Subject: User Seperation Issue
Posted by HostRail on Mon, 02 Feb 2009 17:11:01 GMT
View Forum Message <> Reply to Message

I have 2 VMs running.

The 2nd vm I setup I have shoutcast and icecast loaded.

But I see this from the host node top:

```
12984 carcheck  18348 3416 1644 S   16  0.1   1:19.48 ices2
12694 carcheck  24232 2204  756 S    6  0.1   0:30.61 sc_trans_linux
12840 carcheck  14364 2064 1384 S    5  0.1   0:23.43 ices
```

carcheck is the main user on VM 1. But its running the scripts from VM 2.

How can this be?

Subject: Re: User Seperation Issue
Posted by curx on Mon, 02 Feb 2009 20:00:02 GMT
View Forum Message <> Reply to Message

in your container the user running the icecast has the same uid (=userid) like in your hardwarenode and in your hardware node uid x is mapped to username carcheck.

Bye,
Thorsten

Subject: Re: User Seperation Issue
Posted by HostRail on Mon, 02 Feb 2009 20:02:39 GMT
View Forum Message <> Reply to Message

OK so are you saying this is the correct or incorrect way operating?

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

Subject: Re: User Seperation Issue
Posted by HostRail on Mon, 02 Feb 2009 20:41:16 GMT
View Forum Message <> Reply to Message

ok. So you are saying vm1 can change/kill proccesses on vz2?

So what stops commen users like nobody, apache, mysql, etc from conflicting?

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

Isn't this a huge security risk?

Subject: Re: User Seperation Issue
Posted by curx on Mon, 02 Feb 2009 21:06:23 GMT
View Forum Message <> Reply to Message

[quote title=HostRail wrote on Mon, 02 February 2009 21:41]ok. So you are saying vm1 can

change/kill proccesses on vz2?

ct0 = hardware node

no!, if you on hardwarenode and you have the same userid like the user in your container
its possbile to send signals from the hardwarenode to processes in the container like kill, term etc...

but if you a user in a container you doesnt see any processes of other containers context!

it isolate vm1 vm2 vm3 ... vmX but not the hardware node,
the hardware node is the "Achilles' heel"

Bye,
Thorsten

Subject: Re: User Seperation Issue
Posted by HostRail on Mon, 02 Feb 2009 21:09:27 GMT
View Forum Message <> Reply to Message

ok I see. So each container has its own set of users, groups, uids, pids?

But what the host node sees it may attribute the process to a different user?

thanks for your detailed answers!
