Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

NEW QUESTION 1
- (Exam Topic 1)
When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

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

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtypes When multiple event types with different color values are assigned to the same event, the color displayed for the events is determined by the priority of the event types. The priority is a numerical value that indicates how important an event type is. The higher the priority, the more important the event type. The event type with the highest priority will determine the color of the event.

NEW QUESTION 2
- (Exam Topic 1)
Which of the following searches show a valid use of macro? (Select all that apply)

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

Answer: AC

Explanation:
Reference:
https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html
To use a macro in a search, you must enclose the macro name and any arguments in single quotation marks1. For example, 'my_macro(arg1,arg2)' is a valid way to use a macro with two arguments. You can use macro anywhere in your search string where you would normally use a search command or expression1. Therefore, options A and C are valid searches that use macros, while options B and D are invalid because they do not enclose the macros in single quotation marks.

NEW QUESTION 3
- (Exam Topic 1)
What is required for a macro to accept three arguments?

A. The macro's name ends with (3).
B. The macro's name starts with (3).
C. The macro's argument count setting is 3 or more.
D. Nothing, all macros can accept any number of arguments.

Answer: A

Explanation:
To create a macro that accepts arguments, you must include the number of arguments in parentheses at the end of the macro name1. For example, my_macro(3) is a macro that accepts three arguments. The number of arguments in the macro name must match the number of arguments in the definition1. Therefore, option A is correct, while options B, C and D are incorrect.

NEW QUESTION 4
- (Exam Topic 1)
What do events in a transaction have In common?

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

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions
A transaction is a group of events that share some common characteristics, such as fields, time, or both. A transaction can be created by using the transaction command or by defining an event type with transactiontype=true in props.conf. Events in a transaction have one or more fields in common that relate them to each other. For example, you can create a transaction based on JSESSIONID, which is a unique identifier for each user session in web logs. Events in a transaction do not have to have the same timestamp, sourcetype, or exact same set of fields. They only have to share one or more fields that define the transaction.

NEW QUESTION 5
- (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 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)
Data model are composed of one or more of which of the following datasets? (select all that apply.)

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

Answer: ABC

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels
Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:
Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.
Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.
Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 1)
A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

A. Both will appear in the All Fields list, but only if the alias is specified in the search.
B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Answer: B

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

NEW QUESTION 10
- (Exam Topic 1)
Which of the following statements describes this search? sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

A. This is a valid search and will display a timechart of the average duration, of each transaction event.
B. This is a valid search and will display a stats table showing the maximum pause among transactions.
C. No results will be returned because the transaction command must include the startswith and endswith options.
D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Answer: A

Explanation:
This search uses the transaction command to group events that share a common value for JSESSIONID into transactions1. The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction1. The search then uses the timechart command to create a time-series chart of the average duration of each transaction1. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field. Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction1. Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search1.

NEW QUESTION 15
- (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 18
- (Exam Topic 1)
What does the transaction command do?

A. Groups a set of transactions based on time.
B. Creates a single event from a group of events.
C. Separates two events based on one or more values.
D. Returns the number of credit card transactions found in the event logs.

Answer: B

Explanation:

The transaction command is a search command that creates a single event from a group of events that share some common characteristics. The transaction command can group events based on fields, time, or both. The transaction command can also create some additional fields for each transaction, such as duration, eventcount, startime, etc. The transaction command does not group a set of transactions based time, but rather groups a set of events into a transaction based on time. The transaction command does not separate two events based on one or more values, but rather joins multiple events based on one or more values. The transaction command does not return the number of credit card transactions found in the event logs, but rather creates transactions from the events that match the search criteria.

NEW QUESTION 23
- (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 26
- (Exam Topic 1)
Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

A. Auto-Extracted fields can be hidden in Pivot.
B. Auto-Extracted fields can have their data type changed.
C. Auto-Extracted fields can be given a friendly name for use in Pivot.
D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Answer: ABCD

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

NEW QUESTION 30
- (Exam Topic 1)
What is the relationship between data models and pivots?

A. Data models provide the datasets for pivots.
B. Pivots and data models have no relationship.
C. Pivots and data models are the same thing.
D. Pivots provide the datasets for data models.

Answer: A

Explanation:
The relationship between data models and pivots is that data models provide the datasets for pivots. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivots are user interfaces that allow you to create data visualizations that present different aspects of a data model. Pivots let you select options from menus and forms to create charts, tables, maps, etc., without writing any SPL code. Pivots use datasets from data models as their source of data. Pivots and data models are not the same thing, as pivots are tools for visualizing data models. Pivots do not provide datasets for data models, but rather use them as inputs.
Therefore, only statement A is true about the relationship between data models and pivots.

NEW QUESTION 32
- (Exam Topic 1)
Which of the following statements describe calculated fields? (select all that apply)

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

Answer: ABD

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

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

NEW QUESTION 33
- (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 34
- (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 35
- (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 40
- (Exam Topic 2)
Which of the following searches will show the number of categoryld used by each host?

A. Sourcetype=access_* |sum bytes by host
B. Sourcetype=access_* |stats sum(categoryl
C. by host
D. Sourcetype=access_* |sum(bytes) by host
E. Sourcetype=access_* |stats sum by host

Answer: B

NEW QUESTION 45
- (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 47
- (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 50
- (Exam Topic 2)
What fields does the transaction command add to the raw events? (select all that apply)

A. count
B. duration
C. eventcount
D. transaction id

Answer: BD

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

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

NEW QUESTION 53
- (Exam Topic 2)
When using the timechart command, how can a user group the events into buckets based on time?

A. Using the span argument.
B. Using the duration argument.
C. Using the interval argument.
D. Adjusting the fieldformat options.

Answer: A

NEW QUESTION 57
- (Exam Topic 2)
What information must be included when using the datamodel command?

A. status field
B. Multiple indexes
C. Data model field name.
D. Data model dataset name.

Answer: D

NEW QUESTION 58
- (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 59
- (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 62
- (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 64
- (Exam Topic 2)
How are event types different from saved reports?

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

Answer: D

Explanation:
Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies. The correct answer is D. Event types do not include a time range.
The explanation is as follows:
- Event types are a categorization system that help you make sense of your data by matching events with the same search string1. Event types are applied to events at search time and can be used as search terms or filters12.
- Saved reports are results saved from a search action that can show statistics and visualizations of events3. Saved reports can be run anytime, and they fetch fresh results each time they are run34. Saved reports can be shared with other users and added to dashboards4.
- The main difference between event types and saved reports is that event types do not include a time range, while saved reports do14. This means that event types can match events from any time period, while saved reports are limited by the time range specified when they are created or run14.

NEW QUESTION 68
- (Exam Topic 2)
Which of the following eval commands will provide a new value for host from src if it exists?

A. | eval host = if (isnu11 (src), src, host)
B. | eval host = if (NOT src = host, src, host)
C. | eval host = if (src = host, src, host)
D. | eval host = if (isnotnull (src), src, host)

Answer: D

Explanation:

- The eval command is a Splunk command that allows you to create or modify fields using expressions .
- The if function is an expression that evaluates a condition and returns a value based on whether the condition is true or false. The syntax of the if function is if(X,Y,Z), where X is the condition, Y is th value to return if X is true, and Z is the value to return if X is false.
- The isnotnull function is an expression that returns true if the argument is not null, and false otherwise The syntax of the isnotnull function is isnotnull(X), where X is the argument to check.
- Therefore, the expression if (isnotnull (src), src, host) returns the value of src if it is not null, and th value of host otherwise. This means that it will provide a new value for host from src if it exist keep the original value of host otherwise.

NEW QUESTION 70
- (Exam Topic 2)
Which of the following is true about Pivot?

A. Users can save reports from Pivot.
B. Users cannot share visualizations created with Pivot.
C. Users must use SPL to find events in a Pivot.
D. Users cannot create visualizations with Pivot.

Answer: A

Explanation:
In Splunk, Pivot is a tool that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL™)1. You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations12.
One of the features of Pivot is that it allows you to save your reports1. This can be useful when you want to reuse a report or share it with others1. Therefore, it's not true that users cannot share visualizations created with Pivot or that they must use SPL to find events in a Pivot12. It's also not true that users cannot create visualizations with Pivot, as creating visualizations is one of the main functions of Pivot12.

NEW QUESTION 73
- (Exam Topic 2)
When would a user select delimited field extractions using the Field Extractor (FX)?

A. When a log file has values that are separated by the same character, for example, commas.
B. When a log file contains empty lines or comments.
C. With structured files such as JSON or XML.
D. When the file has a header that might provide information about its structure or format.

Answer: A

Explanation:
The correct answer is A. When a log file has values that are separated by the same character, for example, commas.
The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions1.
The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them1.
The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds1.
Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions.
The other options are not correct because they are not suitable for the delimited field extraction method. These options are:
- B. When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or include some unwanted values.
- C. With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions2. The delimited method might not work well with this type of data, as it might not recognize the nested structure or the special characters.
- D. When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data, as it might not be able to identify the fields based on the header information.

References:
- Build field extractions with the field extractor
- Configure indexed field extraction

NEW QUESTION 78
- (Exam Topic 2)
When a search returns _____, you can view the results as a list.

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

Answer: C

NEW QUESTION 83
- (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 87
- (Exam Topic 2)
Which of the following statements are true for this search? (Select all that apply.)
SEARCH: sourcetype=access* |fields action productId status

A. is looking for all events that include the search terms: fields AND action AND productId AND status
B. users the table command to improve performance
C. limits the fields are extracted
D. returns a table with 3 columns

Answer: C

NEW QUESTION 89
- (Exam Topic 2)
When should transaction be used?

A. Only in a large distributed Splunk environment.
B. When calculating results from one or more fields.
C. When event grouping is based on start/end values.
D. When grouping events results in over 1000 events in each group.

Answer: C

NEW QUESTION 94
- (Exam Topic 2)
Which of the following objects can a calculated field use as a source?

A. An alias of a field.
B. A field added by an automatic lookup.
C. The tag field.
D. The eventtype field.

Answer: B

Explanation:
The correct answer is B. A field added by an automatic lookup.
A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can use any field as a source, as long as the field is extracted before the calculated field is defined1.
An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field2. An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields3.
Therefore, a calculated field can use a field added by an automatic lookup as a source. References:

- About calculated fields
- About lookups
- Search time processing

NEW QUESTION 96
- (Exam Topic 2)
Which of the following statements about tags is true? (select all that apply.)

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

Answer: BD

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

- Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a

tag called “alert” for the field name “status” and the field value “critical”. This means that only events that have status=critical will have the “alert” tag applied to them.

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

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

NEW QUESTION 100
- (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 104
- (Exam Topic 2)
Why are tags useful in Splunk?

A. Tags look for less specific data.
B. Tags visualize data with graphs and charts.
C. Tags group related data together.
D. Tags add fields to the raw event data.

Answer: C

Explanation:
Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as router, and then search for tag=router to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values. For example, you can tag the field values error, fail, and critical as severity=high, and then search for severity=high to find all the events with high severity level2
1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION 105
- (Exam Topic 2)
How is an event type created from the search window? (select all that apply)

A. In the top right corner, click Save As > Event Type.
B. In an event's detail dropdown, click Event Actions > Build Event Type.
C. Edit eventtypes.conf and add a new stanza.
D. Add | eventtype to the SPL and execute the search.

Answer: AC

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

NEW QUESTION 110
- (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 113
- (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 118
- (Exam Topic 2)
If a calculated field has the same name as an extracted field, what happens to the extracted field?

A. The calculated field will override the extracted field.
B. The calculated and extracted fields will be combined.
C. The calculated field will duplicate the extracted field.
D. An error will be returned and the search will fail.

Answer: A

Explanation:
When you define a calculated field, you can specify the name of the field that the eval expression will create or modify. If the name of the calculated field matches the name of an existing extracted field, the calculated field will override the extracted field and replace its value with the result of the eval expression. This means that the original value of the extracted field will not be available for searching or analysis. To avoid this, you should use a unique name for your calculated field or use a different name for your extracted field2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Configure calculated fields with props.conf.

NEW QUESTION 121
- (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 124
- (Exam Topic 2)
Which command can include both an over and a by clause to divide results into sub-groupings?

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

Answer: A

NEW QUESTION 126
- (Exam Topic 2)
Which is not a comparison operator in Splunk

A. <=
B. =
C. !=
D. >
E. ?=

Answer: E

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

NEW QUESTION 130
- (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 132
- (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 133
- (Exam Topic 2)
This function of the stats command allows you to identify the number of values a field has.

A. max
B. distinct_count
C. fields
D. count

Answer: D

NEW QUESTION 136
- (Exam Topic 2)
Which of the following is NOT a stats function:

A. sum
B. addtotals
C. count
D. avg

Answer: B

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

NEW QUESTION 141
- (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 142
- (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 145
- (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 150
- (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 151
- (Exam Topic 2)
Why would the following search produce multiple transactions instead of one?

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

Events (641) Patterns **Statistics (147)** Visualization

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

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

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

Answer: A

Explanation:
The correct answer is A. The maxspan option is not included1.
In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1.
However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.
Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.
Here is an example of how you can use the maxspan option in a search:
index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h
In this search, the transaction command groups events that share the same someuniqefield value into a single transaction, but only if the time span between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

NEW QUESTION 153
- (Exam Topic 2)
Which of the following searches will return all clientip addresses that start with 108?

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

Answer: A

NEW QUESTION 156
- (Exam Topic 2)
which of the following are valid options with the chart command

A. useother
B. usenull
C. fillfield
D. usefiled

Answer: AB

NEW QUESTION 159
- (Exam Topic 2)
The time range specified for a historical search defines the _____.------questionable on ans

A. Amount of data shown on the timeline as data streams in
B. Amount of data fetched from index matching that time range

C. Time range for the static results

Answer: B

Explanation:
The time range specified for a historical search defines the amount of data fetched from the index matching that time range2. A historical search is a search that runs over a fixed period of time in the past2. When you run a historical search, Splunk searches the index for events that match your search string and fall within the specified time range2. Therefore, option B is correct, while options A and C are incorrect because they are not what the time range defines for a historical search.

NEW QUESTION 162
- (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 164
- (Exam Topic 2)
How is a Search Workflow Action configured to run at the same time range as the original search?

A. Set the earliest time to match the original search.
B. Select the same time range from the time-range picker.
C. Select the "Use the same time range as the search that created the field listing" checkbox.
D. Select the "Overwrite time range with the original search" checkbox.

Answer: C

Explanation:
To configure a Search Workflow Action to run at the same time range as the original search, you need to
select the “Use the same time range as the search that created the field listing” checkbox. This will ensure that the workflow action search uses the same earliest and latest time parameters as the original search.

NEW QUESTION 169
- (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 173
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-1002 Practice Test Here