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

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

QUESTION 1

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:

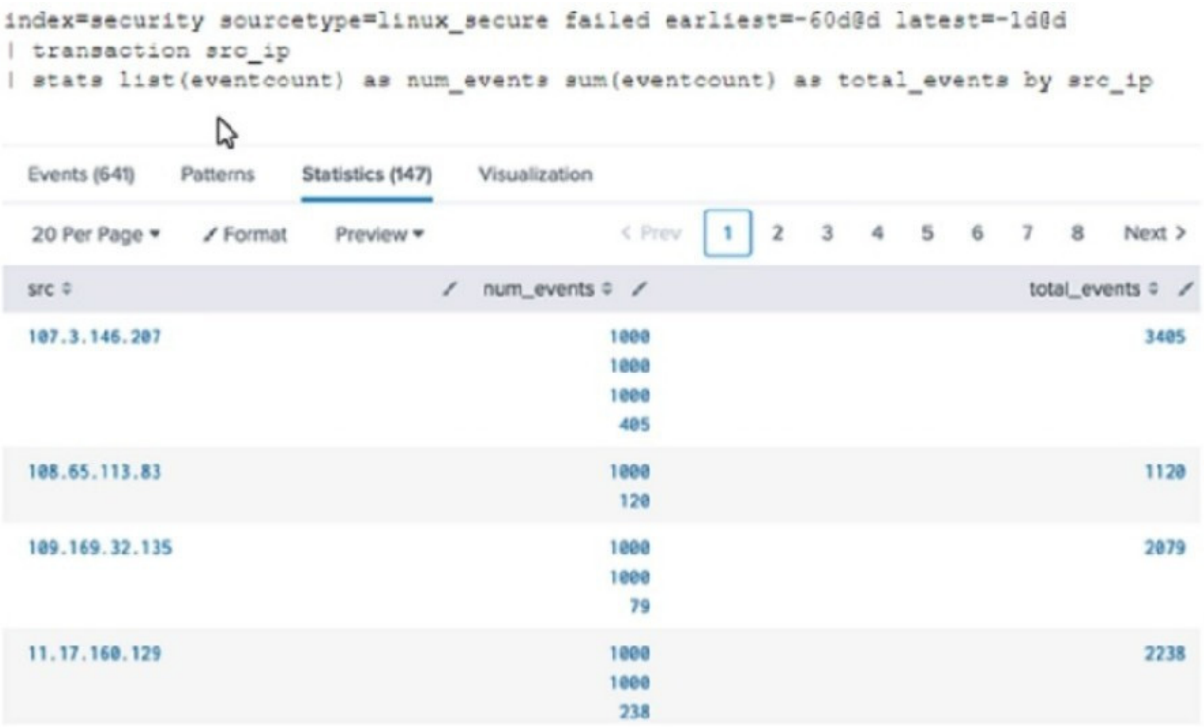
About calculated fields

About field aliases

Create field aliases in Splunk Web

QUESTION 2

Why would the following search produce multiple transactions instead of one?



```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

src	num_events	total_events
107.3.146.207	1000 1000 1000 405	3405
108.65.113.83	1000 120	1120
109.169.32.135	1000 1000 79	2079
11.17.160.129	1000 1000 238	2238

A. The maxspan option is not included.

B. The transaction command has a limit of 1000 events per transaction.

C. The transaction and commands cannot be used together.

D. The stats list () function is used.

Correct Answer: A

In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1. However, you can use the

maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1. Therefore, if the maxspan option

is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.

Here is an example of how you can use the maxspan option in a search:

index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h In this search, the transaction command groups events that share the same someuniqefield value into a single transaction, but only if the time span

between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

QUESTION 3

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.

B. The field being extracted will be required for all future events.

C. The events without the required field will not display in searches.

D. Only events with the required string will be included in the extraction.

Correct Answer: D

The Field Extractor (FX) allows you to use regular expressions (regex) to extract fields from your events using a graphical interface or by manually editing the regex2. When you use the FX to perform a regex field extraction, you can use the require option to specify a string that must be present in an event for it to be included in the extraction2. This way, you can filter out events that do not contain the required string and focus on the events that are relevant for your extraction2. Therefore, option D is correct, while options A, B and C are incorrect.

QUESTION 4

When defining a macro, what are the required elements?

A. Name and arguments.

B. Name and a validation error message.

C. Name and definition.

D. Definition and arguments.

Correct Answer: C

When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced. The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation2

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Define search macros in Settings.

QUESTION 5

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.