Subject: Kill in HN
Posted by molliver on Wed, 17 May 2006 09:45:16 GMT
View Forum Message <> Reply to Message

Hi,

Is there a way to only see the processes running on the Hardware node if you are logged onto the HN rather than seeing all processes. As I accidently just killed a process running on a VPS thinking it was running on the HN. Surely for security processes from VPS's should not appear listed on the HN otherwise if the main HN gets attacked then anything can be done.

Mark

Subject: Re: Kill in HN
Posted by dev on Wed, 17 May 2006 10:37:54 GMT
View Forum Message <> Reply to Message

You can try the following simple patch for this:

--- ./fs/proc/base.c.procstr 2006-05-11 13:05:40.000000000 +0400
+++ ./fs/proc/base.c 2006-05-17 14:33:14.000000000 +0400
@@ -1745,6 +1745,8 @@ static int get_tgid_list(int index, unsi
  int tgid = get_task_pid_ve(p, owner);
  if (!pid_alive(p))
   continue;
+ if (!ve_accessible_strict(get_exec_env(), VE_TASK_INFO(p)->owner_env))
+   continue;
  if (--index >= 0)
   continue;
  tgids[nr_tgids] = tgid;

Subject: Re: Kill in HN
Posted by molliver on Wed, 17 May 2006 11:17:29 GMT
View Forum Message <> Reply to Message

Hi,

I take it that was a patch to the release stable kernel?

Thanks

Mark

Subject: Re: Kill in HN
Posted by dev on Wed, 17 May 2006 11:21:54 GMT
View Forum Message <> Reply to Message

yup. against stable 2.6.8.

Subject: Re: Kill in HN
Posted by John Kelly on Wed, 17 May 2006 16:12:53 GMT
View Forum Message <> Reply to Message

molliver wrote on Wed, 17 May 2006 05:45I accidently just killed a process running on a VPS thinking it was running on the HN.

Mistakes can be catastrohpic when logged in as root. On HN, you are "superroot." Why use HN to kill processes? OpenVZ recommends running only sshd on the HN.

molliver wrote on Wed, 17 May 2006 05:45Surely for security processes from VPS's should not appear listed on the HN otherwise if the main HN gets attacked then anything can be done.

This is the architecture. If you accept it and work with it, OpenVZ is a good solution for many needs. If you work against it, who can you blame besides yourself?

Subject: Re: Kill in HN
Posted by kir on Thu, 18 May 2006 22:23:58 GMT
View Forum Message <> Reply to Message

Seeing all the VPS processes (and files) and ability to do vzctl enter from the hardware node is a principle of OpenVZ. That makes VE mass management and troubleshooting possible. If something is wrong with the VPS, you can kill it from the host system.

At the same time, you are right, this is not good for security. Thus we do not recommend to run anything but the very basic stuff on the hardware node itself -- ideally, the only network port opened on hardware node is port 22, sshd. If you want to run anything else - create a VE and run it in this dedicated VE.