

This repository was archived by the owner on Nov 3, 2023. It is now read-only.

zzzgydi / clash-verge Public archive

<> Code Issues 232 Pull requests 3 Discussions Actions Projects Wiki Security Insights

This repository was archived by the owner on Nov 3, 2023. It is now read-only.



## linux 下 tun 需要 setcap 配置权限才能用 #182

Closed



inRm3D opened on Sep 3, 2022

Contributor ...

一直没注意到 tun 没开（虽然开关是打开的，但是实际没有生效）。

命令行启动后发现 permission 报错。查了一圈发现要

```
sudo setcap cap_net_bind_service,cap_net_admin=+ep /usr/bin/clash
```

参考 <https://blog.icpz.dev/articles/tools/setup-clash-premium-on-linux/#Optional-Setup>

一些简单解释

CAP\_NET\_BIND\_SERVICE: 允许绑定到小于 1024 的端口

CAP\_NET\_ADMIN: 允许执行网络管理任务

cap\_effective (e),cap\_inheritable (i),cap\_permitted (p)

cap\_effective: 当一个进程要进行某个特权操作时，操作系统会检查 cap\_effective 的对应位是否有效，而不再是检查进程的有效 UID 是否为 0.

cap\_permitted: 表示进程能够使用的能力，在 cap\_permitted 中可以包含 cap\_effective 中没有的能力，这些能力是被进程自己临时放弃的，也可以说 cap\_effective 是 cap\_permitted 的一个子集.

然后就能 ping 通了

```
> ping -c 4 google.com
PING google.com (198.18.0.5) 56(84) 字节的数据:
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=1 ttl=64 时间=0.064 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=2 ttl=64 时间=0.093 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=3 ttl=64 时间=0.109 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=4 ttl=64 时间=0.121 毫秒
--- google.com ping 统计 ---
已发送 4 个包, 已接收 4 个包, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.064/0.096/0.121/0.021 ms
```



👍 4



inRm3D on Sep 4, 2022

Contributor

Author

...

补充, clash 字段里的勾, 除了 redir-port 不勾 <https://github.com/Dreamacro/clash/issues/2146#issuecomment-1133891285>, 其余都勾上。

## Clash 字段

- ☒ edpr
- ☒ hosts
- ☒ script
- ☒ payload
- ☒ profile
- ☒ sniffer
- ☒ iptables
- ☒ auto-redir
- ☐ redir-port



返回

保存

A circular profile picture of a person wearing glasses.

zzzgydi on Sep 4, 2022

Owner



tun的开启确实要权限。我在macOS里是这样设置的

```
sudo chown root:admin ./clash
sudo chmod +sx ./clash
```



bind-address

inRm3D on Sep 5, 2022 · edited by inRm3D

Edits ▾

Contributor

Author



感觉做成一个交互会好些？

比如 try open tun, except permission error, pop 一个输入密码的框，然后跑一下这个 sudo setcap, cfw 就是会有个 pop up 的弹窗。

从产品的角度考虑，用户应该不怎么看手册。

🔖 + on comment

🔖 zzzgydi added enhancement on Sep 6, 2022

🔗 inRm3D mentioned this on Nov 11, 2022

🔗 macOS 无法开启 tun 模式 #82

🔗 Binly42 mentioned this on Dec 3, 2022

🔗 ApplImage 使用 TUN模式 不太正常: setcap会无效, 而root执行则会有错 #312

🔗 Tadion mentioned this on Dec 11, 2022

🔗 修复 clash-meta 使用 tun 模式时的打包错误 archlinuxcn/repo#3075

🔗 Binly42 mentioned this on Dec 12, 2022

🔗 deb安装的包在普通用户下无法启动TUN模式代理，在root模式下无法保存用户数据 #320



br7roy on Dec 15, 2022



执行了相关命令，然后还是permission denied



br7roy mentioned this on Dec 15, 2022



[ArchLinux上无法启用TUN模式 #323](#)



Itsusinn mentioned this on Jan 5, 2023



[linux上非root用户使用TUN需要额外配置 #347](#)



inRm3D mentioned this on Jan 11, 2023



[TUN模式启动报错 #336](#)



jiesou on Jan 15, 2023



用 Applmage 的话运行时应用会被挂载到 /tmp/.mount\_\*\*\*  
比如 clash 的位置可能就是 /tmp/.mount\_clash-pzbvec/usr/bin/clash

但每次启动都会重新挂载，路径也是不一样的。肯定是软件里默认设一下比较好



cvpas on Mar 15, 2023



verge 1.2.3 , macOS13.1。已经

```
sudo chmod +sx /Applications/Clash\ Verge.app/Contents/MacOS/clash-meta 和  
sudo chown root:admin /Applications/Clash\ Verge.app/Contents/MacOS/clash-meta 但是还是一样提示  
Start TUN listening error: configure tun interface: Connect: operation not permitted
```



sarahgdc on Mar 16, 2023



verge 1.2.3 , macOS13.1。已经

```
``sudo chmod +sx /Applications/Clash\ Verge.app/Contents/MacOS/clash-meta
```

``和

```
``sudo chown root:admin /Applications/Clash\ Verge.app/Contents/MacOS/clash-meta
```

``但是还是一样提示

```
Start TUN listening error: configure tun interface: Connect: operation not permitted
```

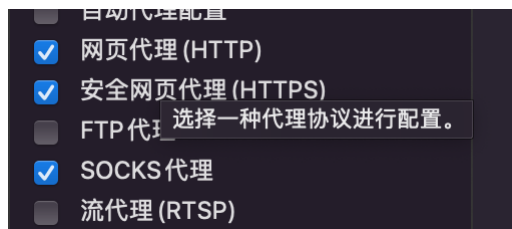
我也用了这个，然后Safari就打不开任何网页了，关掉clash verge后也不行，连百度也连不上，一直显示“cannot connect to the server”..请问这两行命令可以撤销吗？



zzzgydi on Mar 16, 2023 · edited by zzzgydi

Edits ▾ Owner ⋮

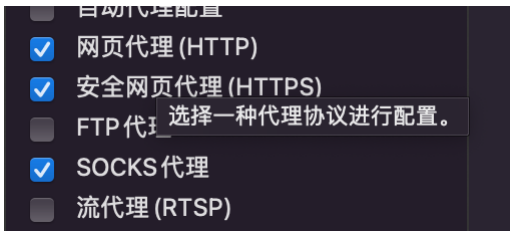
@sarahgdc 你这个不撤销也没事，如果打开verge还是上不了网，可以看看是否开了tun模式，开了的话，关掉就好。如果是关了verge也不能上网，就看看网络设置里的代理是不是没有清空，下图这些。



sarahgdc on Mar 16, 2023 · edited by sarahgdc

Edits ▾ ⋮

@sarahgdc 你这个不撤销也没事，如果打开verge还是上不了网，可以看看是否开了tun模式，开了的话，关掉就好。如果是关了verge也不能上网，就看看网络设置里的代理是不是没有清空，下图这些。



zzzgydi on Mar 17, 2023

Owner ...

1.3.0版本已经支持给clash内核点击提权啦，Linux的实现就是参考该issue的方案，可以试试有没有问题

zzzgydi closed this as completed on Mar 17, 2023



sarahgdc on Mar 17, 2023

...

1.3.0版本已经支持给clash内核点击提权啦，Linux的实现就是参考该issue的方案，可以试试有没有问题  
今天刚试了新版本，可以开tun了！感恩的心🙏



fecet on Mar 18, 2023 · edited by fecet

Edits ...

1.3.0版本已经支持给clash内核点击提权啦，Linux的实现就是参考该issue的方案，可以试试有没有问题  
点击了会提示refresh config, 但日志还是显示没有权限, 可能是什么原因  
edit: 原来是在clash内核那里设置提权, ok了

👍 1



lightingteeth on Mar 21, 2023

...

clash内核已经勾选了除redir-port以外的所有选项，开启tun模式，但是YouTube偶尔无法访问，访问后视频无法播放但是页面加载正常，Ubuntu。



**Binly42** on Mar 26, 2023



给 debian bullseye stable 的同志提个醒: (这里说的都是 deb包安装版)

- 1.1.2 , 即使做了全套, 也还是不行的
  - tun开启倒是没再报错, 但是更前面会有一条 `Permission denied (os error 13)` 的日志, 总之就是tun没法实际生效
- 1.2.3 已经开始有 glibc版本问题了, 先不要用
- 1.2.0 做全套之后是ok的 (我这clash默认是 `1001:lpadmin` ,也没用改



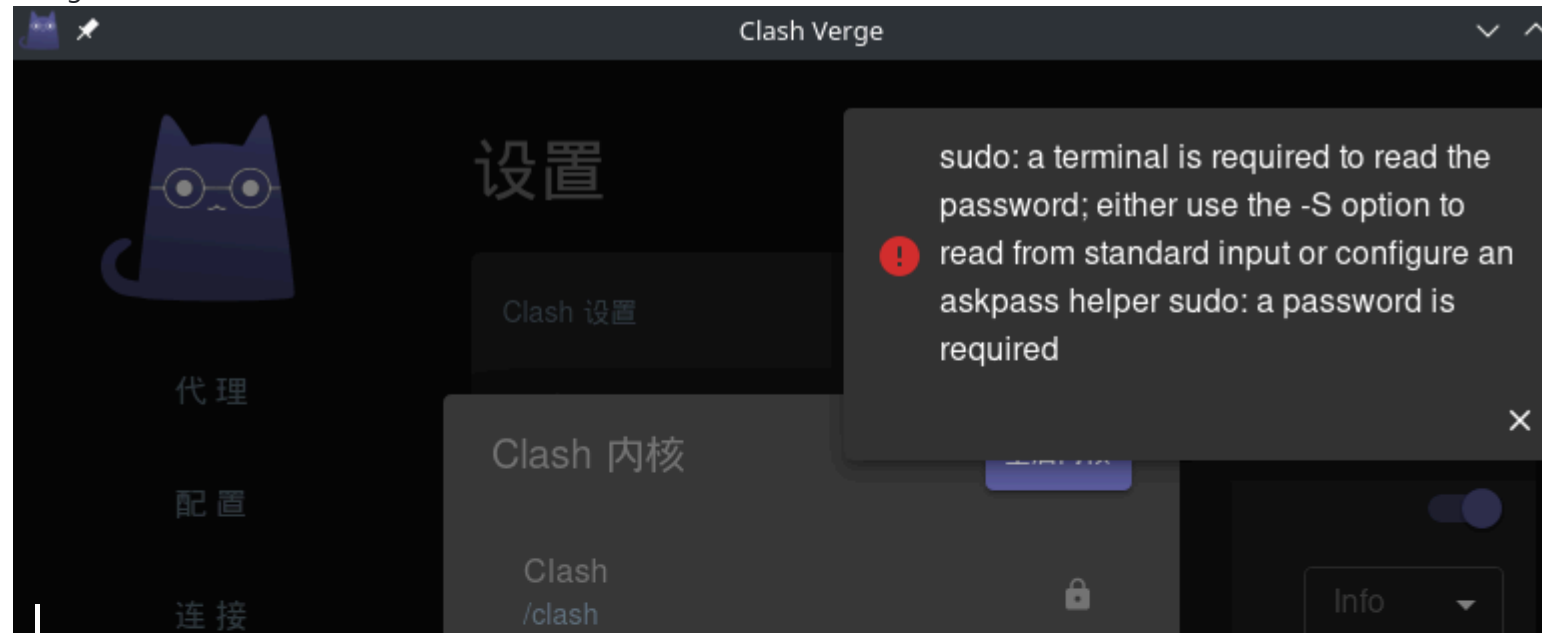
**Itsusinn** on Apr 14, 2023 · edited by Itsusinn

Edits ▼





Using non-root



sqwwqw5 on May 21, 2023

Same as [#182 \(comment\)](#) with the appimage version.

perqin on Jul 2, 2023

[@ltsusinn](#) [@sqwwqw5](#) To fix this issue:

1. Install any askpass helper, like `x11-ssh-askpass`, or `ksshaskpass` for KDE;
2. Edit `/etc/sudo.conf` and set the askpass helper path, like `Path askpass /path/to/your/askpass`

Now click the lock icon in Clash Verge again and it should work.

tigerinus on Oct 2, 2023

一直没注意到 tun 没开（虽然开关是打开的，但是实际没有生效）。

命令行启动后发现 permission 报错。查了一圈发现要

```
sudo setcap cap_net_bind_service,cap_net_admin=+ep /usr/bin/clash
```



参考 <https://blog.icpz.dev/articles/tools/setup-clash-premium-on-linux/#Optional-Setup>

一些简单解释

CAP\_NET\_BIND\_SERVICE: 允许绑定到小于 1024 的端口 CAP\_NET\_ADMIN: 允许执行网络管理任务

cap\_effective (e),cap\_inheritable (i),cap\_permitted (p)

cap\_effective: 当一个进程要进行某个特权操作时，操作系统会检查 cap\_effective 的对应位是否有效，而不再是检查进程的有效 UID 是否为 0. cap\_permitted: 表示进程能够使用的能力，在 cap\_permitted 中可以包含 cap\_effective 中没有的能力，这些能力是被进程自己临时放弃的，也可以说 cap\_effective 是 cap\_permitted 的一个子集.

然后就能 ping 通了

```
> ping -c 4 google.com
PING google.com (198.18.0.5) 56(84) 字节的数据。
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=1 ttl=64 时间=0.064 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=2 ttl=64 时间=0.093 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=3 ttl=64 时间=0.109 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=4 ttl=64 时间=0.121 毫秒
--- google.com ping 统计 ---
已发送 4 个包, 已接收 4 个包, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.064/0.096/0.121/0.021 ms
```



解决了我的大问题。

希望作者能把这一步集成到 cfw 初始化中。



然后就能 ping 通了

```
> ping -c 4 google.com
PING google.com (198.18.0.5) 56(84) 字节的数据。
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=1 ttl=64 时间=0.064 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=2 ttl=64 时间=0.093 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=3 ttl=64 时间=0.109 毫秒
64 字节, 来自 198.18.0.5 (198.18.0.5): icmp_seq=4 ttl=64 时间=0.121 毫秒
--- google.com ping 统计 ---
已发送 4 个包, 已接收 4 个包, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.064/0.096/0.121/0.021 ms
```



题外话顺便说一下, TUN模式下的 ping 好像是有问题的, 我这里试着:

- 用 原版的 clash premium , 域名或者ip随便写 都必然能通
- 用 clash meta , 无论如何都ping不通

好像说是 [不支持 icmp](#), 具体我没细究了;

但反正 `curl www.google.com` 啥的 应该是能用于验证的

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

#### Assignees

No one assigned

#### Labels

enhancement

#### Projects

No projects


Milestone

No milestone

Relationships

None yet






Development

 Code with agent mode

▼

No branches or pull requests

Participants

 +8