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

Which of the following searches will return events contains a tag name Privileged?

A. Tag= Priv

B. Tag= Pri*

C. Tag= Priv*

D. Tag= Privileged

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

A tag is a descriptive label that you can apply to one or more fields or field values in your events1. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags1. To search for events that contain a tag name, you can use the tag keyword followed by an equal sign and the tag name1. You can also use wildcards (*) to match partial tag names1. Therefore, option B is correct because it will return events that contain a tag name that starts with Pri. Options A and D are incorrect because they will only return events that contain an exact tag name match. Option C is incorrect because it will return events that contain a tag name that starts with Priv, not Privileged.

QUESTION 2

What do events in a transaction have In common?

A. All events In a transaction must have the same timestamp.

B. All events in a transaction must have the same sourcetype.

C. All events in a transaction must have the exact same set of fields.

D. All events in a transaction must be related by one or more fields.

Correct Answer: D

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

A transaction is a group of events that share some common characteristics, such as fields, time, or both. A transaction can be created by using the transaction command or by defining an event type with transactiontype=true in props.conf. Events in a transaction have one or more fields in common that relate them to each other. For example, you can create a transaction based on JSESSIONID, which is a unique identifier for each user session in web logs. Events in a transaction do not have to have the same timestamp, sourcetype, or exact same set of fields. They only have to share one or more fields that define the transaction.

QUESTION 3

Which of the following statements best describes a macro?

A. A macro is a method of categorizing events based on a search.

B. A macro is a way to associate an additional (new) name with an existing field name.

C. A macro is a portion of a search that can be reused in multiple place

D. A macro is a knowledge object that enables you to schedule searches for specific events.

Correct Answer: C

The correct answer is C. A macro is a portion of a search that can be reused in multiple places.

A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which

are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1. To create a macro, you need to define its name, definition, arguments, and

description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments

if any1. For example, if you have a macro named my_macro that takes one argument named object and has the following definition:

search sourcetype= object

You can use it in a search by writing:

my_macro(web)

This will expand the macro and run the following SPL code:

search sourcetype=web

The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.

The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:

A. An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports2.
B. A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.

D. An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4. References: About event types About field aliases About alerts Define search macros in Settings Use search macros in searches

QUESTION 4

A field alias is created where field1--fieid2 and the Overwrite Field Values checkbox is selected.

What happens if an event only contains values for fieid1?

A. field2 values are removed from the events.

B. field1 and field2 values are merged.

C. field2 values are unchanged.

D. field2 values are replaced with the value of the field1.

Correct Answer: D

The correct answer is D. field2 values are replaced with the value of the field1.

A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used

to rename fields for clarity or convenience1.

When you create a field alias in Splunk Web, you can select the Overwrite Field Values option to change the behavior of the field alias. This option affects how the Splunk software handles situations where the original field has no value or

does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field2.

If you select the Overwrite Field Values option, the following rules apply:

If the original field does not exist or has no value in an event, the alias field is removed from that event.

If the original field and the alias field both exist in an event, the value of the alias field is replaced with the value of the original field. If you do not select the Overwrite Field Values option, the following rules apply:

If the original field does not exist or has no value in an event, the alias field is unchanged in that event.

If the original field and the alias field both exist in an event, both fields are retained with their respective values.

Therefore, if you create a field alias where field1--field2 and select the Overwrite Field Values option, and an event only contains values for field1, then the value of field2 will be replaced with the value of field1.

References:

About calculated fields

About field aliases Create field aliases in Splunk Web

QUESTION 5

Which of the following search control will not re-rerun the search? (Select all that apply.)

A. zoom out

B. selecting a bar on the timeline

C. deselect

D. selecting a range of bars on the timelines

Correct Answer: BCD

Explanation: The timeline is a graphical representation of your search results that shows the distribution of events over time2. You can use the timeline to zoom in or out of a specific time range or to select one or more bars on the timeline to filter your results by that time range2. However, these actions will not re-run the search, but rather refine the existing results based on the selected time range2. Therefore, options B, C and D are correct, while option A is incorrect because zooming out will re-run the search with a broader time range.

Latest SPLK-1002 Dumps SPLK-1002 Practice Test SPLK-1002 Study Guide