These allow you to categorize events based on search terms. Select your answer.

A. Groups
B. Event Types
C. Macros
D. Tags

Correct Answer: B

QUESTION 145
Which of the following commands support the same set of functions?

A. stats, eval, table
B. search, where, eval
C. stats, chart, timechart
D. transaction, chart, timechart

Correct Answer: C

QUESTION 146
For choropleth maps,splunk ships with the following KMZ files (select all that apply)

A. States of the United States
B. States and provinces of the united states and Canada
C. Countries of the European Union
D. Countries of the World

Correct Answer: AD

QUESTION 147
Which of the following searches would return a report of sales by product-name?

A. chart sales by product_name
B. chart sum(price) as sales by product_name
C. stats sum(price) as sales over product_name
D. timechart list(sales), values(product_name)

Correct Answer: B

QUESTION 148
By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?

A. Turned off
B. Turned on
C. Determined automatically based on the sourcetype.
D. Determined automatically based on the data source.

Correct Answer: D

QUESTION 149

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