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 using the transaction command, how are evicted transactions identified?

A. Closed_txn field is set to o, or false.

B. Max_txn field is set to O, or false.

C. Txn_field is set to 1, or true.

D. open_txn field is set to 1, or true.

Correct Answer: A

The transaction command is a Splunk command that finds transactions based on events that meet various constraints1.

Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member1.

The transaction command adds some fields to the raw events that are part of the transaction12. These fields are:

Therefore, evicted transactions can be distinguished from non-evicted transactions by checking the value of the closed_txn field. The closed_txn field is set to 0, or false, for evicted transactions and 1, or true for non-evicted, or closed,

transactions23.

QUESTION 2

Consider the the following search run over a time range of last 7 days:

index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane

Which option is used to change the default time span so that results are grouped into 12 hour intervals?

A. span=12h

B. timespan=12h

C. span=12

D. timespan=12

Correct Answer: A

The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals. The timespan option is not a valid option for the timechart command2

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, timechart command.

QUESTION 3

Which of these search strings is NOT valid:

A. index=web status=50* | chart count over host, status

B. index=web status=50* | chart count over host by status

C. index=web status=50* | chart count by host, status

Correct Answer: A

This search string is not valid: index=web status=50* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

QUESTION 4

Which are valid ways to create an event type? (select all that apply)

A. By using the searchtypes command in the search bar.

B. By editing the event_type stanza in the props.conf file.

C. By going to the Settings menu and clicking Event Types > New.

D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Correct Answer: CD

Event types are custom categories of events that are based on search criteria. Event types can be used to label events with meaningful names, such as error, success, login, logout, etc. Event types can also be used to create transactions,

alerts, reports, dashboards, etc. Event types can be created in two ways:

By going to the Settings menu and clicking Event Types > New. This will open a form where you can enter the name, description, search string, app context, and tags for the event type. By selecting an event in search results and clicking

Event Actions > Build Event Type. This will open a dialog box where you can enter the name and description for the event type. The search string will be automatically populated based on the selected event.

Event types cannot be created by using the searchtypes command in the search bar, as this command does not exist in Splunk. Event types can also be created by editing the event_type stanza in the transforms.conf file, not the props.conf

file.

QUESTION 5

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.