Prelude Manager - Bug #248

prelude-manager crash

07/12/2007 07:05 AM - prmarino1-gmail-com -

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	invalid		

Description

running the prelude-manager with aproximitly 400 lml agents i get this message in syslog

```
prelude-manager: idmef-message-scheduler.c:init_file_output:573: couldn't open /var/spool/prelude/
prelude-manager/mid-priority-fifo.146 in append mode: Too many open files.
```

shortly after that if im lucky the prelude-manager stops reporting but is still running and the lmls start crashing with messages like

```
 prelude-lml: prelude-client: error starting prelude-client: TLS handshake failed: A TLS packet wi
th unexpected length was received..  In order to register this sensor, please run: prelude-adduser
 register prelude-lml "idmef:w" hostnamehere --uid 0 --gid 0  Profile 'prelude-lml' does not exist
. In order to create it, please run: prelude-adduser register prelude-lml "idmef:w" <manager addre
ss> --uid 0 --gid 0.
```

If im not lucky the box running the lml becomes inaccessable via ssh or concole until it is rebooted. I suspect that this might be solved be increasing fs.file-max in /etc/sysctrl however this is still untested. if it works a note should be added to the installation instructions about large installs.

I will provide more debuging information as I find it but this should be looked into

History

#1 - 07/12/2007 12:02 PM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

Hello Paul,

From your report, it isn't clear whether Prelude-Manager or Prelude-LML crash, or both? If one of them do, could you try to reproduce the issue under GDB, so that we can trace where the problem come from?

Another things is that the file descriptor limit is usually a per-process limit. Could you open a session on the machine where it occur (where you will be monitoring system logfile and cpu / memory usage), then attempt to reproduce the problem, to see what is the cause of the SSH/console inaccessibility.

Thanks,

#2 - 07/13/2007 10:28 PM - prmarino1-gmail-com -

I did some testing and I found this was caused by the default setting in ulimit -n of 1024.
the fix is to increase the nofile setting in /etc/security/limits.conf

```
*               -       nofile          4096
```

I will add this to the prelude-managet trouble shooting page latter tonight

To clarify what happened it seems like the prelude manager creates 3 fifos for each sensor that attaches to it (400 sensors * 3 fifos = 1200 files). The person who installed the prelude-manager on this host (not me) configured it to run as root rather than its own user. when the prelude-manager excided the maximum number of open files for the user it caused several other processs running as root to hang. The system lock out until a reboot was a side effect caused by an other process not being able to open files.

#3 - 07/19/2007 06:25 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to invalid

I'm marking this bug as Invalid since it was not Prelude-Manager related. Don't hesitate to add documentation to the wiki concerning the configuration for working around the 'Too many open files' problem.

Regards,

#4 - 04/29/2009 12:20 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude Manager

- Category deleted (3)