SPLK-1002

Number: SPLK-1002
Passing Score: 800
Time Limit: 120 min
File Version: 1

SPLK-1002

Exam A

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand

QUESTION 2
Which of the following actions can the `eval` command perform?

A. Remove fields from results.
B. Create or replace an existing field.
C. Group transactions by one or more fields.
D. Save SPL commands to be reused in other searches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

When can a pipe follow a macro?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

When using the Field Extractor (FX), which of the following delimiters will work? (Choose all that apply.)

A. Tabs
B. Pipes
C. Colons
D. Spaces

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 5

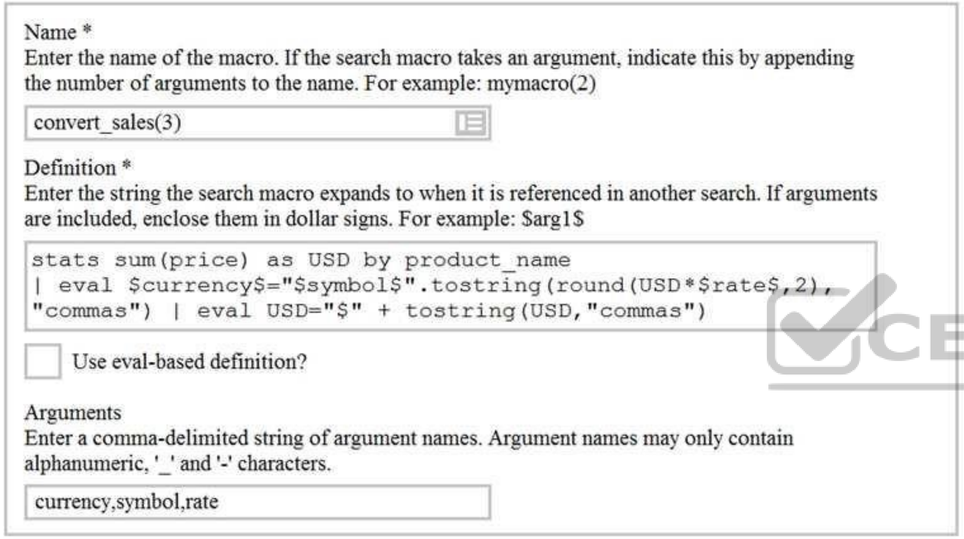
When multiple event types with different color values are assigned to the same event, what determines the color displayed for the event?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtypes

QUESTION 6
Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2),
"commas") | eval USD="$" + tostring(USD,"commas")
```

□ Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

A. `"convert_sales(euro,€,.79)"`

B. `'convert_sales(euro,€,.79)'`

C. `"convert_sales($euro$,$€$,$.79$)"`

D. `'convert_sales($euro$,$€$,$.79$)'`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros

QUESTION 7

There are several ways to access the field extractor.

Which option automatically identifies the data type, source type, and sample event?

A. Event Actions > Extract Fields
B. Fields sidebar > Extract New Fields
C. Settings > Field Extractions > New Field Extraction D. Settings > Field Extractions > Open Field Extractor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.4/Knowledge/Managesearch-timefieldextractions

QUESTION 8

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

A. `stats` can only group events using IP addresses.
B. The `transaction` command is faster and more efficient.
C. There is a 1000 event limitation with the `transaction` command.
D. Use `stats` when the events need to be viewed as a single correlated event.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 9

Which of the following statements describe the Common Information Model (CIM)? (Choose 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.

Correct Answer: ABD
Section: (none)
Explanation

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

QUESTION 10
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Splexicon:Calculatedfield

QUESTION 11
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Eval

QUESTION 12

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

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

Correct Answer: ABD
Section: (none)
Explanation

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

QUESTION 13

Calculated fields can be based on which of the following?

A. Tags
B. Extracted fields
C. Output fields for a lookup
D. Fields generated from a search string

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 14

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.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 15
When using `| timechart by host`, which field is represented in the x-axis?

A. `date`
B. `host`
C. `time`
D. `_time`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart

QUESTION 16
Which of the following searches will return events containing a tag named **Privileged**?

A. tag=Priv
B. tag=Priv*
C. tag=priv*
D. tag=privileged

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

QUESTION 17

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`

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html

QUESTION 18
A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, the `eval` or the `sort`?

A. It doesn't matter whether `eval` or `sort` is used first.
B. Convert the numeric to a string with `eval` first, then `sort`.
C. Use `sort` first, then convert the numeric to a string with `eval`.
D. You cannot use the `sort` command and the `eval` command on the same field.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which Knowledge Object does the Splunk Common Information Model (CIM) use to normalize data, in addition to field aliases, event types, and tags?

A. Macros
B. Lookups
C. Workflow actions

D. Field extractions

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

QUESTION 20
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
If no value is specified with the `fillnull` command, what default value will be used?

A. 0
B. N/A
C. –D. NULL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specfying-a-field.html

QUESTION 22

What are the two parts of a root event dataset?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects

QUESTION 23

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

A. 0, because timechart doesn't support using a by clause.
B. 1, because _time is already implied as the x-axis.
C. 2, because one field would represent the x-axis and the other would represent the y-axis.
D. There is no limit specific to timechart.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

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

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge

QUESTION 25
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 the 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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 26
When creating a Search workflow action, which field is required?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction

QUESTION 27
To identify all of the contributing events within a transaction that contain at least one `REJECT` event, which syntax is correct?

A. `index=main REJECT | transaction sessionid`

B. `index=main | transaction sessionid | search REJECT`

C. `index=main | transaction sessionid | where transaction=reject`

D. `index=main | transaction sessionid | where transaction="REJECT*"`

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 28
Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.
B. POST workflow actions can be configured to send email to the URI location.
C. By default, POST workflow actions are shown in both the event and field menus.
D. POST workflow actions can be configured to send POST arguments to the URI location.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaPOSTworkflowaction

QUESTION 29
Which of the following statements about event types is true? (Choose all that apply.)

A. Event types can be tagged.
B. Event types must include a time range.
C. Event types categorize events based on a search.
D. Event types can be a useful method for capturing and sharing knowledge.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.edureka.co/blog/splunk-events-event-types-and-tags/

QUESTION 30
The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization.

If another person in the organization runs the shared report and no results are returned, why might this be? (Choose all that apply.)
A. Fast mode is enabled.
B. The dashboard is private.
C. The extraction is private.
D. The person in the organization running the report does not have access to the index.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following statements describe the search string below?

```
| datamodel Application_State All_Application_State search
```

A. Events will be returned from dataset named `Application_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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

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

A. `tag=<field>`

B. `tag=<field>(<tagname>)`

C. `tag=<field>::<tagname>`

D. `tag::<field>=<tagname>`

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 33
Which workflow uses field values to perform a secondary search?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/CreateworkflowactionsinSplunkWeb

QUESTION 34
Which of the following statements describes the use of the Field Extractor (FX)?

A. The Field Extractor automatically extracts all fields at search time.
B. The Field Extractor uses PERL to extract fields from the raw events.
C. Fields extracted using the Field Extractor persist as knowledge objects.
D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following searches would return a report of `sales` by `product_name`?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://hilllaneconsulting.co.uk/blog/?p=640

QUESTION 36
Which of the following data models are included in the Splunk Common Information Model (CIM) add-on? (Choose all that apply.)

A. Alerts
B. Email
C. Databases
D. User permissions

Correct Answer: ABC
Section: (none)
Explanation

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

QUESTION 37

What is a limitation of searches generated by workflow actions?

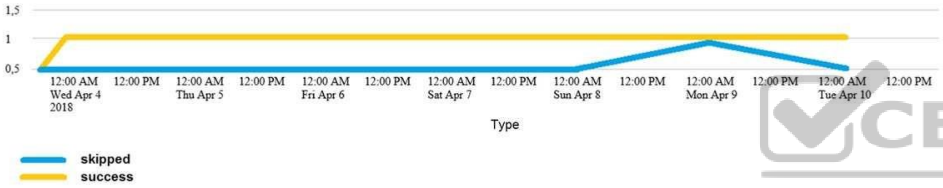
A. Searches generated by workflow actions cannot use macros.
B. Searches generated by workflow actions must be less than 256 characters long.
C. Searches generated by workflow actions must run in the same app as the workflow action.
D. Searches generated by workflow actions run with the same permissions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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38

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



A. `index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=1d | stats count by status`
B. `index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=1d | chart count OVER status by _time`
C. `index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status`
D. None of these searches would generate a similar graph.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

None of these functions related to the graph in exhibit. All of these functions have maxspan=ld which is not a valid argument.

QUESTION 39

What is the relationship between data models and pivots?

A. Data models provide the datasets for pivots.
B. Pivots and data models have no relationship.
C. Pivots and data models are the same thing.
D. Pivots provide the datasets for data models.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 40

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41

Which of the following statements about data models and pivot are true? (Choose 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Data model fields can be added using the Auto-Extracted method.

Which of the following statements describe Auto-Extracted fields? (Choose all that apply.)
A. Auto-Extracted fields can be hidden in Pivot.
B. Auto-Extracted fields can have their data type changed.
C. Auto-Extracted fields can be given a friendly name for use in Pivot.
D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is a function of the Splunk Common Information Model (CIM)?

A. Normalizing data across a Splunk deployment.
B. Providing templates for reports and dashboards.
C. Algorithmically shifting events to other indexes.
D. Reingesting previously indexed data with new field names.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/CIM/4.18.0/User/Overview

QUESTION 44

What information must be included when using the `datamodel` command?

A. `status` field
B. Multiple indexes
C. Data model field name.
D. Data model dataset name.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/Datamodel

QUESTION 45
A data model can consist of what three types of datasets?

A. Pivot, searches, and events.
B. Pivot, events, and transactions.
C. Searches, transactions, and pivot.
D. Events, searches, and transactions.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Splexicon:Datamodeldataset

QUESTION 46
Which of the following statements describe GET workflow actions?

A. GET workflow actions must be configured with POST arguments.
B. Configuration of GET workflow actions includes choosing a sourcetype.
C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
D. GET workflow actions can be configured to open the URI link in the current window or in a new window.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaGETworkflowaction

QUESTION 47
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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/search-commands-stats-chart-and-timechart.html

QUESTION 48
When should you use the `transaction` command instead of the `stats` command?

A. When you need to group on multiple values.
B. When duration is irrelevant in search results.
C. When you have over 1000 events in a transaction.
D. When you need to group based on start and end constraints.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/book-excerpt-when-to-use-transaction-and-when-to-use-stats.html

QUESTION 49

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/CIM/4.18.0/User/Overview

QUESTION 50
Which of the following statements about tags is true?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following file formats can be extracted using a delimiter field extraction?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Extractfieldsfromfileswithstructureddata

QUESTION 52
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following are required to create a POST workflow action?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaPOSTworkflowaction