Subject: "vzctl stop" is taking too much time when called from a setuid binary
Posted by scythe on Tue, 23 May 2006 22:09:30 GMT
View Forum Message <> Reply to Message

Hi!

I wrote a simple setuid binary to be able to call "vzctl stop" as a non-root user.
After compiling the binary and making it setuid it takes about 5 minutes for it to run the simple command "vzctl stop VSID". It completes successfully, but only after this delay.
Running the same command from a root shell or with sudo takes less then 10 seconds.

I attached the source of the small program.
If you run it as root it completes at normal time.
If you run it as an other user it takes a few minutes
(at least on my system, which got only 3 vps-es).

Any ideas what may cause this wait?

File Attachments
1) vzstop.tgz, downloaded 444 times

Subject: Re: "vzctl stop" is taking too much time when called from a setuid binary
Posted by RapidVPS on Wed, 24 May 2006 00:59:19 GMT
View Forum Message <> Reply to Message

if you strace the program when you run it, you should be able to see what calls the program is waiting on. ie..

strace -ff vzctl2 stop 1234

it will display a ton of text, then it should stop for a while or loop. send us that text and we may be able to help..

Rick

Subject: Re: "vzctl stop" is taking too much time when called from a setuid binary
Posted by scythe on Wed, 24 May 2006 08:13:43 GMT
View Forum Message <> Reply to Message

Hi, and thanks for your help!

Unfortunately I found out that strace is not really capable of tracing setuid programs, only when

run as root and supplied the -u parameter.

I tried this method of stracing my vzstop program, but it just completed normally under a few secs.

The other strange thing is that vzctl start is completing in time even when forked form the setuid binary.

I also forgot to tell that im using kernel 2.6.16 - 026test009 with utilities 3.0.0-7, which are not to most recent beta kernel and tools. I upgrade them, if anything changes I will say so.

Subject: Re: "vzctl stop" is taking too much time when called from a setuid binary
Posted by Vasily Tarasov on Wed, 24 May 2006 08:56:16 GMT
View Forum Message <> Reply to Message

When vzctl stops VPS it does something like that:
1) forks process. This child process enters VPS
2.1) Child process executes "halt" command inside VPS
2.2) parent process waits for VPS dead. <---------- HERE IS YOUR ~5 MINUTS
3) If VPS isn't stopped for some time parent process stops it more roughly: kills init inside VPS.

The question is why child process doesn't execute "halt"?
The reason is that vzctl uses getenv("PATH") standard function,
that returns environment variable PATH. It's nessecary to determine the location of halt command.
Unfortunately getenv() returns variable from your user environment - not root environment. And there is no /sbin in PATH, where halt usually resides...

So you can add /sbin in PATH (or where is halt in your vps?).
I rewrote a little your programm - it works quckly now. It's in attachment.

HTH!

File Attachments
1) vzstop.c, downloaded 456 times

Subject: Re: "vzctl stop" is taking too much time when called from a setuid binary
Posted by scythe on Wed, 24 May 2006 09:13:26 GMT
View Forum Message <> Reply to Message

Hi!

Thank you, that solved the problem.
(I feel a bit dumb, I could have tought about the environment)

Thanks again!
