QUESTION 70
Complete the search, ... | _____ failure>successes

A. Search
B. Where
C. If
D. Any of the above

Correct Answer: B
QUESTION 71
These kinds of charts represent a series in a single bar with multiple sections

A. Multi-Series
B. Split-Series
C. Omit nulls
D. Stacked

Correct Answer: D

QUESTION 72
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 73
Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.
B. POST workflow actions can be configured to send email to the URI location.
C. By default, POST workflow action are shown in both the event and field menus.
D. POST workflow actions can be configured to send POST arguments to the URI location.

Correct Answer: D

QUESTION 74
Information needed to create a GET workflow action includes which of the following? (select all that apply.)

A. A name of the workflow action
B. A URI where the user will be directed at search time.
C. A label that will appear in the Event Action menu at search time.
D. A name for the URI where the user will be directed at search time.

Correct Answer: ABC

QUESTION 75
In most large Splunk environments, what is the most efficient command that can be used to group events by fields/

A. join
B. stats
C. streamstats
D. transaction
Correct Answer: B

QUESTION 76
Which of the following is NOT a stats function:

A. sum
B. addtotals
C. count
D. avg

Correct Answer: B

QUESTION 77
Which statement is true?

A. Pivot is used for creating datasets.
B. Data model are randomly structured datasets.
C. Pivot is used for creating reports and dashboards.
D. In most cases, each Splunk user will create their own data model.

Correct Answer: C

QUESTION 78
What information must be included when using the datamodel command?

A. status field
B. Multiple indexes
C. Data model field name.
D. Data model dataset name.

Correct Answer: D

QUESTION 79
We can use the rename command to _____ (Select all that apply.)

A. Change indexed fields
B. Exclude fields from our search results
C. Extract new fields from our data using regular expressions
D. Give a field a new name at search time

Correct Answer: D

QUESTION 80

What is the Splunk Common Information Model (CIM)?

A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.
B. The CIM provides a methodology to normalize data from different sources and source types.
C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.
D. The CIM is a data exchange initiative between software vendors.

Correct Answer: B

QUESTION 81
This function of the stats command allows you to return the sample standard deviation of a field.

A. stdev
B. dev
C. count deviation
D. by standarddev

Correct Answer: A

QUESTION 82
By default search results are not returned in ________ order.

A. Chronological
B. Reverser chronological
C. ASCIE
D. Alphabetical

Correct Answer: AD

QUESTION 83
Which of the following statements describes the use of the Field Extractor (FX)?

A. The Field Extractor automatically extracts all fields at search time.
B. The Field Extractor uses PERL to extract fields from the raw events.
C. Fields extracted using the Field Extractor persist as knowledge objects.
D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Correct Answer: C

QUESTION 84
When using | timechart by host, which field is represented in the x-axis?

A. date
B. host
C. time
D. _time

Correct Answer: D

QUESTION 85

If a search returns ____________ it can be viewed as a chart.

A. timestamps
B. statistics
C. events
D. keywords

Correct Answer: B

QUESTION 86
Data models are composed of one or more of which of the following datasets? (select all that apply)

A. Transaction datasets
B. Events datasets
C. Search datasets
D. Any child of event, transaction, and search datasets

Correct Answer: ABC

QUESTION 87
Which of the following are valid options with the chart command ?(select all that apply)

A. usenull=f
B. useother=f
C. split=t
D. transcation=t

Correct Answer: AB

QUESTION 88
__________ datasets can be added to root dataset to narrow down the search

A. parent
B. extracted
C. event
D. child

Correct Answer: D

QUESTION 89
Which of the following eval command functions is valid?

A. int()
B. count()
C. print()
D. tostring()

Correct Answer: D

QUESTION 90

In which Settings section are macros defined?

A. Fields
B. Tokens
C. Advanced Search
D. Searches, Reports, Alerts

Correct Answer: C

QUESTION 91
The eval command allows you to do which of the following? (Choose all that apply.)

A. Format values
B. Convert values
C. Perform calculations
D. Use conditional statements

Correct Answer: ABCD

QUESTION 92
When can a pipe follow a macro?

A. A pipe may always follow a macro.
B. The current user must own the macro.
C. The macro must be defined in the current app.
D. Only when sharing is set to global for the macro.

Correct Answer: A

QUESTION 93
Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

A. Macros
B. Lookups
C. Workflow actions
D. Field extractions

Correct Answer: B

QUESTION 94
This is what Splunk uses to categorize the data that is being indexed.

A. Host
B. Sourcetype
C. Index
D. Source

Correct Answer: B

QUESTION 95