Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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

NEW QUESTION 1
- (Exam Topic 1)
Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

A. | datamodel web search | filed web *
B. | Search datamodel web web | filed web*
C. | datamodel web web field | search web*
D. Datamodel=web | search web | filed web*

Answer: A

Explanation:
The data model command allows you to run searches on data models that have been accelerated1. The synta for using the data model command is | datamodel <model_name> <dataset_name> [search <search_string>]1.
Therefore, option A is the correct way to use the data model command to search fields in the data model within the web dataset. Options B and C are incorrect because they do not follow the syntax for the data model command. Option D is incorrect because it does not use the data model command at all.

NEW QUESTION 2
- (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 3
- (Exam Topic 1)
Which of the following actions can the eval command perform?

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

Answer: B

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

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

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

Answer: C

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

NEW QUESTION 5
- (Exam Topic 1)
Which of the following statements 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 6
- (Exam Topic 1)
Which of the following searches will return events contains a tag name Privileged?

A. Tag= Priv
B. Tag= Pri*
C. Tag= Priv*
D. Tag= Privileged

Answer: B

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

NEW QUESTION 7
- (Exam Topic 1)
Which of the following searches show a valid use of macro? (Select all that apply)

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

Answer: AC

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

NEW QUESTION 8
- (Exam Topic 1)
Which of the following statements is true, especially in large environments?

A. Use the scats command when you next to group events by two or more fields.
B. The stats command is faster and more efficient than the transaction command
C. The transaction command is faster and more efficient than the stats command.
D. Use the transaction command when you want to see the results of a calculation.

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html
The stats command is faster and more efficient than the transaction command, especially in large environments. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command can group events by one or more fields or by time buckets. The stats command does not create new events from groups of events, but rather creates new fields with statistical values. The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command creates new events from groups of events that share one or more fields. The transaction command also creates some additional fields for each transaction, such as duration, eventcount, startime, etc. The transaction command is slower and more resource-intensive than the stats command because it has to process more data and create more events and fields.

NEW QUESTION 9
- (Exam Topic 1)
What is required for a macro to accept three arguments?

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

Answer: A

Explanation:

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

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
What do events in a transaction have In common?

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

Answer: D

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

NEW QUESTION 15
- (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 20
- (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 21
- (Exam Topic 1)
Which of the following can be used with the eval command tostring function (select all that apply)

A. ''hex''
B. ''commas''
C. ''Decimal''
D. ''duration''

Answer: ABD

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY The tostring function in the eval command converts a numeric value to a string value. It can take an optional second argument that specifies the format of the string value. Some of the possible formats are:

- hex: converts the numeric value to a hexadecimal string.
- commas: adds commas to separate thousands in the numeric value.
- duration: converts the numeric value to a human-readable duration string, such as "2h 3m 4s". Therefore, the formats A, B, and D can be used with the tostring function.

NEW QUESTION 24
- (Exam Topic 1)
Which of the following statements describes POST workflow actions?

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

Answer: D

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

NEW QUESTION 29
- (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 30
- (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 31
- (Exam Topic 1)
Which of the following statements describes the command below (select all that apply) Sourcetype=access_combined | transaction JSESSIONID

A. An additional filed named maxspan is created.
B. An additional field named duration is created.
C. An additional field named eventcount is created.
D. Events with the same JSESSIONID will be grouped together into a single event.

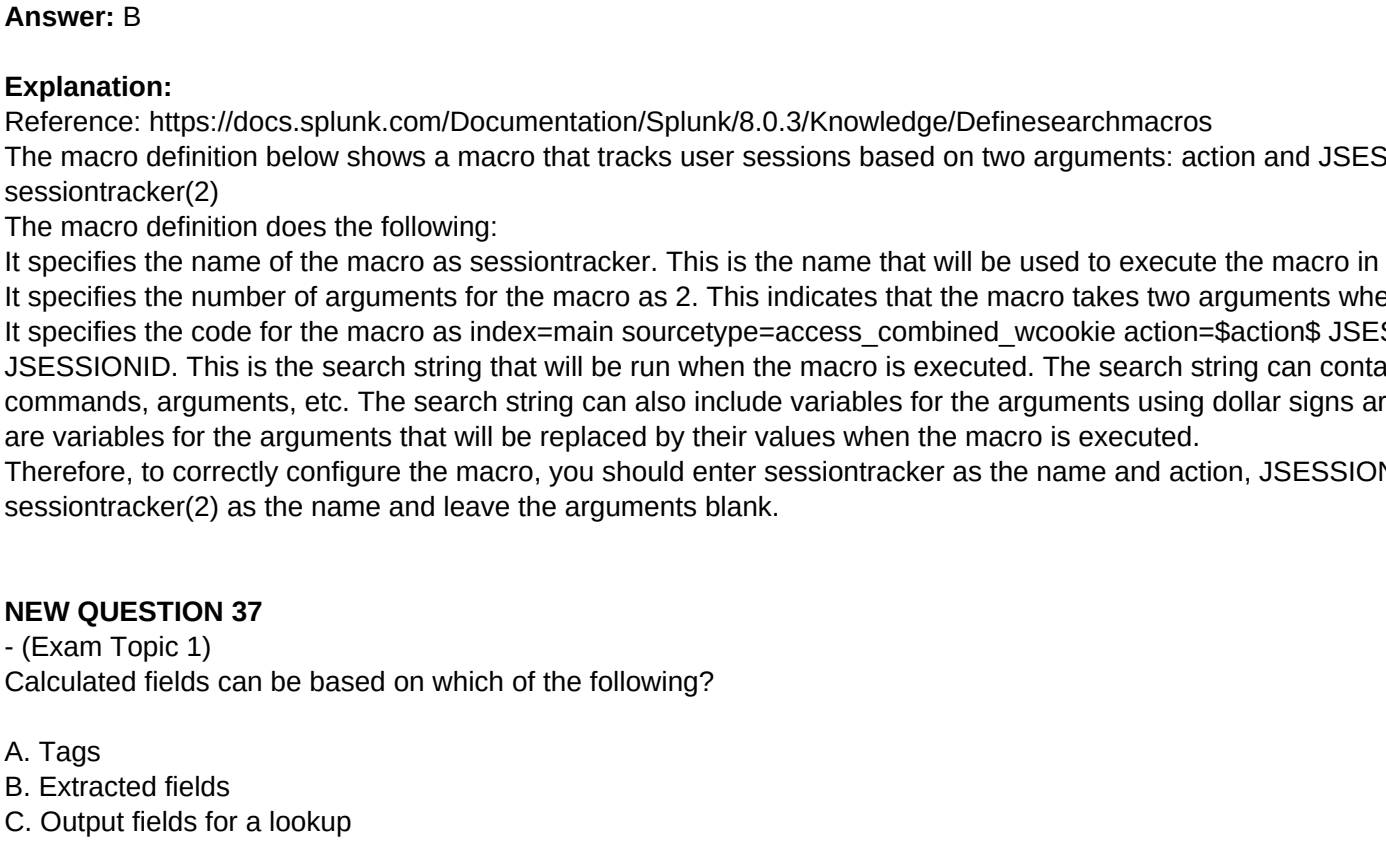
Answer: BCD

Explanation:
The command sourcetype=access_combined | transaction JSESSIONID does three things:

- It filters the events by the sourcetype access_combined, which is a predefined sourcetype for Apache web server logs.
- It groups the events by the field JSESSIONID, which is a unique identifier for each user session.
- It creates a single event from each group of events that share the same JSESSIONID value. This single event will have some additional fields created by the transaction command, such as duration, eventcount, and startime.

Therefore, the statements B, C, and D are true.

NEW QUESTION 33
- (Exam Topic 1)
Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



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

Answer: 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 37
- (Exam Topic 1)
Calculated fields can be based on which of the following?

A. Tags
B. Extracted fields
C. Output fields for a lookup
D. Fields generated from a search string

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields
A calculated field is a field that you create based on the value of another field or fields1. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format1. Calculated fields 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 pairs1. Therefore, option B is correct, while options A, C and D are incorrect because tags, output fields for a lookup, and fields generated from a search string are not types of extracted fields.

NEW QUESTION 38
- (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 40
- (Exam Topic 1)
A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

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

Answer: B

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

NEW QUESTION 45
- (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 47
- (Exam Topic 1)
What does the transaction command do?

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

Answer: B

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

NEW QUESTION 48
- (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 52
- (Exam Topic 1)
When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

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

Answer: D

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

NEW QUESTION 54
- (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 59
- (Exam Topic 1)
Which of the following describes the Splunk Common Information Model (CIM) add-on?

A. The CIM add-on uses machine learning to normalize data.
B. The CIM add-on contains dashboards that show how to map data.
C. The CIM add-on contains data models to help you normalize data.
D. The CIM add-on is automatically installed in a Splunk environment.

Answer: C

Explanation:
The Splunk Common Information Model (CIM) add-on is a Splunk app that contains data models to help you normalize data from different sources and formats.

The CIM add-on defines a common and consistent way of naming and categorizing fields and events in Splunk. This makes it easier to correlate and analyze data across different domains, such as network, security, web, etc. The CIM add-on does not use machine learning to normalize data, but rather relies on predefined field names and values. The CIM add-on does not contain dashboards that show how to map data, but rather provides documentation and examples on how to use the data models. The CIM add-on is not automatically installed in a Splunk environment, but rather needs to be downloaded and installed from Splunkbase.

NEW QUESTION 63
- (Exam Topic 1)
Which of the following file formats can be extracted using a delimiter field extraction?

A. CSV
B. PDF
C. XML
D. JSON

Answer: A

Explanation:
A delimiter field extraction is a method of extracting fields from data that uses a character or a string to separate fields in each event. A delimiter field extraction can be performed by using the Field Extractor (FX) tool or by editing the props.conf file. A delimiter field extraction can be applied to any file format that uses a delimiter to separate fields, such as CSV, TSV, PSV, etc. A CSV file is a comma-separated values file that uses commas as delimiters. Therefore, a CSV file can be extracted using a delimiter field extraction.

NEW QUESTION 65
- (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 66
- (Exam Topic 1)
When creating a Search workflow action, which field is required?

A. Search string
B. Data model name
C. Permission setting
D. An eval statement

Answer: A

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

NEW QUESTION 69
- (Exam Topic 1)
Which of the following statements describe the search string below?
| datamodel Application_State All_Application_State search

A. Evenrches would return a report of sales by state.
B. Events will be returned from the data model named Application_State.
C. Events will be returned from the data model named All_Application_state.
D. No events will be returned because the pipe should occur after the datamodel command

Answer: B

Explanation:
The search string below returns events from the data model named Application_State.
| datamodel Application_State All_Application_State search The search string does the following:
> It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.

- It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications.
- It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from all child datasets.
- It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.

NEW QUESTION 70
- (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)
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 75
- (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 80
- (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 83
- (Exam Topic 2)
The eval command 'if' function requires the following three arguments (in order):

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

Answer: A

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

NEW QUESTION 87
- (Exam Topic 2)
Field aliases are used to _____ data

A. clean
B. transform
C. calculate
D. normalize

Answer: D

NEW QUESTION 91
- (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 93
- (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 96
- (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 99
- (Exam Topic 2)
A calculated field is a shortcut for performing repetitive, long, or complex transformations using which of the following commands?

A. transaction
B. lookup
C. stats
D. eval

Answer: D

Explanation:
The correct answer is D. eval.
A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1.
A calculated field is a shortcut for performing repetitive, long, or complex transformations using the eval command. The eval command is used to create or modify fields by using expressions. The eval command can perform mathematical, string, date and time, comparison, logical, and other operations on fields or values2.
For example, if you want to create a new field named total that is the sum of two fields named price and tax, you can use the eval command as follows:
| eval total=price+tax
However, if you want to use this new field in multiple searches, reports, or dashboards, you can create a calculated field instead of writing the eval command every time. To create a calculated field with Splunk Web, you need to go to Settings > Fields > Calculated Fields and enter the name of the new field (total), the name of the sourcetype (sales), and the eval expression (price+tax). This will create a calculated field named total that will be added to all events with the sourcetype sales at search time. You can then use the total field like any other extracted field without writing the eval expression1.
The other options are not correct because they are not related to calculated fields. These options are:

- A. transaction: This command is used to group events that share some common values into a single record, called a transaction. A transaction can span multiple events and multiple sources, and can be useful for correlating events that are related but not contiguous3.
- B. lookup: This command is used to enrich events with additional fields from an external source, such as a CSV file or a database. A lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field.
- C. stats: This command is used to calculate summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields.

References:

- About calculated fields
- eval command overview
- transaction command overview
- [lookup command overview]
- [stats command overview]

NEW QUESTION 102
- (Exam Topic 2)
In most large Splunk environments, what is the most efficient command that can be used to group events by fields/

A. join
B. stats
C. streamstats
D. transaction

Answer: B

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Abouttransactions
In other cases, it's usually better to use the stats command, which performs more efficiently, especially in a distributed environment. Often there is a unique ID in the events and stats can be used.

NEW QUESTION 106
- (Exam Topic 2)
The transaction command allows you to _____ events across multiple sources

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

Answer: B

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

NEW QUESTION 109
- (Exam Topic 2)
When can a pipe follow a macro?

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

Answer: A

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

NEW QUESTION 112
- (Exam Topic 2)
Data models are composed of one or more of which of the following datasets? (select all that apply)

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

Answer: ABC

Explanation:
Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.
https://docs.splunk.com/Splexicon:Datamodeldataset

NEW QUESTION 117
- (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 118
- (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)
When using the transaction command, what does the argument maxspan do?

A. Sets the maximum total time between events in a transaction.
B. Sets the maximum length of all events within a transaction.
C. Sets the maximum total time between the earliest and latest events in a transaction.
D. Sets the maximum length that any single event can reach to be included in the transaction.

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction

NEW QUESTION 124
- (Exam Topic 2)
What other syntax will produce exactly the same results as | chart count over vendor_action by user?

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

Answer: A

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

NEW QUESTION 128
- (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 129
- (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 131
- (Exam Topic 2)
Which of the following statements describes calculated fields?

A. Calculated fields are only used on fields added by lookups.
B. Calculated fields are a shortcut for repetitive and complex eval commands.
C. Calculated fields are a shortcut for repetitive and complex calc commands.
D. Calculated fields automatically calculate the simple moving average for indexed fields.

Answer: B

NEW QUESTION 133
- (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 134
- (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 of the following statements describes the use of the Filed Extractor (FX)?

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

Answer: C

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

NEW QUESTION 140
- (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 145
- (Exam Topic 2)
When a search returns _____, you can view the results as a list.

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

Answer: C

NEW QUESTION 148
- (Exam Topic 2)
A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being _____.

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

Answer: A

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

NEW QUESTION 149
- (Exam Topic 2)
Select this in the fields sidebar to automatically pipe you search results to the rare command

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

Answer: B

Explanation:
The fields sidebar is a panel that shows the fields that are present in your search results2. The fields sidebar has two sections: selected fields and interesting fields2. Selected fields are fields that you choose to display in your search results by clicking on them in the fields sidebar or by using the fields command2. Interesting field are fields that appear in at least 20 percent of events or have high variability among values2. For each field in the fields sidebar, you can select one of the following options: events with this field, rare values, top values by time or top values2. If you select rare values, Splunk will automatically pipe your search results to the rare command, which shows the least common values of a field2. Therefore, option B is correct, while options A, C and D are incorrect because they do not pipe your search results to the rare command.

NEW QUESTION 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 152
- (Exam Topic 2)
When should transaction be used?

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

Answer: C

NEW QUESTION 153
- (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 157
- (Exam Topic 2)
Which of the following searches show a valid use of a macro? (Choose all that apply.)

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

Answer: AC

Explanation:
The searches A and C show a valid use of a macro. A macro is a reusable piece of SPL code that can be called by using single quotes (''). A macro can take arguments, which are passed inside parentheses after the macro name. For example, 'makeMyField(oldField)' calls a macro named makeMyField with an argument oldField. The searches B and D are not valid because they use double quotes ("") instead of single quotes ('').

NEW QUESTION 158
- (Exam Topic 2)
Which of the following objects can a calculated field use as a source?

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

Answer: B

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

NEW QUESTION 160
- (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 164
- (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 168
- (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 170
- (Exam Topic 2)
How is an event type created from the search window? (select all that apply)

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

Answer: AC

Explanation:
In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type1. This opens the Save as Event Type dial you can provide the event type name and optionally apply tags to it1.

You can also create an event type by editing the eventtypes.conf file and adding a new stanza1. Each stanz the eventtypes.conf file represents an event type1. The stanza name is the name of the event type, and
the search attribute specifies the search string that defines the event type1.
It's important to note that while you can use the eventtype command in a search to find events associated wit a specific event type, adding | eventtype to the SPL and executing the search does not create a new event type1. Similarly, clicking Event Actions > Build Event Type in an event's detail dropdown does not create new event type1.

NEW QUESTION 171
- (Exam Topic 2)
These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Answer: BC

NEW QUESTION 172
- (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 175
- (Exam Topic 2)
This is what Splunk uses to categorize the data that is being indexed.

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

Answer: B

NEW QUESTION 176
- (Exam Topic 2)
When defining a macro, what are the required elements?

A. Name and arguments.
B. Name and a validation error message.
C. Name and definition.
D. Definition and arguments.

Answer: C

Explanation:
When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced. The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation2
1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Define search macros in Settings.

NEW QUESTION 178
- (Exam Topic 2)
Which search would limit an "alert" tag to the "host" field?

A. tag=alert
B. host::tag::alert
C. tag==alert
D. tag::host=alert

Answer: D

Explanation:

The search below would limit an “alert” tag to the “host” field. tag::host=alert
The search does the following:

- It uses tag syntax to filter events by tags. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data.
- It specifies tag::host=alert as the tag filter. This means that it will only return events that have an “alert” tag applied to their host field or host field value.
- It uses an equal sign (=) to indicate an exact match between the tag and the field or field value.

NEW QUESTION 181
- (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 184
- (Exam Topic 2)
The gauge command:

A. creates a single-value visualization
B. allows you to set colored ranges for a single-value visualization
C. creates a radial gauge visualization

Answer: B

NEW QUESTION 188
- (Exam Topic 2)
The fields sidebar does not show _____. (Select all that apply.)

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

Answer: C

Explanation:
The fields sidebar is a panel that shows the fields that are present in your search results2. The fields sidebar does not show all extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs2. The fields sidebar only shows selected fields and interesting fields2. Selected fields are fields that you choose to display in your search results by clicking on them in the fields sidebar or by using the fields command2. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. Therefore, option C is correct, while options A and B are incorrect because they are types of fields that the fields sidebar does show.

NEW QUESTION 192
- (Exam Topic 2)
When extracting fields, we may choose to use our own regular expressions

A. True
B. False

Answer: A

NEW QUESTION 197
- (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 198
- (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 202
- (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 203
- (Exam Topic 2)
Which statement is true?

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

Answer: C

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

NEW QUESTION 207
- (Exam Topic 2)
A user wants to create a new field alias for a field that appears in two sourcetypes. How many field aliases need to be created?

A. One.
B. Two.
C. It depends on whether the original fields have the same name.
D. It depends on whether the two sourcetypes are associated with the same index.

Answer: B

NEW QUESTION 208
- (Exam Topic 2)
Which of the following transforming commands can be used with transactions?

A. chart, timechart, stats, eventstats
B. chart, timechart, stats, diff
C. chart, timeehart, datamodel, pivot
D. chart, timecha:t, stats, pivot

Answer: A

Explanation:
The correct answer is A. chart, timechart, stats, eventstats.
Transforming commands are commands that change the format of the search results into a table or a chart. They can be used to perform statistical calculations, create visualizations, or manipulate data in various ways1.
Transactions are groups of events that share some common values and are related in some way. Transactions can be defined by using the transaction command or by creating a transaction type in the transactiontypes.conf file2.
Some transforming commands can be used with transactions to create tables or charts based on the transaction fields. These commands include:

- chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics3.
- timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers4.
- stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields5.
- eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.

These commands can be applied to transactions by using the transaction fields as arguments. For example, if you have a transaction type named “login” that groups events based on the user field and has fields such as duration and eventcount, you can use the following commands with transactions:

- | chart count by user : This command creates a table or a chart that shows how many transactions each user has.
- | timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.
- | stats sum(eventcount) as total_events by user : This command creates a table that shows the total number of events for each user across all transactions.
- | eventstats avg(duration) as avg_duration : This command adds a new field named avg_duration to each transaction that shows the average duration of all transactions.

The other options are not valid because they include commands that are not transforming commands or cannot be used with transactions. These commands are:

- diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.
- datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.

- pivot: This command creates a pivot report, which is a way to analyze data from a data model using a graphical interface. It is not a transforming command and it does not work with transactions.

References:

- About transforming commands
- About transactions
- chart command overview
- timechart command overview
- stats command overview
- [eventstats command overview]
- [diff command overview]
- [datamodel command overview]
- [pivot command overview]

NEW QUESTION 211
- (Exam Topic 2)
The eval command allows you to do which of the following? (Choose all that apply.)

A. Format values
B. Convert values
C. Perform calculations
D. Use conditional statements

Answer: ABCD

NEW QUESTION 213
- (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 214
- (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 217
- (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 218
- (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 222
- (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 223
- (Exam Topic 2)
A macro has another macro nested within it, and this inner macro requires an argument. How can the user pass this argument into the SPL?

A. An argument can be passed through the outer macro.
B. An argument can be passed to the outer macro by nesting parentheses.
C. There is no way to pass an argument to the inner macro.
D. An argument can be passed to the inner macro by nesting parentheses.

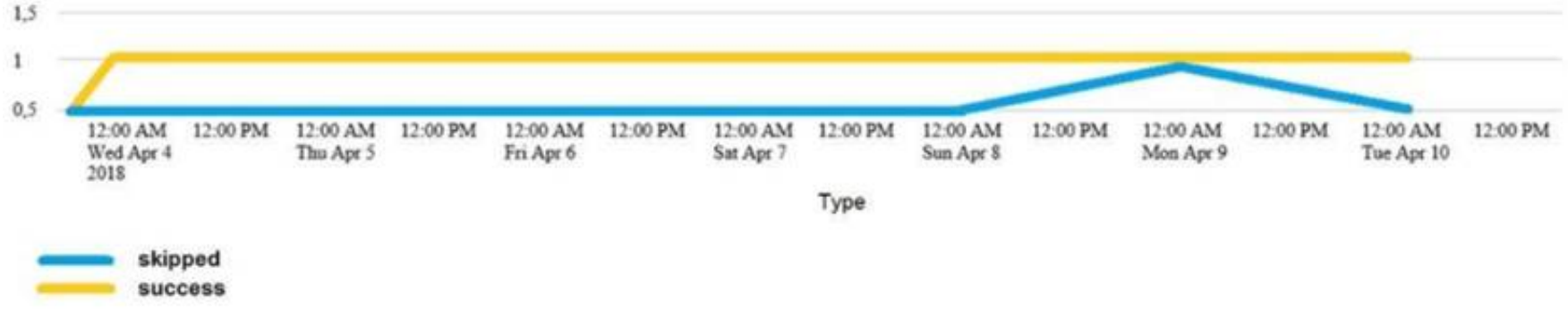
Answer: D

Explanation:
The correct answer is D. An argument can be passed to the inner macro by nesting parentheses.
A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain another search macro within it, which is called a nested macro. A nested macro can also take arguments, which can be passed from the outer macro or directly from the search string.

To pass an argument to the inner macro, you need to use parentheses to enclose the argument value and separate it from the outer macro argument. For example, if you have a search macro named outer_macro (1) that contains another search macro named inner_macro (2), and both macros take one argument each, you can pass an argument to the inner macro by using the following syntax:
outer_macro (argument1, inner_macro (argument2))
This will replace the argument1 and argument2 with the values you provide in the search string. For example, if you want to pass “foo” as the argument1 and “bar” as the argument2, you can write:
outer_macro ("foo", inner_macro ("bar"))
This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:

- Search macro examples
- Use search macros in searches

NEW QUESTION 228
- (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 233
- (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 235
- (Exam Topic 2)
Which of the following searches will return all clientip addresses that start with 108?

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

Answer: A

NEW QUESTION 237
- (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 239
- (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 243
- (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 245
- (Exam Topic 2)
which of the following are valid options with the chart command

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

Answer: AB

NEW QUESTION 247
- (Exam Topic 2)
Which of the following statements would help a user choose between the transaction and stats commands?

A. state can only group events using IP addresses.

B. The transaction command is faster and more efficient.
C. There is a 1000 event limitation with the transaction command.
D. Use state when the events need to be viewed as a single event.

Answer: C

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

NEW QUESTION 251
- (Exam Topic 2)
Splunk alerts can be based on search that run _____. (Select all that apply.)

A. in real-time
B. on a regular schedule
C. and have no matching events

Answer: AB

Explanation:
Splunk alerts can be based on searches that run in real-time or on a regular schedule3. An alert is a way to monitor your data and get notified when certain conditions are met3. You can create an alert by specifying a search and a triggering condition3. You can also specify how often you want to run the search and how you want to receive the alert notifications3. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk3. Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day3. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

NEW QUESTION 255
- (Exam Topic 2)
Which of the following options will define the first event in a transaction?

A. startswith
B. with
C. startingwith
D. firstevent

Answer: A

Explanation:
The correct answer is A. startswith. The Explanation: is as follows:
- The transaction command is used to find transactions based on events that meet various constraints12.
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member1.
- The startswith option is used to define the first event in a transaction by specifying a search term or an expression that matches the event13.
- For example, | transaction clientip JSESSIONID startswith="view" will create transactions based on the clientip and JSESSIONID fields, and the first event in each transaction will contain the term “view” in the _raw field2.

NEW QUESTION 256
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SPLK-1002 Practice Exam Features:

* SPLK-1002 Questions and Answers Updated Frequently

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

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

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