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.pass4itsure.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

By default search results are not returned in _____ order.

A. Chronological

B. Reverser chronological

C. ASCIE

D. Alphabetical

Correct Answer: AD

QUESTION 2

This is what Splunk uses to categorize the data that is being indexed.

A. Host

B. Sourcetype

C. Index

D. Source

Correct Answer: B

QUESTION 3

When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

A. OR

B. ( )

C. AND

D. NOT

Correct Answer: ABD

When you mouse over and click to add a search term from the Fields sidebar or from an event in your search results, Splunk automatically adds the term to your search string with an implied AND operator2. However, this does not apply to some Boolean operators such as OR, NOT and parentheses (). These operators are not implied when you add a search term and you have to type them manually if you want to use them in your search string2. Therefore, options A, B and D are correct, while option C is incorrect because AND is implied when you add a search term.

QUESTION 4

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 5

Information needed to create a GET workflow action includes which of the following? (select all that apply.)

A. A name of the workflow action

B. A URI where the user will be directed at search time.

C. A label that will appear in the Event Action menu at search time.

D. A name for the URI where the user will be directed at search time.

Correct Answer: ABC

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowactio n

Information needed to create a GET workflow action includes the following: a name of the workflow action, a URI where the user will be directed at search time, and a label that will appear in the Event Action menu at search time. A GET workflow action is a type of workflow action that performs a GET request when you click on a field value in your search results. A GET workflow action can be configured with various options, such as:

A name of the workflow action: This is a unique identifier for the workflow action that is used internally by Splunk. The name should be descriptive and meaningful for the purpose of the workflow action.

A URI where the user will be directed at search time: This is the base URL of the external web service or application that will receive the GET request. The URI can include field value variables that will be replaced by the actual field values at search time. For example, if you have a field value variable ip, you can write it as http://example.com/ip=$ip to

send the IP address as a parameter to the external web service or application.

A label that will appear in the Event Action menu at search time: This is the display name of the workflow action that will be shown in the Event Action menu when you click on a field value in your search results. The label should be clear and concise for the user to understand what the workflow action does.

Therefore, options A, B, and C are correct.