PRELUDE SIEM - Bug #1211

prelude-admin does not work on Debian after fresh install

06/23/2020 03:32 PM - Sebastian K

Status:	New	**Start date:**	06/23/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

I am trying to use prelude-admin on a Ubuntu-like system. In particular, I want to register to a server. Unfortunately, this is not possible.

When installing prelude 5.1.0 via sources, it does build successfully, but I get a single failed test during 'make check':

```
...
PASS: test-localename
../../test-driver: line 95:  6213 Aborted                 "$@" > $log_file 2>&1
FAIL: test-rwlock1
PASS: test-lock
...
```

The command 'prelude-admin' does show the help menu, but adding any argument or command, e.g. 'prelude-admin register' results in a SegFault (similar to another issue: https://www.prelude-siem.org/issues/1092). The log file states "Unexpected outcome 3".

Then I tried installing the binaries (v4.1.0) after removing everything with 'make uninstall' and rebooting the system. Following the docs, I installed it via

```
apt install prelude-utils
```

Now, I can execute the registration command like this without an SegFault:

```
prelude-admin register my_sensor_name "idmef:w" <x.x.x.x> --uid 0 --gid 0
```

This throws an error stating that

```
error creating directory /var/spool/prelude/my_sensor_name: No such file or directory.
```

I am root on this system, so it shouldn't be a kind of access issue. Also, the server works just fine.

Can somebody tell me, where these errors come from and how I can fix them?

Thanks in advance,
Sebastian

History

#1 - 06/23/2020 03:53 PM - Thomas ANDREJAK

Hello

Can you create the folder /var/spool/prelude and retry "prelude-admin register" ?

Regards