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

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 2

Splunk alerts can be based on search that run_____. (Select all that apply.)

A. in real-time

B. on a regular schedule

C. and have no matching events

Correct Answer: AB

Splunk alerts can be based on searches that run in real-time or on a regular schedule3. An alert is a way to monitor your data and get notified when certain conditions are met3. You can create an alert by specifying a search and a triggering condition3. You can also specify how often you want to run the search and how you want to receive the alert notifications3. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk3. Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day3. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

QUESTION 3

Using the Field Extractor (FX) tool, a value is highlighted to extract and give a name to a new field. Splunk has not successfully extracted that value from all appropriate events. What steps can be taken so Splunk successfully extracts the value from all appropriate events? (select all that apply)

A. Select an additional sample event with the Field Extractor (FX) and highlight the missing value in the event.

B. Re-ingest the data and attempt to extract from a new dataset.

C. Click on the event where the field was not extracted and choose "Change to Delimited".

D. Edit the regular expression manually.

Correct Answer: AD

When using the Field Extractor (FX) tool in Splunk and the tool fails to extract a value from all appropriate events, there are specific steps you can take to improve the extraction process. These steps involve interacting with the FX tool and possibly adjusting the extraction method:

A. Select an additional sample event with the Field Extractor (FX) and highlight the missing value in the event. This approach allows Splunk to understand the pattern better by providing more examples. By highlighting the value in another

event where it wasn\\'t extracted, you help the FX tool to learn the variability in the data format or structure, improving the accuracy of the field extraction. D. Edit the regular expression manually. Sometimes the FX tool might not generate the

most accurate regular expression for the field extraction, especially when dealing with complex log formats or subtle nuances in the data. In such cases, manually editing the regular expression can significantly improve the extraction process.

This involves understanding regular expression syntax and how Splunk extracts fields, allowing for a more tailored approach to field extraction that accounts for variations in the data that the automatic process might miss.

Options B and C are not typically related to improving field extraction within the Field Extractor tool. Re-ingesting data (B) does not directly impact the extraction process, and changing to a delimited extraction method (C) is not always

applicable, as it depends on the specific data format and might not resolve the issue of missing values across events.

QUESTION 4

Which of the following statements describes this search?

sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

A. This is a valid search and will display a timechart of the average duration, of each transaction event.

B. This is a valid search and will display a stats table showing the maximum pause among transactions.

C. No results will be returned because the transaction command must include the startswith and endswith options.

D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Correct Answer: A

This search uses the transaction command to group events that share a common value for JSESSIONID into transactions1. The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction1. The search then uses the timechart command to create a time-series chart of the average duration of each transaction1. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field. Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction1. Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search1.

QUESTION 5

Which search string would only return results for an event type called success ful_purchases?

A. tag=success ful_purchases

B. Event Type:: successful purchases

C. successful_purchases

D. event type--success ful_purchases

Correct Answer: C

This is because event types are added to events as a field named eventtype, and you can use this field as a search term to find events that match a specific event type. For example, eventtype=successful_purchases returns all events that have been categorized as successful purchases by the event type definition. The other options are incorrect because they either use a different field name (tag), a different syntax (Event Type:: or event type--), or have a typo (success ful_purchases). You can learn more about how to use event types in searches from the Splunk documentation1.