Suricata - Feature #3293
eve: per thread output files
11/01/2019 03:57 PM - Andreas Herz

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Target version: 6.0.0beta1
Effort:
Difficulty:
Description

Related issues:
Related to Task #3288: Suricon 2019 brainstorm Assigned
Related to Bug #2726: writing large number of json events on high speed traffic... Closed

History
#1 - 11/02/2019 08:53 AM - Victor Julien
- Subject changed from Add support to split eve json output to dedicated worker thread files similiar to pcap to eve: per thread output files

To avoid contention on the single output structure (+lock) when having many worker threads, add a mode where we have a eve.json per thread.
Modern tools like logstash/filebeat support tracking & processing multiple files w/o issue.

#2 - 11/05/2019 10:53 AM - Victor Julien
- Parent task deleted (#3288)

#3 - 11/05/2019 10:53 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#4 - 11/06/2019 08:55 PM - Victor Julien
- Related to Bug #2726: writing large number of json events on high speed traffic results in packet drops added

#5 - 01/22/2020 12:43 AM - Jeff Lucovsky
@Mats Klepsland Will you be able to work on this issue? If not, I'd be happy to pick it up.

#6 - 01/28/2020 06:30 PM - Mats Klepsland
Jeff Lucovsky wrote:

@Mats Klepsland Will you be able to work on this issue? If not, I'd be happy to pick it up.

Hi, Jeff.

My time is stretched both at work and at home, at the moment, so please do if you want to. This is a feature that I think would be awesome to have, performance wise :)

#7 - 07/06/2020 08:44 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from Mats Klepsland to Jeff Lucovsky
- Target version changed from 70 to 6.0.0beta1

#8 - 07/30/2020 11:59 AM - Jeff Lucovsky
- Status changed from Assigned to In Review
#9 - 08/03/2020 11:35 AM - Jeff Lucovsky

- Status changed from In Review to Closed