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.

https://vceplus.com/ 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
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

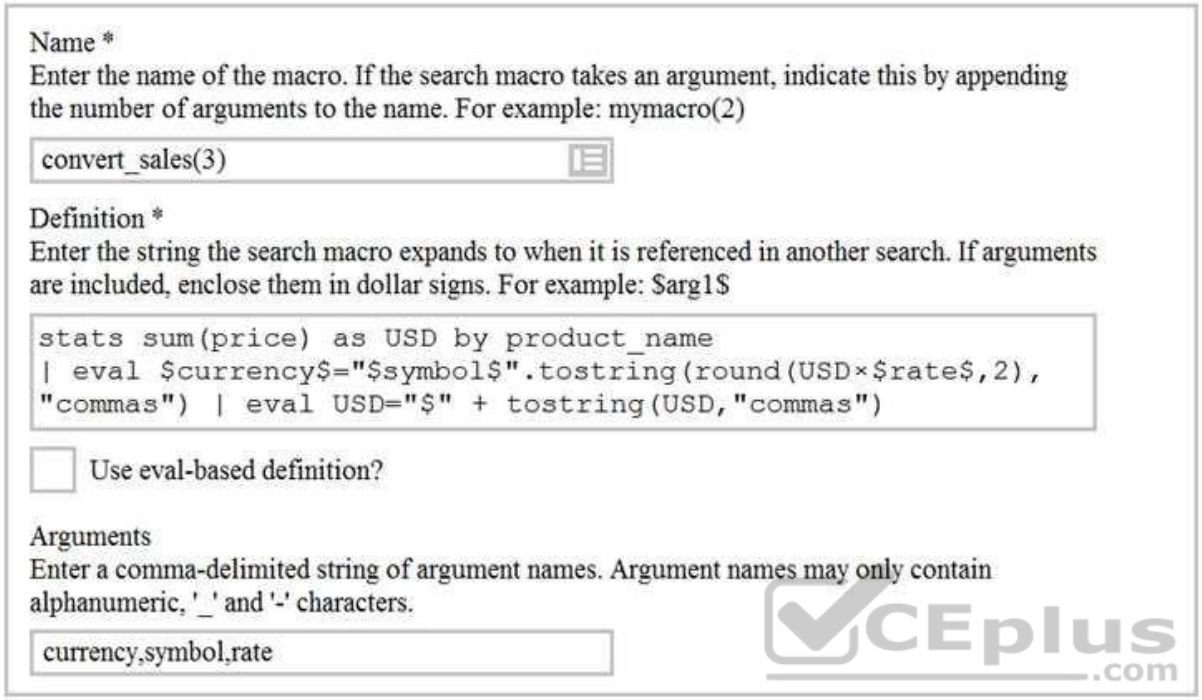
QUESTION 3
Which group of users would most likely use pivots?

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 4
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 5
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: C
Section: (none)
Explanation

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

QUESTION 6
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 7
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 8
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 9
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 10

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 11
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 12
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 13
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 14
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 15**
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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