使用云平台下发运维脚本配合威胁情报做安全威胁阻断

1. 简介

前段时间 Panabit 联合天际友盟发布了威胁情报 2.0APP 集成下发了威胁情报域名及 IP 库，有小伙伴反馈自己管理的设备比较多，每台登录进行配置非常麻烦而且很耗时间，有没有什么方法能完成批量设备的阻断策略，本文档主要介绍如何，结合云平台的运维脚本下发功能配合安全情报库完成对恶意域名及 IP 库的阻断。

2. 威胁情报库阻断

2.1. 前期准备

2.1.1. 必备清单

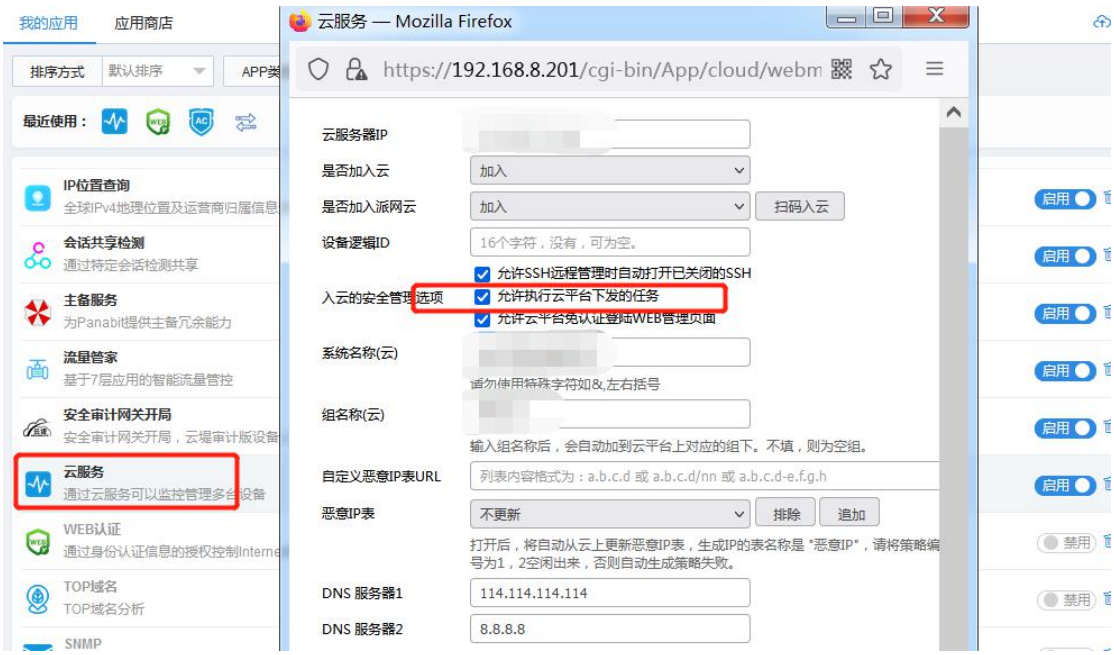
序号	名称	功能及用途说明	备注
1	云平台	集中管理设备，集中下发运维脚本，如阻断僵尸网络，挖矿行为管理等策略。	需升级到 2022.03.21 隋 R2P2 以上版本，脚本运维优化下发更快
2	Panabit 设备	通过 DNS 管控，http 管控，流量控制策略阻断非法行为	需升级到 2022.03.21 隋 R2P2 以上版本，新版本解决库数量过大导致失效的问题
3	威胁情报 2.0APP	用于实时接收更新天际友盟的安全库	
4	运维脚本	用于实现一键下发 DNS 管控，http 管控，流量控制策略给 Panabit	只针对威胁情报 APP 下发的群组有效
5	云服务 APP	用于对接云平台服务	必须勾选允许执行下发任务

2.1.2. 版本获取途径

Panabit 版本，云平台版本，云服务版本，安全情报 2.0APP 都可以在论坛专用版块进行获取，论坛地址为：https://bbs.panabit.com/

2.1.3. 云服务配置

云服务勾选示例图



2.1.4. 脚本说明

本脚本会根据威胁情报 2.0APP 同步后的 IP 及域名群组进行检测将获取到的 IP 及域名群组，添加至 DNS 管控，流量控制，http 管控策略中，设备上如果没有策略组，会生成名称为 default 策略组，并自动添加策略后调度策略组为缺省，如有策略组，序号 10-X 往后根据获取到的威胁情报 IP 群组数进行策略添加。

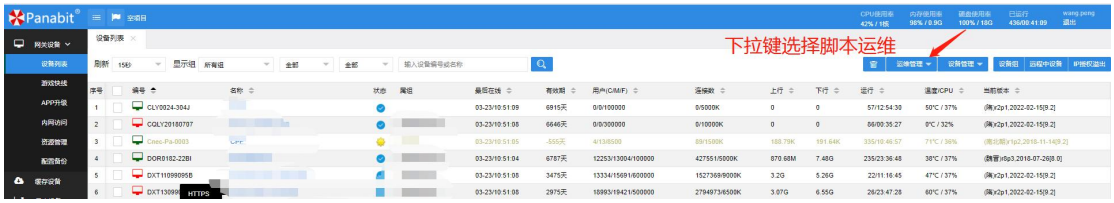
2.1.5. 脚本附件

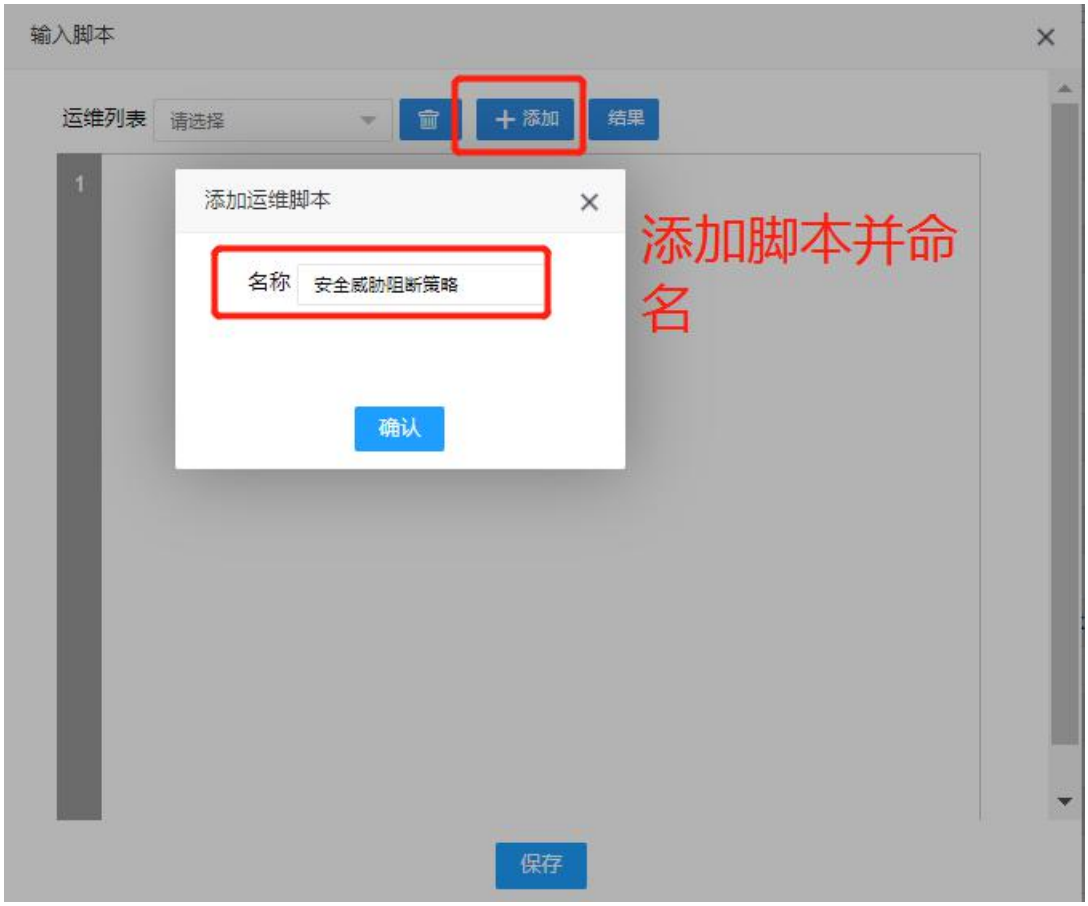
脚本文件下载
https://www.kdocs.cn/view/l/cnCcJ9q4WmKu

2.2. 配置步骤

2.2.1. 创建脚本

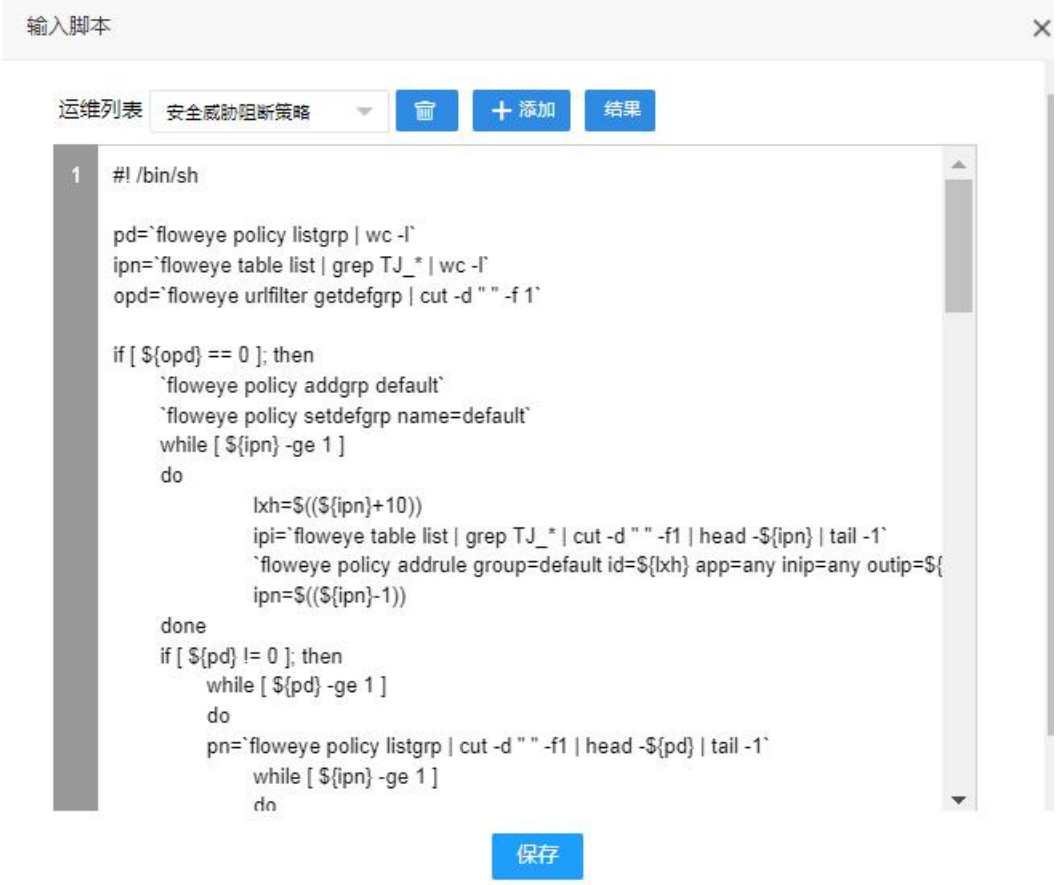
在云平台中，依次打开【网关设备】-【设备列表中】-鼠标移动到【运维管理】下拉框-点击【脚本运维】添加脚本并命名。





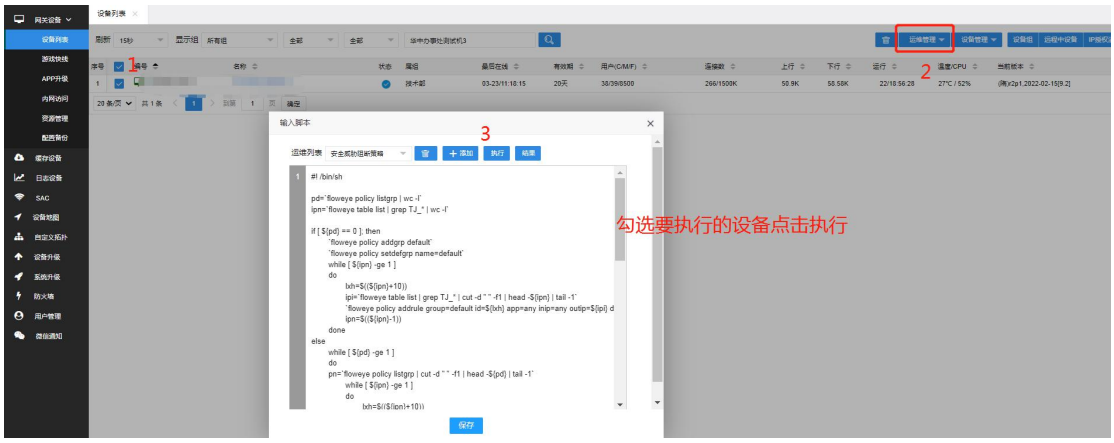
2.2.2. 添加脚本内容并保存

选择创建好的脚本，并复制脚本内容到云平台提供的剪切板，点击保存。



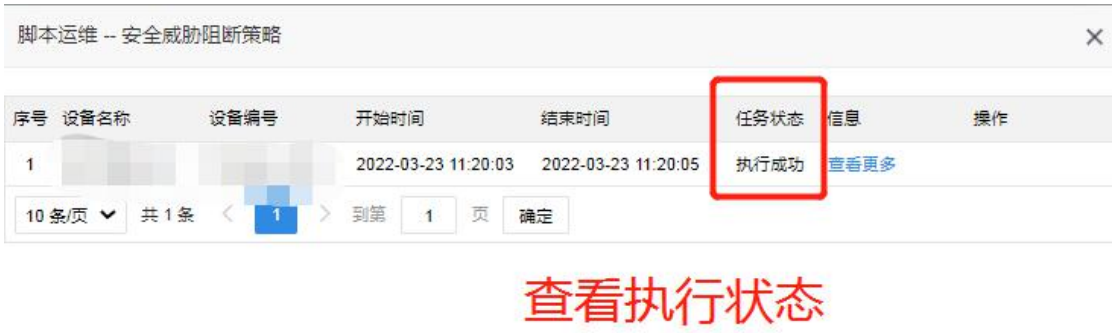
2.2.3. 执行脚本任务

选中要执行的设备（带有威胁安全情报库）的设备，在【运维管理】-【脚本运维】，选择我们之前创建好的脚本点击执行。



2.2.4. 查看执行结果

点击结果按钮查询脚本的执行结果。



查看执行状态

3. 总结：

Panabit 云平台是可以集中对派网产品 Panabit、IXCache、Panalog、小派 AP，进行远程监控和管理的可视化免费云服务平台。云平台功能丰富，其中有非常多的实用功能帮助我们实现简单方便的运维管理，脚本运维能集中下发指令给多台 Panabit 设备，一键批量添加策略、IP 群组、域名群组域名路由等非常实用的功能，不仅仅是能针对挖矿恶意木马僵尸网络等行为进行统一进行封堵还有更多的实用使用方法，欢迎大家在论坛踊跃地提出配置需求。