Subject: Re: [RFC][PATCH 0/2] user namespace [try #2]
Posted by ebiederm on Thu, 31 Aug 2006 15:17:57 GMT
View Forum Message <> Reply to Message

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

> Quoting Cedric Le Goater (clg@fr.ibm.com):
>> Cedric Le Goater wrote:
>> > Hi all,
>> >
>> > Here's a second version. It's very close from the first one and takes into
>> > account some discussions we had with kirill on the topic during OLS. 2
>> > patches follow, the first introduces the user namespace core and the last
>> > enables to use it with unshare.
>> >
>> > Changes [try #2]
>> >
>> > - removed struct user_namespace* argument from find_user()
>> > - added a root_user per user namespace
>> >
>> > execns() syscall is back in the attic for the moment. I'm still maintaining
>> > it and we'll see if it's of any use when we address the user space API of
>> > the full conainer. soon, I hope !
>> >
>> > This user namespace patchset does not try to address all the issues that
>> > were raised by the previous thread on the topic, like user mapping per
>> > namespace, per mount, etc. It tries to solve some simple issues with the
>> > current implementation of containers in mind. It should be especially
>> > useful the existing solutions and lay ground basic objects.
>> >
>> > thanks for your comments,
>>
>> I didn't get much comments on that one. is everybody happy with it ? can we
>> merge ask andrew to merge in -mm ?
>>
>> thanks,
>
> Ideally we could collect Acked-by: or Signed-off-by: from Eric, Kir or
> Kirill, and Herbert or Sam, to show we are all in agreement.
>
> Or a NACK :)

Ok for the collection

Nacked-by: Eric Biederman

My gut feel is that this is terribly incomplete, and doesn't
come with enough description to tell me why it could possibly be complete.

I don't think this addresses any of my primary objections from last
round.

This doesn't change the kernel to make uid comparisons as (uid_ns, uid)
tuples or explain why that isn't necessary. It doesn't touch keys.
it doesn't explain why we are not introducing possibly subtle security problems.

Cedric sorry for not saying so earlier, but I thought that the incompleteness
was obvious.

Eric

_____

Containers mailing list
Containers@lists.osdl.org
https://lists.osdl.org/mailman/listinfo/containers