

---

Subject: Re: [patch -mm 10/17] nsproxy: add unshare\_ns and bind\_ns syscalls  
Posted by [Cedric Le Goater](#) on Mon, 11 Dec 2006 15:21:05 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Eric W. Biederman wrote:

> clg@fr.ibm.com writes:

>

>> From: Cedric Le Goater <clg@fr.ibm.com>

>>

>> The following patch defines 2 new syscalls specific to nsproxy and

>> namespaces :

>>

>> \* unshare\_ns :

>>

>> enables a process to unshare one or more namespaces. this

>>       duplicates the unshare syscall for the moment but we

>> expect to diverge when the number of namespaces increases

>

> Are we out of clone flags yet? If not this is premature.

>

>> \* bind\_ns :

>>

>> allows a process to bind

>> 1 - its nsproxy to some identifier

>> 2 - to another nsproxy using an identifier or -pid

>

> NAK

>

> Don't use global identifiers. Use pids. i.e. struct pid \* for your

> identifiers. Is there is a reason pids are unsuitable?

(1) gives a little more freedom to the sysadmin managing its

(2) uses pids. do you also nak it ?

do you always have access to pid ?

> I'm also worried about the security implications of switching namespaces

> on a process. That is something that needs to be looked at very closely.

this is required by at least 3 products I know of.

> These two changes certainly don't belong in a single patch, and they

> certainly use a bit more explanation. syscalls are not something to

> add lightly. Because they must be supported forever.

agree.

C.

---

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

---