
Subject: *SOLVED* VE capabilities
Posted by [dagr](#) on Fri, 30 Mar 2007 11:07:04 GMT
[View Forum Message](#) <> [Reply to Message](#)

How can i see the current list of capabilities of VE?
And where can i find description what are they for - couldnt find in wiki.

You can use the following values for capname: chown, dac_override, dac_read_search, fowner, fsetid, kill, setgid, setuid, setpcap, linux_immutable, net_bind_service, net_broadcast, net_admin, net_raw, ipc_lock, ipc_owner, sys_module, sys_rawio, sys_chroot, sys_ptrace, sys_pacct, sys_admin, sys_boot, sys_nice, sys_resource, sys_time, sys_tty_config, mknod, lease, setveid, ve_admin.

Subject: Re: VE capabilities
Posted by [Vasily Tarasov](#) on Fri, 30 Mar 2007 11:53:37 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

well, you can obtain information about what capabilities are on by inspecting /proc/<pid>/status file of any process in VE. For example:

```
[root@white ~]# vzctl enter 1
entered into VE 1
[root@white /]# cat /proc/1/status
Name:  init.real
State:  S (sleeping)
SleepAVG:  98%
Tgid:  1
Pid:  1
PPid:  0
TracerPid:  0
FNid:  1
Uid:  0  0  0  0
Gid:  0  0  0  0
FDSize: 256
Groups: 0 1 2 3 4 6 10
envID: 1
VPid:  1
PNState:  0
StopState:  0
VmPeak:  1628 kB
VmSize:  1624 kB
VmLck:  0 kB
VmHWM:  600 kB
```

VmRSS: 600 kB
VmData: 184 kB
VmStk: 16 kB
VmExe: 28 kB
VmLib: 1360 kB
VmPTE: 16 kB
Threads: 1
SigQ: 0/36864
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: ffffffff57f0d8fc
SigCgt: 00000000280b2603
SigSvd: 0000000000000000
CapInh: 000000005dcceeff
CapPrm: 000000005dcceeff
CapEff: 000000005dcceeff
TaskUB: 1
MMUB: 1

This part concerns capabilities:

CapInh: 000000005dcceeff
CapPrm: 000000005dcceeff
CapEff: 000000005dcceeff

The only question is how to translate these digits into something more meaningful? Well, you can dig in kernel sources and investigate it. You can even write a tool (or kernel patch), that will extract needed information to VE0. Then we'll include it in OpenVZ

Vasily

Subject: Re: VE capabilities
Posted by [dagr](#) on Fri, 30 Mar 2007 12:08:02 GMT
[View Forum Message](#) <> [Reply to Message](#)

very strange - you give tool to set/unset property. At the same time nobody can say, if this property was set before . Not saying about unclear meaning . For instance "ve_admin" - can it give some more features to VE, or is it set already by default ? Quite confusing to find it in man vzctl and nowhere else.

Subject: Re: VE capabilities
Posted by [Vasily Tarasov](#) on Fri, 30 Mar 2007 12:14:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

I agree, it is a big field for work, but this functionality (I mean adding/removing capabilities to VE) is utilized very seldom and this is the reason why nobody has tried to implement it.

Subject: Re: VE capabilities
Posted by [curx](#) on Fri, 30 Mar 2007 12:52:55 GMT
[View Forum Message](#) <> [Reply to Message](#)

Maybe its possible to virtualize the /proc/sys/kernel/cap-bound to VE so the program lcap can show the used capabilities ?

Subject: Re: VE capabilities
Posted by [Vasily Tarasov](#) on Fri, 30 Mar 2007 13:55:40 GMT
[View Forum Message](#) <> [Reply to Message](#)

Good idea! For me it seems to be a very good solution. Can you post a bug in bugzilla about it?

Thanks,
Vasily.

Subject: Re: VE capabilities
Posted by [curx](#) on Fri, 30 Mar 2007 14:13:16 GMT
[View Forum Message](#) <> [Reply to Message](#)

done, http://bugzilla.openvz.org/show_bug.cgi?id=524
