Suricata - Feature #3321
Evaluate different encoders for eve-log
11/06/2019 08:04 AM - Davide Setti

Status: New
Priority: Low
Assignee: Community Ticket
Category: 
Target version: TBD
Effort: 
Difficulty: 
Label: 

Description
We were thinking that it could be useful to be able to choose a specific encoders for eve JSON logs.
As of now these logs are encoded as normal JSON strings, however in some use cases it could be better to use a different encoder to write output.
In example msgpack could be a good choice when sending output to redis (or even to file) because it reduces output size. This may also help increasing output performances in high throughput environments.

History
#1 - 11/06/2019 08:21 AM - Victor Julien
- Assignee set to Community Ticket

We will definitely need help with this.

#2 - 11/06/2019 02:16 PM - Jason Ish
Some discussion of this has occurred before. Do we find some intermediate data format that we can then render to JSON, msgpack, etc? Or do we give up that idea and make the most performance JSON output we can.

The most common answer I hear is JSON, but its something that needs to be settled before doing anything about it, as its a huge change to do either.

#3 - 11/07/2019 10:02 PM - Andreas Herz
- Target version set to TBD

#4 - 11/26/2019 03:30 PM - Jason Ish
- Priority changed from Normal to Low

Optimizing eve output for performance is the current priority. That may be hard to do, and offer alternative output formats.

#5 - 11/12/2020 12:51 PM - Victor Julien
I think we have been successful at speeding up eve, through #3707 and #3293.