format

Description

This command is used implicitly by subsearches. This command takes the results of a subsearch, formats the results into a single result and places that result into a new field called search.

Syntax

format [mvsep="<mv separator>"] [maxresults=<int>] [<row prefix>" "<column prefix>" "<column separator>" "<column end>" "<row separator>" "<row end>"]

If you want to specify a row or column options, you must specify all of the row and column options.

Optional arguments

mvsep

Syntax: mvsep="<string>"
Description: The separator to use for multivalue fields.
Default: OR

maxresults

Syntax: maxresults=<int>
Description: The maximum results to return.
Default: 0, which means no limitation on the number of results returned.

<row prefix>

Syntax: "<string>"
Description: The value to use for the row prefix.
Default: The open parenthesis character "/"

<column prefix>

Syntax: "<string>"
Description: The value to use for the column prefix.
Default: The open parenthesis character "/"

<column separator>
Syntax: "<string>"
Description: The value to use for the column separator.
Default: AND

<column end>
Syntax: "<string>"
Description: The value to use for the column end.
Default: The close parenthesis character ")"

<row separator>
Syntax: "<string>"
Description: The value to use for the row separator.
Default: OR

<row end>
Syntax: "<string>"
Description: The value to use for the column end.
Default: The close parenthesis character ")"

Usage

By default, when you do not specify any of the optional row and column arguments, the output of the format command defaults to: "(" "(" "AND" ")" "OR" ")".

The only reason to specify the row and column arguments is to export the query to another system that requires different formatting.

Examples

1. Example with no optional parameters

Suppose that you have results that look like this:

<table>
<thead>
<tr>
<th>source</th>
<th>sourcetype</th>
<th>host</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog.log</td>
<td>syslog</td>
<td>my_laptop</td>
</tr>
<tr>
<td>bob-syslog.log</td>
<td>syslog</td>
<td>bobs_laptop</td>
</tr>
<tr>
<td>laura-syslog.log</td>
<td>syslog</td>
<td>lauras_laptop</td>
</tr>
</tbody>
</table>

The following search returns the top 2 results, and creates a search based on the host, source, and sourcetype fields. The default format settings are used.
This search returns the syntax for a search that is based on the field values in the top 2 results. The syntax is placed into a new field called `search`.

<table>
<thead>
<tr>
<th>source</th>
<th>sourcetype</th>
<th>host</th>
<th>search</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>( host=&quot;mylaptop&quot; AND source=&quot;syslog.log&quot; AND sourcetype=&quot;syslog&quot; ) OR ( host=&quot;bobslaptop&quot; AND source=&quot;bob-syslog.log&quot; AND sourcetype=&quot;syslog&quot; )</td>
</tr>
</tbody>
</table>

2. Example using the optional parameters

You want to produce output that is formatted to use on an external system.

```
... | format "[ "[ "&&" ""]" "||" ""]"
```

Using the data in Example 1, the result is:

<table>
<thead>
<tr>
<th>source</th>
<th>sourcetype</th>
<th>host</th>
<th>search</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>[ [ host=&quot;mylaptop&quot; &amp;&amp; source=&quot;syslog.log&quot; &amp;&amp; sourcetype=&quot;syslog&quot; ]</td>
</tr>
</tbody>
</table>

3. Multivalue separator example

The following search uses the `eval` command to create a field called "foo" that contains one value "eventtype,log_level". The `makemv` command is used to make the foo field a mulitvalue field and specifies the comma as the delimiter between the values. The search then outputs only the foo field and formats that field.

```
index=_internal |head 1 |eval foo="eventtype,log_level" | makemv delim="", foo | fields foo | format mvsep="mvseparator" "{" "[ "AND" " ]" "AND" " }"
```

This results in the following output:

<table>
<thead>
<tr>
<th>foo</th>
<th>search</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[ ( foo=&quot;eventtype&quot; mvseparator foo=&quot;log_level&quot; ) ]</td>
</tr>
</tbody>
</table>

3
See also

search

Answers

Have questions? Visit Splunk Answers and see what questions and answers the Splunk community has using the format command.