



**Splunk**

## **Exam Questions SPLK-1002**

Splunk Core Certified Power User Exam

#### NEW QUESTION 1

- (Exam Topic 1)

A space is an implied \_\_\_\_\_ in a search string.

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

**Answer: B**

#### Explanation:

A space is an implied AND in a search string, which means that it acts as a logical operator that returns events that match both terms on either side of the space. For example, `status=200 method=GET` will return event that have both `status=200` and `method=GET`. Therefore, option B is correct, while options A, C and D are incorrect because they are not implied by a space in a search string.

#### NEW QUESTION 2

- (Exam Topic 1)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 3

- (Exam Topic 1)

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 4

- (Exam Topic 1)

Which of the following statements about tags is true?

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 5

- (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 marks<sup>1</sup>. 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 expression<sup>1</sup>. 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 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 describes POST workflow actions?

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

**Answer:** D

**Explanation:**

A workflow action is a link that appears when you click an event field value in your search results<sup>1</sup>. A workflow action can open a web page or run another search based on the field value<sup>1</sup>. There are two types of workflow actions: GET and POST<sup>1</sup>. A GET workflow action appends the field value to the end of a URI and opens it in a web browser<sup>1</sup>. A POST workflow action sends the field value as part of an HTTP request to a web server<sup>1</sup>. You can configure a workflow action to open a web page in either the same window or a new window<sup>1</sup>. Therefore, option D is correct, while options A, B and C are incorrect.

**NEW QUESTION 8**

- (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 fields<sup>2</sup>. You can display a chart in stack mode by changing the Stack Mode option in the Format menu<sup>2</sup>. Sta mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series<sup>2</sup>. 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 9**

- (Exam Topic 1)

Which of the following statements describes the command below (select all that apply) Sourcetype=access\_combined | transaction JSESSIONID

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

**Answer:** BCD

**Explanation:**

The command sourcetype=access\_combined | transaction JSESSIONID does three things:

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

as duration, eventcount, and starttime.  
Therefore, the statements B, C, and D are true.

#### NEW QUESTION 10

- (Exam Topic 1)

Which of the following are required to create a POST workflow action?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 10

- (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 datasets<sup>1</sup>. To enable data model acceleration, you must have administrative permissions or the accelerate\_datamodel capability<sup>1</sup>. Therefore, option D is correct. Accelerated data models cannot be edited unless you disable the acceleration first<sup>1</sup>. Therefore, option B is correct. Private data models cannot be accelerated because they are not visible to other users<sup>1</sup>. Therefore, option C is correct. Root events can be accelerated as long as they are not based on a search string<sup>1</sup>. Therefore, option A is incorrect.

#### NEW QUESTION 13

- (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 it<sup>3</sup>. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more<sup>3</sup>. 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 correlated<sup>3</sup>. 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 tags<sup>3</sup>. 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-ons<sup>3</sup>. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.

#### NEW QUESTION 18

- (Exam Topic 1)

Which of the following statements describes this search? sourcetype=access\_combined | transaction JSESSIONID | timechart avg (duration)

- A. This is a valid search and will display a timechart of the average duration, of each transaction event.
- B. This is a valid search and will display a stats table showing the maximum pause among transactions.
- C. No results will be returned because the transaction command must include the startswith and endswith options.
- D. No results will be returned because the transaction command must be the last command used in the search pipeline.

**Answer:** A

#### Explanation:

This search uses the transaction command to group events that share a common value for JSESSIONID into transactions<sup>1</sup>. The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction<sup>1</sup>. The search then uses the timechart command to create a time-series chart of the average duration of each transaction<sup>1</sup>. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field. Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction<sup>1</sup>. Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search<sup>1</sup>.

### NEW QUESTION 23

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event\_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

**Answer:** CD

#### Explanation:

Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error, success, login, logout, etc. Event types can also be used to create transactions, alerts, reports, dashboards, etc. Event types can be created in two ways:

- By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type.
  - By selecting an event in search results and clicking Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on the selected event.
- Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event\_type stanza in the transforms.conf file, not the props.conf file.

### NEW QUESTION 24

- (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 26

- (Exam Topic 1)

What is the correct syntax to search for a tag associated with a value on a specific fields?

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

**Answer:** D

#### Explanation:

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

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

### NEW QUESTION 27

- (Exam Topic 1)

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

- A. Auto-Extracted fields can be hidden in Pivot.
- B. Auto-Extracted fields can have their data type changed.
- C. Auto-Extracted fields can be given a friendly name for use in Pivot.
- D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

**Answer:** ABCD

#### Explanation:

Data model fields are fields that describe the attributes of a dataset in a data model<sup>2</sup>. Data model fields can be added using various methods such as Auto-Extracted, Evaluated or Lookup<sup>2</sup>. Auto-Extracted fields are fields that are automatically extracted from your raw data using various techniques such as regular expressions, delimiters or key-value pairs<sup>2</sup>. Auto-Extracted fields can be hidden in Pivot, which means that you can choose whether to display them or not in the Pivot interface<sup>2</sup>. Therefore, option A is correct. Auto-Extracted fields can have their data type changed, which means that you can specify whether they are strings, numbers, booleans or timestamps<sup>2</sup>. Therefore, option B is correct. Auto-Extracted fields can be given a friendly name for use in Pivot, which means that you can assign an alternative name to them that is more descriptive or user-friendly than the original field name<sup>2</sup>. Therefore, option C is correct. Auto-Extracted fields can be added if they already exist in the dataset with constraints, which means that you can include them in your data model even if they are already extracted from your raw data by applying filters or constraints to limit the scope of your dataset<sup>2</sup>. Therefore, option D is correct.



### NEW QUESTION 31

- (Exam Topic 1)

What are the two parts of a root event dataset?

- A. Fields and variables.
- B. Fields and attributes.
- C. Constraints and fields.
- D. Constraints and lookups.

**Answer:** C

#### Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects> A root event dataset is the base dataset for a data model that defines the source or sources of the data and the constraints and fields that apply to the data<sup>1</sup>. A root event dataset has two parts: constraints and fields<sup>1</sup>. Constraints are filters that limit the data to a specific index, source, sourcetype, host or search string<sup>1</sup>. Fields are the attributes that describe the data and can be extracted, calculated or looked up<sup>1</sup>. Therefore, option C is correct, while options A, B and D are incorrect.

### NEW QUESTION 35

- (Exam Topic 1)

Which of the following workflow actions can be executed from search results? (select all that apply)

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

**Answer:** ABD

#### Explanation:

As mentioned before, there are two types of workflow actions: GET and POST<sup>1</sup>. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it<sup>1</sup>. Another type of workflow action is Search, which runs another search based on the field value<sup>1</sup>. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

### NEW QUESTION 36

- (Exam Topic 1)

Which one of the following statements about the search command is true?

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

**Answer:** D

#### Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand> The search command is used to filter or refine your search results based on a search string that matches the events<sup>2</sup>. The search command behaves exactly like search strings before the first pipe, which means that you can use the same syntax and operators as you would use in the initial part of your search<sup>2</sup>. Therefore, option D is correct, while options A, B and C are incorrect because they are not true statements about the search command.

### NEW QUESTION 37

- (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 38

- (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 39**

- (Exam Topic 1)

Which of the following statements describe calculated fields? (select all that apply)

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

**Answer:** ABD

**Explanation:**

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

Calculated fields are fields that are created by performing calculations on existing fields using the eval command. Calculated fields can be used in the search bar to filter and transform events based on the calculated values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for performing calculations using the eval command, but rather results of performing calculations using the eval command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype. Therefore, statements A, B, and D are true about calculated fields.

**NEW QUESTION 43**

- (Exam Topic 1)

What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

- A. Custom visualizations
- B. Pre-configured data models
- C. Fields and event category tags
- D. Automatic data model acceleration

**Answer:** BC

**Explanation:**

The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it<sup>3</sup>. The CIM add-on includes pre-configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more<sup>3</sup>. Therefore, option B is correct. The CIM add-on also includes fields and event category tags that define the common attributes and labels for the data models<sup>3</sup>. Therefore, option C is correct. The CIM add-on does not include custom visualizations or automatic data model acceleration. Therefore, options A and D are incorrect.

**NEW QUESTION 48**

- (Exam Topic 2)

The timechart command is an example of which of the following command types?

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

**Answer:** B

**Explanation:**

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

- The timechart command is a Splunk command that creates a time series chart with corresponding table of statistics<sup>12</sup>.
- A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis<sup>1</sup>. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart<sup>1</sup>.
- Transforming commands are commands that change the format of the search results into a data structure that can be easily visualized<sup>3</sup>. Transforming commands often use stats functions to aggregate and summarize data<sup>3</sup>.
- Therefore, the timechart command is an example of a transforming command, as it transforms the search results into a chart and a table using stats functions<sup>123</sup>.

**NEW QUESTION 49**

- (Exam Topic 2)

This function of the stats command allows you to return the middle-most value of field X.

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

**Answer:** A

### NEW QUESTION 51

- (Exam Topic 2)

A field alias is created where field1—field2 and the Overwrite Field Values checkbox is selected. What happens if an event only contains values for field1?

- 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 convenience<sup>1</sup>.

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 field<sup>2</sup>.

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 52

- (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-axis<sup>2</sup>. 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 200<sup>2</sup>. 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)<sup>2</sup>. The values in the table are calculated by applying the function before the over clause to the events in each group<sup>2</sup>. 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 55

- (Exam Topic 2)

When using the transaction command, how are evicted transactions identified?

- A. Closed\_txn field is set to 0, or false.
- B. Max\_txn field is set to 0, or false.
- C. Txn\_field is set to 1, or true.
- D. open\_txn field is set to 1, or true.

**Answer:** A

#### Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints<sup>1</sup>.
- 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<sup>1</sup>.

- The transaction command adds some fields to the raw events that are part of the transaction<sup>12</sup>. These fields are:

- duration: The difference, in seconds, between the timestamps for the first and last events in the transaction<sup>12</sup>.

- eventcount: The number of events in the transaction<sup>12</sup>.

- closed\_txn: A Boolean field that indicates whether the transaction is closed or evicted<sup>2</sup>. A transaction is closed if it meets one of the following conditions: maxevents, maxpause, maxsp or startswith<sup>2</sup>. A transaction is evicted if it does not meet any of these conditions and exceeds the memory limit specified by maxopentxn or maxopenevents<sup>23</sup>.

- Therefore, evicted transactions can be distinguished from non-evicted transactions by checking the value of the closed\_txn field. The closed\_txn field is set to 0, or false, for evicted transactions and 1 for non-evicted, or closed, transactions<sup>23</sup>.

### NEW QUESTION 59

- (Exam Topic 2)

The eval command 'if' function requires the following three arguments (in order):



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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 64**

- (Exam Topic 2)

Field aliases are used to \_\_\_\_\_ data

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

**Answer:** D

**NEW QUESTION 65**

- (Exam Topic 2)

Which of the following search control will not re-rerun the search? (Select all that apply.)

- A. zoom out
- B. selecting a bar on the timeline
- C. deselect
- D. selecting a range of bars on the timelines

**Answer:** BCD

**Explanation:**

The timeline is a graphical representation of your search results that shows the distribution of events over time<sup>2</sup>. You can use the timeline to zoom in or out of a specific time range or to select one or more bars on the timeline to filter your results by that time range<sup>2</sup>. However, these actions will not re-run the search, but rather refine the existing results based on the selected time range<sup>2</sup>. Therefore, options B, C and D are correct, while option A is incorrect because zooming out will re-run the search with a broader time range.

**NEW QUESTION 68**

- (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 71**

- (Exam Topic 2)

Which field extraction method should be selected for comma-separated data?

- A. Regular expression
- B. Delimiters
- C. eval expression
- D. table extraction

**Answer:** B

**Explanation:**

The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation<sup>1</sup>. The other options are incorrect because they are not suitable for comma-separated data. The regular expression method works best with unstructured event data, where you select and highlight one or more fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation<sup>23</sup>.

### NEW QUESTION 73

- (Exam Topic 2)

The transaction command allows you to \_\_\_\_\_ events across multiple sources

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

**Answer: B**

#### Explanation:

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

### NEW QUESTION 76

- (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 81

- (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 84

- (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 89

- (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 92**

- (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 time<sup>23</sup>

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 93**

- (Exam Topic 2)

When using the transaction command, what does the argument maxspan do?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 95**

- (Exam Topic 2)

What commands can be used to group events from one or more data sources?

- A. eval, coalesce
- B. transaction, stats
- C. stats, format
- D. top, rare

**Answer:** B

**Explanation:**

The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of a subsearch, not to group events. The top and rare commands are used to rank the most or least common values of a field, not to group events<sup>23</sup>

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command. 3: Splunk Documentation, stats command.

**NEW QUESTION 100**

- (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 operator<sup>2</sup>. 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 string<sup>2</sup>. 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 104**

- (Exam Topic 2)

What are search macros?

- A. Lookup definitions in lookup tables.
- B. Reusable pieces of search processing language.
- C. A method to normalize fields.
- D. Categories of search results.

**Answer:** B

**Explanation:**

The correct answer is B. Reusable pieces of search processing language. The explanation is as follows:

- Search macros are knowledge objects that allow you to insert chunks of SPL into other searches<sup>12</sup>.
- Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command<sup>12</sup>.
- You can also specify whether the macro field takes any arguments and define validation expressions for them<sup>12</sup>.
- Search macros can help you make your SPL searches shorter and easier to understand<sup>3</sup>.
- To use a search macro in a search string, you need to put a backtick character ( ` ) before and after the macro name<sup>[^1^][1]</sup>. For example, mymacro`.

**NEW QUESTION 106**

- (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 111**

- (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 expression<sup>2</sup>. The FX has a button that displays events that do not contain extracted fields, which is the Non-Matches button<sup>2</sup>. The Non-Matches button shows you the events that do not match the regular expression that you have defined for your field extraction<sup>2</sup>. This way, you can check if your field extraction is accurate and complete<sup>2</sup>. 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 115**

- (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 118

- (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 120

- (Exam Topic 2)

Which of the following eval commands will provide a new value for host from src if it exists?

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

**Answer:** D

#### Explanation:

- The eval command is a Splunk command that allows you to create or modify fields using expressions .
- The if function is an expression that evaluates a condition and returns a value based on whether the condition is true or false. The syntax of the if function is if(X,Y,Z), where X is the condition, Y is th value to return if X is true, and Z is the value to return if X is false.
- The isnotnull function is an expression that returns true if the argument is not null, and false otherwise The syntax of the isnotnull function is isnotnull(X), where X is the argument to check.
- Therefore, the expression if (isnotnull (src), src, host) returns the value of src if it is not null, and th value of host otherwise. This means that it will provide a new value for host from src if it exist keep the original value of host otherwise.

#### NEW QUESTION 121

- (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 122

- (Exam Topic 2)

Which of these search strings is NOT valid:

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

**Answer:** A



**Explanation:**

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

**NEW QUESTION 125**

- (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 128**

- (Exam Topic 2)

When would a user select delimited field extractions using the Field Extractor (FX)?

- A. When a log file has values that are separated by the same character, for example, commas.
- B. When a log file contains empty lines or comments.
- C. With structured files such as JSON or XML.
- D. When the file has a header that might provide information about its structure or format.

**Answer:** A

**Explanation:**

The correct answer is A. When a log file has values that are separated by the same character, for example, commas.

The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions<sup>1</sup>.

The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them<sup>1</sup>.

The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds<sup>1</sup>.

Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions.

The other options are not correct because they are not suitable for the delimited field extraction method. These options are:

- B. When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or include some unwanted values.
- C. With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions<sup>2</sup>. The delimited method might not work well with this type of data, as it might not recognize the nested structure or the special characters.
- D. When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data, as it might not be able to identify the fields based on the header information.

References:

- Build field extractions with the field extractor
- Configure indexed field extraction

**NEW QUESTION 132**

- (Exam Topic 2)

Which method in the Field Extractor would extract the port number from the following event?

| 10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin <web error>

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

**Answer:** B

**Explanation:**

The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:

```
rex "\+\\+\\+\\+port (?<port>\\d+)"
```

This will create a field called port with the value 54 for the event.

The delimiter method is not suitable for this event because there is no consistent delimiter between the fields. The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.

Reference: 1

Splunk Core Certified Power User | Splunk

**NEW QUESTION 135**

- (Exam Topic 2)

For the following search, which field populates the x-axis? `index=security sourcetype=linux secure | timechart count by action`

- A. action
- B. source type
- C. `_time`
- D. time

**Answer:** C

**Explanation:**

The correct answer is C. `_time`.

The timechart command creates a time series chart with corresponding table of statistics, with time used as the X-axis<sup>1</sup>. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart<sup>1</sup>. In this case, the split-by field is action, which means that the chart will have different lines for different actions, such as accept, reject, or fail<sup>2</sup>. The count function will calculate the number of events for each action in each time bin<sup>1</sup>.

For example, the following image shows a timechart of the count by action for a similar search<sup>3</sup>:

As you can see, the x-axis is populated by the `_time` field, which represents the time range of the search. The y-axis is populated by the count function, which represents the number of events for each action. The legend shows the different values of the action field, which are used to split the chart into different series.

Reference:

2: Timechart Command In Splunk With Example - Mindmajix 1: timechart - Splunk Documentation 3: timechart command examples - Splunk Documentation

**NEW QUESTION 140**

- (Exam Topic 2)

These allow you to categorize events based on search terms. Select your answer.

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

**Answer:** B

**NEW QUESTION 145**

- (Exam Topic 2)

Complete the search, `.... | _____ failure>successes`

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

**Answer:** B

**Explanation:**

The where command can be used to complete the search below.

`... | where failure>successes`

The where command is a search command that allows you to filter events based on complex or custom criteria. The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as `>`, `<`, `=`, `+`, `-`, etc. The where command can be used after any transforming command that creates a table or a chart.

The search string below does the following:

- It uses `...` to represent any search criteria or commands before the where command.
- It uses the where command to filter events based on a comparison between two fields: failure and successes.
- It uses the greater than operator (`>`) to compare the values of failure and successes fields for each event.
- It only keeps events where failure is greater than successes.

**NEW QUESTION 149**

- (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 150**

- (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 defined<sup>1</sup>.

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 field<sup>2</sup>. 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 fields<sup>3</sup>.

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 153**

- (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 157**

- (Exam Topic 2)

Which of the following examples would use a POST workflow action?

- A. Perform an external IP lookup based on a domain value found in events.
- B. Use the field values in an HTTP error event to create a new ticket in an external system.
- C. Launch secondary Splunk searches that use one or more field values from selected events.
- D. Open a web browser to look up an HTTP status code.

**Answer:** B

**Explanation:**

The correct answer is B. Use the field values in an HTTP error event to create a new ticket in an external system.

A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create HTML links, generate HTTP POST requests, or launch secondary searches based on field values<sup>1</sup>.

There are three types of workflow actions that can be set up using Splunk Web: GET, POST, and Search<sup>2</sup>.

➤ GET workflow actions create typical HTML links to do things like perform Google searches on specific values or run domain name queries against external WHOIS databases<sup>2</sup>.

➤ POST workflow actions generate an HTTP POST request to a specified URI. This action type enables you to do things like creating entries in external issue management systems using a set of relevant field values<sup>2</sup>.

➤ Search workflow actions launch secondary searches that use specific field values from an event, such as a search that looks for the occurrence of specific combinations of ipaddress and http\_status field values in your index over a specific time range<sup>2</sup>.

Therefore, the example that would use a POST workflow action is B. Use the field values in an HTTP error event to create a new ticket in an external system. This example requires sending an HTTP POST request to the URI of the external system with the field values from the event as arguments.

The other examples would use different types of workflow actions. These examples are:

- A. Perform an external IP lookup based on a domain value found in events: This example would use a GET workflow action to create a link to an external IP lookup service with the domain value as a parameter.
- C. Launch secondary Splunk searches that use one or more field values from selected events: This example would use a Search workflow action to run another Splunk search with the field values from the event as search terms.
- D. Open a web browser to look up an HTTP status code: This example would also use a GET workflow action to create a link to a web page that explains the meaning of the HTTP status code.

References:

- Splxicon:Workflowaction
- About workflow actions in Splunk Web

**NEW QUESTION 158**

- (Exam Topic 2)

Which of the following statements about calculated fields in Splunk is true?

- A. Calculated fields cannot be chained together to create more complex fields
- B. Calculated fields can be chained together to create more complex fields.
- C. Calculated fields can only be used in dashboards.

D. Calculated fields can only be used in saved reports.

**Answer:** B

**Explanation:**

The correct answer is B. Calculated fields can be chained together to create more complex fields.

Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field<sup>1</sup>.

Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as:

discount = total \* 0.9

This will create a new field named discount that is equal to 90% of the total field value for each event<sup>2</sup>. References:

- > About calculated fields
- > Chaining calculated fields

**NEW QUESTION 161**

- (Exam Topic 2)

How is an event type created from the search window? (select all that apply)

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

**Answer:** AC

**Explanation:**

In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type<sup>1</sup>. This opens the Save as Event Type dial you can provide the event type name and optionally apply tags to it<sup>1</sup>.

You can also create an event type by editing the eventtypes.conf file and adding a new stanza<sup>1</sup>. Each stanza in the eventtypes.conf file represents an event type<sup>1</sup>.

The stanza name is the name of the event type, and

the search attribute specifies the search string that defines the event type<sup>1</sup>.

It's important to note that while you can use the eventtype command in a search to find events associated with a specific event type, adding | eventtype to the SPL and executing the search does not create a new event type<sup>1</sup>. Similarly, clicking Event Actions > Build Event Type in an event's detail dropdown does not create new event type<sup>1</sup>.

**NEW QUESTION 163**

- (Exam Topic 2)

Which of the following is included with the Common Information Model (CIM) add-on?

- A. Search macros
- B. Event category tags
- C. Workflow actions
- D. tsidx files

**Answer:** B

**Explanation:**

The correct answer is B. Event category tags. This is because the CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category. You can learn more about event category tags from the Splunk documentation<sup>12</sup>. The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

**NEW QUESTION 164**

- (Exam Topic 2)

A data model consists of which three types of datasets?

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

**Answer:** B

**Explanation:**

The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole.

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

<https://docs.splunk.com/Spdexicon:Datamodeldataset>



#### NEW QUESTION 168

- (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 170

- (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 171

- (Exam Topic 2)

Which search would limit an "alert" tag to the "host" field?

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

**Answer:** D

#### Explanation:

The search below would limit an "alert" tag to the "host" field. tag::host=alert

The search does the following:

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

#### NEW QUESTION 174

- (Exam Topic 2)

The limit attribute will \_\_\_\_\_.

- A. override default of 10
- B. only work with top command
- C. override default of 20
- D. override default of 15

**Answer:** A

#### NEW QUESTION 178

- (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 documentation<sup>1</sup>.

#### NEW QUESTION 179

- (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 184**

- (Exam Topic 2)

Consider the following search: index=web sourcetype=access\_corabined

The log shows several events that share the same jsessionid value (SD462K101O2F267). View the events as a group.

From the following list, which search groups events by jSESSIONID?

- A. index=web sourcetype=access\_combined | transaction JSESSIONID | search SD462K101C2F267  
B. index=web sourcetype=access\_combined SD462K101O2F267 | table JSESSIONID  
C. index=web sourcetype=access\_combined | highlight JSESSIONID | search SD462K101O2F267  
D. index=web sourcetype=access\_combined JSESSTONID <SD4€2K101O2F267>

**Answer:** A

**Explanation:**

The transaction command groups events that share a common value in a specified field, such as JSESSIONID, and that occur within a specified time range. The search command filters the results to show only the events that match the given value of JSESSIONID. This search groups the events by JSESSIONID and then shows only the events that have the value SD462K101C2F267 for JSESSIONID2

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command.

**NEW QUESTION 187**

- (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 192**

- (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 results<sup>2</sup>. 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 pairs<sup>2</sup>. The fields sidebar only shows selected fields and interesting fields<sup>2</sup>. 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 command<sup>2</sup>. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values<sup>2</sup>. 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 194**

- (Exam Topic 2)

When extracting fields, we may choose to use our own regular expressions

- A. True
- B. False

**Answer:** A

**NEW QUESTION 195**

- (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 200**

- (Exam Topic 2)

Which of the following statements about tags is true?

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

**Answer:** B

**Explanation:**

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

➤ Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or value 404 as not\_found .

**NEW QUESTION 201**

- (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 205**

- (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 more<sup>2</sup>. The stats command supports various functions that you can use to perform calculations on your fields<sup>2</sup>. 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 group<sup>2</sup>. Therefore, option B is correct, while options A, C and D are incorrect because they are valid stats functions.

### NEW QUESTION 209

- (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 expressions<sup>1</sup>.

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 211

- (Exam Topic 2)

Which of the following transforming commands can be used with transactions?

- A. chart, timechart, stats, eventstats
- B. chart, timechart, stats, diff
- C. chart, timechart, datamodel, pivot
- D. chart, timechart, stats, pivot

**Answer:** A

#### Explanation:

The correct answer is A. chart, timechart, stats, eventstats.

Transforming commands are commands that change the format of the search results into a table or a chart. They can be used to perform statistical calculations, create visualizations, or manipulate data in various ways<sup>1</sup>.

Transactions are groups of events that share some common values and are related in some way. Transactions can be defined by using the transaction command or by creating a transaction type in the transactiontypes.conf file<sup>2</sup>.

Some transforming commands can be used with transactions to create tables or charts based on the transaction fields. These commands include:

➤ chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics<sup>3</sup>.

➤ timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers<sup>4</sup>.

➤ stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields<sup>5</sup>.

➤ eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.

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

➤ | chart count by user : This command creates a table or a chart that shows how many transactions each user has.

➤ | timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.

➤ | stats sum(eventcount) as total\_events by user : This command creates a table that shows the total number of events for each user across all transactions.

➤ | eventstats avg(duration) as avg\_duration : This command adds a new field named avg\_duration to each transaction that shows the average duration of all transactions.

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

➤ diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.

➤ datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.

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

References:

➤ [About transforming commands](#)

➤ [About transactions](#)

➤ [chart command overview](#)

➤ [timechart command overview](#)

➤ [stats command overview](#)

➤ [\[eventstats command overview\]](#)

➤

[diff command overview]

➤ [datamodel command overview]

➤ [pivot command overview]

#### NEW QUESTION 213

- (Exam Topic 2)

The eval command allows you to do which of the following? (Choose all that apply.)

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

**Answer:** ABCD

#### NEW QUESTION 218

- (Exam Topic 2)

Highlighted search terms indicate \_\_\_\_\_ search results in Splunk.

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 223

- (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 225

- (Exam Topic 2)

Which workflow uses field values to perform a secondary search?

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

**Answer:** C

#### Explanation:

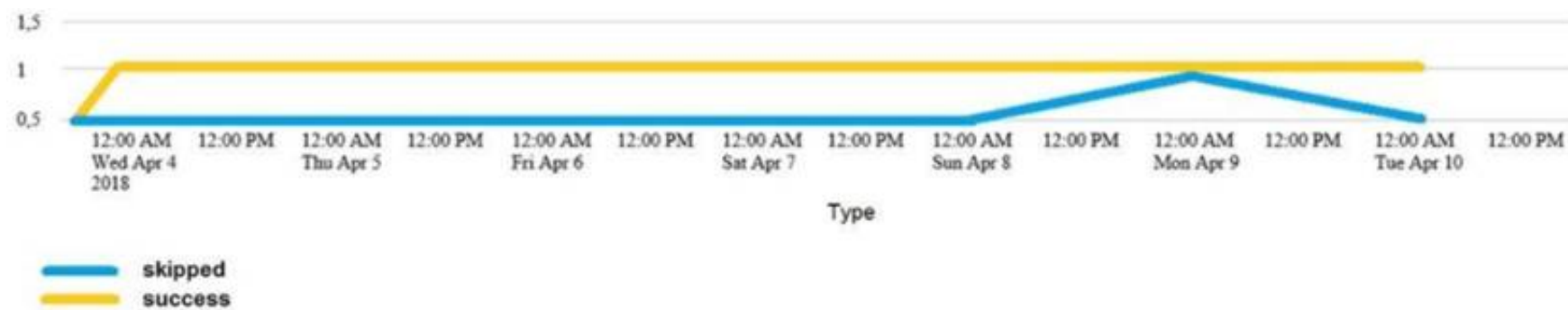
<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb>

#### NEW QUESTION 228

- (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 230**

- (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 234**

- (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<br>1000<br>1000<br>405 | 3405         |
| 108.65.113.83  | 1000<br>120                 | 1120         |
| 109.169.32.135 | 1000<br>1000<br>79          | 2079         |
| 11.17.160.129  | 1000<br>1000<br>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 239

- (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 240

- (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 241

- (Exam Topic 2)

Which of the following statements would help a user choose between the transaction and stats commands?

- A. state can only group events using IP addresses.
- B. The transaction command is faster and more efficient.

- C. There is a 1000 event limitation with the transaction command.
- D. Use state when the events need to be viewed as a single event.

**Answer:** C

**Explanation:**

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

One of the statements that would help a user choose between the transaction and stats commands is that there is a 1000 event limitation with the transaction command<sup>3</sup>. The transaction command is used to group events that share a common value for one or more fields into transactions<sup>3</sup>. The transaction command has a default limit of 1000 events per transaction, which means that it will not group more than 1000 events into a single transaction<sup>3</sup>. This limit can be changed by using the maxevents parameter, but it can affect the performance and memory usage of Splunk<sup>3</sup>. Therefore, option C is correct, while options A, B and D are incorrect because they are not statements that would help a user choose between the transaction and stats commands.

**NEW QUESTION 242**

- (Exam Topic 2)

How is a Search Workflow Action configured to run at the same time range as the original search?

- A. Set the earliest time to match the original search.
- B. Select the same time range from the time-range picker.
- C. Select the "Use the same time range as the search that created the field listing" checkbox.
- D. Select the "Overwrite time range with the original search" checkbox.

**Answer:** C

**Explanation:**

To configure a Search Workflow Action to run at the same time range as the original search, you need to select the "Use the same time range as the search that created the field listing" checkbox. This will ensure that the workflow action search uses the same earliest and latest time parameters as the original search.

**NEW QUESTION 243**

- (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 schedule<sup>3</sup>. An alert is a way to monitor your data and get notified when certain conditions are met<sup>3</sup>. You can create an alert by specifying a search and a triggering condition<sup>3</sup>. You can also specify how often you want to run the search and how you want to receive the alert notifications<sup>3</sup>. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk<sup>3</sup>. 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 day<sup>3</sup>. 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 248**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons and Answers in PDF Format

### SPLK-1002 Practice Exam Features:

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

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