



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.geekcert.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

A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, the eval or the sort?

- A. It doesn't matter whether eval or sort is used first.
- B. Convert the numeric to a string with eval first, then sort.
- C. Use sort first, then convert the numeric to a string with eval.
- D. You cannot use the sort command and the eval command on the same field.

Correct Answer: C

Explanation: The eval command is used to create new fields or modify existing fields based on an expression². The sort command is used to sort the results by one or more fields in ascending or descending order². If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings². This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 2

Which of the following statements describes an event type?

- A. A log level measurement: info, warn, error.
- B. A knowledge object that is applied before fields are extracted.
- C. A field for categorizing events based on a search string.
- D. Either a log, a metric, or a trace.

Correct Answer: C

Explanation: This is because an event type is a knowledge object that assigns a user- defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards. You can learn more about event types from the Splunk documentation¹. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

QUESTION 3

Which of the following is a function of the Splunk Common Information Model (CIM)?



- A. Normalizing data across a Splunk deployment.
- B. Providing templates for reports and dashboards.
- C. Algorithmically shifting events to other indexes.
- D. Reingesting previously indexed data with new field names.

Correct Answer: A

QUESTION 4

What does the transaction command do?

- A. Groups a set of transactions based on time.
- B. Creates a single event from a group of events.
- C. Separates two events based on one or more values.
- D. Returns the number of credit card transactions found in the event logs.

Correct Answer: B

Explanation: The transaction command is a search command that creates a single event from a group of events that share some common characteristics. The transaction command can group events based on fields, time, or both. The transaction command can also create some additional fields for each transaction, such as duration, eventcount, starttime, etc. The transaction command does not group a set of transactions based on time, but rather groups a set of events into a transaction based on time. The transaction command does not separate two events based on one or more values, but rather joins multiple events based on one or more values. The transaction command does not return the number of credit card transactions found in the event logs, but rather creates transactions from the events that match the search criteria.

QUESTION 5

What will you learn from the results of the following search?

```
sourcetype=cisco_esa | transaction mid, dclid, icid | timechart avg(duration)
```

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

Correct Answer: A