



链滴

# Linux ping: socket: 不允许的操作

作者: [expoli](#)

原文链接: <https://ld246.com/article/1578647657753>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

# Linux ping: socket: 不允许的操作

今天因为在安装系统的时候错误地估计了系统所需要的空间、最终导致根分区被文件全部占用没有剩空间了，所以使用 timeshift 将原系统整体备份灌装到另一拥有较大储存空间的硬盘中去（注：此硬已经做好了分区工作，在 GUI 界面上选择好对应的分区，然后进行恢复操作），恢复完成后在使用时候发现 ping 命令没办法正常工作、总是提示 **ping: socket: 不允许的操作**。

## 相关原因

在查阅相关资料之后发现这是 ping 没有相应的网络权限导致的问题：ping 命令在运行中采用了 ICMP 协议，需要发送 ICMP 报文。但只有 **root** 用户才能建立 ICMP 报文。而正常情况下，ping 命令的限应为 -rwsr-xr-x，即带有 suid 的文件，一旦该权限被修改，那么普通用户无法正常使用该命令。

## 解决方案

于是大家就会想到那么给它加上相应的权限不就行了。即：

```
sudo chmod u+s /bin/ping
```

一开始我也是这样认为得、不过因为系统的拥有者并不是 root 所以这个方法没有奏效，也幸好是这，所以查询到了另一种比较好的解决方案，即：

The practice of using setuid can be pretty dangerous, and so it is mostly discouraged. Linux has a "capabilities" system, where you can add only specific capabilities, instead of full system access. Ping most likely needs raw socket usage, in which case you'd run:

---

使用 setuid 的做法可能非常危险，因此不鼓励这样做。Linux 有一个“功能”系统，您只能在其中加特定功能，而不是完全访问系统。Ping 很可能需要使用原始套接字，在这种情况下，您需要运行：

```
setcap cap_net_raw+ep $(which ping)
```

```
$ getcap /bin/ping  
/bin/ping = cap_net_raw+ep
```

这时再次测试 ping 命令，它已经可以正常工作了。

参考资料：

[1] <https://github.com/microsoft/WSL/issues/1303>

[2] <https://github.com/MichaIng/DietPi/issues/1012>