

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

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



NEW QUESTION 1

- (Exam Topic 1)

In which of the following scenarios is an event type more effective than a saved search?

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

Answer: C

Explanation:

Reference: <https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html>

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

NEW QUESTION 2

- (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 3

- (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 4

- (Exam Topic 1)

Which of the following knowledge objects represents the output of an eval expression?

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

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Splexicon:Calculatedfield>

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

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

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

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview>

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

NEW QUESTION 9

- (Exam Topic 1)

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

- A. Tabs

- B. Pipes
- C. Spaces
- D. Commas

Answer: BCD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep>

The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings that separate fields in your data. The FX can detect some common delimiters automatically, such as pipes (|), spaces (), commas (,), semicolons (;), etc. The FX cannot detect tabs (\t) as delimiters automatically, but you can specify them manually in the FX interface.

NEW QUESTION 10

- (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 10

- (Exam Topic 1)

Which of the following file formats can be extracted using a delimiter field extraction?

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

Answer: A

Explanation:

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

NEW QUESTION 12

- (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 13

- (Exam Topic 2)

When using a field value variable with a Workflow Action, which punctuation mark will escape the data

- A. *
- B. !
- C. ^
- D. #

Answer: B

Explanation:

When using a field value variable with a Workflow Action, the exclamation mark (!) will escape the data. A Workflow Action is a custom action that performs a task when you click on a field value in your search results. A Workflow Action can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. A field value variable is a placeholder for the field value that will be used to replace the variable in the URL or post argument of the Workflow Action. A field value variable is written as fieldname, where field_name is the name of the field whose value will be used. However, if the field value contains special characters that need to be escaped, such as spaces, commas, etc., you can use the exclamation mark (!) before and after the field value variable to escape the data. For example, if you have a field value variable host, you can write it as !\$host! to escape any special characters in the host field value. Therefore, option B is the correct answer.

NEW QUESTION 15

- (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 19

- (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 22

- (Exam Topic 2)

Which command is used to create choropleth maps?

- A. geostats
- B. cluster
- C. geom

Answer: C

NEW QUESTION 26

- (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 27

- (Exam Topic 2)

When can a pipe follow a macro?

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

Answer: A

Explanation:

A macro is a way to save a segment of a search string as a variable and reuse it in other searches². A macro can be followed by a pipe, which is a symbol that

separates commands in a search pipeline². A pipe may always follow a macro, regardless of who owns the macro, where the macro is defined or how the macro is shared². For example, if you have a macro called `us_sales` that returns events from the US region, you can use it in a search like this: `us_sales | stats sum(price) by product`². This search will use the macro to filter the events and then calculate the total price for each product². Therefore, option A is correct, while options B, C and D are incorrect because they are not conditions that affect whether a pipe can follow a macro.

NEW QUESTION 32

- (Exam Topic 2)

This clause is used to group the output of a stats command by a specific name.

- A. Rex
- B. As
- C. List
- D. By

Answer: B

NEW QUESTION 35

- (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 37

- (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 38

- (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 42

- (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 43

- (Exam Topic 2)

In the Field Extractor, when would the regular expression method be used?

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

Answer: C

Explanation:

The correct answer is C. When events contain unstructured data.

The regular expression method works best with unstructured event data, such as log files or text messages, where the fields are not separated by a common delimiter, such as a comma or space¹. You select a sample event and highlight one or more fields to extract from that event, and the field extractor generates a regular expression that matches similar events in your dataset and extracts the fields from them¹. The regular expression method provides several tools for testing and refining the accuracy of the regular expression. It also allows you to manually edit the regular expression¹.

The delimiters method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space¹. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds¹. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats¹.

Reference:

1: Build field extractions with the field extractor - Splunk Documentation

NEW QUESTION 46

- (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 48

- (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 51

- (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 55

- (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 58

- (Exam Topic 2)

In which Settings section are macros defined?

- A. Fields
- B. Tokens
- C. Advanced Search
- D. Searches, Reports, Alerts

Answer: C

NEW QUESTION 61

- (Exam Topic 2)

When using | timchart by host, which field is represented in the x-axis?

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

Answer: A

NEW QUESTION 65

- (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 field.

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Configure calculated fields with props.conf.

NEW QUESTION 69

- (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 71

- (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 75

- (Exam Topic 2)

When is a GET workflow action needed?

- A. To send field values to an external resource.
- B. To retrieve information from an external resource.
- C. To use field values to perform a secondary search.
- D. To define how events flow from forwarders to indexes.

Answer:

B

NEW QUESTION 77

- (Exam Topic 2)

Tags can reference which of the following knowledge objects?

- A. Lookups and event types only.
- B. Extracted fields, field aliases, calculated fields, lookups, and event types.
- C. Tags cannot reference any of these knowledge objects because tags are the last knowledge objects generated in the search-time operation sequence.
- D. Extracted fields, calculated fields, and field aliases only.

Answer: B**Explanation:**

Tags are a type of knowledge object that enable you to assign descriptive keywords to events. Tags can reference any of the following knowledge objects: extracted fields, field aliases, calculated fields, lookups, and event types. Tags cannot reference other tags or search macros. Tags are applied to events at search time based on the values of the fields that they reference²

1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION 81

- (Exam Topic 2)

Which field will be used to populate the field if the productName and product:d fields have values for a given event?

```
| eval productINFO=coalesce(productName,productid)
```

- A. Both field values will be used and the product INFO field will become a multivalue field for the given event.
- B. The value for the productName field because it appears first.
- C. Neither field value will be used and the field will be assigned a NULL value for the given event.
- D. The value for the field because it appears second.

Answer: B**Explanation:**

The correct answer is B. The value for the productName field because it appears first.

The coalesce function is an eval function that takes an arbitrary number of arguments and returns the first value that is not null. A null value means that the field has no value at all, while an empty value means that the field has a value, but it is "" or zero-length¹.

The coalesce function can be used to combine fields that have different names but represent the same data, such as IP address or user name. The coalesce function can also be used to rename fields for clarity or convenience².

The syntax for the coalesce function is: `coalesce(<field1>,<field2>,...)`

The coalesce function will return the value of the first field that is not null in the argument list. If all fields are null, the coalesce function will return null.

For example, if you have a set of events where the IP address is extracted to either clientip or ipaddress, you can use the coalesce function to define a new field called ip, that takes the value of either clientip or ipaddress, depending on which is not null:

```
| eval ip=coalesce(clientip,ipaddress)
```

In your example, you have a set of events where the product name is extracted to either productName or productid, and you use the coalesce function to define a new field called productINFO, that takes the value of either productName or productid, depending on which is not null:

```
| eval productINFO=coalesce(productName,productid)
```

If both productName and productid fields have values for a given event, the coalesce function will return the value of the productName field because it appears first in the argument list. The productid field will be ignored by the coalesce function.

Therefore, the value for the productName field will be used to populate the productINFO field if both fields have values for a given event.

References:

> Search Command> Coalesce

> USAGE OF SPLUNK EVAL FUNCTION : COALESCE

NEW QUESTION 85

- (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 87**

- (Exam Topic 2)

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:**

The fillnull command replaces null values with 0 by default, if the value argument is not specified. You can use the value argument to specify a different value to replace null values with, such as N/A or NULL.

NEW QUESTION 88

- (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 92

- (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 93

- (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 95

- (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 99

- (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 101

- (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 103

- (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 105

- (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
```

src	num_events	total_events
107.3.146.207	1000	3405
108.65.113.83	1000	1120
109.169.32.135	1000	2079
11.17.160.129	1000	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 included. In Splunk, the transaction command is used to group events that share common characteristics into a single transaction. By default, the transaction command groups all matching events into a single transaction. However, you can use the maxspan option to limit the time span of the transactions. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction. 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 value. 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 108

- (Exam Topic 2)

Which of the following searches will return all clientip addresses that start with 108?

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

Answer: A

NEW QUESTION 110

- (Exam Topic 2)

Clicking a SEGMENT on a chart, _____.

- A. drills down for that value
- B. highlights the field value across the chart
- C. adds the highlighted value to the search criteria

Answer: C

NEW QUESTION 114

- (Exam Topic 2)

During the validation step of the Field Extractor workflow: Select your answer.

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

Answer: A

Explanation:

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

NEW QUESTION 119

- (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 121

- (Exam Topic 2)

which of the following are valid options with the chart command

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

Answer: AB

NEW QUESTION 123

- (Exam Topic 2)

Which of the following options will define the first event in a transaction?

- A. startswith

- B. with
- C. startingwith
- D. firstevent

Answer: A

Explanation:

The correct answer is A. startswith. The Explanation: is as follows:

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

NEW QUESTION 125

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SPLK-1002 Practice Exam Features:

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