Subject: Re: User Seperation Issue
Posted by curx on Mon, 02 Feb 2009 20:31:59 GMT
View Forum Message <> Reply to Message

this is the correct way, on the hardware node you see all processes and effective uid/gid mapped to username depends on hardwarenodes /etc/passwd and groups to /etc/group

e.g: create a user in the container which has not been created on your hardwardnode, like a uid with 5555

on execute the ps on ct0/hardware node you will see the uid only, an has nothing to do with a seperation issue, only mapping the uid to the username set up in the hardwarenode's /etc/passwd

// running screen session with uid 5555, uid 5555 isnt setup in ct0/hardwarenode //

```
root      4715  0.0  0.0   1944   640 ?        Ss   20:36   0:00 init [2]
root      5302  0.0  0.0   1724   688 ?        Ss   20:36   0:00  \_ /sbin/syslogd
root      5421  0.0  0.1   4924  1084 ?        Ss   20:36   0:00  \_ /usr/sbin/sshd
root      5443  0.0  0.0   2192   756 ?        Ss   20:36   0:00  \_ /usr/sbin/cron
5555      6727  0.0  0.1   2768  1144 ?        Ss   21:09   0:00  \_ SCREEN
5555      6728  4.7  0.2   3996  2604 /var/lib/vz/root/102/dev/pts/1 Ss+ 21:09   0:00      \_ /bin/bash
```

warning:
if a user in your hardwarenode has the same uid like in your containers, the nonpriv user can kill processes running with the same uid in all containers.

e.g with icecast, the ct0 user carcheck can kill processes in container #2

```
$ su - carcheck
$ kill -9 12984 12694 12840
```

Bye,
Thorsten