Splunk® Enterprise Search Reference 8.0.0

convert

Generated: 11/13/2019 10:29 pm
convert

Description

The convert command converts field values in your search results into numerical values. Unless you use the AS clause, the original values are replaced by the new values.

Alternatively, you can use evaluation functions such as strftime(), strptime(), or tonumber() to convert field values.

Syntax

convert [timeformat=string] (<convert-function> [AS <field>])...

Required arguments

<convert-function>

Syntax: auto() | ctime() | dur2sec() | memk() | mktime() | mstime() | none() | num() | rmcomma() | rmunit()

Description: Functions to use for the conversion.

Optional arguments

timeformat

Syntax: timeformat=<string>

Description: Specify the output format for the converted time field. The timeformat option is used by ctime and mktime functions. For a list and descriptions of format options, see Common time format variables in the Search Reference.

Default: %m/%d/%Y %H:%M:%S. Note that this default does not conform to the locale settings.

<field>

Syntax: <string>

Description: Creates a new field with the name you specify to place the converted values into. The original field and values remain intact.

Convert functions

auto()

Syntax: auto(<wc-field>)
**Description:** Automatically convert the fields to a number using the best conversion. Note that if not all values of a particular field can be converted using a known conversion type, the field is left untouched and no conversion at all is done for that field. You can use wild card characters in the field name.

**ctime()**

**Syntax:** ctime(<wc-field>)

**Description:** Convert an epoch time to an ascii human readable time. Use the `timeformat` option to specify exact format to convert to. You can use wild card characters in the field name.

**dur2sec()**

**Syntax:** dur2sec(<wc-field>)

**Description:** Convert a duration format "[D+]HH:MM:SS" to seconds. You can use wild card characters in the field name.

**memk()**

**Syntax:** memk(<wc-field>)

**Description:** Accepts a positive number (integer or float) followed by an optional "k", "m", or "g". The letter k indicates kilobytes, m indicates megabytes, and g indicates gigabytes. If no letter is specified, kilobytes is assumed. The output field is a number expressing quantity of kilobytes. Negative values cause data incoherency. You can use wild card characters in the field name.

**mktime()**

**Syntax:** mktime(<wc-field>)

**Description:** Convert a human readable time string to an epoch time. Use `timeformat` option to specify exact format to convert from. You can use wild card characters in the field name.

**mstime()**

**Syntax:** mstime(<wc-field>)

**Description:** Convert a [MM:]SS.SSS format to seconds. You can use wild card characters in the field name.

**none()**

**Syntax:** none(<wc-field>)

**Description:** In the presence of other wildcards, indicates that the matching fields should not be converted. You can use wild card characters in the field name.
num()

**Syntax:** num(<wc-field>)
**Description:** Like auto(), except non-convertible values are removed. You can use wild card characters in the field name.

rmcomma()

**Syntax:** rmcomma(<wc-field>)
**Description:** Removes all commas from value, for example rmcomma(1,000,000.00) returns 1000000.00. You can use wild card characters in the field name.

rmunit()

**Syntax:** rmunit(<wc-field>)
**Description:** Looks for numbers at the beginning of the value and removes trailing text. You can use wild card characters in the field name.

**Usage**

The `convert` command is a **distributable streaming command.** See Command types.

**Basic examples**

1. **Convert all field values to numeric values**

   Use the `auto` convert function to convert all field values to numeric values.

   ```
   ... | convert auto(*)
   ```

2. **Convert field values except for values in specified fields**

   Convert every field value to a number value except for values in the field `foo`. Use the `none` convert function to specify fields to ignore.

   ```
   ... | convert auto(*) none(foo)
   ```

3. **Change the duration values to seconds for the specified fields**

   Change the duration values to seconds for the specified fields

   ```
   ... | convert dur2sec(xdelay) dur2sec(delay)
   ```
4. **Change the sendmail syslog duration format to seconds**

Change the sendmail syslog duration format (D+HH:MM:SS) to seconds. For example, if `delay="00:10:15"`, the resulting value is `delay="615"`. This example uses the `dur2sec` convert function.

```plaintext
... | convert dur2sec(delay)
```

5. **Convert field values that contain numeric and string values**

Convert the values in the `duration` field, which contain numeric and string values, to numeric values by removing the string portion of the values. For example, if `duration="212 sec"`, the resulting value is `duration="212"`. This example uses the `rmunit` convert function.

```plaintext
... | convert rmunit(duration)
```

6. **Change memory values to kilobytes**

Change all memory values in the `virt` field to KBs. This example uses the `memk` convert function.

```plaintext
... | convert memk(virt)
```

**Extended Examples**

1. **Convert a UNIX time to a more readable time format**

Convert a UNIX time to a more readable time formatted to show hours, minutes, and seconds.

```plaintext
source="all_month.csv" | convert timeformat="%H:%M:%S" ctime(_time) AS c_time | table _time, c_time
```

- The `ctime()` function converts the `_time` value in the CSV file events to the format specified by the `timeformat` argument.
- The `timeformat="%H:%M:%S"` argument tells the search to format the `_time` value as HH:MM:SS.
- The converted time `ctime` field is renamed `c_time`.
- The `table` command is used to show the original `_time` value and the `ctime` field.

The results appear on the Statistics tab and look something like this:
The `ctime()` function changes the timestamp to a non-numerical value. This is useful for display in a report or for readability in your events list.

2. Convert a time in MM:SS.SSS to a number in seconds

Convert a time in MM:SS.SSS (minutes, seconds, and subseconds) to a number in seconds.

```
sourcetype=syslog | convert mstime(_time) AS ms_time | table _time, ms_time
```

- The `mstime()` function converts the `_time` field values from minutes and seconds to just seconds.

The converted time field is renamed `ms_time`.

- The `table` command is used to show the original `_time` value and the converted time.

<table>
<thead>
<tr>
<th>_time</th>
<th>ms_time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-03-27 17:20:14.839</td>
<td>1522196414.839</td>
</tr>
<tr>
<td>2018-03-27 17:21:05.724</td>
<td>1522196465.724</td>
</tr>
<tr>
<td>2018-03-27 17:27:03.790</td>
<td>1522196823.790</td>
</tr>
<tr>
<td>2018-03-27 17:28:41.869</td>
<td>1522196921.869</td>
</tr>
<tr>
<td>2018-03-27 17:34:40.900</td>
<td>1522197280.900</td>
</tr>
<tr>
<td>2018-03-27 17:38:47.120</td>
<td>1522197527.120</td>
</tr>
<tr>
<td>2018-03-27 17:40:10.345</td>
<td>1522197610.345</td>
</tr>
</tbody>
</table>
The `mstime()` function changes the timestamp to a numerical value. This is useful if you want to use it for more calculations.

3. **Convert a string time in HH:MM:SS into a number**

Convert a string field `time_elapsed` that contains times in the format HH:MM:SS into a number. Sum the `time_elapsed` by the `user_id` field. This example uses the `eval` command to convert the converted results from seconds into minutes.

```plaintext
...| convert num(time_elapsed) | stats sum(eval(time_elapsed/60)) AS Minutes BY user_id
```

**See also**

Commands
- `eval`
- `fieldformat`

Functions
- `tonumber`
- `strptime`

**Answers**

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