

Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



NEW QUESTION 1

- (Exam Topic 1)

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

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

Answer: C

Explanation:

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

NEW QUESTION 2

- (Exam Topic 1)

What does the fillnull command replace null values with, if the value argument is not specified?

- A. N/A
- B. NaN
- C. NULL

Answer: A

Explanation:

Reference: <https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specifying-a-field.html> The fillnull command is a search command that replaces null values with a specified value or 0 if no value is specified. Null values are values that are missing, empty, or undefined in Splunk. The fillnull command can replace null values for all fields or for specific fields. The fillnull command can take an optional argument called value that specifies the value to replace null values with. If no value argument is specified, the fillnull command will replace null values with 0 by default.

NEW QUESTION 3

- (Exam Topic 1)

Which of the following searches will return events that contain 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 4

- (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 5

- (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, starttime, 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 6

- (Exam Topic 1)

Which of the following statements describes Search workflow actions?

- A. By default
- 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 7

- (Exam Topic 1)

Which of the following statements about data models and pivot are true? (select all that apply)

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Exam Topic 1)

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 9

- (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. Stack mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series². Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

NEW QUESTION 10

- (Exam Topic 1)

A calculated field may be based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

Answer: B

Explanation:

As mentioned before, a calculated field is a field that you create based on the value of another field or fields². A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

NEW QUESTION 10

- (Exam Topic 1)

When using timechart, how many fields can be listed after a by clause?

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

Answer: B

Explanation:

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

NEW QUESTION 12

- (Exam Topic 1)

Which of the following statements describe data model acceleration? (select all that apply)

- A. Root events cannot be accelerated.
- B. Accelerated data models cannot be edited.
- C. Private data models cannot be accelerated.
- D. You must have administrative permissions or the `accelerate_dacamodel` capability to accelerate a data model.

Answer: BCD

Explanation:

Data model acceleration is a feature that speeds up searches on data models by creating and storing summaries of the data model datasets¹. To enable data model acceleration, you must have administrative permissions or the `accelerate_datamodel` capability¹. Therefore, option D is correct. Accelerated data models cannot be edited unless you disable the acceleration first¹. Therefore, option B is correct. Private data models cannot be accelerated because they are not visible to other users¹. Therefore, option C is correct. Root events can be accelerated as long as they are not based on a search string¹. Therefore, option A is incorrect.

NEW QUESTION 17

- (Exam Topic 1)

In what order are the following knowledge objects/configurations applied?

- A. Field Aliases, Field Extractions, Lookups
- B. Field Extractions, Field Aliases, Lookups
- C. Field Extractions, Lookups, Field Aliases
- D. Lookups, Field Aliases, Field Extractions

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge> Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze². Some examples of knowledge objects are field extractions, field aliases and lookups². Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs². Field aliases are ways to assign alternative names to existing fields without changing the original field names or values². Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases². The order in which these knowledge objects/configurations are applied is as follows: field

extractions, field aliases and then lookups². This means that Splunk first extracts fields from your raw data, then applies any aliases to the extracted fields and then performs any lookups on the aliased fields². Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 19

- (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 24

- (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, starttime, 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 26

- (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 30

- (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 32

- (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 35

- (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 38

- (Exam Topic 2)

A field alias is created where field1—fieid2 and the Overwrite Field Values checkbox is selected. What happens if an event only contains values for fieid1?

- A. field2 values are removed from the events.
- B. field1 and field2 values are merged.
- C. field2 values are unchanged.
- D. field2 values are replaced with the value of the field1.

Answer: D

Explanation:

The correct answer is D. field2 values are replaced with the value of the field1.

A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience¹.

When you create a field alias in Splunk Web, you can select the Overwrite Field Values option to change the behavior of the field alias. This option affects how the Splunk software handles situations where the original field has no value or does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field².

If you select the Overwrite Field Values option, the following rules apply:

- If the original field does not exist or has no value in an event, the alias field is removed from that event.
- If the original field and the alias field both exist in an event, the value of the alias field is replaced with the value of the original field.

If you do not select the Overwrite Field Values option, the following rules apply:

- If the original field does not exist or has no value in an event, the alias field is unchanged in that event.
- If the original field and the alias field both exist in an event, both fields are retained with their respective values.

Therefore, if you create a field alias where field1—field2 and select the Overwrite Field Values option, and an event only contains values for field1, then the value of field2 will be replaced with the value of field1. References:

- [About calculated fields](#)
- [About field aliases](#)
- [Create field aliases in Splunk Web](#)

NEW QUESTION 39

- (Exam Topic 2)

What are the expected results for a search that contains the command | where A=B?

- A. Events that contain the string value where A=B.
- B. Events that contain the string value A=B.
- C. Events where values of field are equal to values of field B.
- D. Events where field A contains the string value B.

Answer: C

Explanation:

The correct answer is C. Events where values of field A are equal to values of field B.

The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions¹.

The syntax for the where command is:

| where <expression>

The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.

To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the field A match the values for the field

B, you can use the following syntax:

| where A=B

This will return only the events where the two fields have the same value.

The other options are not correct because they use different syntax or fields that are not related to the where command. These options are:

- A. Events that contain the string value where A=B: This option uses the string value where A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text “where A=B” in them.
- B. Events that contain the string value A=B: This option uses the string value A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text “A=B” in them.
- D. Events where field A contains the string value B: This option uses quotation marks around the value B, which is not valid syntax for comparing fields with the where command. Quotation marks are used to enclose phrases or exact matches in a search². This option will return events where the field A contains the string value “B”.

References:

- where command usage
- Search command cheatsheet

NEW QUESTION 44

- (Exam Topic 2)

Field aliases are used to _____ data

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

Answer: D

NEW QUESTION 48

- (Exam Topic 2)

Given the following eval statement:

...| eval field1 - if(isnotnull(field1),field1,0), field2 = if(isnull<field2>, "NO-VALUE", field2) Which of the following is the equivalent using fillnull?

- A. There is no equivalent expression using fillnull
- B. ... | fillnull values=(0,"NO-VALUE") fields=(field1,field2)
- C. ... | fillnull value=0 field1 | fillnull fields
- D. ... | fillnull field1 | fillnull 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 49

- (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 52

- (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 53

- (Exam Topic 2)

When using the timechart command, how can a user group the events into buckets based on time?

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

Answer: A

NEW QUESTION 55

- (Exam Topic 2)

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

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

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction> Information needed to create a GET workflow action includes the following: a name of the workflow action, a URI where the user will be directed at search time, and a label that will appear in the Event Action menu at search time. A GET workflow action is a type of workflow action that performs a GET request when you click on a field value in your search results. A GET workflow action can be configured with various options, such as:

A name of the workflow action: This is a unique identifier for the workflow action that is used internally by Splunk. The name should be descriptive and meaningful for the purpose of the workflow action.

A URI where the user will be directed at search time: This is the base URL of the external web service or application that will receive the GET request. The URI can include field value variables that will be replaced by the actual field values at search time. For example, if you have a field value variable ip, you can write it as [http://example.com/ip=\\$ip](http://example.com/ip=$ip) to send the IP address as a parameter to the external web service or application.

A label that will appear in the Event Action menu at search time: This is the display name of the workflow action that will be shown in the Event Action menu when you click on a field value in your search results. The label should be clear and concise for the user to understand what the workflow action does.

Therefore, options A, B, and C are correct.

NEW QUESTION 60

- (Exam Topic 2)

A user runs the following search:

index=X sourcetype=Y | chart count (domain) as count, sum (price) as sum by product, action usenull=f useother=f

Which of the following table headers match the order this command creates?

- A. The chart command does not allow for multiple statistical functions.
- B. Product, sum: addtocart, sum: remove, sum: purchase, count: addtocart, count: remove, count: purchase
- C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase
- D. Count: product, sum: product, count: action, sum: action

Answer: C

Explanation:

The correct answer is C. Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, sum: purchase1.

In Splunk, the chart command is used to create a table or a chart visualization from your data2. The chart command takes at least one function and one field, and optionally another field to group by2.

In the given search, the chart command is used with two functions (count and sum), two fields (domain and price), and two fields to group by (product and action). The usenull=f and useother=f options are used to exclude null values and other values from the chart2.

The chart command creates a table with headers that match the order of the fields and functions in the command1. The headers for the count function are prefixed with count:, and the headers for the sum function are prefixed with sum:1. The values of the product and action fields are used as the suffixes for the headers1.

Therefore, the table headers created by this command are Product, count: addtocart, count: remove, count: purchase, sum: addtocart, sum: remove, and sum: purchase1.

NEW QUESTION 63

- (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 64

- (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 65

- (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 67

- (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 68

- (Exam Topic 2)

Which statement is true?

- A. Pivot is used for creating datasets.
- B. Data model 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:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot>

Pivot is used for creating reports and dashboards. Pivot is a tool that allows you to create reports and dashboards from your data models without writing any SPL commands. Pivot can help you visualize and analyze your data using various options, such as filters, rows, columns, cells, charts, tables, maps, etc. Pivot can also help you accelerate your reports and dashboards by using summary data from your accelerated data models.

Pivot is not used for creating datasets or data models. Datasets are collections of events that represent your data in a structured and hierarchical way. Data models are predefined datasets for various domains, such as network traffic, web activity, authentication, etc. Datasets and data models can be created by using commands such as datamodel or pivot.

NEW QUESTION 70

- (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 73

- (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 75

- (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 78

- (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 83

- (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 87

- (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 89

- (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 91

- (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 96

- (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 98

- (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 99

- (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 100

- (Exam Topic 2)

Which of the following eval command functions is valid?

- A. int()
- B. count()
- C. print()
- D. tostring()

Answer: D

Explanation:

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions>

The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns “3.14”. The other functions are not valid eval command functions.

NEW QUESTION 103

- (Exam Topic 2)

Which of the following searches would return a report of sales by product-name?

- A. chart sales by product_name
- B. chart sum(price) as sales by product_name
- C. stats sum(price) as sales over product_name
- D. timechart list(sales), values(product_name)

Answer: B

Explanation:

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

NEW QUESTION 104

- (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 108

- (Exam Topic 2)

These kinds of charts represent a series in a single bar with multiple sections

- A. Multi-Series
- B. Split-Series
- C. Omit nulls
- D. Stacked

Answer: D

Explanation:

Stacked charts represent a series in a single bar with multiple sections. A chart is a graphical representation of data that shows trends, patterns, or comparisons. A chart can have different types, such as column, bar, line, area, pie, etc. A chart can also have different modes, such as split-series, multi-series, stacked, etc. A stacked chart is a type of chart that shows multiple series in a single bar or area with different sections for each series

NEW QUESTION 113

- (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 116

- (Exam Topic 2)

Which search string would only return results for an event type called success ful_purchases?

- A. tag=success ful_purchases
- B. Event Type:: successful purchases
- C. successful_purchases
- D. event type—success ful_purchases

Answer: C

Explanation:

This is because event types are added to events as a field named eventtype, and you can use this field as a search term to find events that match a specific event type. For example, eventtype=successful_purchases returns all events that have been categorized as successful purchases by the event type definition. The other options are incorrect because they either use a different field name (tag), a different syntax (Event Type:: or event type—), or have a typo (success ful_purchases). You can learn more about how to use event types in searches from the Splunk documentation1.

NEW QUESTION 118

- (Exam Topic 2)
How is a macro referenced in a search?

- A. By using the macroname command.
- B. By using the macro command.
- C. By enclosing the macro name in backtick characters (`).
- D. By enclosing the macro name in single-quote characters (').

Answer: C

Explanation:

The correct answer is C. By enclosing the macro name in backtick characters (`).

A macro is a way to reuse a piece of SPL code in different searches. A macro can take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro¹.

To reference a macro in a search, you need to enclose the macro name in backtick characters (`). For example, if you have a macro named my_macro` that takes one argument, you can reference it in a search by using the following syntax:

```
| my_macro(argument) | ...
```

This will replace the macro name and argument with the SPL code contained in the macro definition. For example, if the macro definition is:

```
[my_macro(argument)] search sourcetype=$argument$ And you reference it in a search with:
```

```
index=main | my_macro(web) | stats count by host
```

This will expand the macro and run the following SPL code: index=main | search sourcetype=web | stats count by host References:

➤ [Use search macros in searches](#)

NEW QUESTION 120

- (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 122

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

Answer: B

NEW QUESTION 124

- (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 125

- (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 128

- (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 133

- (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 10yearAnniversary=Renewal-MonthYear
- B. | where '10yearAnniversary=Renewal-MonthYear
- C. | where 10yearAnniversary='Renewal-MonthYear'
- D. | where '10yearAnniversary'='Renewal-MonthYear'

Answer: A

Explanation:

The correct answer is A. | where 10yearAnniversary=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 10yearAnniversary field match the values for the Renewal-MonthYear field, you can use the following syntax:

| where 10yearAnniversary=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 '10yearAnniversary'='Renewal-MonthYear'

This will return no events because there are no events where the string value '10yearAnniversary' is equal to the string value 'Renewal-MonthYear'.

References:

> where command usage

NEW QUESTION 135

- (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 137

- (Exam Topic 2)

Which of these is NOT a field that is automatically created with the transaction command?

- A. maxcount
- B. duration
- C. eventcount

Answer: A

NEW QUESTION 140

- (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 142

- (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"))

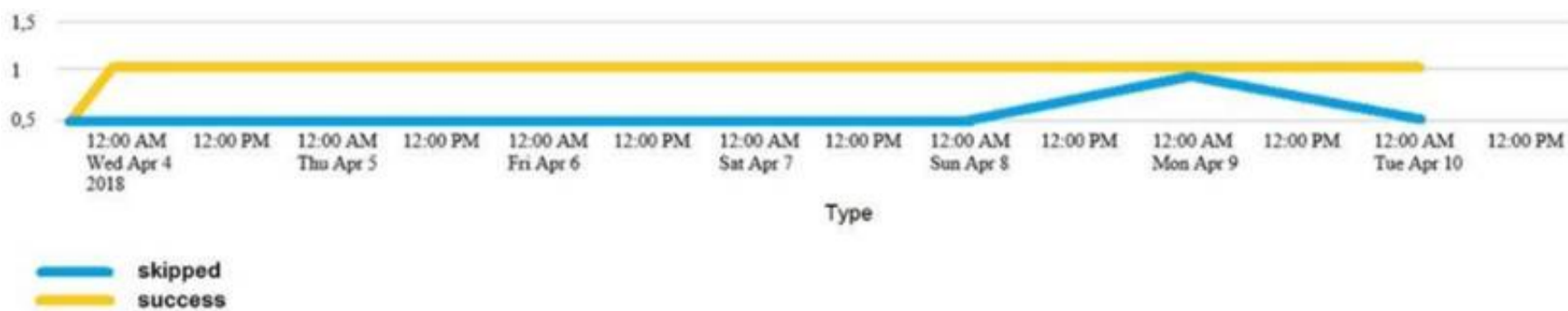
This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:

- Search macro examples
- Use search macros in searches

NEW QUESTION 144

- (Exam Topic 2)

Which of the following searches would create a graph similar to the one below?



- A. index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=id | start count states
- B. index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=id | chart count states by -time
- C. index_internal sourcetype=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 148

- (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 152

- (Exam Topic 2)

In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")

- A. The description field would contain no value.
- B. The description field would contain the value 0.
- C. The description field would contain the value "Internal Server Error".
- D. This statement would produce an error in Splunk because it is incomplete.

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions>

NEW QUESTION 157

- (Exam Topic 2)

Why would the following search produce multiple transactions instead of one?

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

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

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

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

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

Answer: A

Explanation:

The correct answer is A. The maxspan option is not included1.

In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1.

However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.

Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.

Here is an example of how you can use the maxspan option in a search:

```
index=main sourcetype=access_combined | transaction someuniquefield maxspan=1h
```

In this search, the transaction command groups events that share the same someuniquefield value into a single transaction, but only if the time span between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

NEW QUESTION 158

- (Exam Topic 2)

Which of the following describes the | 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 159

- (Exam Topic 2)

The time range specified for a historical search defines the _____.-----questionable on ans

- A. Amount of data shown on the timeline as data streams in
- B. Amount of data fetched from index matching that time range
- C. Time range for the static results

Answer: B

Explanation:

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

NEW QUESTION 163

- (Exam Topic 2)

Splunk alerts can be based on search that run _____. (Select all that apply.)

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

Answer: AB

Explanation:

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

NEW QUESTION 167

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SPLK-1002 Practice Exam Features:

- * SPLK-1002 Questions and Answers Updated Frequently
- * SPLK-1002 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1002 Practice Test Here](#)