Cellular Network Infrastructure - Feature #4107
Start systemd services as non-root user
07/15/2019 06:56 AM - osmith

<table>
<thead>
<tr>
<th>Status: New</th>
<th>Start date: 07/15/2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority: High</td>
<td>Due date:</td>
</tr>
<tr>
<td>Assignee: msuraev</td>
<td>% Done: 10%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Spec Reference:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

laforge wrote in OS#3369:

Ideally, as far as possible, we should start them as non-root user (which may require changes to our systemd service files, etc. in the individual git repos - but that is fine!). Starting them as non-root will also means that any writes to unintended directories like ‘/’ will be discovered as they then would make the program start fail.

**Subtasks:**

Feature # 5684: Create osmocom user via OE recipe

**Related issues:**

<table>
<thead>
<tr>
<th>Related to Cellular Network Infrastructure - Bug #3369: no automatic testing ...</th>
<th>Resolved 06/29/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related to Cellular Network Infrastructure - Bug #4821: Update working dir in...</td>
<td>Stalled 10/20/2020</td>
</tr>
<tr>
<td>Related to OsmoGGSN (former OpenGGSN) - Bug #2250: OpenGGSN requires to run a...</td>
<td>Closed 05/10/2017</td>
</tr>
<tr>
<td>Related to Cellular Network Infrastructure - Bug #5669: Test .deb packages bu...</td>
<td>New 08/30/2022</td>
</tr>
<tr>
<td>Related to Cellular Network Infrastructure - Bug #5685: Dropping debian 10 (b...</td>
<td>Feedback 09/19/2022</td>
</tr>
<tr>
<td>Related to Cellular Network Infrastructure - Bug #5687: Document and implemen...</td>
<td>New 09/20/2022</td>
</tr>
</tbody>
</table>

**History**

#1 - 07/15/2019 06:56 AM - osmith
- Related to Bug #3369: no automatic testing of Debian/Ubuntu packages added

#2 - 12/01/2019 09:38 AM - laforge
- Priority changed from Normal to Low

#3 - 10/01/2020 02:42 PM - laforge

Programs like osmo-msc, osmo-sgsn, osmo-cbc, osmo-smc, osmo-hlr have no real time requirements or special needs in terms of raw networks sockets or tun devices. All of those should be executed as normal, non-privileged user from the start. This could be done via the systemd unit files. This could be done via the systemd unit files, or explicitly inside the osmocom programs via a privilege dropping approach.

For those above, we basically have three possible strategies:

- at least drop all privileges except those we really ever need in the specific proram (CAP_NET_RAW / CAP_NET_ADMIN / CAP_SYS_NICE). We can first constrain the permitted capabilities using cap_set_flag, then use prctl(PR_SET_KEEPCAPS, 1L) to keep capabilities while changing from root to non-root, and then change the user ID / group ID. [https://stackoverflow.com/a/13186076](https://stackoverflow.com/a/13186076) has a nice example
- if it is sufficient to perform those privileged operations once on start-up, we could even drop those capabilities after performing the operations like creating netdev, binding socket, changing scheduler policy. This would mean that no subsequent changes can be made later on.

09/22/2022
IMHO, we should start by

- create an osmocom user during package installation (if it doesn’t exist yet)
  - alternatively call it osmo-cni if osmocom is deemed too generic
- modify the systemd.service files to run the processes as that user
- modify /etc/osmocom and its contents to be owned by that user
- modify /var/lib/osmocom (HLR + SMS databases) to be owned by that user

For some programs, this is a no-brainer (e.g. BSC, MSC, SGSN)

For some others (TRX, BTS but possibly also MGW: SCHED_RR; GGSN: tun devices) we should work with capabilities, as described above.

laforge wrote:

IMHO, we should start by

- modify /etc/osmocom and its contents to be owned by that user

That’s untypical - do we want the programs to be able to change their own configs?

osmith wrote:

laforge wrote:

IMHO, we should start by

- modify /etc/osmocom and its contents to be owned by that user

That's untypical - do we want the programs to be able to change their own configs?

We should, otherwise the user cannot store back the running-config to the .cfg file through VTY command.

Some configs in /etc has non-root group. Assuming we also create osmocom group, we can have /etc/osmocom owned by root:osmocom while /etc/osmocom/osmo.bsc.cfg owned by osmocom:osmocom - that’s similar to how transmission-daemon handle its config files.
# Related to Bug #5669: Test .deb packages built by our OBS added

# Test .deb packages built by our OBS added

#13 - 08/30/2022 03:42 PM - msuraev

laforge wrote in **note-6**:

- modify /var/lib/oslomcom (HLR + SMS databases) to be owned by that user

Once #4821 is resolved, this point will be done automatically: systemd autoadjust the state dir permissions to match unit's User=/Group= settings.

#14 - 09/09/2022 02:52 PM - msuraev

To make sure no project is left behind let's summarize the current state

<table>
<thead>
<tr>
<th>Repo</th>
<th>Service</th>
<th>Status</th>
<th>Comment</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>osmo-hlr</td>
<td>osmo-hlr</td>
<td>review</td>
<td></td>
<td><a href="https://gerrit.osmocom.org/c/osmo-hlr/+/29311">https://gerrit.osmocom.org/c/osmo-hlr/+/29311</a></td>
</tr>
<tr>
<td>osmo-ggsn</td>
<td>osmo-ggsn</td>
<td>WIP</td>
<td>tun devices</td>
<td><a href="https://gerrit.osmocom.org/c/osmo-ggsn/+/29412">https://gerrit.osmocom.org/c/osmo-ggsn/+/29412</a></td>
</tr>
<tr>
<td>osmo-msc</td>
<td>osmo-msc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-gbproxy</td>
<td>osmo-gbproxy</td>
<td></td>
<td>CAP_NET_RAW</td>
<td></td>
</tr>
<tr>
<td>osmo-bsc</td>
<td>osmo-bsc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-mgw</td>
<td>osmo-mgw</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-sgsn</td>
<td>osmo-sgsn</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-sgsn</td>
<td>osmo-gtphub</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-hnbgw</td>
<td>osmo-hnbgw</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-hnodeb</td>
<td>osmo-hnodeb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-upf</td>
<td>osmo-upf</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-cbc</td>
<td>osmo-cbc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>libosmo-sccp</td>
<td>osmo-stp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-bts</td>
<td>/<em>-mgr</em>/</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-bts</td>
<td>osmo-bts-*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-pcu</td>
<td>osmo-pcu</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-trx</td>
<td>osmo-trx-*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-pcap</td>
<td>osmo-pcap-*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-smc</td>
<td>osmo-smc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-sip-connector</td>
<td>osmo-sip-connector</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-python-tests</td>
<td>osmo-trap2cgi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>osmo-python-tests</td>
<td>osmo-trap2cgi</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Have I missed anything?

#15 - 09/09/2022 03:01 PM - fixeria

We may also want to run osmo-pcu with SCHED_RR.

#16 - 09/09/2022 03:15 PM - pespin

This may be of use to list the projects: [https://osmocom.org/projects/cellular-infrastructure/wiki/Make_a_new_release#Dependency-graph](https://osmocom.org/projects/cellular-infrastructure/wiki/Make_a_new_release#Dependency-graph)

#17 - 09/18/2022 01:35 PM - msuraev

The example code adding user/group is available in [https://gerrit.osmocom.org/c/osmo-hlr/+/29311](https://gerrit.osmocom.org/c/osmo-hlr/+/29311)

The following tests were made:

- clean install
- upgrade from previous ("root") version
- upgrade from previous ("user") version
* writing config file via telnet
* package uninstall
* piuparts:

```
sudo piuparts osmo-hlr_1.5.0_amd64.deb libosmo-gsup-client0_1.5.0_amd64.deb libosmo-mslookup0_1.5.0_amd64.deb
libosmocore19_1.7.0_amd64.deb libosmogsm18_1.7.0_amd64.deb
...```

PASS: Installation, upgrade and purging tests.

In general, possible source of problem is mix-n-match between "root" and "user" packages where "root" package is installed after the "user", overriding permissions and disabling read/write access to config files. I'm not sure if it's worth investing time into dealing with that - seems like coordinating release so root->user transition happens simultaneously is easier.

#18 - 09/18/2022 02:43 PM - msuraev
laforge wrote in #note-3:

- osmo-ggsn requires CAP_NET_ADMIN for setting up the gtp0/tun0 devices (unless this is done externally before starting it)

At least for tun0 device we can install corresponding .network file in addition to .service with proper User/Group settings.

#19 - 09/18/2022 02:43 PM - msuraev
- % Done changed from 0 to 10

#20 - 09/19/2022 02:09 AM - msuraev
How should we deal with .spec files? Shall I update those as well?

Creating user during package install is a distro-specific thing. Are there some other distros we care about?

What about OE?

#21 - 09/19/2022 08:44 AM - osmith
msuraev wrote in #note-20:

How should we deal with .spec files? Shall I update those as well?

Creating user during package install is a distro-specific thing. Are there some other distros we care about?

What about OE?

As I understand, the systemd files get adjusted to expect the user to exist, and these systemd files are used in the rpms and on OE too. So we would need to make sure that the user exists there as well or else the systemd services wouldn't work there anymore.

#22 - 09/19/2022 01:16 PM - msuraev
- Related to Bug #5685: Dropping debian 10 (buster) added

#23 - 09/20/2022 09:11 AM - msuraev
Do we have some kind of hierarchy with regards to realtime scheduling? Like "osmo-pcu should have higher priority than osmo-trx" and such?

#24 - 09/20/2022 09:20 AM - pespin
msuraev I personally use:
osmo-trx-uhd.cfg: "policy rr 18"
osmo-bts-trx.cfg: "policy rr 1"
osmo-pcu.cfg: "policy rr 1"

#25 - 09/20/2022 12:54 PM - laforge
On Tue, Sep 20, 2022 at 09:11:35AM +0000, msuraev wrote:

Do we have some kind of hierarchy with regards to realtime scheduling? Like "osmo-pcu should have higher priority than osmo-trx" and such?

no, but I think for CNI it's relatively "obvious" to me:

- osmo-trx should be higher than anything else
- osmo-bts-* below osmo-trx
- osmo-mgw below osmo-bts-
- osmo-pcu below osmo-bts-
- everything else isn't really timing critical.

#26 - 09/20/2022 02:21 PM - msuraev
- Related to Bug #5687: Document and implement realtime scheduling hierarchy added

#27 - 09/20/2022 02:34 PM - pespin

laforge osmo-pcu now depends on getting FNs on time to calculate when to send stuff regarding scheduling, that's why I use same prio for osmo-bts and osmo-pcu.

#28 - 09/20/2022 02:44 PM - msuraev

Seems like it's not that obvious so the topic deserve ticket of its own - see #5687.