## Suricata - Feature #4149

### Research: Dynamic datasets

11/14/2020 02:42 PM - Jeff Lucovsky

<table>
<thead>
<tr>
<th>Status:</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</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></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**  
Chris G Nov 12th at 11:23 AM  
We are not using datasets yet in production, but one big issue is our datasets are constantly changing and managing static files and suricata reloads is pain. What about tying a dataset to a Redis keyspace? Much easier to dynamically swap out data there. (edited)

2 replies

Andreas Herz 1 day ago  
Can you elaborate a bit more why it's a pain?  
Not to say that using something like redis might be worth to look into, right now it's only used for logging output

Chris G 1 day ago  
Missed this one. Mostly because we already want that data in place where other applications can easily access and not worry about keeping it in sync. Also if I understand it correctly, we basically want to use dynamic sets exclusively and have them persist across restarts/reloads.

**Related issues:**  
Related to Task #4097: Suricon 2020 brainstorm

**Assigned**

## History

**#1 - 11/14/2020 02:43 PM - Jeff Lucovsky**  
- Related to Task #4097: Suricon 2020 brainstorm added

**#2 - 11/19/2020 09:15 PM - Victor Julien**  
- Status changed from New to Feedback  
- Assignee set to Community Ticket  
- Target version set to TBD

Datasets are persistent (suricata restart will save/load). Data can be added and removed through the unix socket interface. What else is needed? I think using extra tooling the bridge with redis could be made.