DUMPSGATE

Splunk

SPLK-1002

Splunk Core Certified Power User

QUESTION & ANSWERS

QUESTION 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

Correct Answer: A

QUESTION 2

In what order arc the following knowledge objects/configurations applied?

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

Correct Answer: B

QUESTION 3

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

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

Correct Answer: D

QUESTION 4

Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

A. maxpause
B. endswith

C. maxduration
D. maxspan

Correct Answer: D

QUESTION 5

Alert throttling is used to______.

A. verify each alert
B. stagger search request in a time sequenced order
C. stop spamming yourself with alerts
D. check severity

Correct Answer: C

QUESTION 6

Which of the following are required to create a POST workflow action?

A. Label, URI, search string.
B. XMl attributes, URI, name.
C. Label, URI, post arguments.
D. URI, search string, time range picker.

Correct Answer: B

QUESTION 7

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

A. | datamodel web search | filed web *
B. | Search datamodel web web | filed web*
C. | datamodel web web field | search web*
D. Datamodel=web | search web | filed web*

Correct Answer: A

QUESTION 8

Which of the following statements about data models and pivot are true? (select all that apply)

A. They are both knowledge objects.
B. Data models are created out of datasets called pivots.
C. Pivot requires users to input SPL searches on data models.
D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Correct Answer:B,D

QUESTION 9

Which of the following statements describe the Common Information Model (QM)? (select 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: A,C

QUESTION 10

The eval command 'if' function requires the following three arguments (in order):

A. Boolean expression, result if true, result if false
B. Result if true, result if false, boolean expression
C. Result if false, result if true, boolean expression
D. Boolean expression, result if false, result if true

Correct Answer: A

QUESTION 11

Clicking a SEGMENT on a chart,_______.

A. drills down for that value
B. highlights the field value across the chart
C. adds the highlighted value to the search criteria

Correct Answer: C

QUESTION 12

Which of the following statements describe the search below? (select all that apply)
Index=main I transaction clientip host maxspan=30s maxpause=5s

A. Events in the transaction occurred within 5 seconds.
B. It groups events that share the same clientip and host.
C. The first and last events are no more than 5 seconds apart.
D. The first and last events are no more than 30 seconds apart.

Correct Answer: B

QUESTION 13

What is the correct way to name a macro with two arguments?

A. us_sales2
B. us_sales(1,2)
C. us_sale,2
D. us_sales(2)

Correct Answer: D

QUESTION 14

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 15

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 Held 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: B,C,D