
Subject: Re: NFS causing oops when freeing namespace
Posted by [Oleg Nesterov](#) on Wed, 17 Jan 2007 18:58:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

On 01/17, Daniel Hokka Zakrisson wrote:

>
> >> Call Trace:
> >> [> >> [> >> [> >> [> >> [> >> [> >> [> >> [> >> [> >> [> >> [> >> [>

> It was the only semi-plausible explanation I could come up with. I added a
> printk in do_exit right before exit_task_namespaces, where sighand was
> still set, and one right before the spin_lock_irq in lockd_down, where it
> had suddenly been set to NULL.

I can't reproduce the problem, but

```
do_exit:  
    exit_notify(tsk);  
    exit_task_namespaces(tsk);
```

the task could be reaped by its parent in between.

We should not use ->signal/->sighand after exit_notify().

Can we move exit_task_namespaces() up?

Oleg.

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