Subject: Re: [patch 0/8] unprivileged mount syscall
Posted by Miklos Szeredi on Mon, 09 Apr 2007 20:10:41 GMT
View Forum Message <> Reply to Message

> > The one in pam-0.99.6.3-29.1 in opensuse-10.2 is totally broken. Are
> > you interested in the details? I can reproduce it, but forgot to note
> > down the details of the brokenness.
>
> I don't know how far removed that is from the one being used by redhat,
> but assuming it's the same, then redhat-lspp@redhat.com will be
> very interested.

OK.

> > - user namespace setup: what if user has multiple sessions?
> >
> > 1) namespaces are shared? That's tricky because the session needs to
> > be a child of a namespace server, not of login. I'm not sure PAM
> > can handle this
> >
> > 2) or mounts are copied on login? That's not possible currently,
> > as there's no way to send a mount between namespaces. Also it's
> > tricky to make sure that new mounts are also shared
>
> See toward the end of the 'shared subtrees' OLS paper from last year for
> a suggestion on how to let users effectively 'log in to' an existing
> private mounts ns.

This?

1. create a new namespace
2. bind /share/$USER to /share
3. for each pair ($who, $what) such that
   /share/$USER/$who/$what exists, look
   in /share/$who/allowed for "peer $what
   $USER" or "slave $what $USER". If the
   former is found, rbind /share/$who/$what
   on /share/$USER/$who/$what; if the
   latter is found, do the same and
   follow with marking subtree under
   /share/$USER/$who/$what as slave.
4. rbind /share/$USER to /share
5. mark subtree under /share as private.
6. umount -l /share

Well, someone please explain using short words, because I don't
understand at all.

Thanks,
Miklos

_____

Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers