



Criblable Splunk® Optimization Pack v1.0.0

Splunk® is a trademark or registered trademark of Splunk Inc. in the United States and other countries

Overview:

This Pack enables administrators so that they may reduce license usage.

Using various eval techniques, the pack allows for the shortening of timestamps in events to reduce license consumption.

The concepts are simple but powerful and just the tip of the iceberg when it comes to what Criblable LLC can do for your organization. Contact us today to hire one of our Cribl Certified Observability Expert Consultants! Email info@criblable.com or call 844-DATA-PRO.

Using The Pack:


To use this Pack, follow these steps:

1. Attach the SLOv1 pipeline to your route
2. Open the long_timestamps.log sample file (included with the pack)
3. Enable the evals in the pipeline top to bottom, noting the differences between in/out.

Release Notes:

Version 1.0.0 - 2022-12-12

In this release, we have added a number of great features. We've goat you covered!



Here we take a timestamp that is unnecessarily long reducing it by more than 30%...

Before:

```
{
  "_raw": "08-22-2022 16:48:52.123456789 +0000 a super long
timestamp",
  "_time": 1661186932.123
}
```

After:

```
{
  "_raw": "1661186932123 a super long timestamp",
  "_time": 1661186932.123,
}
```

Length of _raw before: 58 Characters

Length of _raw after: 36 Characters

Savings: 22 Characters per event or roughly **38% difference in the**
length of raw!



Help

TSO Level 1: This eval will match events that have a timezone offset of +0000, and remove the timezone offset as well as the space before it from the events, saving 6 characters per event.

☐ No



Keep Fields ?

Enter field names

Remove Fields (?)

Enter field names



Sample Data

[Preview Simple](#)[Preview Full](#)

Sample data file

long_timestamps.log

IN

OUT

#

Event

1 α _raw: 08-22-2022 16:48:52.123456789 +0000
2022-08-22 # _time: 1661186932.123
12:48:52.123
-04:00

2 α _raw: 08-22-2022 16:48:52.123456789 a long timestamp
2022-08-22 # _time: 1661201332.123
16:48:52.123
-04:00

3 α _raw: 08-22-2022 16:48:52.123456 a medium timestamp
2022-08-22 # _time: 1661201332.123
16:48:52.123
-04:00

4 α _raw: 08-22-2022 16:48:52.123 a normal timestamp
2022-08-22 # _time: 1661201332.123
16:48:52.123
-04:00

	_raw Length	Full Event Length	Number of Fields	Number of Events
IN	199.00B	327.00B	2	4
OUT	138.00B	350.00B	3	4
DIFF	↓ -30.65%	↑ 7.03%	↑ 50.00%	0.00%

30.65%

Whoa! This being the savings with just a couple of modifications!
Think of all the savings Criblable could help you attain!

Now if you're ready to get your copy of the pack, contact us today!

Info@criblable.com

