Exam : **SPK-102**

Title : Splunk Core Certified Power User

Version : DEMO

1.When should the regular expression mode of Field Extractor (FX) be used? (select all that apply)
A. For data cleanly separated by a space, a comma, or a pipe character.
B. For data in a CSV (comma-separated value) file.
C. For data with multiple, different characters separating fields.
D. For unstructured data.
Answer: C, D
Explanation:
The regular expression mode of Field Extractor (FX) should be used for data with multiple, different characters separating fields or for unstructured data. The regular expression mode allows you to select a sample event and highlight the fields that you want to extract, and the field extractor generates a regular expression that matches similar events and extracts the fields from them.
References See Build field extractions with the field extractor - Splunk Documentation and Field Extractor: Select Method step - Splunk Documentation.

2.A user wants a table that will show the total revenue made for each product in each sales region. Which would be the correct SPL query to use?
A. index=X source type=Y | chart sum(product) by price AND region
B. index=X | chart sum(price) by product, region
C. index=X | chart total(product) over price by region
D. index=X | chart total(price) by product, region
Answer: B
Explanation:
The chart command with sum(price) by product, region will return a table where the total revenue (price) is aggregated (sum) for each product and sales region. This is the correct way to aggregate data in Splunk.
References:
Splunk Docs - chart command

3. The limit attribute will_____.
A. override default of 10
B. only work with top command
C. override default of 20
D. override default of 15
Answer: A

4.Which of the following does not describe how to create an event type?
A. Run a search string and use the Save As button.
B. Use the New Event Type button from the Settings menu.
C. Use the Field Extractor to analyze and use the Save As button.
D. Select search criteria within the Event Type Builder.
Answer: C
Explanation:
Event types are created from searches, not field extraction.
Extract: “You can create event types by running a search and saving it as an event type, or by using

Settings > Event types > New Event Type.”
The Field Extractor is used for field extractions, not for creating event types.
Therefore, optionCis correct.

5.This is what Splunk uses to categorize the data that is being indexed.
A. source type
B. index
C. source
D. host
Answer: A