Subject: /dev (devtmpfs) permissions is 1777
Posted by umask on Mon, 15 Oct 2012 14:30:02 GMT
View Forum Message <> Reply to Message

Hello,

Please suggest me how it happens.

Case 1. On started container:

vzctl exec2 777 "ls -lad /dev"
drwxrwxrwt 8 root root 2440 Oct 15 18:07 /dev

ls -lad /vz/private/777/dev
drwxr-xr-x 3 root root 4.0K Oct 15 18:07 /vz/private/777/dev

ls -lad /vz/root/777/dev
drwxrwxrwt 8 root root 2.4K Oct 15 18:07 /vz/root/777/dev

Case 2. On stopped container:
ls -lad /vz/private/777/dev
drwxr-xr-x 3 root root 4.0K Oct 15 18:07 /vz/private/777/dev

This problem happened on Scientific Linux 6 x86_64 container which created from precreated template (http://download.openvz.org/template/precreated/scientific-6- x86_64.tar.gz).

The problem here is that /dev has permissions like /tmp (1777). Probably this may follow to security issues/vulnerabilities.

I checked that CentOS 6 x86_64 precreated template has the same issue.

Both container and HW node running on Scientific Linux/Centos 6 x86_64.

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by umask on Mon, 15 Oct 2012 14:39:56 GMT
View Forum Message <> Reply to Message

I noticed this problem some time ago.

I suspected that reason of problem is in precreated templates.

For check this fact I wrote script which creates el6 (based on centos) container from scratch:

```
#!/bin/bash -x

TMPDIR=$(mktemp -d)

vzctl stop 777

DESTDIR=/vz/private/777

[[ -d ${DESTDIR} ]] && rm -rf ${DESTDIR}

mkdir -p ${DESTDIR}

rpm --root ${DESTDIR} --initdb

yum install -y yum-utils

yumdownloader --destdir ${TMPDIR} centos-release centos-release-cr

TO_INSTALL=""
for i in ${TMPDIR}/*.rpm; do
 TO_INSTALL="${TO_INSTALL} ${i}"
done
rpm --root ${DESTDIR} -i ${TO_INSTALL}

# Save random seed
touch ${DESTDIR}/var/lib/random-seed
chmod 600 ${DESTDIR}/var/lib/random-seed
dd if=/dev/urandom of=/var/lib/random-seed count=1 bs=512 2>/dev/null

rpm --root ${DESTDIR} --import /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

yum --installroot=${DESTDIR} install -y postfix filesystem tzdata glibc procps \
 coreutils rpm yum yum-utils udev openssh basesystem bash grep MAKEDEV \
 openssl gnupg2 logrotate rsyslog screen openssh-server openssh-clients \
 info ca-certificates libuuid sed vim-enhanced findutils iproute tmpwatch \
 wget curl patch vixie-cron sysstat htop telnet which diffutils rsync \
 sudo yum-cron psacct lftp tcpdump numactl git vconfig nc xz bzip2 \
 nscd

cat << _EOF_ > ${DESTDIR}/etc/fstab
none  /dev/pts devpts gid=5,mode=620 0 0
_EOF_
chmod 0644 ${DESTDIR}/etc/fstab

mkdir -p ${DESTDIR}/dev/pts

for INPATH in dev etc/udev/devices; do
 /sbin/MAKEDEV -x -d ${DESTDIR}/${INPATH} console core fd full kmem kmsg mem null port \
```

```
  ptmx {p,t}ty{a,p}{0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f} random \
  urandom zero ram{,0,1,disk} std{in,out,err}
done

sed -i 's/^ACTIVE_CONSOLES=\(.*\)/#ACTIVE_CONSOLES=\1\nACTIVE_CONSOLES=""/g'
${DESTDIR}/etc/sysconfig/init

SERVICES="(network|crond|sshd|sysstat|snmpd|syslog|psacct|udev-post|nscd)"
chroot ${DESTDIR} "/sbin/chkconfig" "--list" | grep -oP '^\S+' | sort | uniq | egrep -vE
"${SERVICES}" | xargs -I{} chroot ${DESTDIR} "/sbin/chkconfig" "{}" "off"
chroot ${DESTDIR} "/sbin/chkconfig" "--list" | grep -oP '^\S+' | sort | uniq | egrep -E
"${SERVICES}" | xargs -I{} chroot ${DESTDIR} "/sbin/chkconfig" "{}" "--level" "2345" "on"

cat << _EOF_ > ${DESTDIR}/etc/sysconfig/clock
ZONE="Europe/Moscow"
_EOF_
chroot ${DESTDIR} "/usr/sbin/tzdata-update"
chroot ${DESTDIR} "rm -fv /etc/mtab; ln -s /proc/mounts /etc/mtab"
```

Issue with /dev permissions reproduces in container which created by above script.

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by cctо on Thu, 25 Oct 2012 10:24:57 GMT
View Forum Message <> Reply to Message

I run a test CentOS 6.3 HW and VE

The VE is centos-6-x86_64.tar.gz (downloaded from openvz.org)

Inside the VE, if I run

```
mkdir /z
mount -n -o mode=0755 -t devtmpfs none /z

ls -l /
..
drwxrwxrwt  8 root root  2140 Oct 25 18:15 z
```

It also shows the folder z (/devtmpfs) is 1777 when mount.

The command "mount -n -o mode=0755 -t devtmpfs none "$udev_root"" is inside /sbin/start_udev where /sbin/start_udev triggered during startup

and the above command make the /dev become 1777

I tried to compare the script - /sbin/start_udev to the standard CentOS 6 one, they are identical.

Does it relate to OpenVZ and the devtmpfs handling !?

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by umask on Thu, 25 Oct 2012 12:08:09 GMT
View Forum Message <> Reply to Message

http://bugzilla.openvz.org/show_bug.cgi?id=2397

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by ccto on Thu, 25 Oct 2012 15:01:14 GMT
View Forum Message <> Reply to Message

At the moment, shall we simply chmod 755 /dev in /etc/rc.d/rc.local temporarily before patch?

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by umask on Thu, 25 Oct 2012 18:04:58 GMT
View Forum Message <> Reply to Message

ccto wrote on Thu, 25 October 2012 11:01At the moment, shall we simply chmod 755 /dev in /etc/rc.d/rc.local temporarily before patch?

May be "yes" in this manner:

(sleep 60; chmod 0755 /dev;) &

However this way (chmod anytime in rc.local) still make possible access to /dev when perms still 1777.

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by mustardman on Tue, 06 Nov 2012 21:00:28 GMT
View Forum Message <> Reply to Message

Don't know if this addresses your particular problem but I recreate the dev devices after each reboot in /etc/rc.local. If you are having a problem with some other one like /dev/tmp then you could add that as well.

/bin/rm -rf /dev/null
/bin/rm -rf /dev/random
/bin/rm -rf /dev/tty*
/bin/rm -rf /dev/pty*
/bin/mknod -m 0666 /dev/null c 1 3
/bin/mknod -m 0644 /dev/random c 1 8
/sbin/MAKEDEV tty
/sbin/MAKEDEV pty

Subject: Re: /dev (devtmpfs) permissions is 1777
Posted by umask on Wed, 07 Nov 2012 04:06:26 GMT
View Forum Message <> Reply to Message

> Don't know if this addresses your particular problem but...

The problem which I described is not connected with device creation.

> but I recreate the dev devices after each reboot in /etc/rc.local.

Probably it is very stupid idea.
For example /dev/null may absent and some daemons will start before your rc.local and you will lose disk space (file descriptor will be opened, daemon will write something to it, but file will be deleted).
