Subject: Re: [PATCH 1/9] Add a user_namespace as creator/owner of uts_namespace
Posted by ebiederm on Wed, 23 Feb 2011 23:54:12 GMT
View Forum Message <> Reply to Message

David Howells <dhowells@redhat.com> writes:

> Eric W. Biederman <ebiederm@xmission.com> wrote:
>
>> > Which means that unless the uts_namespace belongs to our user_namespace, we
>> > cannot change it. Is that correct?
>>
>> No. If you are root in a parent namespace you can also change it.
>
> But surely, by definition, if you're a user in this namespace, you can't also
> be root in a parent namespace...

To be clear the case you looked at was:

> - if (!capable(CAP_SYS_ADMIN))
> + if (!ns_capable(current->nsproxy->uts_ns->user_ns, CAP_SYS_ADMIN))
>
> what is it you're actually asking? I presume it's 'does this user have
> CAP_SYS_ADMIN capability over objects belonging to the uts_namespace's
> user_namespace?'

Here "current->nsproxy->uts_ns->user_ns" (the target_ns value) is only
refers to the uts_ns we are talking about.

The user itself comes from current_user().

> For the case I worked through current_user() is a member of current_user_ns()
> and can't also be a member of its parent, grandparent, etc. - or can
> it?

Right now if you are looking at current_user() because of limitations in
the creation ordering I think you are correct.

However in the near term pile of changes to merge, are the syscalls for
joining an existing namespace. At which point there is no reason in
general to suppose the current limitations of creation apply.

Although it is conceivable that unshare of namespaces can also get you
to someplace similar to joining prexisting namespaces.

Eric

_____
Containers mailing list