SPLK-1002 Q&As

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

The timechart command buckets data in time intervals depending on:

A. the number of events returned

B. the selected time range

C. the type of visualization selected

Correct Answer: B

The timechart command buckets data in time intervals depending on the selected time range2. The timechart command is similar to the chart command but it automatically groups events into time buckets based on the _time field2. The size of the time buckets depends on the time range that you select for your search. For example, if you select Last 24 hours as your time range, Splunk will use 30-minute buckets for your timechart. If you select Last 7 days as your time range, Splunk will use 4-hour buckets for your timechart2. Therefore, option B is correct, while options A and C are incorrect because they are not factors that affect the size of the time buckets.

QUESTION 2

Which of the following is true about the Splunk Common Information Model (CIM)?

A. The data models included in the CIM are configured with data model acceleration turned off.

B. The CIM contains 28 pre-configured datasets.

C. The CIM is an app that needs to run on the indexer.

D. The data models included in the CIM are configured with data model acceleration turned on.

Correct Answer: D

The Splunk Common Information Model (CIM) is an app that contains a set of predefined data models that apply a common structure and naming convention to data from any source. The CIM enables you to use data from different sources in a consistent and coherent way. The CIM contains 28 pre-configured datasets that cover various domains such as authentication, network traffic, web, email, etc. The data models included in the CIM are configured with data model acceleration turned on by default, which means that they are optimized for faster searches and analysis. Data model acceleration creates and maintains summary data for the data models, which reduces the amount of raw data that needs to be scanned when you run a search using a data model. Splunk Core Certified Power User Track, page 10. : Splunk Documentation, About the Splunk Common Information Model.

QUESTION 3

When would transaction be used instead of stats?

A. To group events based on a single field value.

B. To see results of a calculation.

C. To have a faster and more efficient search.

D. To group events based on start/end values.

Correct Answer: D

The transaction command is used to group events that are related by some common fields or conditions, such as start/end values, time span, or pauses. The stats command is used to calculate statistics on a group of events by a common field value. References Splunk Community Splunk Transaction - Exact Details You Need

QUESTION 4

Which of the following statements are true for this search? (Select all that apply.) SEARCH: sourcetype=access* |fields action productId status

A. is looking for all events that include the search terms: fields AND action AND productId AND status

B. users the table command to improve performance

C. limits the fields are extracted

D. returns a table with 3 columns

Correct Answer: C

QUESTION 5

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

A. Tabs

B. Pipes

C. Spaces

D. Commas

Correct Answer: BCD

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep The Field Extractor (FX) is a tool that helps you extract fields from your data using delimiters or regular expressions. Delimiters are characters or strings

that separate fields in your data. The FX can detect some common delimiters automatically, such as pipes (|), spaces ( ), commas (,), semicolons (;), etc. The FX cannot detect tabs (\t) as delimiters automatically, but you can specify them

manually in the FX interface.