Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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

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 statements about tags is true?

A. Tags are case insensitive.
B. Tags are created at index time.
C. Tags can make your data more understandable.
D. Tags are searched by using the syntax tag: : <fieldneme>

Answer: C

Explanation:
Tags are aliases or alternative names for field values in Splunk. They can make your data more understandable by using common or descriptive terms instead of cryptic or technical terms. For example, you can tag a field value such as “200” with “OK” or “success” to indicate that it is a HTTP status code for a successful request. Tags are case sensitive, meaning that “OK” and “ok” are different tags. Tags are created at search time, meaning that they are applied when you run a search on your data. Tags are searched by using the syntax tag::<tagname>, where <tagname> is the name of the tag you want to search for.

NEW QUESTION 3
- (Exam Topic 1)
Which of the following Statements about macros is true? (select all that apply)

A. Arguments are defined at execution time.
B. Arguments are defined when the macro is created.
C. Argument values are used to resolve the search string at execution time.
D. Argument values are used to resolve the search string when the macro is created.

Answer: BC

Explanation:
A macro is a way to save a commonly used search string as a variable that you can reuse in other searches1. When you create a macro, you can define arguments that are placeholders for values that you specify at execution time1. The argument values are used to resolve the search string when the macro is invoked, not when it is created1. Therefore, statements B and C are true, while statements A and D are false.

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
Which of the following statements describes Search workflow actions?

A. By defaul
B. Search workflow actions will run as a real-time search.
C. Search workflow actions can be configured as scheduled searches,
D. The user can define the time range of the search when created the workflow action.

E. Search workflow actions cannot be configured with a search string that includes the transaction command

Answer: C

Explanation:
Search workflow actions are custom actions that run a search when you click on a field value in your search results. Search workflow actions can be configured with various options, such as label name, search string, time range, app context, etc. One of the options is to define the time range of the search when creating the workflow action. You can choose from predefined time ranges, such as Last 24 hours, Last 7 days, etc., or
specify a custom time range using relative or absolute time modifiers. Search workflow actions do not run as real-time searches by default, but rather use the same time range as the original search unless specified otherwise. Search workflow actions cannot be configured as scheduled searches, as they are only triggered by user interaction. Search workflow actions can be configured with any valid search string that includes any search command, such as transaction.

NEW QUESTION 6
- (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 7
- (Exam Topic 1)
Which of the following statements about data models and pivot are true? (select all that apply)

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

Answer: D

Explanation:
Data models and pivot are both knowledge objects in Splunk that allow you to analyze and visualize your data in different ways. 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. Pivot is a user interface that allows you to create data visualizations that present different aspects of a data model. Pivot does not require users to input SPL searches on data models, but rather lets them select options from menus and forms. Data models are not created out of datasets called pivots, but rather pivots are created from datasets in data models.

NEW QUESTION 8
- (Exam Topic 1)
Which of the following knowledge objects represents the output of an eval expression?

A. Eval fields
B. Calculated fields
C. Field extractions
D. Calculated lookups

Answer: B

Explanation:
Reference: https://docs.splunk.com/Splexicon:Calculatedfield
The eval command is used to create new fields or modify existing fields based on an expression2. The output of an eval expression is a calculated field, which is a field that you create based on the value of another field or fields2. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format2. Therefore, option B is correct, while options A, C and D are incorrect because they are not names of knowledge objects that represent the output of an eval expression.

NEW QUESTION 9
- (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 10
- (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.

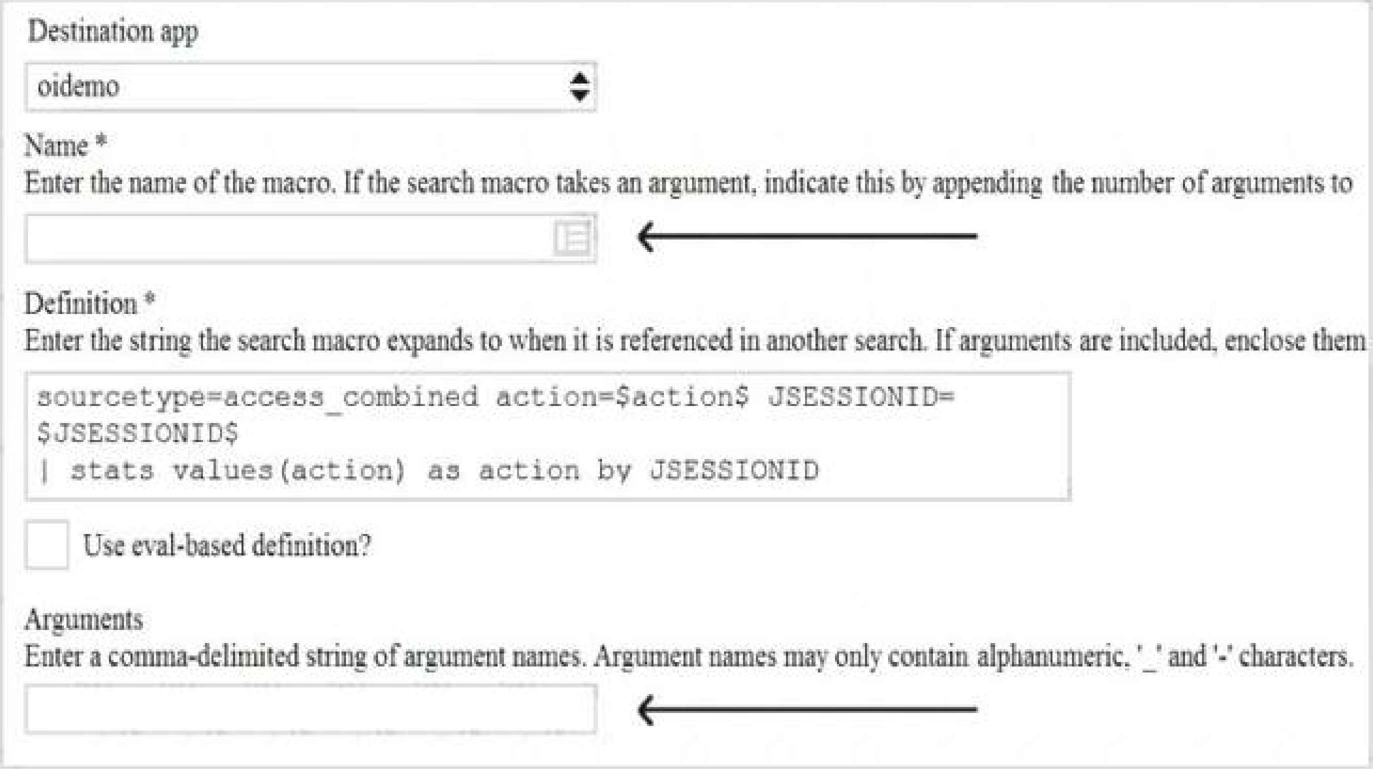
NEW QUESTION 10
- (Exam Topic 1)
When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

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

Answer: ABD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep https://community.splunk.com/t5/Splunk-Search/Field-Extraction-Separate-on-Colon/m-p/29751
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. Some of the delimiters that will work with FX are:
Tabs: horizontal spaces that align text in columns.
Pipes: vertical bars that often indicate logical OR operations. Spaces: blank characters that separate words or symbols. Therefore, the delimiters A, B, and D will work with FX.

NEW QUESTION 14
- (Exam Topic 1)
Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



Destination app
oidemo
Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to
Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

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

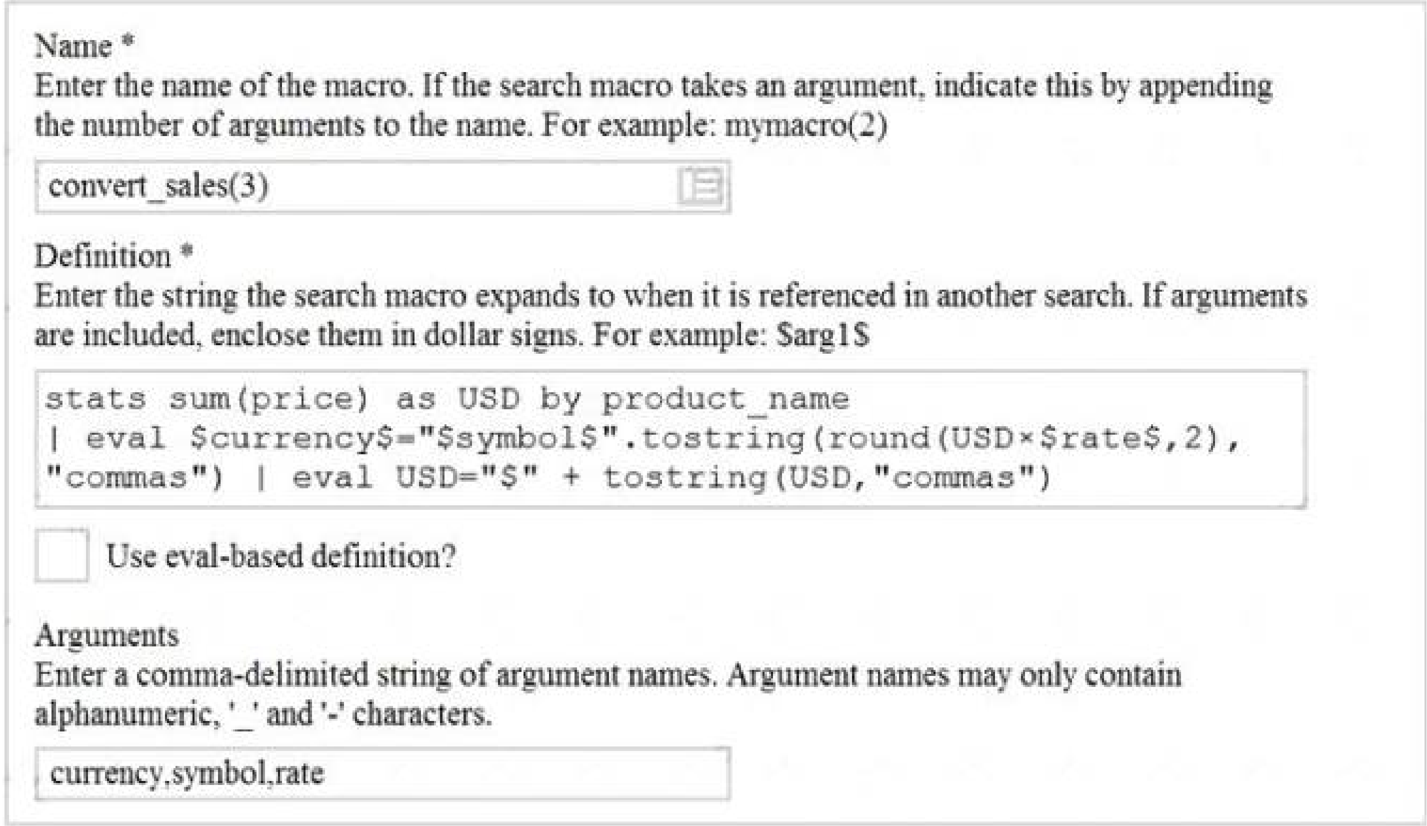
□ Use eval-based definition?
Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

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

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros
The macro definition below shows a macro that tracks user sessions based on two arguments: action and JSESSIONID.
sessiontracker(2)
The macro definition does the following:
It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string.
It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when it is executed.
It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them. In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.
Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.

NEW QUESTION 19
- (Exam Topic 1)
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



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

convert_sales(3)

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

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

□ Use eval-based definition?

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

currency,symbol,rate

A. Convert_sales (euro, €, 79)”
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 21
- (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 24
- (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 26
- (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 29
- (Exam Topic 1)
To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

A. Index-main | REJECT trans sessionid
B. Index-main | transaction sessionid | search REJECT
C. Index=main | transaction sessionid | whose transaction=reject
D. Index=main | transaction sessionid | where transaction=reject’’

Answer: B

Explanation:
The transaction command is used to group events that share a common value for one or more fields into transactions2. The transaction command assigns a transaction ID to each group of events and creates new fields such as duration, eventcount and eventlist for each transaction2. To identify all of the contributing events within a transaction that contains at least one REJECT event, you can use the following
syntax: index=main | transaction sessionid | search REJECT2. This search will first group the events by sessionid, then filter out the transactions that do not contain REJECT in any of their events2. Therefore, option B is correct, while options A, C and D are incorrect because they do not follow the correct syntax for using the transaction command or the search command.

NEW QUESTION 33
- (Exam Topic 1)
Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

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

Answer: ABC

Explanation:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview
The Common Information Model (CIM) is a methodology for normalizing data from different sources and making it easier to analyze and report on it3. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more3. One of the statements that describe the CIM is that it is a methodology for normalizing data, which means that it provides a standard way to name and structure data from different sources so that they can be compared and correlated3. Therefore, option A is correct. Another statement that describes the CIM is that it can correlate data from different sources, which means that it enables you to run searches and reports across data from different sources that share common fields and tags3. Therefore, option B is correct. Another statement that describes the CIM is that the Knowledge Manager uses the CIM to create knowledge objects, which means that the person who is responsible for creating and managing knowledge objects such as data models, field aliases, tags and event types can use the CIM as a guide to make their knowledge objects consistent and compatible with other apps and add-ons3. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.

NEW QUESTION 38
- (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 40
- (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 44
- (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 47
- (Exam Topic 1)
Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

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

Answer: ABD

Explanation:
The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction.
index=main | transaction clientip host maxspan=30s maxpause=5s The search does the following:
- It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.
- It uses the transaction command to group events into transactions based on two fields: clientip and host.

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

NEW QUESTION 49
- (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.

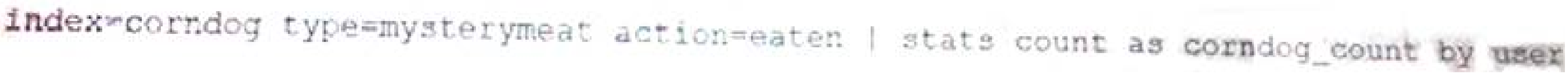
NEW QUESTION 51
- (Exam Topic 1)
Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

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 52
- (Exam Topic 1)
What does the following search do?



```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

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

Answer: B

Explanation:
The search string below creates a table of the total count of mysterymeat corndogs split by user.
| stats count by user | where corndog=mysterymeat The search string does the following:

➢ It uses the stats command to calculate the count of events for each value of the user field. The stats command creates a table with two columns: user and count.

➢ It uses the where command to filter the results by the value of the corndog field. The where command only keeps the rows where corndog equals mysterymeat.
Therefore, the search string creates a table of the total count of mysterymeat corndogs split by user.

NEW QUESTION 53
- (Exam Topic 1)
Which of the following workflow actions can be executed from search results? (select all that apply)

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

Answer: ABD

Explanation:
As mentioned before, there are two types of workflow actions: GET and POST1. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it1. Another type of workflow action is Search, which runs another search based on the field value1. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

NEW QUESTION 58
- (Exam Topic 1)
Which one of the following statements about the search command is true?

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

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand The search command is used to filter or refine your search results based on a search string that matches the events2. The search command behaves exactly like search strings before the first pipe, which means that you can use the same syntax and operators as you would use in the initial part of your search2. Therefore, option D is correct, while options A, B and C are incorrect because they are not true statements about the search command.

NEW QUESTION 59
- (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 62
- (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 66
- (Exam Topic 2)
Which of the following about reports is/are true?

A. Reports are knowledge objects.
B. Reports can be scheduled.
C. Reports can run a script.
D. All of the above.

Answer: D

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

NEW QUESTION 69
- (Exam Topic 2)
The timechart command is an example of which of the following command types?

A. Orchestrating
B. Transforming
C. Statistical
D. Generating

Answer: B

Explanation:
The correct answer is B. Transforming. The explanation is as follows:

- The timechart command is a Splunk command that creates a time series chart with corresponding table of statistics12.
- A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis1. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart1.
- Transforming commands are commands that change the format of the search results into a data structure that can be easily visualized3. Transforming commands often use stats functions to aggregate and summarize data3.
- Therefore, the timechart command is an example of a transforming command, as it transforms the search results into a chart and a table using stats functions123.

NEW QUESTION 72
- (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 77
- (Exam Topic 2)
What approach is recommended when using the Splunk Common Information Model (CIM) add-on to normalize data?

A. Consult the CIM data model reference tables.
B. Run a search using the authentication command.
C. Consult the CIM event type reference tables.
D. Run a search using the correlation command.

Answer: A

Explanation:
The recommended approach when using the Splunk Common Information Model (CIM) add-on to normalize data is A. Consult the CIM data model reference tables. This is because the CIM data model reference tables provide detailed information about the fields and tags that are expected for each dataset in a data model. By consulting the reference tables, you can determine which data models are relevant for your data source and how to map your data fields to the CIM fields. You can also use the reference tables to validate your data and troubleshoot any issues with normalization. You can find the CIM data model reference tables in the Splunk documentation1 or in the Data Model Editor page in Splunk Web2. The other options are incorrect because they are not related to the CIM add-on or data normalization. The authentication command is a custom command that validates events against the Authentication data model, but it does not help you to normalize other types of data. The correlation command is a search command that performs statistical analysis on event fields, but it does not help you to map your data fields to the CIM fields. The CIM event type reference tables do not exist, as event types are not part of the CIM add-on.

NEW QUESTION 81
- (Exam Topic 2)
In this search, ________ will appear on the y-axis. SEARCH: sourcetype=access_combined status!=200 | chart count over host

A. status
B. host
C. count

Answer: C

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

NEW QUESTION 84
- (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 86
- (Exam Topic 2)
What type of command is eval?

A. Streaming in some modes
B. Report generating
C. Distributable streaming
D. Centralized streaming

Answer: C

Explanation:
The correct answer is C. Distributable streaming. This is because the eval command is a type of command that can run on the indexers before the results are sent to the search head. This reduces the amount of data that needs to be transferred and improves the search performance. Distributable streaming commands can operate on each event or result individually, without depending on other events or results. You can learn more about the types of commands and how they affect search performance from the Splunk documentation1.

NEW QUESTION 88
- (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 91
- (Exam Topic 2)
What is the correct syntax to find events associated with a tag?

A. tag:<field>=<value>
B. tags=<value>
C. tags:<field>=<value>
D. tag=<value>

Answer: D

Explanation:
The correct syntax to find events associated with a tag in Splunk is tag=<value>1. So, the correct answer is D. tag=<value>. This syntax allows you to annotate specified fields in your search results with tags1.
In Splunk, tags are a type of knowledge object that you can use to add meaningful aliases to field values in your data1. For example, if you have a field called status_code in your data, you might have different status codes like 200, 404, 500, etc. You can create tags for these status codes like success for 200, not_found for 404, and server_error for 500. Then, you can use the tag command in your searches to find events associated with these tags1.
Here is an example of how you can use the tag command in a search: index=main sourcetype=access_combined | tag status_code
In this search, the tag command annotates the status_code field in the search results with the corresponding tags. If you have tagged the status code 200 with success, the status code 404 with not_found, and the status code 500 with server_error, the search results will include these tags1.
You can also use the tag command with a specific tag value to find events associated with that tag. For example, the following search finds all events where the status code is tagged with success:
index=main sourcetype=access_combined | tag status_code | search tag::status_code=success
In this search, the tag command annotates the status_code field with the corresponding tags, and the search command filters the results to include only events where the status_code field is tagged with success1.

NEW QUESTION 93
- (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 98
- (Exam Topic 2)
Using the export function, you can export search results as _________ .(Select all that apply)

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

Answer: AB

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

NEW QUESTION 100
- (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 105
- (Exam Topic 2)
We can use the rename command to ________ (Select all that apply.)

A. Change indexed fields
B. Exclude fields from our search results
C. Extract new fields from our data using regular expressions
D. Give a field a new name at search time

Answer: D

NEW QUESTION 110
- (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 114
- (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 117
- (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 121
- (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 123
- (Exam Topic 2)
Consider the the following search run over a time range of last 7 days: index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane
Which option is used to change the default time span so that results are grouped into 12 hour intervals?

A. span=12h

B. timespan=12h
C. span=12
D. timespan=12

Answer: A

Explanation:
The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals. The timespan option is not a valid option for the timechart command2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, timechart command.

NEW QUESTION 125
- (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 127
- (Exam Topic 2)
Which of the following commands support the same set of functions?

A. stats, eval, table
B. search, where, eval
C. stats, chart, timechart
D. transaction, chart, timechart

Answer: C

NEW QUESTION 129
- (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 130
- (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 132
- (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 135
- (Exam Topic 2)
Which method in the Field Extractor would extract the port number from the following event?
| 10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin <web error>

A. Delimiter
B. rex command
C. The Field Extractor tool cannot extract regular expressions.
D. Regular expression

Answer: B

Explanation:
The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:
rex "\+\+\+\+port (?<port>\d+)"
This will create a field called port with the value 54 for the event.
The delimiter method is not suitable for this event because there is no consistent delimiter between the fields. The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.
Reference: 1
Splunk Core Certified Power User | Splunk

NEW QUESTION 140
- (Exam Topic 2)
These allow you to categorize events based on search terms. Select your answer.

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

Answer: B

NEW QUESTION 145
- (Exam Topic 2)
Which of the following statements describes the use of the Field Extractor (FX)?

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

Answer: C

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

NEW QUESTION 146
- (Exam Topic 2)
Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

A. POST
B. Search
C. GET
D. Format

Answer: A

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

NEW QUESTION 150
- (Exam Topic 2)
Complete the search, …. | _______ failure>successes

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

Answer: B

Explanation:
The where command can be used to complete the search below.
… | where failure>successes
The where command is a search command that allows you to filter events based on complex or custom criteria. The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.
The search string below does the following:
- It uses … to represent any search criteria or commands before the where command.
- It uses the where command to filter events based on a comparison between two fields: failure and successes.
- It uses the greater than operator (>) to compare the values of failure and successes fields for each event.
- It only keeps events where failure is greater than successes.

NEW QUESTION 155
- (Exam Topic 2)
In the Field Extractor, when would the regular expression method be used?

A. When events contain JSON data.
B. When events contain comma-separated data.
C. When events contain unstructured data.
D. When events contain table-based data.

Answer: C

Explanation:
The correct answer is C. When events contain unstructured data.
The regular expression method works best with unstructured event data, such as log files or text messages, where the fields are not separated by a common delimiter, such as a comma or space1. You select a sample event and highlight one or more fields to extract from that event, and the field extractor generates a regular expression that matches similar events in your dataset and extracts the fields from them1. The regular expression method provides several tools for testing and refining the accuracy of the regular expression. It also allows you to manually edit the regular expression1.
The delimiters 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 or space1. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds1. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats1.
Reference:
1: Build field extractions with the field extractor - Splunk Documentation

NEW QUESTION 158
- (Exam Topic 2)
If a search returns _______ it can be viewed as a chart.

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

Answer: B

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

can be viewed as a chart.

NEW QUESTION 162
- (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 163
- (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 167
- (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 172
- (Exam Topic 2)
When using | timechart by host, which field is represented in the x-axis?

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

Answer: D

Explanation:

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

NEW QUESTION 177
- (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 180
- (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 182
- (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 187
- (Exam Topic 2)
When using | timchart by host, which filed is representted in the x-axis?

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

Answer: A

NEW QUESTION 192
- (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 196
- (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 201
- (Exam Topic 2)
Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

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

Answer: D

NEW QUESTION 205
- (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 210

- (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 212
- (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 215
- (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 220
- (Exam Topic 2)
What is a limitation of searches generated by workflow actions?

A. Searches generated by workflow action cannot use macros.
B. Searches generated by workflow actions must be less than 256 characters long.
C. Searches generated by workflow action must run in the same app as the workflow action.
D. Searches generated by workflow action run with the same permissions as the user running them.

Answer: D

NEW QUESTION 222
- (Exam Topic 2)
It is mandatory for the lookup file to have this for an automatic lookup to work.

A. Source type
B. At least five columns
C. Timestamp
D. Input filed

Answer: D

NEW QUESTION 223
- (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 224
- (Exam Topic 2)
There are several ways to access the field extractor. Which option automatically identifies data type, source type, and sample event?

A. Event Actions > Extract Fields
B. Fields sidebar > Extract New Field
C. Settings > Field Extractions > New Field Extraction
D. Settings > Field Extractions > Open Field Extraction

Answer: B

Explanation:
There are several ways to access the field extractor. The option that automatically identifies data type, source type, and sample event is Fields sidebar > Extract New Field. The field extractor is a tool that helps you extract fields from your data using delimiters or regular expressions. The field extractor can generate a regex for you based on your selection of sample values or you can enter your own regex in the field extractor. The field extractor can be accessed by using various methods, such as:

- Fields sidebar > Extract New Field: This is the easiest way to access the field extractor. The fields sidebar is a panel that shows all available fields for your data and their values. When you click on Extract New Field in the fields sidebar, Splunk will automatically identify the data type, source type, and sample event for your data based on your current search criteria. You can then use the field extractor to select sample values and generate a regex for your new field.
- Event Actions > Extract Fields: This is another way to access the field extractor. Event actions are actions that you can perform on individual events in your search results, such as viewing event details, adding to report, adding to dashboard, etc. When you click on Extract Fields in the event actions menu, Splunk will use the current event as the sample event for your data and ask you to select the source type and data type for your data. You can then use the field extractor to select sample values and generate a regex for your new field.
- Settings > Field Extractions > New Field Extraction: This is a more advanced way to access the field extractor. Settings is a menu that allows you to configure various aspects of Splunk, such as indexes, inputs, outputs, users, roles, apps, etc. When you click on New Field Extraction in the Settings menu, Splunk will ask you to enter all the details for your new field extraction manually, such as app context, name, source type, data type, sample event, regex, etc. You can then use the field extractor to verify or modify your regex for your new field.

NEW QUESTION 226
- (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 230
- (Exam Topic 2)
Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

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

Answer: B

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

NEW QUESTION 233
- (Exam Topic 2)
What will you learn from the results of the following search? sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

A. The average time elapsed during each transaction for all transactions
B. The average time for each event within each transaction
C. The average time between each transaction

Answer: A

NEW QUESTION 237
- (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 241
- (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 245
- (Exam Topic 2)
Which of the following is a feature of the Pivot tool?

A. Creates lookups without using SPL.
B. Data Models are not required.
C. Creates reports without using SPL
D. Datasets are not required.

Answer: C

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

NEW QUESTION 248
- (Exam Topic 2)
The stats command will create a _______ by default.

A. Table
B. Report
C. Pie chart

Answer: A

NEW QUESTION 249
- (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 252

- (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 254
- (Exam Topic 2)
The macro weekly sales (2) contains the search string: index=games | eval ProductSales = $Price$ * $AmountSold$
Which of the following will return results?

A. ‘weekly sales (3)’
B. ‘weekly_sales($3.995, $108)’
C. ‘weekly_sales (3.99, 10)’
D. ‘weekly sales (3.99, 10)’

Answer: C

Explanation:
To use a search macro in a search string, you need to place a back tick character (`) before and after the macro name1. You also need to use the same number of arguments as defined in the macro2. The macro weekly sales (2) has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.
The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses spaces instead of commas to separate the argument values.
Reference: 1 Use search macros in searches - Splunk Documentation 2 Define search macros in Settings - Splunk Documentation

NEW QUESTION 255
- (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 260
- (Exam Topic 2)
Which of the following commands will show the maximum bytes?

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

Answer: C

NEW QUESTION 263
- (Exam Topic 2)
Highlighted search terms indicate ________ search results in Splunk.

A. Display as selected fields.
B. Sorted
C. Charted based on time
D. Matching

Answer: D

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

NEW QUESTION 266
- (Exam Topic 2)
Which workflow action type performs a secondary search?

A. POST
B. Drilldown
C. GET
D. Search

Answer: D

Explanation:
The correct answer is D. Search.
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 workflow action type that performs a secondary search is Search. References:

- Splexicon:Workflowaction
- About workflow actions in Splunk Web

NEW QUESTION 270
- (Exam Topic 2)
which of the following commands are used when creating visualizations(select all that apply.)

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

Answer: ACD

Explanation:
The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are:

- geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions.
- geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters.
- iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

NEW QUESTION 272
- (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 274
- (Exam Topic 2)
Which workflow uses field values to perform a secondary search?

A. POST
B. Action
C. Search
D. Sub-Search

Answer: C

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb

NEW QUESTION 278
- (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

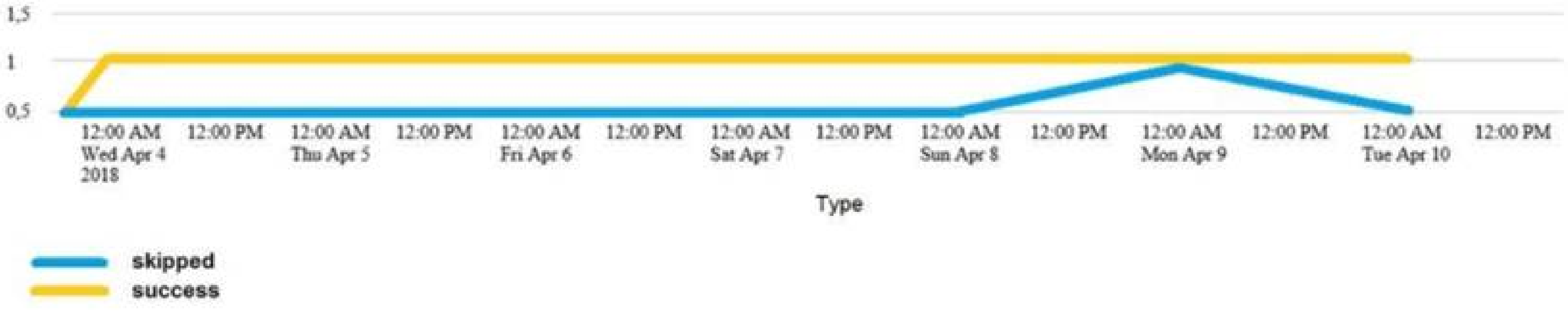
NEW QUESTION 282
- (Exam Topic 2)
_________ datasets can be added to root dataset to narrow down the search

A. parent
B. extracted
C. event
D. child

Answer: D

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

NEW QUESTION 287
- (Exam Topic 2)
Which of the following searches would create a graph similar to the one below?



A. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states
B. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time
C. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status
D. None of these searches would generate a similart graph.

Answer: C

Explanation:
The following search would create a graph similar to the one below:
index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status
The search does the following:

- It uses index_internal to specify the internal index that contains Splunk logs and metrics.
- It uses sourcetype=Savesplunker to filter events by the sourcetype that indicates the Splunk Enterprise Security app.
- It uses fields sourcetype, status to keep only the sourcetype and status fields in the events.
- It uses transaction status maxspan=1d to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction.
- It uses timechart count by status to create a time-based chart that shows the count of transactions for each status value over time.

The graph shows the following:

- It is a line graph with two lines, one yellow and one blue.
- The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018.
- The y-axis is labeled with numbers from 0 to 15.
- The yellow line represents “shipped” and the blue line represents “success”.
- The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.
- The graph is titled “Type”. Therefore, option C is the correct answer.

NEW QUESTION 288
- (Exam Topic 2)
Which of the following is true about the Splunk Common Information Model (CIM)?

A. The data models included in the CIM are configured with data model acceleration turned off.
B. The CIM contains 28 pre-configured datasets.
C. The CIM is an app that needs to run on the indexer.
D. The data models included in the CIM are configured with data model acceleration turned on.

Answer: D

Explanation:
The Splunk Common Information Model (CIM) is an app that contains a set of predefined data models that apply a common structure and naming convention to data from any source. The CIM enables you to use data from different sources in a consistent and coherent way. The CIM contains 28 pre-configured datasets that cover various domains such as authentication, network traffic, web, email, etc. The data models included in the CIM are configured with data model acceleration turned on by default, which means that they are optimized for faster searches and analysis. Data model acceleration creates and maintains summary data for the data models, which reduces the amount of raw data that needs to be scanned when you run a search using a data model.
Splunk Core Certified Power User Track, page 10. : Splunk Documentation, About the Splunk Common Information Model.

NEW QUESTION 292
- (Exam Topic 2)
Which of the following expressions could be used to create a calculated field called gigabytes?

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

Answer: B

NEW QUESTION 293
- (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 295
- (Exam Topic 2)
What is the correct way to name a macro with two arguments?

A. us_sales2

B. us_sales(1,2)
C. us_sale,2
D. us_sales(2)

Answer: D

NEW QUESTION 296
- (Exam Topic 2)
During the validation step of the Field Extractor workflow: Select your answer.

A. You can remove values that aren't a match for the field you want to define
B. You can validate where the data originated from
C. You cannot modify the field extraction

Answer: A

Explanation:
During the validation step of the Field Extractor workflow, you can remove values that aren’t a match for the field you want to define2. The validation step allows you to review and edit the values that have been extracted by the FX and make sure they are correct and consistent2. You can remove values that aren’t a match by clicking on them and selecting Remove Value from the menu2. This will exclude them from your
field extraction and update the regular expression accordingly2. Therefore, option A is correct, while options B and C are incorrect because they are not actions that you can perform during the validation step of the Field Extractor workflow.

NEW QUESTION 298
- (Exam Topic 2)
If there are fields in the data with values that are " " or empty but not null, which of the following would add a value?

A. | eval notNULL = if(isnull (notNULL), “0” notNULL)
B. | eval notNULL = if(isnull (notNULL), “0”
C. | eval notNULL = “” | nullfill value=0 notNULL
D. | eval notNULL = “” fillnull value=0 notNULL

Answer: D

Explanation:
The correct answer is D. | eval notNULL = “” fillnull value=0 notNULL

- Option A is incorrect because it is missing a comma between the “0” and the notNULL in the if function. The correct syntax for the if function is if (condition, true_value, false_value).
- Option B is incorrect because it is missing the false_value argument in the if function. The correct syntax for the if function is if (condition, true_value, false_value).
- Option C is incorrect because it uses the nullfill command, which only replaces null values, not empty strings. The nullfill command is equivalent to fillnull value=null.
- Option D is correct because it uses the eval command to assign an empty string to the notNULL field, and then uses the fillnull command to replace the empty string with a zero. The fillnull command can replace any value with a specified replacement, not just null values.

NEW QUESTION 300
- (Exam Topic 2)
Where are the results of eval commands stored?

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

Answer: A

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

- If the field name that you specify does not match a field in the output, a new field is added to the search results.
- If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION 301
- (Exam Topic 2)
Which of the following describes the I transaction command?

A. It is an SPL command that groups at least two events together based on shared values in selected fields.
B. It allows an exchange of data from one Splunk index to another Splunk index.
C. It is an SPL command that groups events together with shared values in selected fields.
D. It allows an exchange of data from one Splunk system to another Splunk system.

Answer: C

Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints .

- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member .
- The transaction command groups events together by matching one or more fields that have the same value across the events . For example, | transaction clientip will group events that have the same value the clientip field.

NEW QUESTION 303
- (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 308
......