



将 [SSH 用户会话限制](#) 访问到特定的目录内，特别是在 web 服务器上，这样做有多个原因，但最显而易见的是为了系统安全。为了锁定 SSH 用户在某个目录，我们可以使用 [chroot](#) 机制。

在诸如 Linux 之类的类 Unix 系统中更改 root ( [chroot](#) ) 是将特定用户操作与其他 Linux 系统分离的一种手段；使用称为 [chrooted](#) [监狱](#) 的新根目录更改当前运行的用户进程及其子进程的明显根目录。

在本教程中，我们将向你展示如何限制 SSH 用户访问 Linux 中指定的目录。注意，我们将以 root 用户身份运行所有命令，如果你以普通用户身份登录服务器，请使用 [sudo 命令](#)。



## 步骤 1：创建 SSH chroot 监狱

1、使用 `mkdir` 命令开始创建 chroot 监狱：

```
1. | # mkdir -p /home/test
```

2、接下来，根据 [sshd\\_config](#) 手册找到所需的文件，[ChrootDirectory](#) 选项指定在身份验证后要 chroot 到的目录的路径名。该目录必须包含支持用户会

话所必需的文件和目录。

对于交互式会话，这需要至少一个 shell，通常为 `sh` 和基本的 `/dev` 节点，例如 `null`、`zero`、`stdin`、`stdout`、`stderr` 和 `tty` 设备：

```
1. # 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 ~]#
```

列出所需文件

3、现在，使用 `mknod` 命令创建 `/dev` 下的文件。在下面的命令中，`-m` 标志用来指定文件权限位，`c` 意思是字符文件，两个数字分别是文件指向的主要号和次要号。

```
1. # mkdir -p /home/test/dev/
2. # cd /home/test/dev/
3. # mknod -m 666 null c 1 3
4. # mknod -m 666 tty c 5 0
5. # mknod -m 666 zero c 1 5
6. # 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]#
```

创建 `/dev` 和所需文件

4、在此之后，在 `chroot` 监狱中设置合适的权限。注意 `chroot` 监狱和它的子目录以及子文件必须被 `root` 用户所有，并且对普通用户或用户组不可写：

```
1. # chown root:root /home/test
2. # chmod 0755 /home/test
3. # 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]#
```



## 步骤 2 : 为 SSH chroot 监狱设置交互式 shell

5、首先, 创建 `bin` 目录并复制 `/bin/bash` 到 `bin` 中:

```
1. # mkdir -p /home/test/bin
2. # 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]#
```

复制文件到 bin 目录中

6、现在, 识别 bash 所需的共享库, 如下所示复制它们到 `lib64` 中:

```
1. # ldd /bin/bash
2. # mkdir -p /home/test/lib64
3. # 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]#
```

复制共享库文件



## 步骤 3 : 创建并配置 SSH 用户

7、现在, 使用 `useradd` 命令 创建 SSH 用户, 并设置安全密码:

```
1. # useradd tecmint
2. # passwd tecmint
```

8、创建 chroot 监狱通用配置目录 `/home/test/etc` 并复制已更新的账号文件 ( `/etc/passwd` 和 `/etc/group` ) 到这个目录中：

```
1. # mkdir /home/test/etc
2. # 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]#
```

复制密码文件

注意：每次向系统添加更多 SSH 用户时，都需要将更新的帐户文件复制到 `/home/test/etc` 目录中。



## 步骤 4：配置 SSH 来使用 chroot 监狱

9、现在打开 `sshd_config` 文件。

```
1. # vi /etc/ssh/sshd_config
```

在此文件中添加或修改下面这些行。

```
1. # 定义要使用 chroot 监狱的用户
2. Match User tecmint
3. # 指定 chroot 监狱
4. 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
```

配置 SSH chroot 监狱

保存文件并退出，重启 sshd 服务：

```
1. # systemctl restart sshd
2. 或者
3. # service sshd restart
```



## 步骤 5：测试 SSH 的 chroot 监狱

10、这次，测试 chroot 监狱的设置是否如希望的那样成功了：

```
1. # ssh tecmint@192.168.0.10
2. -bash-4.1$ ls
3. -bash-4.1$ date
4. -bash-4.1$ uname
```

```
tecmint@TecMint ~ $ ssh tecmint@192.168.0.10
tecmint@192.168.0.10's password:
-bash-4.1$ ls
-bash: ls: command not found
-bash-4.1$ date
-bash: date: command not found
-bash-4.1$ uname
-bash: uname: command not found
-bash-4.1$
```

测试 SSH 用户 chroot 监狱

从上面的截图上来看，我们可以看到 SSH 用户被锁定在了 chroot 监狱中，并且不能使用任何外部命令如（`ls`、`date`、`uname` 等等）。

用户只可以执行 `bash` 以及它内置的命令（比如：`pwd`、`history`、`echo` 等等）：

```
1. # ssh tecmint@192.168.0.10
2. -bash-4.1$ pwd
3. -bash-4.1$ echo "Tecmint - Fastest Growing Linux Site"
4. -bash-4.1$ history
```

```
tecmint@TecMint ~ $ ssh tecmint@192.168.0.10
tecmint@192.168.0.10's password:
Last login: Fri Mar 3 20:47:04 2017 from 192.168.0.103
-bash-4.1$ pwd
/
-bash-4.1$ echo "Tecmint - Fastest Growing Linux Site"
Tecmint - Fastest Growing Linux Site
-bash-4.1$
-bash-4.1$ history
 1  pwd
 2  echo "Tecmint - Fastest Growing Linux Site"
 3  history
-bash-4.1$
```

SSH 内置命令

## 步骤 6：创建用户的主目录并添加 Linux 命令

11、从前面的步骤中，我们可以看到用户被锁定在了 root 目录，我们可以为 SSH 用户创建一个主目录（以及为所有将来的用户这么做）：

```
1. # mkdir -p /home/test/home/tecmint
2. # chown -R tecmint:tecmint /home/test/home/tecmint
3. # chmod -R 0700 /home/test/home/tecmint
```

```
[root@tecmint dev]# mkdir -p /home/test/home/tecmint
[root@tecmint dev]# chown -R tecmint:tecmint /home/test/home/tecmint
[root@tecmint dev]# chmod -R 0700 /home/test/home/tecmint
[root@tecmint dev]#
```

创建 SSH 用户主目录

12、接下来，在 bin 目录中安装几个用户命令，如 ls、date、mkdir：

```
1. # cp -v /bin/ls /home/test/bin/
2. # cp -v /bin/date /home/test/bin/
3. # cp -v /bin/mkdir /home/test/bin/
```

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

向 SSH 用户添加命令

13、接下来，检查上面命令的共享库并将它们移到 chroot 监狱的库目录中：

```
1. # ldd /bin/ls
2. # 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} /home/test/lib64/
```

```
[root@tecmint dev]#
[root@tecmint dev]# ldd /bin/ls
linux-vdso.so.1 => (0x00007fff415ff000)
libselinux.so.1 => /lib64/libselinux.so.1 (0x00007f25046b5000)
librt.so.1 => /lib64/librt.so.1 (0x00007f25044ad000)
libcap.so.2 => /lib64/libcap.so.2 (0x00007f25042a8000)
libacl.so.1 => /lib64/libacl.so.1 (0x00007f25040a0000)
libc.so.6 => /lib64/libc.so.6 (0x00007f2503d0c000)
libdl.so.2 => /lib64/libdl.so.2 (0x00007f2503b07000)
/lib64/ld-linux-x86-64.so.2 (0x00007f25048e7000)
libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f25038ea000)
```



```
libattr.so.1 => /lib64/libattr.so.1 (0x00007f25036e5000)
[root@tecmint dev]# 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} /home/test/lib64/
`/lib64/libselinux.so.1' -> `/home/test/lib64/libselinux.so.1'
`/lib64/libcap.so.2' -> `/home/test/lib64/libcap.so.2'
`/lib64/libacl.so.1' -> `/home/test/lib64/libacl.so.1'
cp: overwrite `/home/test/lib64/libc.so.6'? yes
`/lib64/libc.so.6' -> `/home/test/lib64/libc.so.6'
cp: cannot stat `/lib64/libpcre.so.1': No such file or directory
cp: overwrite `/home/test/lib64/libdl.so.2'? yes
`/lib64/libdl.so.2' -> `/home/test/lib64/libdl.so.2'
cp: overwrite `/home/test/lib64/ld-linux-x86-64.so.2'? yes
`/lib64/ld-linux-x86-64.so.2' -> `/home/test/lib64/ld-linux-x86-64.so.2'
`/lib64/libattr.so.1' -> `/home/test/lib64/libattr.so.1'
`/lib64/libpthread.so.0' -> `/home/test/lib64/libpthread.so.0'
[root@tecmint dev]#
```

复制共享库



## 步骤 7：测试 sftp 的用 chroot 监狱

14、最后用 sftp 做一个测试；测试你先前安装命令是否可用。

在 `/etc/ssh/sshd_config` 中添加下面的行：

```
1. # 启用 sftp 的 chroot 监狱
2. ForceCommand internal-sftp
```

保存并退出文件。接下来重启 sshd 服务：

```
1. # systemctl restart sshd
2. 或者
3. # service sshd restart
```

15、现在使用 ssh 测试，你会得到下面的错误：

```
1. # ssh tecmint@192.168.0.10
```

```
tecmint@TecMint ~$ ssh tecmint@192.168.0.10
tecmint@192.168.0.10's password:
This service allows sftp connections only.
Connection to 192.168.0.10 closed.
tecmint@TecMint ~$
```

测试 SSH Chroot 监狱

试下使用 sftp：

```
1. | # sftp tecmint@192.168.0.10
```

```
tecmint@TecMint ~ $ sftp tecmint@192.168.0.10
tecmint@192.168.0.10's password:
Connected to 192.168.0.10.
sftp> pwd
Remote working directory: /home/tecmint
sftp> ls
sftp>
sftp> mkdir uploads
sftp>
sftp> ls
uploads
sftp> ls -l
drwxr-xr-x  2 tecmint  tecmint    4096 Mar  3 15:48 uploads
sftp> date
```

测试 sFTP SSH 用户

建议阅读：[使用 chroot 监狱将 sftp 用户限制在主目录中](#)。

就是这样了！在文本中，我们向你展示了如何在 Linux 中限制 ssh 用户到指定的目录中（chroot 监狱）。请在评论栏中给我们提供你的想法。

作者简介：

Aaron Kili 是一个 Linux 及 F.O.S.S 热衷者，即将成为 Linux 系统管理员、web 开发者，目前是 TecMint 的内容创作者，他喜欢用电脑工作，并坚信分享知识。

via: <http://www.tecmint.com/restrict-ssh-user-to-directory-using-chrooted-jail/>

作者：[Aaron Kili](#) 译者：[geekpi](#) 校对：[jasminepeng](#)

本文由 [LCTT](#) 原创编译，[Linux中国](#) 荣誉推出



#### 最新评论

发表评论

文剑一飞 [Chrome 58.0|Windows 10] 2017-06-01 16:53

赞 回复

不行哦，使用WinSCP工具，登录不成功。  
2017-06-01 16:49:29.097 Enumerating network events for socket 1280  
2017-06-01 16:49:29.097 Enumerated 32 network events making 32 cumulative events for socket 1280  
2017-06-01 16:49:29.097 Handling network close event on socket 1280 with error 10053  
2017-06-01 16:49:29.097 Selecting events 0 for socket 1280  
2017-06-01 16:49:29.097 Network error: Software caused connection abort  
\* 2017-06-01 16:49:29.190 (EFatal) 网络错误：软件造成的连接中止  
\* 2017-06-01 16:49:29.190 验证日志(具体情况参见会话日志)：  
\* 2017-06-01 16:49:29.190 使用用户名 "user02"。  
\* 2017-06-01 16:49:29.190  
\* 2017-06-01 16:49:29.190 验证失败。



按照楼主的方法测下来并不行啊

来自北京的 Chrome 45.0|Windows 10 用户 2017-03-22 15:382 赞 回复

同样不行

11hrj294055233 [Firefox 52.0|Ubuntu] 发表于 2017-03-16 22:28 的评论 :2 赞 回复

又学到了一招，不过然并卵

来自北京的 Chrome 45.0|Windows 10 用户 2017-03-22 15:371 赞 回复

然而并不是没有什么乱用！

vio [Firefox 51.0|GNU/Linux] 2017-03-17 14:334 赞 回复

got it

来自四川|成都的 Chrome 56.0|GNU/Linux 用户 2017-03-17 09:051 赞 回复

不是现在有容器了吗？比如 LXC，LXD，systemd-nspawn，Docker 等吗？

译自：tecmint.com  
原创：LCTT <https://linux.cn/article-8313-1.html>

作者：Aaron Kili  
译者：geekpi

本文由 LCTT 原创翻译，Linux中国首发。也想加入译者行列，为开源做一些自己的贡献么？欢迎加入 LCTT！  
翻译工作和译文发表仅用于学习和交流目的，翻译工作遵照 CC-BY-NC-SA 协议规定，如果我们的工作有侵犯到您的权益，请及时联系我们。  
**欢迎遵照 CC-BY-NC-SA 协议规定转载，敬请在正文中标注并保留原文/译文链接和作者/译者等信息。**  
文章仅代表作者的知识和看法，如有不同观点，请楼下排队吐槽 :D

★ 📄

上一篇：如何在 Ubuntu 下安装和配置 FTP 服务器

下一篇：如何在 CentOS 7 上安装和安全配置 MariaDB 10

LCTT 译者



**geekpi**  
共计翻译：**1615.5** 篇 | 共计贡献：**3013** 天  
贡献时间：2013-10-25 -> 2022-01-24  
[访问我的 LCTT 主页](#) | [在 GitHub 上关注我](#)

相关阅读

🔗 SSH

🔗 Chroot

在 Linux 中为非 SSH 用户配置 SFTP 环境2014-08-26

SSH 密钥管理工具2020-03-01

如何在 Linux 上为特定的用户或用户组启用或2020-03-23

如何在 Debian 10 中配置 Chroot 环境的2020-05-05

怎样在 Linux 下用 SSH 搭建个人文件服务器2020-05-27

