
Subject: Re: [PATCH] namespaces: introduce sys_hijack (v4)
Posted by [Cedric Le Goater](#) on Fri, 12 Oct 2007 09:30:33 GMT
[View Forum Message](#) <> [Reply to Message](#)

Serge E. Hallyn wrote:

```
> Quoting Serge E. Hallyn (serue@us.ibm.com):  
>> >From 945fe66259cd0cfdc2fe846287b7821e329a558c Mon Sep 17 00:00:00 2001  
>> From: sergeh@us.ibm.com <hallyn@kernel.(none)>  
>> Date: Tue, 9 Oct 2007 08:30:30 -0700  
>> Subject: [PATCH] namespaces: introduce sys_hijack (v4)  
>>  
>> Move most of do_fork() into a new do_fork_task() which acts on  
>> a new argument, task, rather than on current. do_fork() becomes  
>> a call to do_fork_task(current, ...).  
>>  
>> Introduce sys_hijack (for x86 only so far). It is like clone, but  
>> in place of a stack pointer (which is assumed null) it accepts a  
>> pid. The process identified by that pid is the one which is  
>> actually cloned. Some state - include the file table, the signals  
>> and sighand (and hence tty), and the ->parent are taken from the  
>> calling process.  
>>  
>> The effect is a sort of namespace enter. The following program  
>> uses sys_hijack to 'enter' all namespaces of the specified pid.  
>> For instance in one terminal, do  
>>  
>> mount -t cgroup -ons /cgroup  
>> hostname  
>> qemu  
>> ns_exec -u /bin/sh  
>> hostname serge  
>>     echo $$  
>>     1073  
>> cat /proc/$$/cgroup  
>> ns:/node_1073  
>>  
>> In another terminal then do  
>>  
>> hostname  
>> qemu  
>> cat /proc/$$/cgroup  
>> ns:/  
>> hijack 1073  
>> hostname  
>> serge  
>> cat /proc/$$/cgroup  
>> ns:/node_1073  
>>
```

>> sys_hijack is arch-dependent and is only implemented for i386 so far.
>>
>> Changelog:
>> Aug 23: send a stop signal to the hijacked process
>> (like ptrace does).
>> Oct 09: Update for 2.6.23-rc8-mm2 (mainly pidns)
>> Don't take task_lock under rcu_read_lock
>> Send hijacked process to cgroup_fork() as
>> the first argument.
>> Removed some unneeded task_locks.
>
> Thanks to Cedric for finding an oops when using pid namespaces. The
> following patch fixes the problem.

it works fine now.

Thanks !

C.

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