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

QUESTION 1

Which of the following statements are true for this search? (Select all that apply.) SEARCH:

sourcetype=access* |fields action productId status

A. is looking for all events that include the search terms: fields AND action AND productId AND status

B. users the table command to improve performance

C. limits the fields are extracted

D. returns a table with 3 columns

Correct Answer: C

QUESTION 2

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

A. Rank

B. Weight

C. Priority

D. Precedence

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtype s

When multiple event types with different color values are assigned to the same event, the color displayed for the events is determined by the priority of the event types. The priority is a numerical value that indicates how important an event type is. The higher the priority, the more important the event type. The event type with the highest priority will determine the color of the event.

QUESTION 3

What is the Splunk Common Information Model (CIM)?

A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.

B. The CIM provides a methodology to normalize data from different sources and source types.

C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.

D. The CIM is a data exchange initiative between software vendors.

Correct Answer: B

Explanation: The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

QUESTION 4

What are search macros?

A. Lookup definitions in lookup tables.

B. Reusable pieces of search processing language.

C. A method to normalize fields.

D. Categories of search results.

Correct Answer: B

Explanation: The correct answer is B. Reusable pieces of search processing language.

The explanation is as follows:

Search macros are knowledge objects that allow you to insert chunks of SPL into other searches12.

Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command12. You can also specify whether the macro field takes any arguments and define validation expressions for

them12.

Search macros can help you make your SPL searches shorter and easier to understand3.

To use a search macro in a search string, you need to put a backtick character () before and after the macro name[^1^][1]. For example, mymacro`.

QUESTION 5

Which of the following objects can a calculated field use as a source?

A. An alias of a field.

B. A field added by an automatic lookup.

C. The tag field.

D. The eventtype field.

Correct Answer: B

Explanation: The correct answer is B. A field added by an automatic lookup.

A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can use any field as a source, as long as the field is extracted before the calculated field is defined1. An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field2. An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields3. Therefore, a calculated field can use a field added by an automatic lookup as a source. References: About calculated fields About lookups Search time processing