Subject: Re: [patch 7/8] allow unprivileged mounts
Posted by Miklos Szeredi on Sun, 22 Apr 2007 08:19:54 GMT
View Forum Message <> Reply to Message

> > On Apr 21 2007 10:57, Eric W. Biederman wrote:
> >>
> >>> tmpfs!
> >>
> >>tmpfs is a possible problem because it can consume lots of ram/swap.
> >>Which is why it has limits on the amount of space it can consume.
> >
> > Users can gobble up all RAM and swap already today. (Unless they are
> > confined into an rlimit, which, in most systems, is not the case.)
> > And in case /dev/shm exists, they can already fill it without running
> > into an rlimit early.
>
> There are systems that care about rlimits and there is strong intersection
> between caring about rlimits and user mounts. Although I do agree that
> it looks like we have gotten lazy with the default mount options for
> /dev/shm.
>
> Going a little farther any filesystem that is safe to put on a usb
> stick and mount automatically should ultimately be safe for unprivileged
> mounts as well.

Actually, that's not as simple.

For the usb stick or cdrom you need physical access to the machine.
And once you have that you basically have full control over the system
anyway.

But with block filesystems, the user would still need access to the
device (currently kernel doesn't even check this I think).

So it may make sense to mark all block based filesystems safe, and
defer permission checking to user access on the block device.

But the safe flag is still needed for filesystems, which don't have
such an additional access checking, such as network filesystems.

Miklos

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