Topic 1)
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: BCD

Explanation:
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 10
- (Exam Topic 1)
What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

A. Macros.
B. Field aliases.
C. The rename command.
D. CIM does not work with different names for the same field.

Answer: B

Explanation:
The Splunk Common Information Model (CIM) add-on helps you normalize your data from different sources and make it easier to analyze and report on it3. One of the functionalities that the CIM add-on relies on to normalize fields with different names is field aliases3. Field aliases allow you to assign an alternative name to an existing field without changing the original field name or value2. By using field aliases, you can map different field names from different sources or sourcetypes to a common field name that conforms to the CIM standard3. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 12
- (Exam Topic 1)
Which are valid ways to create an event type? (select all that apply)

A. By using the searchtypes command in the search bar.
B. By editing the event_type stanza in the props.conf file.
C. By going to the Settings menu and clicking Event Types > New.
D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Answer: CD

Explanation:
Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error,

success, login, logout, etc. Event types can also be used to create transactions, alerts, reports, dashboards, etc. Event types can be created in two ways:

- By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type.
- By selecting an event in search results and clicking Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on the selected event.

Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event_type stanza in the transforms.conf file, not the props.conf file.

NEW QUESTION 14
- (Exam Topic 1)
When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.
B. The field being extracted will be required for all future events.
C. The events without the required field will not display in searches.
D. Only events with the required string will be included in the extraction.

Answer: D

Explanation:
The Field Extractor (FX) allows you to use regular expressions (regex) to extract fields from your events using a graphical interface or by manually editing the regex2. When you use the FX to perform a regex field extraction, you can use the require option to specify a string that must be present in an event for it to be included in the extraction2. This way, you can filter out events that do not contain the required string and focu on the events that are relevant for your extraction2. Therefore, option D is correct, while options A, B and C are incorrect.

NEW QUESTION 17
- (Exam Topic 1)
Which delimiters can the Field Extractor (FX) detect? (select all that apply)

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

Answer: BCD

Explanation:
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 18
- (Exam Topic 1)
A user wants to convert numeric field values to strings and also to sort on those values. Which command should be used first, the eval or the sort?

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

Answer: C

Explanation:
The eval command is used to create new fields or modify existing fields based on an expression2. The sort command is used to sort the results by one or more fields in ascending or descending order2. If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings2. This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

NEW QUESTION 21
- (Exam Topic 2)
When using a field value variable with a Workflow Action, which punctuation mark will escape the data

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

Answer: B

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

NEW QUESTION 26
- (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 31
- (Exam Topic 2)
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

Explanation:
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 34
- (Exam Topic 2)
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: B

Explanation:
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 37
- (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 39
- (Exam Topic 2)
Which command is used to create choropleth maps?

A. geostats
B. cluster
C. geom

Answer: C

NEW QUESTION 43
- (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 47
- (Exam Topic 2)
When can a pipe follow a macro?

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

Answer: A

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

NEW QUESTION 48
- (Exam Topic 2)

Information needed to create a GET workflow action includes which of the following? (select all that apply.)

A. A name of the workflow action
B. A URI where the user will be directed at search time.
C. A label that will appear in the Event Action menu at search time.
D. A name for the URI where the user will be directed at search time.

Answer: ABC

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction Information needed to create a GET workflow action includes the following: a name of the workflow action, a URI where the user will be directed at search time, and a label that will appear in the Event Action menu at search time. A GET workflow action is a type of workflow action that performs a GET request when you click on a field value in your search results. A GET workflow action can be configured with various options, such as:
A name of the workflow action: This is a unique identifier for the workflow action that is used internally by Splunk. The name should be descriptive and meaningful for the purpose of the workflow action.
A URI where the user will be directed at search time: This is the base URL of the external web service or application that will receive the GET request. The URI can include field value variables that will be replaced by the actual field values at search time. For example, if you have a field value variable ip, you can write it as http://example.com/ip=$ip to send the IP address as a parameter to the external web service or application.
A label that will appear in the Event Action menu at search time: This is the display name of the workflow action that will be shown in the Event Action menu when you click on a field value in your search results. The label should be clear and concise for the user to understand what the workflow action does.
Therefore, options A, B, and C are correct.

NEW QUESTION 52
- (Exam Topic 2)
This clause is used to group the output of a stats command by a specific name.

A. Rex
B. As
C. List
D. By

Answer: B

NEW QUESTION 55
- (Exam Topic 2)
Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

A. inputlookup
B. lookup

Answer: B

NEW QUESTION 56
- (Exam Topic 2)
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

Explanation:
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 57
- (Exam Topic 2)
What other syntax will produce exactly the same results as | chart count over vendor_action by user?

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

Answer: A

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

NEW QUESTION 60
- (Exam Topic 2)
In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

A. Selected-Fields
B. Non-Matches
C. Non-Extractions
D. Matches

Answer: B

Explanation:
The Field Extractor Utility (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 has a button that displays events that do not contain extracted fields, which is the Non-Matches button2. The Non-Matches button shows you the events that do not match the regular expression that you have defined for your field extraction2. This way, you can check if your field extraction is accurate and complete2. Therefore, option B is correct, while options A, C and D are incorrect because they are not buttons that display events that do not contain extracted fields.

NEW QUESTION 62
- (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 64
- (Exam Topic 2)
What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

A. There is a limit to the number of fields that can be extracted.
B. The user is unable to preview the extractions.
C. The extraction is added at index time.
D. The user is unable to return to the automatic field extraction workflow.

Answer: A

NEW QUESTION 67
- (Exam Topic 2)
Which type of visualization shows relationships between discrete values in three dimensions?

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

Answer: C

Explanation:
https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsBub

NEW QUESTION 72
- (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 76
- (Exam Topic 2)
A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being _____.

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

Answer: A

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

NEW QUESTION 81
- (Exam Topic 2)
Select this in the fields sidebar to automatically pipe you search results to the rare command

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

Answer: B

Explanation:
The fields sidebar is a panel that shows the fields that are present in your search results2. The fields sidebar has two sections: selected fields and interesting fields2. 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. Interesting field are fields that appear in at least 20 percent of events or have high variability among values2. For each field in the fields sidebar, you can select one of the following options: events with this field, rare values, top values by time or top values2. If you select rare values, Splunk will automatically pipe your search results to the rare command, which shows the least common values of a field2. Therefore, option B is correct, while options A, C and D are incorrect because they do not pipe your search results to the rare command.

NEW QUESTION 85
- (Exam Topic 2)
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

Explanation:
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 87
- (Exam Topic 2)
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

Explanation:
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 92
- (Exam Topic 2)
Which of the following examples would use a POST workflow action?

A. Perform an external IP lookup based on a domain value found in events.
B. Use the field values in an HTTP error event to create a new ticket in an external system.
C. Launch secondary Splunk searches that use one or more field values from selected events.
D. Open a web browser to look up an HTTP status code.

Answer: B

Explanation:
The correct answer is B. Use the field values in an HTTP error event to create a new ticket in an external system.
A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create HTML links, generate HTTP POST requests, or launch secondary searches based on field values1.
There are three types of workflow actions that can be set up using Splunk Web: GET, POST, and Search2.

- GET workflow actions create typical HTML links to do things like perform Google searches on specific values or run domain name queries against external WHOIS databases2.
- POST workflow actions generate an HTTP POST request to a specified URI. This action type enables you to do things like creating entries in external issue management systems using a set of relevant field values2.
- Search workflow actions launch secondary searches that use specific field values from an event, such as a search that looks for the occurrence of specific combinations of ipaddress and http_status field values in your index over a specific time range2.

Therefore, the example that would use a POST workflow action is B. Use the field values in an HTTP error event to create a new ticket in an external system. This example requires sending an HTTP POST request to the URI of the external system with the field values from the event as arguments.
The other examples would use different types of workflow actions. These examples are:

- A. Perform an external IP lookup based on a domain value found in events: This example would use a GET workflow action to create a link to an external IP lookup service with the domain value as a parameter.
- C. Launch secondary Splunk searches that use one or more field values from selected events: This example would use a Search workflow action to run another Splunk search with the field values from the event as search terms.
- D. Open a web browser to look up an HTTP status code: This example would also use a GET workflow action to create a link to a web page that explains the meaning of the HTTP status code.

References:

- Splexicon:Workflowaction
- About workflow actions in Splunk Web

NEW QUESTION 94
- (Exam Topic 2)
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: B

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Chart https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Stats

NEW QUESTION 98
- (Exam Topic 2)
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

Explanation:
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 101
- (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 105
- (Exam Topic 2)
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

Explanation:
The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole.
Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.
https://docs.splunk.com/Splexicon:Datamodeldataset

NEW QUESTION 106
- (Exam Topic 2)
This is what Splunk uses to categorize the data that is being indexed.

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

Answer: B

NEW QUESTION 108
- (Exam Topic 2)
This is what Splunk uses to categorize the data that is being indexed.

A. sourcetype
B. index
C. source
D. host

Answer: A

NEW QUESTION 111
- (Exam Topic 2)
When is a GET workflow action needed?

A. To send field values to an external resource.
B. To retrieve information from an external resource.
C. To use field values to perform a secondary search.
D. To define how events flow from forwarders to indexes.

Answer: B

NEW QUESTION 113
- (Exam Topic 2)
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

Explanation:
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 114
- (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 116
- (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 117
- (Exam Topic 2)
Consider the following search: index=web sourcetype=access_corabined
The log shows several events that share the same jsesszonid value (SD462K101O2F267). View the events as a group.
From the following list, which search groups events by jSSESSIONID?

A. index=web sourcetype=access_combined I transaction JSESSZONID I search SD462K101C2F267
B. index=web sourcetype=access_combined SD462K101O2F267 | table JSESSIONID
C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD462K101O2F267
D. index=web sourcetype=access_combined JSESSTONID <SD4€2K101O2F267>

Answer: A

Explanation:
The transaction command groups events that share a common value in a specified field, such as JSESSIONID, and that occur within a specified time range. The search command filters the results to show only the events that match the given value of JSESSIONID. This search groups the events by JSESSIONID and then shows only the events that have the value SD462K101C2F267 for JSESSIONID2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command.

NEW QUESTION 122
- (Exam Topic 2)
The fields sidebar does not show _____. (Select all that apply.)

A. interesting fields
B. selected fields
C. all extracted fields

Answer: C

Explanation:
The fields sidebar is a panel that shows the fields that are present in your search results2. The fields sidebar does not show all extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs2. The fields sidebar only shows selected fields and interesting fields2. 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. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. Therefore, option C is correct, while options A and B are incorrect because they are types of fields that the fields sidebar does show.

NEW QUESTION 126
- (Exam Topic 2) Consider the following search: Index=web sourcetype=access_combined
The log shows several events that share the same JSESSIONID value (SD404K289O2F151). View the events as a group. From the following list, which search groups events by JSESSIONID?

A. index=web sourcetype=access_combined SD404K289O2F151 I table JSESSIONID
B. index=web sourcetype=access_combined JSESSIONID <SD404K289O2F151>
C. index=web sourcetype=access_combined I highlight JSESSIONID I search SD404K289O2F151
D. index-web sourcetype=access_combined I transaction JSESSIONID I search SD404K289O2F151

Answer: B

NEW QUESTION 127
- (Exam Topic 2)
Which statement is true?

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

Answer: C

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

NEW QUESTION 131
- (Exam Topic 2)
Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

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

Answer: A

Explanation:
The correct answer is A. Field alias123.
In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field3. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)12.
The CIM provides a methodology for normalizing values to a common field name1. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact2. By using field aliases, you can map vendor fields to common fields that are the same for each data source in a given domain4. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention1.

NEW QUESTION 136
- (Exam Topic 2)
Use the dedup command to _____.

A. Rename a field in the index
B. remove duplicate values
C. provide an additional alias for the field that can
D. be used in the search criteria

Answer: B

NEW QUESTION 139
- (Exam Topic 2)
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

Explanation:
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 143
- (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 147
- (Exam Topic 2)
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

Explanation:
The correct answer is B. eventtype=web_errors.
An event type is a way to categorize events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports1.
To search for events that have a specific event type, you need to use the eventtype field with the name of the event type as the value. The syntax for this is:
eventtype=<event_type_name>
For example, if you want to search for events that have the event type web_errors, you can use the following syntax:
eventtype=web_errors
This will return only the events that match the search criteria defined by the web_errors event type.

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

- A. tag=web_errors: This option uses the tag field, which is a way to add descriptive keywords to events based on field values. Tags are different from event types, although they can be used together. Tags can be used to filter and group events by common characteristics2.
- C. eventtype “web errors”: This option uses quotation marks around the event type name, which is not valid syntax for the eventtype field. Quotation marks are used to enclose phrases or exact matches in a search3.
- D. eventtype (web_errors): This option uses parentheses around the event type name, which is also not valid syntax for the eventtype field. Parentheses are used to group expressions or terms in a search3.

References:

- About event types
- About tags
- Search command cheatsheet

NEW QUESTION 152
- (Exam Topic 2)
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

Explanation:
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 155
- (Exam Topic 2)
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

Explanation:
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 159
- (Exam Topic 2)
Clicking a SEGMENT on a chart, _____.

A. drills down for that value
B. highlights the field value across the chart
C. adds the highlighted value to the search criteria

Answer: C

NEW QUESTION 163
- (Exam Topic 2)
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: AB

Explanation:
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 165
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1002 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-1002-dumps.html