进入C:\Windows\System32\drivers\etc找到hosts文件，将hosts文件拖出来修改后，再拖进去。

61.174.9.83 zabbix.anquan.io

61.174.9.83 smokeping.anquan.io

61.174.9.83 audit.anquan.io

61.174.9.83 cacti.anquan.io

61.174.9.83 audit.anquan.io

61.174.9.83 manage.anquan.io

61.174.9.83 cmdb.anquan.io

添加进去后电脑即可访问网站。

zabbix.anquan.io

smokeping.anquan.io

audit.anquan.io

cacti.anquan.io

audit.anquan.io

manage.anquan.io

cmdb.anquan.io 以上网站的统一代理

账号 shengchao

密码 Vx40kJbiYMnp6Ejp

audit.anquan.io 账号密码

账号shengchao

密码Vx40kJbiYMnp6Ejp

manage.anquan.io 账号 密码

账号shengchao@fastweb.com.cn

密码1aPNUJ

cacti监控 ：hosts绑定，通过代理连通：  
202.85.220.92 cacti.anquan.io   
C:\Users\sc\AppData\Local\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttp://cacti.anquan.io/cacti  
盛超：  
账号shengchao

密码r!e5s7x

资产管理cmdb.anquan.io

账号shengchao

密码： 6rbuCK

机房网络波动监控网址

<http://smokeping.anquan.io/smokeping/>

worktile 账号 shengchao\_

营销qq

1001@800109969

登录密码：k4taycw2yz

管理子帐号的超级密码：h2k1hzqbfaoe

1002@800109969   牛盾客服1  
密码：r9CliUvRsxqDGkI  
1003@800109969   牛盾客服2  
tangji$123$  
  
牛盾安全云QQ  
2114736369  
GuS@U5ozWja@

牛盾官网账号

1416047852@qq.com

 sql111

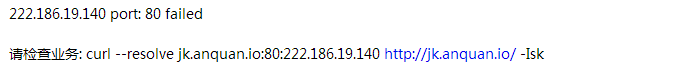
监控机

1、  
119.90.62.82:12321  
用户名 fw    
密码

 iKp\*h%sxRAwe%YmC    
2、  
113.31.30.59:12321  
用户名  administrator   
密码  eExnZrW&&S#m

邮件报警

Vip 异常

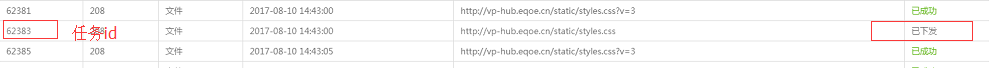


 测试

Curl –x IP:端口 目标网址

curl -x 222.186.19.140:80 jk.anquan.io -Is 返回200则为正常，无返回，或返回其他状态码则为异常

缓存刷新报警

**PROBLEM: purge tid:62383 failed nodes:2** 

正常情况后台显示已成功，如果长时间显示已下发，则表示部分节点下发失败

可在61.174.14.200 上查看节点是是否有刷新任务的id

salt -N waf cmd.run "grep 62505 /var/log/purge.log | tail -3"

重启下没有返回数据的节点上的缓存刷新服务

python /usr/local/ops/purge/sub\_purge restart

或者批量操作 salt -N waf cmd.run "python /usr/local/ops/purge/sub\_purge restart”(普通用户缓存刷新失败操作)

如果批量刷新缓存还是不行，使用强制刷新缓存

salt -N waf cmd.run 'curl -x 127.0.0.1:80 -XPURGE -H "Accept-Encoding:gzip, deflate, sdch" http://www.kgc.cn/zhuanti/tencenthtml.shtml -Isk'

####如果是军网缓存刷新失败需要先执行刷新父层的操作，在执行刷新waf的操作

salt -N pwaf cmd.run "python /usr/local/ops/purge/sub\_purge restart”(军网缓存刷新失败操作)

salt -N waf cmd.run "python /usr/local/ops/purge/sub\_purge restart”

PROBLEM: 42.236.6.29 redis replicate down 6377 redis复制进程down掉会影响用户后台修改后的配置的下法时间

ps aux | grpe redis 查看redis进程是否在

如果进程不在 /etc/init.d/ndserver restart 重启服务

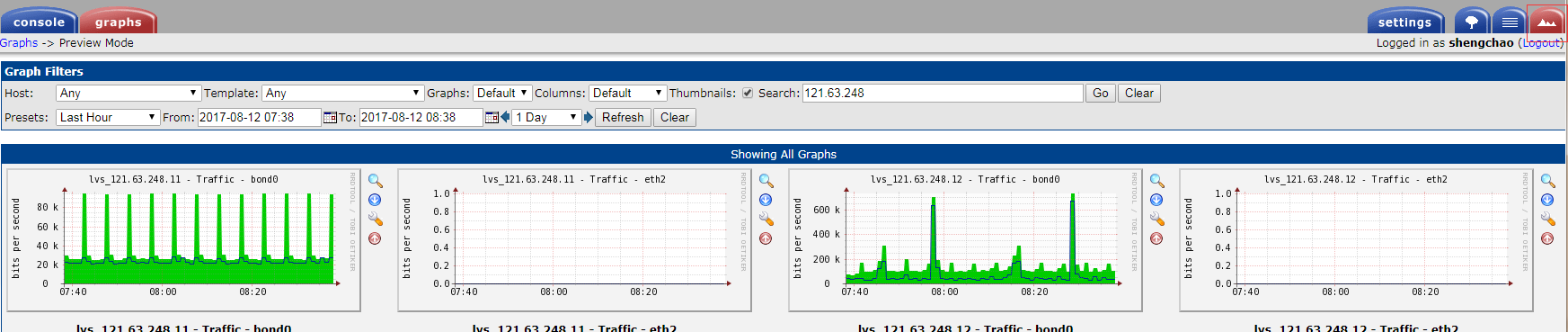
PROBLEM: 124.193.166.140 is unavailable by ICMP

测试是否可以正常ping通，正常登陆，是否丢包.

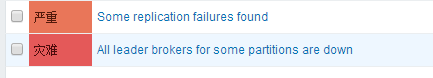
测试正常则忽略，有问题则联系运营商

PROBLEM: 113.207.30.182 traffic in greater than 700M on eth2

Cacti上查看该节点流量情况，lvs机器为万兆网卡，少量攻击节点可以抗住，如果攻击流量达到9G以上需要切清洗节点，先引流，在清洗，就近选择相同的运营商。

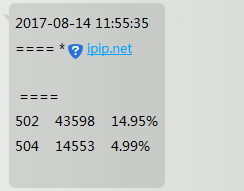






Kafka 报警，有问题及时通知

5XX报警



可在kibana中查看具体是哪个子域名有报警，本地hosts绑定报警域名和源站ip ,查看源站是否正常，如果绑定源站无法访问，及时通知用户查看源站是否正常。

机器人的账号和密码

账号：3235304191  
密码：84h8yegeMPsA  
监控群如果没消息，wugq 61.174.9.83，  
先看是否有二维码文件，如果有直接下载扫码   
sz /tmp/mojo\_webqq\_qrcode\_3235304191.png,  
如果没有文件，执行sh qq\_restart.sh杀死进程，一分钟后进程会自动起来，ps aux | grep perl 看进程是否起来，起来后下载二维码文件扫码登录

### 军网回源切换

1.监控群发现军网域名有5xx报警，去父层机器上测试源站是否正常（wget -SO /dev/null[http://www.81.cn](http://www.81.cn/) -e http\_proxy=111.203.147.1），返回200则正常，连接超时则异常  
2.如果持续异常通知军网检查源站情况  
3.如果军网需要切换回源ip,去61.174.14.200和113.31.27.239修改vim /cache/cache/salt/nginx/pwaf\_mod/upstream\_mod.conf（需要启用哪个源，就把那个源前面的注释拿掉），修改后pwaf设备会自动同步并reload nginx。  
4.检查父层设备是否都同步成功，如果没有手动修改下。（vim /usr/local/ndserver/nginx/conf/mod/upstream\_mod.conf）

### 设备下架操作步骤

1.boss上暂停解析  
2.lvs中踢出集群（sh anzhuang.sh outlvs）  
3.机器上停掉sub\_purge 刷新脚本和对应计划任务（先停计划任务）  
4.9.82redis中删除hostname中对应的主机  
5.删除zabbix监控和cacti  
6.boss上回复case  
7.cmdb中修改设备状态  
redis 删除操作  
history | grep redis 查看历史记录，复制历史命令登录redis  
输入 srem hostname "ctl-zj-061-130-028-072" (删除命令)  
如果误删 输入 sadd hostname "ctl-zj-061-130-028-072" (添加命令)

节点检测，不同的版本，测试网址不同

http://jk.anquan.io/check\_cdn\_health.html 免费版

http://jk.anquan.io/check\_cdn\_health.html?1 专业

http://jk.anquan.io/check\_cdn\_health.html?2 商务版

http://jk.anquan.io/check\_cdn\_health.html?3 企业版

日志字段含义

clientip 客户端ip

domain 域名

hit\_status 缓存状态（HIT-缓存 MISS-没缓存 BYPASS-不缓存回源 EXPIRE-缓存过期）

host waf节点主机名

method 请求方法

p\_response\_time 父层/源站 响应时间

p\_server 父层/源站 ip地址:端口

p\_status 父层/源站 响应状态码

protocol HTTP协议

referer 从哪个页面链接过来的

request 请求uri

size 请求body大小

ss waf节点响应时间

status waf节点响应状态码

time 请求发起时间

审核规范

1. 未取得ICP备案号的网站不允许使用国内安全节点。

2. 网站打不开或无任何实际内容，导致无法判断网站运营范围的网站不允许通过。

3. 网站内容以外文为主且非中文网站不允许通过。

4. 相关机构提示网页有威胁的，有非法信息提示不允许通过。

5. 医院类型网站（流产，皮肤病，性病等医院），未获得卫生部资质网站，不允许通过。

6. 网站主体内容含有色情（视频交友，一夜情交友）、违法（办假证，贩卖仿真枪）、黑客（非技术交流网站）、钓鱼网站、游戏私服、游戏外挂、网赚（传销性质网站）、成人用品、保健用品（减肥药）、两性、美女贴图和动漫贴图（尺度过大）、赌博（含贩卖赌博工具。）等低俗内容。

7. 网站存在恶意流氓广告（存在非法内容视频链接，非法网页内容链接）。不允许通过。

8. 网站内容存在版权风险的网站（视频，小说，音乐网站）不允许通过。

9.网站含有药品销售、保健品销售，但未取得资质的，或严重夸大药效事实。不允许通过。

10.网站主要业务为向非法网站提供支付、交易平台、担保，代理外国金融理财（炒股，炒现货，炒黄金）等服务的网站。不允许通过。

11.网站中大量存在影响社会和谐稳定的内容的网站（涉嫌攻击国家，攻击领导人，攻击人民，言论煽动性质网站）。不允许通过。

12. 工信部通知，所有网站均需在网站首页体现网站备案号及工信部链接http://www.miitbeian.gov.cn/state/outPortal/loginPortal.action