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.leads4pass.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

Which of the following actions can the eval command perform?

A. Remove fields from results.

B. Create or replace an existing field.

C. Group transactions by one or more fields.

D. Save SPL commands to be reused in other searches.

Correct Answer: B

Explanation: The eval command is used to create new fields or modify existing fields based on an expression2. The eval command can perform various actions such as calculations, conversions, string manipulations and more2. One of the actions that the eval command can perform is to create or replace an existing field with a new value based on an

expression2. For example, | eval status=if(status="200","OK","ERROR") will create or replace the status field with either OK or ERROR depending on the original value of status2. Therefore, option B is correct, while options A, C and D are incorrect because they are not actions that the eval command can perform.

QUESTION 3

Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

A. Macros

B. Lookups

C. Workflow actions

D. Field extractions

Correct Answer: B

Explanation: Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups. https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsear chtime

QUESTION 4

A data model can consist of what three types of datasets?

A. Pivot, searches, and events.

B. Pivot, events, and transactions.

C. Searches, transactions, and pivot.

D. Events, searches, and transactions.

Correct Answer: D

QUESTION 5

Which of the following eval command functions is valid?

A. int()

B. count()

C. print()

D. tostring()

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunct ions

The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns "3.14". The other functions are not valid eval command functions.