背景：公司公网网站经常卡顿，经查有些ip对网站发起频繁访问，疑似被黑客攻击，请定位出问题，并解决

- 公司公网网站经常卡顿，经查有些ip对网站发起频繁访问，现要求写一个shell脚本屏蔽这些高频繁访问的ip（基于 firewall防火墙，网站是以Nginx作为中间件，nginx日志路径：/usr/local/nginx/logs，一分钟超过200视为频繁）
  - 答案：

```
#!/bin/bash
DATE=$(date +%d/%b/%Y:%H:%M)
NGINX_PATH=/usr/local/nginx/logs/access.log

#先tail防止文件过大，读取慢，数字可调整每分钟最大的访问量。awk不能直接过滤日志，因为包含特殊字符。
ABNORMAL_IP=$(tail -n5000 ${NGINX_PATH} |grep $DATE |awk '{a[$1]++}END{for(i in a)if(a[i]>200)print i}')

#执行防火墙
if [ ! $ABNORMAL_IP ];then
          exit
  else

      for IP in $ABNORMAL_IP;
          do
firewall-cmd --permanent --add-rich-rule="rule family="ipv4" source address="${IP}" port protocol="tcp" port="80" reject" && firewall-cmd --reload
echo -e  "${IP}\n" >>/usr/local/nginx/shell_script/nginx_firewall_result.txt

          done

fi

#查看防火墙规则
#firewall-cmd --zone=public --list-rich-rules
#放开防火墙对ip的限制
#firewall-cmd --permanent --add-rich-rule="rule family="ipv4" source address="${IP}" port protocol="tcp" port="80" accept" && firewall-cmd --reload
#如果未生效，编辑配置文件
#vi /etc/firewalld/zones/public.xml
#重启防火墙服务
#systemctl restart firewalld.service
```