Subject: Re: - merge-sys_clone-sys_unshare-nsproxy-and-namespace.patch removed from -mm tree
Posted by Oleg Nesterov on Sun, 17 Jun 2007 16:30:04 GMT
View Forum Message <> Reply to Message

On 06/17, Oleg Nesterov wrote:
>
> However, nsproxy's code is full of strange unneeded get/put calls, for
> example:
>
> struct uts_namespace *copy_utsname(int flags, struct uts_namespace *old_ns)
> {
>   struct uts_namespace *new_ns;
>
>   BUG_ON(!old_ns);
>   get_uts_ns(old_ns);
>
>   if (!(flags & CLONE_NEWUTS))
>   return old_ns;
>
>   new_ns = clone_uts_ns(old_ns);
>
>   put_uts_ns(old_ns);
>   return new_ns;
> }

Perhaps I missed something again, but this looks wrong to me.

copy_utsname() assumes that old_ns != NULL. OK, it should not.

However, clone_uts_ns() returns NULL if kmalloc() fails.
create_new_namespaces() checks IS_ERR(new_ns), but IS_ERR(NULL) = false.
So the next copy_namespaces/unshare_nsproxy_namespaces will oops ?

The same for all ->xxx_ns fields.

Oleg.

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