SPLK-1002$^{Q\&As}$

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

QUESTION 1

Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

A. Field alias

B. Event types

C. Search workflow action

D. Tags

Correct Answer: A

The correct answer is A. Field alias123.

In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field3. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)12. The

CIM provides a methodology for normalizing values to a common field name1. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact2. By using field aliases, you can map vendor

fields to common fields that are the same for each data source in a given domain4. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention1.

QUESTION 2

Which of the following searches will return events containing a tag named Privileged?

A. tag=Priv

B. tag=Priv*

C. tag=priv* D. tag=privileged

Correct Answer: B

Explanation: The tag=Priv* search will return events containing a tag named Privileged, as well as any other tag that starts with Priv. The asterisk (*) is a wildcard character that matches zero or more characters. The other searches will not match the exact tag name.

QUESTION 3

A calculated field maybe based on which of the following?

A. Lookup tables

B. Extracted fields

C. Regular expressions

D. Fields generated within a search string

Correct Answer: B

Explanation: As mentioned before, a calculated field is a field that you create based on the value of another field or fields2. A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs2. Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

QUESTION 4

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.

QUESTION 5

When creating a data model, which root dataset requires at least one constraint?

A. Root transaction dataset

B. Root event dataset

C. Root child dataset

D. Root search dataset

Correct Answer: B

Explanation: The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation1. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.