Free Questions for SPLK-1002 by certsdeals

Shared by Vance on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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.

Answer:

C

Question 2

Question Type: MultipleChoice

Which of the following searches show a valid use of a macro? (Choose all that apply.)

Options:

A- index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField

B- index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField

C- index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField

D- index=main source=mySource oldField=* | ''newField('makeMyField(oldField)')'' | table _time newField

Answer:

A, C

Question 3

Question Type: **MultipleChoice**

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

Options:

A- monthly_sales(argument 1, argument 2, argument 3)

B- monthly_sales(3)

C- monthly_sales[3]

D- monthly_sales[argument 1, argument 2, argument 3)

Answer:

C

Question 4

Question Type: MultipleChoice

What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

Options:

A- There is a limit to the number of fields that can be extracted.

B- The user is unable to preview the extractions.

C- The extraction is added at index time.

D- The user is unable to return to the automatic field extraction workflow.

Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following is one of the pre-configured data models included in the Splunk Common Information Model (CIM) add-on?

Options:

A- Access

B- Accounting

C- Authorization

D- Authentication

Answer:

D

Question 6

Question Type: MultipleChoice

Which of the following statements describes calculated fields?

Options:

A- Calculated fields are only used on fields added by lookups.

B- Calculated fields are a shortcut for repetitive and complex eval commands.

C- Calculated fields are a shortcut for repetitive and complex calc commands.

D- Calculated fields automatically calculate the simple moving average for indexed fields.

Answer:

B

Question 7

Question Type: MultipleChoice

In which Settings section are macros defined?

Options:

A- Fields

B- Tokens

C- Advanced Search

D- Searches, Reports, Alerts

Answer:

C

Question 8

Question Type: MultipleChoice

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")

Options:

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.
https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions

Answer:

A