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 should transaction be used?

A. Only in a large distributed Splunk environment.

B. When calculating results from one or more fields.

C. When event grouping is based on start/end values.

D. When grouping events results in over 1000 events in each group.

Correct Answer: C

QUESTION 2

How are event types different from saved reports?

A. Event types cannot be used to organize data into categories.

B. Event types include formatting of the search results.

C. Event types can be shared with Splunk users and added to dashboards.

D. Event types do not include a time range.

Correct Answer: D

Explanation: Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies.

The correct answer is D. Event types do not include a time range.

The explanation is as follows:

Event types are a categorization system that help you make sense of your data by matching events with the same search string1. Event types are applied to events at search time and can be used as search terms or filters12. Saved reports

are results saved from a search action that can show statistics and visualizations of events3. Saved reports can be run anytime, and they fetch fresh results each time they are run34. Saved reports can be shared with other users and added

to dashboards4.

The main difference between event types and saved reports is that event types do not include a time range, while saved reports do14. This means that event types can match events from any time period, while saved reports are limited by the

time range specified when they are created or run14.

QUESTION 3

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

Explanation: 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 4

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

A. sourcetype

B. index

C. source

D. host

Correct Answer: A

QUESTION 5

Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search

A. Evenrches would return a report of sales by state.

B. Events will be returned from the data model named Application_State.

C. Events will be returned from the data model named All_Application_state.

D. No events will be returned because the pipe should occur after the datamodel command

Correct Answer: B

Explanation: The search string below returns events from the data model named Application_State.

| datamodel Application_State All_Application_State search The search string does the following:

It uses the datamodel command to access a data model in Splunk. The datamodel command takes two arguments: the name of the data model and the name of the dataset within the data model.

It specifies the name of the data model as Application_State. This is a predefined data model in Splunk that contains information about web applications. It specifies the name of the dataset as All_Application_State. This is a root dataset in

the data model that contains all events from all child datasets. It uses the search command to filter and transform the events from the dataset. The search command can use any search criteria or command to modify the results.

Therefore, the search string returns events from the data model named Application_State.