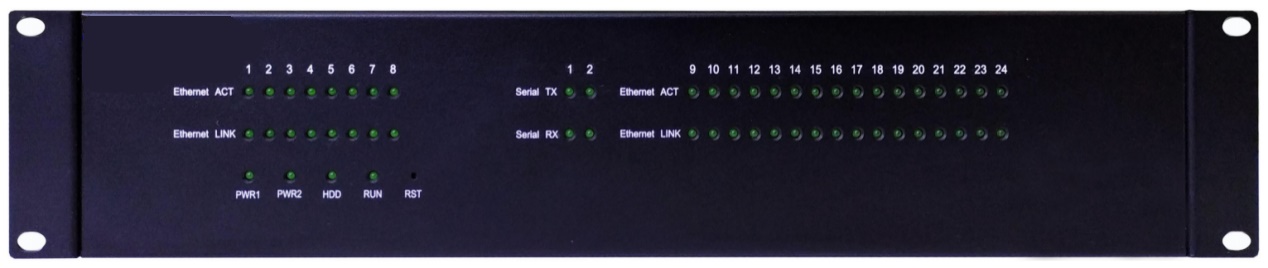
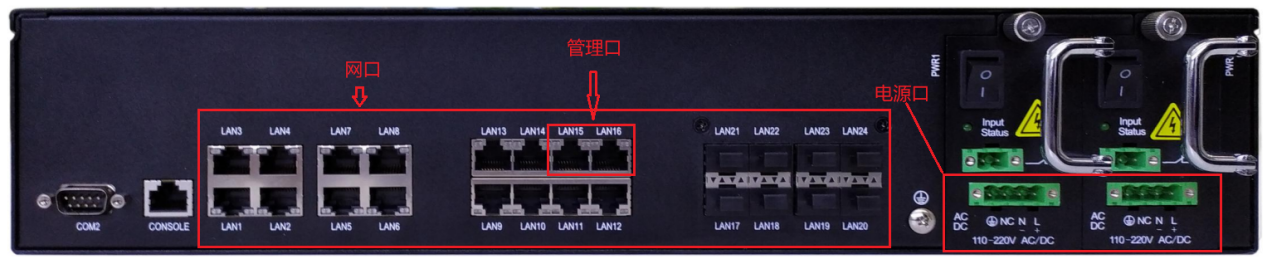
**态势感知UI管理配置手册**

1. 装置面板介绍

1.1网口与网卡的对应关系



前面板图



后面板图

本装置网卡名称前面板标识的对应表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| eth0 | eth1 | eth2 | eth3 | eth4 | eth5 | eth6 | eth7 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| eth8 | eth9 | eth10 | eth11 | eth12 | eth13 | eth14 | eth15 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

1. 装置管理

2.1管理方式

2.1.1.Console

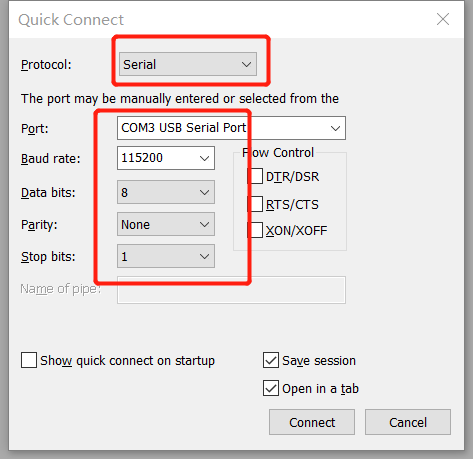
通过装置console口登录后台进行管理，波特率为115200

注：目前新装置的波特率均为115200，较早的装置波特率可能为9600

账号root 密码power@2018

以下为各仿真软件登录界面，需要进行配置的地方已框出

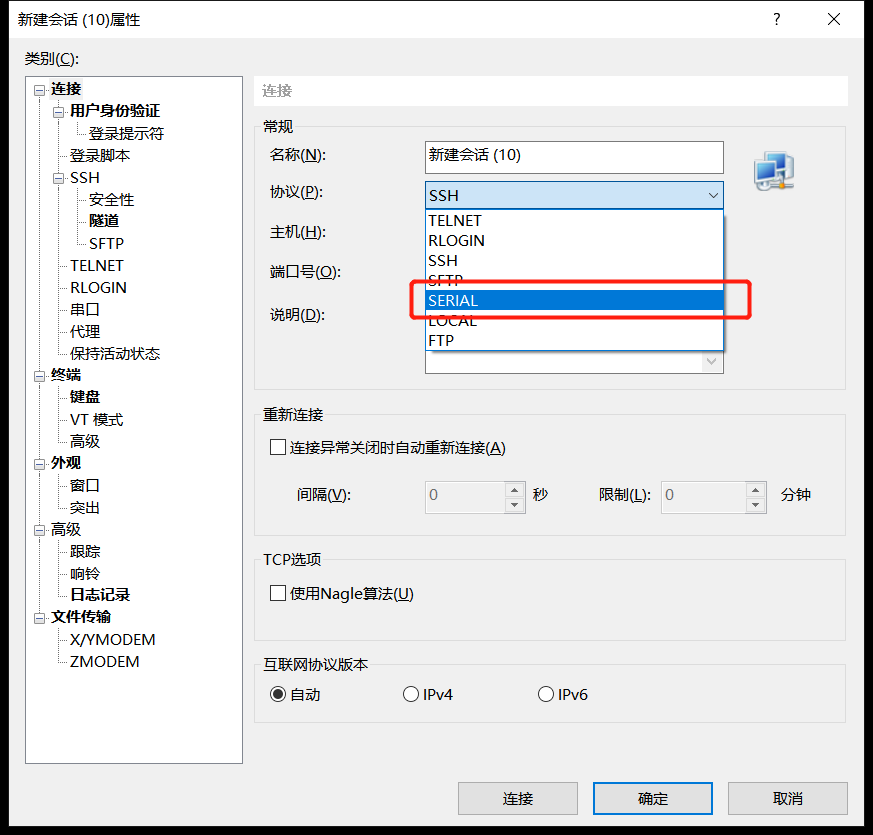
SecureCRT：

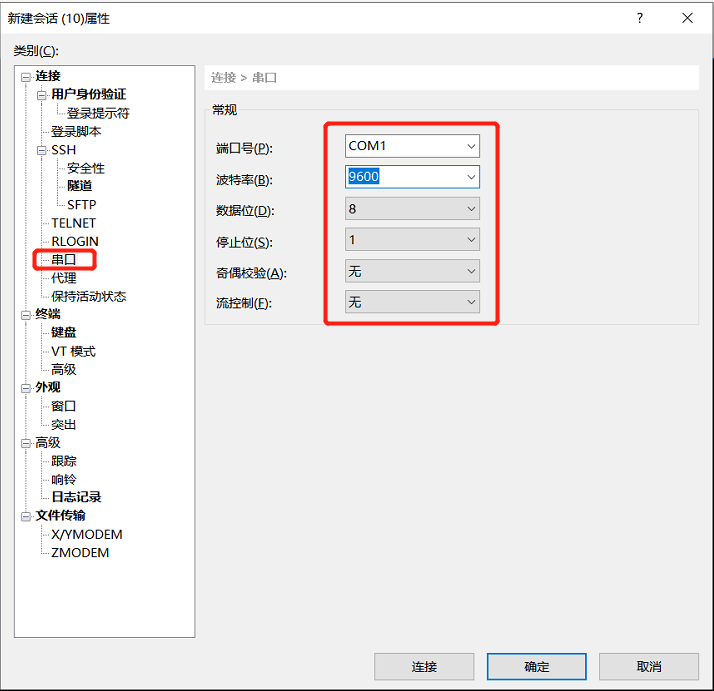


MobaXterm：



Xshell:





2.1.2.SSH

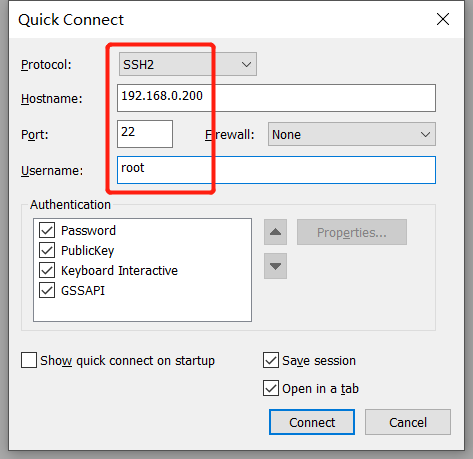
通过SSH登录装置后台进行管理，电脑需连接对应管理网口并配置对应网段IP，电脑能够ping通管理IP。

账号root 密码power@2018

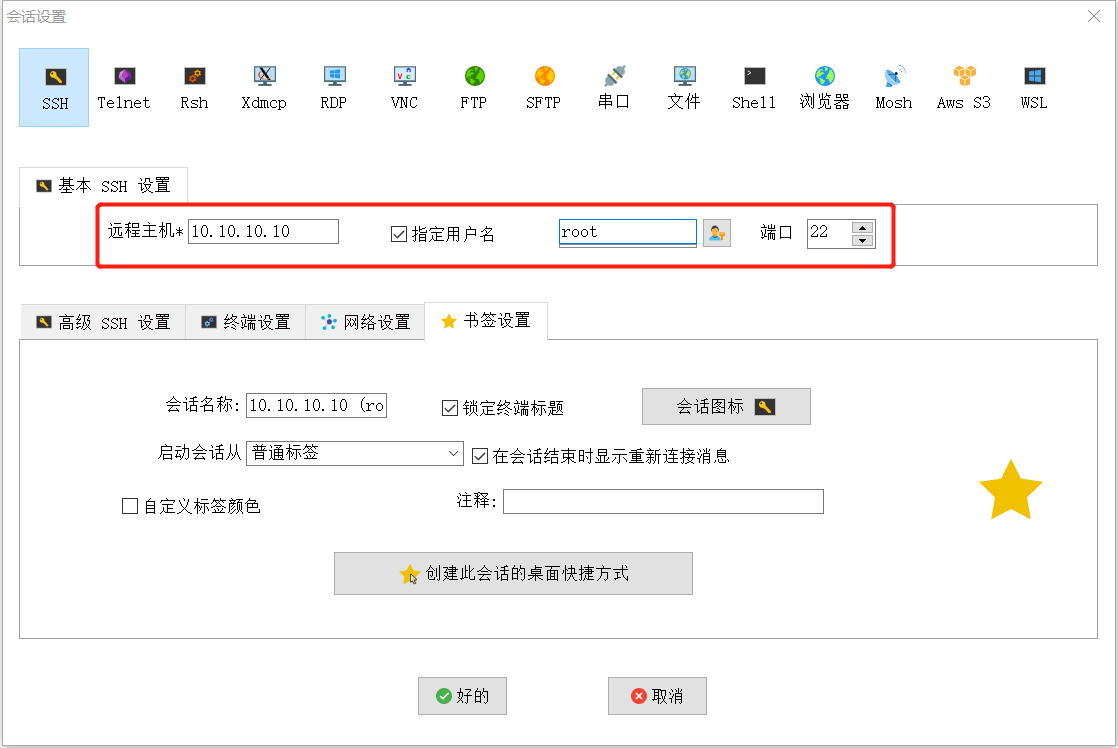
管理网口及IP：15口（10.10.10.10）、16口（192.168.0.200）

以下为各仿真软件的登录方式

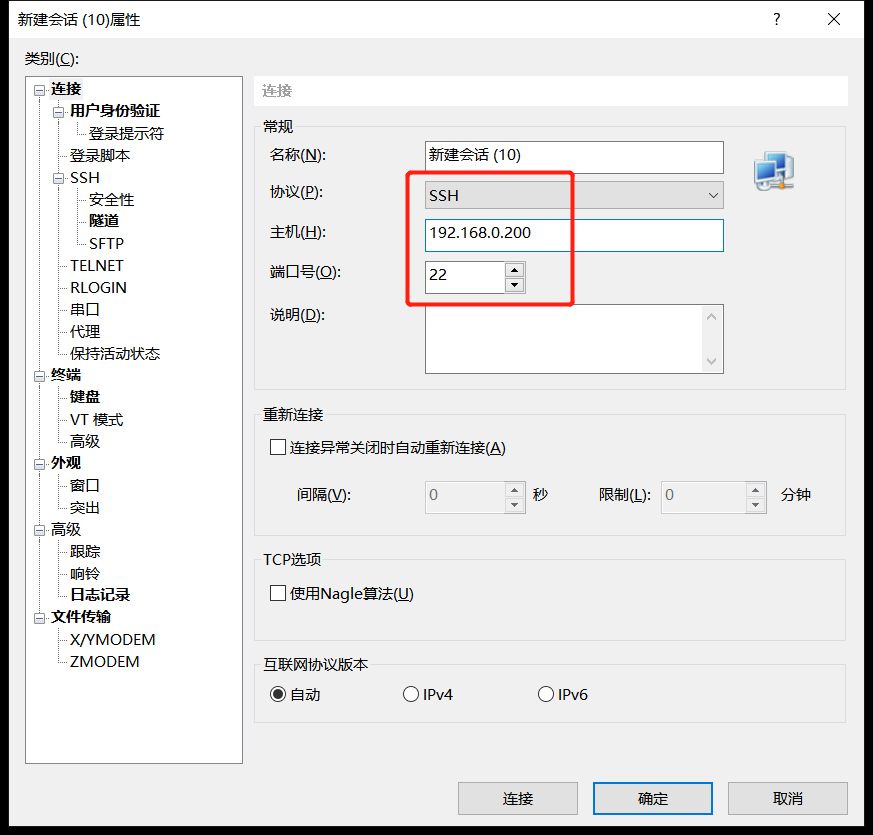
SecureCRT：



MobaXterm：



Xshell:

****

2.1.3.UI（deepeyes软件）

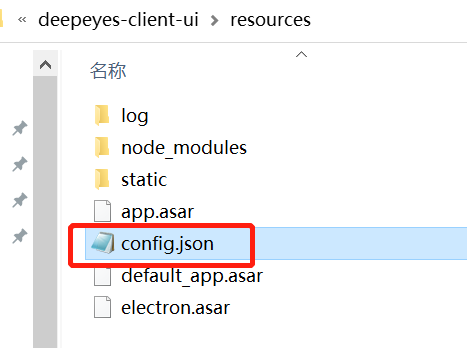
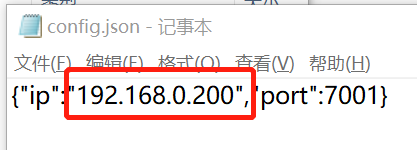
通过UI(deepeyes)登录装置进行管理，电脑需连接对应管理网口并配置对应网段IP，电脑能够ping通管理IP。

管理网口及IP：15口（10.10.10.10）、16口（192.168.0.200）

账号：admin（安全员）、operator（操作员）、auditor（审计员）

新设备默认密码均为123456，第一次登录会提示修改密码。

注：软件默认管理口及IP为16口（192.168.0.200），若需更换15口登录进行管理，需找到UI安装目录下的resources文件夹下的config.json

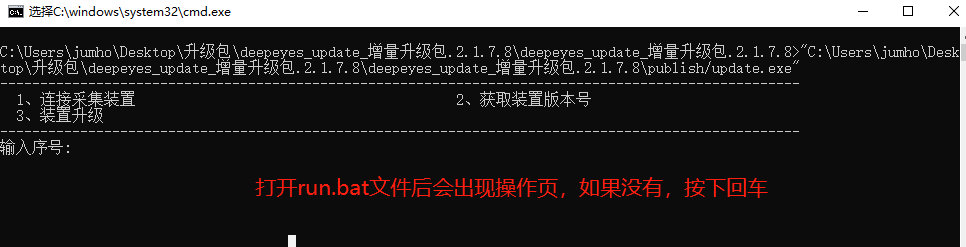
打开后将里面的IP改为10.10.10.10，保存后即可用15口登陆装置。

1. 装置升级

升级前需确保调试电脑与态势感知通信正常，即能ping通管理IP

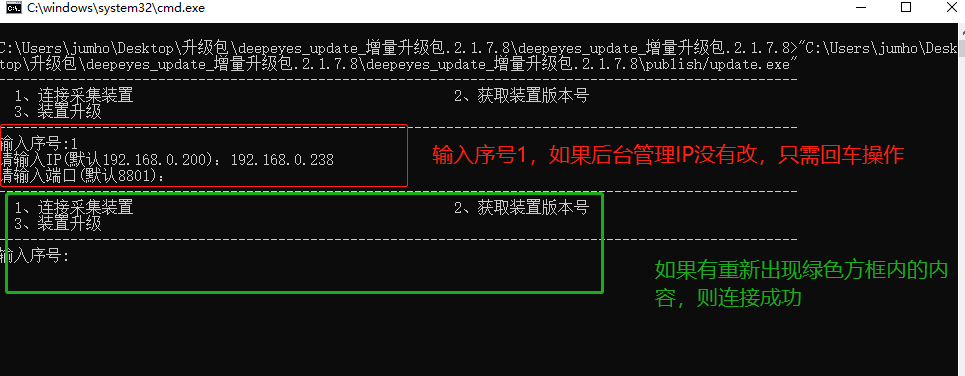
注：2.1.1.1版本及以上可以直接用全量升级包升级到最新版本，2.1.1.1版本以下联系厂家升级。

1.解压升级包，运行升级包里的run.bat文件



2.升级程序连接装置

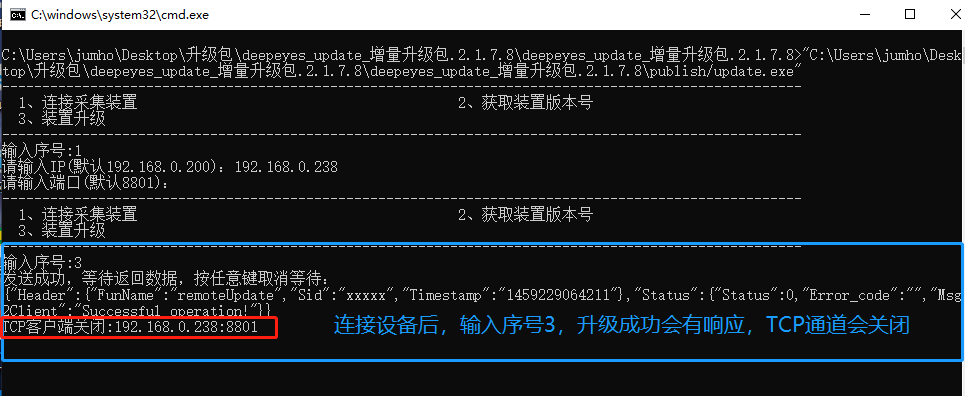
如果后台管理IP与默认IP不同，则输入相应的IP；若相同，则直接回车操作。



3.执行升级过程

输入序号3，执行升级过程，若出现TCP客户端关闭，则升级已完成。

注：不要输入2选项，会断开与装置的连接，需要输入1重新连接才能升级。



4.升级结果检验

登录软件，在 运行概况->版本信息查看



后台查看版本，命令：/data/deepeyes/publish/deepeyes version



1. 装置配置

4.1装置网络配置

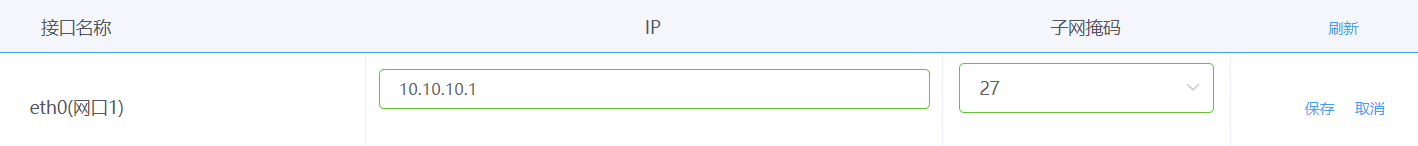
4.1.1.网卡配置

进入系统管理->网络设置->网卡参数



注：态势感知网口1对应客户端的eth0，网口2对应客户端的eth1，以此类推。

点击“编辑”，填好IP和掩码（注意IP必须以点分十进制的格式填写，掩码以网络标识位的长度填写。）然后保存。



不同网段接入态势感知需要给态势感知分配对应网段的IP，需要根据接线在对应网口配置IP和掩码。

以控制区为例，一般需要接入的业务网段有一区网段、站控层ABC网网段、其他一区业务网段，都需要给态势感知分配这些业务网段的IP。

注：任意两个网口不能分配到同一个网段

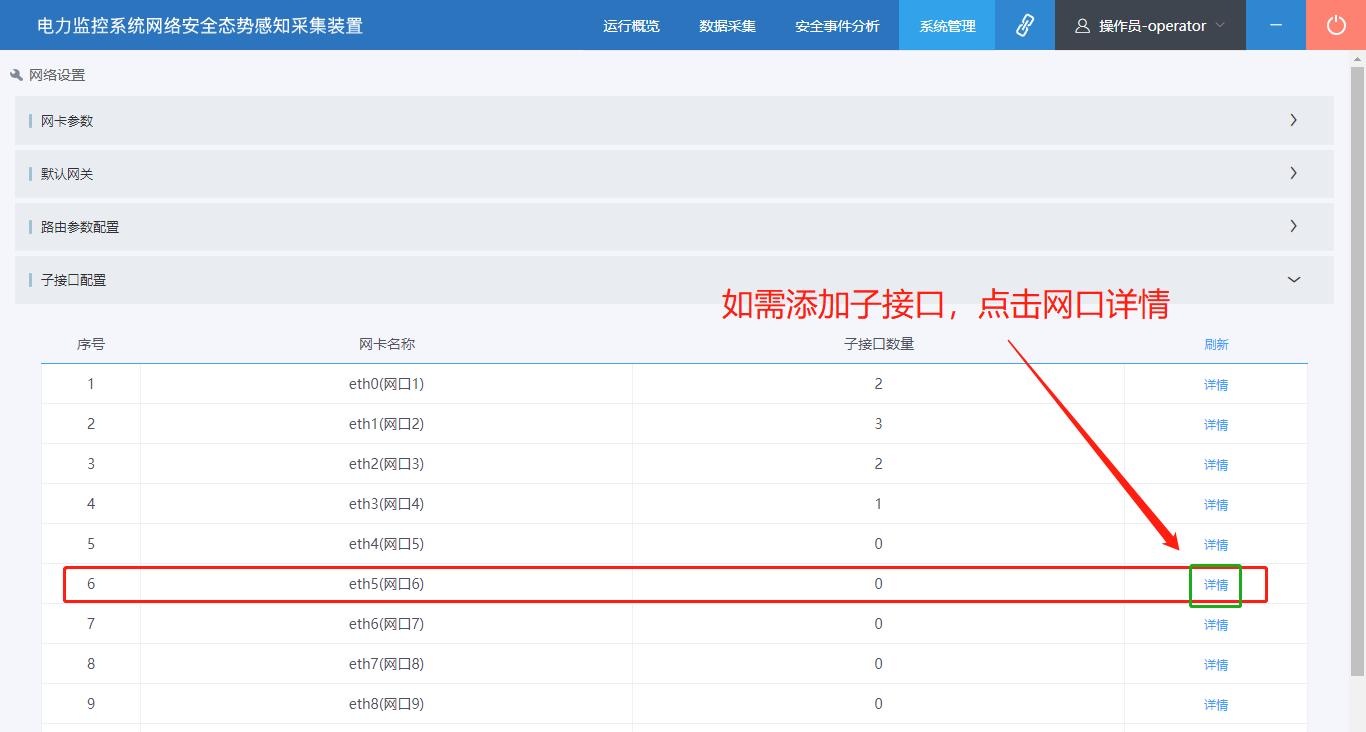
4.1.2.子接口配置

若需要一个接口配置多个IP，则需要用子接口。例如分配了两个不同vlan的态势感知一区IP。

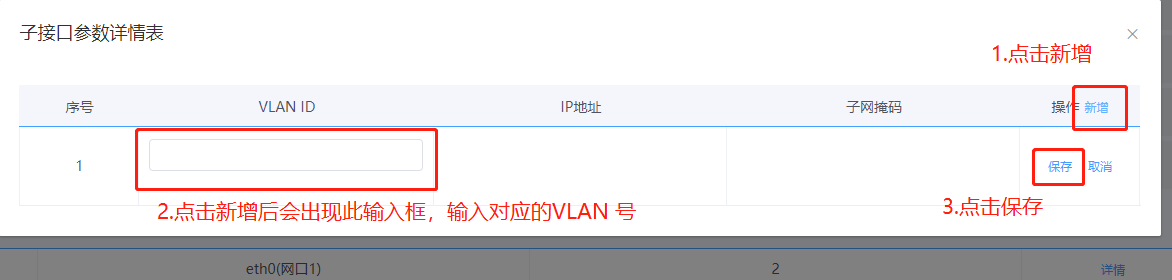
配置如下：

进入系统管理->网络设置->子接口配置

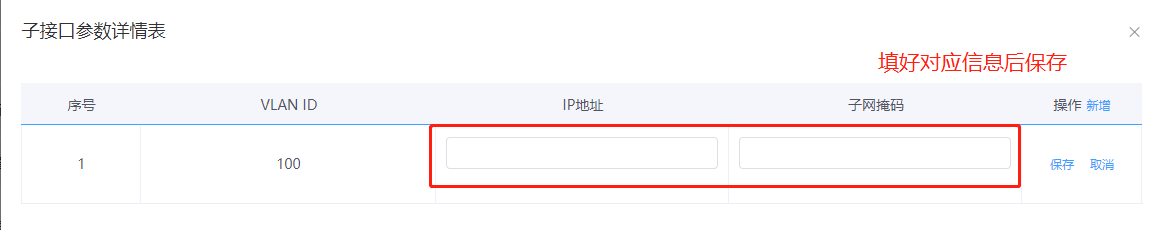
在对应需要添加子接口的网口点击详情：



添加子接口vlan号并保存：



保存后点击编辑，然后填入对应IP地址与掩码，保存：



4.1.3.默认网关配置

默认网关的作用是在没有路由时，装置会默认把流量交给该网关处理。

进入系统管理->网络设置->默认网关

输入网关ip、点击保存；网关地址为态势感知所在VLAN的网关

注：态势感知接口IP地址需要配置后才可配置默认网关



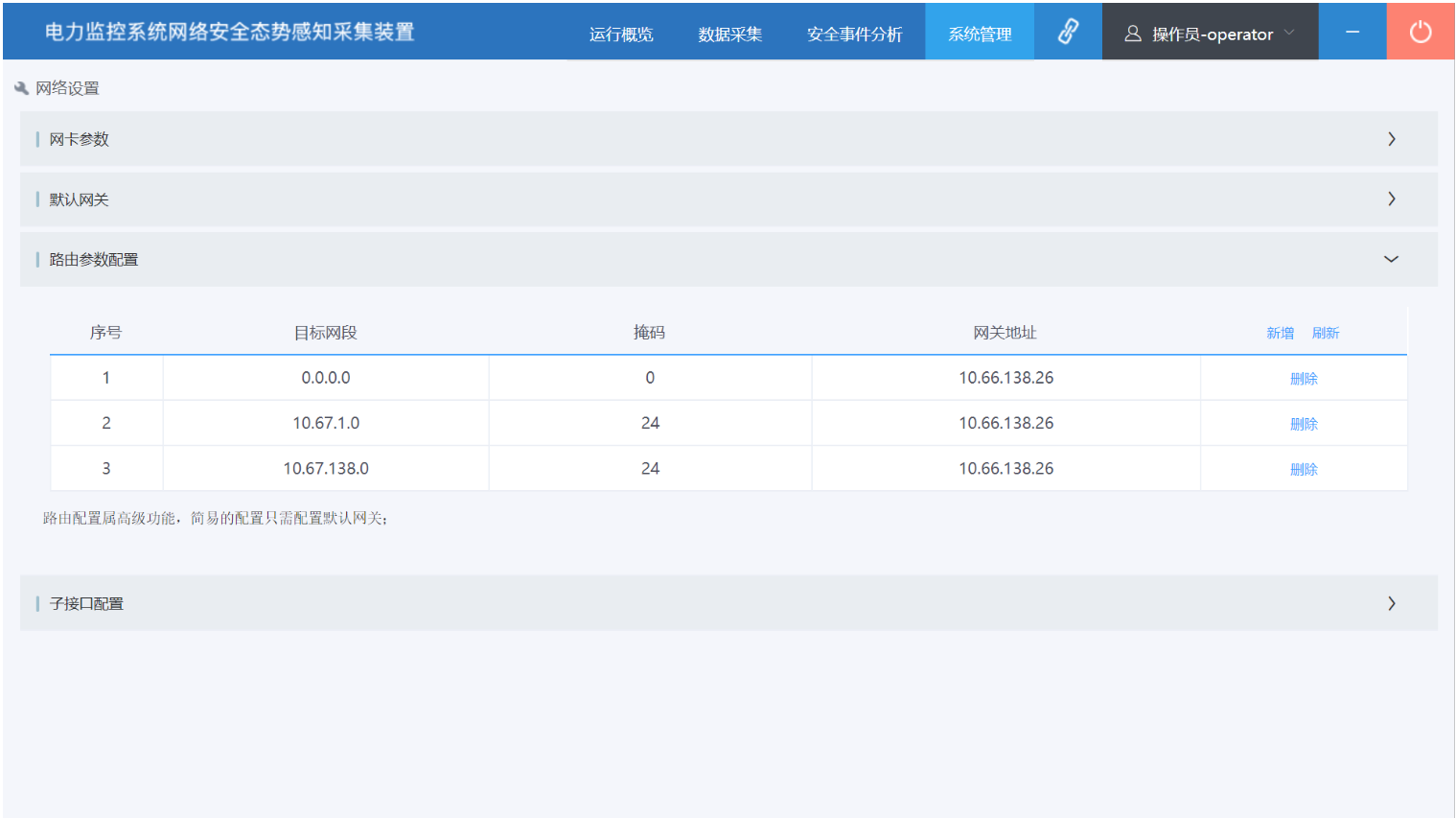
4.1.4.路由参数配置

一般情况下不需要配置路由参数

进入系统管理->网络设置->路由参数配置

点击“编辑”，填好目标网段、掩码、网关地址（下一跳）然后保存；

注：网关地址（下一跳）态势感知必须能ping通。



4.2装置采集配置

4.2.1.采集网段配置

网段分为二层网段与三层网段

二层网段指态势感知网卡所配置IP所属网段，与态势感知直连的网段，一般为一区网段等。

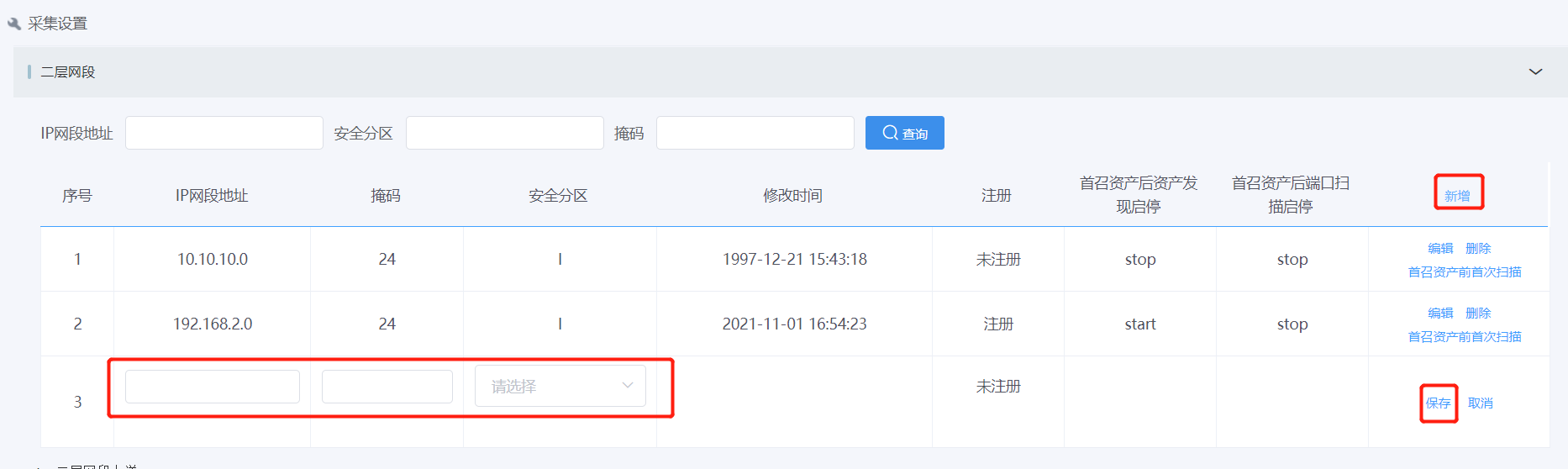
三层网段指需要经过路由转发才能到达的网段，与态势感知非直连的网段，一般为二区网段等。

1. 二层网段配置如下：

进入系统管理->采集设置->二层网段

点击“新增”，填写IP网段、掩码、安全分区等内容，点击“保存”。

若主站未收到二层网段，可以重复点击编辑保存，触发网段上送。



1. 三层网段

进入系统管理->采集设置->三层网段

三层网段由主站下发，无需手动配置。提供网段/掩码、网段别名、Vlan号、安全分区等信息给主站，下发后如下所示



4.2.2.镜像口配置

进入 系统配置->采集配置->镜像口采集

点击“新增”，选择对应的端口，点击“保存”



4.2.3.SNMP团体名配置

新版本软件取消了全局配置snmp团体名功能，需要在资产注册后，对该资产进行配置。

进入数据采集->资产实时运行状态->所有设备

在资产列表找到需配置资产，或者搜索框搜索，点击“详细”进入资产详细页面。

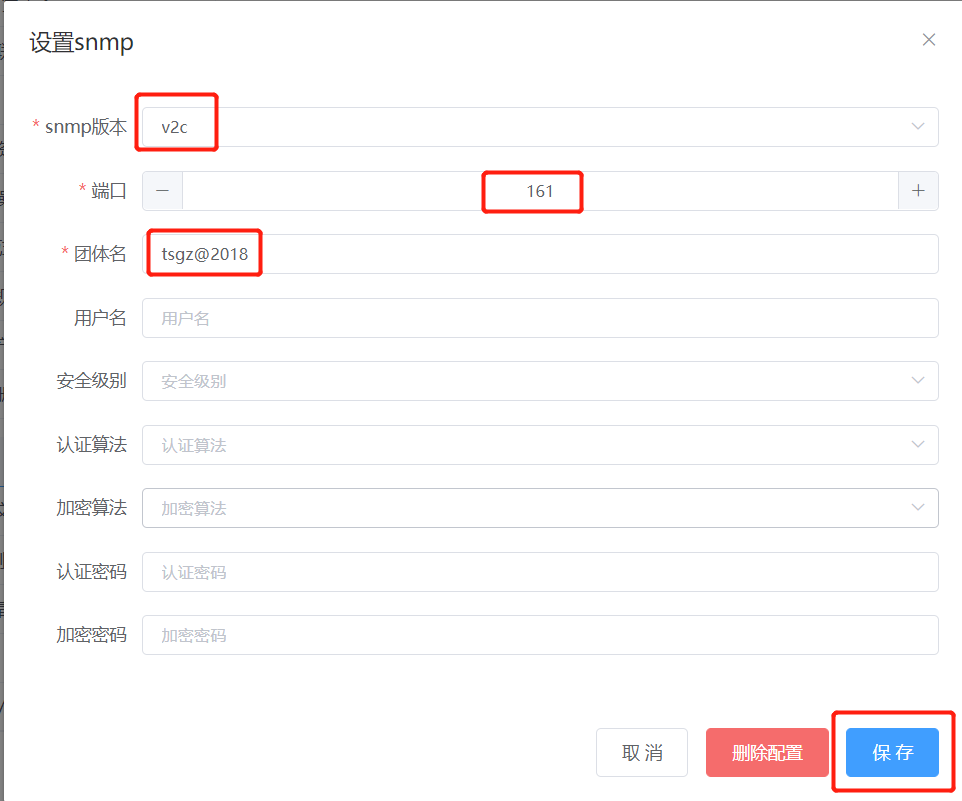


在资产信息界面往下拉，点击“SNMP配置”



注意：资产必须注册后才会显示配置按钮

填写snmp版本、端口、团体名后，点击“保存”



4.2.4.审计员账号配置

通用主机设置好审计员账号后，需要在装置上进行相应的配置，以使装置可以采集通用主机的文件MD5值，达到监测关键性文件变更的目的。

进入数据采集->资产实时运行状态->所有设备

在资产列表找到需配置资产，或者搜索框搜索，点击“详细”进入资产详细页面。



在资产信息界面往下拉，点击“SSH配置”



注意：资产必须注册后才会显示配置按钮

填写端口、登录方式、审计员用户名、登录密码，点击“保存”

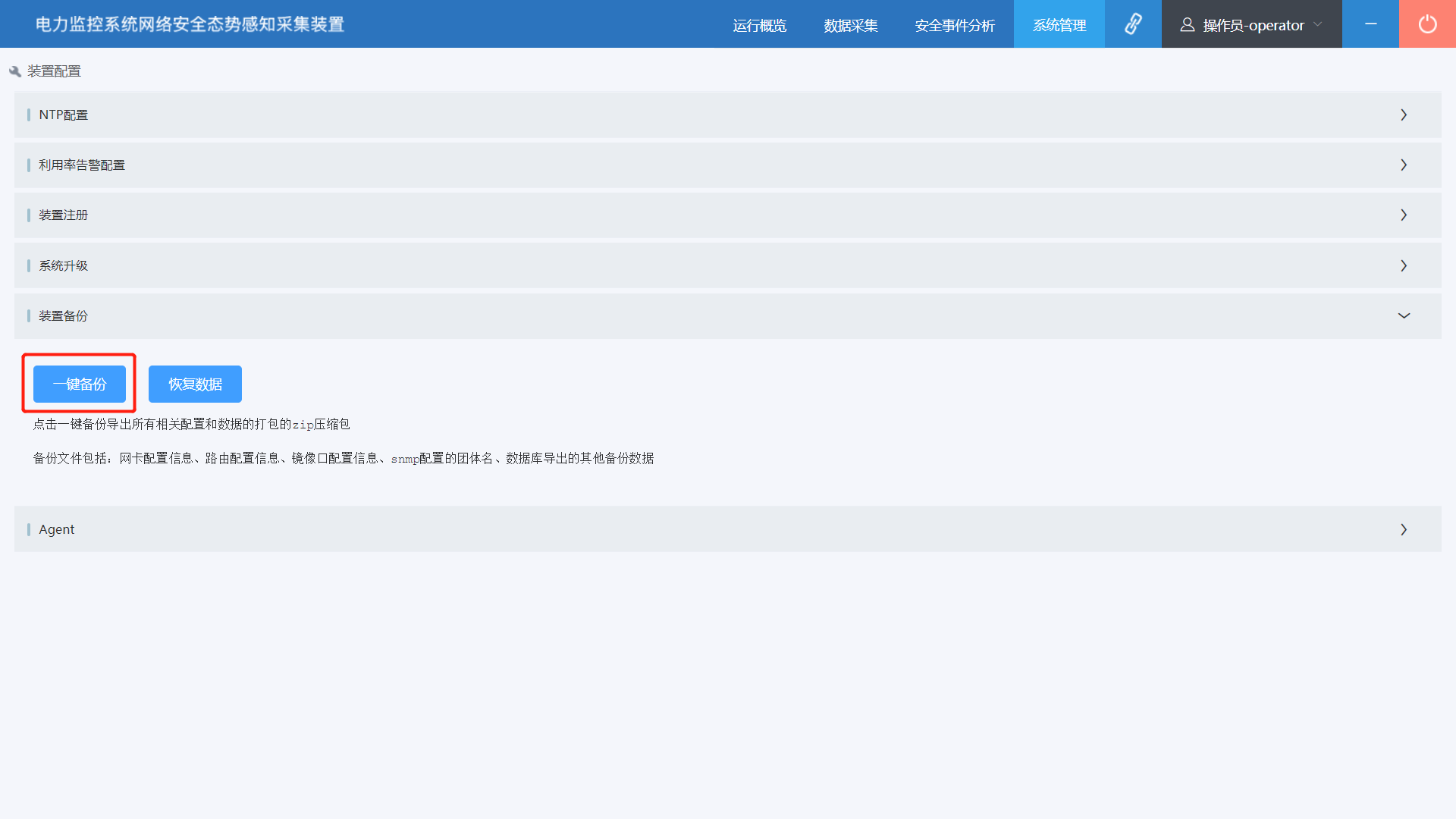


4.3装置备份

进入系统管理->装置配置->装置备份

点击“一键备份”，将装置备份保存到电脑中

备份文件包括：网卡配置信息、路由配置信息、镜像口配置信息、snmp配置的团体名、数据库导出的其他备份数据



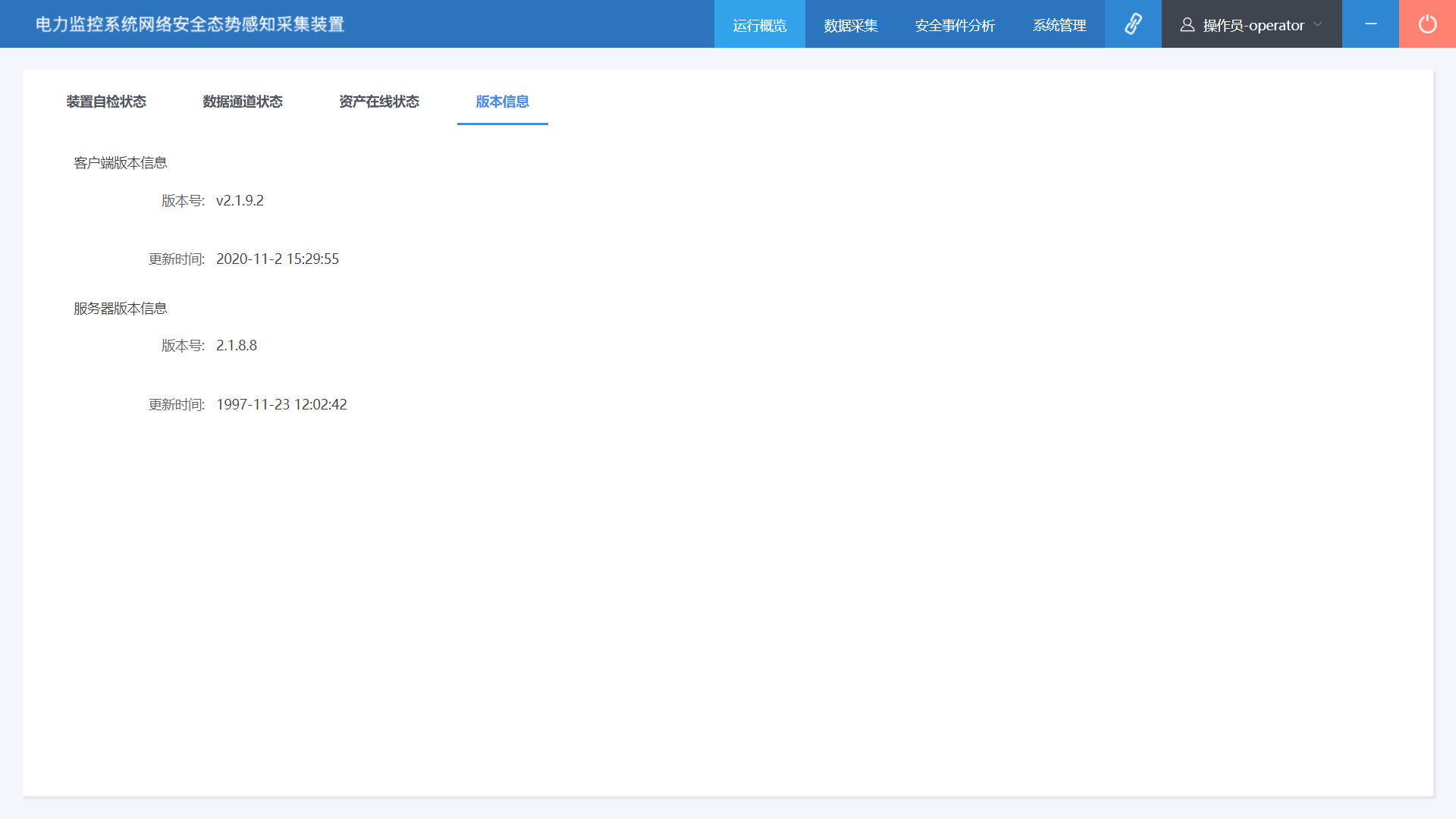
1. 软件常用功能

5.1装置状态及信息

5.1.1.装置版本

进入运行概览->版本信息

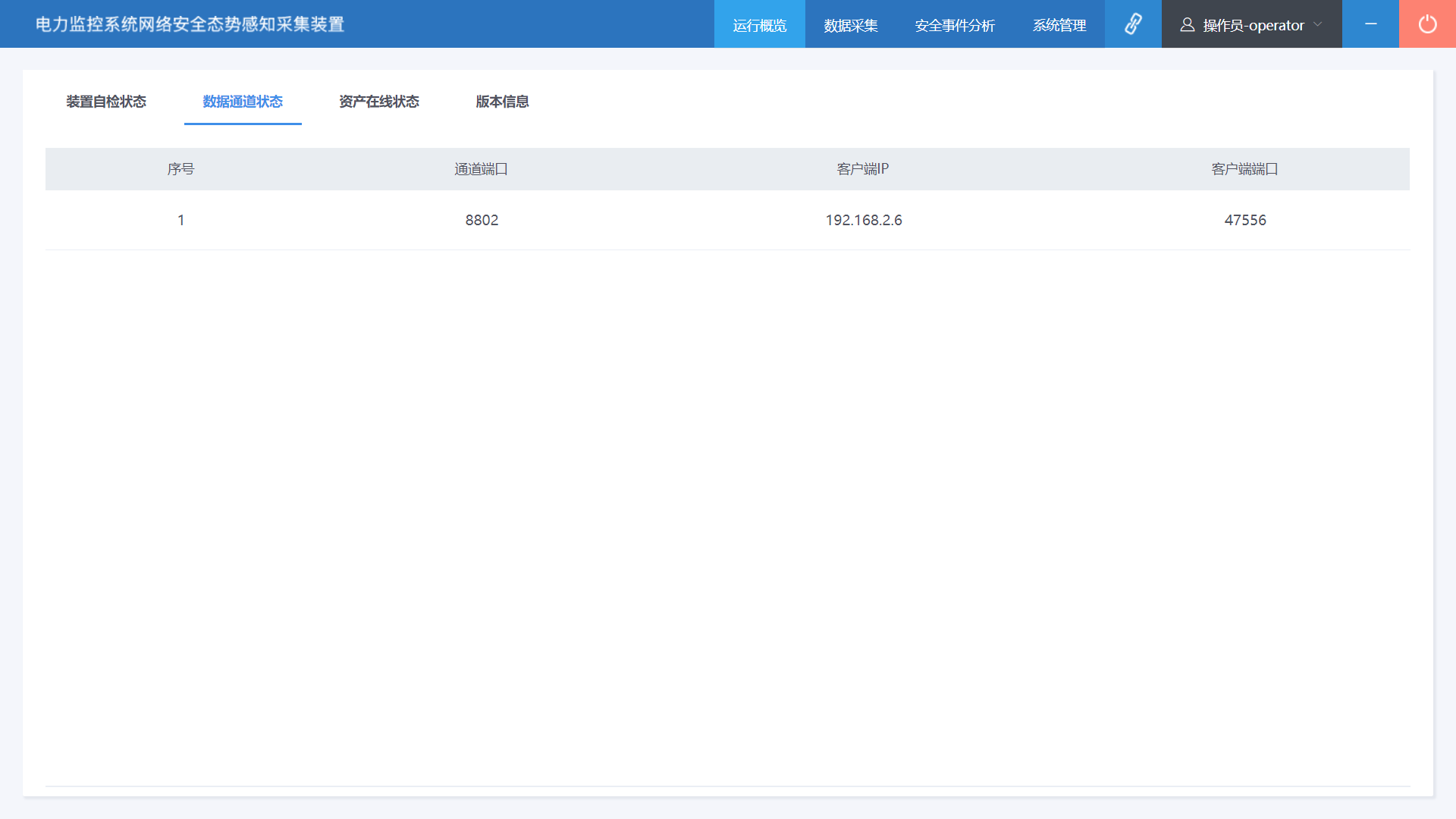
可查看当前软件版本及装置程序版本



5.1.2.数据通道

进入运行概览->数据通道状态

可查看当前8802数据通道是否连接正常



5.1.3.装置注册信息

进入系统管理->装置配置->装置注册

可查看已注册装置的基本信息

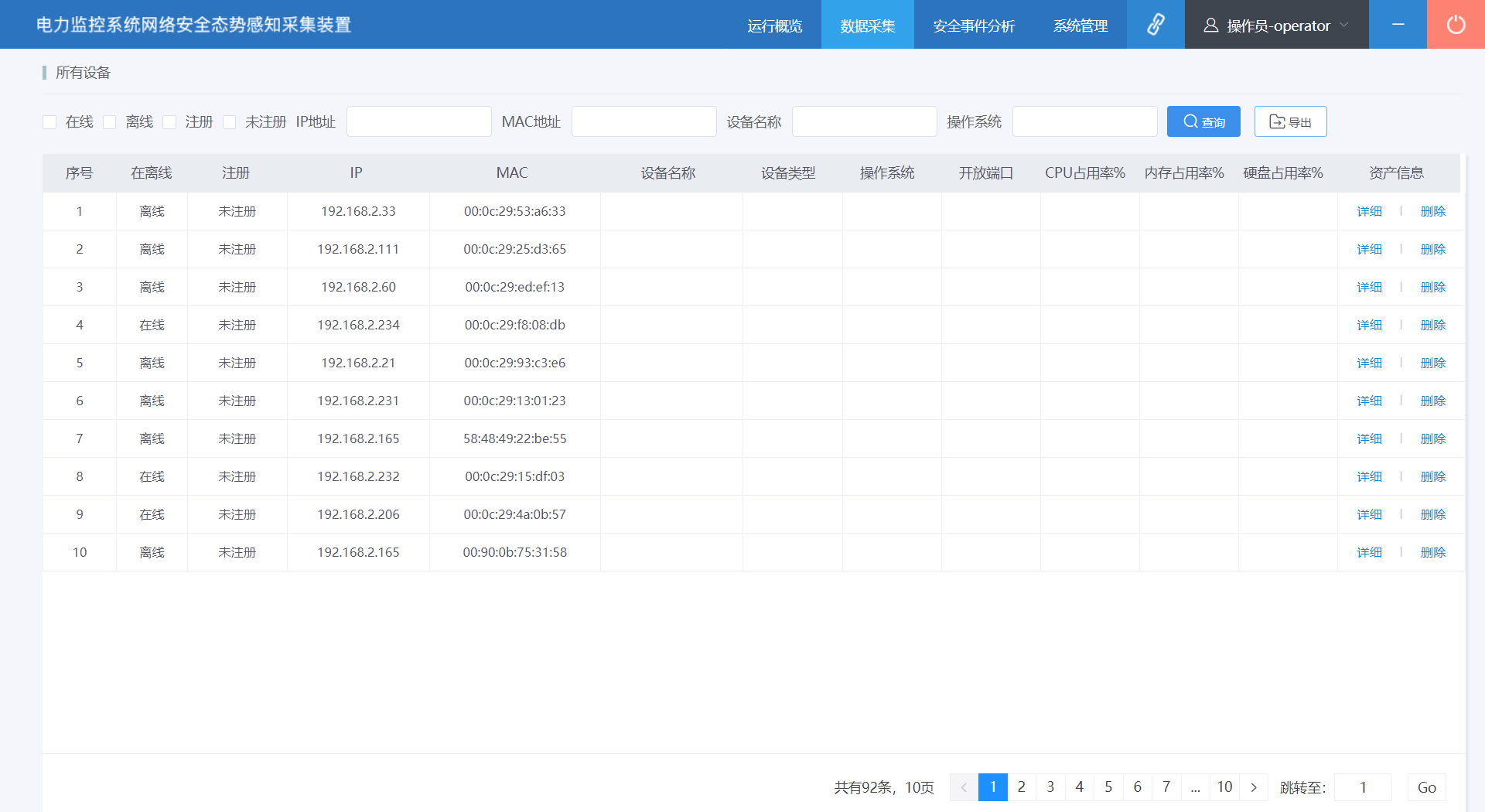


5.2采集内容

5.2.1.资产列表

进入数据采集->资产运行状态->所有设备

可查看当前已扫描到的资产列表，可以查看资产是否注册，以及注册的基本信息。



5.2.2.资产信息

进入数据采集->资产运行状态->所有设备

查找到要查询的资产，点击详情还可查看资产的详细信息、实用化配置状态；还可对已注册资产进行snmp配置、ssh配置；还可查看通用主机的关键性文件变更相关内容。

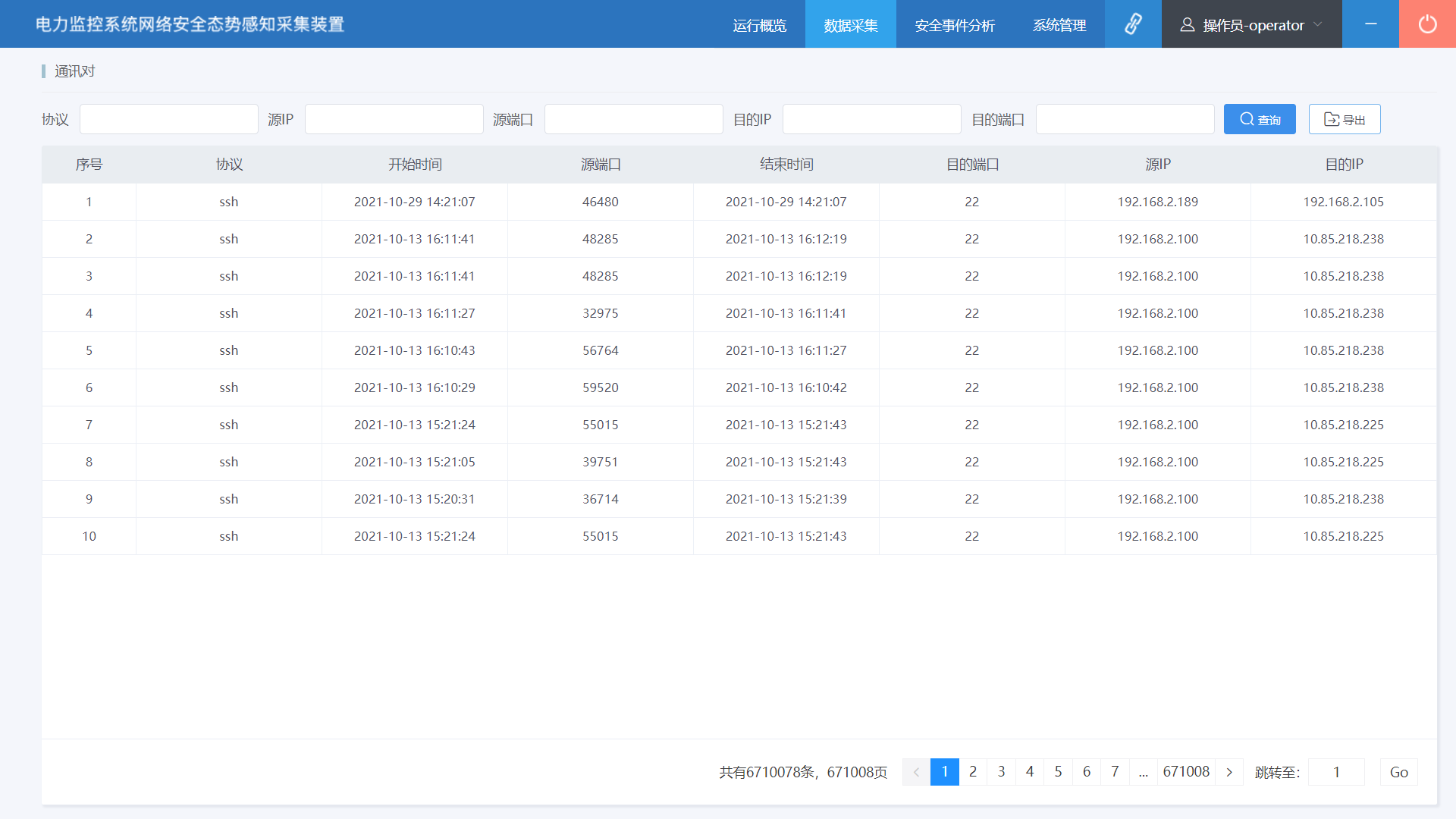




5.2.3.通讯对（镜像流量）

进入数据采集->流量查询->通讯对

可以查看装置采集到的通讯对流量。

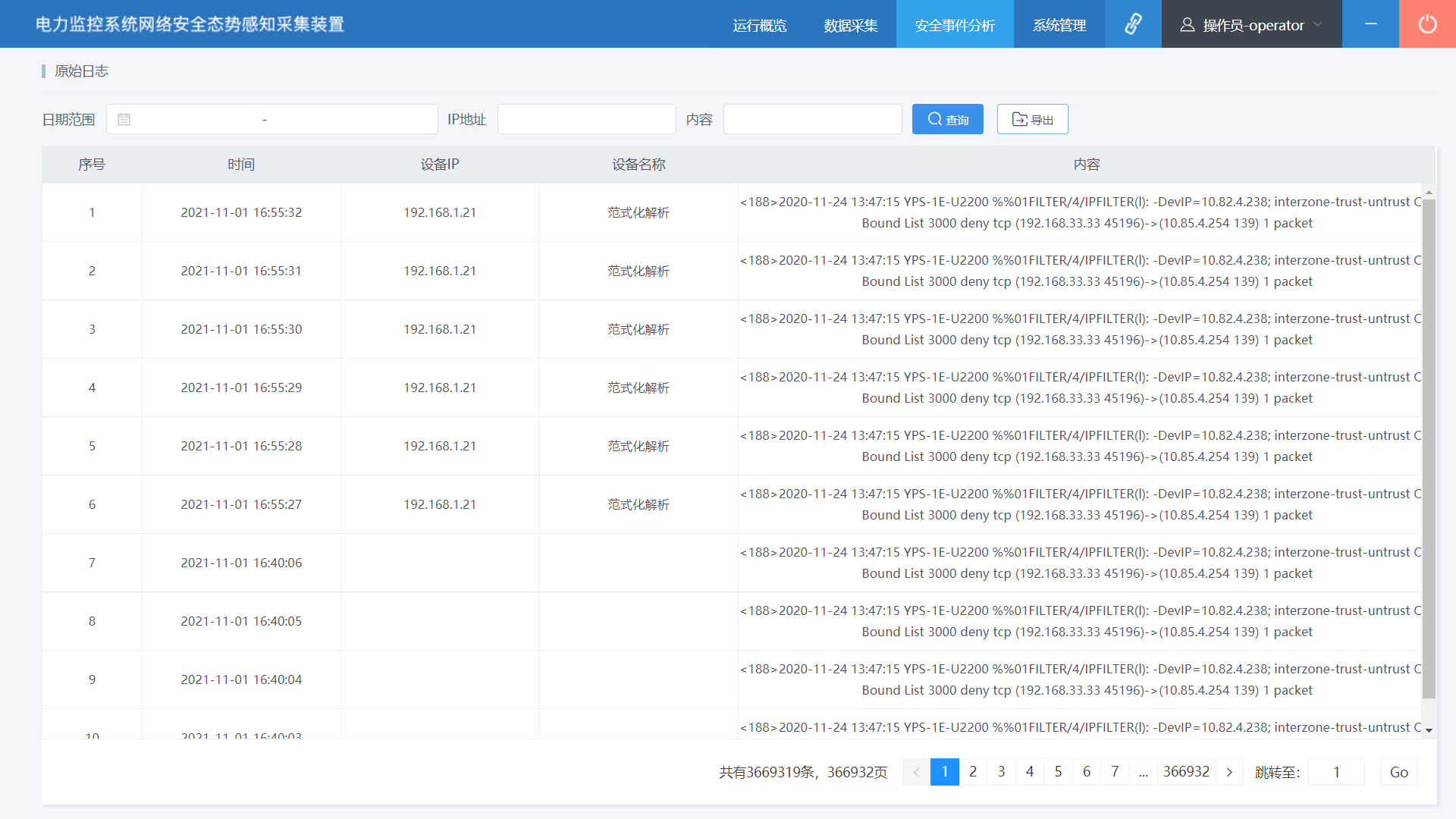


5.3装置日志

5.3.1.资产原始日志

进入安全事件分析->原始日志

可以查看装置采集到的资产原始日志，若已匹配出范式化日志，则不会出现在原始日志。



5.3.2.范式化日志

进入安全事件分析->范式化日志

可以查看匹配后的范式化日志及报文

常见的日志类型有：Login\_success(登录成功)、Login\_failed(登录失败)、Login\_exited(登录退出)、Ethport\_up(网口接入)、Ethport\_down(网口拔出)、Policy\_access\_no\_safety(不符合安全策略访问)、Usb\_insert(USB设备接入)、Usb\_pullout(USB设备拔出)



5.3.3.主站请求日志

进入安全事件分析->主站请求日志

可以查看主站操作日志，包括注册、下发等操作



1. 常见问题排查

6.1账号及登录问题

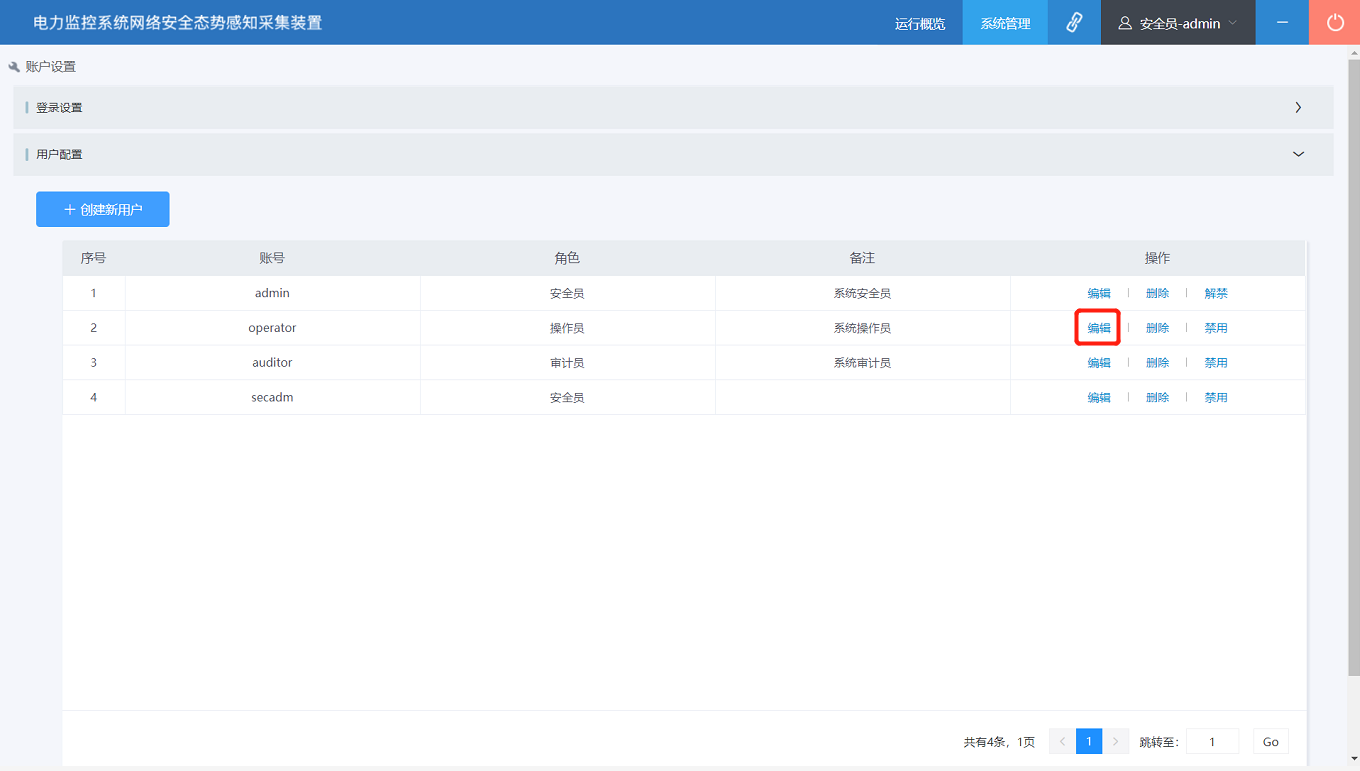
6.1.1.账号密码错误

登录操作员账户operator的时候提示密码错误，可以登录安全员账户admin进行修改。

安全员账户admin默认密码是123456，第一次登录会提示修改密码。

登录安全员账户admin后，进入系统管理->账户设置->角色配置

选择操作员账号，点击“编辑”



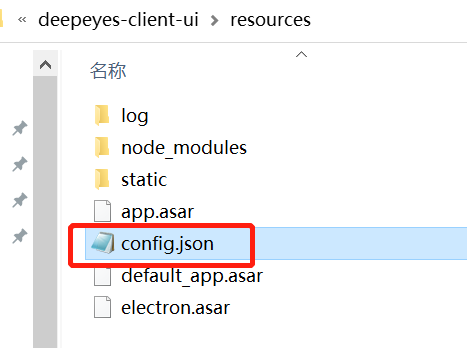
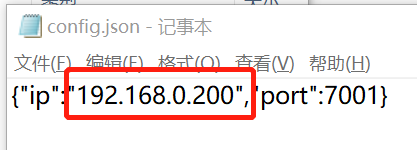
输入新密码进行修改。



6.1.2.登录异常

检查调试电脑与装置的物理连接及网络连接是否正常，确保调试电脑可以ping通装置管理IP。

检查软件安装目录下的resources文件夹下的config.json

ip是否为对应管理口IP，若不是则修改。

管理网口15对应IP为 10.10.10.10，管理网口16对应IP为192.168.0.200。

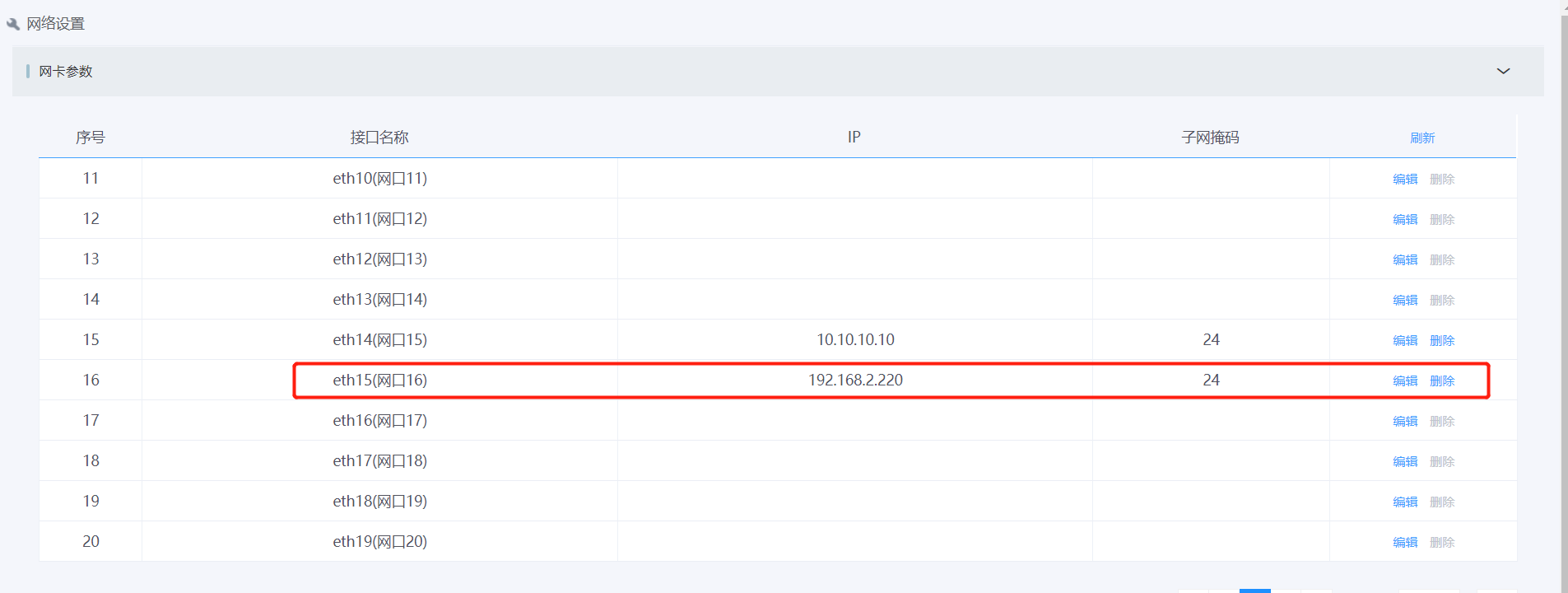
6.2网络问题

6.2.1.配置IP与管理IP冲突

现象：网卡配置时提示与某网卡IP冲突



处理方法：在网卡配置界面，找到对应管理IP，修改管理IP即可

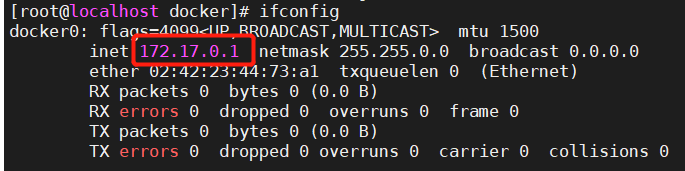


6.2.2.配置IP与dockerIP冲突

现象：配置网卡IP时提示与docker0冲突

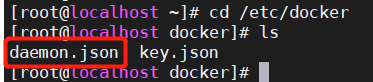


处理方法：登录装置后台，查看docker0的IP：ifconfig



编辑/etc/docker下的daemon.json文件（若没有则新建）

vim /etc/docker/daemon.json

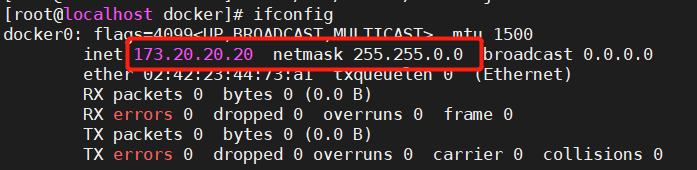


按“I”，添加{"bip":"IP/掩码"},IP为与docker0不冲突的IP，:wq保存修改



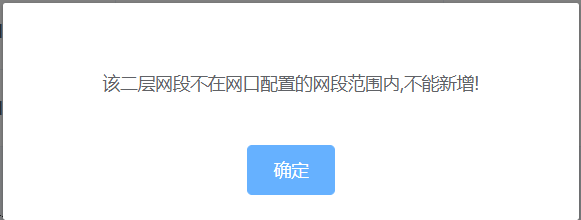
重启docker服务： systemctl resatrt docker

查看docker0 IP是否更改：ifconfig



6.2.3.二层网段无法配置

现象：配置二层网段时出现以下提示



解决方法：排查网卡配置，是否有对应网段的IP配置。

6.2.4.主站收不到二层网段

现象：配置好二层网段后，主站收不到

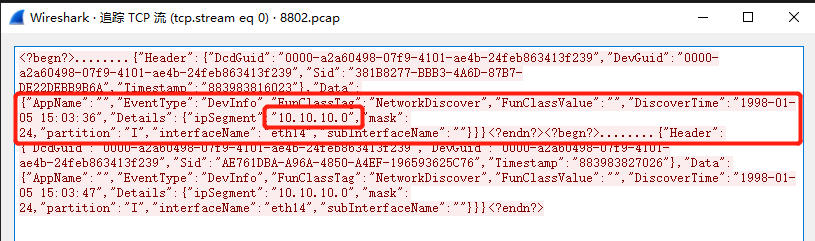
排查方法：先确保链路正常，8802通道保持连接

在“二层网段”配置处，重复点击“编辑”、“保存”触发网段上送





在后台抓取8802通道的数据包判断是否有网段上送



若有上送，则让主站抓包排查，是否有数据积压等原因。

6.2.5.态势感知ping不通网关

现象：态势感知无法ping通交换机网关

排查方法：

1. 检查物理连接及网卡配置是否有误
2. 查看交换机网卡模式是否跟态势感知一样（access、trunk）
3. 排查是否存在IP冲突

6.3功能问题

6.3.1.没有通讯对

现象：主站没有通讯对更新

排查方法：

1. 进入数据采集->流量查询->通讯对，查看是否有通讯对更新

若有，则排查网络链路问题，抓8802通道的报文排查是否有上送主站

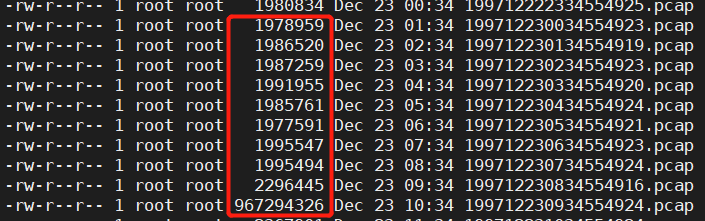
若没有，则进行下一步排查

1. 在装置后台查看是否有流量更新

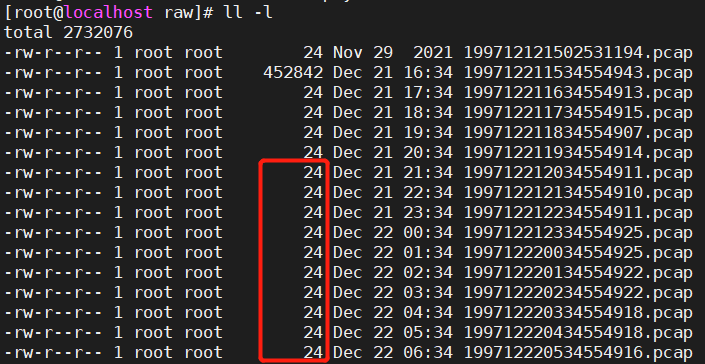
在/data /deepeyes/file/raw下，多次执行ll -l



若出现大量数字增加，则说明镜像流量采集正常，排查链路上送问题



若出现24或0，则说明镜像流量采集不正常



进行下一步操作

1. 重启后台程序：systemctl restart asset
2. 检查装置及交换机镜像口配置或重新配置
3. 检查物理连接是否正常
4. 后台流量有正常增加更新，则等待软件界面通讯对更新即可上送

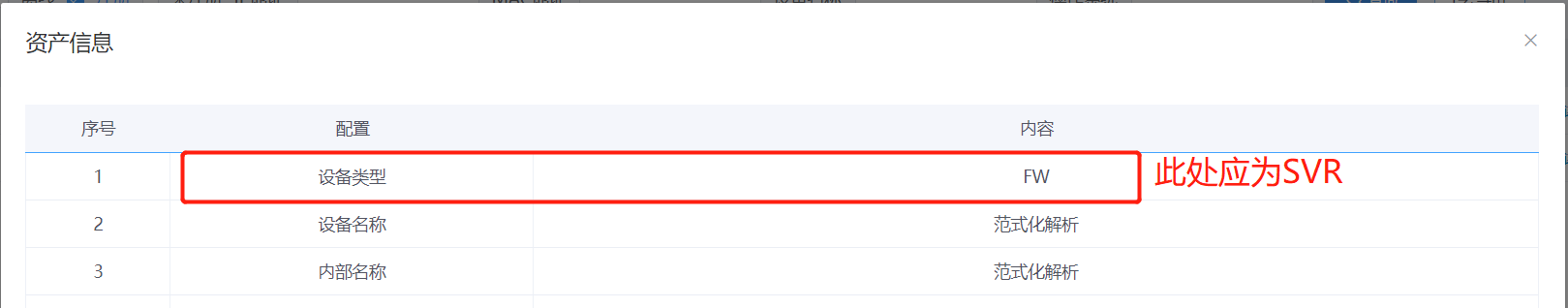
6.3.2.审计员未配置状态

排查方法：

1. 检查资产详细页“ssh配置”是否配置正确，确保配置的“审计员账户”可以远程登录主机



1. 查看资产注册类型，需要为“SVR”即服务器

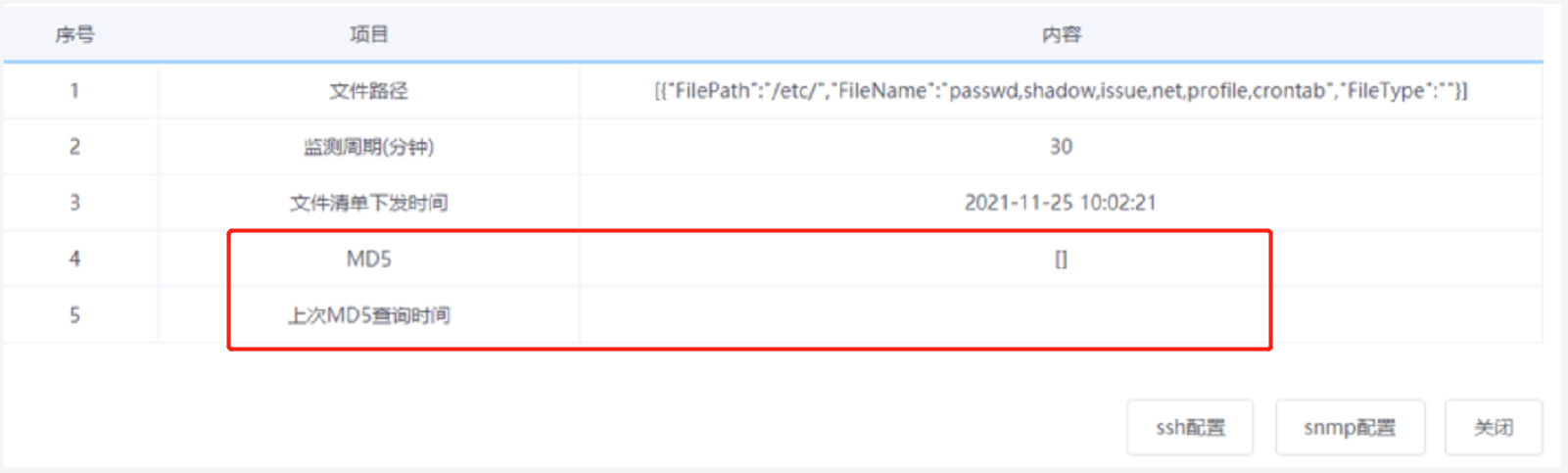


6.3.3.关键性文件MD5值查询问题

现象：审计员账号显示已配置，主站也已下发关键性文件路径，但查询不到文件MD5 值

排查方法：

1. 若“MD5”及“上次MD5查询时间”均为空，则让主站重新下发关键性文件路径；



1. 若仅有“MD5”为空，则看“上次MD5查询时间”是否为当前时间相近的时间，若不是，则后台重启程序：systemctl restart asset；

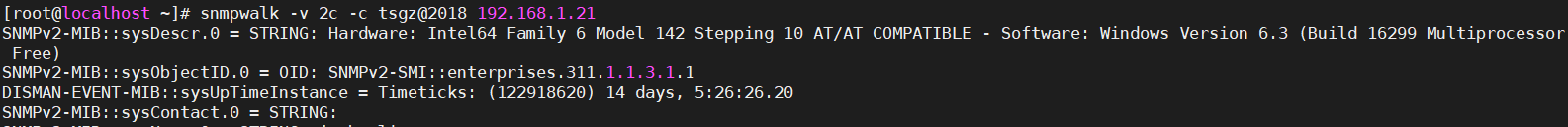
若是，则检查下发的路径是否有误，主机是否存在相应的文件，审计员账号是否能够采集到该文件的MD5值，重新下发资产的关键性文件路径。

6.3.4.snmp未配置状态

排查方法：

1. 在装置后台用命令查看是否能采集到snmp信息

命令：snmpwalk -v 2c -c 团体名 资产IP



若有回显信息，说明装置可以正常采集snmp信息。

若没有回显或超时，则检查资产snmp相关的配置：

包括资产snmp配置、链路及防火墙策略等配置，是否在链路中被某一环节拦截。

例如：二区的资产需要检查横向防火墙有没有放通udp161端口，

主机类设备需要检查自身操作系统防火墙是否禁用相关服务及端口。

1. 查看资产详细页面“snmp配置”是否配置正确，并排查资产snmp相关配置

