Suricata - Feature #1290
handle SIGHUP signal
09/30/2014 03:18 AM - Dariusz Binkul

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

Label:

Description
Hello,

it would be nice to make Suricata to handle SIGHUP signal in a way that it would:
- reopen log files
- reopen unix socket
- reread configuration file

Currently if a unix socket is created after suricata starts, I must restart suricata in order to connect to socket.

If you implement it, I could send SIGHUP (or other) signal to suricata every time when socket is created so it can reconnect successfully.

Kind regards,
Dariusz Binkul

History

#1 - 09/30/2014 10:01 AM - Jason Ish
In 2.0.4 a SIGHUP will re-open all the log files (zeroing them in doing so, on the assumption that a tool like logrotate has moved them out). I believe a SIGUSR2 will re-read the configuration.

I don't know enough about the unix socket to know if its a good idea to re-open it as part of the SIGHUP. Why does it need re-opening?

#2 - 10/01/2014 02:15 AM - Dariusz Binkul
Hello,

like I said. If a unix socket is created after suricata starts, I must restart suricata in order to connect to socket. This is a problem, because you must config your system start scripts to check if a service that provides socket is init before suricata starts.

Another thing is that restart of a service that provide socket must be followed by a suricata restart.

If suricata could reopen unix socket, then suricata and socket provider(service) could work independently.

Kind regards,
Dariusz Binkul

Jason Ish wrote:

In 2.0.4 a SIGHUP will re-open all the log files (zeroing them in doing so, on the assumption that a tool like logrotate has moved them out). I believe a SIGUSR2 will re-read the configuration.

I don't know enough about the unix socket to know if its a good idea to re-open it as part of the SIGHUP. Why does it need re-opening?

#3 - 01/01/2016 06:01 PM - Andreas Herz

- Assignee set to OISF Dev
- Target version set to TBD
So HUP would be like USR2, except it would handle socket reconnects as well?

- Assignee set to Community Ticket