Subject: Re: Q: hardcoded parameters and restrictions
Posted by ldv on Thu, 24 Aug 2006 20:56:23 GMT
View Forum Message <> Reply to Message

Hi,

On Thu, Aug 24, 2006 at 03:30:38PM +0400, Kirill Korotaev wrote:
> Dmitry V. Levin wrote:
> >On Tue, Aug 22, 2006 at 03:06:56PM +0400, Kirill Korotaev wrote:
[...]
> >>>In particular, I mean HOME and PATH environment variables,
> >>
> >>do you mean HOME and PATH which are provided to VPS init?
> >
> >Yes, I mean VPS init, vzctl exec and vzctl enter.
> >
> >>mmm, probably can be made configurable from vps.conf
> >>do you think it is required?
> >
> >I think this is required since each distro has own PATH policy.
> from kernel init/main.c:
> static char * argv_init[MAX_INIT_ARGS+2] = { "init", NULL, };
> char * envp_init[MAX_INIT_ENVS+2] = { "HOME=/", "TERM=linux", NULL, };
>
> i.e. each init is run almost w/o any environment.
> the same for VE.

I agree, lets leave "init" case unchanged.

> on VE enter bash initializes PATH, HOME according to it's scripts.
> So the only "bad" case I see is vzctl exec, right?

Not only "exec", but also "enter", because bash does its initialization
depending on $HOME.

[...]
> >Unfortunately, /proc is notorious to had security-related bugs in the past,
> >including arbitrary code execution in kernel space. Since I'm not sure
> >that all such bugs are fixed, and since not all tasks require /proc to be
> >mounted, I'd like to be able to disable /procfs on per-VPS basis.
> Modern glibc (at least version from FC5) even doesn't work w/o /proc.
> We had a bug with cp due to this :/

No, that was a bug in FC5 coreutils package, fixed in their
coreutils-5.96-1.1 update.

> But in general I don't mind to make everything configurable.
>

> How do you see it? via the same "features" mask as done with sysfs?

To make just procfs configurable like sysfs, features mask should be enough.

> any other features? I think it is better to create a set of
> env_create funtions allowing vzctl to control which features a initialized
> in VE.

It depends on how much features will be made configurable.

> >>>Also, it seems to be no way to disable devices listed in
> >>>default_minor_perms.
> >>
> >>applications do not work w/o /dev/null and others at all :)
> >
> >Yes, /dev/null and /dev/zero are not an issue.
> >I care about /dev/random; how to deal with potential lack of randomness
> >in the system?
> Good point.
> let's move this into vzctl?
> lets start from this one.
> http://bugzilla.openvz.org/show_bug.cgi?id=241

OK

--
ldv