rsyslog funktioniert nicht in LXC-Containern

Wenn man rsyslog in LXC Containern nutzen möchte hat man das Problem das rsyslog nicht gleich läuft,
da die Funktionen als root-user ausgeführt werden und eigentlich nur der User "root" Zugriff auf die Logfiles hat.

wenn man den Befehl systemctl status rsyslog aufruft bekommt man folgende Ausgabe:

```
root@Container:/etc/systemd# systemctl status rsyslog
* rsyslog.service - System Logging Service
 Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
 Active: active (running) since Sat 2019-06-15 11:42:55 UTC; 14s ago
 Docs: man:rsyslogd(8)
 http://www.rsyslog.com/doc/
 Main PID: 21870 (rsyslogd)
 Tasks: 8 (limit: 629130)
 CGroup: /system.slice/rsyslog.service
 `-21870 /usr/sbin/rsyslogd -n

Jun 15 11:42:55 Container systemd[1]: Stopped System Logging Service.
Jun 15 11:42:55 Container systemd[1]: rsyslog.service: Failed to reset devices.list: Operation
not permitted
Jun 15 11:42:55 Container systemd[1]: rsyslog.service: Failed to set invocation ID on control
group /system.slice/rsyslog.service, ignoring: Operation not permitted
Jun 15 11:42:55 Container systemd[1]: Starting System Logging Service...
Jun 15 11:42:55 Container liblogging-stdlog[21870]:  [origin software="rsyslogd"
swVersion="8.24.0" x-pid="21870" x-info="http://www.rsyslog.com"] start
Jun 15 11:42:55 Container liblogging-stdlog[21870]: imklog: cannot open kernel log
(/proc/kmsg): Permission denied.
Jun 15 11:42:55 Container liblogging-stdlog[21870]: activation of module imklog failed [v8.24.0
try http://www.rsyslog.com/e/2145 ]
Jun 15 11:42:55 Container systemd[1]: Started System Logging Service.
```

Man muss den rsyslog dazu bewegen seine Privilegien zu ändern.

Damit Syslog lesend auf die Logfiles bzw auf das Filesystem /proc/kmgs (Kernelmessages) muss er vorher den Benutzer wechseln.

Man fügt in die Configurationsdatei folgendes ein:

Im Abschnitt Rules muss man die Zeile einfügen vor den anderen Kommandos:

```
#############
### RULES ###
#############

$PrivDropToUser nobody
```

Danach die Konfiguration speichern und rsyslog neu starten.

Danach sendet rsyslog ganz brav an den Log-Server.

Viel Spass beim Ausprobieren

Euer Admin