奇固科威
HKW-LAS1000 日志审计与分析系统
用户手册
V1.0.10

杭州奇固科威信息安全技术有限公司

2025 年 3 月 29 日

目 录

1 安装与部署.....5
2 授权.....6
管理员.....6
3 系统配置.....6
3.1 网络配置.....6
3.1.1 IP 配置.....6
3.1.2 路由配置.....6
3.2 升级管理.....7
3.3 系统配置.....7
3.3.1 基本信息.....7
3.3.2 基础配置.....8
3.3.3 邮件服务.....8
3.3.4 校时配置.....9
3.3.5 数据库维护.....9
3.3.6 数据库备份.....10
3.3.7 系统快照.....10
3.3.8 License 管理.....10
3.3.9 情报库.....11
3.3.10 系统告警通知.....11
3.4 白名单.....12
4 系统管理.....12
4.1 用户管理.....12
4.2 角色管理.....13
4.3 转发策略.....15
操作员.....16
5 日志管理.....16
5.1 日志源类别.....16
6 审计管理.....17
6.1 审计事件.....16
6.2 审计策略.....16
6.3 审计类型.....20
7 采集管理.....21
7.1 代理服务器.....21

7.2 采集过滤策略.....211
7.3 采集器管理.....22
7.4 日志源设备.....24
8 报表管理.....25
8.1 报表列表.....25
8.2 报表任务.....25
8.3 报表查询.....26
8.4 自定义报表模板.....26
9 资产管理.....26
9.1 资产列表.....28
9.2 资产类型.....29
9.3 资产属性.....300
9.4 区域管理.....30
9.5 网络管理.....31
9.6 资产发现.....31
9.7 厂商.....32
10 事件管理.....32
10.1 安全事件.....32
10.2 聚合策略.....33
10.3 关联策略.....33
10.4 原始日志.....34
10.5 通用日志.....34
10.6 自定义解析.....35
10.7 事件.....35
10.8 事件类型.....36
10.9 事件特征值.....36
11 告警管理.....37
11.1 审计告警.....37
11.2 告警策略.....37
11.3 系统告警.....38

11.4 系统告警级别配置.....38
审计员.....38
12 日志管理.....38
12.1 日志备份.....38
13 情报库.....39
13.1 威胁情报库.....39
14 漏洞库.....39
14.1 CNNVD 漏洞信息.....39
15 系统日志.....40
15.1 操作日志.....40
15.2 错误日志.....40
15.1 登录日志.....40

1 安装与部署

1、系统要求

系统名称	系统版本
Ubuntu	18.04 x64 及以上

2、环境要求

服务	版本	备注
MySQL 数据库	5.7.38	默认账号：root 默认密码：Linkqi@123
JAVA	1.8.x	-

3、解压

将压缩包上传到服务器的任意普通用户的 home 目录，例如/home/linkqi 目录下，然后执行下述命令：

a）解压 las-2000xxxxxxxx.tar.gz

```
cd /home/linkqi
tar -zxvf las-2000*.tar.gz
./las_install.sh
```

4、安装

a) 数据库自行安装

b) 进入解压后的目录，执行 install 脚本安装（请使用 root 权限安装）：

```
su root
cd las-2000
./las_install.sh
```

5、运行

安装完成后，执行一下命令运行服务：

```
./las_start.sh
```

6、升级

通过 web 升级，点击上传按钮，选择升级的安装包，上传完成后点击升级即可完成升级。

7、默认用户名密码：

账号	权限	密码
superuser	超级管理员	Linkqi@000
operator	超级操作员	Linkqi@111
auditor	超级审计员	Linkqi@222

2 授权

系统配置->License 管理；复制机器码给平台维护人员；上传维护人员给的认证文件即可

管理员

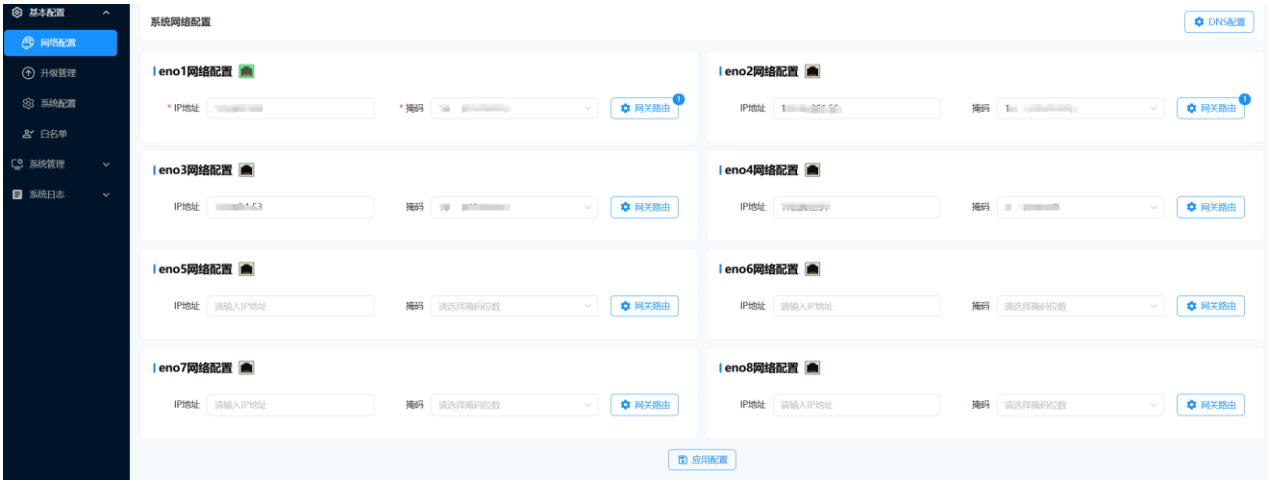
用户名：superuser
密码：Linkqi@000

3 基本配置

3.1 网络配置

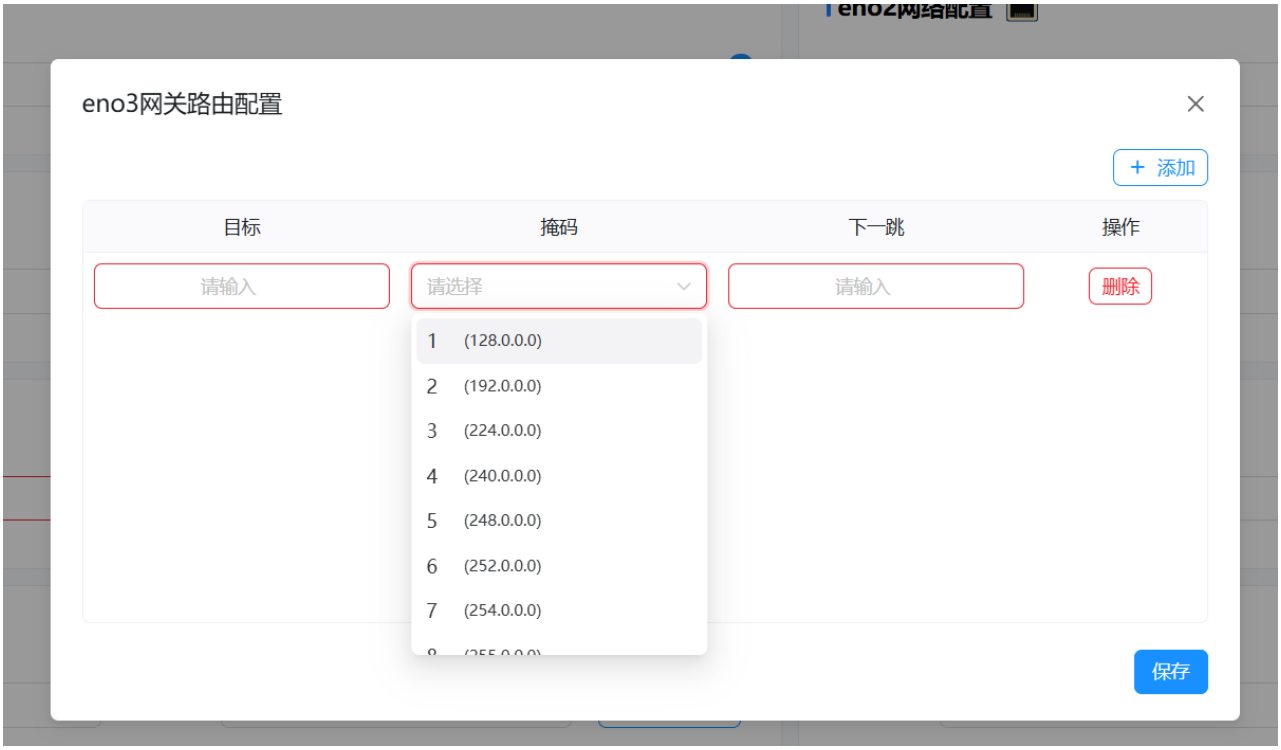
3.1.1 IP 配置

基本配置->网络配置
绿色闪烁网口表示当前网线连接的网口。



3.1.2 路由配置

点击路由配置可进入配置页面，添加完成点击完成



3.2 升级管理

基本配置->升级管理->上传文件->升级
可以升级软件版本

3.3 系统配置

3.3.1 基本信息

产品信息展示可重启或者关机

3.3.2 安全设置

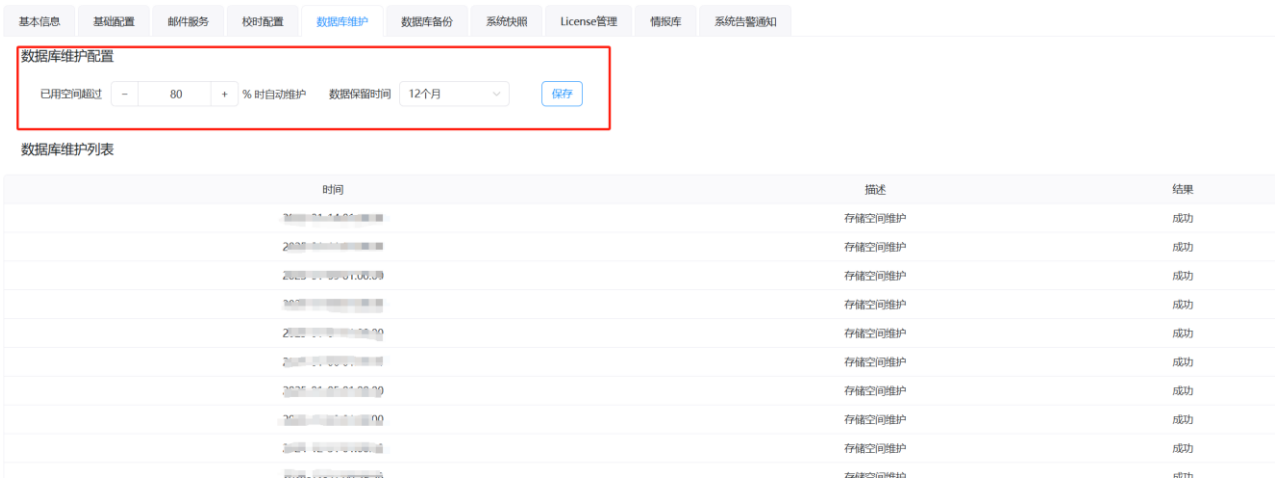
3.3.3 邮件服务

可发送至邮件服务器接受消息

3.3.4 校时配置

3.3.5 数据库维护

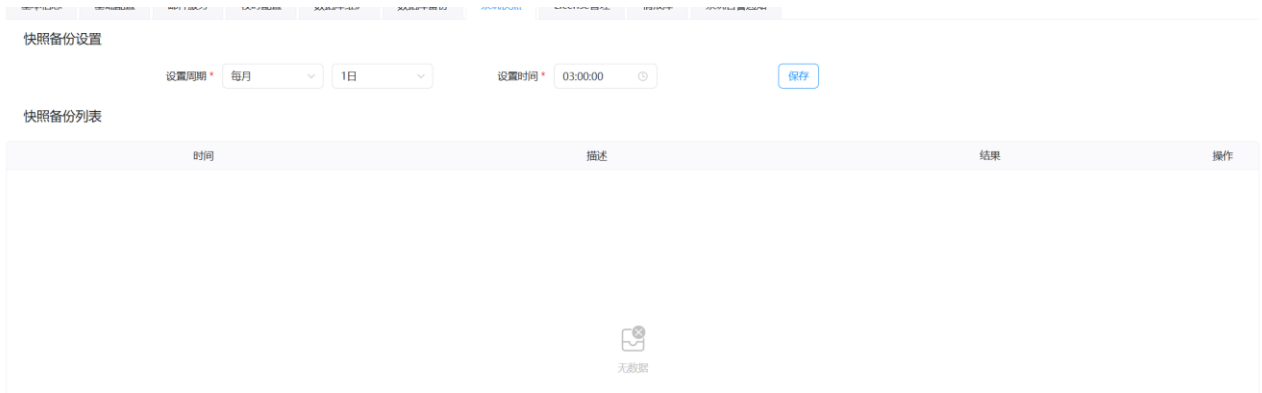
可设置数据库维护时间以及数据保留时间



3.3.6 数据库备份

3.3.7 系统快照

保存系统状态



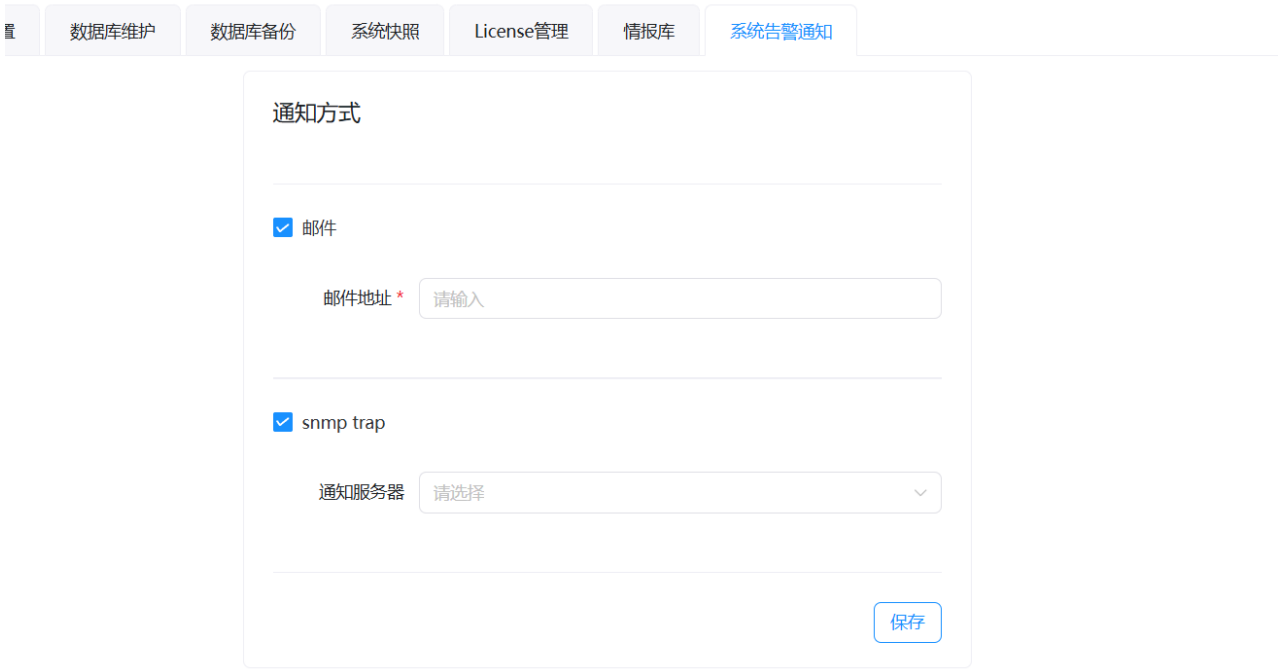
3.3.8 License 管理

授权相关配置

3.3.9 情报库

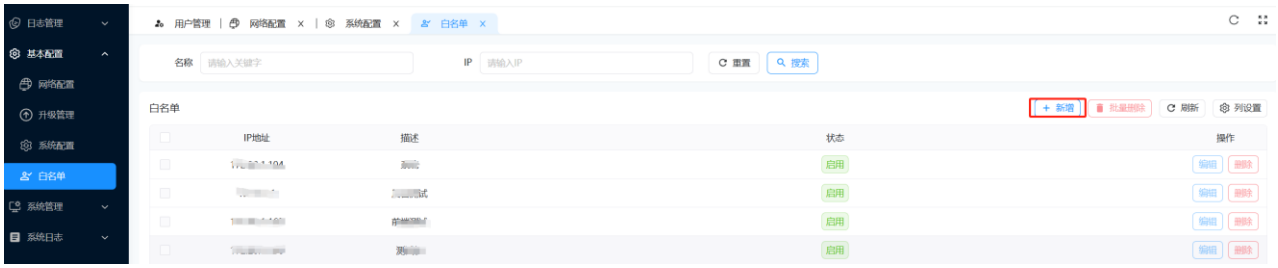
3.3.10 系统告警通知

可自行选择通知方式



3.4 白名单

只有添加了白名单的 ip 可以访问平台
基本配置->白名单->新增
默认是不开启的状态



输入 IP 启用立即生效；

4 系统管理

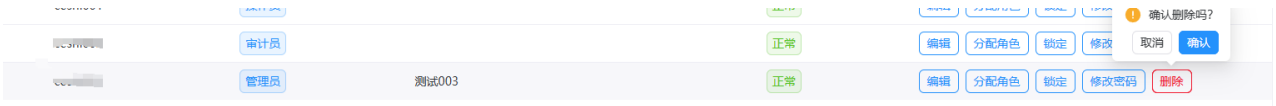
4.1 用户管理

4.1.1 新增

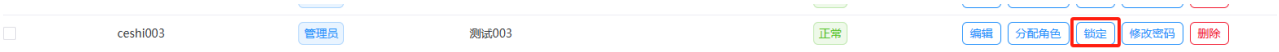
4.1.2 编辑

编辑前需要输入当前账号的密码认证

4.1.3 删除



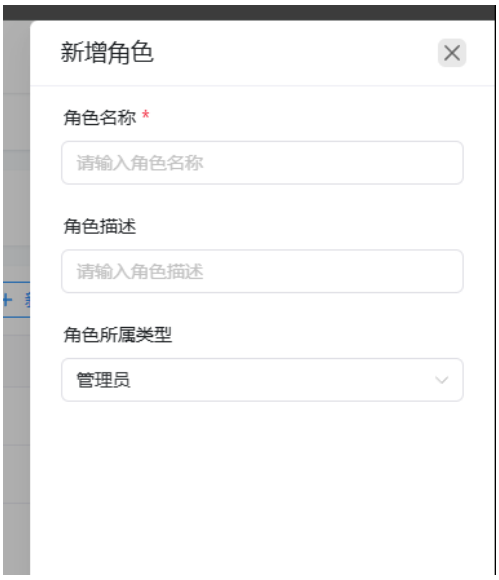
4.1.4 锁定与解锁



4.2 角色管理

按照需要创建角色，可自行分配角色权限，每个用户都有与之对应的角色

4.2.1 新增

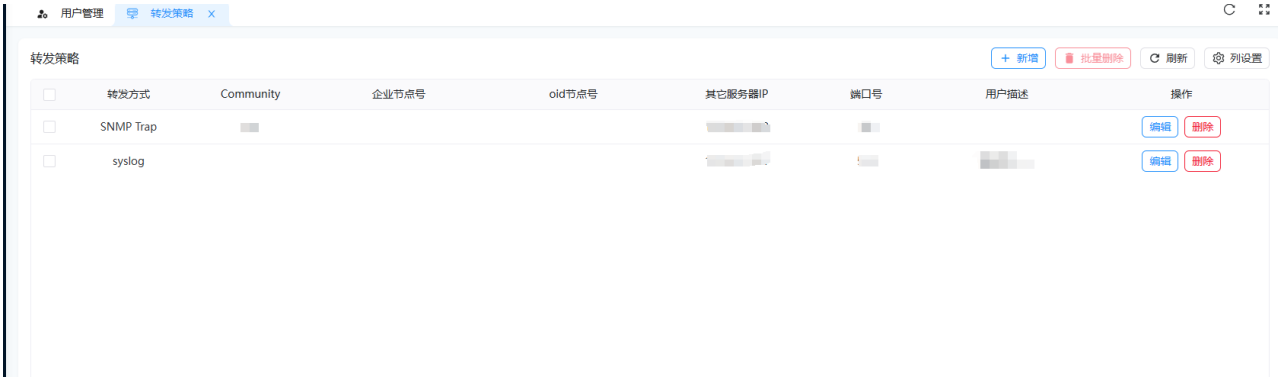


4.2.2 删除

4.2.3 编辑

4.3 转发策略

可以转发系统告警到指定服务器上有 snmp 和 syslog 两种方式



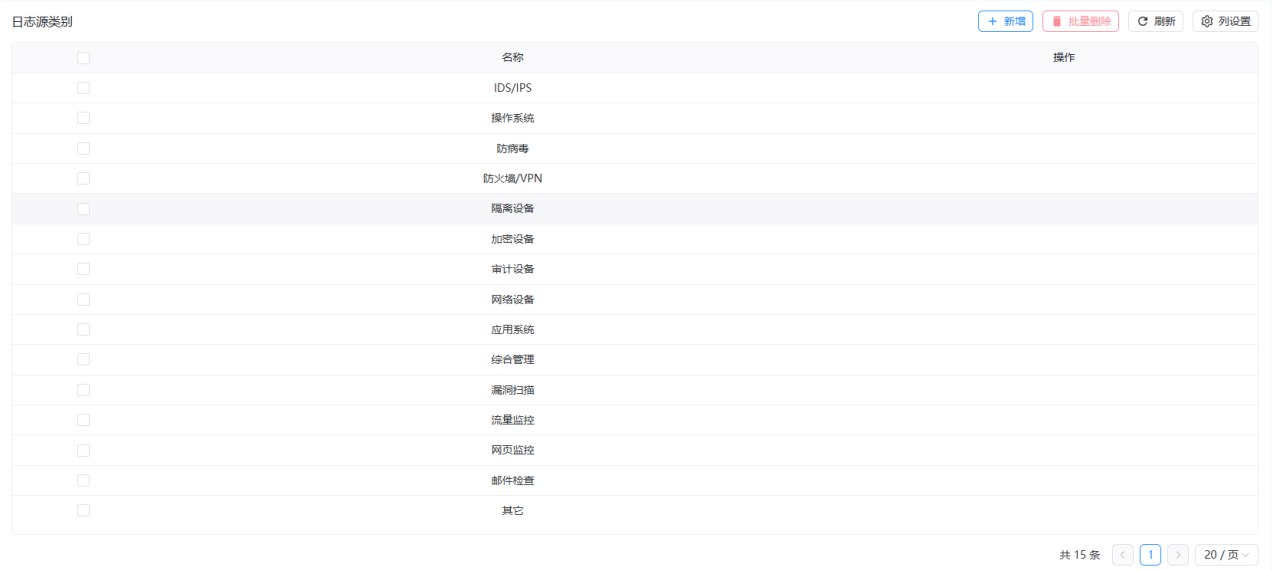
操作员

用户名：operator
密码：Linkqi@111

5 日志管理

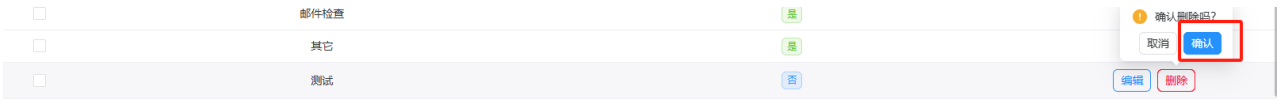
5.1 日志源类别

系统自带的无法操作，可自行添加



5.1.1 新增

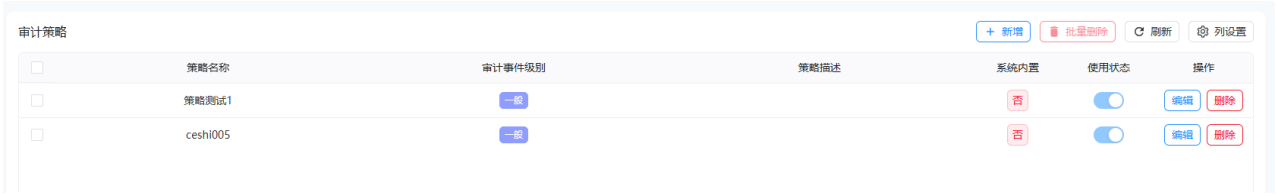
5.1.2 删除



6 审计管理

6.1 审计事件

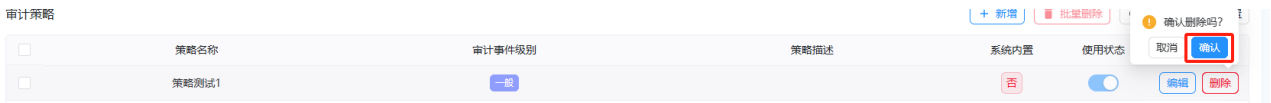
6.2 审计策略



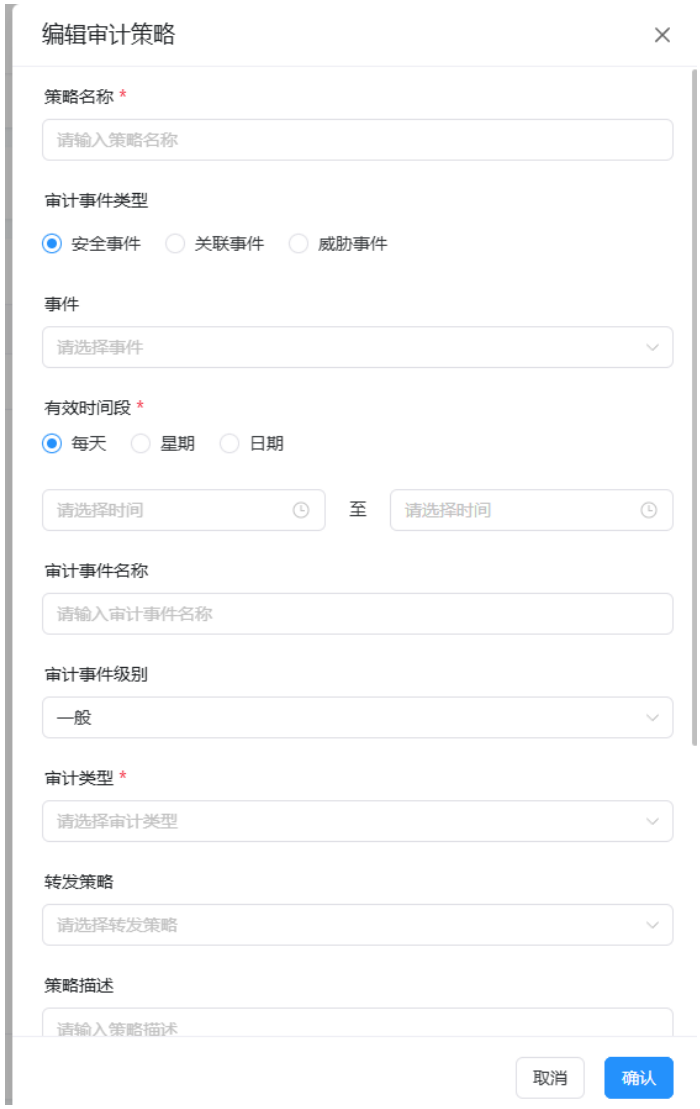
6.2.1 新增


添加审计策略
策略名称 *
请输入策略名称
审计事件类型
安全事件
关联事件
威胁事件
事件
请选择事件
有效时间段 *
每天
星期
日期
请选择时间
至
请选择时间
审计事件名称
请输入审计事件名称
审计事件级别
一般
审计类型 *
请选择审计类型
转发策略
请选择转发策略
策略描述
请输入策略描述
取消
确认

6.2.2 删除


审计策略
+ 新增
批量删除
确认删除吗?
取消
确认
策略名称
审计事件级别
策略描述
系统内置
使用状态
策略测试1
一般
否
编辑
删除

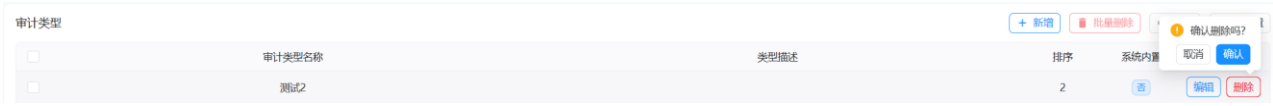
6.2.3 编辑


编辑审计策略
策略名称 *
请输入策略名称
审计事件类型
安全事件
关联事件
威胁事件
事件
请选择事件
有效时间段 *
每天
星期
日期
请选择时间
至
请选择时间
审计事件名称
请输入审计事件名称
审计事件级别
一般
审计类型 *
请选择审计类型
转发策略
请选择转发策略
策略描述
请输入策略描述
取消
确认

6.3 审计类型

6.3.1 新增

6.3.2 删除

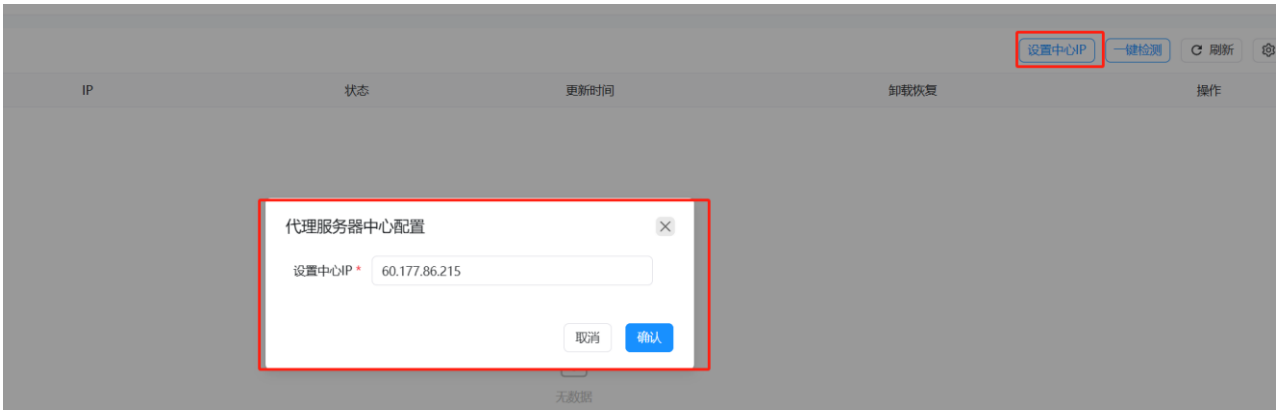


6.3.3 编辑

7 采集管理

7.1 代理服务器

可以设置中心 IP



7.2 采集过滤策略

可自行添加过滤策略

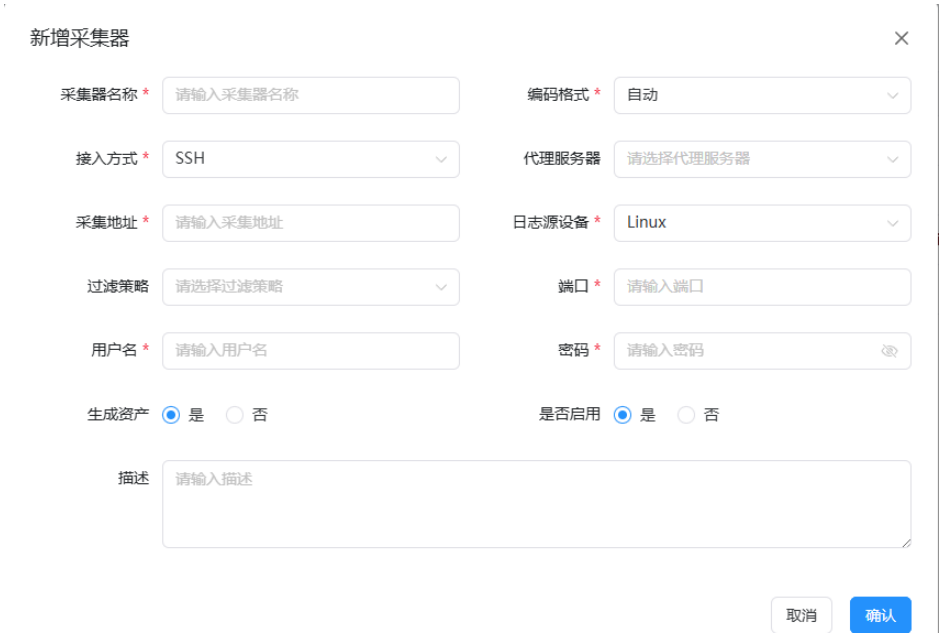
7.3 采集器管理

一、接入方式 snmp 和 syslog 的采集器需要填写采集的地址

Snmp

Syslog

二、Ssh 接入方式需要填写采集地址，端口，用户名和密码



三、Wmi 接入方式需要填写采集地址，用户名密码

Wmi 接入的是 windows 系统需要目标计算机开启 opensshservice 才可以实现连接

具体方法如下

1、Windows 界面中设置

- 打开 **设置**，点击 **应用**。
- 选择 **可选功能**。
- 点击 **添加功能**。
- 搜索 “OpenSSH 服务器”，然后点击 **安装**。
- 打开 **服务**：按 Win + R，输入 `services.msc` 并按 Enter。
- 找到 **OpenSSH SSH Server** 服务，右键点击，选择 **启动**。
- 为了让 SSH 服务器开机自启，可以右键点击该服务，选择 **属性**，将启动类型设置为 **自动**

2、命令行方法

管理员打开 powershell 执行下列操作

#安装 openssh 服务器组件

1)Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

#启动 ssh

2)Start-Service sshd

#设置开机自启

3)Set-Service -Name sshd -StartupType Automatic

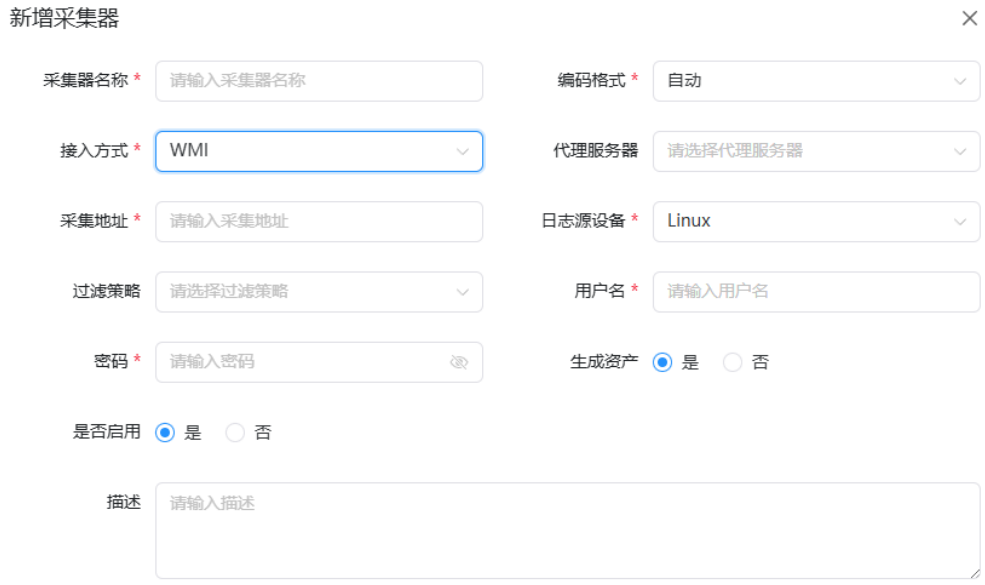
#防火墙放行

4)New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

#查看服务运行状态

5)Get-Service sshd

配置完成后添加采集器



四、Sftp 和 ftp 的接入方式类似，需要填写地址，端口(sftp：22/ftp：21)，用户名和密码以及采集的日志路径例如/var/log/auth.log

7.4 日志源设备

可自行添加

8 报表管理

8.1 报表列表

报表实例展示

8.2 报表任务

可添加定时任务，将报表发送给收件人

8.3 报表查询

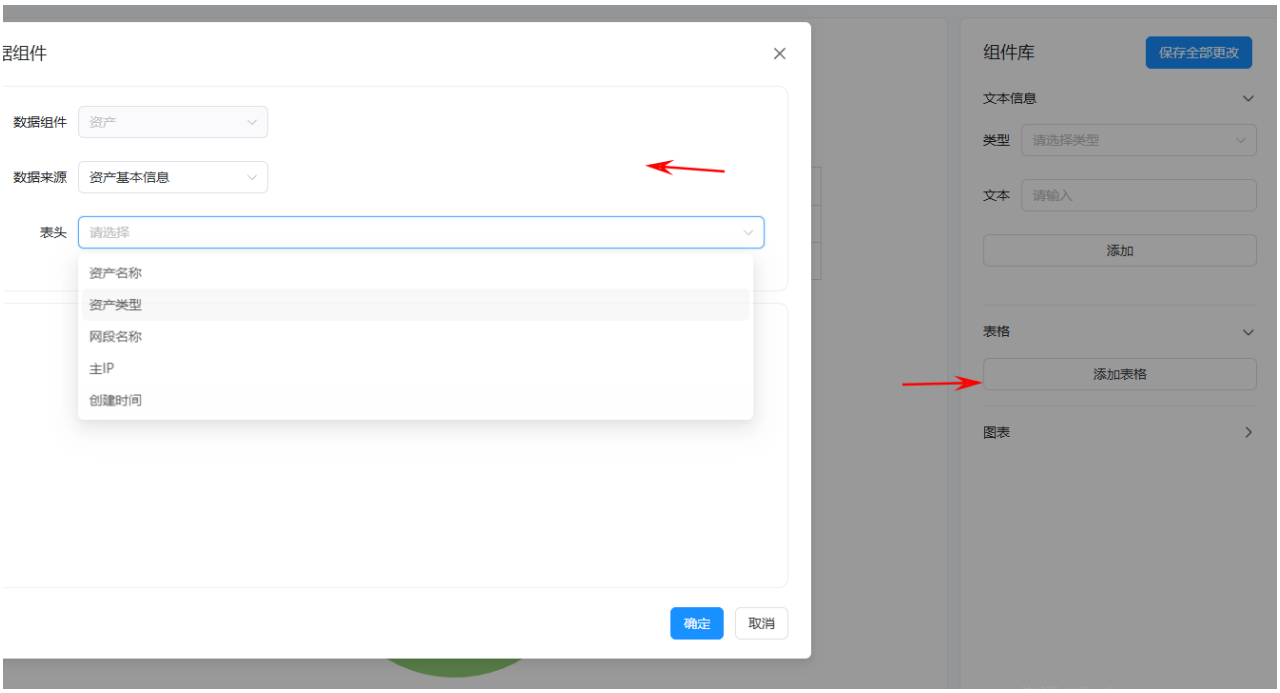
有资产信息报表和综合报表

8.4 自定义报表模板

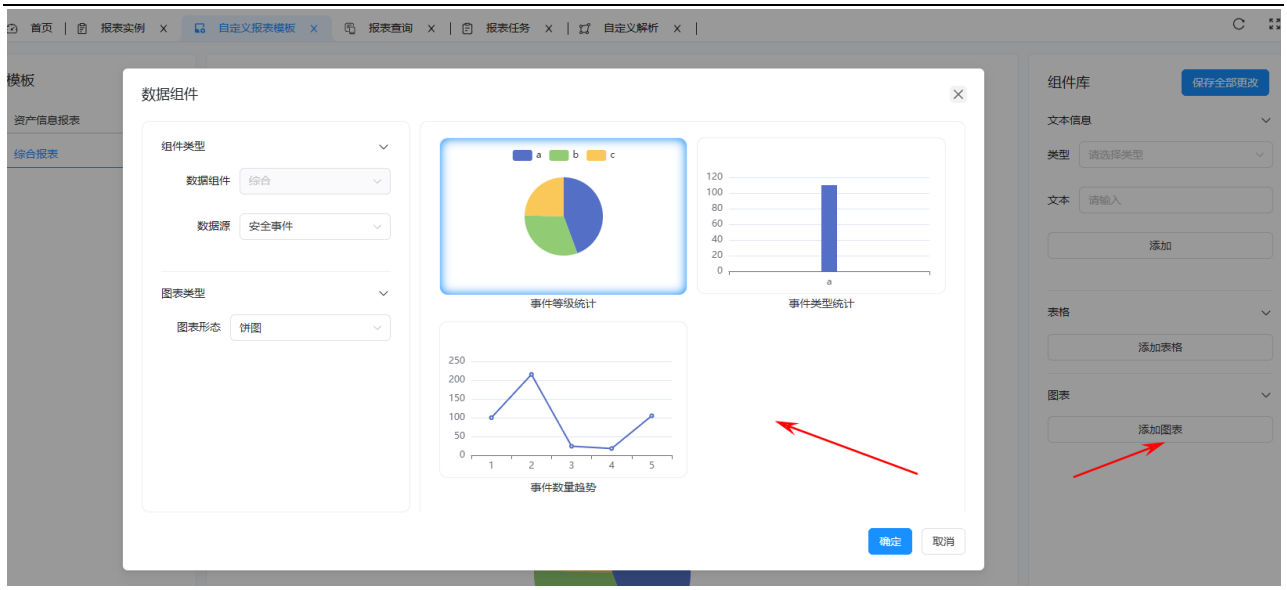
对审计信息报表和综合报表进行自定义展示：


模板
资产信息报表
综合报表
资产信息报表
一、资产基本信息
资产类型
资产名称
网段名称
主IP
创建时间
xxx
二、资产类型分布统计
a
b
c
组件库
保存全部更改
文本信息
类型
请选择类型
文本
请输入
添加
表格
图表

（主界面）


组件
数据组件
资产
数据来源
资产基本信息
表头
请选择
资产名称
资产类型
网段名称
主IP
创建时间
确定
取消
组件库
保存全部更改
文本信息
类型
请选择类型
文本
请输入
添加
表格
添加表格
图表

（添加表格）

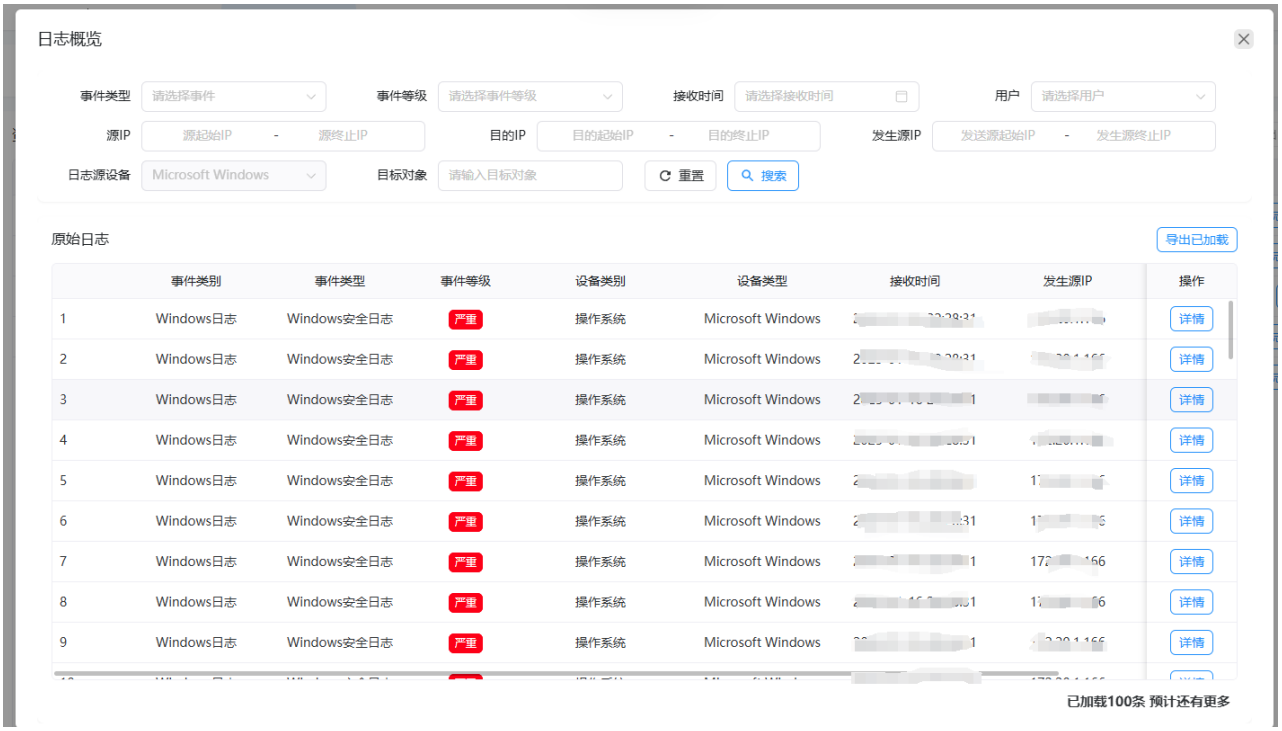


（添加图表）

9 资产管理

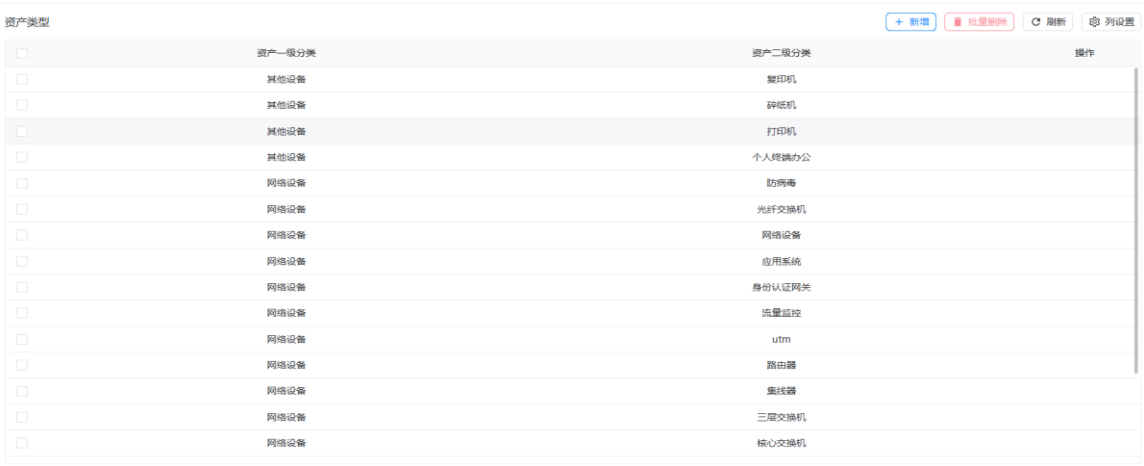
9.1 资产列表

可以管理自己的资产，可以单独查看资产的日志



9.2 资产类型

可自行添加资产



9.3 资产属性

略

9.4 区域管理

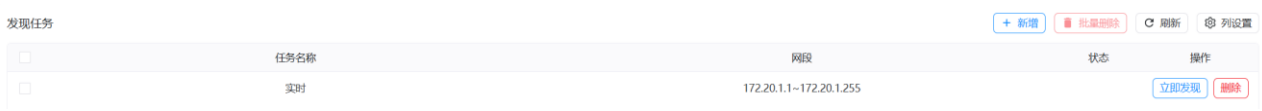
管理区域资源，自行添加

9.5 网络管理

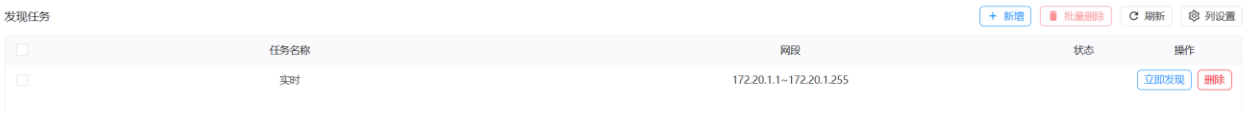
管理网络资源

9.6 资产发现

展示发现的资产列表



也可以设置发现任务



9.7 厂商

9.7.1 新增

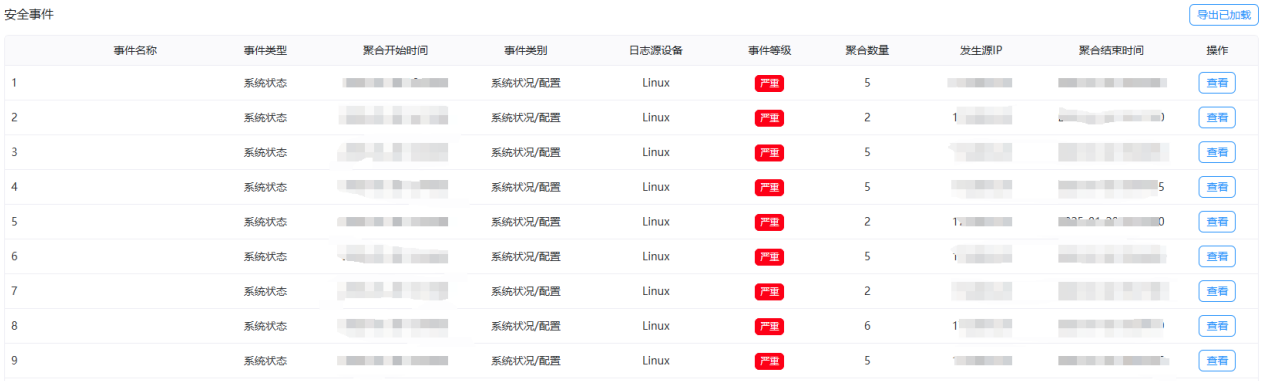
9.7.2 删除

9.7.3 编辑

10 事件管理

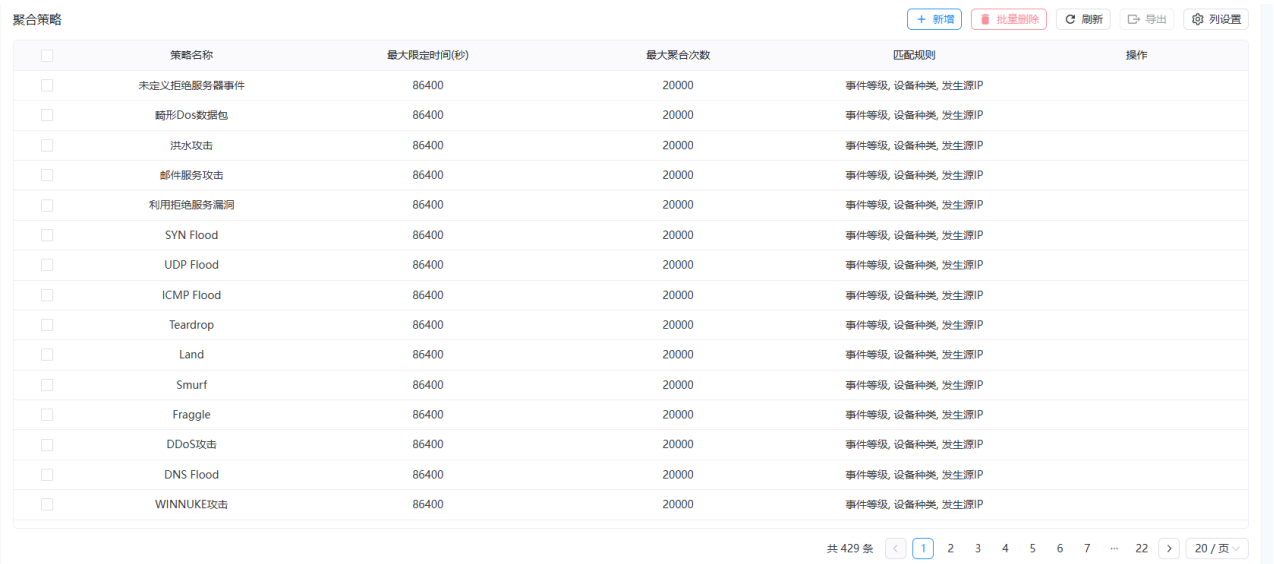
10.1 安全事件

按照聚合策略聚合到一起的事件；



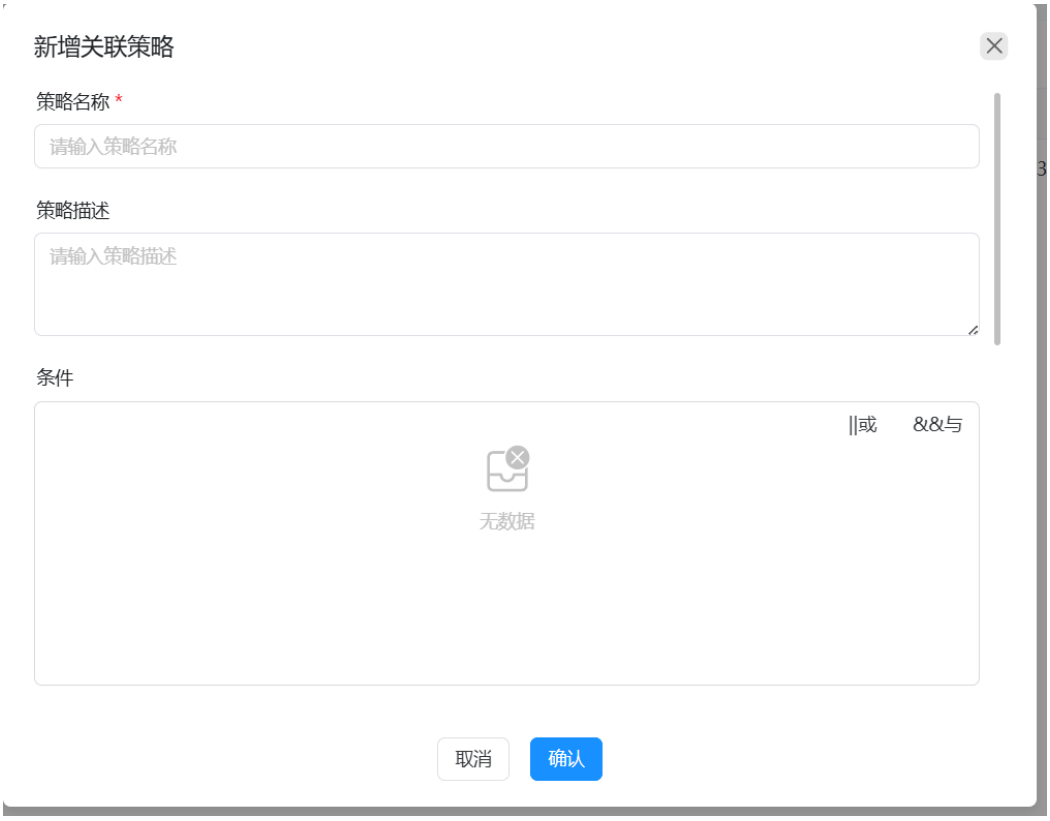
10.2 聚合策略

按照匹配规则把采集到的日志消息归类聚合到一起，可自行添加聚合规则；



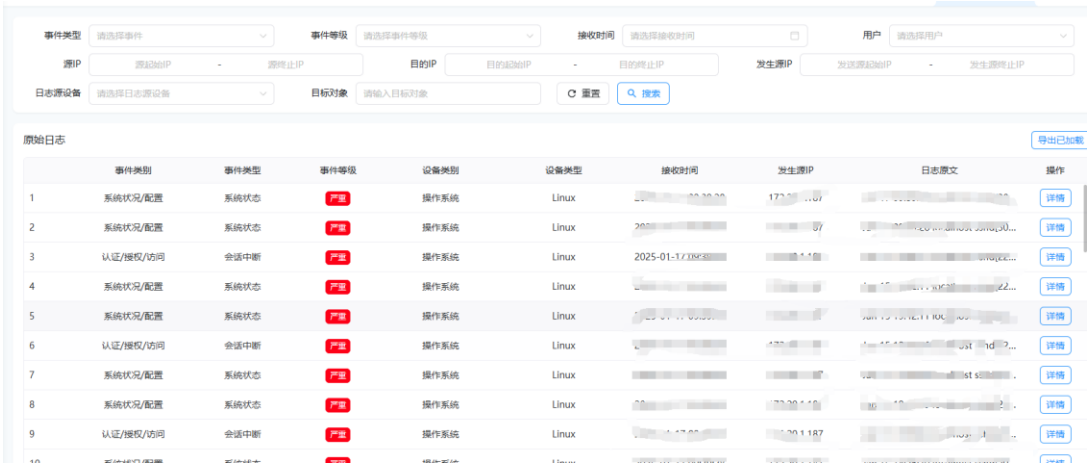
10.3 关联策略

新增关联策略



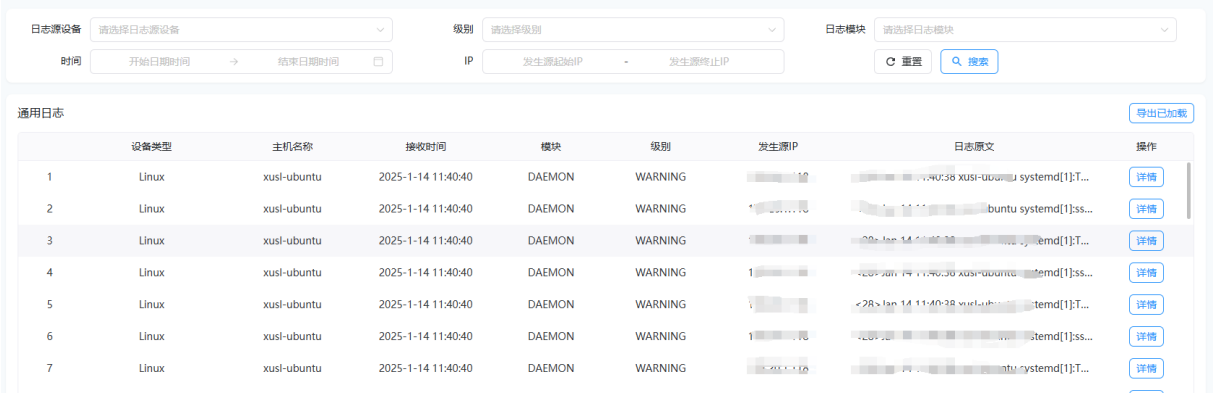
10.4 原始日志

存放 ssh、ftp、sftp、wmi 接入方式的数据



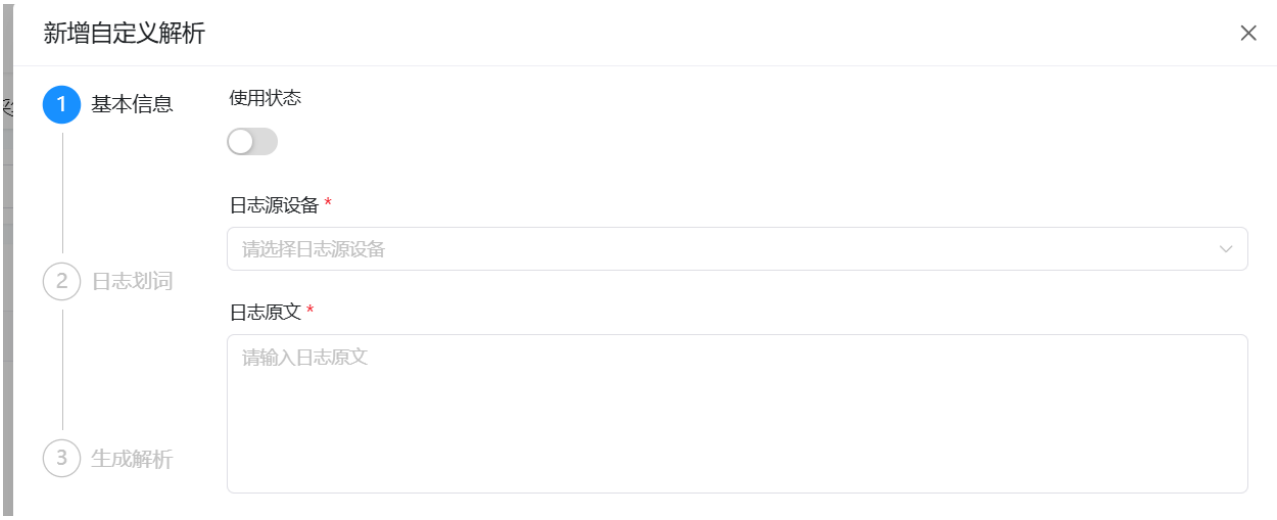
10.5 通用日志

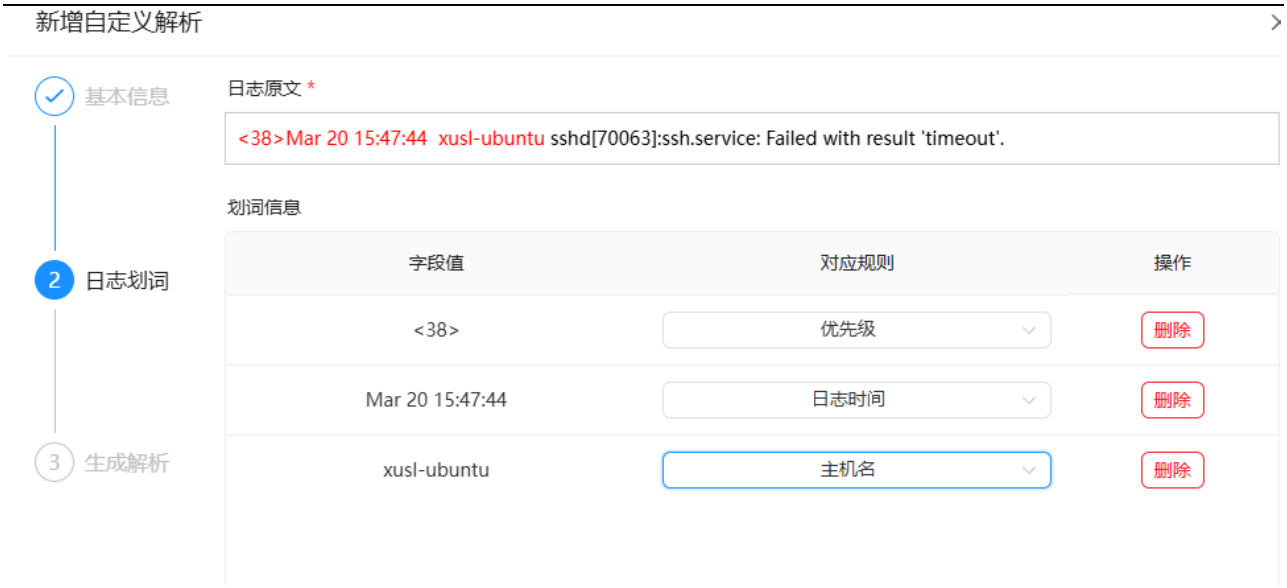
存放 syslog 和 snmp 接入方式的数据

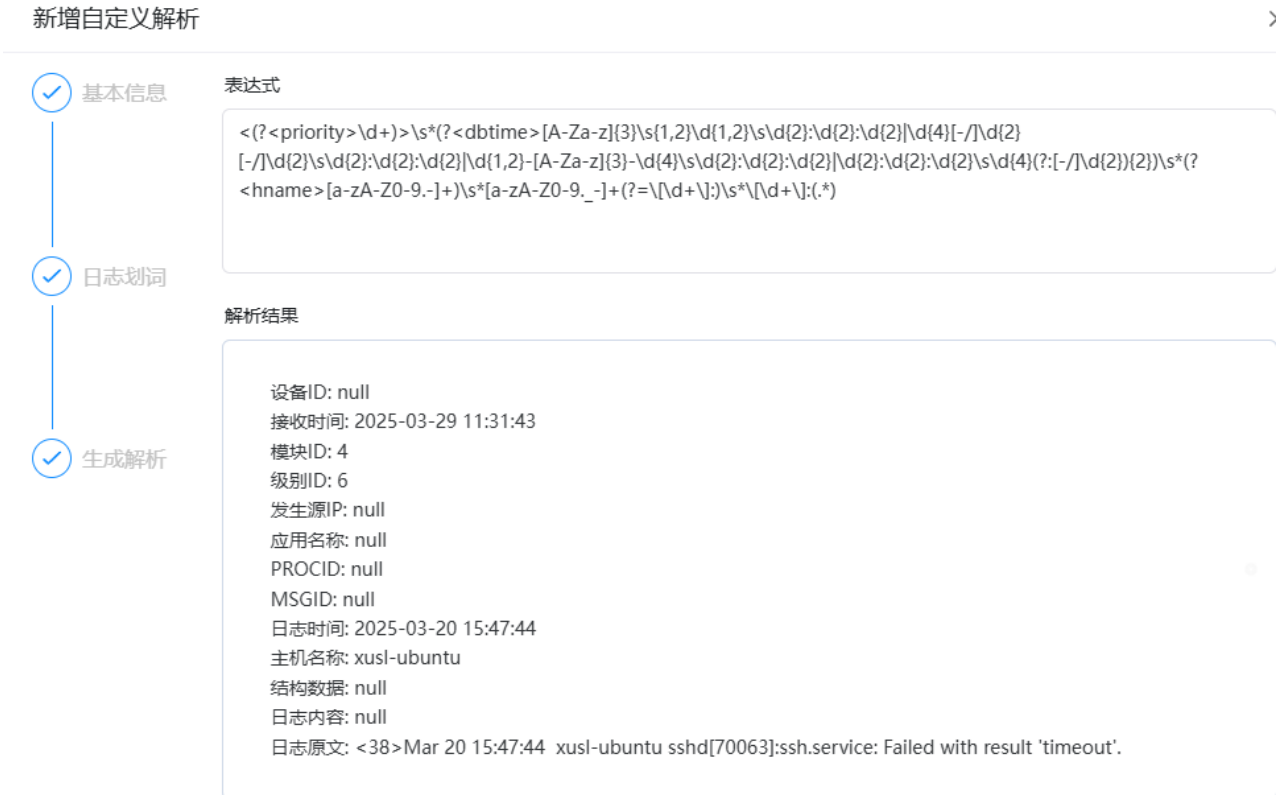


10.6 自定义解析

可设置解析策略



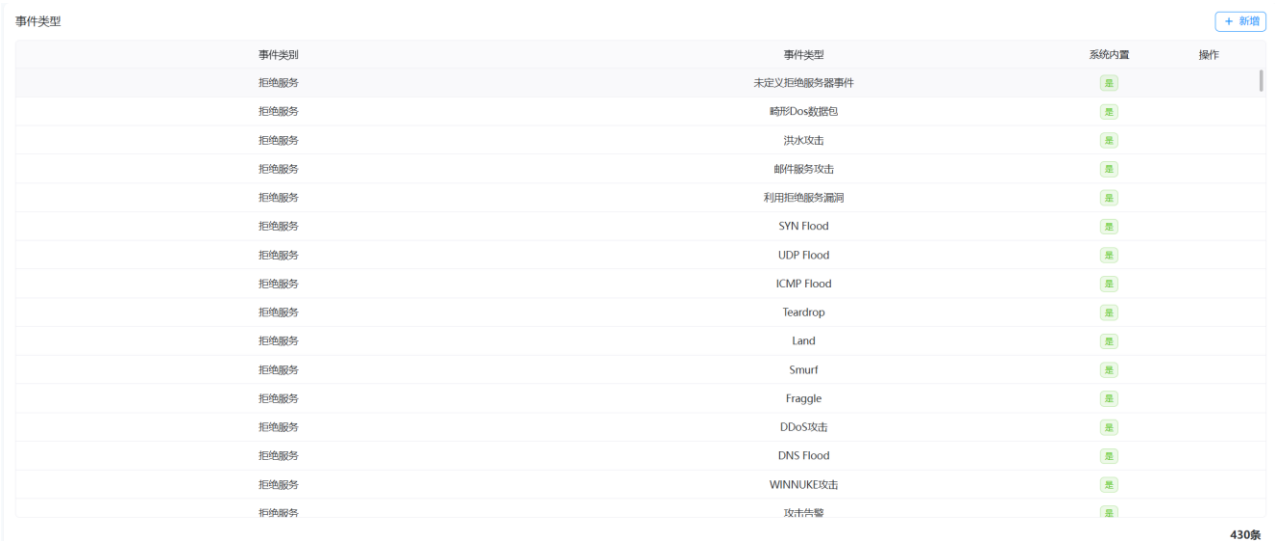

新增自定义解析
基本信息
日志划词
生成解析
日志原文 *
<38>Mar 20 15:47:44 xusl-ubuntu sshd[70063]:ssh.service: Failed with result 'timeout'.
划词信息
字段值
对应规则
操作
<38>
优先级
删除
Mar 20 15:47:44
日志时间
删除
xusl-ubuntu
主机名
删除


新增自定义解析
基本信息
日志划词
生成解析
表达式
<(?<priority>\d+)>\s*(?<dbtime>[A-Za-z]{3}\s{1,2}\d{1,2}\s\d{2}:\d{2}:\d{2}|\d{4}[-/]\d{2}
[-/]\d{2}\s\d{2}:\d{2}:\d{2}|\d{1,2}-[A-Za-z]{3}-\d{4}\s\d{2}:\d{2}:\d{2}|\d{2}:\d{2}:\d{2}\s\d{4}(?:[-/]\d{2}){2})\s*(?
<hname>[a-zA-Z0-9.-]+)\s*[a-zA-Z0-9._-]+(?=\[\d+\]:)\s*\[\d+\]:(.*)
解析结果
设备ID: null
接收时间: 2025-03-29 11:31:43
模块ID: 4
级别ID: 6
发生源IP: null
应用名称: null
PROCID: null
MSGID: null
日志时间: 2025-03-20 15:47:44
主机名称: xusl-ubuntu
结构数据: null
日志内容: null
日志原文: <38>Mar 20 15:47:44 xusl-ubuntu sshd[70063]:ssh.service: Failed with result 'timeout'.

10.7 事件


事件
新增
批量删除
刷新
列设置
事件名称
系统内置
操作
admxx
否
编辑
删除

10.8 事件类型



10.9 事件特征值

11 告警管理

11.1 审计告警

11.2 告警策略

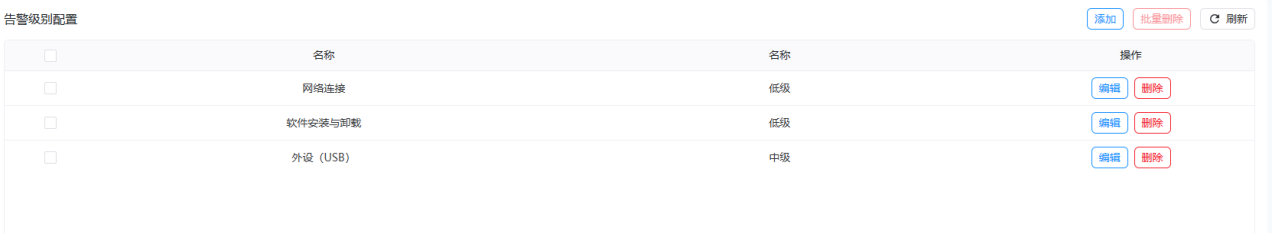
自行添加告警策略

11.3 系统告警

可以批量确认或者删除

11.4 系统告警级别配置

配置系统告警的级别对应：



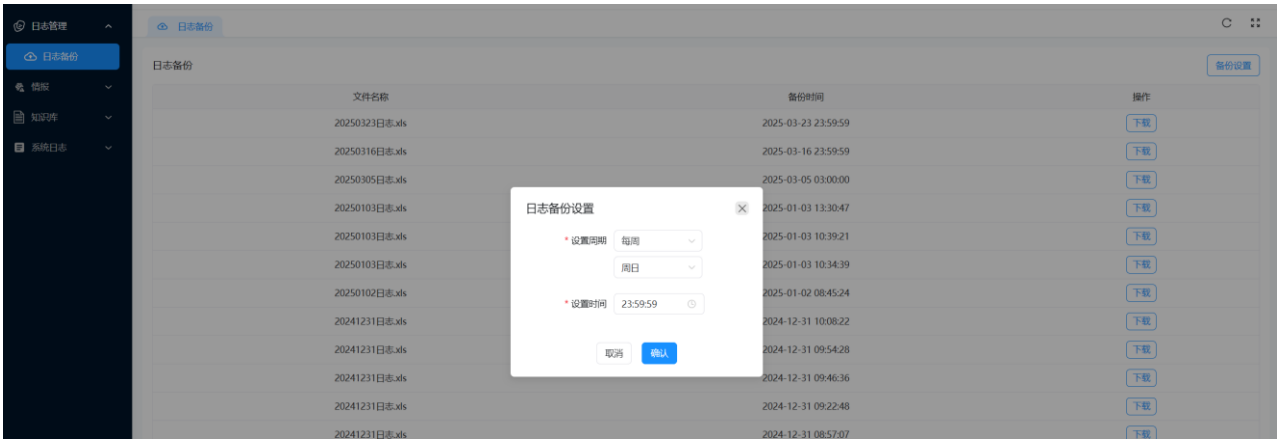
审计员

账号：auditor
密码：Linkqi@222

12 日志管理

12.1 日志备份

可以设置备份的时间和周期

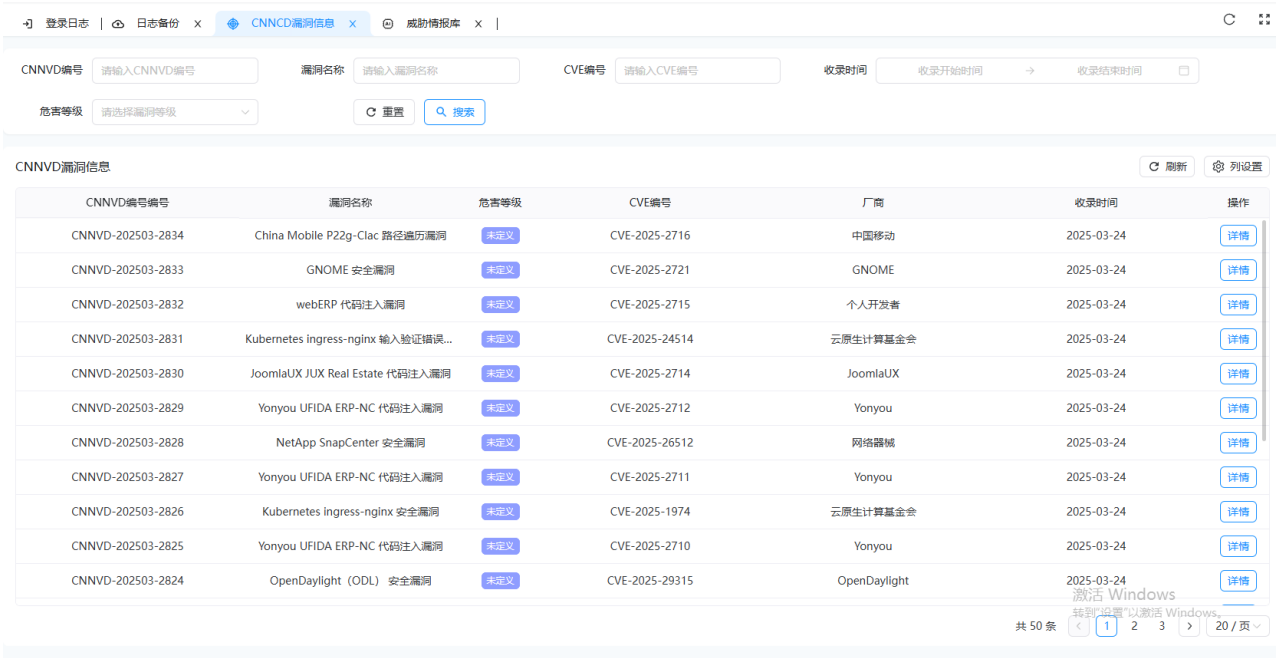


13 情报库

13.1 威胁情报库

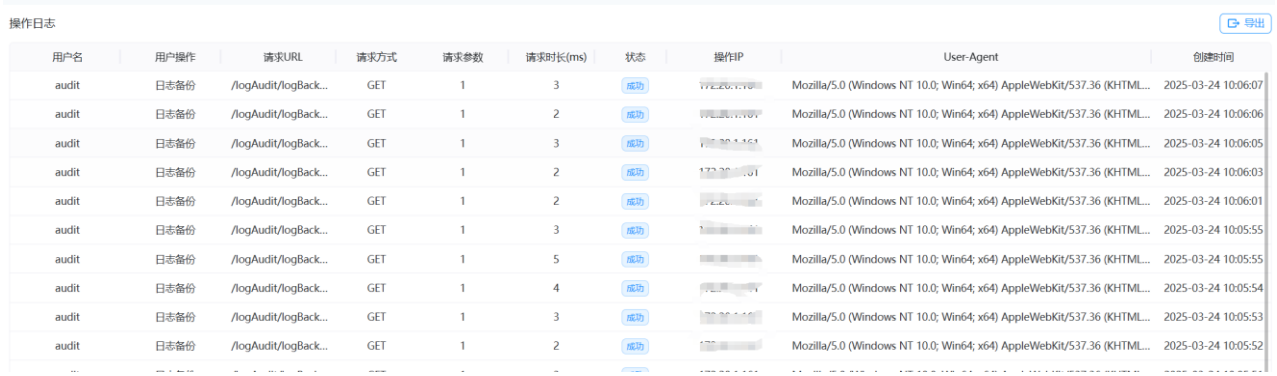
14 漏洞库

14.1 CNNVD 漏洞信息

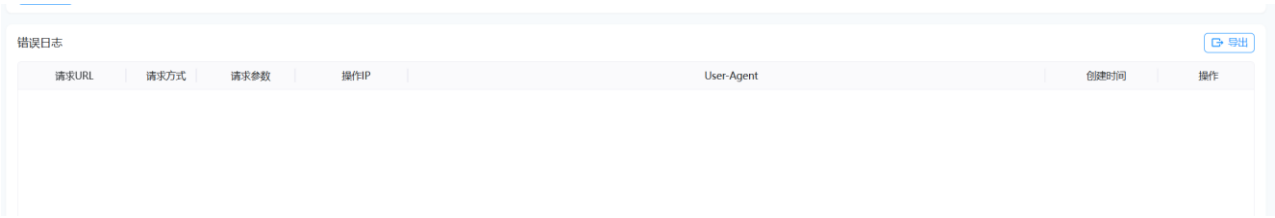


15 系统日志

15.1 操作日志



15.2 错误日志



15.3 登录日志