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

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

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 data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

A. Alerts

B. Email

C. Database

D. User permissions

Correct Answer: ABC

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it3. The CIM add-on includes several data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, options A, B and C are correct because they are names of some of the data models included in the CIM add-on. Option D is incorrect because User permissions is not a name of a data model in the CIM add-on.

QUESTION 3

Which of the following eval commands will provide a new value for host from src if it exists?

A. | eval host = if (isnu11 (src), src, host)

B. | eval host = if (NOT src = host, src, host)

C. | eval host = if (src = host, src, host)

D. | eval host = if (isnotnull (src), src, host)

Correct Answer: D

The eval command is a Splunk command that allows you to create or modify fields using expressions .

The if function is an expression that evaluates a condition and returns a value based on whether the condition is true or false. The syntax of the if function is if(X,Y,Z), where X is the condition, Y is the value to return if X is true, and Z is the

value to return if X is false.

The isnotnull function is an expression that returns true if the argument is not null, and false otherwise. The syntax of the isnotnull function is isnotnull(X), where X is the argument to check.

Therefore, the expression if (isnotnull (src), src, host) returns the value of src if it is not null, and the value of host otherwise. This means that it will provide a new value for host from src if it exists, and keep the original value of host otherwise.

QUESTION 4

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 5

Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

A. CIM is a methodology for normalizing data.

B. CIM can correlate data from different sources.

C. The Knowledge Manager uses the CIM to create knowledge objects.

D. CIM is an app that can coexist with other apps on a single Splunk deployment.

Correct Answer: ABC

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

The Common Information Model (CIM) is a methodology for normalizing data from different sources and making it easier to analyze and report on it3. The CIM defines a common set of fields and tags for various domains such as Alerts, Email, Database, Network Traffic, Web and more3. One of the statements that describe the CIM is that it is a methodology for normalizing data, which means that it provides a standard way to name and structure data from different sources so that they can be compared and correlated3. Therefore, option A is correct. Another statement that describes the CIM is that it can correlate data from different sources, which means that it enables you to run searches and reports across data from different sources that share common fields and tags3. Therefore, option B is correct. Another statement that describes the CIM is that the Knowledge Manager uses the CIM to create knowledge objects, which means that the person who is responsible for creating and managing knowledge objects such as data models, field aliases, tags and event types can use the CIM as a guide to make their knowledge objects consistent and compatible with other apps and add-ons3. Therefore, option C is correct. Option D is incorrect because it does not describe the CIM but rather one of its components.