Subject: Re: Re: [patch 05/10] add "permit user mounts in new namespace" clone flag
Posted by Ram Pai on Wed, 18 Apr 2007 19:41:07 GMT
View Forum Message <> Reply to Message

On Wed, 2007-04-18 at 21:14 +0200, Miklos Szeredi wrote:
> > As I said earlier, I see a case where two mounts that are peers of each
> > other can become un-identical if we dont propagate the "allowusermnt".
> >
> > As a practical example.
> >
> > /tmp and /mnt are peers of each other.
> > /tmp has its "allowusermnt" flag set, which has not been propagated
> > to /mnt.
> >
> > now a normal-user mounts an ext2 file system under /tmp at /tmp/1
> >
> > unfortunately the mount wont appear under /mnt/1
>
> Argh, that is not true. That's what I've been trying to explain to
> you all along.

I now realize you did, but I failed to catch it. sorry :-(

>
> The propagation will be done _regardless_ of the flag. The flag is
> only checked for the parent of the _requested_ mount. If it is
> allowed there, the mount, including any propagations are allowed. If
> it's denied, then obviously it's denied everywhere.
>
> > and in case if you allow the mount to appear under /mnt/1, you will
> > break unpriviledge mounts semantics which promises: a normal user will
> > not be able to mount at a location that does not allow user-mounts.
>
> No, it does not promise that. The flag just promises, that the user
> cannot _request_ a mount on the parent mount.

ok. if the ability for a normal user to mount something *indirectly*
under a mount that has its 'allowusermnt flag' unset,
is acceptable under the definition of 'allowusermnt', i guess my only
choice is to accept it. :-)

RP

>
> Miklos