

# 黑盾综合日志审计分析系统

HD-LAS V4.0

## 用户手册

福建省海峡信息技术有限公司

2023年11月

# 目录

目录.....	2
<b>1 概述.....</b>	<b>4</b>
1.1 初次使用说明 .....	4
1.2 系统简介 .....	4
1.3 系统概述 .....	4
1.4 管理概述 .....	4
1.4.1 客户端分类.....	4
1.4.2 系统授权.....	5
<b>2 功能使用.....</b>	<b>7</b>
2.1 登陆 .....	7
2.2 总览 .....	8
2.2.1 总览.....	8
2.2.2 大屏可视.....	8
2.3 资产管理 .....	9
2.3.1 资产管理.....	9
2.3.2 资产发现.....	11
2.4 事件分析 .....	14
2.4.1 告警监控.....	14
2.4.2 日志检索.....	21
2.4.3 审计事件.....	23
2.4.4 关联事件.....	25
2.5 报表管理 .....	26
2.5.1 安全报告.....	26
2.5.2 统计报表.....	28
2.6 策略管理 .....	33
2.6.1 关联分析规则.....	33
2.6.2 统计分析规则.....	34
2.6.3 审计分析规则.....	35
2.6.4 基线分析规则.....	36
2.6.5 预处理规则.....	37
2.6.6 规则字典.....	39
2.6.7 归并规则.....	40
2.6.8 过滤规则.....	41
2.6.9 分类规则.....	42
2.7 系统管理 .....	43
2.7.1 基础配置.....	43
2.7.2 系统用户.....	48
2.7.3 系统角色.....	48
2.7.4 组织结构.....	49
2.7.5 系统日志.....	49

2.7.6 引擎监控.....	50
2.7.7 设备管理.....	50

# 1 概述

## 1.1 初次使用说明

本文档帮助用户了解黑盾综合日志审计分析系统的主要功能和操作步骤。在进行操作之前，请确认已经获得操作权限的账号。

## 1.2 系统简介

黑盾综合日志审计分析系统是基于 B/S (Browser/Server) 架构。客户端是 Web 浏览器，用于浏览管理界面。服务器运行着系统的主要功能，并与客户端通信，显示各项安全事件信息。

## 1.3 系统概述

黑盾综合日志审计分析系统的服务器分为后端服务器和前端服务器两大部分。

后端服务器负责对各项网元设备的安全事件进行捕获、归类和分析，并将分析结果存储到数据库中。

前端服务器的设计目的是将后端服务器分析结果数据展现给用户，并提供丰富的报表供用户使用。系统可以进行各种形式的服务器和客户端操作的配置，以及数据存储模式的配置，Web 服务器管理等。配置工作通过修改配置文件进行。

## 1.4 管理概述

### 1.4.1 客户端分类

黑盾综合日志审计分析系统 Web 客户端可以查看各项安全事件、安全预警等各项分析结果；并产生各种分析结果报告。登陆界面如图 1-1。



### 1.4.1.1 Web 客户端

Web 客户端完全使用浏览器，不需要安装额外的软件或者 Java 插件。管理员可以在任何地方访问 Web 客户端，并且不受代理和防火墙的限制。

### 1.4.1.2 客户端启动

在启动客户端之前先确定设备已经启动。

启动过程如下：

- (1) 打开浏览器，在地址栏中输入 `https://服务器 IP 地址`。
- (2) 输入用户名、密码及验证码。
- (3) 点击“登录”按钮，客户端随即启动。

## 1.4.2 系统授权

黑盾综合日志审计分析系统授权入口共两处，登录页面-系统授权和设备管理-许可管理；授权类型分为两种，本地授权和网络授权。

系统授权×

### 修正系统时间

当前系统时间： 2022-01-01 14:19:17

修正系统时间：

修正时间

### 产品授权

提示：若选择文件授权，授权文件大小不超过16M！

授权方式： 文件授权  网络授权

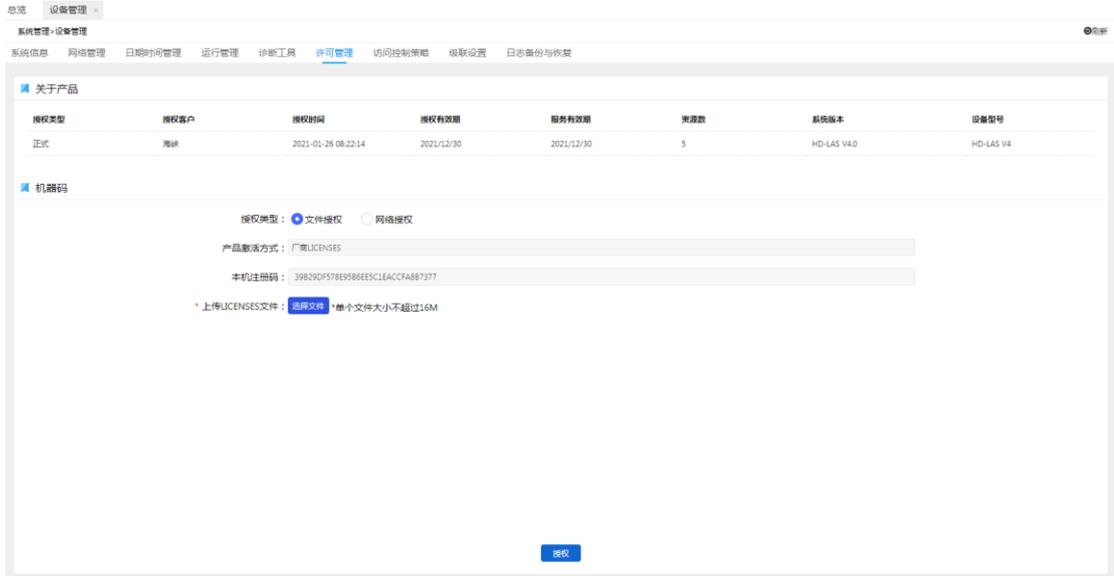
授权服务器IPV4地址：

本地管理口IPV4地址：

本地管理口子网掩码：

网关：

保存并授权



### 1.4.2.1 本地授权

本地授权过程如下：

- (1) 授权类型：文件授权；
- (2) 选择并上传授权文件，点击授权，并确认授权，待授权成功后，授权信息更新。

### 1.4.2.2 网络授权

网络授权过程如下：

- (1) 授权类型：网络授权；
- (2) 输入网络配置信息，点击授权，并确认授权，待授权成功后，授权信息更新。

## 2 功能使用

### 2.1 登陆

要使用该平台需先登录到平台的服务端，输入管理员的账号和密码，点击登录，登录到平台主界面如下图所示：



## 2.2 总览

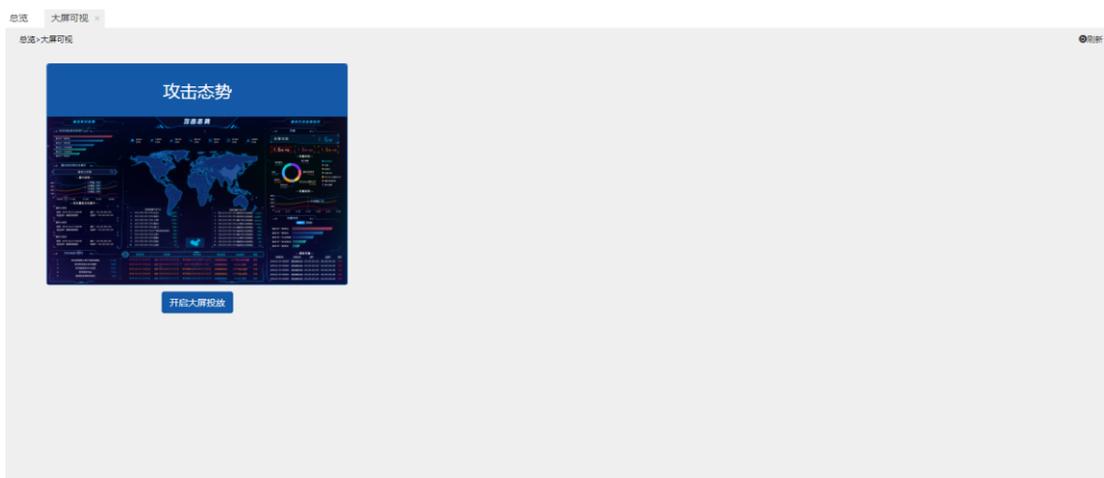
### 2.2.1 总览

路径：总览->总览。可查看总览信息。



### 2.2.2 大屏可视

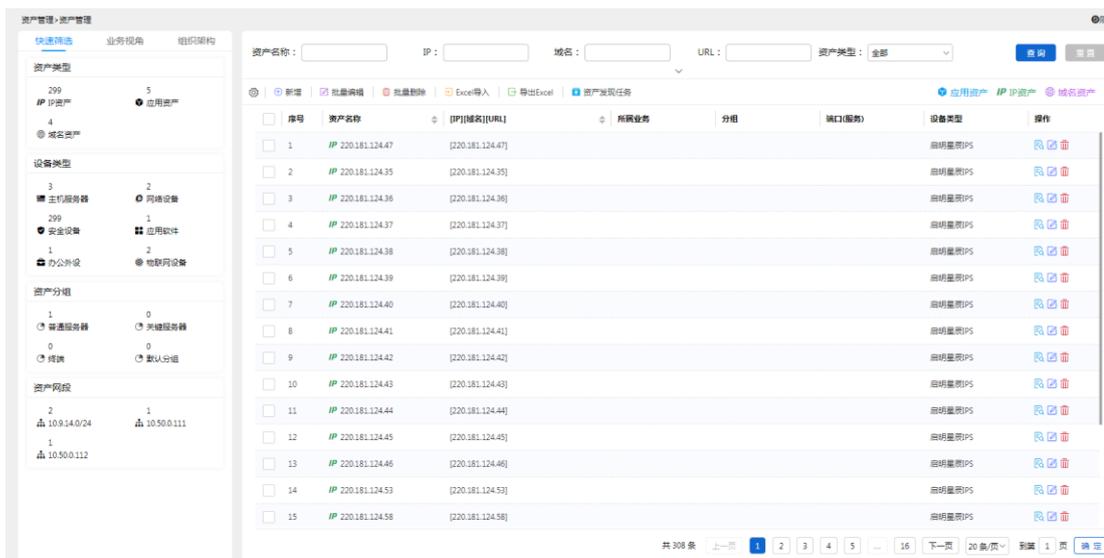
路径：总览->大屏可视。可查看大屏信息。



## 2.3 资产管理

### 2.3.1 资产管理

路径：资产管理->资产管理。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【新增】，跳至新增页面。

点击【提交】，页面跳转至资产管理页面。  
左边勾选框勾选多项，点击【批量编辑】，可以批量编辑资产。  
左边勾选框勾选多项，点击【批量删除】，可以批量删除资产。  
点击【excel 导入】，页面跳至 excel 导入页面。

点击【导入模板下载】，打开模板。

资产名称	资产类型	所属业务系统	资产分组	所属网络区域	IP地址	设备类型(操作系统)	VCPU数量	内存容量	硬盘容量	域名	备注
安全态势感知应用服务器	IP资产	态势感知平台	矩阵实验室网络	矩阵实验室网络	192.168.85.6	服务器	0	0	0	csa.sj.ncbi.cn	
安全态势感知域名服务器	域名资产	态势感知平台	矩阵实验室网络	矩阵实验室网络	192.168.85.7	服务器	0	0	0	0	csa.sj.ncbi.cn
安全态势感知web服务	应用资产	态势感知平台	矩阵实验室网络	矩阵实验室网络	192.168.85.8	web服务器	0	0	0	0	http:

表格内填写相关信息后保存，选择导入文件，验证告警为0时点击【提交】，  
页面跳至资产管理页面。

点击【导出 excel】，可将列表资产导出，导出内容如下所示

序号	IP地址	资产名称	IP域名	URL	资产类型	设备类型	所属单位	所属网络	业务系统	风险等级	创建时间
1	10.50.0.200q		10.50.0.200		IP资产	Linux/Unix系统		政务外网公用区	福州市交通综合行	正常	2020-01-03 09:36:20.0
2	10.50.0.221		10.50.0.221		IP资产	Windows 7		政务外网互联网	福州市交通综合行	正常	2020-01-02 14:30:32.0
3	10.50.0.204		10.50.0.204		IP资产	Windows 7		政务信息网	福州市交通综合行	正常	2020-01-03 09:31:19.0
4	10.50.0.252		10.50.0.252		IP资产	Linux/Unix系统		政务信息网	福州市交通综合行	正常	2020-01-03 09:35:23.0

点击【资产发现任务】，页面跳至资产发现页面。  
 点击操作中的【查看】，跳至查看资产页面，可查看资产信息。  
 点击操作中的【编辑】，跳至编辑资产页面，可编辑资产信息。  
 点击【删除】，可删除资产。

### 2.3.2 资产发现

路径：资产管理->资产发现。

资产发现模块有‘发现资产’和‘发现任务’2个标签页。

1、前者是发现结果，可对发现资产进行审核

序号	IP[域名][URL]	端口(服务)	资产分组	所属业务	任务名称	发现时间	审核状态	审核时间	操作
1	[10.9.14.33]	22(sh,3306(MySQL))			ZCSM-20210119-4065	2021-01-19 18:42:47	未审核		查看 删除
2	[10.50.0.250]	443(HTTPS,8000(dwp),9000(http),9010(http))			ZCSM-20210119-3777	2021-01-19 18:31:41	未审核		查看 删除
3	[10.50.0.240]	22(sh)			ZCSM-20210119-3777	2021-01-19 18:31:41	未审核		查看 删除
4	[10.9.14.3][http://10.9.14.3-9003]	22(sh,80(HTTP),443(HTTPS),3306(MySQL),5100(http),...	65446546...		ZCSM-20210119-8621	2021-01-04 15:34:26	未审核		查看 删除
5	[10.9.14.3][http://10.9.14.3-9002]	22(sh,80(HTTP),443(HTTPS),3306(MySQL),5100(http),...	65446546...		ZCSM-20210119-8621	2021-01-04 15:34:26	未审核		查看 删除
6	[10.9.14.3][http://10.9.14.3-8080]	22(sh,80(HTTP),443(HTTPS),3306(MySQL),5100(http),...	65446546...		ZCSM-20210119-8621	2021-01-04 15:34:26	未审核		查看 删除
7	[10.9.14.3][http://10.9.14.3-9001]	22(sh,80(HTTP),443(HTTPS),3306(MySQL),5100(http),...	65446546...		ZCSM-20210119-8621	2021-01-04 15:34:25	未审核		查看 删除
8	[10.9.14.3][http://10.9.14.3-9400]	22(sh,80(HTTP),443(HTTPS),3306(MySQL),5100(http),...	65446546...		ZCSM-20210119-8621	2021-01-04 15:34:25	未审核		查看 删除
9	[10.9.14.22][http://10.9.14.22-9010]	22(sh,443(HTTPS),8000(dwp),8009(jsp),8080(http),...	65446546...		ZCSM-20210104-3858	2021-01-04 15:34:25	未审核		查看 删除
10	[10.50.0.33]	80(HTTP),443(ssl),3306(MySQL),8680(tcpwrapped)			ZCSM-20210119-3777	2021-01-19 18:31:43	未审核		查看 删除
11	[10.50.0.252]	23(belnet,80(HTTP))			ZCSM-20210119-3777	2021-01-19 18:31:42	未审核		查看 删除

通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【全部选择】，可以选中列表中的所有数据，再次点击，选中效果取消。

左边勾选框勾选单个或多个资产，点击【批量删除】，可以删除选中内容。

左边勾选框勾选单个或多个资产，点击【批量审核通过】，可以批量审核通过未审核资产。

左边勾选框勾选单个或多个资产，点击【批量编辑】，可以编辑选中内容。

点击【查看】，进入已审核资产查看页面。

查看信息

基本信息

资产类别: IP资产

资产名称: 10.50.0.252

URL:

IP地址: 10.50.0.252

所属网络: 政务信息网

部署位置:

告警组:

资产分组: 关键服务器

等级定级:

完整性:

系统用途:

备注:

域名:

监控URL:

所属单位:

所属业务: 福州市交通运输局行政执法支队办公自动化系统开发项目

所属区域:

设备类型: Linux/Unix系统

负责人:

机密性:

可用性:

特殊属性

端口	服务	协议	标签	banner
80	HTTP	tcp		

关闭

点击【审核】，进入未审核资产审核页面。

审核资产

基本信息

资产类别: IP资产

资产名称: 10.50.0.252

IP地址: 10.50.0.252

所属网络: 政务外网公网区

部署位置: 最多输入100个字符

告警组:

资产分组: 请选择分组

等级定级: 请选择等级定级

完整性: 请选择完整性

系统用途: 最多输入100个字符

备注: 最多输入200个字符

域名: 最多输入200个字符

URL: 最多输入200个字符

监控URL: 最多输入200个字符

所属业务:

所属区域: 请选择区域

设备类型: Linux/Unix系统

负责人:

机密性: 请选择机密性

可用性: 请选择可用性

特殊属性

端口	服务	协议	标签	应用指纹
23	telnet	tcp		

删除

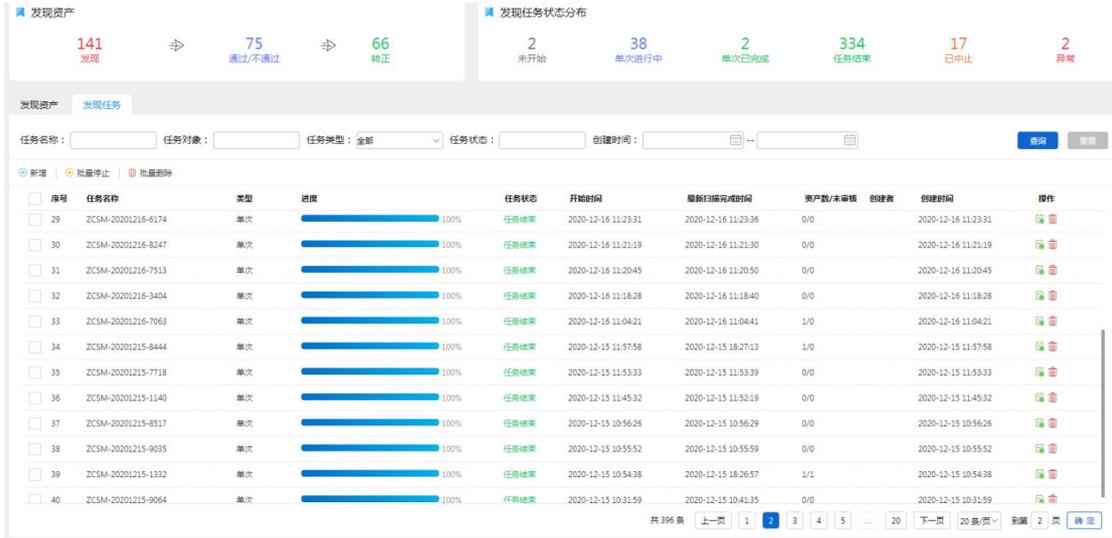
通过

不通过

关闭

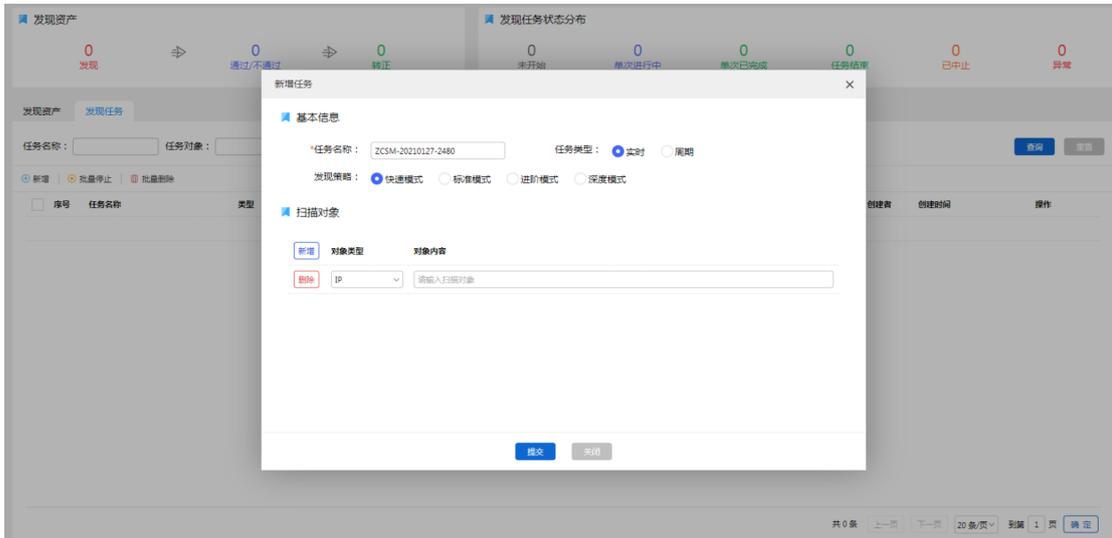
点击【删除】，可删除资产。

2、后者是资产发现任务，可进行资产发现任务操作。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【新增】，进入新增页面

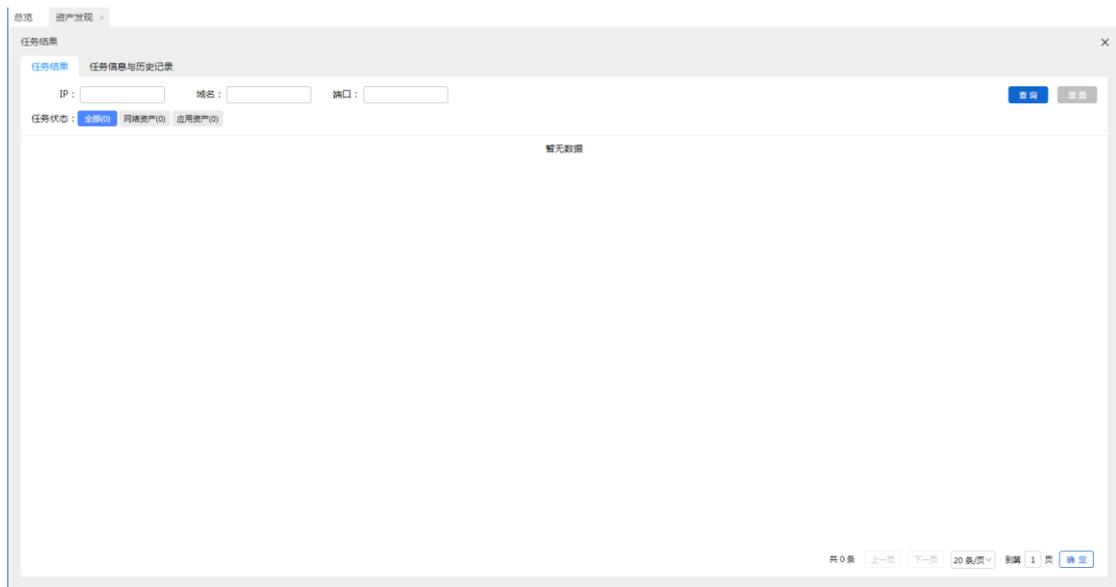


填写相关内容，点击【提交】，进行资产发现任务。

左边勾选框勾选多项，点击【批量停止】，可以批量停止资产发现任务。

左边勾选框勾选多项，点击【批量删除】，可以批量删除资产发现任务。

点击操作中的【查看】，进入查看页面。



- 点击操作中的【编辑】，进入任务编辑页面。
- 点击操作中的【中止】，可以中止资产发现任务。
- 点击操作中的【跳过本轮】，资产发现任务会跳过本轮。
- 点击操作中的【再次执行】，任务再次执行。
- 点击【删除】，删除资产发现任务。

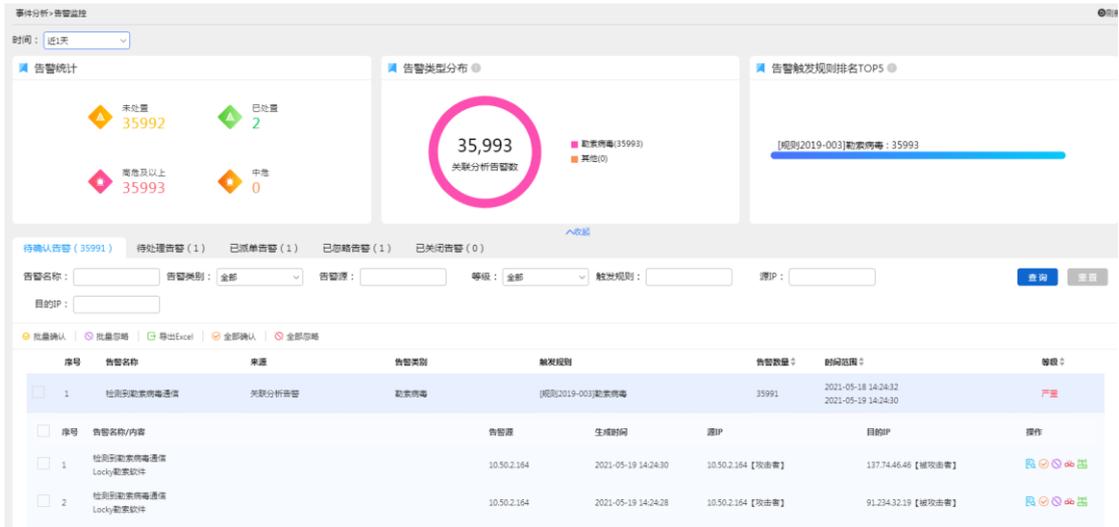
## 2.4 事件分析

### 2.4.1 告警监控

路径：事件分析->告警监控。

通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

- 1、待确认告警页面



点击一条告警事件，左边勾选框勾选多项，点击【批量确认】，可以批量确认告警。

点击一条告警事件，左边勾选框勾选多项，点击【批量忽略】，可以批量忽略告警。

点击【导出 excel】，导出页面如下

序号	告警名称	类别	告警等级	告警源	源IP	目的IP	告警内容	处置状态	发生时间
1	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 11:06:45	
2	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 11:06:42	
4	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 10:54:10	
5	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 10:53:55	
6	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 10:53:45	
7	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 10:52:45	
8	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 10:52:31	
9	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.163	10.50.2.185	220.160.52.163	发现10.50.2.185尝试访问目标220.160.null	2020-01-07 10:52:20	
10	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	61.154.11.191	10.50.2.185	61.154.11.191	发现10.50.2.185尝试访问目标61.154.null	2020-01-07 10:49:24	
11	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	61.154.11.191	10.50.2.185	61.154.11.191	发现10.50.2.185尝试访问目标61.154.null	2020-01-07 10:49:13	
12	HTTP SYS远程执行代码 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP SYS远程执行代码	2020-01-06 13:25:46	
13	HTTP SYS远程执行代码 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP SYS远程执行代码	2020-01-06 13:21:15	
14	HTTP SYS远程执行代码 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP SYS远程执行代码	2020-01-06 12:48:47	
15	HTTP SYS远程执行代码 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP SYS远程执行代码	2020-01-06 12:48:43	
16	HTTP SYS远程执行代码 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP SYS远程执行代码	2020-01-06 12:48:36	
17	HTTP SYS远程执行代码 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	检测到针对HTTP SYS远程执行代码	2020-01-06 12:47:57	
18	访问Tomcat控制台 关联分析告警	Web攻击	中危	218.5.241.22	10.50.2.194	218.5.241.22	10.50.2.194访问18.5.241.22的Tomcat	2020-01-06 12:47:49	
19	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.165	10.50.2.90	220.160.52.165	发现10.50.2.90尝试访问目标220.160.null	2020-01-06 09:55:43	
20	访问Ckeditor编辑器 关联分析告警	Web攻击	中危	220.160.52.165	10.50.2.90	220.160.52.165	发现10.50.2.90尝试访问目标220.160.null	2020-01-06 09:54:41	
21	访问Tomcat控制台 关联分析告警	Web攻击	中危	220.160.52.165	10.50.2.90	220.160.52.165	10.50.2.90访问220.160.52.165的Tomcat	2020-01-06 09:45:21	
22	访问Tomcat控制台 关联分析告警	Web攻击	中危	220.160.52.224	10.50.2.90	220.160.52.224	10.50.2.90访问220.160.52.224的Tomcat	2020-01-06 09:24:22	
23	访问Tomcat控制台 关联分析告警	Web攻击	中危	61.154.11.191	10.50.2.90	61.154.11.191	10.50.2.90访问61.154.11.191的Tomcat	2020-01-06 09:17:54	
24	访问Tomcat控制台 关联分析告警	Web攻击	中危	220.160.52.165	10.50.2.90	220.160.52.165	10.50.2.90访问220.160.52.165的Tomcat	2020-01-06 09:11:38	
25	ThinkPHP v5远程代码执行 关联分析告警	Web攻击	中危	112.111.2.122	10.50.2.71	112.111.2.122	检测到针对112.111.2.122的ThinkPHP	2020-01-03 16:09:04	
26	ThinkPHP v5远程代码执行 关联分析告警	Web攻击	中危	112.111.2.122	10.50.2.71	112.111.2.122	检测到针对112.111.2.122的ThinkPHP	2020-01-03 16:08:44	
27	ThinkPHP v5远程代码执行 关联分析告警	Web攻击	中危	112.111.2.122	10.50.2.71	112.111.2.122	检测到针对112.111.2.122的ThinkPHP	2020-01-03 16:08:34	
28	ThinkPHP v5远程代码执行 关联分析告警	Web攻击	中危	220.160.52.224	10.50.2.71	220.160.52.224	检测到针对220.160.52.224的ThinkPHP	2020-01-03 16:08:15	
29	ThinkPHP v5远程代码执行 关联分析告警	Web攻击	中危	212.64.117.162	10.50.2.71	212.64.117.162	检测到针对212.64.117.162的ThinkPHP	2020-01-03 15:31:49	

点击【全部确认】，可以确认全部告警。

点击【全部忽略】，可以忽略全部告警。

点击一条告警事件，点击操作中的【查看】

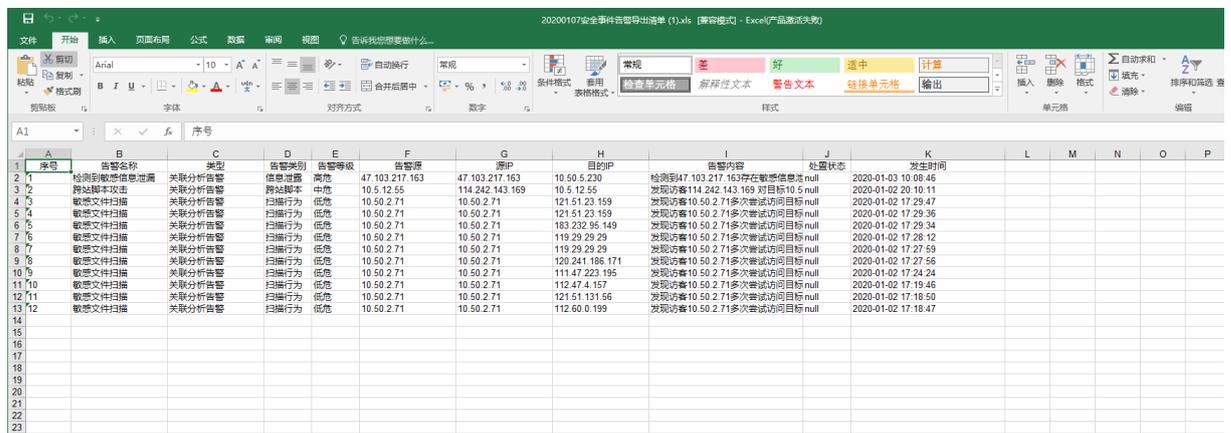


- 点击一条告警事件，点击操作中的【确认】，可以确认告警。
- 点击一条告警事件，点击操作中的【忽略】，可以忽略告警。
- 点击一条告警事件，点击操作中的【一键断网】，可以对 IP 进行封堵。
- 点击一条告警事件，点击操作中的【恢复断网】，可以对 IP 进行解封。

## 2、待处理告警页面

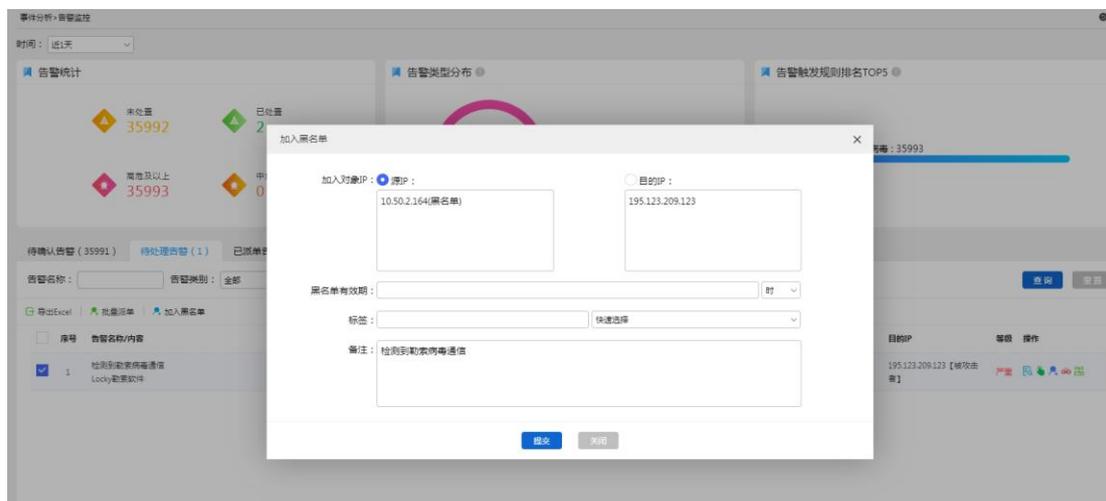


点击【导出 excel】，导出页面如下



左边勾选框勾选多项，点击【批量派单】，可以批量派单告警。

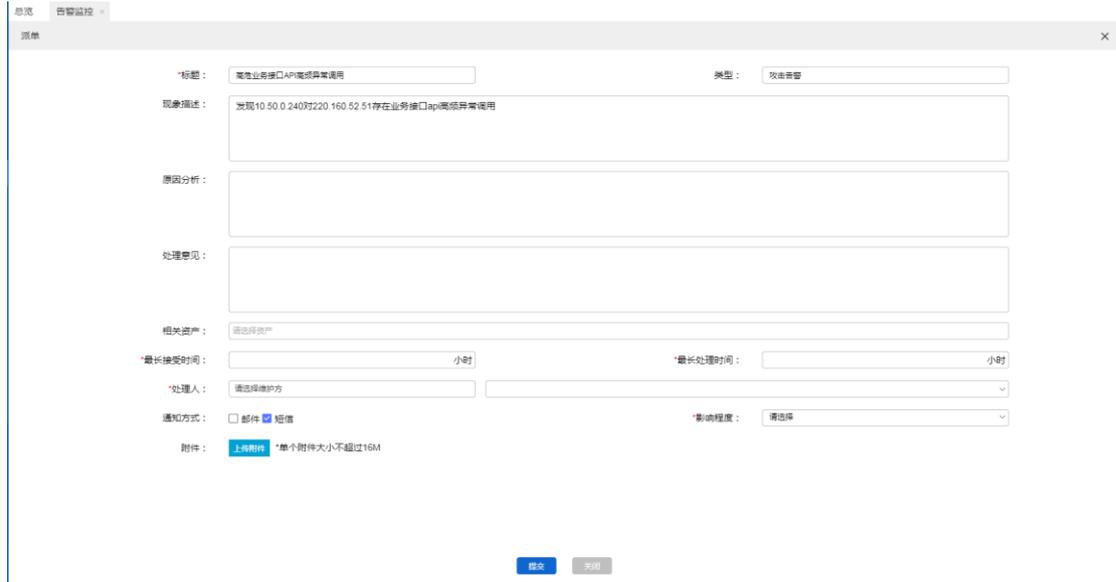
左边勾选框勾选多项，点击【加入黑名单】，可以批量对告警中的源 IP 或目的 IP 加入黑名单。



点击操作中的【查看】

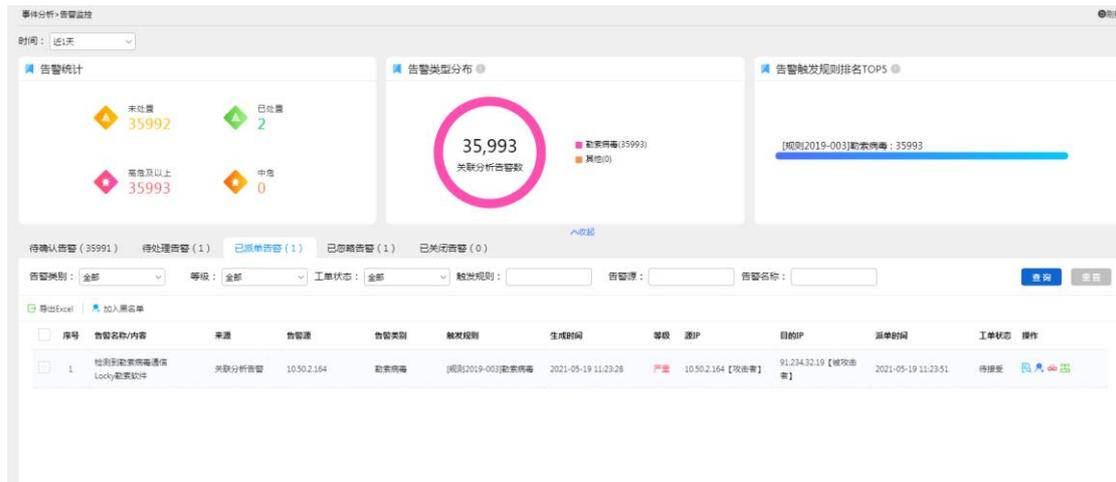


点击操作中的【派单】，可对告警进行派单处理

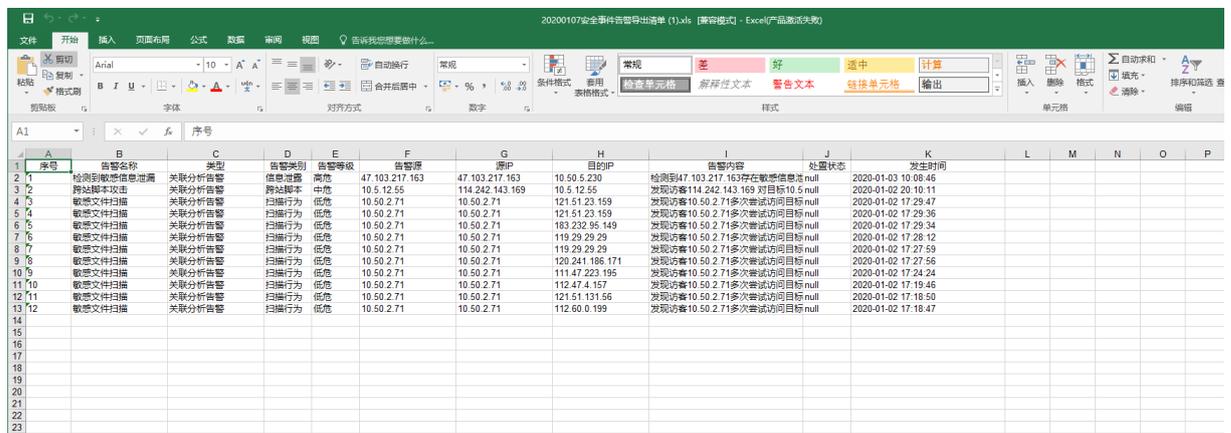


点击操作中的【加入黑名单】，可以对告警中的源 IP 或目的 IP 加入黑名单。  
 点击操作中的【一键断网】，可以对 IP 进行封堵。  
 点击操作中的【恢复断网】，可以对 IP 进行解封。

### 3、已派单告警页面



点击【导出 excel】，导出页面如下



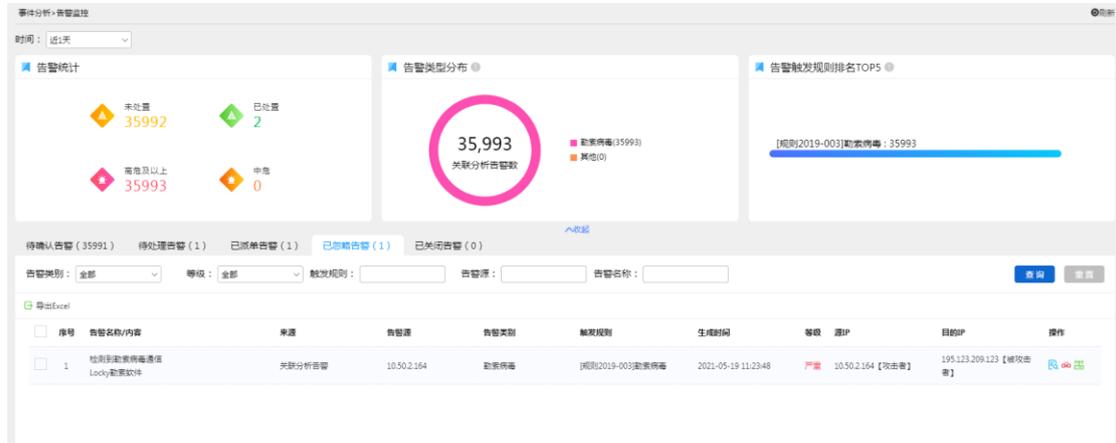
左边勾选框勾选多项，点击【加入黑名单】，可以批量对告警中的源 IP 或目的

## IP 加入黑名单。 点击操作中的【查看】

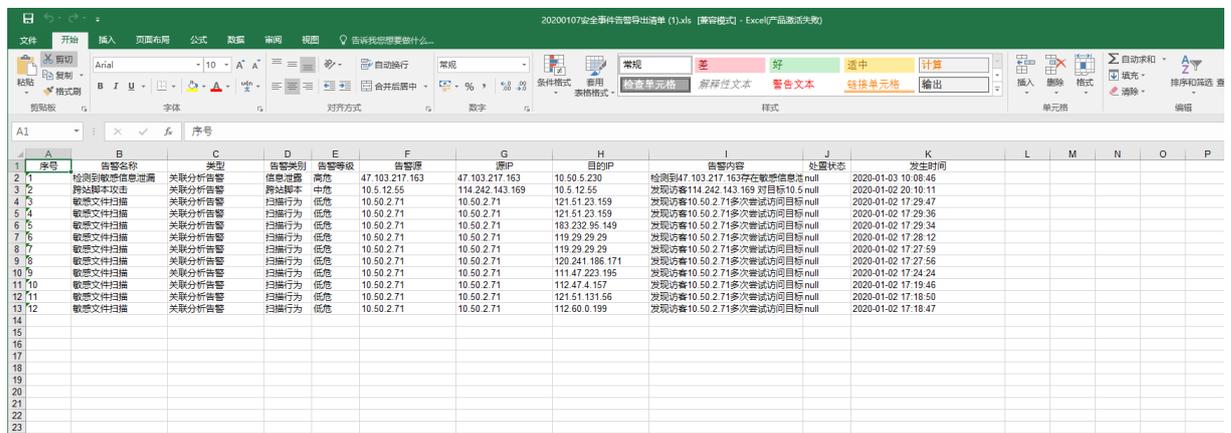


点击操作中的【加入黑名单】，可以对告警中的源 IP 或目的 IP 加入黑名单。  
点击操作中的【一键断网】，可以对 IP 进行封堵。  
点击操作中的【恢复断网】，可以对 IP 进行解封。

## 4、已忽略告警



点击【导出 excel】，导出页面如下



点击操作中的【查看】

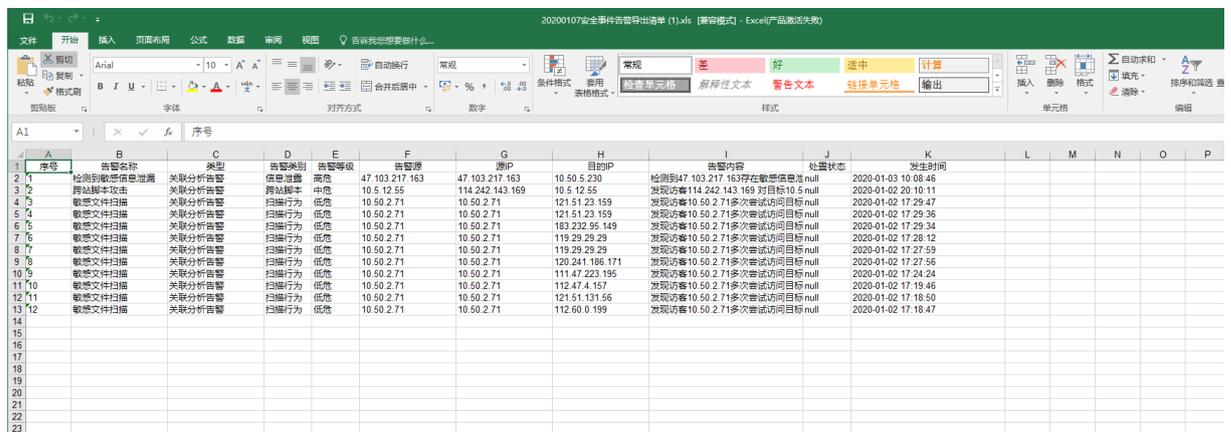


点击操作中的【一键断网】，可以对 IP 进行封堵。  
点击操作中的【恢复断网】，可以对 IP 进行解封。

### 5、已关闭告警



点击【导出 excel】，导出页面如下



左边勾选框勾选多项，点击【加入黑名单】，可以批量对告警中的源 IP 或目的 IP 加入黑名单。

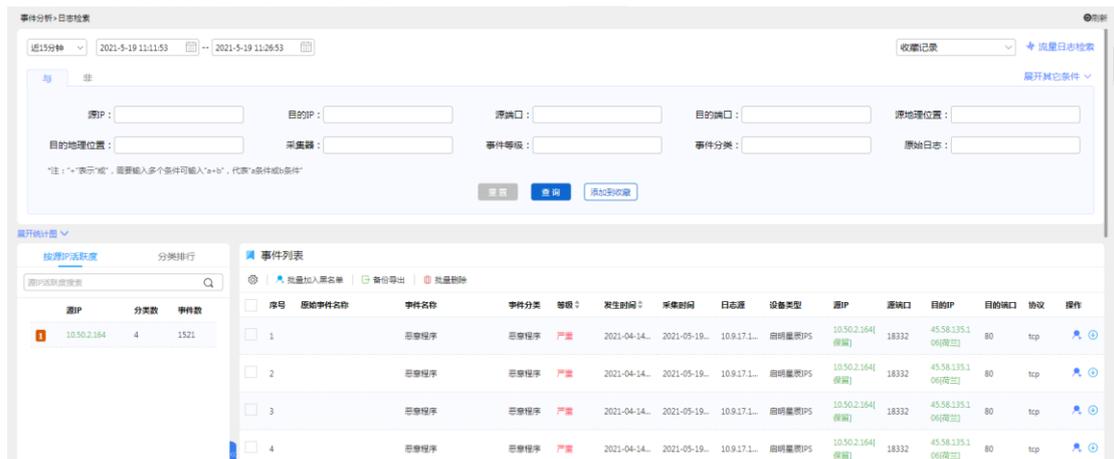
## 点击操作中的【查看】



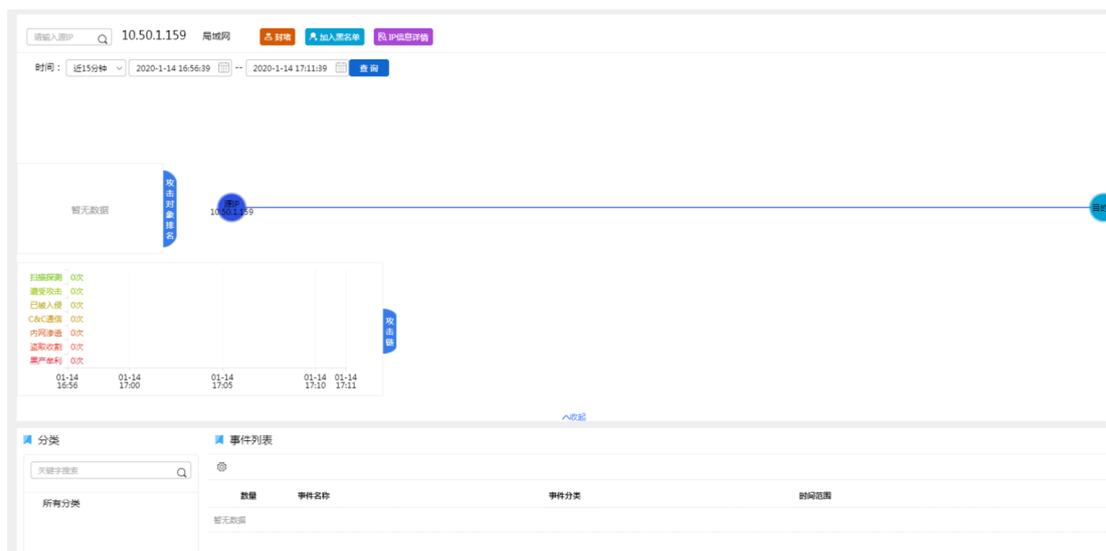
点击操作中的【加入黑名单】，可以对告警中的源 IP 或目的 IP 加入黑名单。  
点击操作中的【一键断网】，可以对 IP 进行封堵。  
点击操作中的【恢复断网】，可以对 IP 进行解封。

## 2.4.2 日志检索

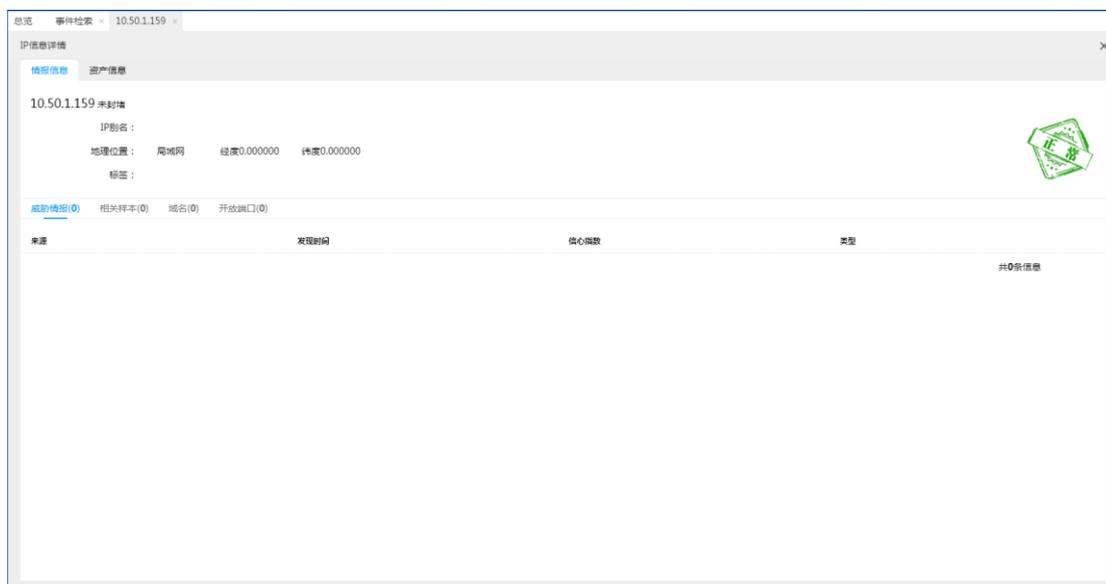
路径：事件分析->日志检索。



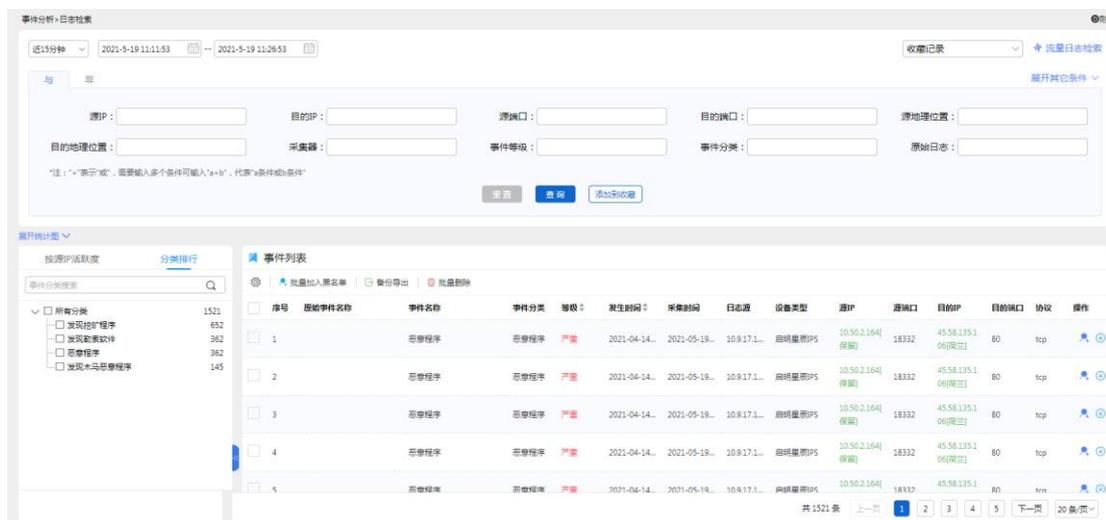
点击源 Ip, 跳至 Ip 画像



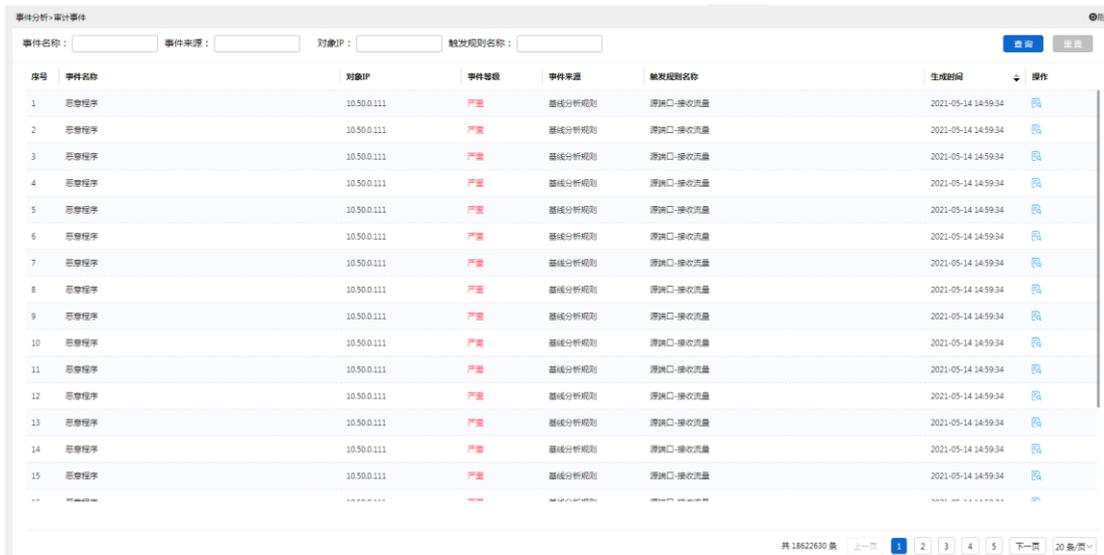
点击【ip 信息详情】，进入 ip 信息详情页面



点击“分类排行”，可勾选分类检索筛选安全事件

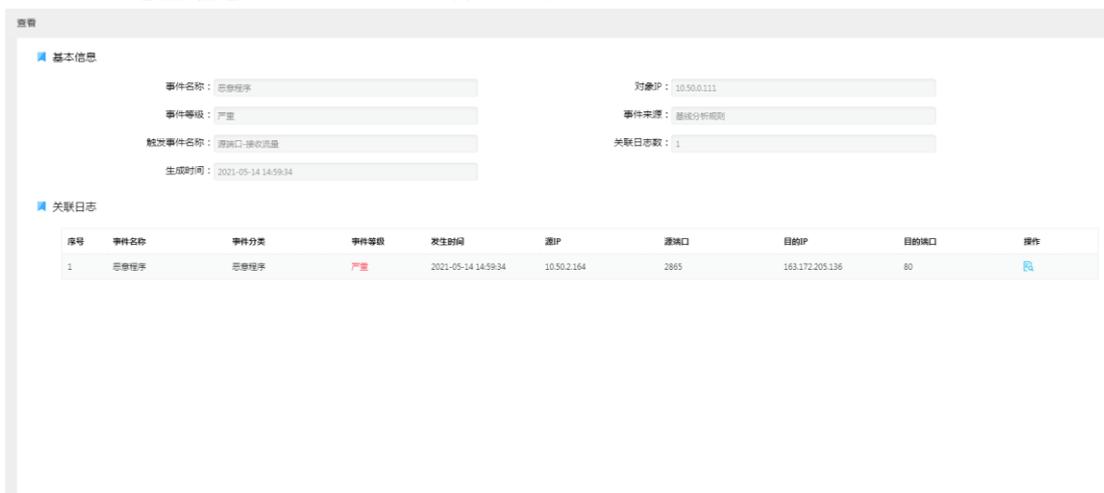






通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【查看】，跳至审计事件详情页面。



点击【查看】，跳至日志详情页面。



## 2.4.4 关联事件

路径：事件分析->关联事件。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【查看】，跳至关联事件详情页面。



点击【查看】，跳至日志详情页面。

查看  
日志详情

**基本属性**

事件名称: 恶意程序	事件等级: 严重
事件分类: 恶意程序	设备类型: 逐步在线威胁检测平台
发生时间: 2021-05-14 14:59:34	采集时间: 2021-05-14 15:00:12
日志源(设备IP): 10.50.0.111	日志源(设备名称): 10.50.0.111
采集器: Collector_127.0.0.1_1	攻击链阶段: 遭受攻击
原始事件类型:	原始规则名称: lujia
操作及响应动作:	操作结果:
准确度: 5	

**网络属性**

源IP: 10.50.2.164	源端口: 2885
目的IP: 163.172.205.136	目的端口: 80
源ip地理位置: [country=德国, province=, city=, longitude=0.000000, latitude=0.000000]	目的ip地理位置: [country=德国, province=, city=巴黎, longitude=2.213749, latitude=46.227638]
源主机名:	目的主机名:
源IP标签:	目的IP标签:
发送字节数: 823	接受字节数: 448
协议: tcp	用户:

关闭

## 2.5 报表管理

### 2.5.1 安全报告

路径：报表管理->安全报告。

威胁分析报告	综合日报	综合周报	综合月报
分析内部资产遭受到的外部威胁情况，以及防护状态。	每日安全状况摘要报告，展示资产状况、攻击事件以及处置情况等内容。	每周安全状况摘要报告，展示资产状况、攻击事件以及处置情况等内容。	每月安全状况摘要报告，展示资产状况、攻击事件以及处置情况等内容。

更多报告  
敬请期待

选择威胁分析报告

### 威胁分析报告

时间范围： 近1天  近1周  近1个月  自定义 查询 重置

被攻击服务器排名： TOP10  TOP50  TOP100

攻击者排名： TOP10  TOP50  TOP100

攻击地区排名： TOP10  TOP50  TOP100

攻击手段列表： TOP10  TOP50  TOP100

[导出报告](#) [历史下载](#)

#### 一、攻击防护总览

在报告期间，共有来自于1个地区的1个攻击者，对您的网络发起过10573次攻击。

10573次 攻击总数	0次 已处置
1个 攻击者	1个 攻击源地区

### 选择综合日报

### 综合日报

时间范围： 今天  昨天  自定义 查询 重置

失陷主机： TOP10  TOP50  TOP100

今日新增漏洞： TOP10  TOP50  TOP100

今日新增威胁： TOP10  TOP50  TOP100

[导出报告](#) [历史下载](#)

#### 一、今日安全概览

今日您的网络整体安全评级为 **良**。主要存在以下不安全条目：已失陷主机1个，高危主机9个，中危主机19个。



其中，各业务系统的失陷主机概况如下：

业务系统	失陷主机	事件总数
------	------	------

### 选择综合周报

### 综合周报

时间范围： 本周  上周  自定义 查询 重置

本周新增漏洞： TOP10  TOP50  TOP100

本周新增威胁： TOP10  TOP50  TOP100

[导出报告](#) [历史下载](#)

#### 一、本周安全概览

本周您的网络整体安全评级为 **良**。主要存在以下不安全条目：已失陷主机1个，高危主机9个，中危主机19个。



其中，各业务系统的失陷主机概况如下：

业务系统	失陷主机	事件总数
海航门户网站0302	0	0

### 选择综合月报

## 综合月报

时间范围： 本月  上月  自定义 查询 重置

本月新增漏洞： TOP10  TOP50  TOP100

本月新增威胁： TOP10  TOP50  TOP100

导出报告 历史下载

### 一、本月安全概览

本月您的网络整体安全评级为 **差**。主要存在以下不安全条目：已失陷主机0个，高危主机2个，中危主机0个。



## 2.5.2 统计报表

路径：报表管理->统计报表。

通过填写相关查询条件，点击【查询】，出现相关查询结果。

选择资产分布统计报表

统计报表类型

- 资产报表
  - 资产分布统计
- 告警报表
  - 告警分布统计
  - 告警产生趋势
  - 告警Top10排行
- 日志统计报表
  - 日志告警统计报表
  - 日志类型统计报表
  - 日志设备来源统计报表
  - 日志等级统计报表
  - 日志发生总数统计报表
  - 日志发生来源统计报表
- 事件统计报表
  - 事件事件分布统计
  - 事件事件产生趋势统计
  - 关联事件分布统计
  - 关联事件产生趋势统计

时间范围：近7天

导出Word | 下载历史

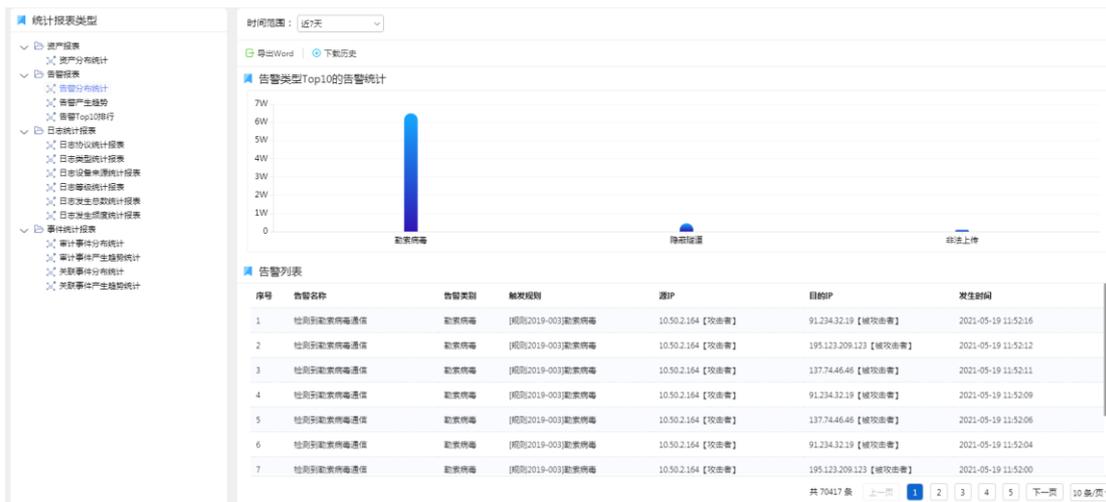
设备类型Top10的资产统计

暂无数据

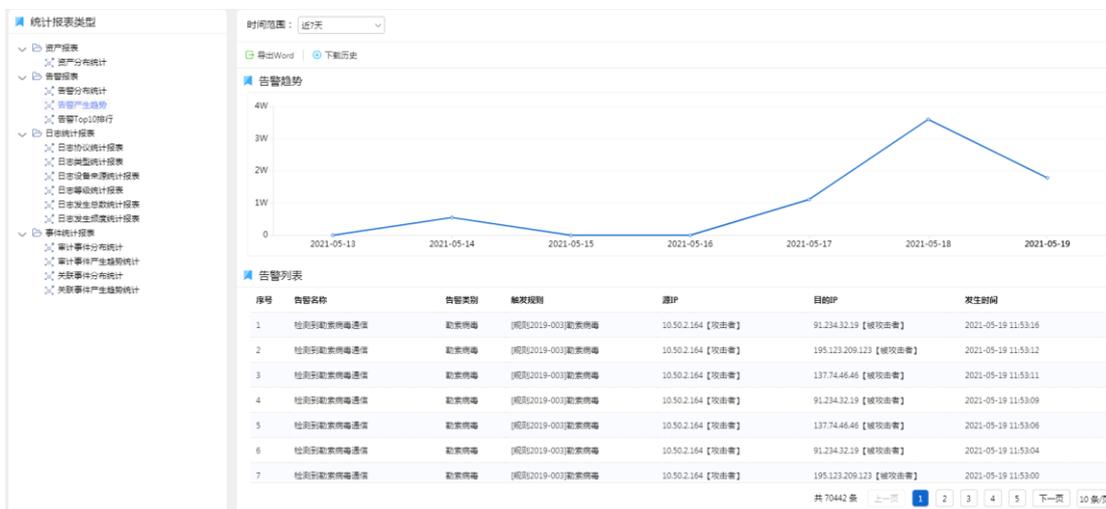
资产列表

序号	资产名称	[IP]域名[URL]	设备类型	所属业务	入库时间
暂无数据					

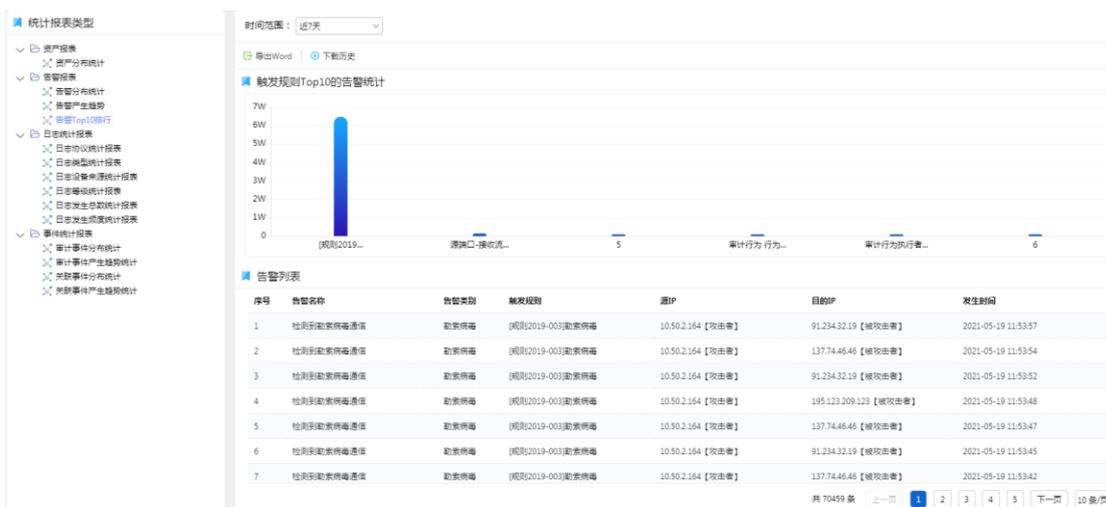
选择告警分布统计报表



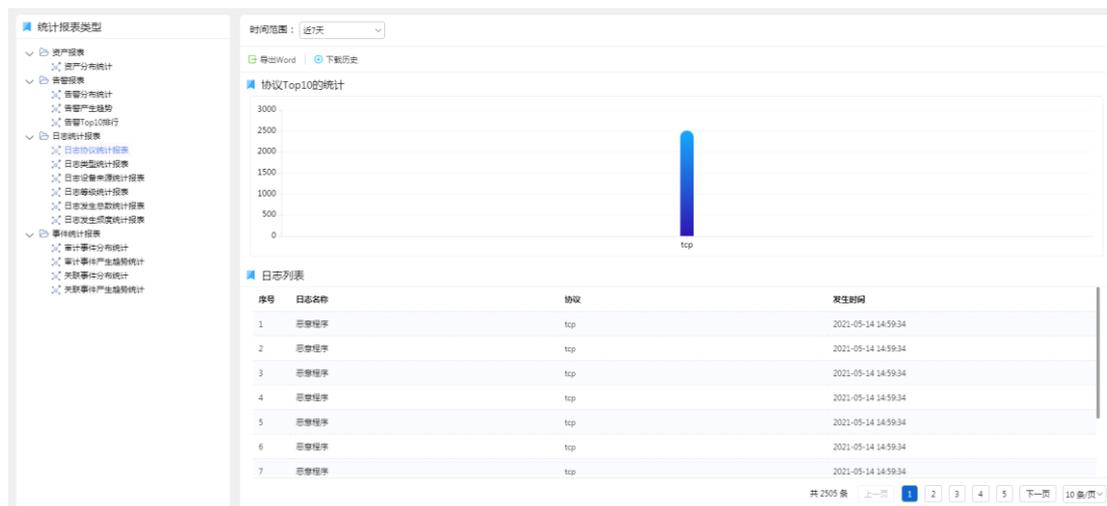
### 选择告警产生趋势报表



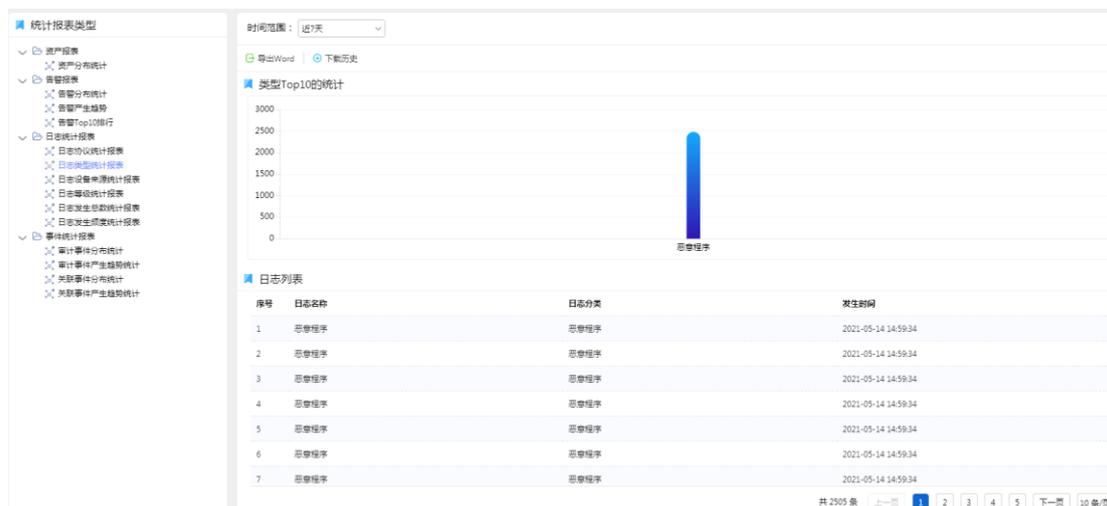
### 选择告警 TOP10 排行报表



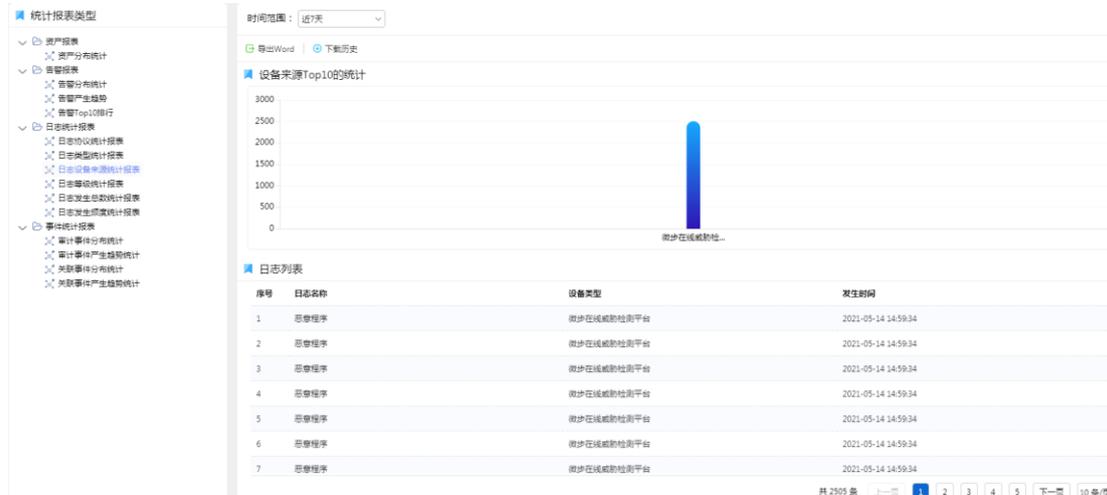
### 选择日志协议统计报表



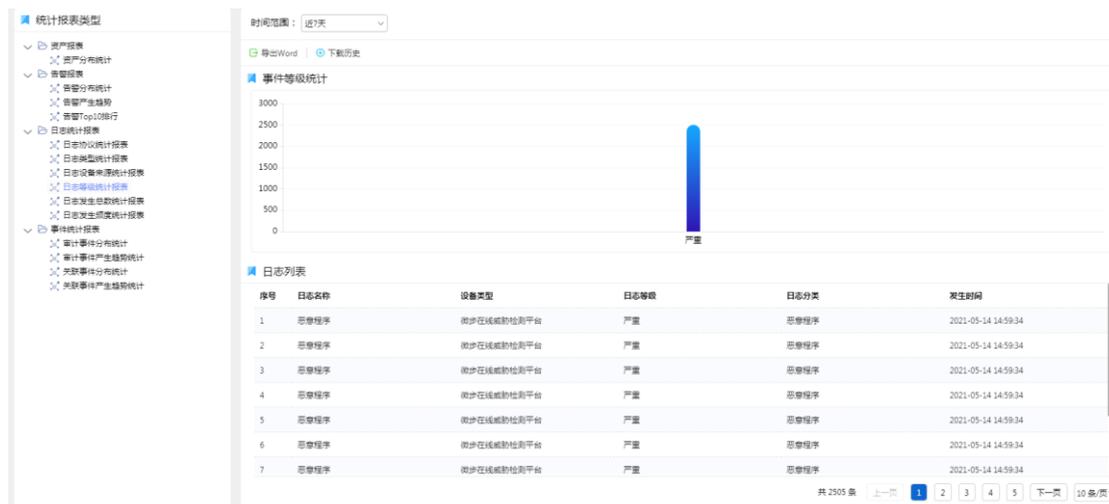
### 选择日志类型统计报表



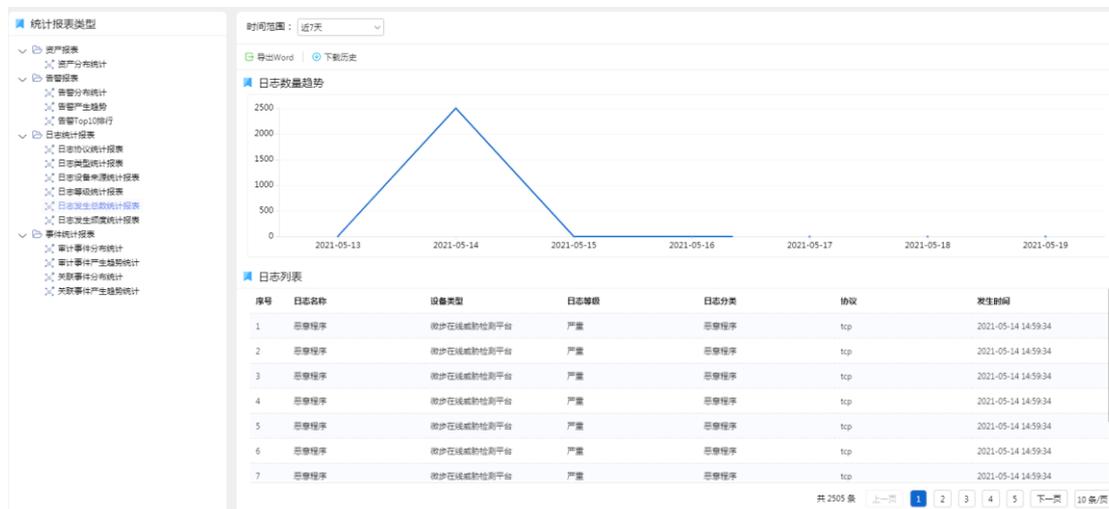
### 选择日志设备来源统计报表



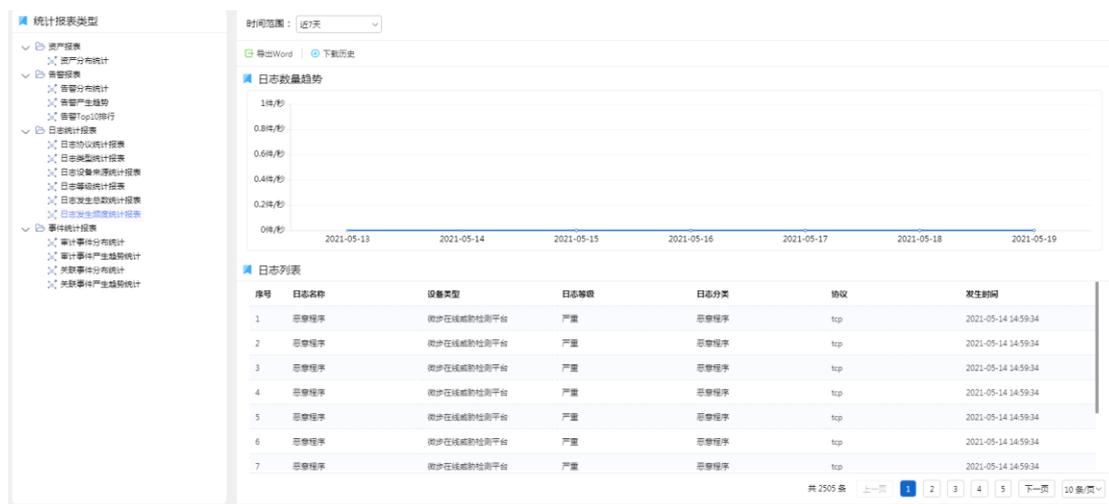
### 选择日志等级统计报表



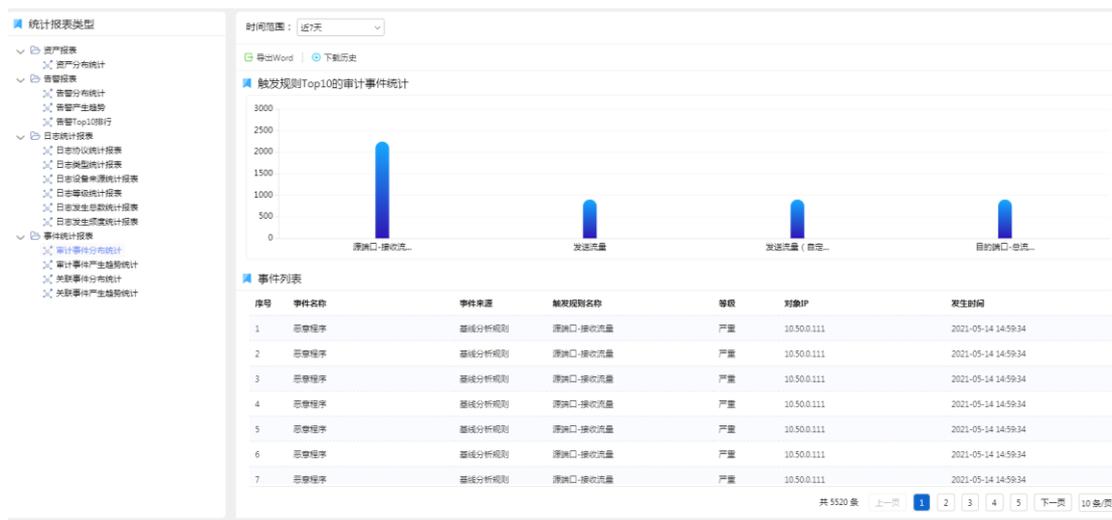
选择日志发生总数统计报表



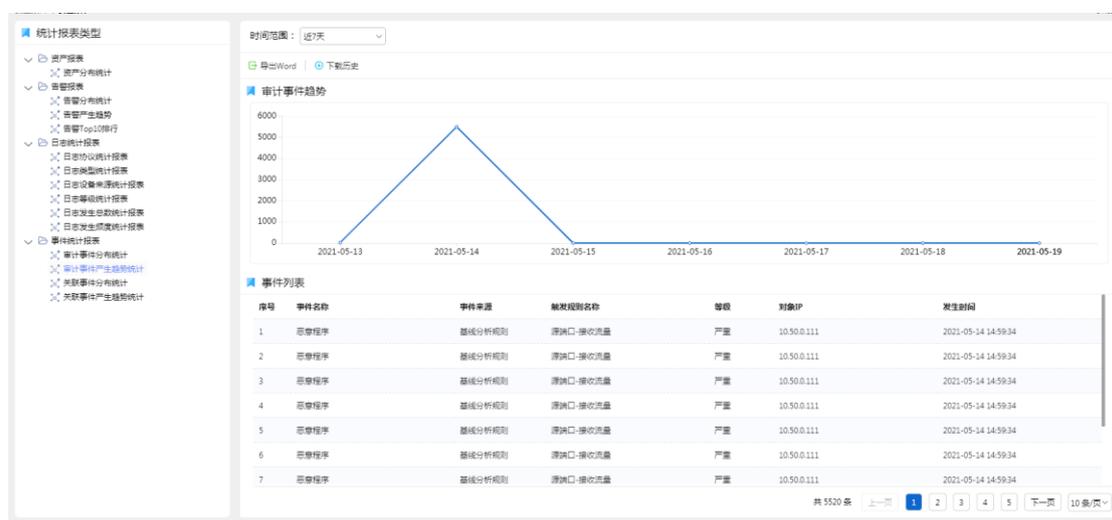
选择日志发生频度统计报表



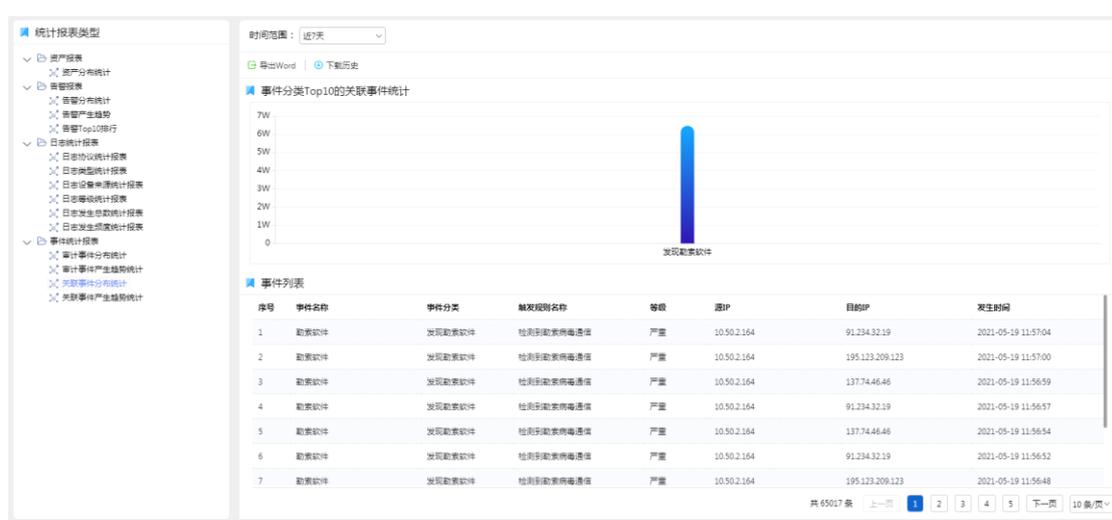
### 选择审计事件分布统计报表



### 选择审计事件产生趋势统计报表



### 选择关联事件分布统计报表



### 选择关联事件产生趋势统计报表



点击【导出 excel】，可导出列表内容。  
点击【下载历史】，进入历史下载页面。

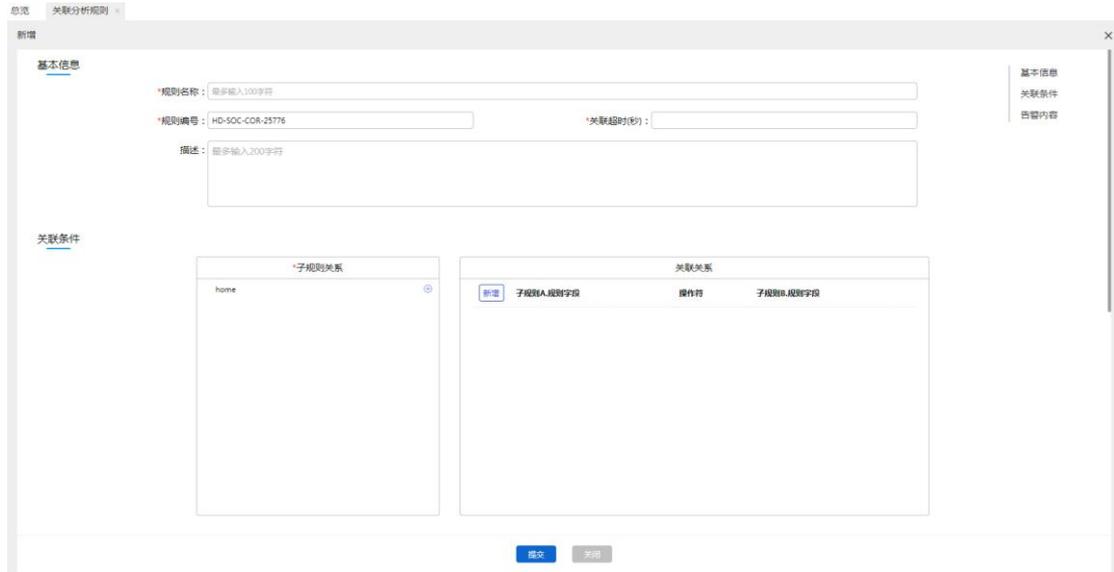
## 2.6 策略管理

### 2.6.1 关联分析规则

路径：策略管理->关联分析规则。

序号	规则编号	规则名称	告警等级	风险级别	状态	创建时间	操作
1	HD-SOC-COR-00096	SQL报障信息告漏	高危	存在漏洞	启用	2021-03-31 11:05:10	编辑 删除
2	HD-SOC-COR-00095	teamviewer	低危	被收集信息	启用	2021-03-31 11:05:10	编辑 删除
3	HD-SOC-COR-00094	[规则2019-070]输出敏感信息	中危	被收集信息	启用	2021-03-12 17:11:30	编辑 删除
4	HD-SOC-COR-00093	[规则2019-069]gp+静音视频	严重	植入木马 (失败)	启用	2021-03-12 17:11:30	编辑 删除
5	HD-SOC-COR-00092	[规则2019-035]存在Jboss反序列化漏洞，/JbossMQ组件成功访问	严重	存在漏洞	启用	2021-03-12 17:11:30	编辑 删除
6	HD-SOC-COR-00091	[规则2019-034]深信服终端攻击-短信端口滥用	中危	被攻击 (不确定)	启用	2021-03-12 17:11:30	编辑 删除
7	HD-SOC-COR-00090	[规则2019-068]Web编辑器恶意脚本上传操作	高危	被攻击 (不确定)	启用	2021-03-12 17:11:30	编辑 删除
8	HD-SOC-COR-00089	[规则2019-033]PH-PCMS2008代码注入漏洞攻击 ( CVE-2018-19127 )	中危	被攻击 (不确定)	启用	2021-03-12 17:11:30	编辑 删除
9	HD-SOC-COR-00088	[规则2019-032]Apache Spark RPC协议Jwa反序列化漏洞攻击(CVE-2018-17190)	中危	被攻击 (不确定)	启用	2021-03-12 17:11:30	编辑 删除
10	HD-SOC-COR-00087	[规则2019-067]业务接口api接口异常调用	中危	被攻击 (成功)	启用	2021-03-12 17:11:30	编辑 删除

点击【新增】，进入新增规则页面



填写相关信息，点击提交，新增规则完成。

左边勾选框勾选多项，点击【批量删除】，可以批量删除选中规则。

左边勾选框勾选多项，点击【批量启用】，可以批量启用选中规则。

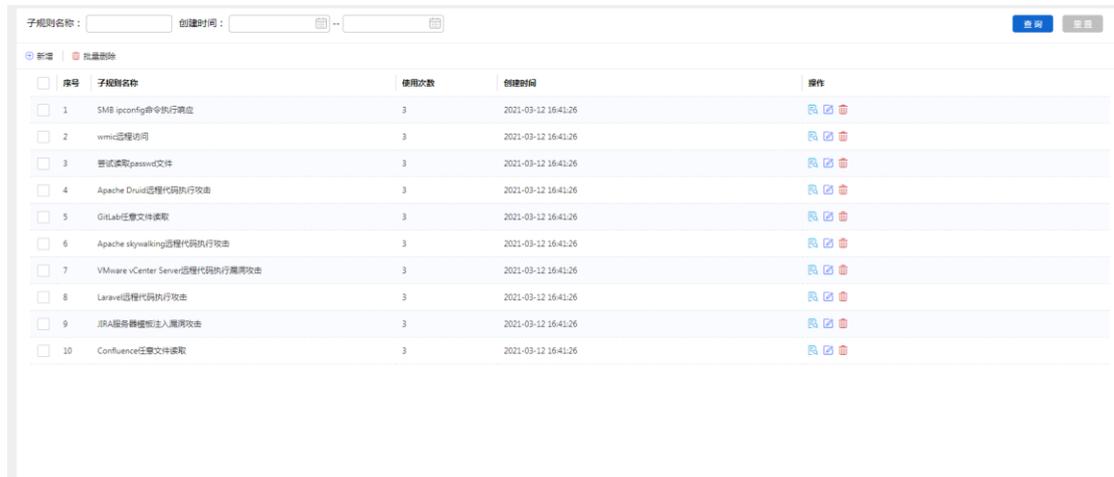
左边勾选框勾选多项，点击【批量禁用】，可以批量禁用选中规则。

左边勾选框勾选多项，点击【批量导出】，可以批量导出选中规则。

点击【全部导出】，可以导出全部规则。

点击【批量导入】，可导入规则。

点击“子规则”，进入子规则页面



点击操作中的【查看】，可查看规则。

点击操作中的【编辑】，可进行编辑。

点击操作中的【删除】，可删除规则。

点击操作中的【禁用】，禁用规则。

点击操作中的【启用】，启用规则。

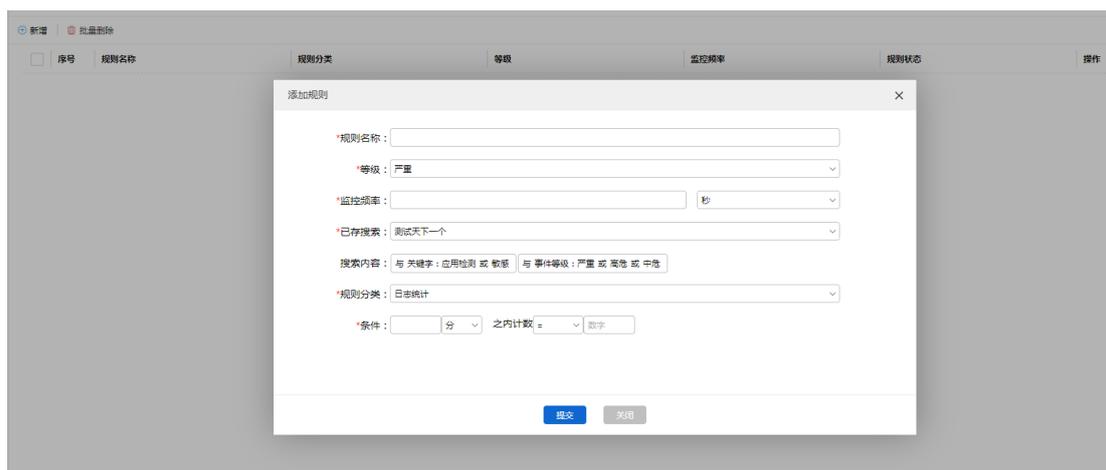
## 2.6.2 统计分析规则

路径：策略管理->统计分析规则。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【新增】，进入添加规则页面



填写相关信息，点击【提交】，添加统计分析规则完成。

左边勾选框勾选多项，点击【批量删除】，可以批量删除规则。

点击操作中的【查看】，进入查看规则页面。

点击操作中的【编辑】，进入编辑页面。

点击操作中的【禁用】，禁用规则。

点击操作中的【启用】，启用规则。

点击操作中的【删除】，删除规则。

### 2.6.3 审计分析规则

路径：策略管理->审计分析规则。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【新增】，进入新增规则页面

新增

规则编号: SIFXGZ-20210519-11038 \*规则名称:

\*过滤内容: **审计目标** 审计行为 审计行为执行者 审计行为来源 审计有效时间段 其它条件

属于  不属于

审计目标类型:  \*审计目标值:

合并条件: 1~86400 秒内发生 1 次

响应方式:  产生告警

\*警告标题:

\*警告等级:  \*警告类别: 请选择警告类型

风险阶段: 无  警告源: 源IP

警告显示:

原理:

填写相关信息，点击提交，新增规则完成。

左边勾选框勾选多项，点击【批量删除】，可以批量删除选中规则。

左边勾选框勾选多项，点击【批量启用】，可以批量启用选中规则。

左边勾选框勾选多项，点击【批量禁用】，可以批量禁用选中规则。

左边勾选框勾选多项，点击【批量导出】，可以批量导出选中规则。

点击【批量导入】，可导入规则。

点击【调整规则处理顺序】，进入调整规则处理顺序页面

调整策略顺序

<input type="checkbox"/>	17	SIFXGZ-20210331-83076	设备类型不属于	17
<input type="checkbox"/>	18	SIFXGZ-20210331-36075	审计行为的警告-不属于	18
<input type="checkbox"/>	19	SIFXGZ-20210331-22742	ip地址的警告-属于	19
<input type="checkbox"/>	20	SIFXGZ-20210331-60379	审计行为执行者的警告-不属于	20

点击操作中的【查看】，可查看规则。

点击操作中的【编辑】，可进行编辑。

点击操作中的【删除】，可删除规则。

点击操作中的【禁用】，禁用规则。

点击操作中的【启用】，启用规则。

## 2.6.4 基线分析规则

路径：策略管理->基线分析规则。

规则名称:  规则描述:  状态: 全部 创建时间:  更新时间:  查询 重置

新增 | 
  批量删除 | 
  批量启用 | 
  批量禁用 | 
  批量导入 | 
  批量导出

<input type="checkbox"/>	序号	规则编号	规则名称	规则描述	状态	创建时间	更新时间	操作
<input type="checkbox"/>	11	JKFKGZ-20210414-58705	发送流量 (自定义)		启用	2021-04-14 17:47:38	2021-04-14 17:47:38	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	12	JKFKGZ-20210414-74813	发送流量 (周)		启用	2021-04-14 17:46:33	2021-04-14 17:46:33	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	13	JKFKGZ-20210414-26035	发送流量 (禁用)		禁用	2021-04-14 17:45:48	2021-04-14 17:45:48	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input checked="" type="checkbox"/>	14	JKFKGZ-20210414-76000	发送流量		启用	2021-04-14 17:44:17	2021-04-28 11:28:54	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	15	JKFKGZ-20210414-24708	源端口-接收流量	规则描述1	启用	2021-04-14 17:41:35	2021-05-14 14:58:57	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input checked="" type="checkbox"/>	16	JKFKGZ-20210414-42657	目的端口-总流量	描述1	启用	2021-04-14 17:39:03	2021-04-28 11:28:54	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	17	JKFKGZ-20210413-56571	基础分析规则-自定义		启用	2021-04-13 17:49:30	2021-04-13 17:49:30	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>
<input checked="" type="checkbox"/>	18	JKFKGZ-20210413-56731	基础分析规则-总流量 (禁用)		禁用	2021-04-13 17:47:41	2021-04-28 11:28:54	<a href="#">查看</a> <a href="#">编辑</a> <a href="#">删除</a>

通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【新增】，进入新增规则页面

新增

规则编号: JKFKGZ-20210519-86607 \*规则名称:

\*过滤内容:

逻辑关系: && 请选择条件:  运算符:  条件值:

\*基础分析方式:

统计方式:  移动平均  移动方差
 基础类型:  日  周

学习时长: 4 日 \*触发条件: 1-99 %超过基准

统计字段:

\*等级: 严重

响应方式:  产生告警

\*告警标题:   
 \*告警等级: 严重 \*告警类别: 请选择告警类型  
 风险阶段: 无 告警源: 源IP  
 告警显示:

原理:

填写相关信息，点击提交，新增规则完成。

左边勾选框勾选多项，点击【批量删除】，可以批量删除选中规则。

左边勾选框勾选多项，点击【批量启用】，可以批量启用选中规则。

左边勾选框勾选多项，点击【批量禁用】，可以批量禁用选中规则。

左边勾选框勾选多项，点击【批量导出】，可以批量导出选中规则。

点击【批量导入】，可导入规则。

点击操作中的【查看】，可查看规则。

点击操作中的【编辑】，可进行编辑。

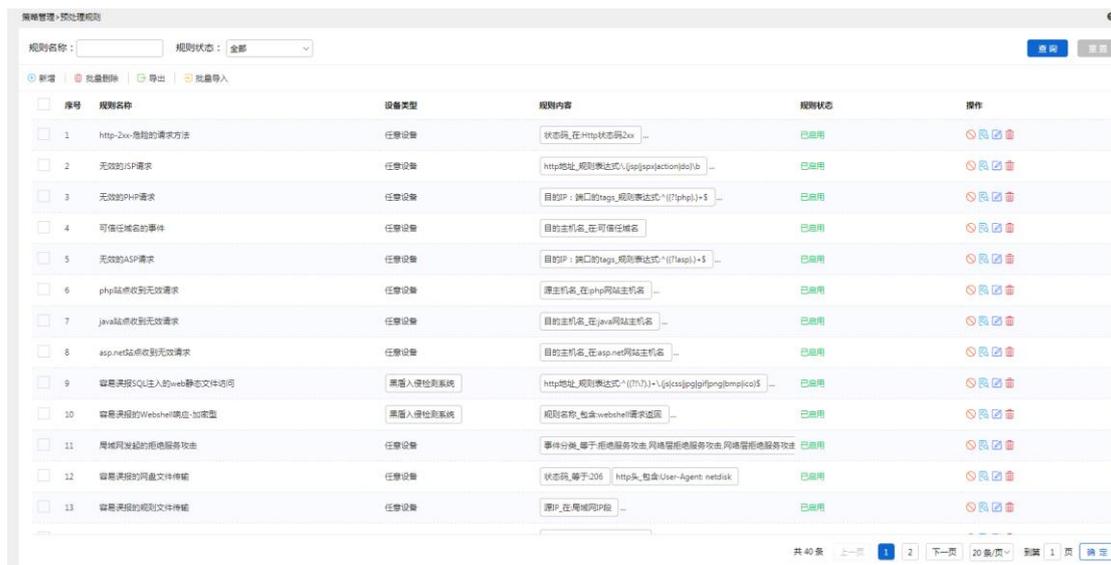
点击操作中的【删除】，可删除规则。

点击操作中的【禁用】，禁用规则。

点击操作中的【启用】，启用规则。

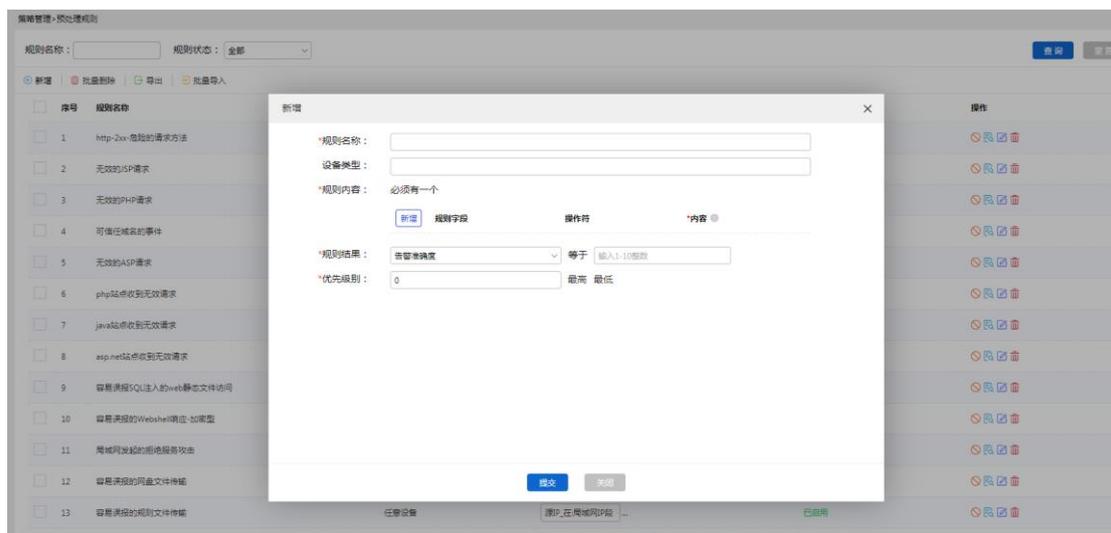
## 2.6.5 预处理规则

路径：策略管理->预处理规则。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

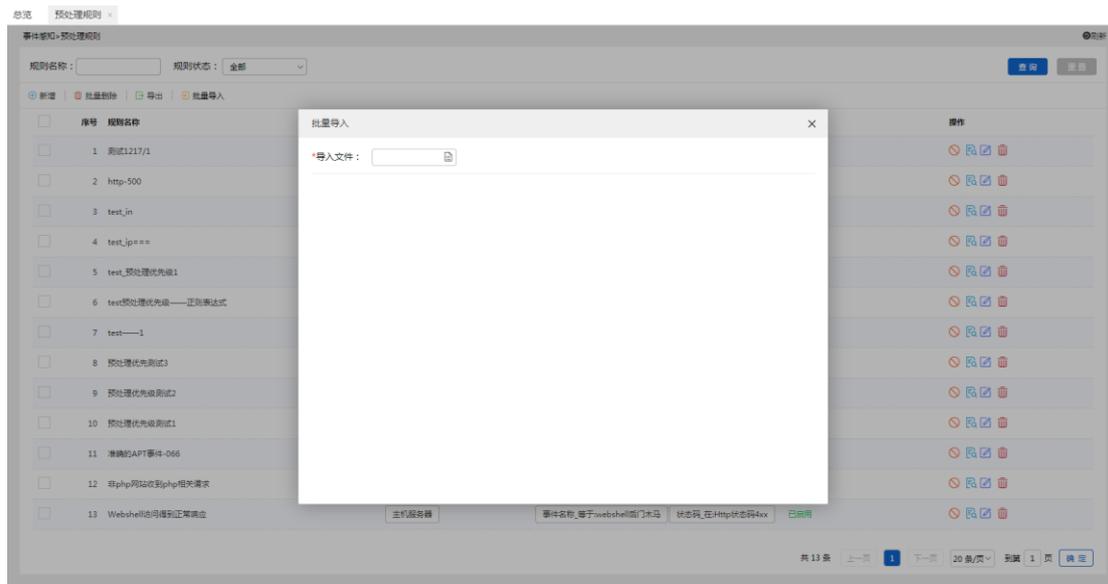
点击【新增】，进入新增页面



填写相关信息，点击【提交】，添加预处理规则完成。

左边勾选框勾选多项，点击【批量删除】，可以批量删除规则。

点击【批量导入】，进入批量导入页面



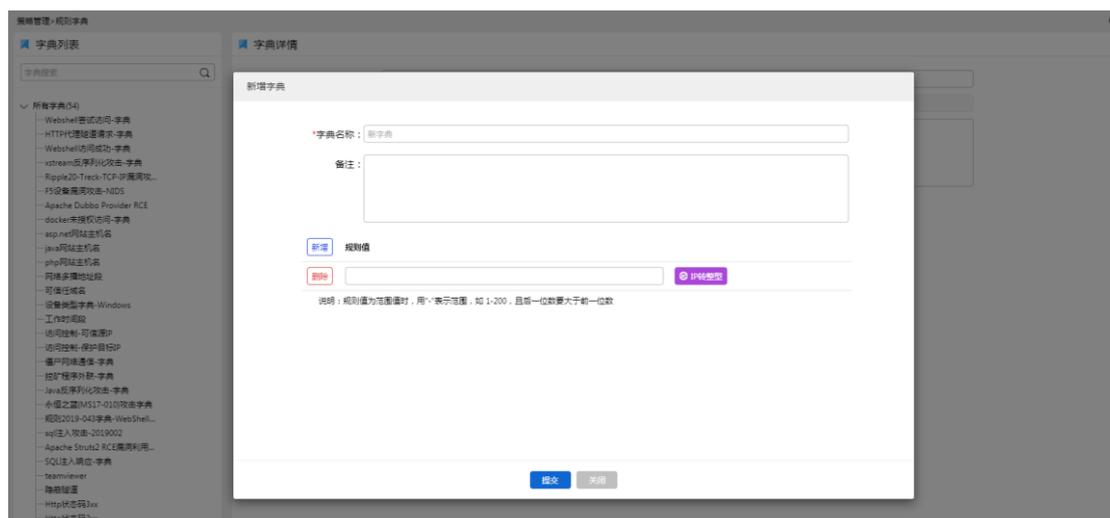
- 点击【导出】，可以导出规则。
- 点击操作中的【查看】，进入查看规则页面。
- 点击操作中的【编辑】进入编辑页面。
- 点击操作中的【禁用】，禁用规则。
- 点击操作中的【启用】，启用规则。
- 点击操作中的【删除】，删除规则。

## 2.6.6 规则字典

路径：策略管理->规则字典。



鼠标移至“所有字典”，出现【新增】，点击【新增】进入新增字典页面



填写相关信息，点击【提交】，添加字典完成。

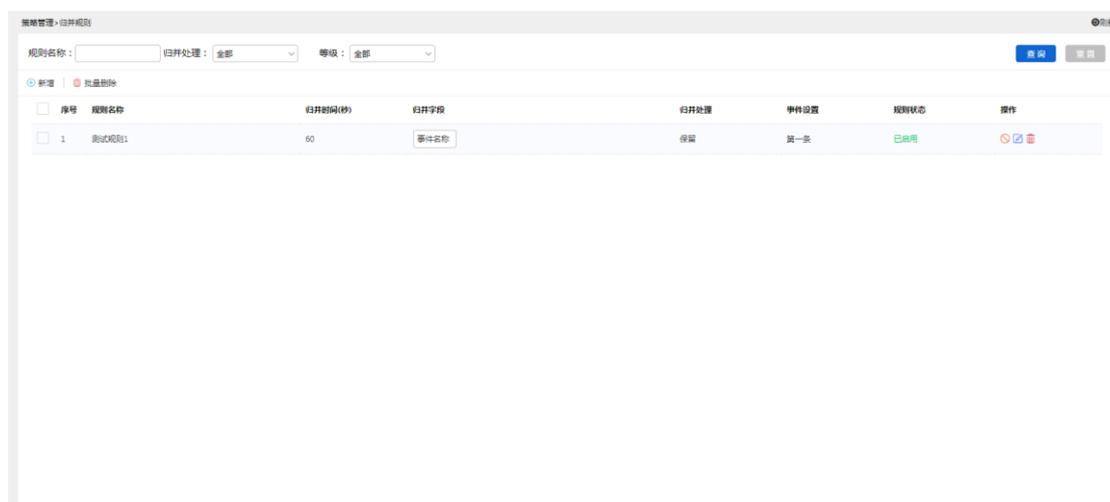
点击【编辑】，进入编辑页面。

点击字典名称，右边显示字典信息。

点击【删除】，删除字典。

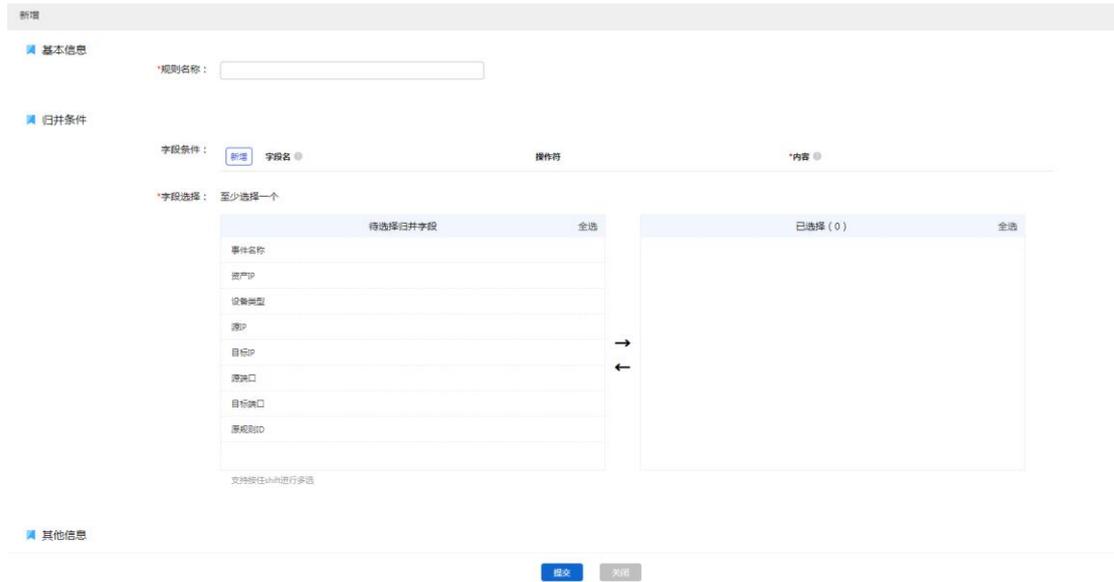
## 2.6.7 归并规则

路径：策略管理->归并规则。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

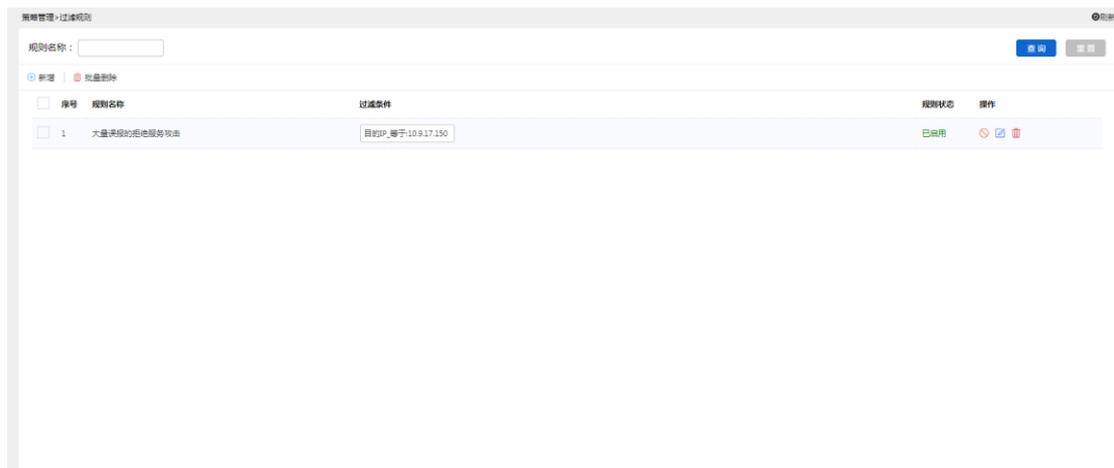
点击【新增】，进入新增页面



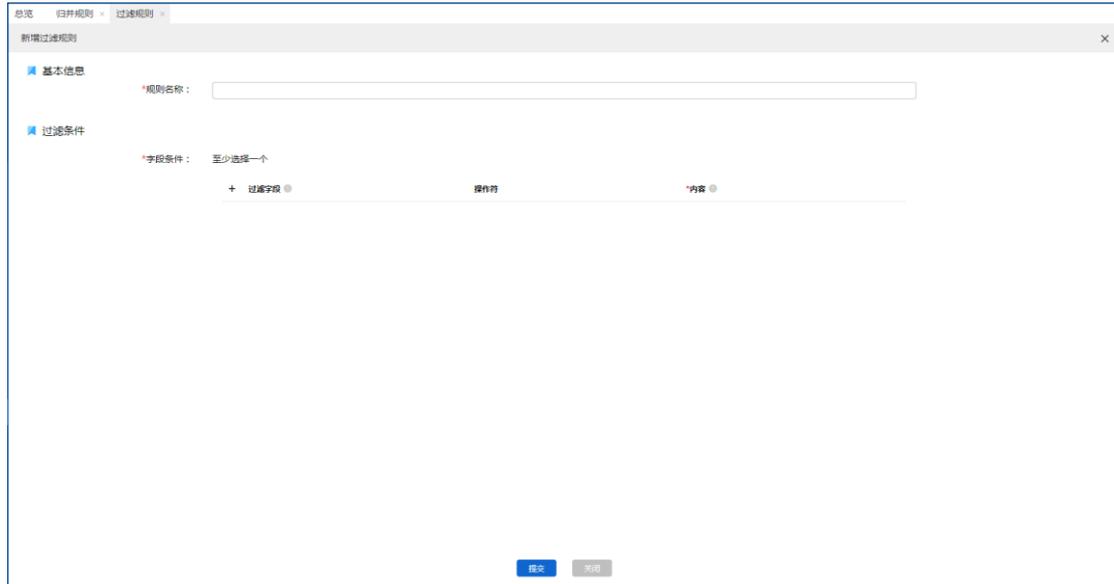
填写相关信息，点击【提交】，添加归并规则完成。  
左边勾选框勾选多项，点击【批量删除】，可以批量删除规则。  
点击操作中的【编辑】，进入编辑页面。  
点击操作中的【禁用】，禁用规则。  
点击操作中的【启用】，启用规则。  
点击操作中的【删除】，删除规则。

## 2.6.8 过滤规则

路径：策略管理->过滤规则。



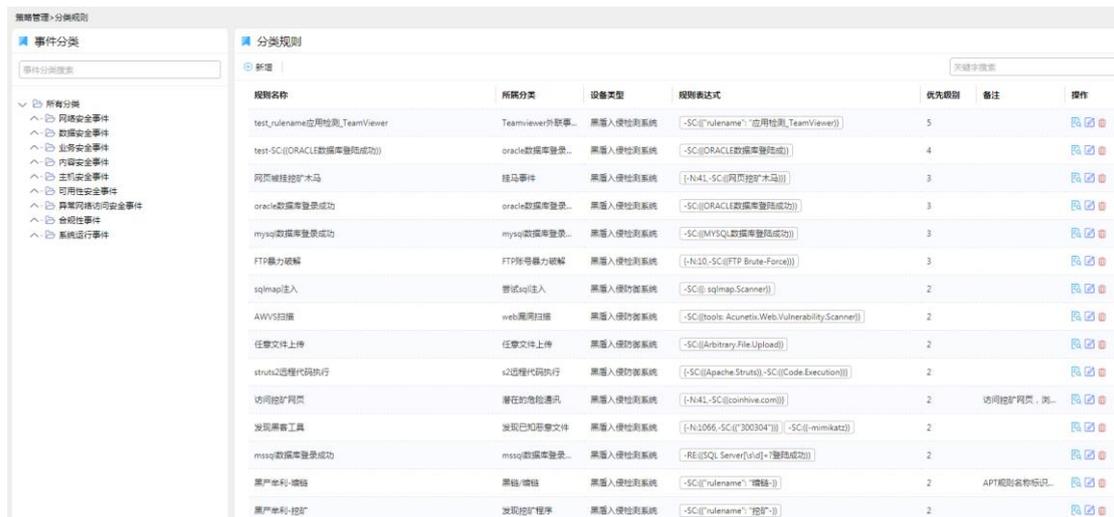
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。  
点击【新增】，进入新增页面



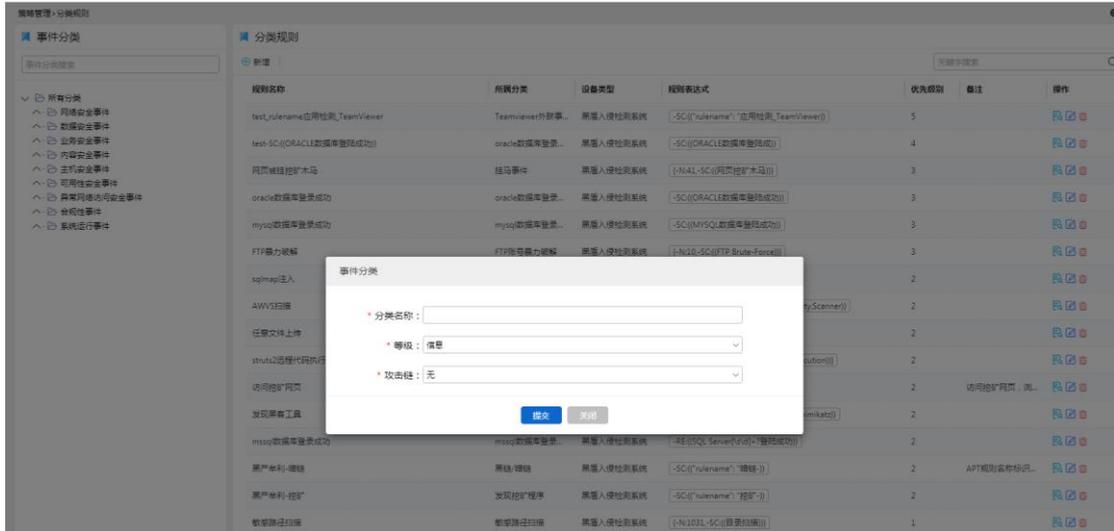
填写相关信息，点击【提交】，添加过滤规则完成。  
 左边勾选框勾选多项，点击【批量删除】，可以批量删除规则。  
 点击操作中的【编辑】，进入编辑页面。  
 点击操作中的【禁用】，禁用规则。  
 点击操作中的【启用】，启用规则。  
 点击操作中的【删除】，删除规则。

## 2.6.9 分类规则

路径：策略管理->分类规则。



鼠标移至菜单栏，出现【新增】、【编辑】、【删除】按钮，点击【新增】，跳出事件分类添加弹框



点击【编辑】，跳出事件分类编辑弹框。  
点击【删除】，可删除菜单中事件分类。  
点击分类规则中的【新增】，进入新增规则页面

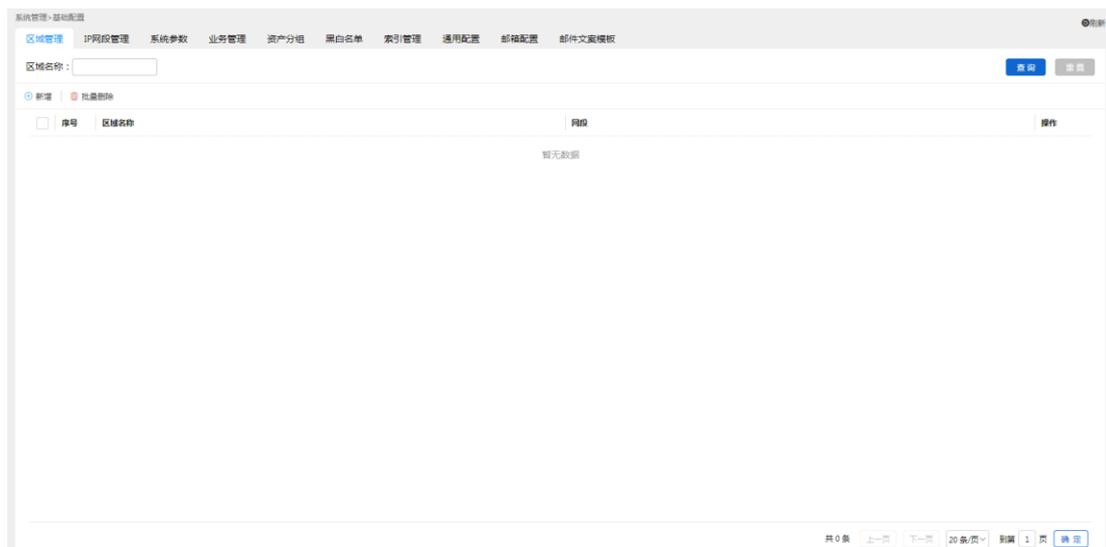


填写相关内容，点击【提交】，新增规则完成。  
点击操作中的【查看】，进入查看页面。  
点击操作中的【编辑】，进入编辑页面。  
点击操作中的【删除】，删除分类规则。

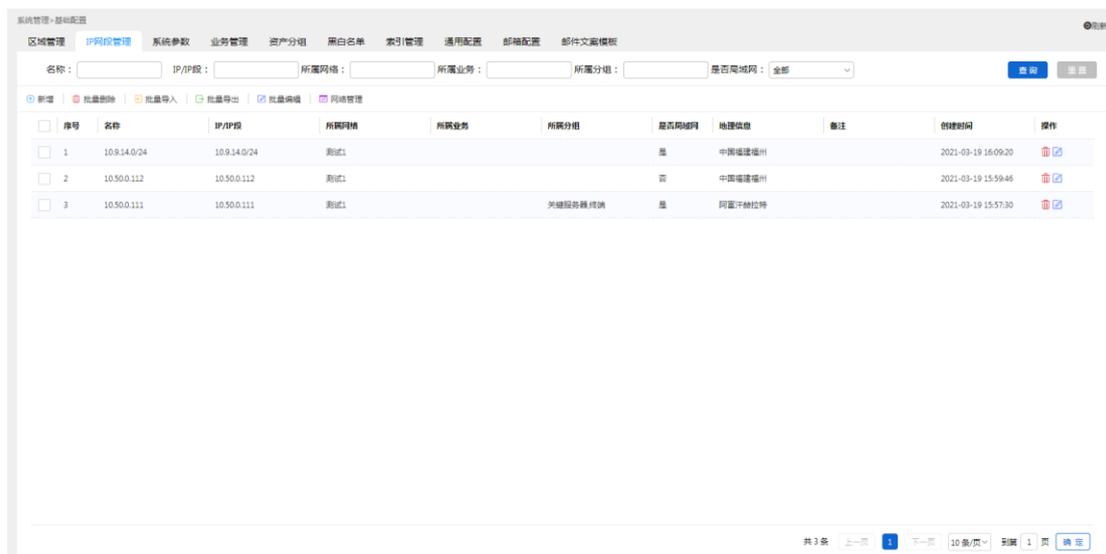
## 2.7 系统管理

### 2.7.1 基础配置

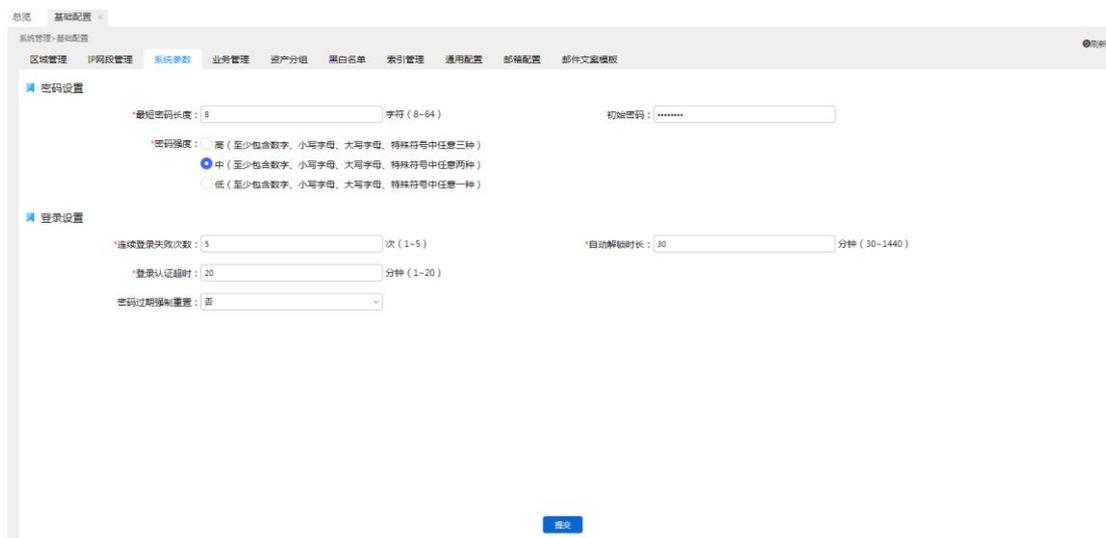
路径：系统管理->基础配置。  
基础配置中可对相关内容进行配置，点击‘区域管理’，进入区域管理页面。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行增删查改操作。  
 点击‘IP 网段管理’，进入 ip 网段管理页面。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行增删查改等操作。  
 点击‘系统参数’，进入系统参数页面。



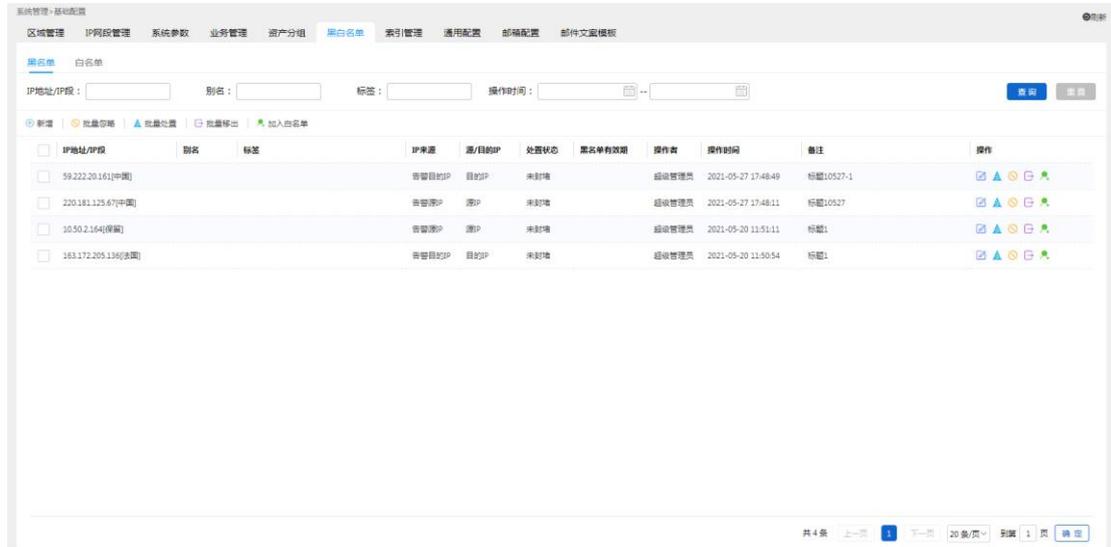
可修改系统参数，点击提交，保存信息。  
点击‘业务管理’，进入业务管理页面。



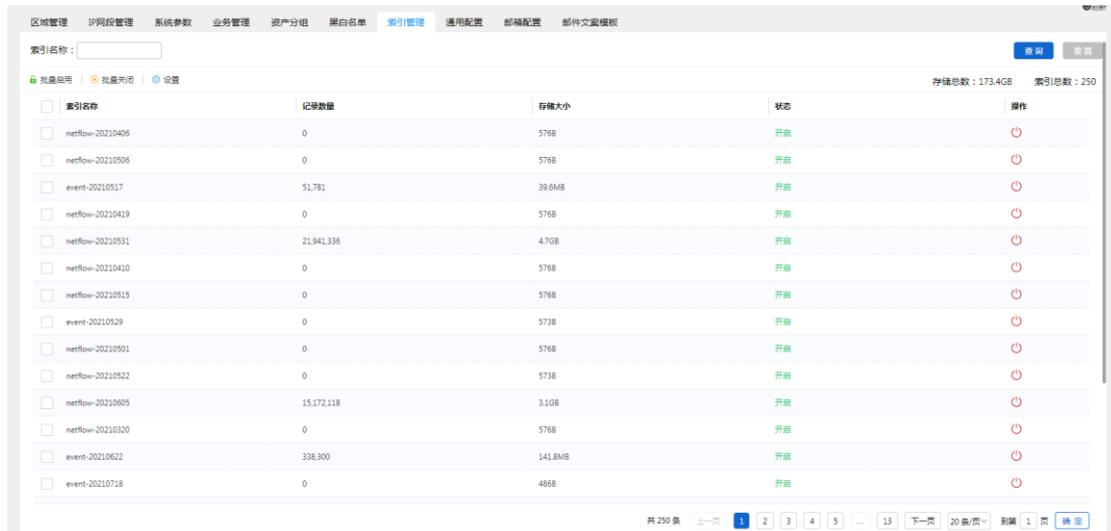
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行增删查改等操作。  
点击‘资产分组’，进入资产分组页面。



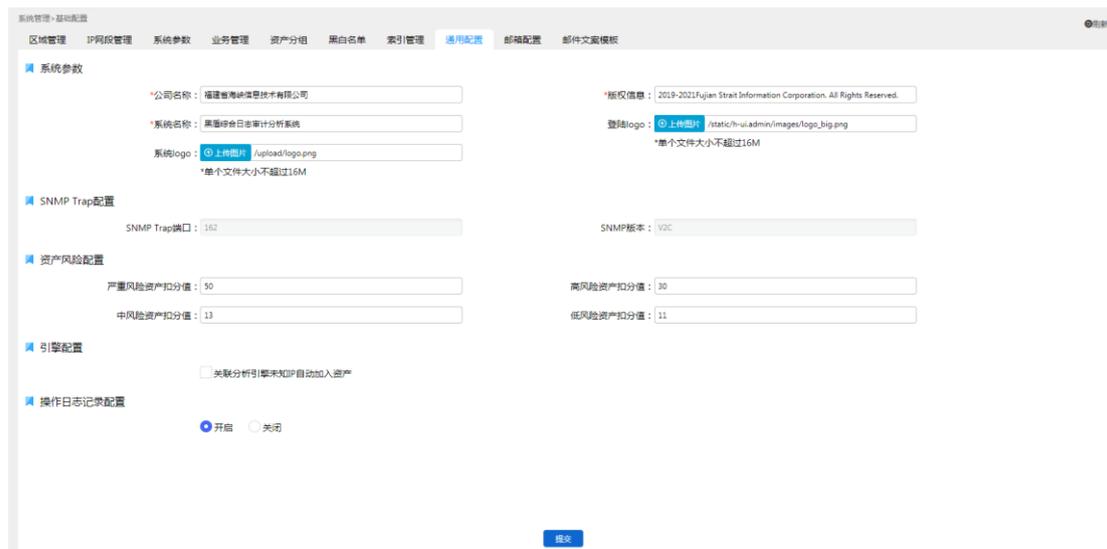
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行增删查改操作。  
点击‘黑白名单’，进入黑白名单页面。



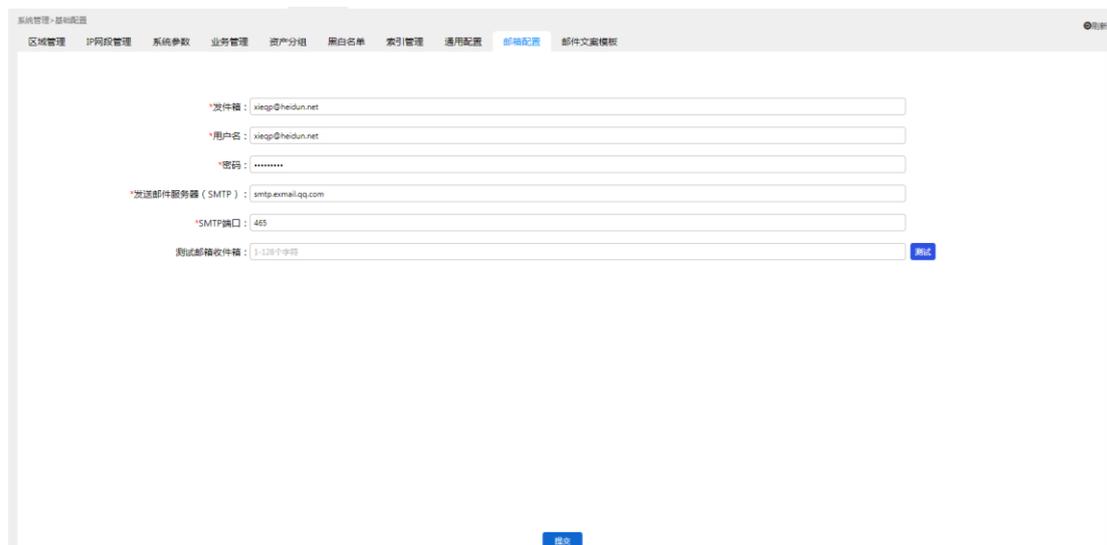
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可对列表中的 IP/IP 段进行忽略、处置、编辑等操作。  
点击‘索引管理’，进入索引管理页面。



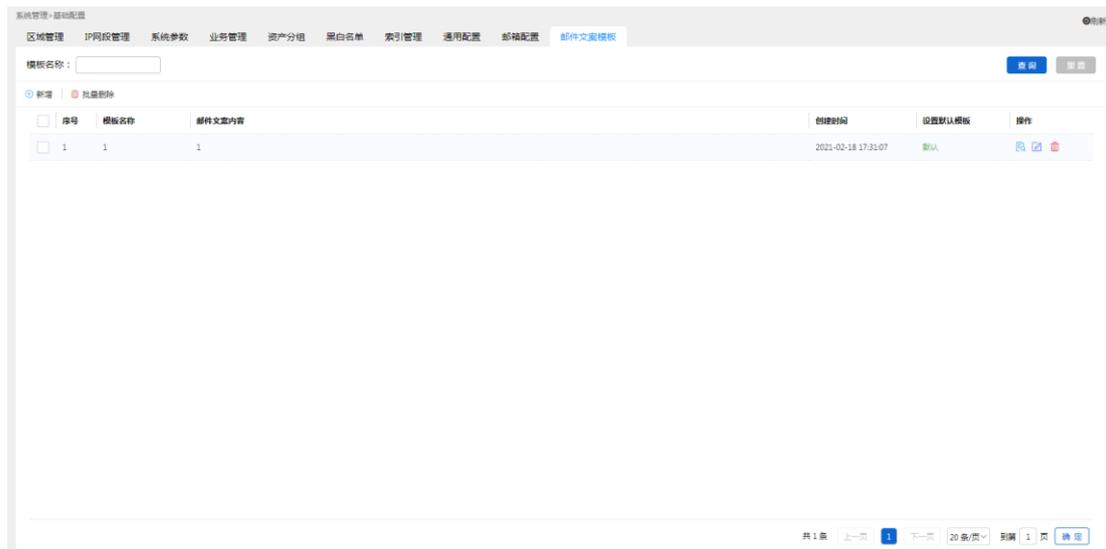
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行启用、关闭及设置操作。  
点击‘通用配置’，进入通用配置页面。



可修改通用配置，点击提交，保存信息。  
点击‘邮箱配置’，进入邮箱配置页面。



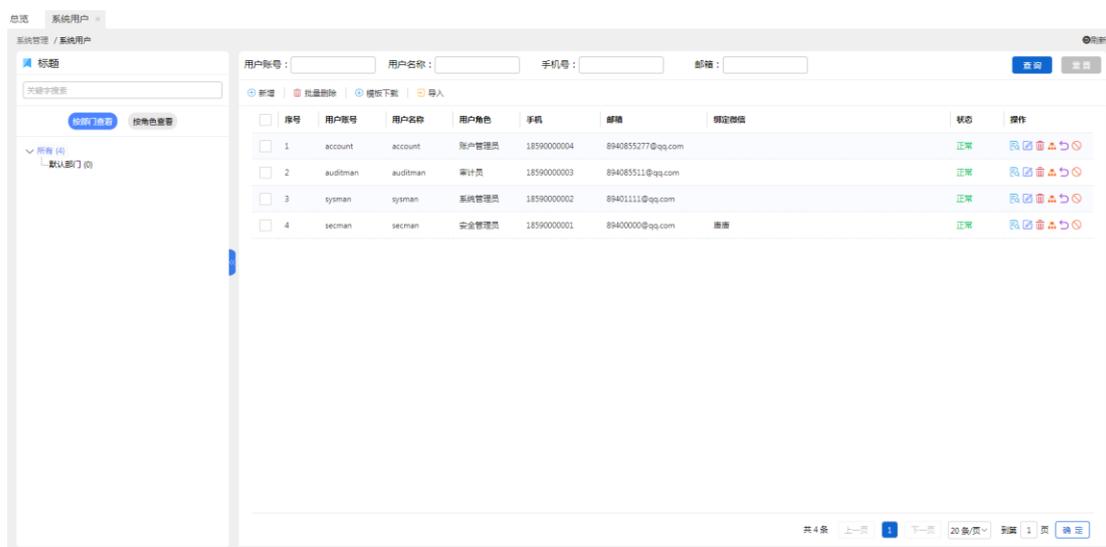
可进行邮箱配置操作。  
点击‘邮件文案模板’，进入邮件文案模板页面。



可进行邮件文案模板的增删查改。

## 2.7.2 系统用户

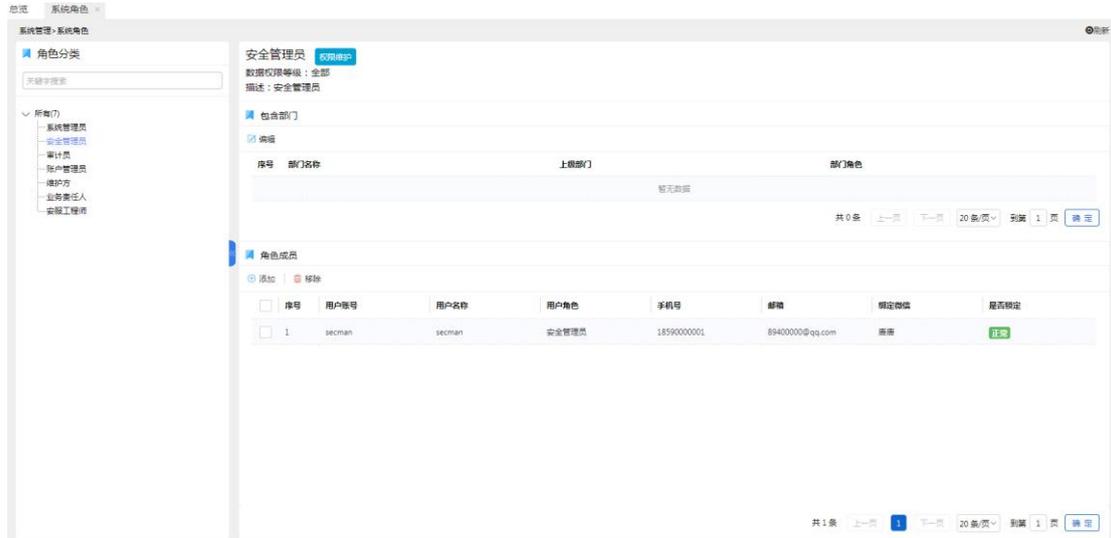
路径：系统管理->系统用户。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行系统用户的增删查改、分配权限等操作。

## 2.7.3 系统角色

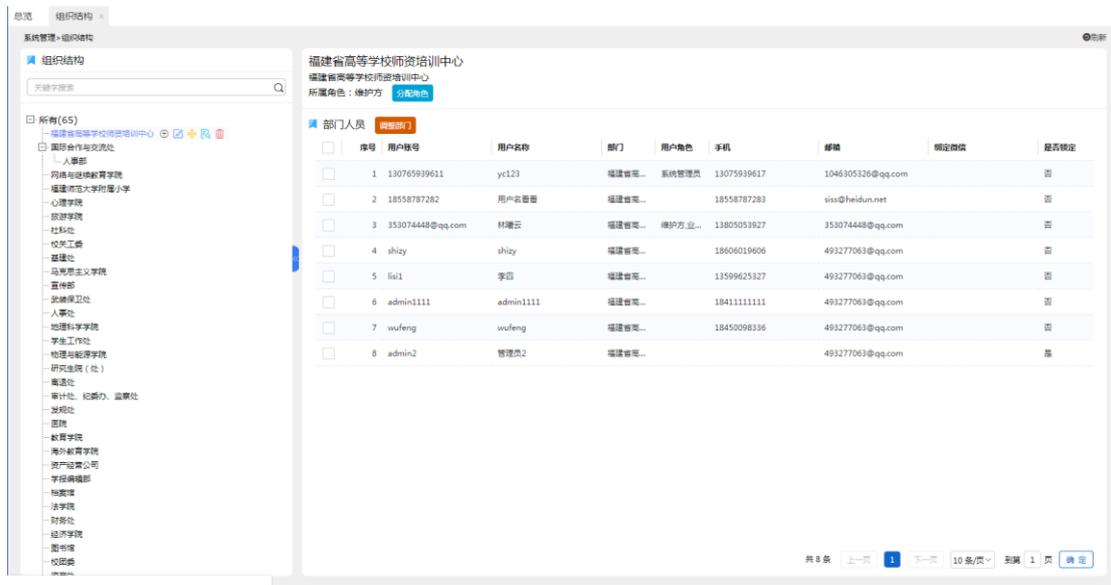
路径：系统管理->系统角色。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行增删查改，权限维护操作。

## 2.7.4 组织结构

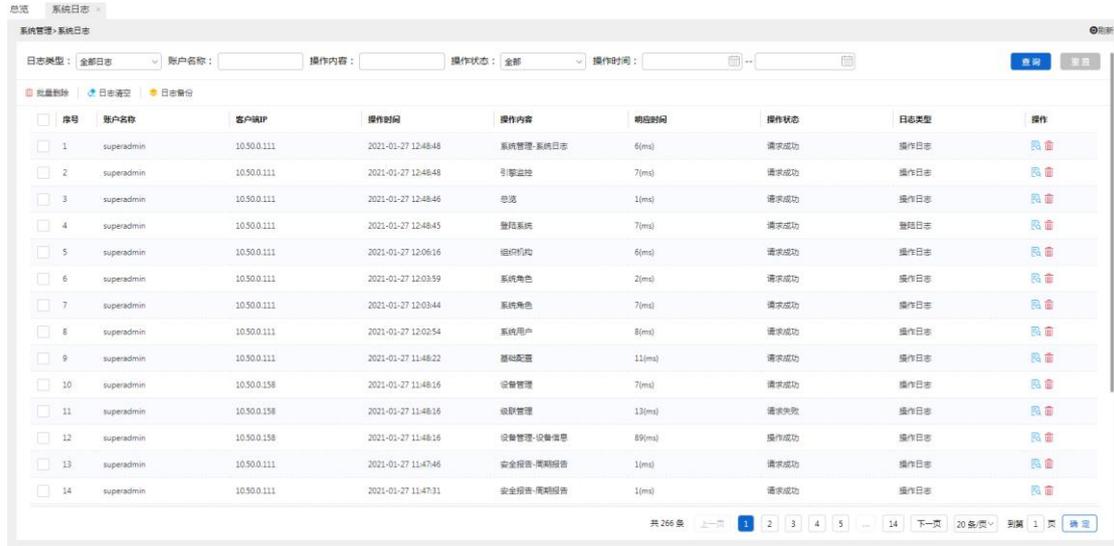
路径：系统管理->组织结构。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行增删查改等组织结构。

## 2.7.5 系统日志

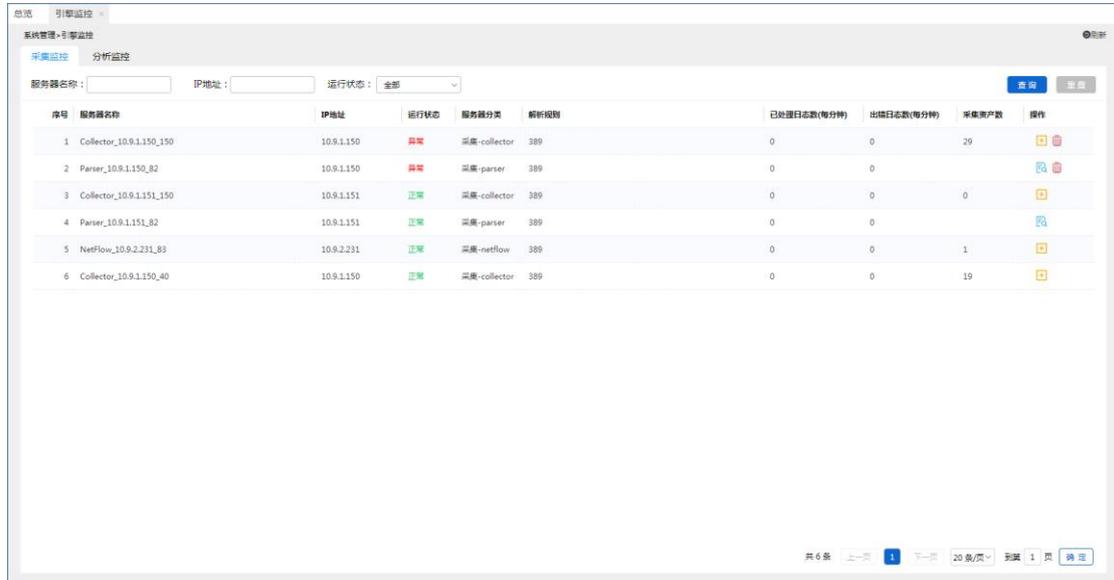
路径：系统管理->系统日志。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行查看、删除及备份等操作。

## 2.7.6 引擎监控

路径：系统管理->引擎监控。



通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行添加、查看及删除操作。

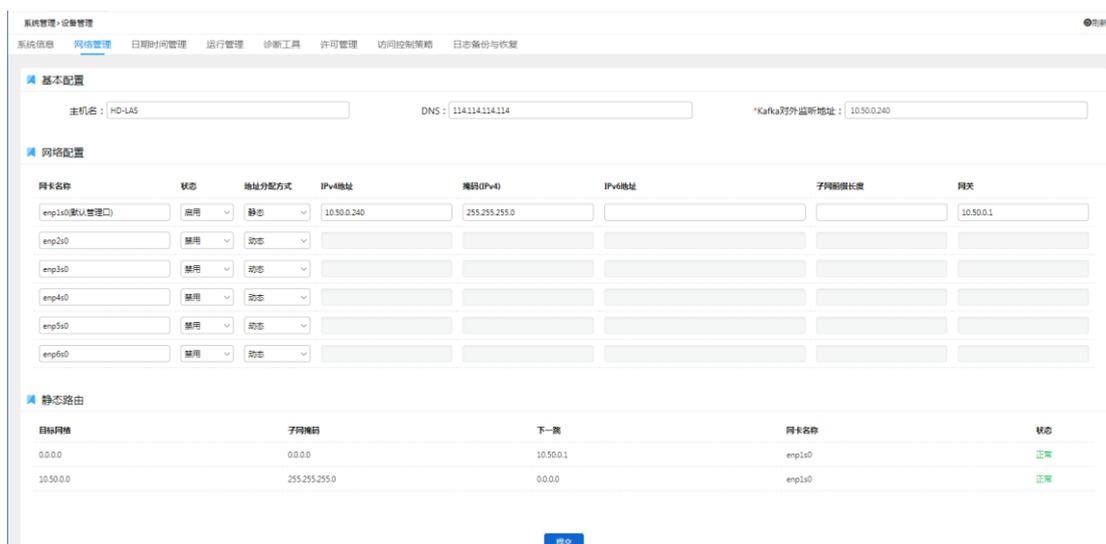
## 2.7.7 设备管理

路径：系统管理->设备管理。

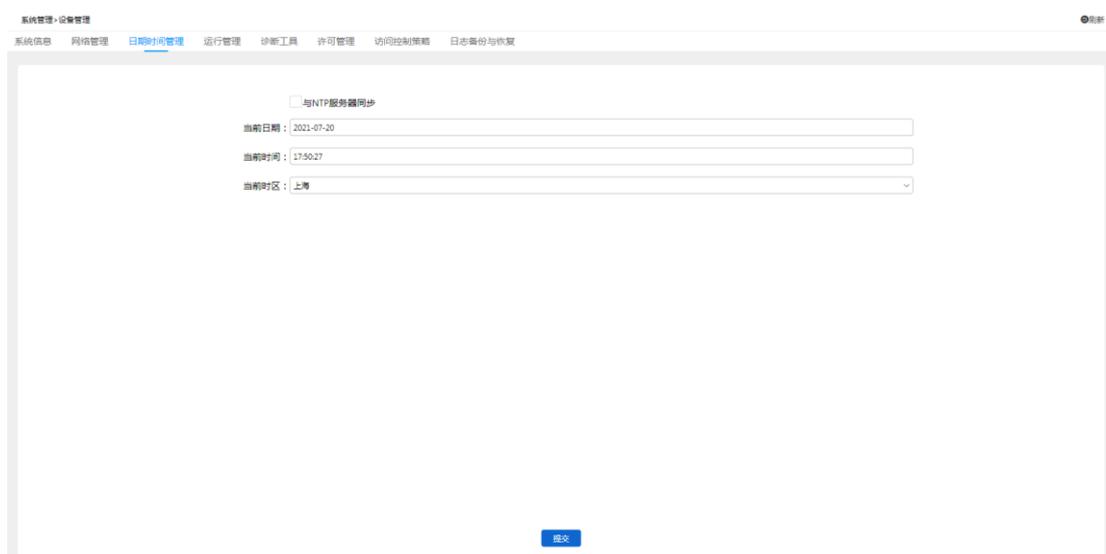
可进行多项设备管理，点击‘系统信息’，进入系统信息页面，可查看系统信息。



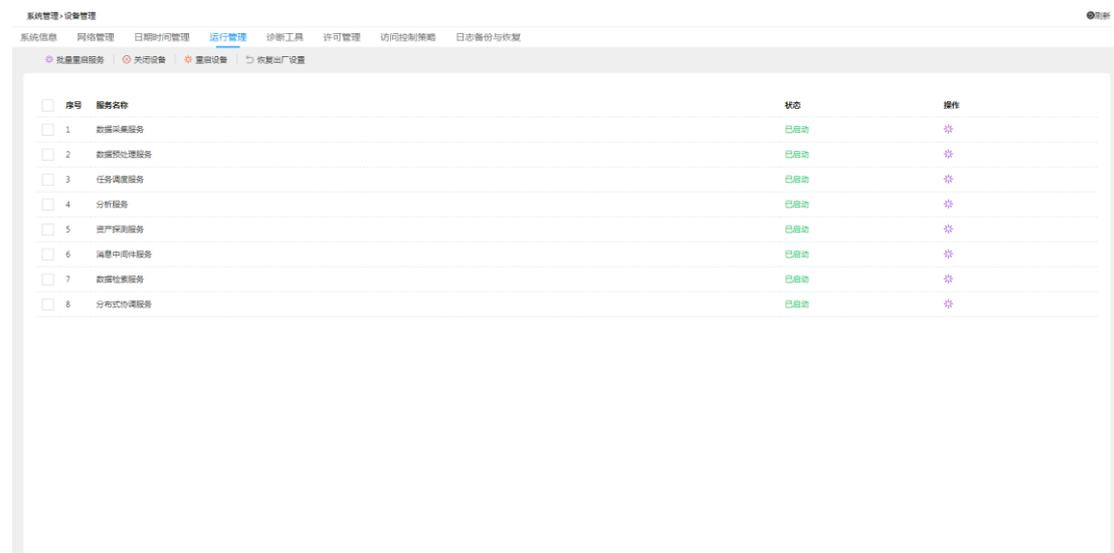
点击‘网络管理’，进入网络管理页面，可继续网络配置和查看路由信息。



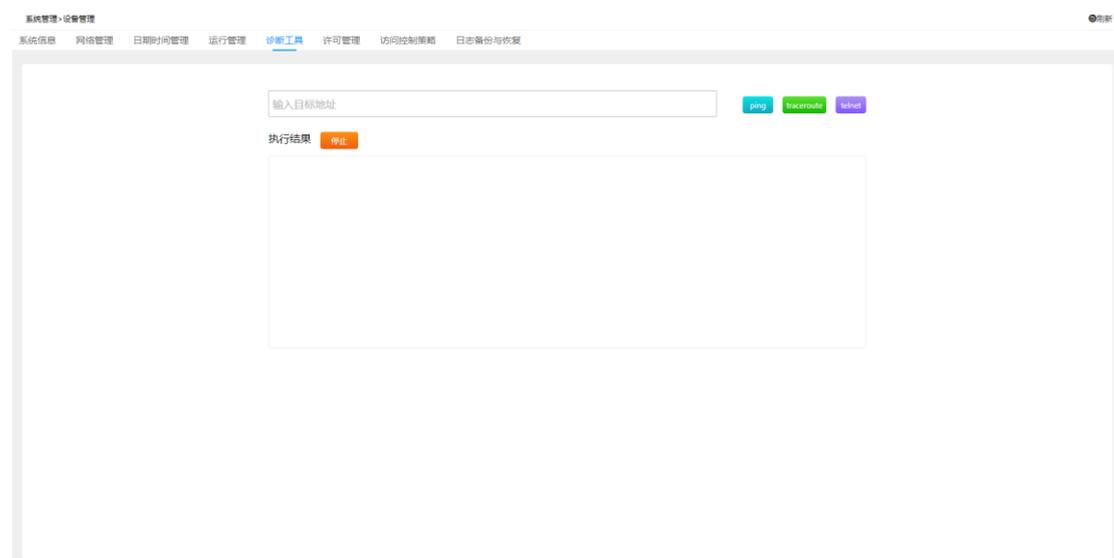
点击‘日期时间管理’，进入日期时间管理页面，填写内容，点击【提交】，日期时间设置完成。



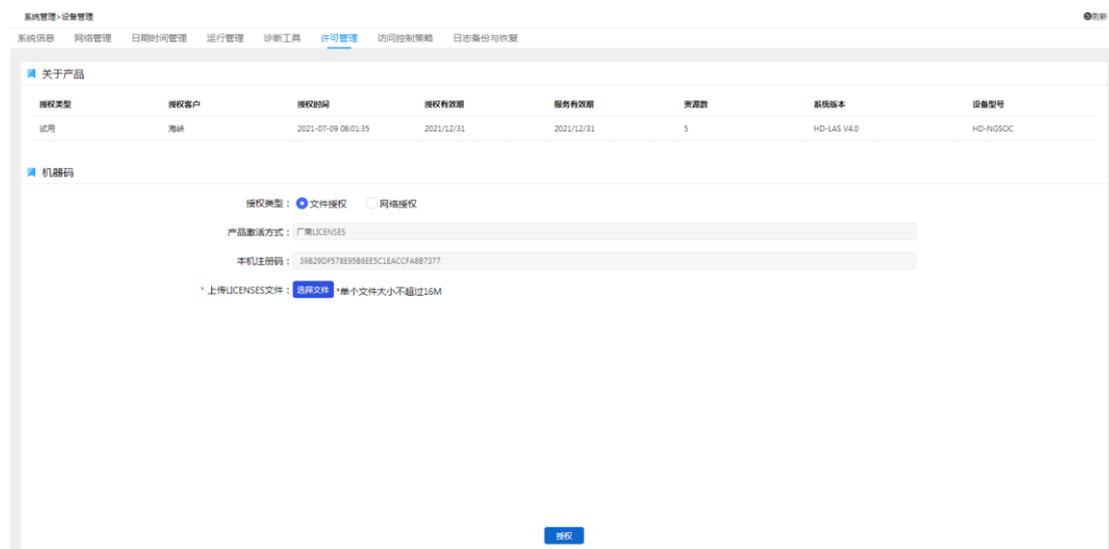
点击‘运行管理’，进入运行管理页面，可查看服务信息，并进行重启服务、重启设备及恢复出厂设置等操作。



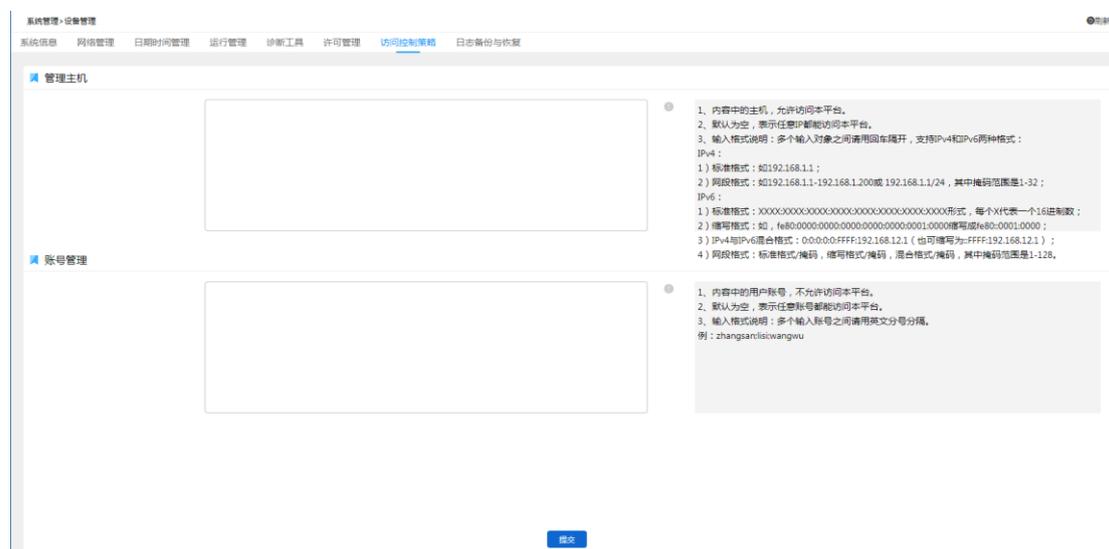
点击‘诊断工具’，进入诊断工具页面。



点击‘许可管理’，进入许可管理页面，可查看产品相关内容，并进行本地授权或网络授权。



点击‘访问控制策略’，进入访问控制策略页面，可对主机和账号进行管理。



点击‘日志备份与恢复’，进入日志备份与恢复页面。  
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行配置、备份及恢复等操作。

系统管理·设备管理 刷新

系统信息 网络管理 日期时间管理 运行管理 诊断工具 许可管理 访问控制策略 日志备份与恢复

备份 恢复

服务器地址:  状态: 全部 备份时间:  --  查询 重置

配置 | 批量恢复

<input type="checkbox"/>	序号	备份策略	备份方式	备份服务器地址	备份时间	创建时间	进度	状态	操作
<input type="checkbox"/>	1	立即备份	SFTP	10.50.0.230	2021-03-12	2021-03-13 17:25:35	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	成功	