Multivalue stats and chart functions

list(<value>)

Description

The `list` function returns a multivalue entry from the values in a field. The order of the values reflects the order of the events.

Usage

You can use this function with the chart, stats, and timechart commands.

- If more than 100 values are in a field, only the first 100 are returned.
- This function processes field values as strings.

Basic example

To illustrate what the `list` function does, let's start by generating a few simple results.

1. Use the `makeresults` and `streamstats` commands to generate a set of results that are simply timestamps and a count of the results which are used as row numbers.

```
| makeresults count=1000 | streamstats count AS rowNumber
```

The results appear on the Statistics tab and look something like this:

_time	rowNumber
2018-04-02 20:27:11	1
2018-04-02 20:27:11	2
2018-04-02 20:27:11	3
2018-04-02 20:27:11	4
2018-04-02 20:27:11	5

```
| makeresults count=1000 | streamstats count AS rowNumber | stats
list(rowNumber) AS numbers
```

The results appear on the Statistics tab and look something like this:

numbers
1 2 3 4 5

Notice that it is a single result. There are no alternating row background colors.

2. Compare this result with the results returned by the `values` function.

values(<values>)

Description

The `values` function returns a list of the distinct values in a field as a multivalue entry. The order of the values is lexicographical.

Usage

You can use the `values(X)` function with the chart, stats, timechart, and tstats commands.

- By default there is no limit to the number of values returned. Users with the appropriate permissions can specify a limit in the `limits.conf` file. You specify the limit in the [stats | sistats] stanza using the `maxvalues` setting.
- This function processes field values as strings.

Lexicographical order

Lexicographical order sorts items based on the values used to encode the items in computer memory. In Splunk software, this is almost always UTF-8 encoding, which is a superset of ASCII.

- Numbers are sorted before letters. Numbers are sorted based on the first digit. For example, the numbers 10, 9, 70, 100 are sorted lexicographically as 10, 100, 70, 9.
- Uppercase letters are sorted before lowercase letters.
- Symbols are not standard. Some symbols are sorted before numeric values. Other symbols are sorted before or after letters.

Basic example

To illustrate what the `values` function does, let's start by generating a few simple results.

1. Use the `makeresults` and `streamstats` commands to generate a set of results that are simply timestamps and a count of the results, which are used as row numbers.

   ```
   | makeresults count=1000 | streamstats count AS rowNumber
   ```

   The results appear on the Statistics tab and look something like this:

_time	rowNumber
2018-04-02 20:27:11	1
2018-04-02 20:27:11	2
2018-04-02 20:27:11	3
2018-04-02 20:27:11	4
2018-04-02 20:27:11	5

   Notice that each result appears on a separate row.

2. Add the `stats` command with the `values` function to the search. The results are returned in lexicographical order.

   ```
   | makeresults count=1000 | streamstats count AS rowNumber | stats
   values(rowNumber) AS numbers
   ```

   The results appear on the Statistics tab and look something like this:

numbers
1 10 100 1000 101 102 103 104 105 106 107 108 109 11 110

Notice that it is a single result. There are no alternating row background colors.

2. Compare these results with the results returned by the `list` function.