SPLK-1002Q&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.pass2lead.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

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 2

What is the correct syntax to find events associated with a tag?

A. tag:=

B. tags=

C. tags:=

D. tag=

Correct Answer: D

The correct syntax to find events associated with a tag in Splunk is tag=1. So, the correct answer is D. tag=. This syntax allows you to annotate specified fields in your search results with tags1.

In Splunk, tags are a type of knowledge object that you can use to add meaningful aliases to field values in your data1. For example, if you have a field called status_code in your data, you might have different status codes like 200, 404, 500,

etc. You can create tags for these status codes like success for 200, not_found for 404, and server_error for 500. Then, you can use the tag command in your searches to find events associated with these tags1. Here is an example of how

you can use the tag command in a search:

index=main sourcetype=access_combined | tag status_code In this search, the tag command annotates the status_code field in the search results with the corresponding tags. If you have tagged the status code 200 with success, the status

code 404 with not_found, and the status code 500 with server_error, the search results will include these tags1.

You can also use the tag command with a specific tag value to find events associated with that tag. For example, the following search finds all events where the status code is tagged with success:

index=main sourcetype=access_combined | tag status_code | search tag::status_code=success

In this search, the tag command annotates the status_code field with the corresponding tags, and the search command filters the results to include only events where the status_code field is tagged with success1.

QUESTION 3

_____ datasets can be added to root dataset to narrow down the search

A. parent

B. extracted

C. event

D. child

Correct Answer: D

Explanation: Child datasets can be added to root datasets to narrow down the search. Datasets are collections of events that represent your data in a structured and hierarchical way. Datasets can be created by using commands such as datamodel or pivot. Datasets can have different types, such as events, search, transaction, etc. Datasets can also have different levels, such as root or child. Root datasets are base datasets that contain all events from a data model or an index. Child datasets are derived datasets that contain a subset of events from a parent dataset based on some constraints, such as search terms, fields, time range, etc. Child datasets can be added to root datasets to narrow down the search and filter out irrelevant events.

QUESTION 4

This function of the stats command allows you to return the sample standard deviation of a field.

A. stdev

B. dev

C. count deviation

D. by standarddev

Correct Answer: A

QUESTION 5

Which of the following describes the I transaction command?

A. It is an SPL command that groups at least two events together based on shared values in selected fields.

B. It allows an exchange of data from one Splunk index to another Splunk index.

C. It is an SPL command that groups events together with shared values in selected fields.

D. It allows an exchange of data from one Splunk system to another Splunk system.

Correct Answer: C

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

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 member .

The transaction command groups events together by matching one or more fields that have the same value across the events . For example, | transaction clientip will group events that have the same value in the clientip field.