Suricata - Feature #1215
journald logging support

06/18/2014 05:16 AM - god lol

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Low</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

Description
Would be great to have an option for logging to systemd's journald directly. This would allow for using advanced log classification facilities provided by journald (structural logging) and securing logs with "log sealing" feature out of the box.

See also https://fedorahosted.org/lumberjack/ for details.

History

#1 - 06/19/2014 03:52 AM - Victor Julien
- Assignee set to Anonymous
- Priority changed from Normal to Low
- Target version set to TBD

Will have to be contributed.

#2 - 06/12/2018 05:52 PM - Jason Ish
Is this worth exploring even when running Suricata from systemd?

#3 - 07/13/2018 06:51 PM - Victor Julien
- Effort set to medium
- Difficulty set to medium

#4 - 02/23/2019 10:15 PM - Andreas Herz
- Assignee set to Community Ticket