Subject: Re: [PATCH 4/4] The control group itself
Posted by Paul Menage on Tue, 15 Jan 2008 17:54:27 GMT
View Forum Message <> Reply to Message

On Jan 15, 2008 9:49 AM, Serge E. Hallyn <serue@us.ibm.com> wrote:
> > One other thought - should the parse/print routines themselves do a
> > translation based on the device mappings for the writer/reader's
> > cgroup? That way you could safely give a VE full permission to write
> > to its children's device maps, but it would only be able to add/remap
> > device targets that it could address itself.
>
> Oh, well if we do this then we can just as well use the translation
> functions to not allow a VE to add to its own set of devices, right?

Right.

>
> Then maybe capable(CAP_NS_OVERRIDE|CAP_SYS_ADMIN) would only be required
> to add devices.

Or simply require that they be added by someone who already has access
to that device via their own control group? The root cgroup would have
access to all devices.

Paul

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