Splunk

Exam SPLK-1002

Splunk Core Certified Power User Exam

Version: 13.0

[Total Questions: 181]

Topic break down

Topic	No. of Questions
Topic 1: Questions Set 1	65
Topic 2: Questions Set 2	116

Topic 1, Questions Set 1

Question No : 1 - (Topic 1)

Which of the following statements describe calculated fields? (select 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.

Answer: A,B,D
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

Question No : 2 - (Topic 1)

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>

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

Question No : 3 - (Topic 1)

Which of the following statements describes the command below (select all that apply)

Sourcetype=access_combined | transaction JSESSIONID

A. An additional filed 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.

Answer: B,C,D

Question No : 4 - (Topic 1)

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 URT link in the current window or in a new window

Answer: D

Question No : 5 - (Topic 1)

Which of the following searches will return events contains a tag name Privileged?

A. Tag= Priv
B. Tag= Pri*
C. Tag= Priv*
D. Tag= Privileged

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

Question No : 6 - (Topic 1)

Which group of users would most likely use pivots?

A. Users
B. Architects

C. Administrators
D. Knowledge Managers

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

Question No : 7 - (Topic 1)

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.

Answer: D

Question No : 8 - (Topic 1)

What does the fillnull command replace null values with, it the value argument is not specified?

A. 0
B. N/A
C. NaN
D. NULL

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

Question No : 9 - (Topic 1)

A calculated field maybe based on which of the following?

A. Lookup tables
B. Extracted fields
C. Regular expressions
D. Fields generated within a search string

Answer: B

Question No : 10 - (Topic 1)

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.

Answer: B

Question No : 11 - (Topic 1)

Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search

A. Evenrches would return a report of sales by 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

Answer: B

Question No : 12 - (Topic 1)

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.

Answer: A

Question No : 13 - (Topic 1)

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

Answer: A,B,C
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

Question No : 14 - (Topic 1)

Which of the following Statements about macros is true? (select 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.

Answer: B,C

Question No : 15 - (Topic 1)

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.

Answer: B

Question No : 16 - (Topic 1)

When should you use the transaction command instead of the scats 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.

Answer: D

Question No : 17 - (Topic 1)

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

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

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

Question No : 18 - (Topic 1)

Selected fields are displayed _____each event in the search results.

A. below
B. interesting fields
C. other fields
D. above

Answer: A

Question No : 19 - (Topic 1)

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.

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

Question No : 20 - (Topic 1)

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’’

Answer: A,B,D
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.29

Question No : 21 - (Topic 1)

Which of the following statements about event types is true? (select 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.

Answer: A,C,D
Reference: https://www.edureka.co/blog/splunk-events-event-types-and-tags/

Question No : 22 - (Topic 1)

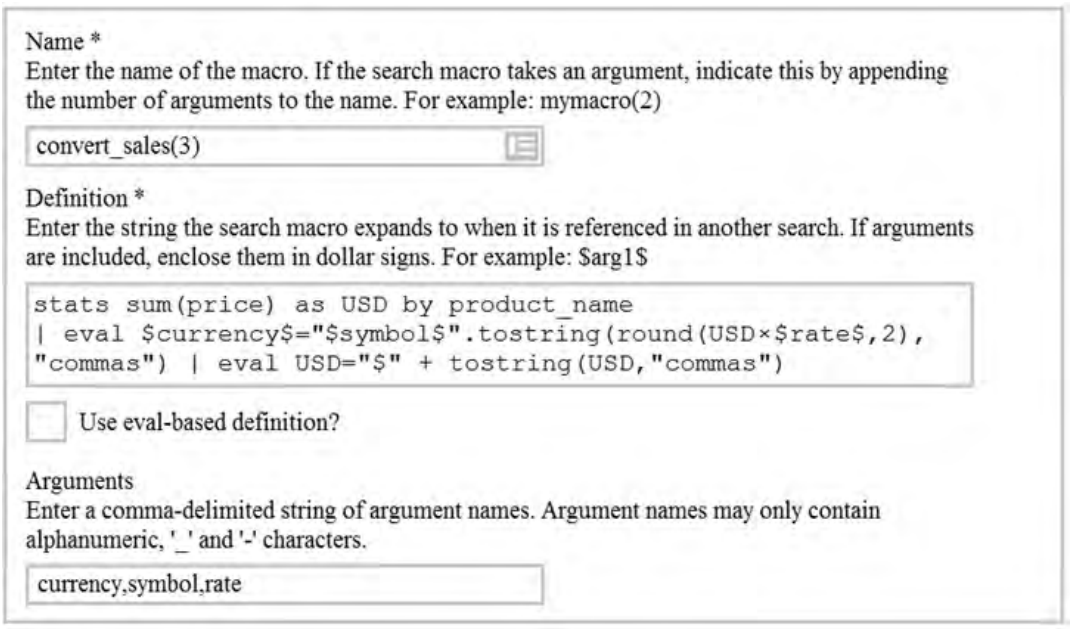
Which are valid ways to create an event type? (select all that apply)

A. By using the searchtypes command in the search bar.
B. By editing the event_type stanza in the props.conf file.
C. By going to the Settings menu and clicking Event Types > New.
D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Answer: C,D

Question No : 23 - (Topic 1)

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 ($euro,$€$,s79$
D. Convert_sales ($euro, $€$,S,79$)

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

Question No : 24 - (Topic 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.

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