Vendor: Splunk

Exam Code: SPLK-1002

Exam Name: Splunk Core Certified Power User Exam

Version: Demo

QUESTION 1
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: D

QUESTION 2
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"

Correct Answer: ABD

QUESTION 3
Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

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

Correct Answer: ABC

QUESTION 4
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

QUESTION 5
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>

Correct Answer: D

QUESTION 6
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

QUESTION 7
What does the transaction command do?

A. Groups a set of transactions based on time.
B. Creates a single event from a group of events.
C. Separates two events based on one or more values.
D. Returns the number of credit card transactions found in the event logs.

Correct Answer: B

QUESTION 8
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: : <fieldneme>

Correct Answer: C

QUESTION 9
What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

A. Macros.
B. Field aliases.
C. The rename command.
D. CIM does not work with different names for the same field.

Correct Answer: B

QUESTION 10
Which of the following statements describes this search?

sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

A. This is a valid search and will display a timechart of the average duration, of each transaction event.
B. This is a valid search and will display a stats table showing the maximum pause among transactions.
C. No results will be returned because the transaction command must include the startswith and endswith options.

D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Correct Answer: A

QUESTION 11
A space is an implied _____ in a search string.

A. OR
B. AND
C. ()
D. NOT

Correct Answer: B

QUESTION 12
Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select 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: ABCD

QUESTION 13
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

QUESTION 14
Data model are composed of one or more of which of the following datasets? (select all that apply.)

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

Correct Answer: ABC

QUESTION 15
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: A

QUESTION 16
Which of the following statements describes POST workflow actions?

A. POST workflow actions are always encrypted.
B. POST workflow actions cannot use field values in their URI.
C. POST workflow actions cannot be created on custom sourcetypes.
D. POST workflow actions can open a web page in either the same window or a new .

Correct Answer: D

QUESTION 17
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

QUESTION 18
Which of the following eval command function is valid?

A. Int ()
B. Count ( )
C. Print ()
D. Tostring ()

Correct Answer: D

QUESTION 19
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: C

QUESTION 20
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?