



# Splunk

## Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (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 2

- (Exam Topic 1)

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

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

**Answer:** C

#### Explanation:

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

An event type is a way to categorize events based on a search string that matches the events<sup>2</sup>. You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names<sup>2</sup>. An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again<sup>2</sup>. Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.

### NEW QUESTION 3

- (Exam Topic 1)

Which of the following Statements about macros is true? (select all that apply)

- A. Arguments are defined at execution time.
- B. Arguments are defined when the macro is created.
- C. Argument values are used to resolve the search string at execution time.
- D. Argument values are used to resolve the search string when the macro is created.

**Answer:** BC

#### Explanation:

A macro is a way to save a commonly used search string as a variable that you can reuse in other searches<sup>1</sup>. When you create a macro, you can define arguments that are placeholders for values that you specify at execution time<sup>1</sup>. The argument values are used to resolve the search string when the macro is invoked, not when it is created<sup>1</sup>. Therefore, statements B and C are true, while statements A and D are false.

### NEW QUESTION 4

- (Exam Topic 1)

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

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

**Answer:** B

#### Explanation:

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

The eval command is used to create new fields or modify existing fields based on an expression<sup>2</sup>. The output of an eval expression is a calculated field, which is a field that you create based on the value of another field or fields<sup>2</sup>. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format<sup>2</sup>. Therefore, option B is correct, while options A, C and D are incorrect because they are not names of knowledge objects that represent the output of an eval expression.

### NEW QUESTION 5

- (Exam Topic 1)

Data model are composed of one or more of which of the following datasets? (select all that apply.)

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

**Answer:** ABC

**Explanation:**

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

Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:

Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.

Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.

Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

**NEW QUESTION 6**

- (Exam Topic 1)

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

**Answer:** A

**Explanation:**

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

A pivot is a tool that allows you to create reports and dashboards using data models without writing any SPL commands<sup>2</sup>. You can use pivots to explore, filter, split and visualize your data using a graphical

interface<sup>2</sup>. Pivots are designed for users who want to analyze and report on their data without having to learn the SPL syntax or the underlying structure of the data<sup>2</sup>. Therefore, option A is correct, while options B, C and D are incorrect because they are not the typical group of users who would use pivots.

**NEW QUESTION 7**

- (Exam Topic 1)

A calculated field maybe based on which of the following?

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

**Answer:** B

**Explanation:**

As mentioned before, a calculated field is a field that you create based on the value of another field or

fields<sup>2</sup>. A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs<sup>2</sup>. Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

**NEW QUESTION 8**

- (Exam Topic 1)

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

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

**Answer:** B

**Explanation:**

A field alias is a way to assign an alternative name to an existing field without changing the original field name or value<sup>2</sup>. You can use field aliases to make your field names more consistent or descriptive across

different sources or sourcetypes<sup>2</sup>. When you run a search without any transforming commands in Smart Mode Splunk automatically identifies and displays interesting fields in your results<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>. If you have created a field alias based on an original field, both the original field name and the alias name will appear in the Interesting Fields list if they meet these criteria<sup>2</sup>. However, only one of them will appear in each event depending on which one you have specified in your search string<sup>2</sup>. Therefore, option B is correct, while options A, C and D are incorrect.

**NEW QUESTION 9**

- (Exam Topic 1)

Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

- A. Alerts
- B. Email
- C. Database
- D. User permissions

**Answer:** ABC

**Explanation:**

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

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 several data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more<sup>3</sup>. Therefore, options A, B and C are correct because they are names of some of the data models included in the CIM add-on. Option D is incorrect because User permissions is not a name of a data model in the CIM add-on.

**NEW QUESTION 10**

- (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 10**

- (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 15**

- (Exam Topic 1)

What does the transaction command do?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 19**

- (Exam Topic 1)

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 22**

- (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 POST1. 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 it1. Another type of workflow action is Search, which runs another search based on the field value1. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

**NEW QUESTION 24**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 25**

- (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 it3. The CIM add-on includes pre-configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. 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 models3. 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 28**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 32**



- (Exam Topic 2)

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Fast
- B. Smart
- C. Verbose

**Answer: C**

**Explanation:**

The search modes determine how Splunk processes your search and displays your results<sup>2</sup>. There are three search modes: Fast, Smart and Verbose<sup>2</sup>. The search mode that automatically returns all extracted fields in the fields sidebar is Verbose<sup>2</sup>. The Verbose mode shows all the fields that are extracted from your events, including default fields, indexed fields and search-time extracted fields<sup>2</sup>. The fields sidebar is a panel that shows the fields that are present in your search results<sup>2</sup>. Therefore, option C is correct, while options A and B are incorrect because they are not search modes that automatically return all extracted fields in the fields sidebar.

**NEW QUESTION 37**

- (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 40**

- (Exam Topic 2)

What type of command is eval?

- A. Streaming in some modes
- B. Report generating
- C. Distributable streaming
- D. Centralized streaming

**Answer: C**

**Explanation:**

The correct answer is C. Distributable streaming. This is because the eval command is a type of command that can run on the indexers before the results are sent to the search head. This reduces the amount of data that needs to be transferred and improves the search performance. Distributable streaming commands can operate on each event or result individually, without depending on other events or results. You can learn more about the types of commands and how they affect search performance from the Splunk documentation<sup>1</sup>.

**NEW QUESTION 45**

- (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 49**

- (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 53**

- (Exam Topic 2)

The Splunk Common Information Model (CIM) is a collection of what type of knowledge object?

- A. KV Store
- B. Lookups
- C. Saved searches
- D. Data models

**Answer: D**

**Explanation:**

The Splunk Common Information Model (CIM) is a collection of data models that apply a common structure and naming convention to data from any source. A data model is a type of knowledge object that defines the structure and relationships of fields in a dataset. A data model can have one or more datasets, which are subsets of the data model that represent different aspects of the data. For example, the Network Traffic data model has datasets such as All Traffic, DNS, HTTP, etc. The CIM contains 28 pre-configured data models that cover various domains such as authentication, network traffic, web, email, etc. The CIM is implemented as an add-on that contains the JSON files for the data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time23

1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, Overview of the Splunk Common Information Model 1. 3: Splunkbase, Splunk Common Information Model (CIM) 2.

**NEW QUESTION 56**

- (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 59**

- (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 62

- (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 66

- (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 68

- (Exam Topic 2)

If a search returns \_\_\_\_\_ it can be viewed as a chart.

- A. timestamps
- B. statistics
- C. events
- D. keywords

**Answer:** B

**Explanation:**

If a search returns statistics, it can be viewed as a chart<sup>2</sup>. Statistics are tabular data that show the relationship between two or more fields<sup>2</sup>. You can create statistics by using commands such as stats, chart or timechart<sup>2</sup>. You can view statistics as a chart by selecting the Visualization tab in the Search app and

choosing a chart type such as column, line or pie2. Therefore, option B is correct, while options A, C and D are incorrect because they are not types of data that can be viewed as a chart.

#### NEW QUESTION 72

- (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 73

- (Exam Topic 2)

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

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

**Answer:** BD

#### Explanation:

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

➤ Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called "alert" for the field name "status" and the field value "critical". This means that only events that have status=critical will have the "alert" tag applied to them.

➤ Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called "web" for the search string sourcetype=access\_combined. This means that only events that match the search string sourcetype=access\_combined will have the "web" tag applied to them.

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

#### NEW QUESTION 74

- (Exam Topic 2)

Why are tags useful in Splunk?

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

**Answer:** C

#### Explanation:

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

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

#### NEW QUESTION 76

- (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 77**

- (Exam Topic 2)

A data model consists of which three types of datasets?

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

**Answer:** B

**Explanation:**

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

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

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

**NEW QUESTION 78**

- (Exam Topic 2)

This is what Splunk uses to categorize the data that is being indexed.

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

**Answer:** A

**NEW QUESTION 81**

- (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 86**

- (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 91**

- (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 94

- (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 multivalued 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-length.

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 convenience.

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 98

- (Exam Topic 2)

By default search results are not returned in \_\_\_\_\_ order.

- A. Chronological
- B. Reverse chronological
- C. ASCII
- D. Alphabetical

**Answer:** AD

#### NEW QUESTION 101

- (Exam Topic 2)

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

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 JSESSIONID <SD462K101O2F267>

**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 JSESSIONID.

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

#### NEW QUESTION 105

- (Exam Topic 2)

The gauge command:

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

**Answer:** B

#### NEW QUESTION 106

- (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 109

- (Exam Topic 2)

A user wants to create a new field alias for a field that appears in two sourcetypes. How many field aliases need to be created?

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

**Answer:** B

#### NEW QUESTION 114

- (Exam Topic 2)

Which of the following commands will show the maximum bytes?

- A. sourcetype=access\_\* | maximum totals by bytes
- B. sourcetype=access\_\* | avg (bytes)
- C. sourcetype=access\_\* | stats max(bytes)
- D. sourcetype=access\_\* | max(bytes)

**Answer:** C

#### NEW QUESTION 117

- (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 120

- (Exam Topic 2)

\_\_\_\_\_ datasets can be added to root dataset to narrow down the search

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 125

- (Exam Topic 2)

Which of the following is true about the Splunk Common Information Model (CIM)?

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



D. The data models included in the CIM are configured with data model acceleration turned on.

**Answer:** D

**Explanation:**

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

**NEW QUESTION 128**

- (Exam Topic 2)

What is the correct format for naming a macro with multiple arguments?

- A. monthly\_sales(argument 1, argument 2, argument 3)
- B. monthly\_sales(3)
- C. monthly\_sales[3]
- D. monthly\_sales[argument 1, argument 2, argument 3]

**Answer:** C

**Explanation:**

The correct format for naming a macro with multiple arguments is monthly\_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as monthly\_sales[region,salesperson,date].

**NEW QUESTION 129**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

The time range specified for a historical search defines the amount of data fetched from the index matching that time range<sup>2</sup>. A historical search is a search that runs over a fixed period of time in the past<sup>2</sup>. When you run a historical search, Splunk searches the index for events that match your search string and fall within the specified time range<sup>2</sup>. Therefore, option B is correct, while options A and C are incorrect because they are not what the time range defines for a historical search.

**NEW QUESTION 130**

- (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 133**

.....

## Relate Links

**100% Pass Your SPLK-1002 Exam with ExamBible Prep Materials**

<https://www.exambible.com/SPLK-1002-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>