客户第一 用心服务

ANYSEC-日志审计快速配置手册

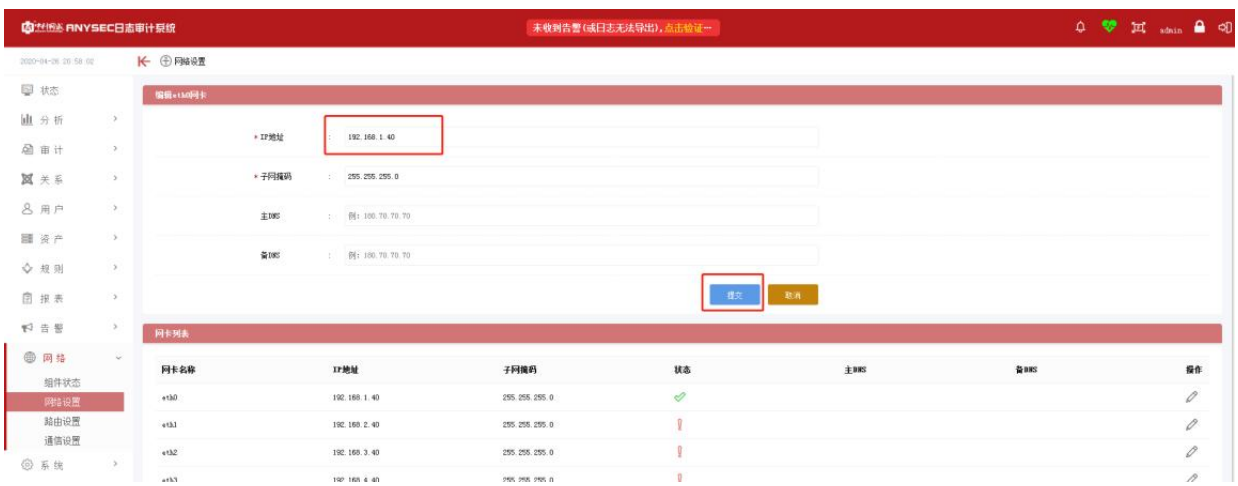
总机电话-- 0755-83658009 技术支持-- 0755-83658229 24 小时技术值班热线-----135-1069-3536
http://www.anysec.com 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

1、登录

E0 口登录地址：https://192.168.1.40

用户名：admin　　密码：admin123456

- IP 地址修改



2、添加资产

资产-资产列表-右上角添加资产或批量导入资产

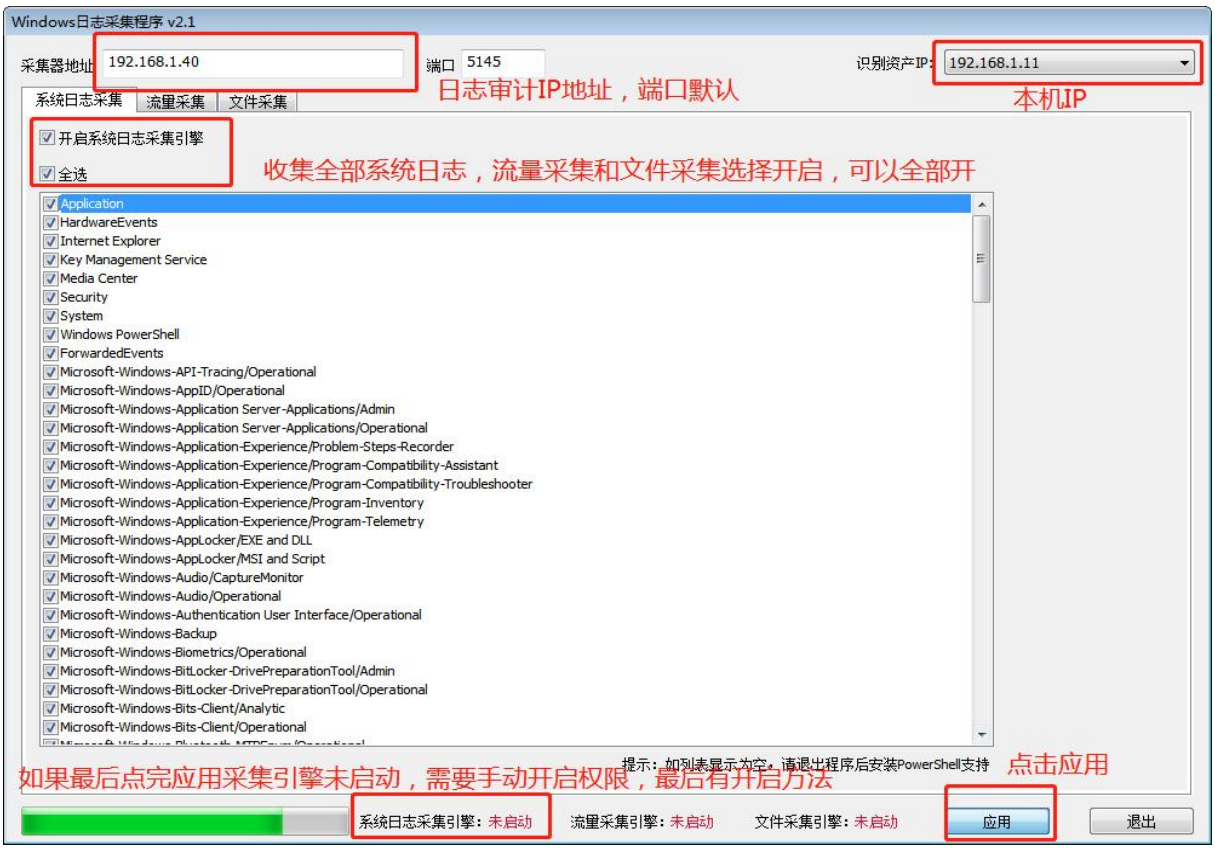
- 添加 Linux_Syslog 资产参数

- 添加 Windows syslog 资产参数

- 添加后的资产列表

3、客户端主动推送设置

收集 Windows 日志：需要在系统-插件中心内下载 windows agent 客户端并安装到设备上。



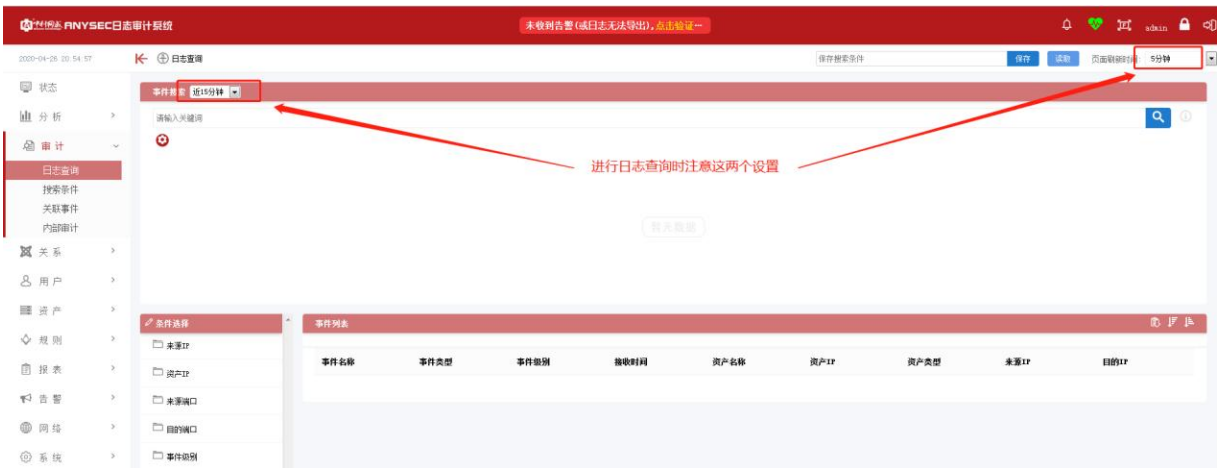
收集 Linux 日志，打开 Linux 服务器命令行界面，按如下步骤执行：

vi /etc/rsyslog.conf　　编辑 rsyslog.conf 配置文件

. @192.168.1.40　　192.168.1.40 是日志审计设备的 IP 地址

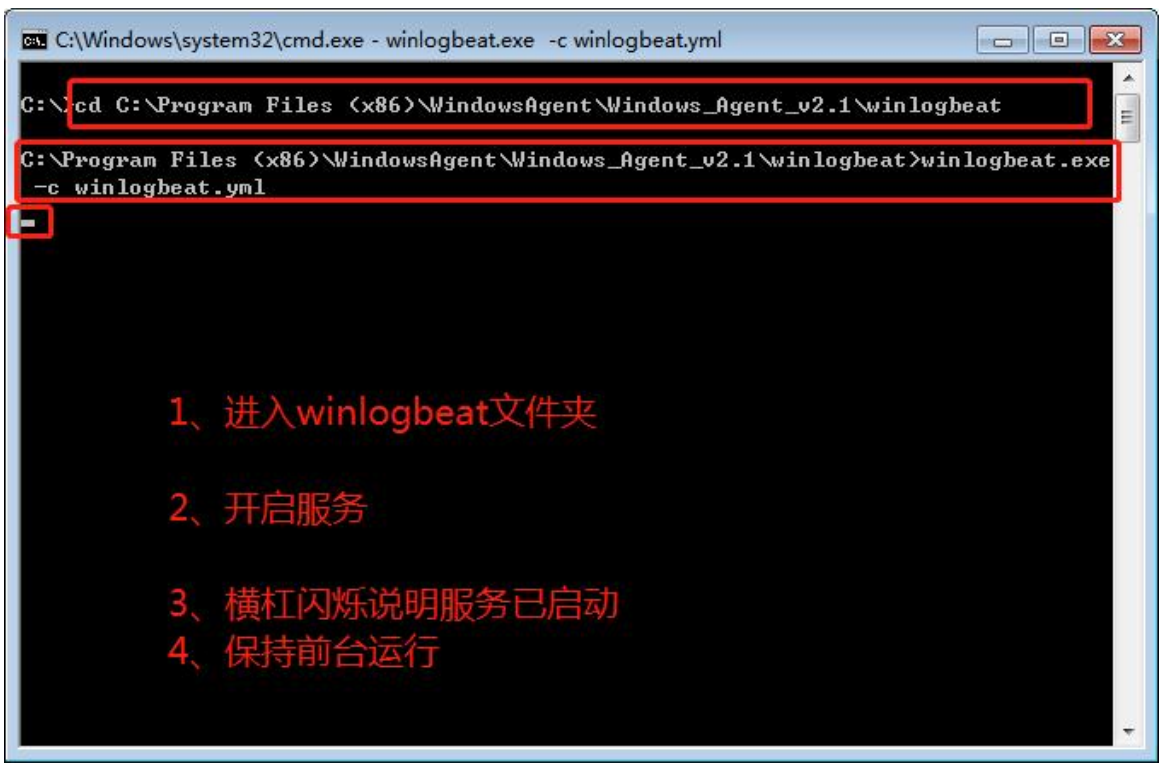
systemctl restart rsyslog　　重启日志服务

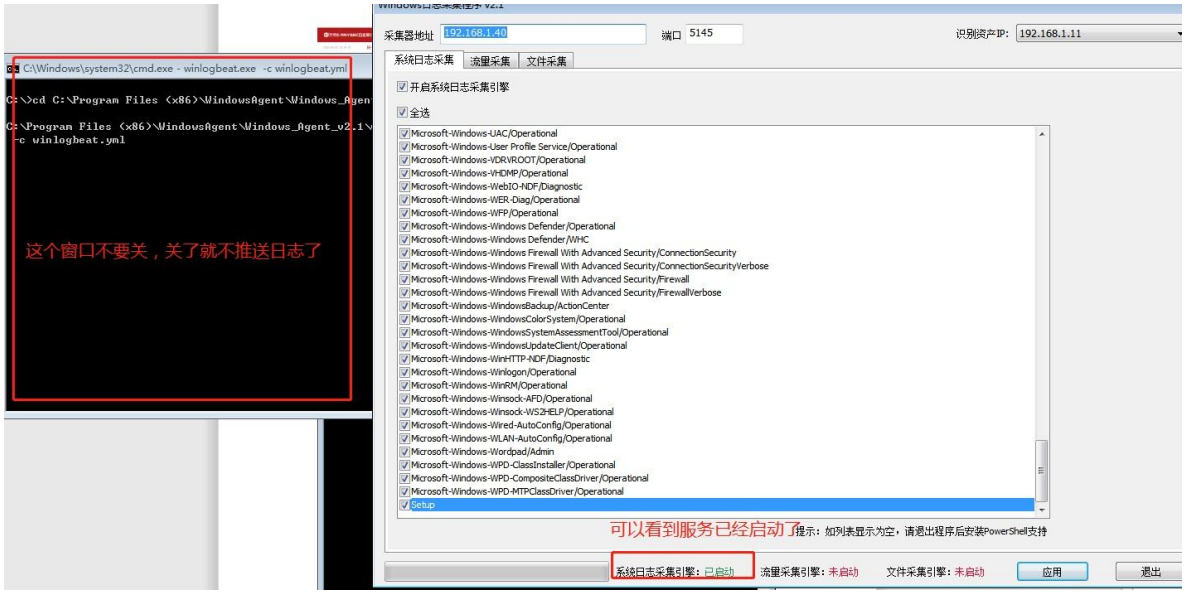
4、日志查询及审计



5、可能遇到的问题

Windows 采集引擎未启动,，需要手动开启系统日志推送服务




C:\Windows\system32\cmd.exe - winlogbeat.exe -c winlogbeat.yml
这个窗口不要关，关了就不推送日志了
采集器地址 192.168.1.40
端口 5145
识别资产IP: 192.168.1.11
系统日志采集
流量采集
文件采集
开启系统日志采集引擎
全选
可以看到服务已经启动了
系统日志采集引擎: 已启动
流量采集引擎: 未启动
文件采集引擎: 未启动
应用
退出

- 可以查看到日志了