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

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 2

When using | timchart by host, which filed is representted in the x-axis?

A. date

B. host

C. time

D. -time

Correct Answer: A

QUESTION 3

Which of the following statements about tags is true? (select all that apply.)

A. Tags are case-insensitive.

B. Tags are based on field/vale pairs.

C. Tags categorize events based on a search.

D. Tags are designed to make data more understandable.

Correct Answer: BD

Explanation: The following statements about tags are true: tags are based on field/value pairs and tags categorize events based on a search. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. Tags can be used to filter or analyze your data based on common concepts or themes. Tags can be created by using various methods, such as search commands, configuration files, user interfaces, etc. Some of the characteristics of tags are: Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called "alert" for the field name "status" and the field value "critical". This means that only events that have status=critical will have the "alert" tag applied to them. Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called "web" for the search string

sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the "web" tag applied to them. The following statements about tags are false: tags are case-insensitive and tags are designed to make data more understandable. Tags are case-sensitive and tags are designed to make data more searchable. Tags are case-sensitive: This means that tags must match the exact case of the field name and field value that they are associated with. For example, if you create a tag called "alert" for the field name "status" and the field value "critical", it will not apply to events that have status=CRITICAL or Status=critical. Tags are designed to make data more searchable: This means that tags can help you find relevant events or patterns in your data by using common concepts or themes. For example, if you create a tag called "web" for the search string sourcetype=access_combined, you can use tag=web to find all events related to web activity.

QUESTION 4

This function of the stats command allows you to return the middle-most value of field X.

A. Median(X)

B. Eval by X

C. Fields(X)

D. Values(X)

Correct Answer: A

QUESTION 5

In which of the following scenarios is an event type more effective than a saved search?

A. When a search should always include the same time range.

B. When a search needs to be added to other users\\' dashboards.

C. When the search string needs to be used in future searches.

D. When formatting needs to be included with the search string.

Correct Answer: C

Reference: https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html

An event type is a way to categorize events based on a search string that matches the events2. You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names2. An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again2. Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.