

---

Subject: init process has other than root group ID  
Posted by [alessio55](#) on Sat, 03 Apr 2010 05:13:05 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

When a container boots, init and other processes started by it (sshd, xinetd, etc) are reported (by top) running under user root, but the group for them is not root, but is somewhere in the range 500+ (on a fresh install without any users /etc/passwd has nothing for those numbers yet). So it looks like pid is virtualized and gid is not. Is this normal for OpenVZ? The consequence is that there are a bunch of files created by those processes in /etc and /var that normally would have group root, but in OpenVZ container have group of a regular user, which is not great for security reasons. Anybody else seeing this (start top, then Shift-F,F,Enter to get top to show group)?

---

---

Subject: Re: init gid is not root  
Posted by [curx](#) on Sat, 03 Apr 2010 09:37:27 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hi,

have you used a precompiled OpenVZ OS-Template or used a downloaded Template (distribution ?)

Bye,  
Thorsten

---

---

Subject: Re: init gid is not root  
Posted by [alessio55](#) on Sat, 03 Apr 2010 09:50:21 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

I don't know. It is on VPS that I am renting. I know they are running SolusVM. They could not explain to me why it is like that.

```
uname -a
Linux ****.com 2.6.18-164.11.1.el5.028stab068.5 #1 SMP Mon Mar 15 19:26:36 MSK 2010
x86_64 x86_64 x86_64 GNU/Linux
```

```
cat /etc/redhat-release
CentOS release 5.4 (Final)
```

---

---

Subject: Re: init gid is not root  
Posted by [curx](#) on Sun, 04 Apr 2010 16:43:23 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

> (...) files created by those processes in /etc and /var (...)

plz post:

```
$ ls -la /  
$ ls -la /etc/<FILES>  
$ ls -la /var/<FILES>
```

Bye,  
Thorsten

---

---

Subject: Re: init gid is not root  
Posted by [alessio55](#) on Sun, 04 Apr 2010 17:16:37 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

I cannot do it anymore, since I fixed group ownership for them already. Those were mostly config files created in the process of installation of various packages and system configuration. A lot of webmin and virtualmin files. Right now only the files that are re-created on every boot have wrong group or whichever config files that I edit through webmin.

```
top - 13:18:24 up 12:32, 1 user, load average: 0.00, 0.00, 0.00  
Tasks: 41 total, 1 running, 40 sleeping, 0 stopped, 0 zombie  
Cpu(s): 0.0%us, 0.2%sy, 0.0%ni, 99.8%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st  
Mem: 1048576k total, 87432k used, 961144k free, 0k buffers  
Swap: 0k total, 0k used, 0k free, 0k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	GROUP	COMMAND
1702	root	15	0	12064	1716	1280	S	0.0	0.2	0:00.01	root	bash
3495	root	15	0	12608	1236	948	R	0.0	0.1	0:00.04	root	top
25767	root	18	0	61728	2500	1852	S	0.0	0.2	0:00.13	root	dovecot-auth
3312	postfix	15	0	54204	2256	1744	S	0.0	0.2	0:00.00	postfix	anvil
25672	postfix	15	0	55100	2248	1748	S	0.0	0.2	0:00.00	postfix	pickup
30629	postfix	15	0	54388	2388	1828	S	0.0	0.2	0:00.00	postfix	qmgr
30638	postfix	15	0	54204	2328	1812	S	0.0	0.2	0:00.03	postfix	tlsmgr
25836	nobody	15	0	51532	1580	576	S	0.0	0.2	0:00.00	nobody	proftpd
1994	dovecot	15	0	33892	2244	1780	S	0.0	0.2	0:00.00	dovecot	pop3-login
3206	dovecot	15	0	33892	2244	1780	S	0.0	0.2	0:00.00	dovecot	pop3-login

```

3239 dovecot  15  0 33892 2244 1780 S 0.0 0.2 0:00.00 dovecot  pop3-login
25833 dovecot  15  0 33896 2256 1792 S 0.0 0.2 0:00.00 dovecot  imap-login
25834 dovecot  15  0 33896 2260 1792 S 0.0 0.2 0:00.01 dovecot  imap-login
25835 dovecot  15  0 33896 2256 1792 S 0.0 0.2 0:00.01 dovecot  imap-login
25853 apache   15  0 246m 4196  492 S 0.0 0.4 0:00.00 apache   httpd
25894 apache   18  0 334m 9876 2448 S 0.0 0.9 0:00.08 apache   httpd
25895 apache   15  0 334m 10m 3116 S 0.0 1.0 0:00.05 apache   httpd
25896 apache   15  0 334m 10m 3192 S 0.0 1.0 0:00.04 apache   httpd
25897 apache   15  0 334m 10m 3216 S 0.0 1.0 0:00.05 apache   httpd
25898 apache   15  0 334m 9992 2524 S 0.0 1.0 0:00.04 apache   httpd
25899 apache   18  0 334m 10m 3040 S 0.0 1.0 0:00.04 apache   httpd
25900 apache   15  0 334m 10m 3236 S 0.0 1.0 0:00.08 apache   httpd
25901 apache   18  0 334m 10m 3172 S 0.0 1.0 0:00.04 apache   httpd
25902 apache   15  0 334m 10m 3120 S 0.0 1.0 0:00.06 apache   httpd
25903 apache   17  0 334m 10m 3060 S 0.0 1.0 0:00.05 apache   httpd

  1 root      15  0 10348  748  624 S 0.0 0.1 0:00.00 alessio   init
1623 root      16  0 87976 3268 2552 S 0.0 0.3 0:00.02 alessio   sshd
1680 alessio    18  0 88120 1952 1112 S 0.0 0.2 0:00.02 alessio   sshd
1683 alessio    15  0 12064 1640 1284 S 0.0 0.2 0:00.00 alessio   bash
1701 root      15  0 47096 1436 1116 S 0.0 0.1 0:00.00 alessio   su
24358 root      16 -4 12604  676  360 S 0.0 0.1 0:00.00 alessio   udevd
25714 root      15  0  5908  620  500 S 0.0 0.1 0:00.04 alessio   syslogd
25738 root      15  0 62632 1216  652 S 0.0 0.1 0:00.00 alessio   sshd
25758 root      18  0 21644  928  716 S 0.0 0.1 0:00.00 alessio   xinetd

```

25766	root	15	0	6052	664	512	S	0.0	0.1	0:00.12	alessio	dovecot
25820	root	15	0	55036	2284	1752	S	0.0	0.2	0:00.17	alessio	master
25847	root	15	0	334m	15m	8256	S	0.0	1.5	0:00.09	alessio	httpd
25856	root	15	0	20876	1188	592	S	0.0	0.1	0:00.00	alessio	crond
25864	root	18	0	48836	1264	812	S	0.0	0.1	0:00.06	alessio	saslauthd
25865	root	18	0	48836	1196	744	S	0.0	0.1	0:00.06	alessio	saslauthd
25917	root	18	0	71840	8924	1676	S	0.0	0.9	0:00.50	alessio	miniserv.pl

```

/etc/sysconfig/network-scripts/ifcfg-venet0:0
/etc/sysconfig/network-scripts/ifcfg-venet0
/etc/webmin/webmin/history
/etc/webmin/webmin/history/memused
/etc/webmin/webmin/history/maxes
/etc/webmin/webmin/history/procs
/etc/webmin/webmin/history/load15
/etc/webmin/webmin/history/cpuio
/etc/webmin/webmin/history/bin
/etc/webmin/webmin/history/bout
/etc/webmin/webmin/history/load
/etc/webmin/webmin/history/cpuuser
/etc/webmin/webmin/history/netcounts
/etc/webmin/webmin/history/load5
/etc/webmin/webmin/history/diskused
/etc/webmin/webmin/history/cpuidle
/etc/webmin/webmin/history/cpukernel
/etc/webmin/webmin/info
/etc/webmin/virtual-server-theme/sections.root
/etc/webmin/virtual-server-theme/sections
/etc/webmin/module.infos.cache
/etc/webmin/package-updates/updates.cache
/etc/webmin/package-updates/current.cache
/etc/webmin/virtual-server/nospam/127024058129970
/etc/resolv.conf
/etc/rc.d/rc1.d/S10vzquota
/etc/rc.d/rc4.d/S10vzquota
/etc/rc.d/rc0.d/S10vzquota
/etc/rc.d/rc6.d/S10vzquota
/etc/rc.d/rc3.d/S10vzquota
/etc/rc.d/rc5.d/S10vzquota
/etc/rc.d/rc2.d/S10vzquota

```

/etc/postfix/main.cf  
/aquota.group  
/aquota.user  
/var/lib/dovecot/ssl-parameters.dat  
/var/lib/rpm/\_\_db.002  
/var/lib/rpm/\_\_db.003  
/var/lib/rpm/\_\_db.001  
/var/cache/yum/virtualmin/repomd.xml  
/var/cache/yum/virtualmin/cachecookie  
/var/cache/yum/virtualmin/primary.xml.gz  
/var/cache/yum/virtualmin/primary.xml.gz.sqlite  
/var/cache/yum/rpmforge/repomd.xml  
/var/cache/yum/rpmforge/cachecookie  
/var/cache/yum/rpmforge/primary.xml.gz  
/var/cache/yum/rpmforge/primary.xml.gz.sqlite  
/var/cache/yum/rpmforge/mirrorlist.txt  
/var/cache/yum/timedhosts.txt  
/var/cache/yum/extras/repomd.xml  
/var/cache/yum/extras/primary.sqlite  
/var/cache/yum/extras/cachecookie  
/var/cache/yum/extras/mirrorlist.txt  
/var/cache/yum/virtualmin-universal/repomd.xml  
/var/cache/yum/virtualmin-universal/cachecookie  
/var/cache/yum/virtualmin-universal/primary.xml.gz  
/var/cache/yum/virtualmin-universal/primary.xml.gz.sqlite  
/var/cache/yum/updates/repomd.xml  
/var/cache/yum/updates/primary.sqlite  
/var/cache/yum/updates/cachecookie  
/var/cache/yum/updates/mirrorlist.txt  
/var/cache/yum/addons/repomd.xml  
/var/cache/yum/addons/cachecookie  
/var/cache/yum/addons/primary.xml.gz  
/var/cache/yum/addons/primary.xml.gz.sqlite  
/var/cache/yum/addons/mirrorlist.txt  
/var/cache/yum/base/repomd.xml  
/var/cache/yum/base/primary.sqlite  
/var/cache/yum/base/cachecookie  
/var/cache/yum/base/mirrorlist.txt  
/var/lock/subsys/saslauthd  
/var/lock/subsys/xinetd  
/var/lock/subsys/dovecot  
/var/lock/subsys/syslog  
/var/lock/subsys/local  
/var/lock/subsys/webmin  
/var/lock/subsys/network  
/var/lock/subsys/proftpd  
/var/lock/subsys/iptables  
/var/lock/subsys/httpd

/var/lock/subsys/postfix  
/var/lock/subsys/crond  
/var/lock/subsys/sshd  
/var/webmin/miniserv.pid  
/var/run/saslauthd/mux  
/var/run/saslauthd/mux.accept  
/var/run/saslauthd/saslauthd.pid  
/var/run/dovecot/dict-server  
/var/run/dovecot/master.pid  
/var/run/dovecot/login/ssl-parameters.dat  
/var/run/fcgid\_shm  
/var/run/xinetd.pid  
/var/run/syslogd.pid  
/var/run/httpd.pid  
/var/run/crond.pid  
/var/run/sshd.pid  
/usr/libexec/webmin/postfix/postfinger.15551.d  
/usr/libexec/webmin/postfix/postfinger.15551.n  
/tmp/.webmin/458785\_1\_right.cgi  
/tmp/.webmin/508412\_1\_right.cgi  
/tmp/.webmin/36711\_1\_right.cgi  
/tmp/.webmin/396838\_1\_right.cgi  
/tmp/.webmin/236818\_1\_right.cgi  
/dev  
/dev/log  
/dev/simfs  
/dev/initctl  
/dev/mapper  
/dev/md0  
/dev/.udev  
/dev/.udev/uevent\_seqnum  
/dev/X0R  
/dev/MAKEDEV  
/dev/core  
/dev/shm

---

Subject: Re: init gid is not root

Posted by [curx](#) on Mon, 05 Apr 2010 11:01:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

---8<...

(...)

1 root 15 0 10348 748 624 S 0.0 0.1 0:00.00 alessio init

-----^

(...)

---8<...

plz check your /etc/group file

Bye,  
Thorsten

---

---

Subject: Re: init gid is not root  
Posted by [alessio55](#) on Mon, 05 Apr 2010 12:40:03 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

The file merely provides numeric group ID to group name mapping. When a fresh new VSP is created with only root and no user accounts yet, there is no even group name in top, just a numeric group ID like 500 (I also saw 501 and 503 on different nodes) instead of 0 for root.

---

---

Subject: Re: init gid is not root  
Posted by [curx](#) on Mon, 05 Apr 2010 14:32:14 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

on a test template i can reproduce this behaviour :

1)  
Set sticky bit change group to not existant group 666

```
$ chmod g+s /sbin/init  
$ chown :666 /sbin/init
```

2) reboot  
after a ct (re)start and top

---8<...

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	GROUP	COMMAND
1	root	15	0	1980	684	592	S	0	0.3	0:00.02	666	init
3875	root	15	0	33136	1220	936	S	0	0.5	0:00.00	666	rsyslogd
3884	root	23	0	5276	1000	648	S	0	0.4	0:00.00	666	sshd
3899	root	15	0	2036	792	640	S	0	0.3	0:00.00	666	cron

---8<...

seems this prob occures on a "bug" on creating the OS template  
check on a "fresh" OS template:

```
$ ls -la /  
(...)  
$ ls -la /sbin/init  
-rwxr-xr-x 1 root root (...)
```

are in your template any sticky bits set, like

-rwxr-sr-x 1 root <anynumbergroup> (...)

Bye,  
Thorsten

---

---

Subject: Re: init gid is not root  
Posted by [alessio55](#) on Tue, 06 Apr 2010 05:23:02 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

I don't have access to the template on the host, but in my VPS I have it correct:  
-rwxr-xr-x 1 root root 40968 Jan 21 2009 /sbin/init

---