# 查看端口占用情况：

[root@abu-app vhost]# lsof -i:80

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

nginx 5289 root 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

nginx 5290 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

nginx 5291 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

nginx 5292 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

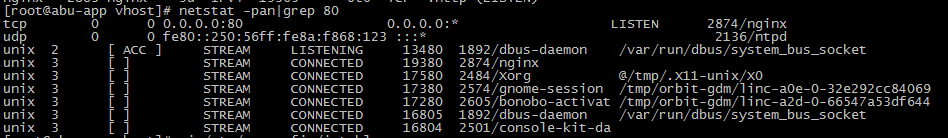
nginx 5294 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

nginx 5295 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

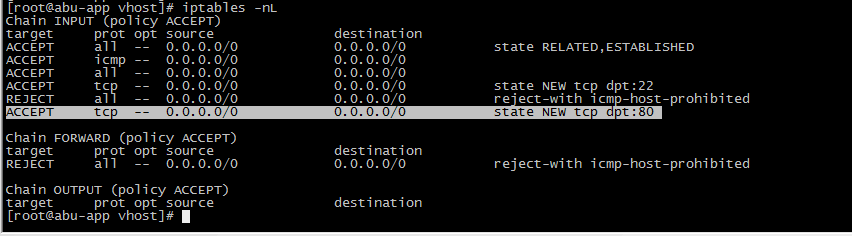
nginx 5296 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

nginx 5297 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)

nginx 5298 nginx 9u IPv4 25494 0t0 TCP \*:http (LISTEN)



# 查看防火墙规则：



# 添加防火墙规则

[root@abu-app vhost]# vi /etc/sysconfig/iptables

-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

# Firewall configuration written by system-config-firewall

# Manual customization of this file is not recommended.

\*filter

:INPUT ACCEPT [0:0]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-host-prohibited

-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT

# 重启防火墙

[root@abu-app vhost]# service iptables restart

iptables：将链设置为政策 ACCEPT：filter [确定]

iptables：清除防火墙规则： [确定]

iptables：正在卸载模块： [确定]

iptables：应用防火墙规则： [确定]

# [nginx: open failed, permission denied](http://www.tlanyan.me/nginx-open-failed-permission-denied/)

[tlanyan](http://www.tlanyan.me/author/tlanyan/) 发布于 [2014 年 11 月 10 日2015 年 7 月 15 日](http://www.tlanyan.me/nginx-open-failed-permission-denied/)

http://www.tlanyan.me/nginx-open-failed-permission-denied/

*估计受bash和ssl漏洞的影响，近期centos系统更新了许多包。对nginx而言，最重要的影响是其context已经被加入到了selinux策略里。nginx的许多行为都受到了这些更新的影响，例如配置文件的读取，执行环境等。*

*另外gitlab的ssh免密码登陆也受到了selinux安全策略更新的影响。*

*文章记录了发现这个现象和找到问题及解决方案的过程。*

个人代码托管平台是使用gitlab自己搭建的。今天推送和更新时发现竟然提示需要git账号的密码。心头不由一阵疑惑：这TM搞的什么鬼？！难道没有把这个开发机的key条件到受信任的key列表里吗？添加当前key到受信任ssh列表，却提示已经添加过了。

心想gitlab估计是抽风了，那就重启一下吧。把服务器重启了，发现这次是nginx不运行了！赶紧chkconfig看了一下，nginx应该是自动启动的啊！近期又没有改动过什么配置，怎么就自动启动会失败了呢？！心中顿时有种万千草泥马狂奔而过的感觉！没办法，那就手动重启吧！

手动重启竟然也失败了！提示是打开gitlab下的nginx 配置文件失败，提示：

接着查看了一下nginx的运行用户和文件权限，该文件为所有人可以访问。可是这么宽容的安全策略，再次尝试重启nginx发现还是这个错误提示！！

这个时候的我已然快要怀疑要么是我疯了，要么是电脑疯了。没办法，只好猜测是不是Nginx对文件有缓存，刚更改的权限没有生效？那就重启一下试试吧！但是这又闹的是哪一出啊？！！这么脑残的理由和解释说出来连自己都不会相信吧？！！

没办法，那就又把服务器重启了。果然，问题还是没有解决，相同的提示，同样的无解！！妈蛋啊，这都在搞毛线啊！没办法了，服务器是大爷。那就把配置文件放到/etc/nginx下面，这样总有权限了吧！

再次启动nginx，结果还是失败！不过提示变了，变成了：

坑爹啊，印象中除了nginx没有其他程序会使用这个端口的啊！使用netstat -alpn | grep 8080一下，果然没有程序占用！root都不能打开，这TM还是root用户吗？！！

8080端口不行，那就试试其他的呗！妈蛋！不管是1024以上的，还是1024以下的都不行！这TM还有没有原则了？！说好的root用户有一切权限的呢？！怎么一个空闲的端口都不能打开和监听！！人与机器之间最基本的信任都去哪了？！！

咆哮已然远不能表达我的内心的感觉了，赶紧喝口水冷静一下。然后分析root用户都没有权限打开的可能性会有什么呢？想来想去唯有selinux才能办到了。将selinux关闭，再次启动，果然，一切问题解决了！

**ps：**

* 受selinux影响，/var/log/audit/audit.log里会记录打开失败的原因。
* 关闭selinux只是临时的办法，如需开启selinux的情况下正常使用nginx，需要更改selinux策略。