Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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)
Which of the following searches show a valid use of macro? (Select all that apply)

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

Answer: AC

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

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

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

Answer: A

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

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

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

Answer: D

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

NEW QUESTION 5
- (Exam Topic 1)
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 6
- (Exam Topic 1)
When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

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

Answer: ABD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep https://community.splunk.com/t5/Splunk-Search/Field-Extraction-Separate-on-Colon/m-p/29751
The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. Some of the delimiters that will work with FX are:
Tabs: horizontal spaces that align text in columns.
Pipes: vertical bars that often indicate logical OR operations. Spaces: blank characters that separate words or symbols. Therefore, the delimiters A, B, and D will work with FX.

NEW QUESTION 7
- (Exam Topic 1)
Which of the following are required to create a POST workflow action?

A. Label, URI, search string.
B. XMI attributes, URI, name.
C. Label, URI, post arguments.
D. URI, search string, time range picker.

Answer: C

Explanation:
POST workflow actions are custom actions that send a POST request to a web server when you click on a field value in your search results. POST workflow actions can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. One of the options that are required to create a POST workflow action is post arguments. Post arguments are key-value pairs that are sent in the body of the POST request to provide additional information to the web server. Post arguments can include field values from your data by using dollar signs around the field names.

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
Selected fields are displayed _____ each event in the search results.

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

Answer: A

Explanation:
Selected fields are fields that you choose to display in your search results by clicking on them in the Fields sidebar or by using the fields command2. Selected fields are displayed below each event in the search results, along with their values2. Therefore, option A is correct, while options B, C and D are incorrect because they are not places where selected fields are displayed.

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

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

Answer: B

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

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

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

Answer: ABD

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

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

duration field shows the time span between the first and last events in a transaction.

NEW QUESTION 13
- (Exam Topic 1)
What is the correct syntax to search for a tag associated with a value on a specific fields?

A. Tag-<field?
B. Tag<filed(tagname.)
C. Tag=<filed>::<tagname>
D. Tag::<filed>=<tagname>

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/TagandaliasfieldvaluesinSplunkWeb
A tag is a descriptive label that you can apply to one or more fields or field values in your events2. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags2. To search for a tag associated with a value on a specific field, you can use the following syntax: tag::<field>=<tagname>2. For example, tag::status=error will search for events where the status fie
has a tag named error. Therefore, option D is correct, while options A, B and C are incorrect because they do not follow the correct syntax for searching tags.

NEW QUESTION 16
- (Exam Topic 1)
Which of the following eval command function is valid?

A. Int ()
B. Count ( )
C. Print ()
D. Tostring ()

Answer: D

Explanation:

The eval command supports a number of functions that you can use in your expressions to perform calculations, conversions, string manipulations and more2. One of the eval command functions is tostring(), which converts a numeric value to a string value2. Therefore, option D is correct, while options A, B and C are incorrect because they are not valid eval command functions.

NEW QUESTION 20
- (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 24
- (Exam Topic 1)
Which one of the following statements about the search command is true?

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

Answer: D

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

NEW QUESTION 29
- (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 33
- (Exam Topic 1)
Which of the following statements describe calculated fields? (select all that apply)

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

Answer: ABD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields
Calculated fields are fields that are created by performing calculations on existing fields using the eval command. Calculated fields can be used in the search bar to filter and transform events based on the calculated values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for performing calculations using the eval command, but

rather results of performing calculations using the eval command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype. Therefore, statements A, B, and D are true about calculated fields.

NEW QUESTION 37
- (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 42
- (Exam Topic 1)
A user wants to convert numeric field values to strings and also to sort on those values. Which command should be used first, the eval or the sort?

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

Answer: C

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

NEW QUESTION 47
- (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 48
- (Exam Topic 2)
Which of the following about reports is/are true?

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

Answer: D

Explanation:
A report is a way to save a search and its results in a format that you can reuse and share with others2. A report is also a type of knowledge object, which is an entity that you create to add knowledge to your data and make it easier to search and analyze2. Therefore, option A is correct. A report can be scheduled, which

means that you can configure it to run at regular intervals and send the results to yourself or others via email or other methods2. Therefore, option B is correct. A report can run a script, which means that you can specify a script file to execute when the report runs and use it to perform custom actions or integrations2. Therefore, option C is correct. Therefore, option D is correct because all of the above statements are true for reports.

NEW QUESTION 52
- (Exam Topic 2)
This function of the stats command allows you to return the middle-most value of field X.

A. Median(X)
B. Eval by X
C. Fields(X)
D. Values(X)

Answer: A

NEW QUESTION 56
- (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 57
- (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 60
- (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 65
- (Exam Topic 2)
Field aliases are used to _____ data

A. clean
B. transform

C. calculate
D. normalize

Answer: D

NEW QUESTION 67
- (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 69
- (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 73
- (Exam Topic 2)
Which command is used to create choropleth maps?

A. geostats
B. cluster
C. geom

Answer: C

NEW QUESTION 75
- (Exam Topic 2)
We can use the rename command to _____ (Select all that apply.)

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

Answer: D

NEW QUESTION 77
- (Exam Topic 2)
Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.
B. POST workflow actions can be configured to send email to the URI location.
C. By default, POST workflow action are shown in both the event and field menus.
D. POST workflow actions can be configured to send POST arguments to the URI location.

Answer: D

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

NEW QUESTION 81

- (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 82
- (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 83
- (Exam Topic 2)
When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

A. OR
B. ( )
C. AND
D. NOT

Answer: ABD

Explanation:
When you mouse over and click to add a search term from the Fields sidebar or from an event in your search results, Splunk automatically adds the term to your search string with an implied AND operator2. However, this does not apply to some Boolean operators such as OR, NOT and parentheses (). These operators are not implied when you add a search term and you have to type them manually if you want to use them in your search string2. Therefore, options A, B and D are correct, while option C is incorrect because AND is implied when you add a search term.

NEW QUESTION 84
- (Exam Topic 2)
What is the Splunk Common Information Model (CIM)?

A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.
B. The CIM provides a methodology to normalize data from different sources and source types.
C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.
D. The CIM is a data exchange initiative between software vendors.

Answer: B

Explanation:
The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

NEW QUESTION 89
- (Exam Topic 2)
Consider the the following search run over a time range of last 7 days: index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane
Which option is used to change the default time span so that results are grouped into 12 hour intervals?

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

Answer: A

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

NEW QUESTION 91
- (Exam Topic 2)
Which workflow action method can be used the action type is set to link?

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

Answer: A

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction
Define a GET workflow action
Steps
- Navigate to Settings > Fields > Workflow Actions.
- Click New to open up a new workflow action form.
- Define a Label for the action.

The Label field enables you to define the text that is displayed in either the field or event workflow menu.
Labels can be static or include the value of relevant fields.

- Determine whether the workflow action applies to specific fields or event types in your data.

Use Apply only to the following fields to identify one or more fields. When you identify fields, the workflow action only appears for events that have those fields, either in their event menu or field menus. If you leave it blank or enter an asterisk the action appears in menus for all fields.
Use Apply only to the following event types to identify one or more event types. If you identify an event type, the workflow action only appears in the event menus for events that belong to the event type.

- For Show action in determine whether you want the action to appear in the Event menu, the Fields menus, or Both.
- Set Action type to link.
- In URI provide a URI for the location of the external resource that you want to send your field values to.

Similar to the Label setting, when you declare the value of a field, you use the name of the field enclosed by dollar signs.
Variables passed in GET actions via URIs are automatically URL encoded during transmission. This means you can include values that have spaces between words or punctuation characters.

- Under Open link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.
- Set the Link method to get.
- Click Save

to save your workflow action definition.

NEW QUESTION 96
- (Exam Topic 2)
What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

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

Answer: A

NEW QUESTION 101
- (Exam Topic 2)
Which of the following eval commands will provide a new value for host from src if it exists?

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

Answer: D

Explanation:

- The eval command is a Splunk command that allows you to create or modify fields using expressions .
- The if function is an expression that evaluates a condition and returns a value based on whether the condition is true or false. The syntax of the if function is if(X,Y,Z), where X is the condition, Y is th value to return if X is true, and Z is the value to return if X is false.
- The isnotnull function is an expression that returns true if the argument is not null, and false otherwise The syntax of the isnotnull function is isnotnull(X), where X is the argument to check.

Therefore, the expression if (isnotnull (src), src, host) returns the value of src if it is not null, and th value of host otherwise. This means that it will provide a new value for host from src if it exist keep the original value of host otherwise.

NEW QUESTION 105
- (Exam Topic 2)
Which of these search strings is NOT valid:

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

Answer: A

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

NEW QUESTION 107
- (Exam Topic 2)
Which type of visualization shows relationships between discrete values in three dimensions?

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

Answer: C

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

NEW QUESTION 110
- (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 113
- (Exam Topic 2)
These allow you to categorize events based on search terms. Select your answer.

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

Answer: B

NEW QUESTION 118
- (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 121
- (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 123
- (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 125
- (Exam Topic 2)
Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

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

Answer: A

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

NEW QUESTION 128
- (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 132
- (Exam Topic 2)
How many ways are there to access the Field Extractor Utility?

A. 3
B. 4
C. 1
D. 5

Answer: A

NEW QUESTION 135
- (Exam Topic 2)

Which of the following statements about tags is true? (select all that apply.)

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

Answer: BD

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

- Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called “alert” for the field name “status” and the field value “critical”. This means that only events that have status=critical will have the “alert” tag applied to them.
- Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called “web” for the search string sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the “web” tag applied to them.

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

NEW QUESTION 139
- (Exam Topic 2)
Why are tags useful in Splunk?

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

Answer: C

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

NEW QUESTION 144
- (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 146
- (Exam Topic 2)
When using | timchart by host, which filed is representted in the x-axis?

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

Answer: A

NEW QUESTION 151
- (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 156
- (Exam Topic 2)
A data model consists of which three types of datasets?

A. Constraint, field, value.
B. Events, searches, transactions.
C. Field extraction, regex, delimited.
D. Transaction, session ID, metadata.

Answer: B

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

NEW QUESTION 160
- (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 162
- (Exam Topic 2)
If a calculated field has the same name as an extracted field, what happens to the extracted field?

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

Answer: A

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

NEW QUESTION 166
- (Exam Topic 2)
Which of the following are valid options to speed up reports? (Select all the apply.)

A. Edit permissions
B. Edit description
C. Edit acceleration
D. Edit schedule

Answer: C

Explanation:
One of the valid options to speed up reports is to edit acceleration, which means that you can enable summary indexing or data model acceleration for your reports to improve their performance2. Summary indexing allows you to create reports that run over large amounts of data by storing the results of scheduled searches in a summary index and using that index for faster reporting2. Data model acceleration allows you to create reports that use data models by creating and storing summaries of the data model datasets and using them for faster reporting2. Therefore, option C is correct, while options A, B and D are incorrect because they are not options to speed up reports.

NEW QUESTION 168
- (Exam Topic 2)
This is what Splunk uses to categorize the data that is being indexed.

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

Answer: A

NEW QUESTION 171
- (Exam Topic 2)
Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

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

Answer: D

NEW QUESTION 173
- (Exam Topic 2)
This function of the stats command allows you to return the sample standard deviation of a field.

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

Answer: A

NEW QUESTION 178
- (Exam Topic 2)
Consider the following search: index=web sourcetype=access_corabined
The log shows several events that share the same jsesszonid value (SD462K101O2F267). View the events as a group.
From the following list, which search groups events by jSSESSIONID?

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

Answer: A

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

NEW QUESTION 183
- (Exam Topic 2)
It is mandatory for the lookup file to have this for an automatic lookup to work.

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

Answer: D

NEW QUESTION 186
- (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 190
- (Exam Topic 2)
Which of the following statements about tags is true?

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

Answer: B

Explanation:

Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .

Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or value 404 as not_found .

NEW QUESTION 192
- (Exam Topic 2)
Which of the following is NOT a stats function:

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

Answer: B

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

NEW QUESTION 197
- (Exam Topic 2)
The timechart command buckets data in time intervals depending on:

A. the number of events returned
B. the selected time range
C. the type of visualization selected

Answer: B

Explanation:
The timechart command buckets data in time intervals depending on the selected time range2. The timechart command is similar to the chart command but it automatically groups events into time buckets based on the _time field2. The size of the time buckets depends on the time range that you select for your search. For example, if you select Last 24 hours as your time range, Splunk will use 30-minute buckets for your timechart. If you select Last 7 days as your time range, Splunk will use 4-hour buckets for your timechart2. Therefore, option B is correct, while options A and C are incorrect because they are not factors that affect the size of the time buckets.

NEW QUESTION 199
- (Exam Topic 2)
Which of the following is a function of the Splunk Common Information Model (CIM)?

A. Normalizing data across a Splunk deployment.
B. Providing templates for reports and dashboards.
C. Algorithmically shifting events to other indexes.
D. Reingesting previously indexed data with new field names.

Answer: A

NEW QUESTION 201
- (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 205
- (Exam Topic 2)
Which of the following is a feature of the Pivot tool?

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

Answer: C

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

NEW QUESTION 209
- (Exam Topic 2)
The stats command will create a _____ by default.

A. Table
B. Report
C. Pie chart

Answer: A

NEW QUESTION 211
- (Exam Topic 2)
Use the dedup command to _____.

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

Answer: B

NEW QUESTION 212
- (Exam Topic 2)
Which syntax will find events where the values for the 1 field match the values for the Renewal-MonthYear field?

A. | where 10yearAnnerversary=Renewal-MonthYear
B. | where ‘10yearAnnerversary=Renewal-MonthYear
C. | where 10yearAnnerversary=’Renewal-MonthYear’
D. | where ‘10yearAnnerversary’=’Renewal-MonthYear’

Answer: A

Explanation:
The correct answer is A. | where 10yearAnnerversary=Renewal-MonthYear.
The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions1.
The syntax for the where command is:
| where <expression>
The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.
To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the 10yearAnnerversary field match the values for the Renewal-MonthYear field, you can use the following syntax:
| where 10yearAnnerversary=Renewal-MonthYear
This will return only the events where the two fields have the same value.
The other options are not correct because they use quotation marks around the field names, which will cause the where command to interpret them as string values instead of field names. For example, if you use:
| where ‘10yearAnnerversary’=‘Renewal-MonthYear’
This will return no events because there are no events where the string value ‘10yearAnnerversary’ is equal to the string value ‘Renewal-MonthYear’.
References:
where command usage

NEW QUESTION 216
- (Exam Topic 2)

Which tool uses data models to generate reports and dashboard panels without using SPL?

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

Answer: B

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

NEW QUESTION 221
- (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 223
- (Exam Topic 2)
When used with the timechart command, which value of the limit argument returns all values?

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

Answer: D

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

NEW QUESTION 228
- (Exam Topic 2)
Which of the following searches will return events containing a tag named Privileged?

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

Answer: B

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

NEW QUESTION 229
- (Exam Topic 2)

Which workflow uses field values to perform a secondary search?

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

Answer: C

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

NEW QUESTION 232
- (Exam Topic 2)
_____ datasets can be added to root dataset to narrow down the search

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

Answer: D

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

NEW QUESTION 237
- (Exam Topic 2)
Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

A. maxpause
B. endswith
C. maxduration
D. maxspan

Answer: D

Explanation:
The maxspan function of the transaction command allows you to set the maximum total time between the earliest and latest events returned. The maxspan function is an argument that can be used with the transaction command to specify the start and end constraints for the transactions. The maxspan function takes a time modifier as its value, such as 30s, 5m, 1h, etc. The maxspan function sets the maximum time span between the first and last events in a transaction. If the time span between the first and last events exceeds the maxspan value, the transaction will be split into multiple transactions.

NEW QUESTION 238
- (Exam Topic 2)
Which of the following is true about the Splunk Common Information Model (CIM)?

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

Answer: D

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

NEW QUESTION 242
- (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 246
- (Exam Topic 2)
What is the correct way to name a macro with two arguments?

A. us_sales2
B. us_sales(1,2)
C. us_sale,2
D. us_sales(2)

Answer: D

NEW QUESTION 250
- (Exam Topic 2)
Where are the results of eval commands stored?

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

Answer: A

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval
The eval command calculates an expression and puts the resulting value into a search results field.
- If the field name that you specify does not match a field in the output, a new field is added to the search results.
- If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION 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 253
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SPLK-1002 Practice Exam Features:

* SPLK-1002 Questions and Answers Updated Frequently

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

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

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