SPLK-1002.VCEplus.premium.exam.65q

Number: SPLK-1002
Passing Score: 800
Time Limit: 120 min
File Version: 2.0

SPLK-1002

Splunk Core Certified Power User

Version 2.0

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: C
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: A
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 Data models are composed of one or more of which of the following datasets? (Choose all that apply.)

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

Correct Answer: ABC

Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

QUESTION 5 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 6 Which group of users would most likely use pivots?

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

Correct Answer: D
Section: (none)
Explanation

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

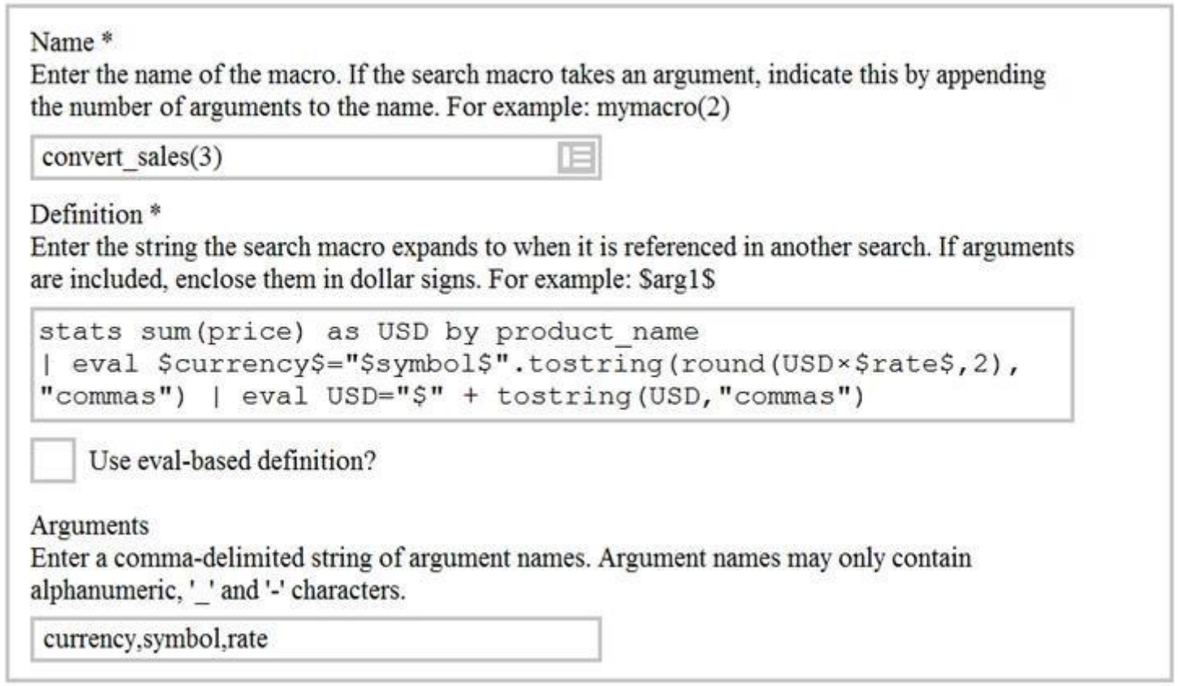
QUESTION 7 When multiple event types with different color values are assigned to the same event, what determines the color displayed for the event?

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 8
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($euro$,$€$,$.79$)"`
D. `'convert_sales($euro$,$€$,$.79$)'`

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 9 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 ExtractionD. Settings > Field Extractions > Open Field Extractor

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 10
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 11 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 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: AB
Section: (none)
Explanation

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

QUESTION 13 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 14 What do events in a transaction have in common?

A. All events in a transaction must have the same timestamp.
B. All events in a transaction must have the same sourcetype.
C. All events in a transaction must have the exact same set of fields.
D. All events in a transaction must be related by one or more fields.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 15 Which delimiters can the Field Extractor (FX) detect? (Choose all that apply.)

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

Correct Answer: BCD
Section: (none)
Explanation

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

QUESTION 16 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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 17
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 18 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: BD
Section: (none)
Explanation

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

QUESTION 19 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 20
When should `transaction` be used?

A. Only in a large distributed Splunk environment.
B. When calculating results from one or more fields.
C. When event grouping is based on start/end values.
D. When grouping events results in over 1000 events in each group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Abouttransactions

QUESTION 21 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: C
Section: (none)

Explanation
Explanation/Reference:

QUESTION 22 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 23 Which of the following is the correct way to use the `datamodel` command to search fields in the `Web` data model within the `Web` dataset?

A. `| datamodel Web Web search | fields Web*`
B. `| search datamodel Web Web | fields Web*`
C. `| datamodel Web Web fields | search Web*`
D. `datamodel=Web | search Web | fields Web*`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24 Which of the following statements describe the command below? (Choose all that apply.)

```
sourcetype=access_combined | transaction JSESSIONID
```

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

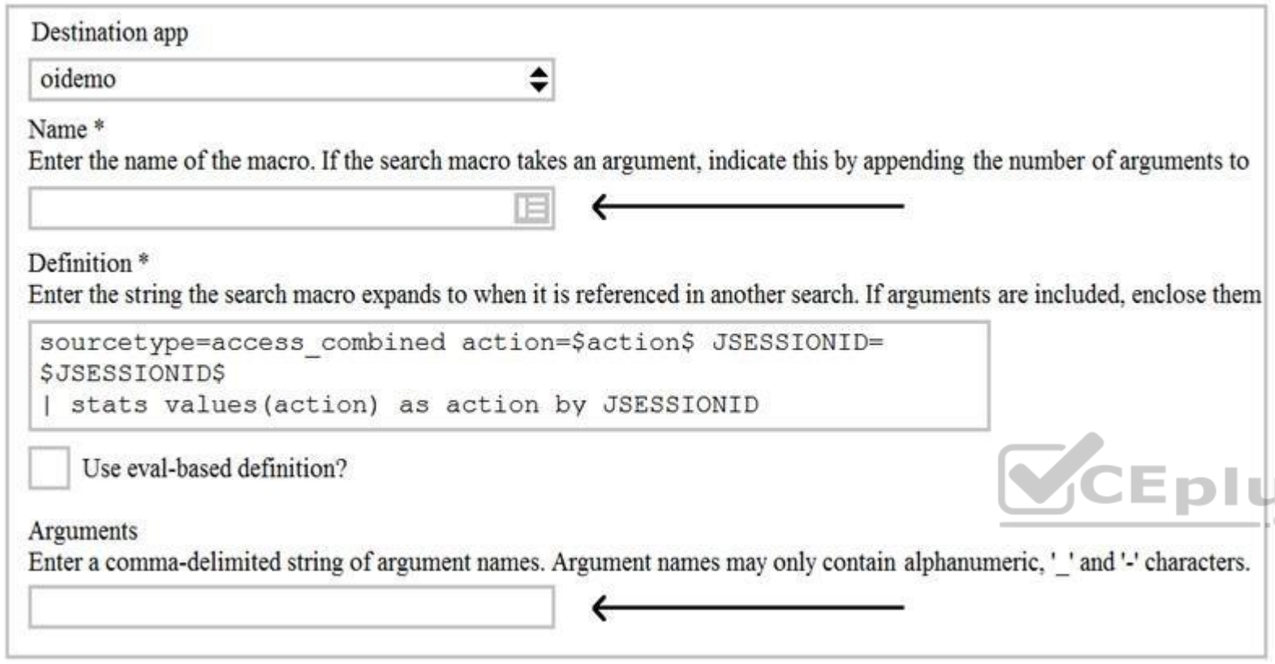
QUESTION 25 Which of the following searches will return events containing a tag named **Privileged**?

A. tag=Priv
B. tag=Priv*

C. tag=priv*
D. tag=privileged
Correct Answer: D
Section: (none)
Explanation

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

QUESTION 26
Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configure the macro?



A. The macro name is `sessiontracker` and the arguments are `action, JESSIONID`.
B. The macro name is `sessiontracker(2)` and the arguments are `action, JESSIONID`.
C. The macro name is `sessiontracker` and the arguments are `$action$, $JESSIONID$`.
D. The macro name is `sessiontracker(2)` and the Arguments are `$action$, $JESSIONID$`.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 27 What is required for a macro to accept three arguments?

A. The macro's name ends with (3).
B. The macro's name starts with (3).
C. The macro's argument count setting is 3 or more.
D. Nothing, all macros can accept any number of arguments.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 Which workflow action method can be used when the action type is set to link?

A. GET
B. PUT
C. Search
D. UPDATE

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 29 Which of the following statements about tags is true? (Choose 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 Which of the following statements about macros is true? (Choose 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 Information needed to create a GET workflow action includes which of the following? (Choose all that apply.)

A. A name for the workflow action.
B. A URI where the user will be directed at search time.
C. A label that will appear in the Event Action menu at search time.

D. A name for the URI where the user will be directed at search time.

Correct Answer: BC
Section: (none)
Explanation

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

QUESTION 32 Which of the following can be used with the `eval` command `tostring` function? (Choose all that apply.)

A. `"hex"`
B. `"commas"`
C. `"decimal"`
D. `"duration"`

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://splunkonbigdata.com/2018/10/27/usage-of-splunk-eval-function-tostring/

QUESTION 33 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 34 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 35

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: B
Section: (none)
Explanation

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

QUESTION 36 Which of the following statements describe data model acceleration? (Choose all that apply.)

A. Root events cannot be accelerated.
B. Accelerated data models cannot be edited.
C. Private data models cannot be accelerated.
D. You must have administrative permissions or the `accelerate_datamodel` capability to accelerate a data model.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37 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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 What does the `fillnull` command replace null values with, if the value argument is not specified?

A. 0
B. N/A
C. NaN
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 39
What other syntax will produce exactly the same results as `| chart count over vendor_action by user`?

A. `| chart count by vendor_action, user`
B. `| chart count over vendor_action, user`
C. `| chart count by vendor_action over user`
D. `| chart count over user by vendor_action`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 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 41 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: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://books.google.com.pk/books?id=7TlECgAAQBAJ&pg=PA72&lpg=PA72&dq=splunk++timechart+how+many+fields+can+be+listed+after+a+by+clause&source=bl&ots=tdFvZfVkFE&sig=ACfU3U21ouOoL1ImlpUPtxysBhJ6bWakSA&hl=en&sa=X&ved=2ahUKEwiY4YXXn9fpAhWlsXEKHf8TD6YQ6AEwEHoECBUQAQ#v=onepage&q=splunk%20%20timechart%20how%20many%20fields%20can%20be%20listed%20after%20a%20by%20clause&f=false

QUESTION 42
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43 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.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 44 In what order are the following knowledge objects/configurations applied?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 45 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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 46
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 47 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 48 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 49 After manually editing a regular expression (regex), which of the following statements is true?

A. Changes made manually can be reverted in the Field Extractor (FX) UI.
B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 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: C
Section: (none)
Explanation

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

QUESTION 51 Which of the following statements is true, especially in large environments?

A. Use the `stats` command when you need to group events by two or more fields.
B. The `stats` command is faster and more efficient than the `transaction` command.
C. The `transaction` command is faster and more efficient than the `stats` command.
D. Use the `transaction` command when you want to see the results of a calculation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html

QUESTION 52 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 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 54
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 55 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 56 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 57 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`

Correct Answer: B

Section: (none)
Explanation
Explanation/Reference:
Reference: https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html

QUESTION 58 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 59 Which of the following statements describes field aliases?

A. Field alias names replace the original field name.
B. Field aliases can be used in lookup file definitions.
C. Field aliases only normalize data across sources and sourcetypes.
D. Field alias names are not case sensitive when used as part of a search.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 61 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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 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 63 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: AB
Section: (none)
Explanation

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

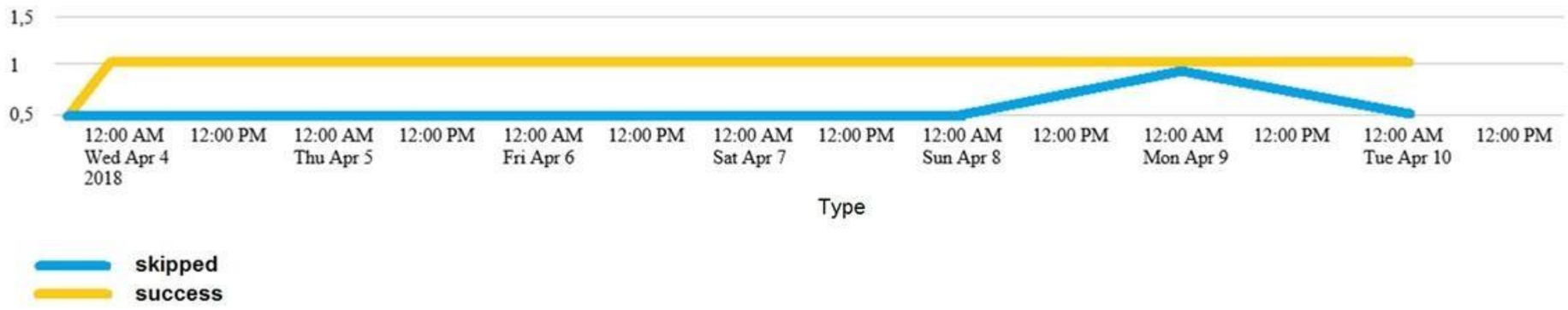
QUESTION 64 What is a limitation of searches generated by workflow actions?

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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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=ld | stats count by status`

B. `index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=ld | chart count OVER status by _time`

C. `index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=ld | 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.