Restrict SSH User Access to Certain Directory Using Chrooted Jail

In order to lock SSH users in a certain directory, we can use chroot mechanism.

change root (chroot) in Unix-like systems such as Linux, is a means of separating specific user operations from the rest of the Linux system; changes the apparent root directory for the current running user process and its child process with new root directory called a chrooted jail.

In this tutorial, we'll show you how to restrict a SSH user access to a given directory in Linux. Note that we'll run the all the commands as root, use the sudo command if you are logged into server as a normal user.

Step 1: Create SSH Chroot Jail

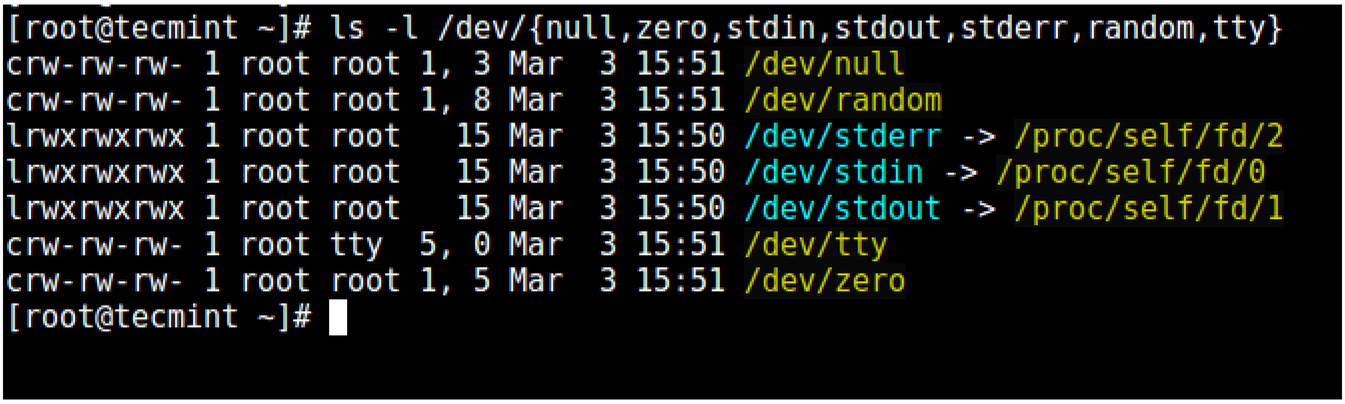
1. Start by creating the chroot jail using the mkdir command below:

```
# mkdir -p /home/test
```

2. Next, identify required files, according to the **sshd_config** man page, the `ChrootDirectory` option specifies the pathname of the directory to chroot to after authentication. The directory must contain the necessary files and directories to support a user's session.

For an interactive session, this requires at least a shell, commonly `sh`, and basic `/dev` nodes such as null, zero, stdin, stdout, stderr, and tty devices:

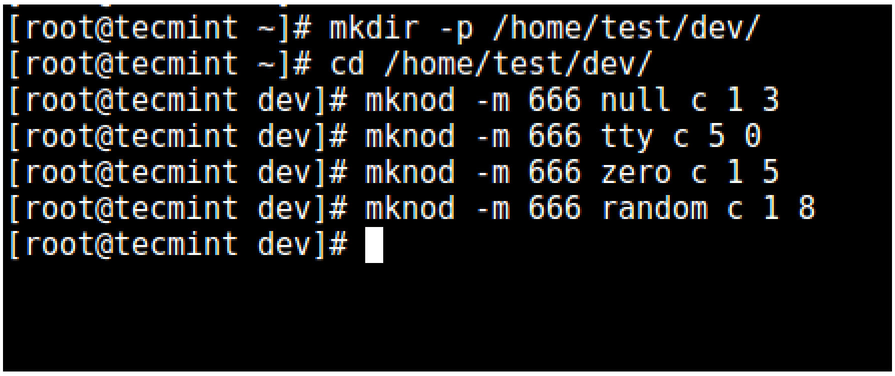
```
# ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
```



```
[root@tecmint ~]# ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
crw-rw-rw- 1 root root 1, 3 Mar  3 15:51 /dev/null
crw-rw-rw- 1 root root 1, 8 Mar  3 15:51 /dev/random
lrwxrwxrwx 1 root root   15 Mar  3 15:50 /dev/stderr -> /proc/self/fd/2
lrwxrwxrwx 1 root root   15 Mar  3 15:50 /dev/stdin -> /proc/self/fd/0
lrwxrwxrwx 1 root root   15 Mar  3 15:50 /dev/stdout -> /proc/self/fd/1
crw-rw-rw- 1 root tty  5, 0 Mar  3 15:51 /dev/tty
crw-rw-rw- 1 root root 1, 5 Mar  3 15:51 /dev/zero
[root@tecmint ~]#
```

3. Now, create the `/dev` files as follows using the **mknod command**. In the command below, the `-m` flag is used to specify the file permissions bits, `c` means character file and the two numbers are major and minor numbers that the files point to.

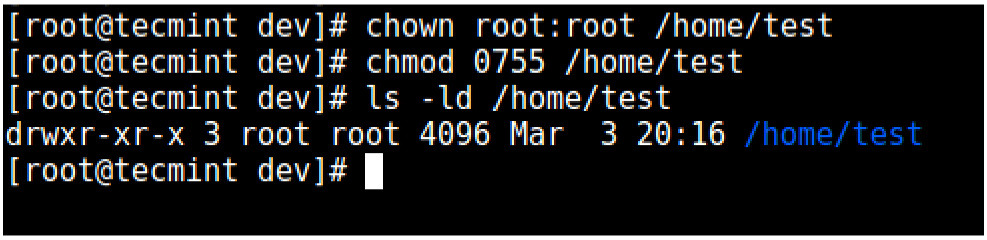
```
# mkdir -p /home/test/dev/
# cd /home/test/dev/
# mknod -m 666 null c 1 3
# mknod -m 666 tty c 5 0
# mknod -m 666 zero c 1 5
# mknod -m 666 random c 1 8
```



```
[root@tecmint ~]# mkdir -p /home/test/dev/
[root@tecmint ~]# cd /home/test/dev/
[root@tecmint dev]# mknod -m 666 null c 1 3
[root@tecmint dev]# mknod -m 666 tty c 5 0
[root@tecmint dev]# mknod -m 666 zero c 1 5
[root@tecmint dev]# mknod -m 666 random c 1 8
[root@tecmint dev]#
```

4. Afterwards, set the appropriate permission on the chroot jail. Note that the chroot jail and its subdirectories and subfiles must be owned by **root** user, and not writable by any normal user or group:

```
# chown root:root /home/test
# chmod 0755 /home/test
# ls -ld /home/test
```

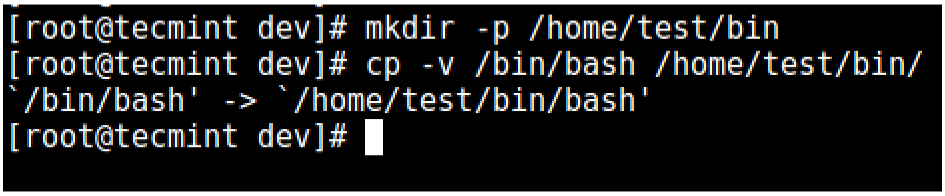


```
[root@tecmint dev]# chown root:root /home/test
[root@tecmint dev]# chmod 0755 /home/test
[root@tecmint dev]# ls -ld /home/test
drwxr-xr-x 3 root root 4096 Mar  3 20:16 /home/test
[root@tecmint dev]#
```

Step 2: Setup Interactive Shell for SSH Chroot Jail

5. First, create the `bin` directory and then copy the `/bin/bash` files into the `bin` directory as follows:

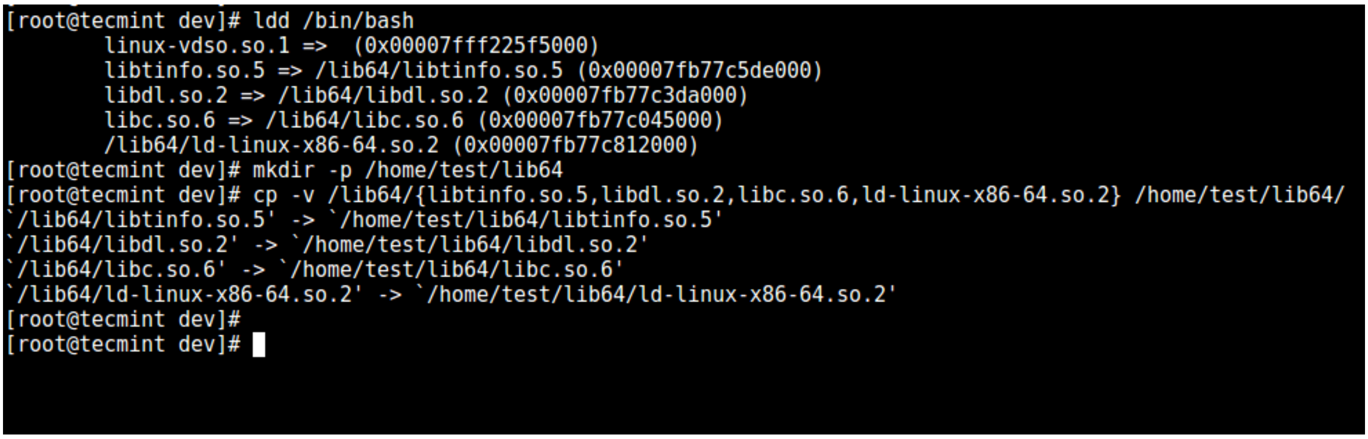
```
# mkdir -p /home/test/bin
# cp -v /bin/bash /home/test/bin/
```



```
[root@tecmint dev]# mkdir -p /home/test/bin
[root@tecmint dev]# cp -v /bin/bash /home/test/bin/
`/bin/bash' -> `/home/test/bin/bash'
[root@tecmint dev]#
```

6. Now, identify bash required shared `libs`, as below and copy them into the `lib` directory:

```
# ldd /bin/bash
# mkdir -p /home/test/lib64
# cp -v /lib64/{libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2}
/home/test/lib64/
```



```
[root@tecmint dev]# ldd /bin/bash
        linux-vdso.so.1 =>  (0x00007fff225f5000)
        libtinfo.so.5 => /lib64/libtinfo.so.5 (0x00007fb77c5de000)
        libdl.so.2 => /lib64/libdl.so.2 (0x00007fb77c3da000)
        libc.so.6 => /lib64/libc.so.6 (0x00007fb77c045000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fb77c812000)
[root@tecmint dev]# mkdir -p /home/test/lib64
[root@tecmint dev]# cp -v /lib64/{libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2} /home/test/lib64/
`/lib64/libtinfo.so.5' -> `/home/test/lib64/libtinfo.so.5'
`/lib64/libdl.so.2' -> `/home/test/lib64/libdl.so.2'
`/lib64/libc.so.6' -> `/home/test/lib64/libc.so.6'
`/lib64/ld-linux-x86-64.so.2' -> `/home/test/lib64/ld-linux-x86-64.so.2'
[root@tecmint dev]#
[root@tecmint dev]#
```

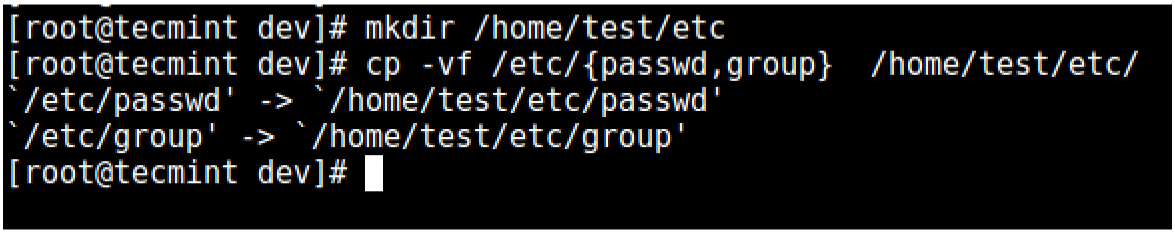
Step 3: Create and Configure SSH User

7. Now, create the SSH user with the useradd command and set a secure password for the user:

```
# useradd tuxi
# passwd tuxi
```

8. Create the chroot jail general configurations directory, `/home/test/etc` and copy the updated account files (**/etc/passwd** and **/etc/group**) into this directory as follows:

```
# mkdir /home/test/etc
# cp -vf /etc/{passwd,group} /home/test/etc/
```



```
[root@tecmint dev]# mkdir /home/test/etc
[root@tecmint dev]# cp -vf /etc/{passwd,group}  /home/test/etc/
`/etc/passwd' -> `/home/test/etc/passwd'
`/etc/group' -> `/home/test/etc/group'
[root@tecmint dev]#
```

Note: Each time you add more SSH users to the system, you will need to copy the updated account files into the `/home/test/etc` directory.

Step 4: Configure SSH to Use Chroot Jail

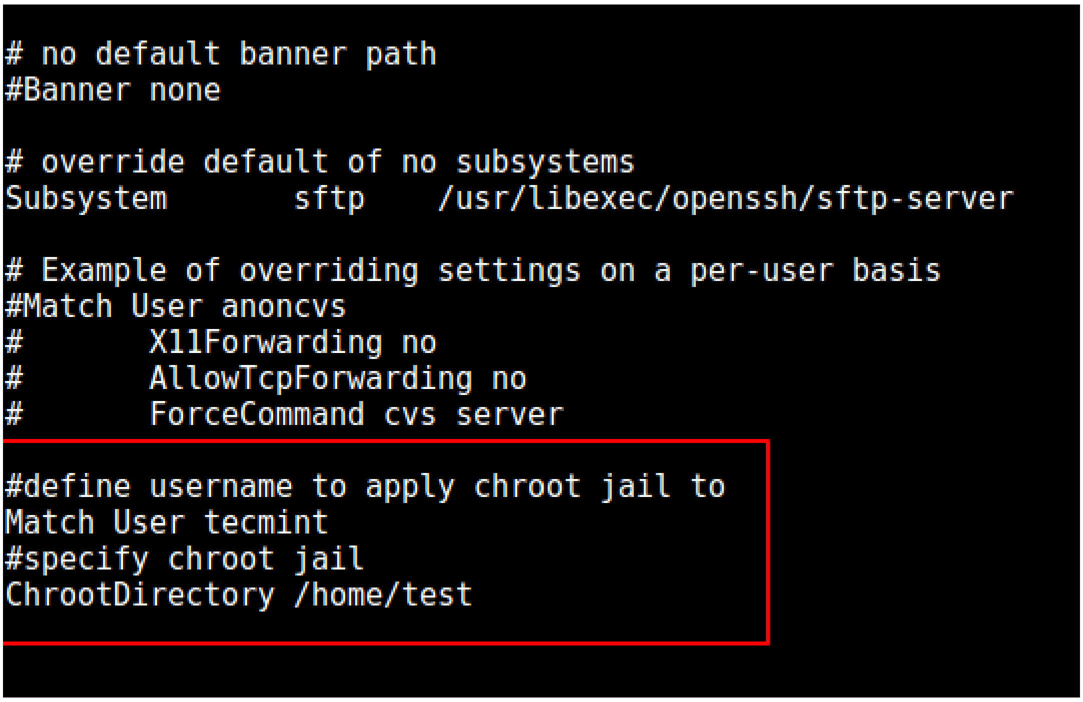
9. Now, open the `sshd_config` file.

```
# vi /etc/ssh/sshd_config
```

and add/modify the lines below in the file.

```
#define username to apply chroot jail to
```

```
Match User tecmint
#specify chroot jail
ChrootDirectory /home/test
```



```
# no default banner path
#Banner none

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       ForceCommand cvs server

#define username to apply chroot jail to
Match User tecmint
#specify chroot jail
ChrootDirectory /home/test
```

From:
https://www.cooltux.net/ - **TuxNet DokuWiki**

Permanent link:
https://www.cooltux.net/doku.php?id=it-wiki:linux:ssh_chrooted_jail&rev=1615408162

Last update: **2021/03/10 20:29**