Subject: Re: [patch 05/10] add "permit user mounts in new namespace" clone flag
Posted by ebiederm on Fri, 13 Apr 2007 14:22:10 GMT
View Forum Message <> Reply to Message

"Serge E. Hallyn" <serue@us.ibm.com> writes:

> Quoting Miklos Szeredi (miklos@szeredi.hu):
>> > Given the existence of shared subtrees allowing/denying this at the mount
>> > namespace level is silly and wrong.
>> >
>> > If we need more than just the filesystem permission checks can we
>> > make it a mount flag settable with mount and remount that allows
>> > non-privileged users the ability to create mount points under it
>> > in directories they have full read/write access to.
>>
>> OK, that makes sense.
>>
>> > I don't like the use of clone flags for this purpose but in this
>> > case the shared subtress are a much more fundamental reasons for not
>> > doing this at the namespace level.
>>
>> I'll drop the clone flag, and add a mount flag instead.
>>
>> Thanks,
>> Miklos
>
> Makes sense, so then on login pam has to spawn a new user namespace and
> construct a root fs with no shared subtrees and with the
> user-mounts-allowed flag specified?

I was expecting the usage in the normal case to be the Al Viro style
with shared subtrees setup for each user, with the shared subtree marked
with user-mounts-allowed. Then on login pam would unshare the namespace
and restrict the user to their specific portion of the shared subtree.

If you don't use multiple mount namespaces all of the users have to
agree on what they want the non-privileged part of the namespace
to look like.

If you don't use shared subtrees you have to deal with all of the
joys of implementing enter, or else multiple logins from the same user
have problems.

Eric