

## chroot Jail Walkthrough

**NOTE:** This walkthrough assumes use on a Debian-based machine to install a chroot jail running on Debian Bullseye, although other OSs can use debootstrap to install other OSs as well. “#” indicates superuser commands, “\$” indicates user commands.

1. Create shell variable for the mount directory
  - a. **(host):** # echo 'BULLSEYE\_CHROOT=/mnt/chroot/bullseye-mini' >> /etc/environment
  - b. **(host):** # source /etc/environment
  - c. **NOTE:** Not really necessary, but will save time and keystrokes now and in the future.
2. Create mount directory
  - a. **(host):** # mkdir -p \$BULLSEYE\_CHROOT
3. Install debootstrap
  - a. **(host):** # apt install debootstrap
4. Create chroot jail and mount appropriate jail directories
  - a. **(host):** # debootstrap bullseye \$BULLSEYE\_CHROOT <https://deb.debian.org/debian>
  - b. **(host):** # mount -t proc proc \$BULLSEYE\_CHROOT/proc
  - c. **(host):** # mount -t devpts devpts \$BULLSEYE\_CHROOT/dev/pts
5. Login to chroot jail as root
  - a. **(host):** # chroot \$BULLSEYE\_CHROOT /bin/bash --login
6. **(jail):** # nano ~/.profile
  - a. Comment the bottom line and replace with:
    - i. (tty > /dev/null) && (msg n || true)
  - b. **NOTE:** This may not be necessary with Bullseye. This was needed for a chroot jail using Debian Buster.
7. Change the shell prompt to something normal
  - a. **(jail):** # echo 'bullseye-chroot' > /etc/debian\_chroot
  - b. **(jail):** # echo 'PS1="\u@\$ (cat /etc/debian\_chroot):\w# "' >> ~/.bashrc
  - c. **(jail):** # source /etc/bash.bashrc
  - d. **(jail):** # source ~/.bashrc
  - e. **NOTE:** The hostname in /etc/hostname is actually shared between the host and the chroot jail, hence the use of /etc/debian\_chroot instead.
8. Install and configure locale options
  - a. **(jail):** # apt install locales
  - b. **(jail):** # dpkg-reconfigure locales
  - c. Select preferred language from menu.

9. Install SSH and PAM modules, and configure SSH daemon
  - a. **(jail):** # apt install ssh libpam-ssh libpam-ssh-agent-auth
  - b. **(jail):** # sed -i "s;#Port 22;Port <some other #>;"  
/etc/ssh/sshd\_config
    - i. **NOTE:** This configures SSH to work on a different port number besides the default port 22 because the host (localhost) is already using port 22.
    - ii. We'll be creating a user and giving them sudo permissions later (Step 11), but if you want to allow login to root directly, add "PermitRootLogin yes" somewhere in this file. It doesn't matter where.
  - c. **(jail):** # /etc/init.d/ssh restart
10. Add host machine's hostname to chroot jail's /etc/hosts
  - a. **(jail):** # echo -e "127.0.1.1\t<host's hostname>" >>  
/etc/hosts
11. Add "non-free" and "contrib" repositories to APT's sources.list, if desired.
  - a. **(jail):** # nano /etc/apt/sources.list
    - i. Add "non-free" and/or "contrib" to the end of desired repository entries.
12. Create password for root
  - a. **(jail):** # passwd
    - i. Set the password to whatever you want
13. Create user and add them to groups
  - a. **(jail):** # apt install sudo
  - b. **(jail):** # adduser <username>
    - i. Set password to whatever you want
  - c. **(jail):** # addgroup <username> users
  - d. **(jail):** # addgroup <username> sudo
14. Exit chroot jail and return to normal user on host
  - a. **(jail):** # exit
  - b. **(host):** # exit
15. Login to chroot jail as user
  - a. **(host):** \$ ssh -p <port # from Step 9.b.i> <username from Step 11.b>@localhost
    - i. Note: If you've previously created a chroot jail on the same port, this might not work at first. To fix this, try one of the following
      1. ssh-keygen -f "/home/\$USER/.ssh/known\_hosts" -R  
"[localhost]:<port #>"
        - i. This will remove the previous known host at  
localhost:<port #>
      2. reboot the host machine
      3. Both 1 & 2

16. Install Z shell and change shell prompt to something normal
  - a. **NOTE:** Change only unbolded lines
  - b. **(jail):** `$ sudo apt install zsh`
  - c. **(jail):** `$ nano ~/.zprofile`
    - i. `BF="%B%F"`
    - ii. `bf="%f%b"`
    - iii. `export PS1="[ $BF{green}`  
`%n$bf$BF{yellow}@$bf$BF{magenta}%m$bf: $BF{blue}%~ $bf] $ "`
  - d. **(jail):** `$ nano ~/.zshrc`
    - i. `source "$HOME"/.zprofile`
  - e. **(jail):** `$ source ~/.zshrc`
17. The chroot jail is now ready to use like a regular Linux machine. If the host is rebooted or shut down, the chroot jail's /proc and /dev/pts directories will need to be re-mounted, and the SSH server on the chroot jail will also need to be restarted before you can SSH into it. The file "chroot\_startup.ssh" has been provided for as a convenience.
  - a. **(host):** `$ bash chroot_startup.sh $BULLSEYE_CHROOT`
18. If your chroot jail does not connect to Internet at different locations, try the following:
  - a. **(host):** `# mount --bind /etc/resolv.conf`  
`$BULLSEYE_MINI/etc/resolv.conf`
    - i. **NOTE:** This command is also part of chroot\_startup.sh, so re-executing that script should also fix Internet connectivity issues