

chroot "jail"

**A chroot on Unix operating systems is an operation that changes any designated directory for the current running process and its children. A program that is run in such a modified environment cannot name, access files outside the designated directory tree. The modified environment is called a chroot jail.**

***A chroot environment can be used to create and host a separate virtualized copy of the software system. This can be useful for:***

**Recovery:**

***chroot is used to move back into the damaged OS environment after bootstrapping from an alternate boot image such as from installation media,ISO image or a Live CD/DVD***

**Testing and development:**

***A test environment can be set up in the chroot for software that would otherwise be too risky to deploy on a production system.***

**Dependency control:**

***Software can be developed, built and tested in a chroot populated only with its expected dependencies. This can prevent some kinds of linkage skew that can result from developers building projects with different sets of program libraries installed.***

**Compatibility:**

***Legacy software or software using a different ABI must sometimes be run in a chroot because their supporting libraries or data files may otherwise clash in name or linkage with those of the host system.***

**Privilege separation:**

***Programs are allowed to carry open file descriptors (for files, pipelines and network connections) into the chroot, which can simplify jail design by making it unnecessary to leave working files inside the chroot directory. This also simplifies the common arrangement of running the potentially vulnerable parts of a privileged program in a sandbox, in order to pre-emptively contain a security breach.***

***ftp users access are restricted this way for accessing ftp data and not to gain any other access on remotes system other than ftp directory after ftp login. Note that chroot is not necessarily enough to contain a process with root privileges***

=================================================================================

**Here below an example to restrict /bin/bash commands to a designated directory (chroot directory)**

**>>*Below one local used designated a chroot directory under its home directory path to have no access other than***

[devinder@master ~]$ id

uid=10007(devinder) gid=10007(devinder) groups=10007(devinder) context=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023

[devinder@master ~]$ sudo -l

Matching Defaults entries for devinder on master:

!visiblepw, always\_set\_home, match\_group\_by\_gid, always\_query\_group\_plugin, env\_reset, env\_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS\_COLORS",

env\_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC\_ADDRESS LC\_CTYPE", env\_keep+="LC\_COLLATE LC\_IDENTIFICATION LC\_MEASUREMENT LC\_MESSAGES", env\_keep+="LC\_MONETARY

LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE", env\_keep+="LC\_TIME LC\_ALL LANGUAGE LINGUAS \_XKB\_CHARSET XAUTHORITY", secure\_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User devinder may run the following commands on master:

(root) NOPASSWD: /usr/sbin/chroot

**>> Create below "jail" directory to set as chroot for /bin/bash commands**

[devinder@master ~]$ JAIL=$HOME/jail

[devinder@master ~]$

[devinder@master ~]$ mkdir -p $JAIL

[devinder@master ~]$

**>> create a bin directory to keep bash shell & its commands and "lib64,lib" directory to keep required library for bash and its commands for their operation**

[devinder@master ~]$ mkdir -p $JAIL/{bin,lib64,lib}

[devinder@master ~]$

[devinder@master ~]$ cd $JAIL

[devinder@master jail]$ pwd

/home/devinder/jail

[devinder@master jail]$ ls

bin lib lib64

[devinder@master jail]$

**>>Copy bash and lets only one command "ls" under $JAIL/bin**

[devinder@master jail]$ cp -v /bin/{bash,ls} $JAIL/bin

‘/bin/bash’ -> ‘/home/devinder/jail/bin/bash’

‘/bin/ls’ -> ‘/home/devinder/jail/bin/ls’

[devinder@master jail]$

**>>Find required shared libraries for bash shell**

[devinder@master jail]$ ldd /bin/bash

linux-vdso.so.1 => (0x00007ffdf0f62000)

libtinfo.so.5 => /lib64/libtinfo.so.5 (0x0000003b0a800000)

libdl.so.2 => /lib64/libdl.so.2 (0x0000003b06800000)

libc.so.6 => /lib64/libc.so.6 (0x0000003b06000000)

/lib64/ld-linux-x86-64.so.2 (0x00007f1a50500000)

[devinder@master jail]$

**>>Copy all required libraries for bash shell under $JAIL/lib64/ alone, since no library is found under lib**

[devinder@master jail]$ cp -v /lib64/{libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2} $JAIL/lib64/

‘/lib64/libtinfo.so.5’ -> ‘/home/devinder/jail/lib64/libtinfo.so.5’

‘/lib64/libdl.so.2’ -> ‘/home/devinder/jail/lib64/libdl.so.2’

‘/lib64/libc.so.6’ -> ‘/home/devinder/jail/lib64/libc.so.6’

‘/lib64/ld-linux-x86-64.so.2’ -> ‘/home/devinder/jail/lib64/ld-linux-x86-64.so.2’

[devinder@master jail]$

**>>similarly find required libraries for "ls" command and then copy accordingly under $JAIL/lib\*/**

[devinder@master jail]$ ldd /bin/ls

linux-vdso.so.1 => (0x00007fff65793000)

libselinux.so.1 => /lib64/libselinux.so.1 (0x0000003b07400000)

libcap.so.2 => /lib64/libcap.so.2 (0x0000003b09400000)

libacl.so.1 => /lib64/libacl.so.1 (0x0000003b0f400000)

libc.so.6 => /lib64/libc.so.6 (0x0000003b06000000)

libpcre.so.1 => /lib64/libpcre.so.1 (0x0000003b07000000)

libdl.so.2 => /lib64/libdl.so.2 (0x0000003b06800000)

/lib64/ld-linux-x86-64.so.2 (0x00007f45e8979000)

libattr.so.1 => /lib64/libattr.so.1 (0x0000003b08800000)

libpthread.so.0 => /lib64/libpthread.so.0 (0x0000003b06400000)

[devinder@master jail]$

**>> Copy required libraries for "ls" command under $JAIL/lib64/ since no library under lib**

[devinder@master jail]$ cp -v /lib64/{libselinux.so.1,libcap.so.2,libacl.so.1,libc.so.6,libpcre.so.1,libdl.so.2,ld-linux-x86-64.so.2,libattr.so.1,libpthread.so.0} $JAIL/lib64/

‘/lib64/libselinux.so.1’ -> ‘/home/devinder/jail/lib64/libselinux.so.1’

‘/lib64/libcap.so.2’ -> ‘/home/devinder/jail/lib64/libcap.so.2’

‘/lib64/libacl.so.1’ -> ‘/home/devinder/jail/lib64/libacl.so.1’

‘/lib64/libc.so.6’ -> ‘/home/devinder/jail/lib64/libc.so.6’

‘/lib64/libpcre.so.1’ -> ‘/home/devinder/jail/lib64/libpcre.so.1’

‘/lib64/libdl.so.2’ -> ‘/home/devinder/jail/lib64/libdl.so.2’

‘/lib64/ld-linux-x86-64.so.2’ -> ‘/home/devinder/jail/lib64/ld-linux-x86-64.so.2’

‘/lib64/libattr.so.1’ -> ‘/home/devinder/jail/lib64/libattr.so.1’

‘/lib64/libpthread.so.0’ -> ‘/home/devinder/jail/lib64/libpthread.so.0’

[devinder@master jail]$

**>> As usual We could see user is able to ls command outside his home directory as well.**

[devinder@master jail]$ ls /

app bin boot dev home lib64 media newdir proc run scripts sys TOOL usr

AUTOMATION bindmount dd etc lib LVM-FILTER mnt opt root sbin srv tmp u01 var

[devinder@master jail]$ ls /etc

abrt dconf groff localtime passwd- rpm sysconfig

adjtime default group login.defs pinforc rsyncd.conf sysctl.conf

aliases depmod.d group- logrotate.conf pkcs11 rsyslog.conf sysctl.d

aliases.db dhcp grub2.cfg logrotate.d pki rsyslog.d systemd

alternatives DIR\_COLORS grub.d lsm plymouth rwtab system-release

anacrontab DIR\_COLORS.256color gshadow lvm pm rwtab.d system-release-cpe

ansible DIR\_COLORS.lightbgcolor gshadow- machine-id polkit-1 sasl2 tcsd.conf

asound.conf dnsmasq.conf gss magic popt.d scl terminfo

at.deny dnsmasq.d host.conf mail.rc postfix securetty tmpfiles.d

audisp dracut.conf hostname makedumpfile.conf.sample ppp security trusted-key.key

audit dracut.conf.d hosts man\_db.conf prelink.cache selinux tuned

bash\_completion.d e2fsck.conf hosts.allow mke2fs.conf prelink.conf services udev

bashrc egl hosts.deny modprobe.d prelink.conf.d sestatus.conf updatedb.conf

binfmt.d environment init.d modules-load.d printcap setuptool.d usb\_modeswitch.conf

centos-release ethertypes inittab motd profile shadow vconsole.conf

centos-release-upstream exports inputrc mtab profile.d shadow- vimrc

chkconfig.d favicon.png iproute2 my.cnf protocols shells virc

chrony.conf filesystems issue my.cnf.d python shells.rpmnew vmware-tools

chrony.keys firewalld issue.net nanorc rc0.d skel vsftpd

cifs-utils fonts kdump.conf netconfig rc1.d smartmontools wgetrc

cron.d fprintd.conf kernel NetworkManager rc2.d sos.conf wpa\_supplicant

cron.daily fstab krb5.conf networks rc3.d ssh X11

cron.deny fuse.conf krb5.conf.d nsswitch.conf rc4.d ssl xdg

cron.hourly gcrypt ld.so.cache nsswitch.conf.bak rc5.d statetab xinetd.d

cron.monthly gdbinit ld.so.conf nsswitch.conf.rpmnew rc6.d statetab.d yum

crontab gdbinit.d ld.so.conf.d ntp rc.d subgid yum.conf

cron.weekly GeoIP.conf libaudit.conf openldap rc.local subuid yum.repos.d

crypttab GeoIP.conf.default libnl opt rdma sudo.conf

csh.cshrc glvnd libreport os-release redhat-release sudoers

csh.login gnupg libuser.conf pam.d resolv.conf sudoers.d

dbus-1 GREP\_COLORS locale.conf passwd rpc sudo-ldap.conf

**>> Once we chroot the $JAIL user wouldn’t be able to access files outside $JAIL Also other than command "ls" he wouldn’t be able to run any other command**

**>> setting chroot for /home/devinder/jail ($JAIL)**

[devinder@master jail]$ sudo chroot $JAIL /bin/bash

bash-4.2#

bash-4.2# ls /

bin lib lib64

**bash-4.2# ls /etc**

**ls: cannot access /etc: No such file or directory**

**bash-4.2# ls /var**

**ls: cannot access /var: No such file or directory**

**bash-4.2#**

**bash-4.2# mkdir new**

**bash: mkdir: command not found**

**bash-4.2#**

**bash-4.2# touch file**

**bash: touch: command not found**

**>> to come out from chroot (chroot jail) just type exit**

bash-4.2# exit

exit

**>>Now user can access file outside /home/devinder/jail ($JAIL) and run other commands as well**

[devinder@master jail]$ ls /

app bin boot dev home lib64 media newdir proc run scripts sys TOOL usr

AUTOMATION bindmount dd etc lib LVM-FILTER mnt opt root sbin srv tmp u01 var

[devinder@master jail]$ ls /etc

abrt dconf groff localtime passwd- rpm sysconfig

adjtime default group login.defs pinforc rsyncd.conf sysctl.conf

aliases depmod.d group- logrotate.conf pkcs11 rsyslog.conf sysctl.d

aliases.db dhcp grub2.cfg logrotate.d pki rsyslog.d systemd

alternatives DIR\_COLORS grub.d lsm plymouth rwtab system-release

anacrontab DIR\_COLORS.256color gshadow lvm pm rwtab.d system-release-cpe

ansible DIR\_COLORS.lightbgcolor gshadow- machine-id polkit-1 sasl2 tcsd.conf

asound.conf dnsmasq.conf gss magic popt.d scl terminfo

at.deny dnsmasq.d host.conf mail.rc postfix securetty tmpfiles.d

audisp dracut.conf hostname makedumpfile.conf.sample ppp security trusted-key.key

audit dracut.conf.d hosts man\_db.conf prelink.cache selinux tuned

bash\_completion.d e2fsck.conf hosts.allow mke2fs.conf prelink.conf services udev

bashrc egl hosts.deny modprobe.d prelink.conf.d sestatus.conf updatedb.conf

binfmt.d environment init.d modules-load.d printcap setuptool.d usb\_modeswitch.conf

centos-release ethertypes inittab motd profile shadow vconsole.conf

centos-release-upstream exports inputrc mtab profile.d shadow- vimrc

chkconfig.d favicon.png iproute2 my.cnf protocols shells virc

chrony.conf filesystems issue my.cnf.d python shells.rpmnew vmware-tools

chrony.keys firewalld issue.net nanorc rc0.d skel vsftpd

cifs-utils fonts kdump.conf netconfig rc1.d smartmontools wgetrc

cron.d fprintd.conf kernel NetworkManager rc2.d sos.conf wpa\_supplicant

cron.daily fstab krb5.conf networks rc3.d ssh X11

cron.deny fuse.conf krb5.conf.d nsswitch.conf rc4.d ssl xdg

cron.hourly gcrypt ld.so.cache nsswitch.conf.bak rc5.d statetab xinetd.d

cron.monthly gdbinit ld.so.conf nsswitch.conf.rpmnew rc6.d statetab.d yum

crontab gdbinit.d ld.so.conf.d ntp rc.d subgid yum.conf

cron.weekly GeoIP.conf libaudit.conf openldap rc.local subuid yum.repos.d

crypttab GeoIP.conf.default libnl opt rdma sudo.conf

csh.cshrc glvnd libreport os-release redhat-release sudoers

csh.login gnupg libuser.conf pam.d resolv.conf sudoers.d

dbus-1 GREP\_COLORS locale.conf passwd rpc sudo-ldap.conf

[devinder@master jail]$ ls /var

account adm cache crash db empty ftp games gopher kerberos lib local lock log mail nis opt preserve run spool tmp yp

[devinder@master jail]$

[devinder@master jail]$ touch file

[devinder@master jail]$

**Devinder Singh Lalotra**

**Devinder.lalotra@mphasis.com**