Correct Answer: B

QUESTION 45
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.

Correct Answer: ACD

QUESTION 46
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.

Correct Answer: C

QUESTION 47
Which of the following workflow actions can be executed from search results? (select all that apply)

A. GET
B. POST
C. LOOKUP
D. Search

Correct Answer: ABD

QUESTION 48
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 49
A user wants to convert numeric field values to strings and also to sort on those values. Which command should be used first, the eval or the sort?

A. It doesn't matter whether eval or sort is used first.
B. Convert the numeric to a string with eval first, then sort.
C. Use sort first, then convert the numeric to a string with eval.

D. You cannot use the sort command and the eval command on the same field.

Correct Answer: C

QUESTION 50
Which of the following statements describes field aliases?

A. Field alias names replace the original field name.
B. Field aliases can be used in lookup file definitions.
C. Field aliases only normalize data across sources and sourcetypes.
D. Field alias names are not case sensitive when used as part of a search.

Correct Answer: B

QUESTION 51
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.
Correct Answer: CD

QUESTION 52
Which of the following statements describe data model acceleration? (select 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_dacamodel capability to accelerate a data model.

Correct Answer: BCD

QUESTION 53
Which of the following statements describe the Common Information Model (CIM)? (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: ABC

QUESTION 54
Selected fields are displayed _____each event in the search results.

A. below
B. interesting fields
C. other fields

D. above

Correct Answer: A

QUESTION 55
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

Correct Answer: B

QUESTION 56
When creating a Search workflow action, which field is required?

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

Correct Answer: A

QUESTION 57
When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

A. Tabs
B. Pipes
C. Colons
D. Spaces

Correct Answer: ABD

QUESTION 58
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

Correct Answer: D

QUESTION 59
Calculated fields can be based on which of the following?

A. Tags
B. Extracted fields

C. Output fields for a lookup
D. Fields generated from a search string

Correct Answer: B

QUESTION 60
Which of the following searches will show the number of categoryId used by each host?

A. Sourcetype=access_* |sum bytes by host
B. Sourcetype=access_* |stats sum(categorylD. by host
C. Sourcetype=access_* |sum(bytes) by host
D. Sourcetype=access_* |stats sum by host

Correct Answer: B

QUESTION 61
Which of the following is a function of the Splunk Common Information Model (CIM)?

A. Normalizing data across a Splunk deployment.
B. Providing templates for reports and dashboards.
C. Algorithmically shifting events to other indexes.
D. Reingesting previously indexed data with new field names.

Correct Answer: A

QUESTION 62
When using the transaction command, what does the argument maxspan do?

A. Sets the maximum total time between events in a transaction.
B. Sets the maximum length of all events within a transaction.
C. Sets the maximum total time between the earliest and latest events in a transaction.
D. Sets the maximum length that any single event can reach to be included in the transaction.

Correct Answer: C

QUESTION 63
Which command can include both an over and a by clause to divide results into sub-groupings?

A. chart
B. stats
C. xyseries
D. transaction

Correct Answer: A

QUESTION 64
which of the following commands are used when creating visualizations(select all that apply.)

A. Geom
B. Choropleth
C. Geostats

D. iplocation

Correct Answer: ACD

QUESTION 65
which of the following are valid options with the chart command

A. useother
B. usenull
C. fillfield
D. usefiled

Correct Answer: AB
QUESTION 66
This is what Splunk uses to categorize the data that is being indexed.

A. sourcetype
B. index
C. source
D. host

Correct Answer: A

QUESTION 67
Field aliases are used to _____ data

A. clean
B. transform
C. calculate
D. normalize

Correct Answer: D

QUESTION 68
Which of the following are valid options to speed up reports? (Select all the apply.)

A. Edit permissions
B. Edit description
C. Edit acceleration
D. Edit schedule

Correct Answer: C

QUESTION 69
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: C