Subject: Re: [patch] unprivileged mounts update
Posted by Miklos Szeredi on Thu, 26 Apr 2007 19:56:26 GMT
View Forum Message <> Reply to Message

> Quoting Miklos Szeredi (miklos@szeredi.hu):
> > > So then as far as you're concerned, the patches which were in -mm will
> > > remain unchanged?
> >
> > Basically yes. I've merged the update patch, which was not yet added
> > to -mm, did some cosmetic code changes, and updated the patch headers.
> >
> > There's one open point, that I think we haven't really explored, and
> > that is the propagation semantics. I think you had the idea, that a
> > propagated mount should inherit ownership from the parent into which
> > it was propagated.
>
> Don't think that was me. I stayed out of those early discussions
> because I wasn't comfortable guessing at the proper semantics yet.

Yes, sorry, it was Eric's suggestion.

> But really, I, as admin, have to set up both propagation and user mounts
> for a particular subtree, so why would I *not* want user mounts to be
> propagated?
>
> So, in my own situation, I have done
>
> make / rshared
> mount --bind /share /share
> make /share unbindable
> for u in $users; do
>   mount --rbind / /share/$u/root
>   make /share/$u/root rslave
>   make /share/$u/root rshared
>   mount --bind -o user=$u /share/$u/root/home/$u /share/$u/root/home/$u
> done
>
> All users get chrooted into /share/$USER/root, some also get their own
> namespace. Clearly if a user in a new namespace does
>
> mount --bind -o user=me ~/somedir ~/otherdir
>
> then logs out, and logs back in, I want the ~/otherdir in the new
> namespace (and the one in the 'init' namespace) to also be owned by
> 'me'.
>
> > That sounds good if everyone agrees?
>

> I've shown where I think propagating the mount owner is useful. Can you
> detail a scenario where doing so would be bad? Then we can work toward
> semantics that make sense...

But in your example, the "propagated mount inherits ownership from parent mount" would also work, since in all namespaces the owner of the parent would necessary be "me".

The "inherits parent" semantics would work better for example in the "all nosuid" namespace, where the user is free to modify it's mount namespace.

If for example propagation is set up from the initial namespace to this user's namespace and a new mount is added to the initial namespace, it would be nice if the propagated new mount would also be owned by the user (and be "nosuid" of course).

Does the above make sense? I'm not sure I've explained clearly enough.

Miklos

_____

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