Subject: Re: Re: [RFC][PATCH 0/2] user namespace [try #2]
Posted by dev on Tue, 12 Sep 2006 13:48:46 GMT
View Forum Message <> Reply to Message

Herbert Poetzl wrote:
> On Thu, Sep 07, 2006 at 08:09:38PM +0400, Kirill Korotaev wrote:
>
>>>>imho this in acceptable for OpenVZ as makes VE files to be
>>>>inaccessiable from host. At least this is how I understand your
>>>>idea... Am I correct?
>>>>
>>>>
>>>>
>>>>>I assume the list of other things we'll need to consider includes
>>>>> signals between user namespaces
>>>>> keystore
>>>>> sys_setpriority and the like
>>>>>I might argue that all of these should be sufficiently protected
>>>>>by proper setup by userspace. Can you explain why that is not
>>>>>the case?
>>>
>>>
>>>>>The same requirement (ability to send signals from host to VE)
>>>>>is also applicable to signals.
>>>
>>>
>>>at some point, we tried to move all cross context
>>>signalling (from the host to the guests) into a special
>>>context, but later on we moved away from that, because
>>>it was much simpler and more intuitive to handle the
>>>signalling with a separate syscall command
>
>
>>I'm not sure what a separate context is for, but a separate syscall
>>is definetely not a good idea.
>
>
> care to explain _why_ you think so?
cause duplicating syscalls with the same meaning but just working in a bit
different situations doesn't look good.

Kirill