Subject: Re: [patch 8/9] unprivileged mounts: propagation: inherit owner from parent
Posted by serue on Tue, 15 Jan 2008 14:21:15 GMT
View Forum Message <> Reply to Message

Quoting Miklos Szeredi (miklos@szeredi.hu):
> > Quoting Miklos Szeredi (miklos@szeredi.hu):
> > > From: Miklos Szeredi <mszeredi@suse.cz>
> > >
> > > On mount propagation, let the owner of the clone be inherited from the
> > > parent into which it has been propagated. Also if the parent has the
> > > "nosuid" flag, set this flag for the child as well.
> >
> > What about nodev?
>
> Hmm, I think the nosuid thing is meant to prevent suid mounts being
> introduced into a "suidless" namespace. This doesn't apply to dev
> mounts, which are quite safe in a suidless environment, as long as the
> user is not able to create devices. But that should be taken care of
> by capability tests.
>
> I'll update the description.

Hmm,

Part of me wants to say the safest thing for now would be to refuse
mounts propagation from non-user mounts to user mounts.

I assume you're thinking about a fully user-mounted chroot, where
the user woudl still want to be able to stick in a cdrom and have
it automounted under /mnt/cdrom, propagated from the root mounts ns?

But then are there no devices which the user could create on a floppy
while inserted into his own laptop, owned by his own uid, then insert
into this machine, and use the device under the auto-mounted /dev/floppy
to gain inappropriate access?

-serge

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