
# Splunk

## Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

**NEW QUESTION 1**
- (Exam Topic 1)
Which of the following can be used with the eval command tostring function (select all that apply)

A. ''hex''
B. ''commas''
C. ''Decimal''
D. ''duration''

**Answer:** ABD

**Explanation:**
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY The tostring function in the eval command converts a numeric value to a string value. It can take an optional second argument that specifies the format of the string value. Some of the possible formats are:

- hex: converts the numeric value to a hexadecimal string.
- commas: adds commas to separate thousands in the numeric value.
- duration: converts the numeric value to a human-readable duration string, such as "2h 3m 4s". Therefore, the formats A, B, and D can be used with the tostring function.

**NEW QUESTION 2**
- (Exam Topic 1)
Which of the following statements describes macros?

A. A macro is a reusable search string that must contain the full search.
B. A macro is a reusable search string that must have a fixed time range.
C. A macro Is a reusable search string that may have a flexible time range.
D. A macro Is a reusable search string that must contain only a portion of the search.

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros
A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

**NEW QUESTION 3**
- (Exam Topic 1)
Which of the following statements about data models and pivot are true? (select all that apply)

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

**Answer:** D

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

**NEW QUESTION 4**
- (Exam Topic 1)
How does a user display a chart in stack mode?

A. By using the stack command.
B. By turning on the Use Trellis Layout option.
C. By changing Stack Mode in the Format menu.
D. You cannot display a chart in stack mode, only a timechart.

**Answer:** C

**Explanation:**
A chart is a graphical representation of your search results that shows the relationship between two or more fields2. You can display a chart in stack mode by changing the Stack Mode option in the Format menu2. Sta mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series2. Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

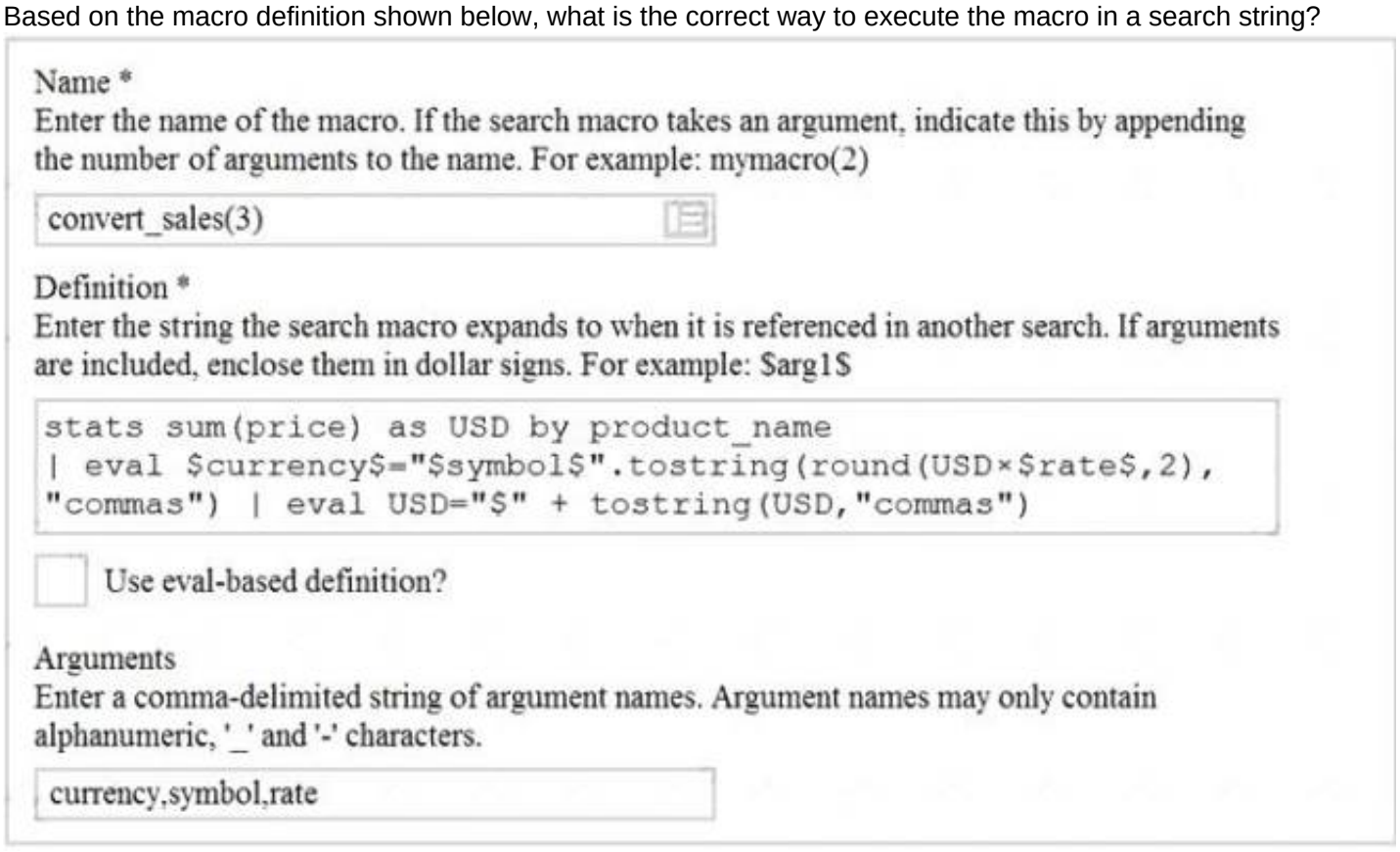
**NEW QUESTION 5**
- (Exam Topic 1)
Which of the following are required to create a POST workflow action?

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 6**
- (Exam Topic 1)
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?




A. Convert_sales (euro, €, 79)”
B. Convert_sales (euro, €, .79)
C. Convert_sales ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)

**Answer:** B

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros
The correct way to execute the macro in a search string is to use the format macro_name($arg1$, $arg2$, ...) where $arg1$, $arg2$, etc. are the arguments for the macro. In this case, the macro name is convert_sales and it takes three arguments: currency, symbol, and rate. The arguments are enclosed i signs and separated by commas. Therefore, the correct way to execute the macro is convert_sales($euro$, $€$ .79).

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

**NEW QUESTION 8**
- (Exam Topic 1)
In what order arc the following knowledge objects/configurations applied?

A. Field Aliases, Field Extractions, Lookups
B. Field Extractions, Field Aliases, Lookups

C. Field Extractions, Lookups, Field Aliases
D. Lookups, Field Aliases, Field Extractions

**Answer:** B

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze2. Some examples of knowledge objects are field extractions, field aliases and lookups2. Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. Field aliases are ways to assign alternative names to existing fields without changing the original field names or values2. Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases2. The order in which these knowledge objects/configurations are applied is as follows: field extractions, field aliases and then lookups2. This means that Splunk first extracts fields from your raw data, then applies any aliases to the extracted fields and then performs any lookups on the aliased fields2. Therefore, option B is correct, while options A, C and D are incorrect.

**NEW QUESTION 9**
- (Exam Topic 1)
Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

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

**Answer:** ABD

**Explanation:**
The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction.
index=main | transaction clientip host maxspan=30s maxpause=5s The search does the following:

- It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes.
- It uses the transaction command to group events into transactions based on two fields: clientip and host.

The transaction command creates new events from groups of events that share the same clientip and host values.

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

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

**NEW QUESTION 10**
- (Exam Topic 1)
What is the correct syntax to search for a tag associated with a value on a specific fields?

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

**Answer:** D

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

**NEW QUESTION 10**
- (Exam Topic 1)
What does the following search do?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

A. Creates a table of the total count of users and split by corndogs.
B. Creates a table of the total count of mysterymeat corndogs split by user.
C. Creates a table with the count of all types of corndogs eaten split by user.
D. Creates a table that groups the total number of users by vegetarian corndogs.

**Answer:** B

**Explanation:**
The search string below creates a table of the total count of mysterymeat corndogs split by user.
| stats count by user | where corndog=mysterymeat The search string does the following:

- It uses the stats command to calculate the count of events for each value of the user field. The stats command creates a table with two columns: user and count.
- It uses the where command to filter the results by the value of the corndog field. The where command only keeps the rows where corndog equals mysterymeat.

Therefore, the search string creates a table of the total count of mysterymeat corndogs split by user.

**NEW QUESTION 11**
- (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 14**
- (Exam Topic 1)
When creating a Search workflow action, which field is required?

A. Search string
B. Data model name
C. Permission setting
D. An eval statement

**Answer:** A

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction A workflow action is a link that appears when you click an event field value in your search results2. A
workflow action can open a web page or run another search based on the field value2. There are two types of workflow actions: GET and POST2. A GET workflow action appends the field value to the end of a URI and opens it in a web browser2. A POST workflow action sends the field value as part of an HTTP request to a web server2. When creating a Search workflow action, which is a type of GET workflow action that runs another search based on the field value, the only required field is the search string2. The search string defines the search that will be run when the workflow action is clicked2. Therefore, option A is correct, while options B, C and D are incorrect because they are not required fields for creating a Search workflow action.

**NEW QUESTION 15**
- (Exam Topic 1)
Which of the following statements describe the search string below?
| datamodel Application_State All_Application_State search

A. Evenrches would return a report of sales by state.
B. Events will be returned from the data model named Application_State.
C. Events will be returned from the data model named All_Application_state.
D. No events will be returned because the pipe should occur after the datamodel command

**Answer:** B

**Explanation:**
The search string below returns events from the data model named Application_State.
| datamodel Application_State All_Application_State search The search string does the following:
- It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.
- It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications.
- It specifies the name of the dataset as All_Application_State. This is a root dataset in the data model that contains all events from all child datasets.
- It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.

**NEW QUESTION 19**
- (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 results2. There are three search modes: Fast, Smart and Verbose2. The search mode that automatically returns all extracted fields in the fields sidebar is Verbose2. The Verbose mode shows all the fields that are extracted from your events, including default fields, indexed fields and search-time extracted fields2. The fields sidebar is a panel that shows the fields that are present in your search results2. 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 20**
- (Exam Topic 2)
By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?

A. Turned off
B. Turned on
C. Determined automatically based on the sourcetype.
D. Determined automatically based on the data source.

**Answer:** D

**Explanation:**
By default, acceleration is determined automatically based on the data source in the Splunk Common Information Model (CIM) add-on. The Splunk CIM Add-on is an app that provides common data models for various domains, such as network traffic, web activity, authentication, etc. The CIM Add-on allows you to normalize and enrich your data using predefined fields and tags. The CIM Add-on also allows you to accelerate your data models for faster searches and reports.
Acceleration is a feature that pre-computes summary data for your data models and stores them in tsidx files. Acceleration can improve the performance and efficiency of your searches and reports that use data models.
By default, acceleration is determined automatically based on the data source in the CIM Add-on. This means that Splunk will decide whether to enable or disable acceleration for each data model based on some factors, such as data volume, data type, data model complexity, etc. However, you can also manually enable or disable acceleration for each data model by using the Settings menu or by editing the datamodels.conf file.

**NEW QUESTION 21**
- (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 25**
- (Exam Topic 2)
What is the correct syntax to find events associated with a tag?

A. tag:<field>=<value>
B. tags=<value>
C. tags:<field>=<value>
D. tag=<value>

**Answer:** D

**Explanation:**
The correct syntax to find events associated with a tag in Splunk is tag=<value>1. So, the correct answer is D. tag=<value>. This syntax allows you to annotate specified fields in your search results with tags1.
In Splunk, tags are a type of knowledge object that you can use to add meaningful aliases to field values in your data1. For example, if you have a field called status_code in your data, you might have different status codes like 200, 404, 500, etc. You can create tags for these status codes like success for 200, not_found for 404, and server_error for 500. Then, you can use the tag command in your searches to find events associated with these tags1.
Here is an example of how you can use the tag command in a search: index=main sourcetype=access_combined | tag status_code
In this search, the tag command annotates the status_code field in the search results with the corresponding tags. If you have tagged the status code 200 with success, the status code 404 with not_found, and the status code 500 with server_error, the search results will include these tags1.
You can also use the tag command with a specific tag value to find events associated with that tag. For example, the following search finds all events where the status code is tagged with success:
index=main sourcetype=access_combined | tag status_code | search tag::status_code=success
In this search, the tag command annotates the status_code field with the corresponding tags, and the search command filters the results to include only events where the status_code field is tagged with success1.

**NEW QUESTION 26**
- (Exam Topic 2)
Using the export function, you can export search results as _____ .( Select all that apply)

A. Xml
B. Json
C. Html
D. A php file

**Answer:** AB

**Explanation:**
Using the export function, you can export search results as XML or JSON2. The export function allows you to save your search results in a structured format that can be used by other applications or tools2. You can use the output_mode parameter to specify whether you want to export your results as XML or JSON2. Therefore, options A and B are correct, while options C and D are incorrect because they are not formats that you can export your search results as.

**NEW QUESTION 28**
- (Exam Topic 2)
When using the timechart command, how can a user group the events into buckets based on time?

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

**Answer:** A

**NEW QUESTION 32**
- (Exam Topic 2)
We can use the rename command to _____ (Select all that apply.)

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

**Answer:** D

**NEW QUESTION 35**
- (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, startime, etc.

**NEW QUESTION 40**
- (Exam Topic 2)
Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

A. inputlookup
B. lookup

**Answer:** B

**NEW QUESTION 43**
- (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 46**

- (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 48**
- (Exam Topic 2)
Which statement is true?

A. Pivot is used for creating datasets.
B. Data model are randomly structured datasets.
C. Pivot is used for creating reports and dashboards.
D. In most cases, each Splunk user will create their own data model.

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot
Pivot is used for creating reports and dashboards. Pivot is a tool that allows you to create reports and dashboards from your data models without writing any SPL commands. Pivot can help you visualize and analyze your data using various options, such as filters, rows, columns, cells, charts, tables, maps, etc. Pivot can also help you accelerate your reports and dashboards by using summary data from your accelerated data models.
Pivot is not used for creating datasets or data models. Datasets are collections of events that represent your data in a structured and hierarchical way. Data models are predefined datasets for various domains, such as network traffic, web activity, authentication, etc. Datasets and data models can be created by using commands such as datamodel or pivot.

**NEW QUESTION 49**
- (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 52**
- (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 53**
- (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 57**
- (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 60**
- (Exam Topic 2)
In the Field Extractor, when would the regular expression method be used?

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

**Answer:** C

**Explanation:**
The correct answer is C. When events contain unstructured data.
The regular expression method works best with unstructured event data, such as log files or text messages, where the fields are not separated by a common delimiter, such as a comma or space1. You select a sample event and highlight one or more fields to extract from that event, and the field extractor generates a regular expression that matches similar events in your dataset and extracts the fields from them1. The regular expression method provides several tools for testing and refining the accuracy of the regular expression. It also allows you to manually edit the regular expression1.
The delimiters method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space1. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds1. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats1.
Reference:
1: Build field extractions with the field extractor - Splunk Documentation

**NEW QUESTION 63**
- (Exam Topic 2)

How many ways are there to access the Field Extractor Utility?

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

**Answer:** A

**NEW QUESTION 64**
- (Exam Topic 2)
Which of the following statements about tags is true? (select all that apply.)

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

**Answer:** BD

**Explanation:**
The following statements about tags are true: tags are based on field/value pairs and tags categorize events based on a search. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. Tags can be used to filter or analyze your data based on common concepts or themes. Tags can be created by using various methods, such as search commands, configuration files, user interfaces, etc. Some of the characteristics of tags are:
- Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called “alert” for the field name “status” and the field value “critical”. This means that only events that have status=critical will have the “alert” tag applied to them.
- Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called “web” for the search string sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the “web” tag applied to them.

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

**NEW QUESTION 66**
- (Exam Topic 2)
When creating a data model, which root dataset requires at least one constraint?

A. Root transaction dataset
B. Root event dataset
C. Root child dataset
D. Root search dataset

**Answer:** B

**Explanation:**
The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation1. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

**NEW QUESTION 67**
- (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 72**
- (Exam Topic 2)
In which Settings section are macros defined?

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

**Answer:** C

**NEW QUESTION 73**
- (Exam Topic 2)
When using | timchart by host, which filed is representted in the x-axis?

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

**Answer:** A

**NEW QUESTION 78**
- (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 79**
- (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 83**
- (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 88**
- (Exam Topic 2)
Which command can include both an over and a by clause to divide results into sub-groupings?

A. chart
B. stats
C. xyseries

D. transaction

**Answer:** A

**NEW QUESTION 90**
- (Exam Topic 2)
What is a limitation of searches generated by workflow actions?

A. Searches generated by workflow action cannot use macros.
B. Searches generated by workflow actions must be less than 256 characters long.
C. Searches generated by workflow action must run in the same app as the workflow action.
D. Searches generated by workflow action run with the same permissions as the user running them.

**Answer:** D

**NEW QUESTION 94**
- (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 99**
- (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 100**
- (Exam Topic 2)
What will you learn from the results of the following search? sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

A. The average time elapsed during each transaction for all transactions
B. The average time for each event within each transaction
C. The average time between each transaction

**Answer:** A

**NEW QUESTION 101**
- (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 106**
- (Exam Topic 2)
Which of the following is NOT a stats function:

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

**Answer:** B

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

**NEW QUESTION 111**
- (Exam Topic 2)
Which statement is true?

A. Pivot is used for creating datasets.
B. Data models are randomly structured datasets.
C. Pivot is used for creating reports and dashboards.
D. In most cases, each Splunk user will create their own data model.

**Answer:** C

**Explanation:**
The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

**NEW QUESTION 114**
- (Exam Topic 2)
The stats command will create a _____ by default.

A. Table
B. Report
C. Pie chart

**Answer:** A

**NEW QUESTION 115**
- (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 116**
- (Exam Topic 2)
Use the dedup command to _____.

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

**Answer:** B

**NEW QUESTION 118**
- (Exam Topic 2)
Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

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

**Answer:** D

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

**NEW QUESTION 119**
- (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 121**
- (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 someuniqefield maxspan=1h
In this search, the transaction command groups events that share the same someuniqefield 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 122**
- (Exam Topic 2)
Where are the results of eval commands stored?

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

**Answer:** A

**Explanation:**
https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval
The eval command calculates an expression and puts the resulting value into a search results field.

- If the field name that you specify does not match a field in the output, a new field is added to the search results.
- If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

**NEW QUESTION 126**
- (Exam Topic 2)
Which of the following describes the I transaction command?

A. It is an SPL command that groups at least two events together based on shared values in selected fields.
B. It allows an exchange of data from one Splunk index to another Splunk index.
C. It is an SPL command that groups events together with shared values in selected fields.
D. It allows an exchange of data from one Splunk system to another Splunk system.

**Answer:** C

**Explanation:**
- The transaction command is a Splunk command that finds transactions based on events that meet various constraints .
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member .
- The transaction command groups events together by matching one or more fields that have the same value across the events . For example, | transaction clientip will group events that have the same value the clientip field.

**NEW QUESTION 128**
- (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 131**
.....

# 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