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

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。

1.4.1.1Web 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。

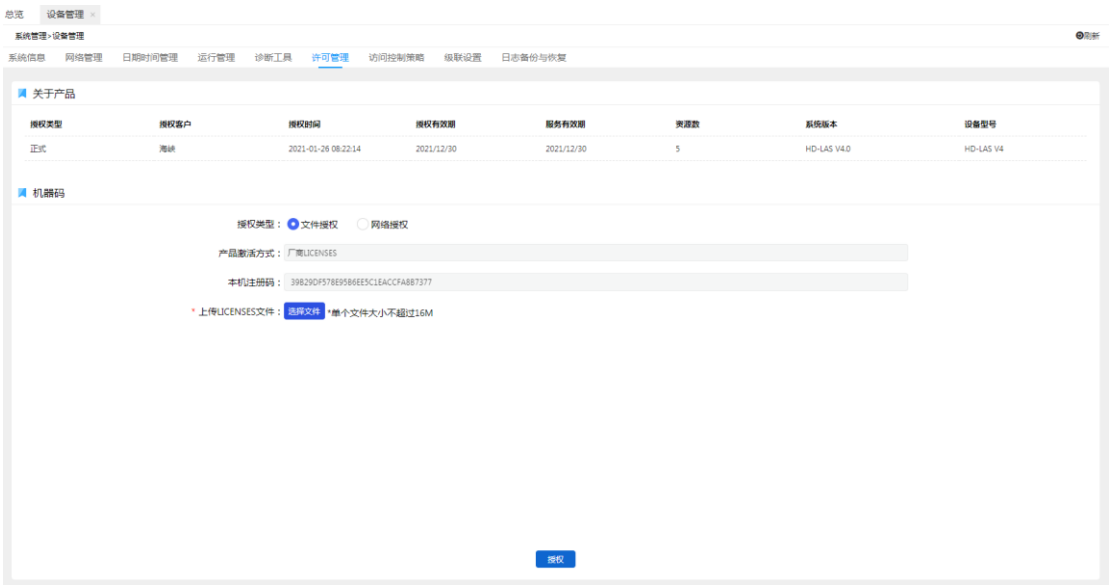
（2）输入用户名、密码及验证码。

（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： 2022-01-01 14:19:20
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： 10.5.17.29
本地管理口IPV4地址： 10.9.14.163
本地管理口子网掩码： 255.255.0.0
网关： 10.9.14.254
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：

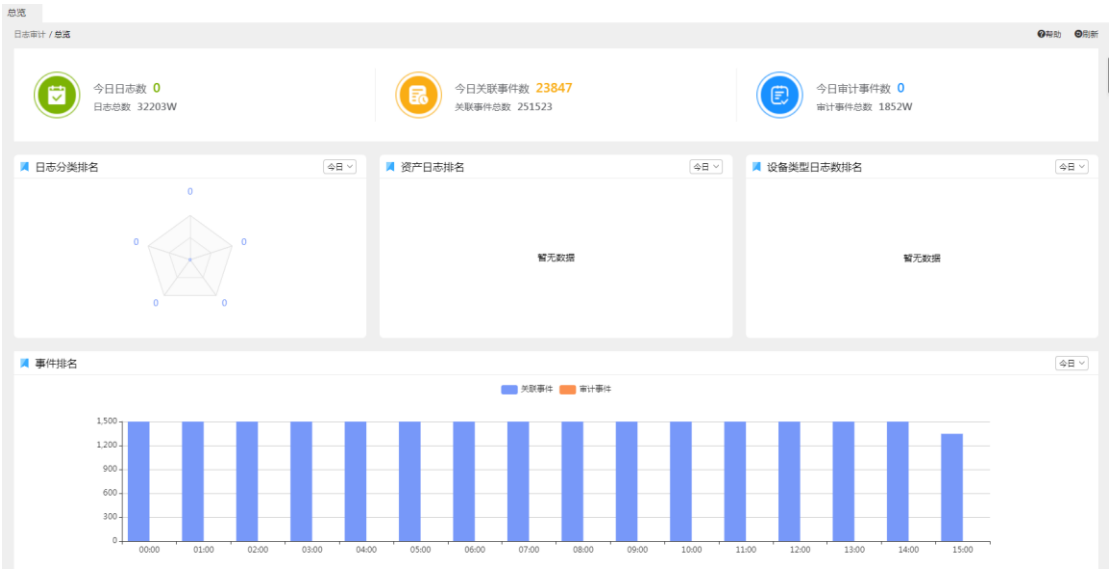
（1）授权类型：网络授权；

（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：



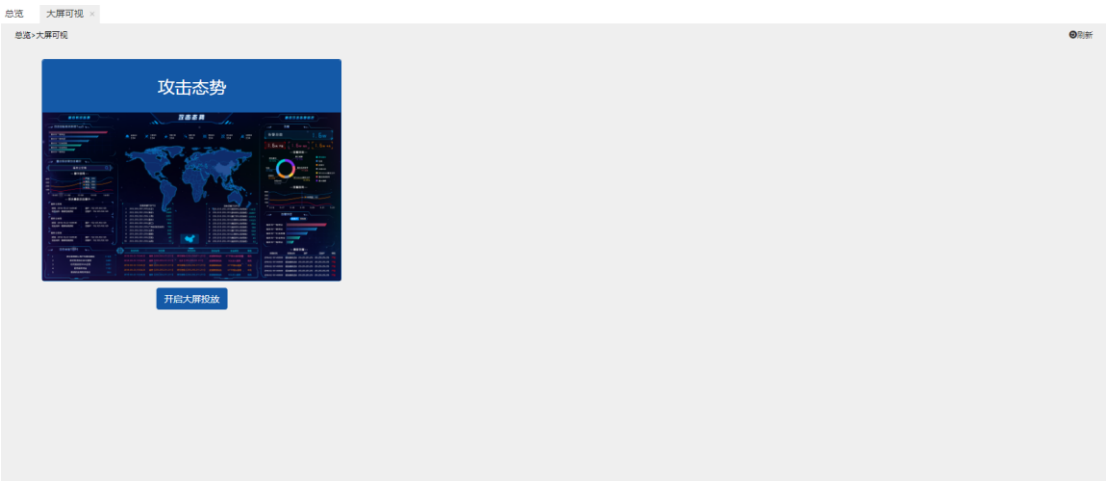
2.2 总览

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

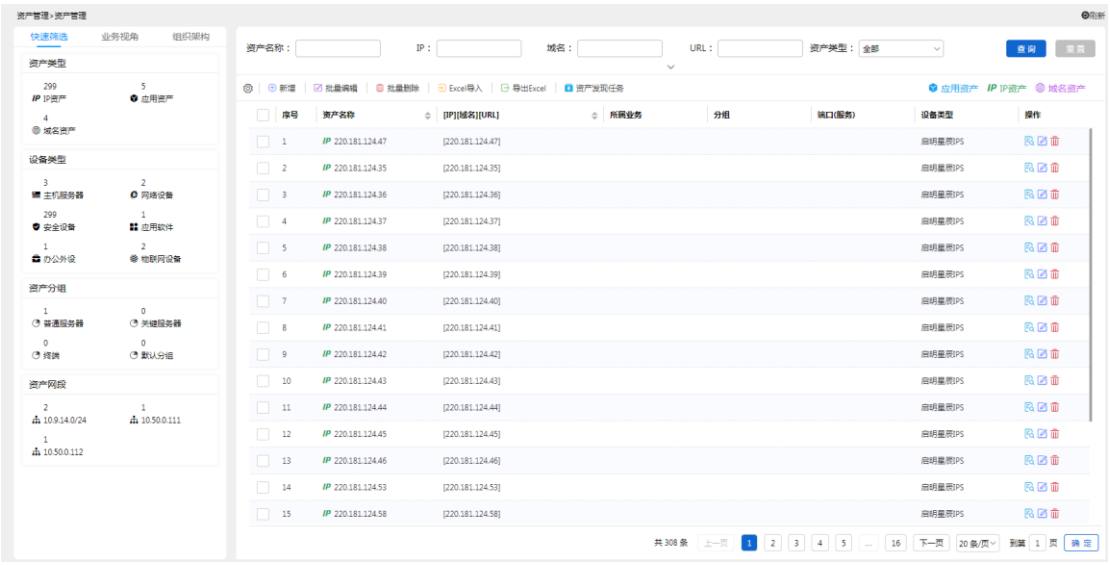
路径：总览->大屏可视。可查看大屏信息。



2.3 资产管理

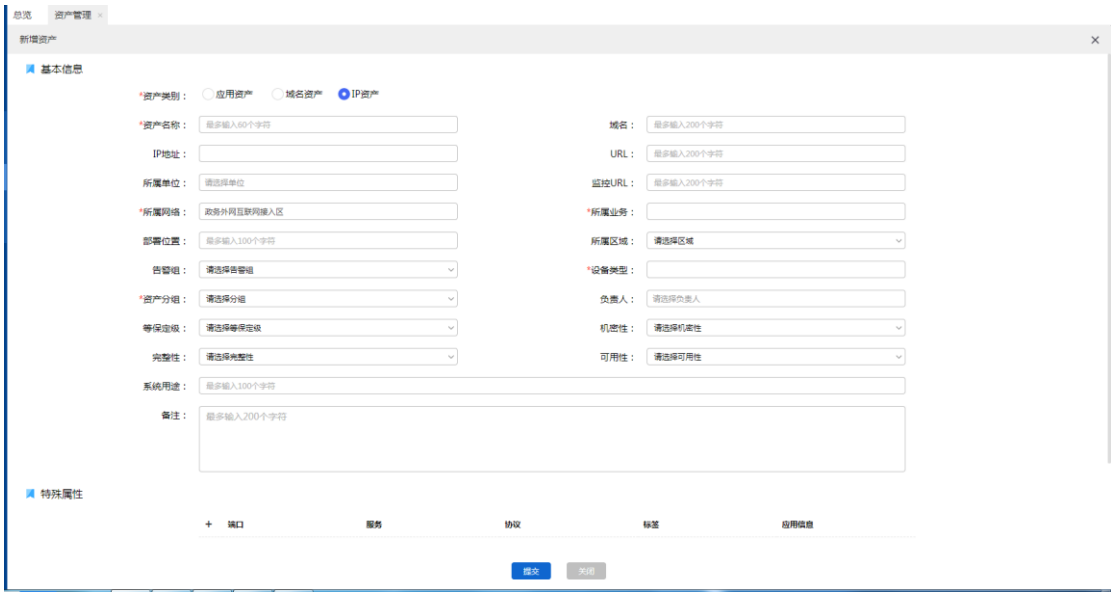
2.3.1 资产管理

路径：资产管理->资产管理。

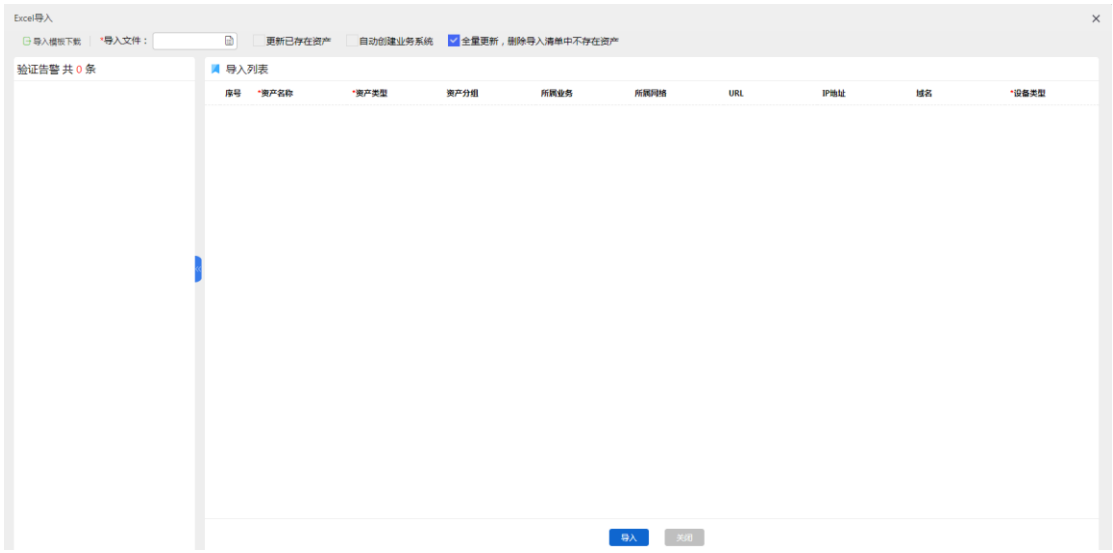


通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【新增】，跳至新增页面。



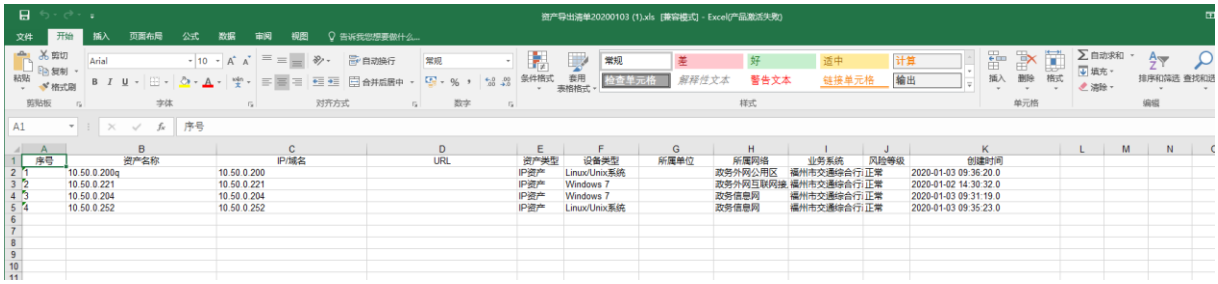
点击【提交】，页面跳转至资产管理页面。
左边勾选框勾选多项，点击【批量编辑】，可以批量编辑资产。
左边勾选框勾选多项，点击【批量删除】，可以批量删除资产。
点击【excel 导入】，页面跳至 excel 导入页面。



点击【导入模板下载】，打开模板。

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



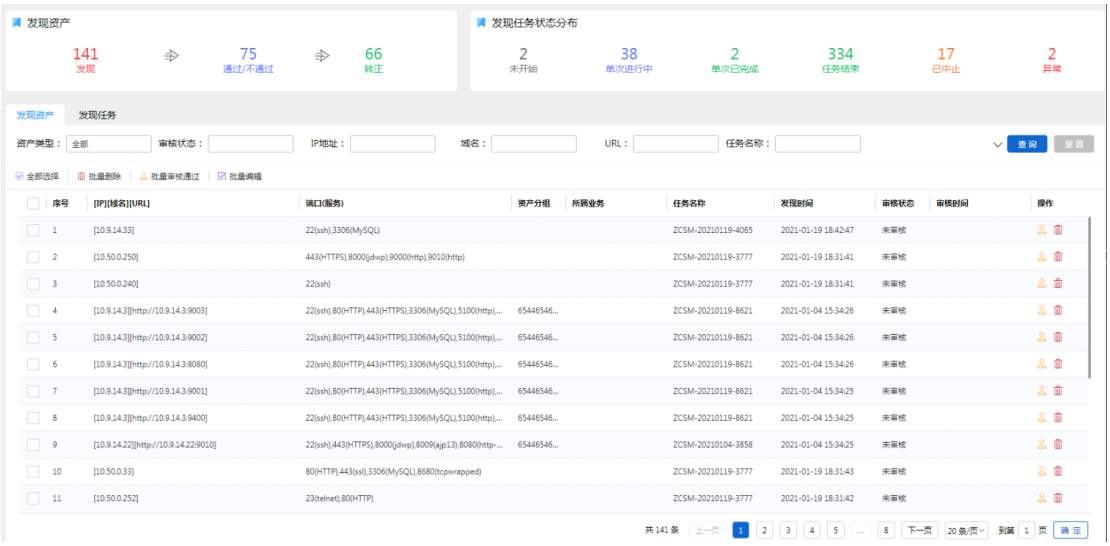
序号	资产名称	IP/域名	URL	资产类型	设备类型	所属单位	所属网络	业务系统	风险等级	创建时间
1	10.50.0.200q	10.50.0.200		IP资产	Linux/Unix系统		政务外网公用区	福州市交通综合行	正常	2020-01-03 09:36:20.0
2	10.50.0.221	10.50.0.221		IP资产	Windows 7		政务外网互联网接	福州市交通综合行	正常	2020-01-02 14:30:32.0
3	10.50.0.204	10.50.0.204		IP资产	Windows 7		政务信息网	福州市交通综合行	正常	2020-01-03 09:31:19.0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



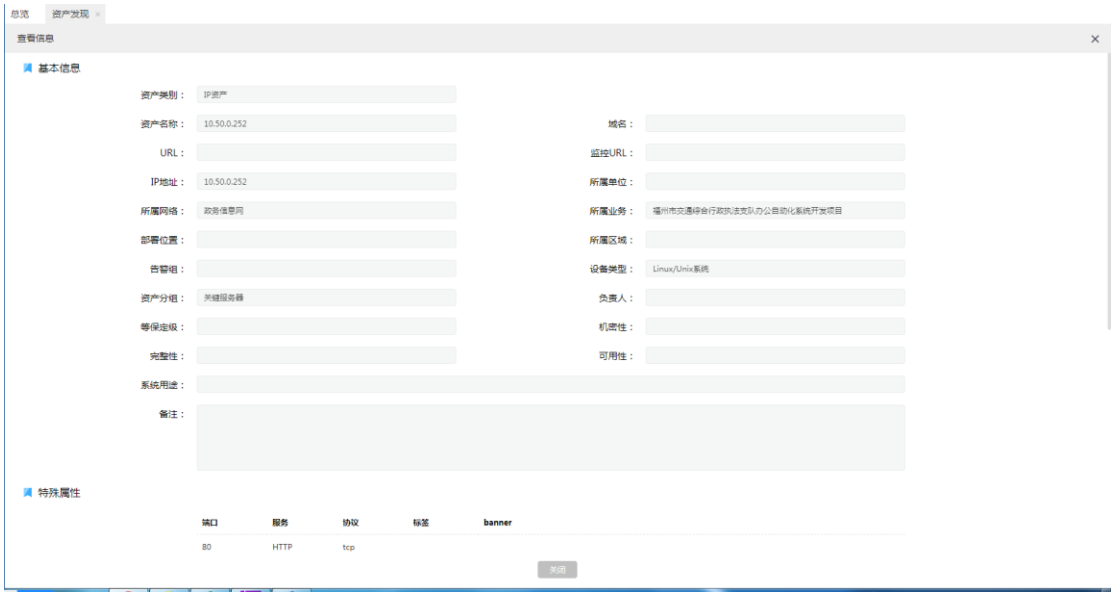
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

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。

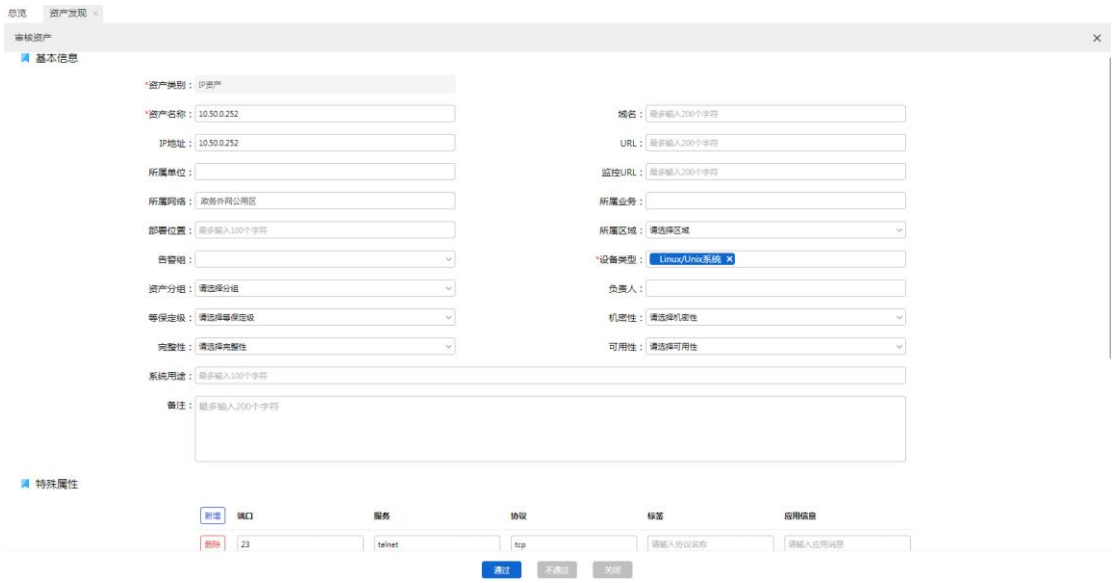
左边勾选框勾选单个或多个资产，点击【批量删除】，可以删除选中内容。

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。



点击【审核】，进入未审核资产审核页面。

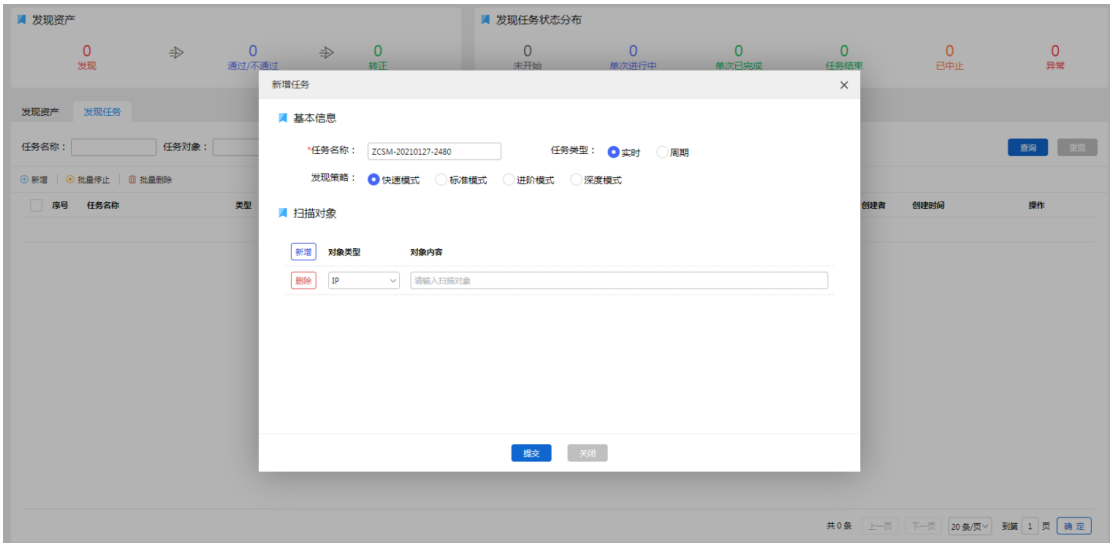


点击【删除】，可删除资产。

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

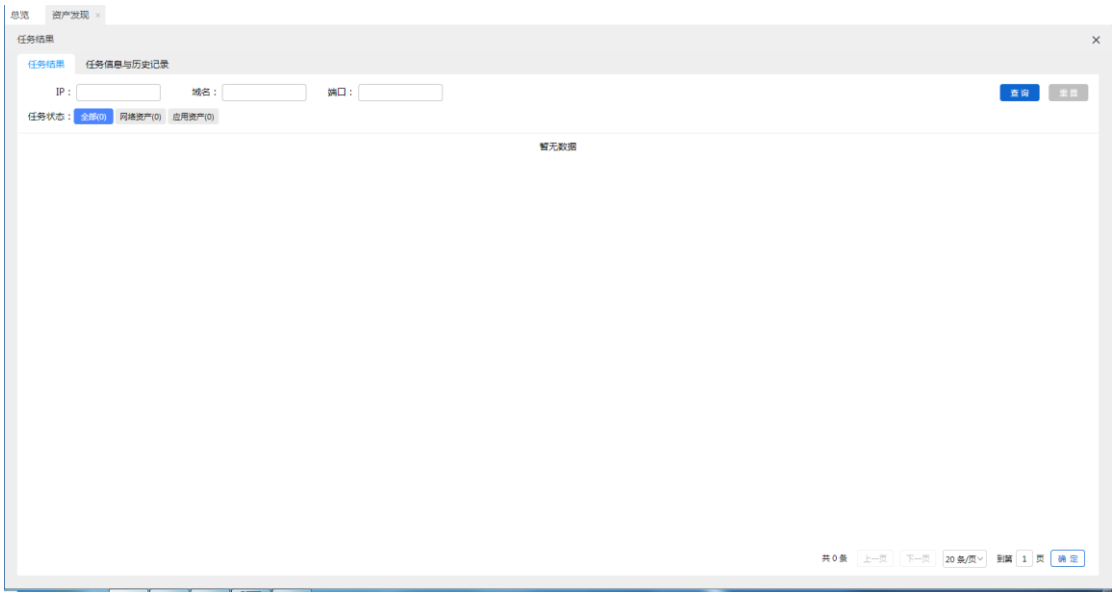


填写相关内容，点击【提交】，进行资产发现任务。

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。

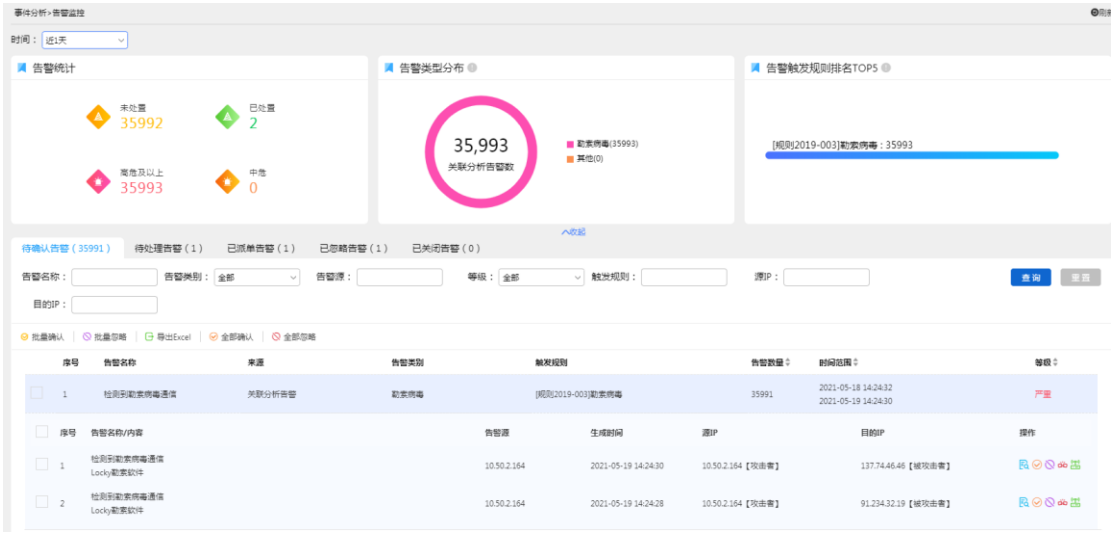
2.4 事件分析

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。

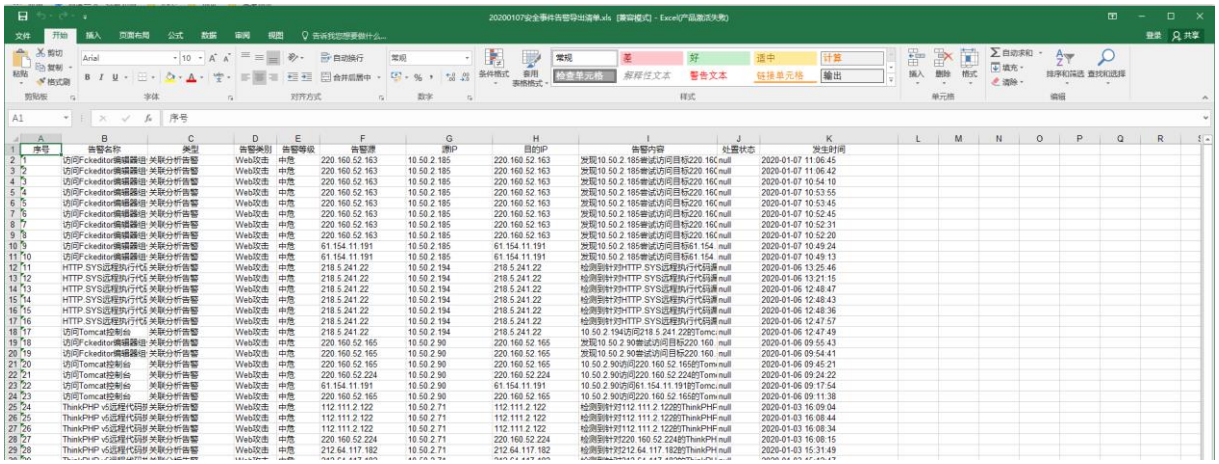
1、 待确认告警页面



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



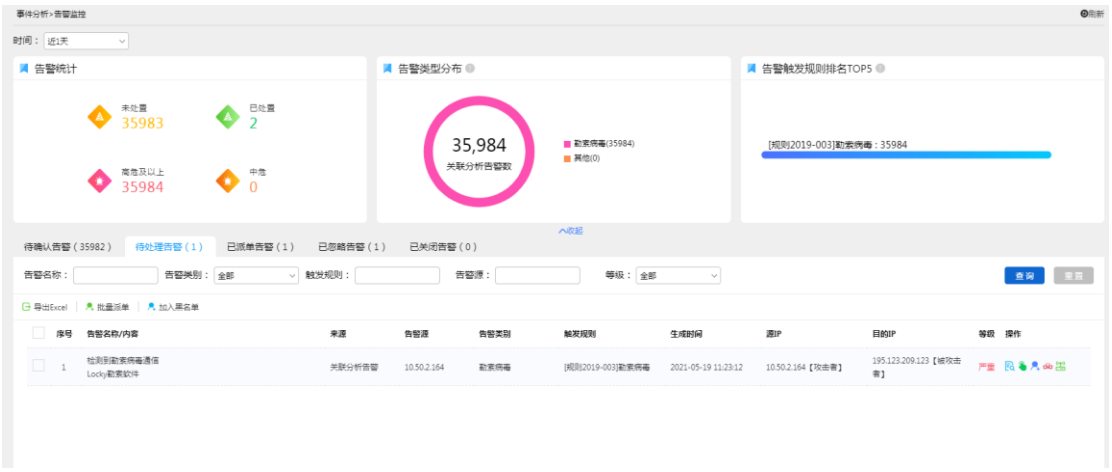
点击【全部确认】，可以确认全部告警。

点击【全部忽略】，可以忽略全部告警。

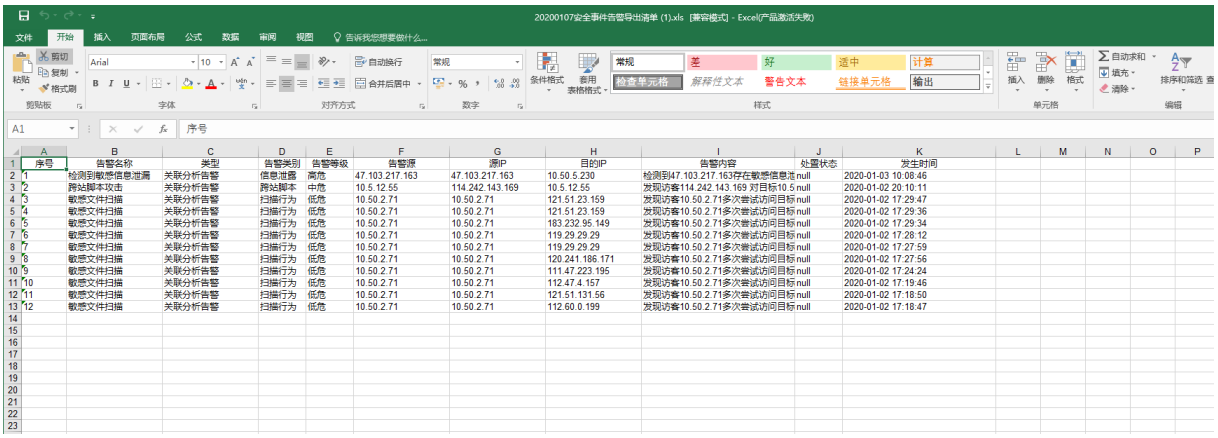
点击一条告警事件，点击操作中的【查看】

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

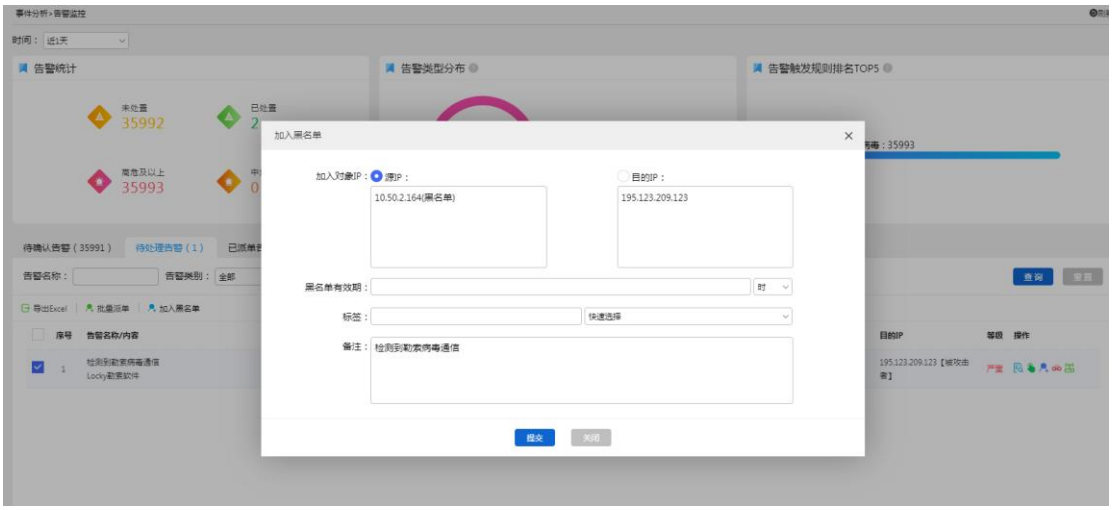


点击【导出 excel】，导出页面如下



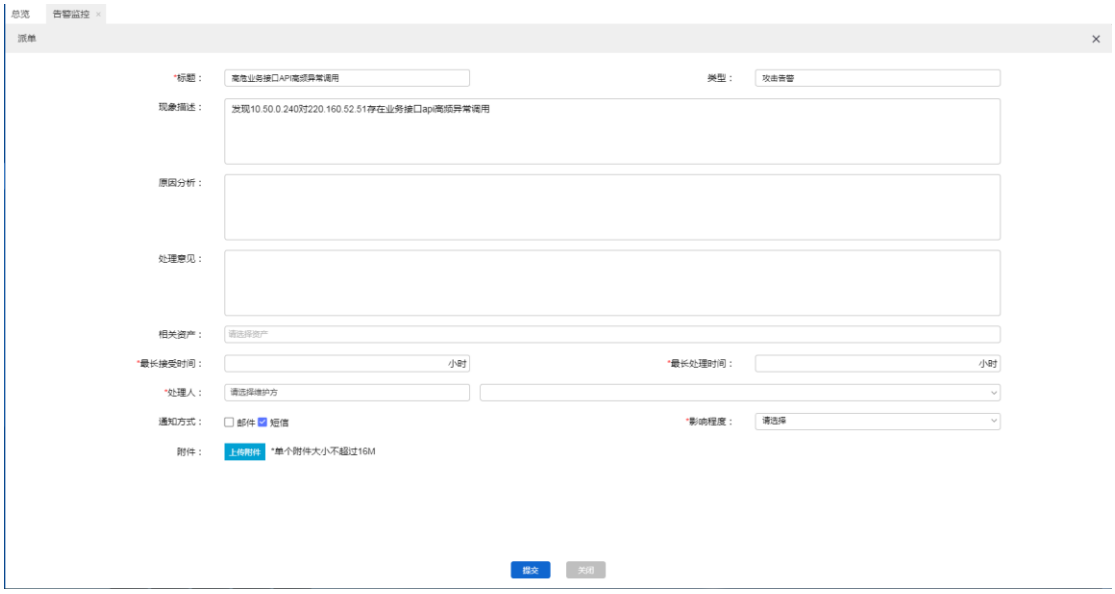
左边勾选框勾选多项，点击【批量派单】，可以批量派单告警。

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。



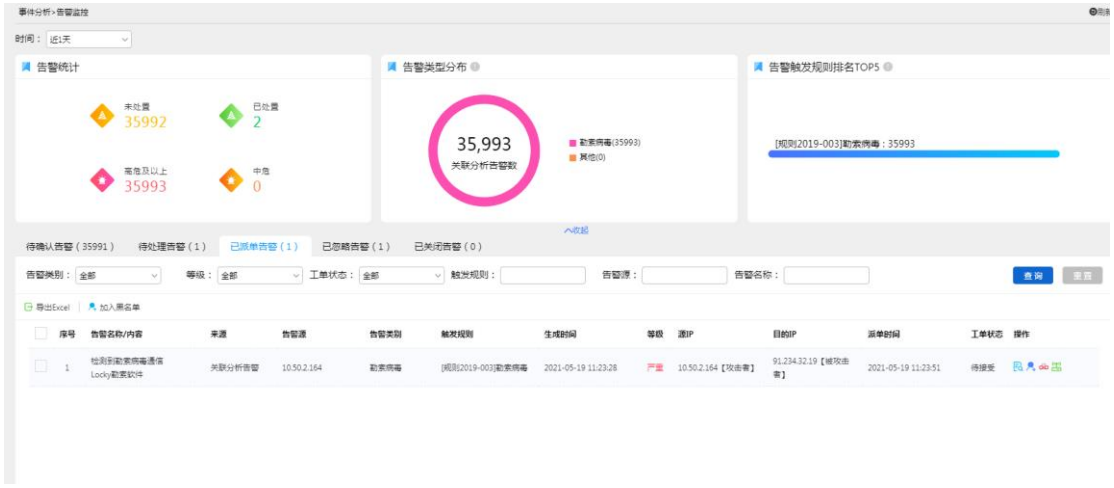
点击操作中的【查看】

点击操作中的【派单】，可对告警进行派单处理

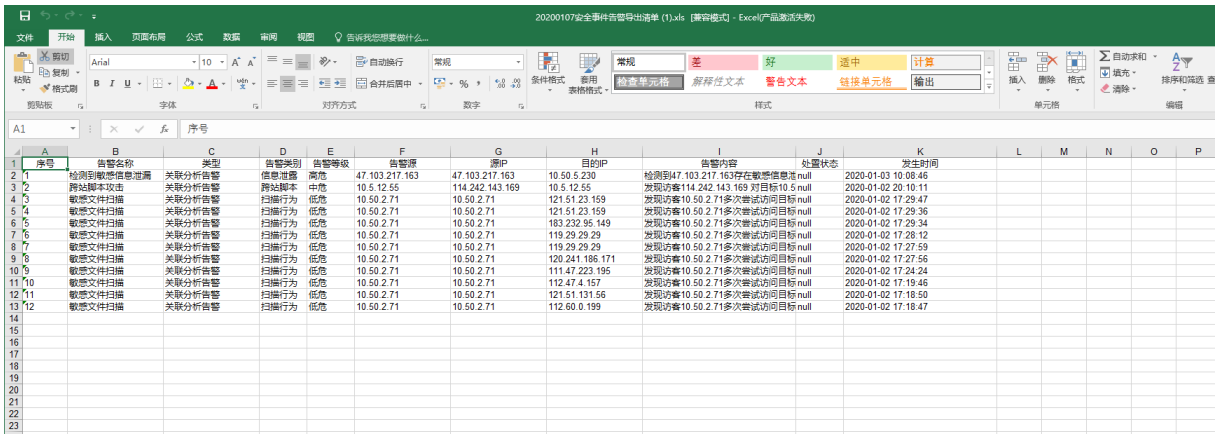


点击操作中的【加入黑名单】，可以对告警中的源 IP 或目的 IP 加入黑名单。
点击操作中的【一键断网】，可以对 IP 进行封堵。
点击操作中的【恢复断网】，可以对 IP 进行解封。

3、 已派单告警页面



点击【导出 excel】，导出页面如下



序号	告警名称	类型	告警类别	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	检测到敏感信息泄漏	关联分析告警	信息泄露	高危	47.103.217.163	47.103.217.163	10.50.5.230	检测到47.103.217.163存在敏感信息泄	null	2020-01-03 10:08:46
2	跨站脚本攻击	关联分析告警	跨站脚本	中危	10.5.12.55	114.242.143.169	10.5.12.55	发现访客114.242.143.169 对目标10.5	null	2020-01-02 20:10:11
3	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:29:47
4	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.23.159	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:29:36
5	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	183.232.96.149	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:29:34
6	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:28:12
7	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	119.29.29.29	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:27:59
8	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	120.241.186.171	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:27:56
9	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	111.47.223.195	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:24:24
10	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.47.4.157	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:19:46
11	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	121.51.131.56	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:18:50
12	敏感文件扫描	关联分析告警	扫描行为	低危	10.50.2.71	10.50.2.71	112.60.0.199	发现访客10.50.2.71多次尝试访问目标	null	2020-01-02 17:18:47

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。

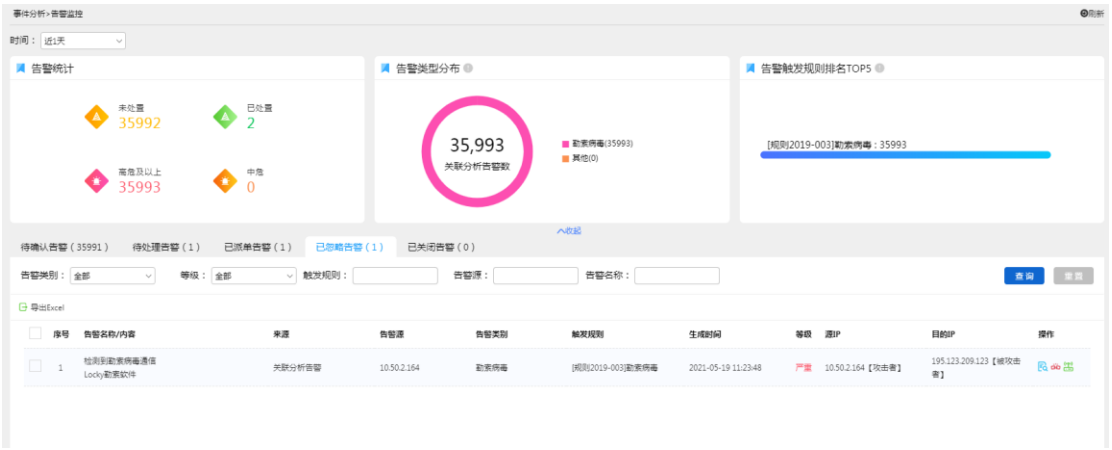
点击操作中的【查看】

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。

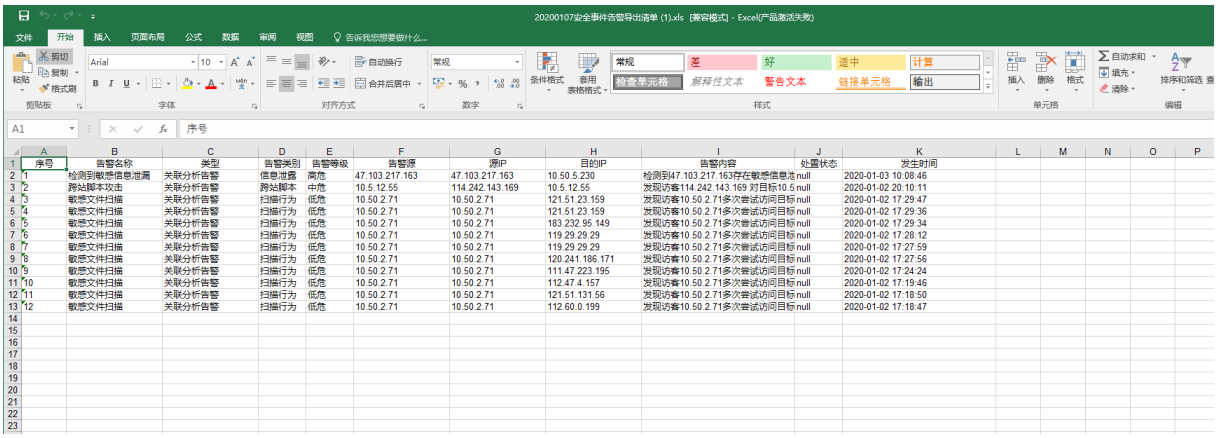
点击操作中的【一键断网】，可以对 IP 进行封堵。

点击操作中的【恢复断网】，可以对 IP 进行解封。

4、 已忽略告警



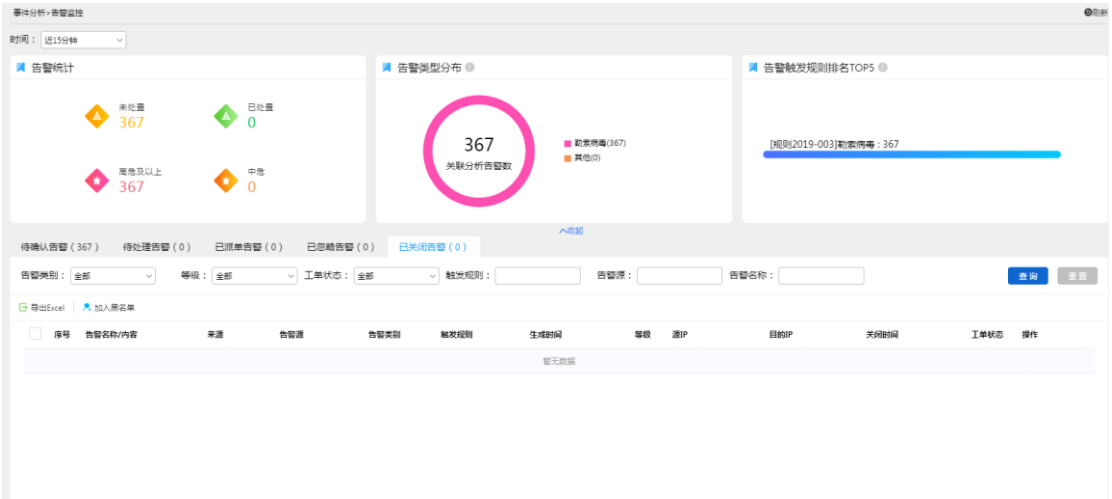
点击【导出 excel】，导出页面如下



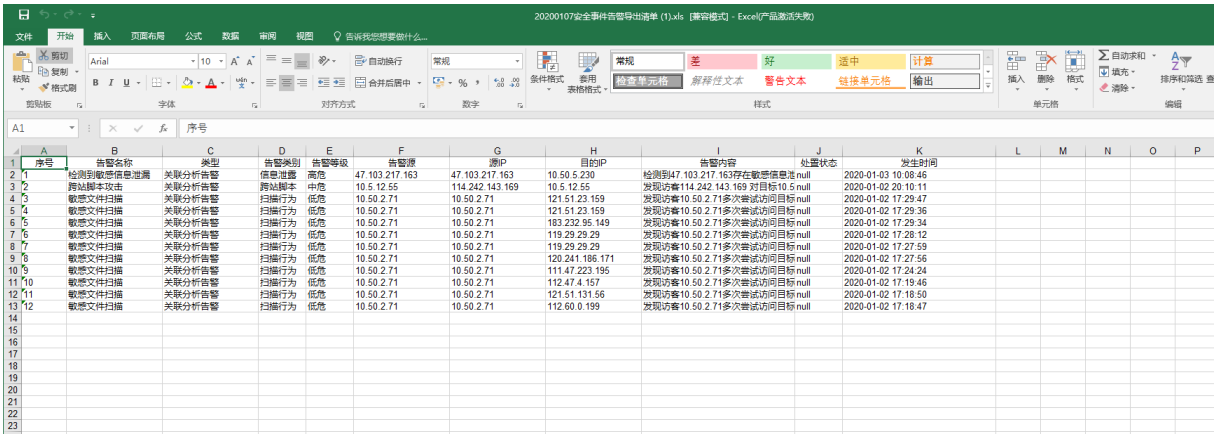
点击操作中的【查看】

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



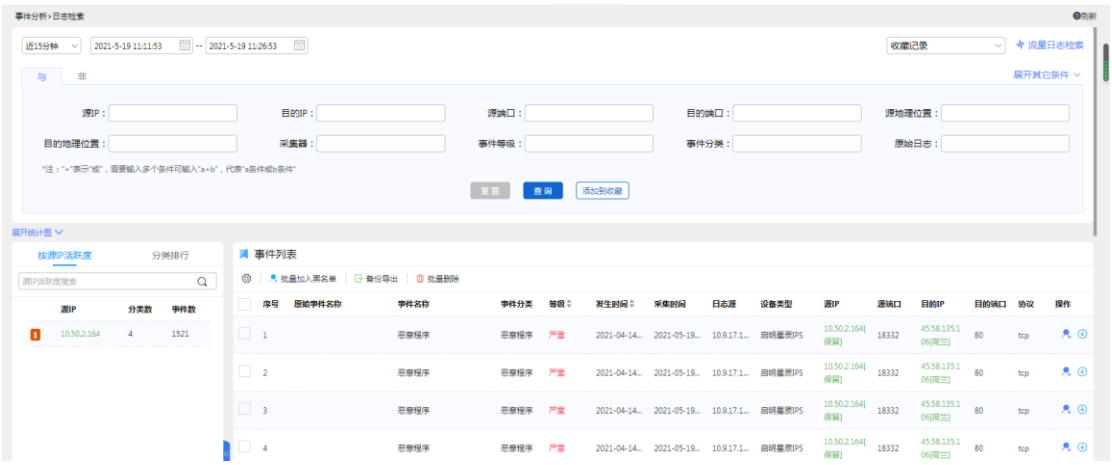
左边勾选框勾选多项，点击【加入黑名单】，可以批量对告警中的源 IP 或目的 IP 加入黑名单。

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。

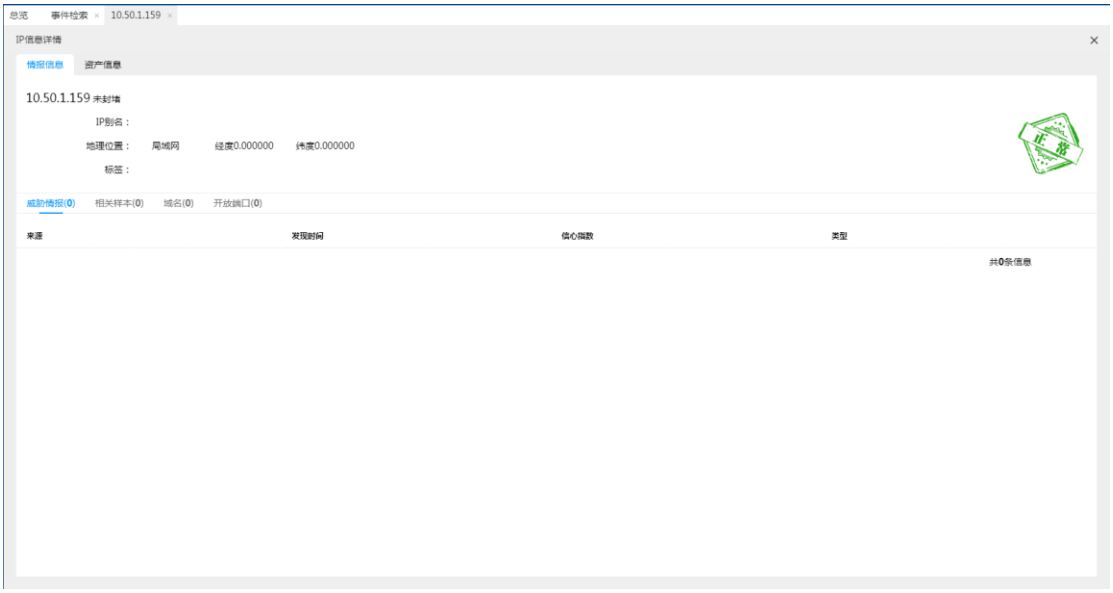
2.4.2 日志检索

路径：事件分析->日志检索。

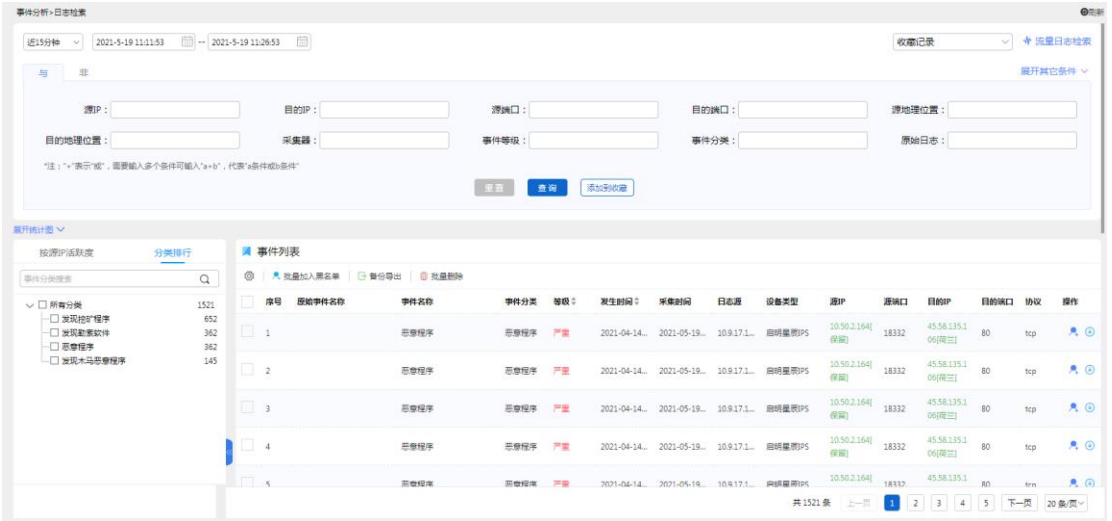


点击源 Ip, 跳至 Ip 画像

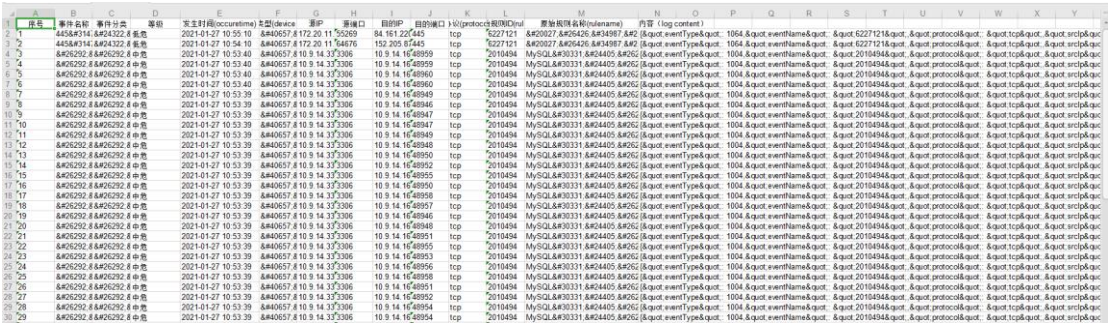
点击【ip 信息详情】，进入 ip 信息详情页面



点击“分类排行”，可勾选分类检索筛选安全事件

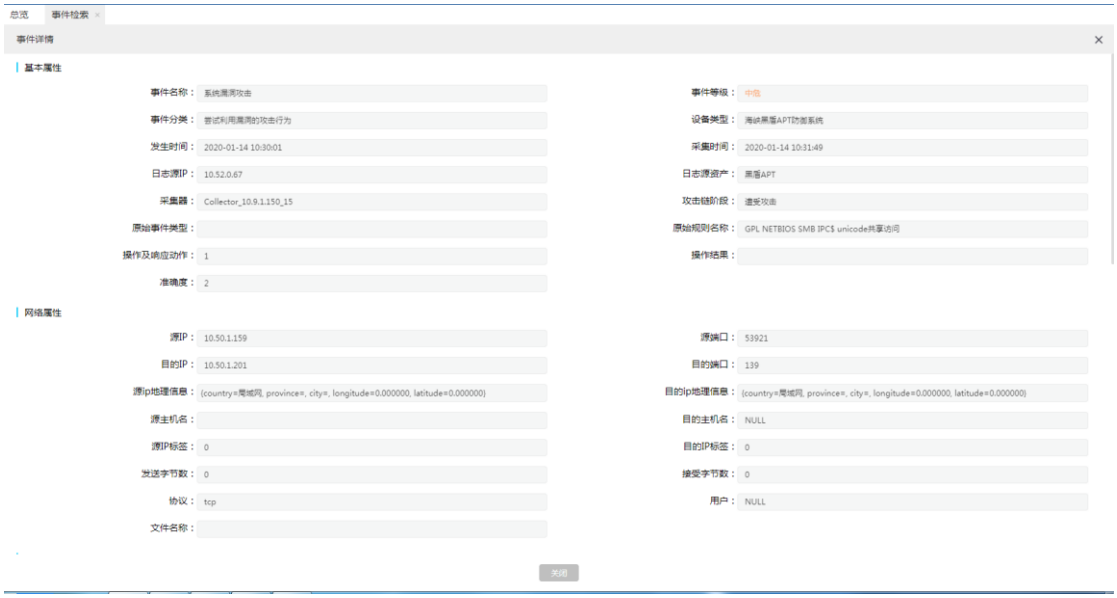


左边勾选框勾选多项，点击【批量加入黑名单】，可将一个或多个源 ip 或目的 ip 加入黑名单。
左边勾选框勾选多项，点击【备份导出】，导出页面如下



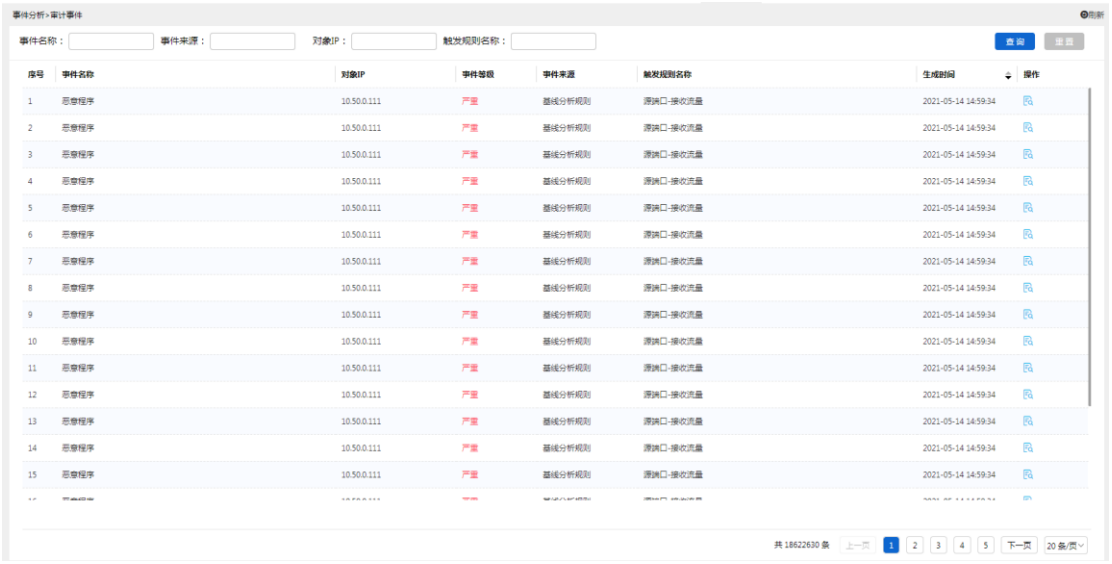
序号	事件名称	事件分类	等级	发生时间(occurrtime)	类型(device	源IP	源端口	目的IP	目的端口	协议(protocol	规则ID(rul	原始规则名称(rulename)	内容（log content）
1	445ĺ异&#鉴危			2021-01-27 10:55:10	黑&#10	9.14.37.&#3306	55269	84.161.22	445	tcp	6227121	主机被&#2	{"eventType": 1064,"eventName": "6227121","protocol": "tcp","srcIp&quo
2	1	445ĺ异&#鉴危		2021-01-27 10:54:10	黑&#10	9.14.37.&#3306	54676	152.205.8	7445	tcp	6227121	主机被&#2	{"eventType": 1064,"eventName": "6227121","protocol": "tcp","srcIp&quo
3	2	暴暴&#中危		2021-01-27 10:53:40	黑&#10	9.14.37.&#3306		10.9.14.16	48959	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
4	3	暴暴&#中危		2021-01-27 10:53:40	黑&#10	9.14.37.&#3306		10.9.14.16	48959	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
5	4	暴暴&#中危		2021-01-27 10:53:40	黑&#10	9.14.37.&#3306		10.9.14.16	48959	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
6	5	暴暴&#中危		2021-01-27 10:53:40	黑&#10	9.14.37.&#3306		10.9.14.16	48960	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
7	6	暴暴&#中危		2021-01-27 10:53:40	黑&#10	9.14.37.&#3306		10.9.14.16	48960	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
8	7	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48949	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
9	8	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48946	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
10	9	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48947	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
11	10	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48947	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
12	11	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48949	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
13	12	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48948	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
14	13	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48950	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
15	14	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48952	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
16	15	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48955	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
17	16	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48950	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
18	17	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48958	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
19	18	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48957	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
20	19	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48946	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
21	20	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48948	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
22	21	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48951	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
23	22	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48955	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
24	23	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48953	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
25	24	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48956	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
26	25	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48958	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
27	26	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48951	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
28	27	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48952	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
29	28	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48954	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo
30	29	暴暴&#中危		2021-01-27 10:53:39	黑&#10	9.14.37.&#3306		10.9.14.16	48954	tcp	2010494	MySQL登录&#26	{"eventType": 1004,"eventName": "2010494","protocol": "tcp","srcIp&quo

左边勾选框勾选多项，点击【批量删除】，可以批量删除选中内容。
点击操作中的【加入黑名单】，可将源 ip 或目的 ip 加入黑名单。
点击操作中的【pcap 下载】，可下载 pcap。
点击查询结果中单个安全事件，下方下拉安全事件详情,点击更多详情，跳转至事件详情页面



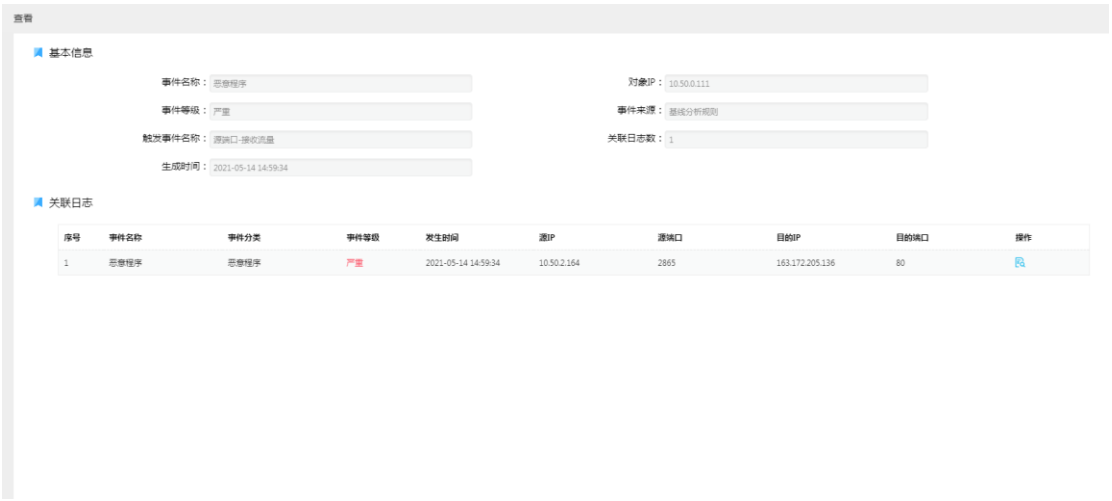
2.4.3 审计事件

路径：事件分析->审计事件。

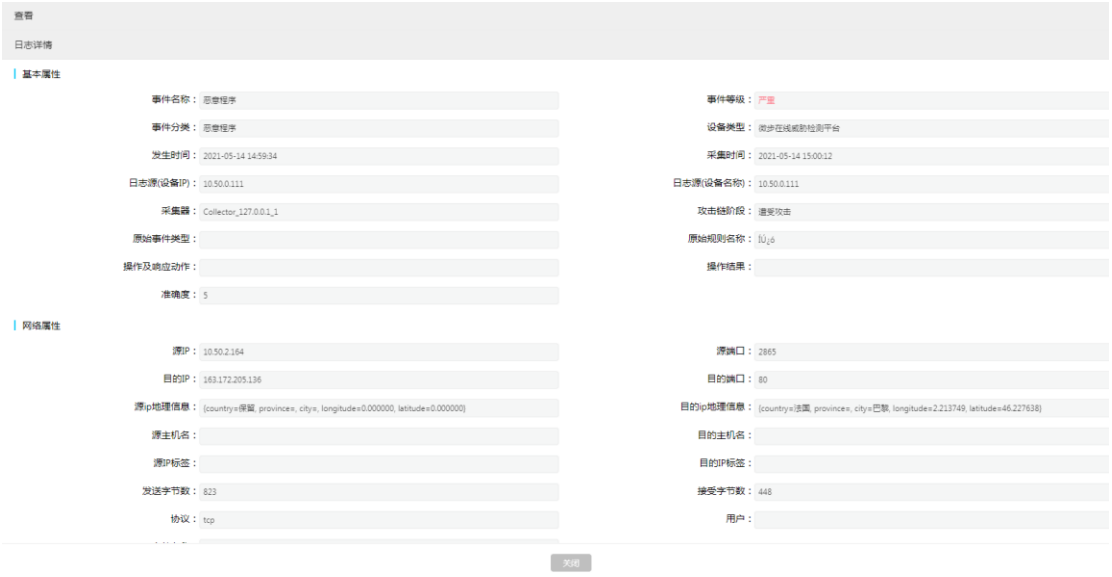


通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。

点击【查看】，跳至审计事件详情页面。

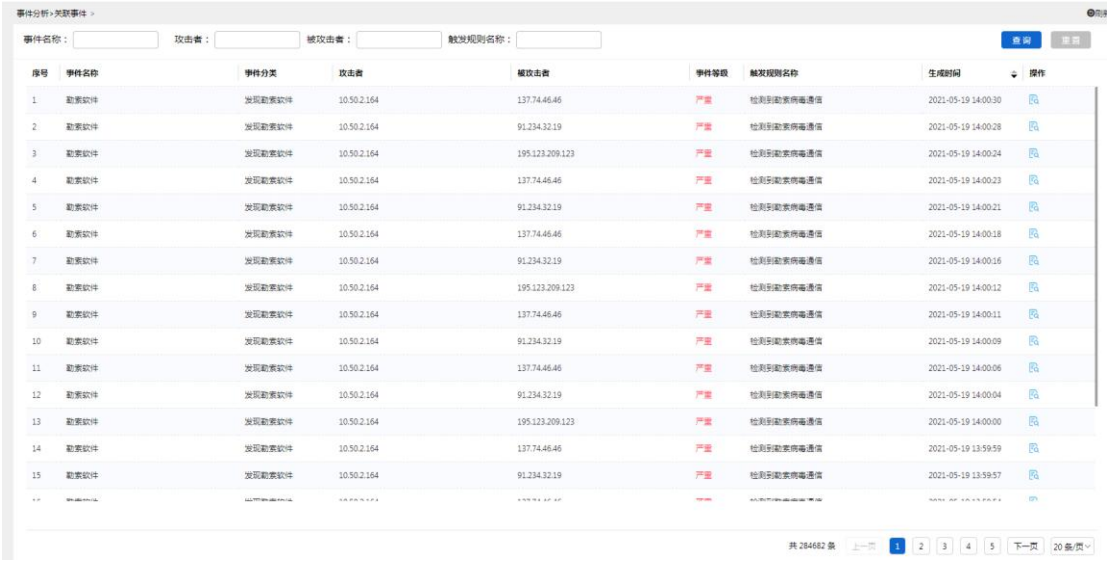


点击【查看】，跳至日志详情页面。



2.4.4 关联事件

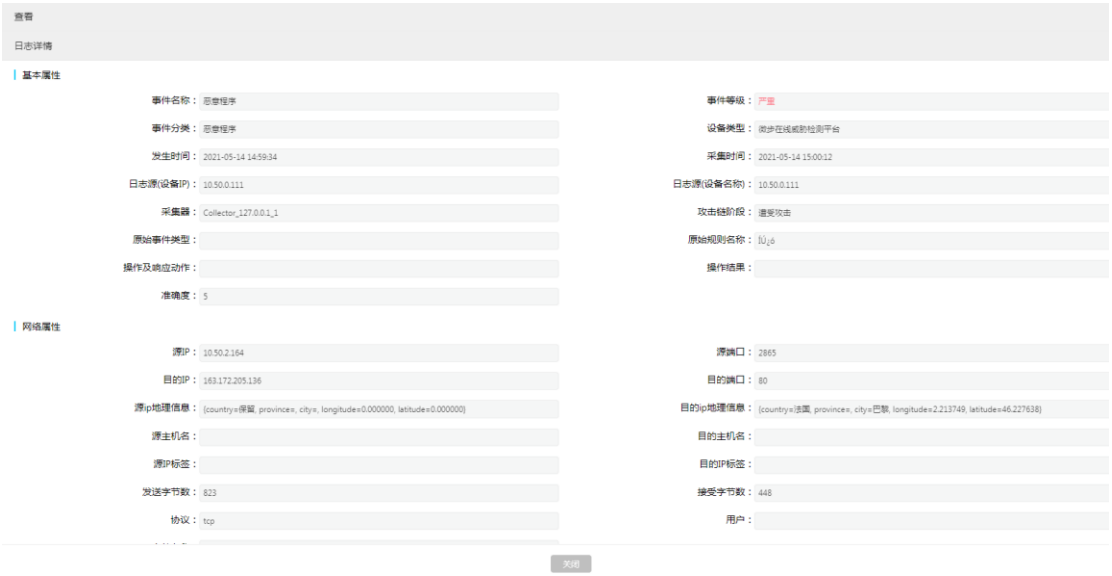
路径：事件分析->关联事件。



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。



2.5 报表管理

2.5.1 安全报告

路径：报表管理->安全报告。

选择威胁分析报告

选择综合日报

选择综合周报

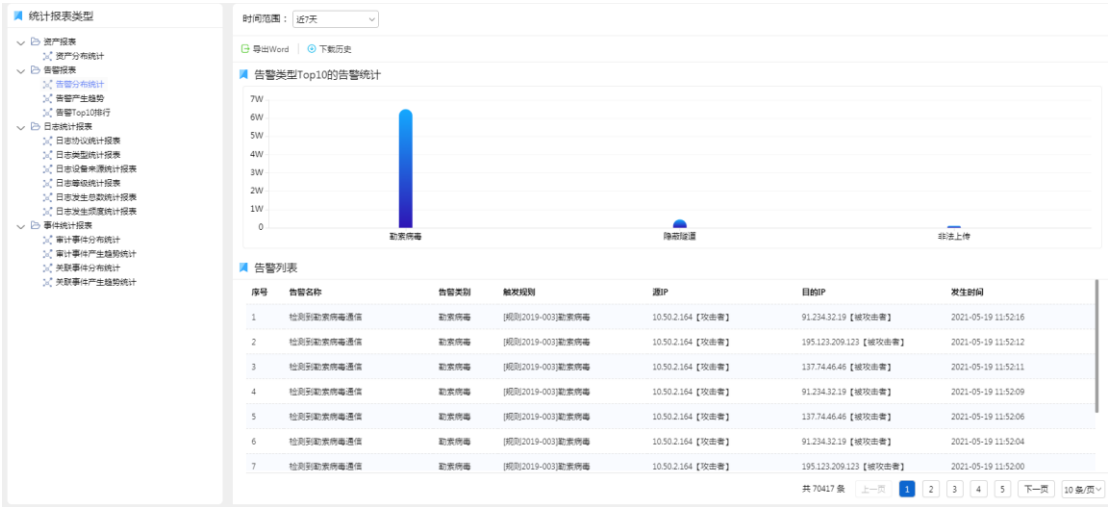
选择综合月报

2.5.2 统计报表

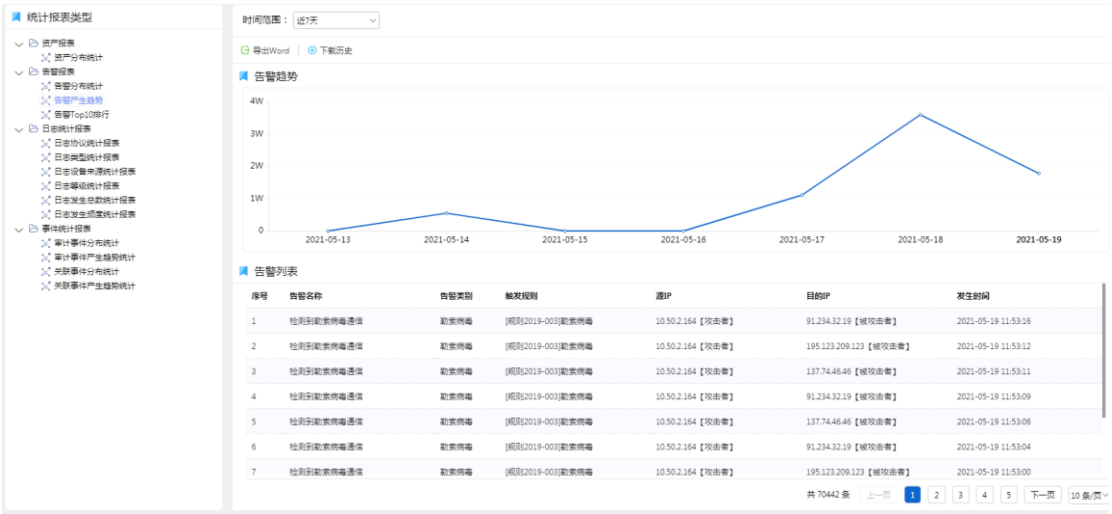
路径：报表管理->统计报表。
通过填写相关查询条件，点击【查询】，出现相关查询结果。

选择资产分布统计报表

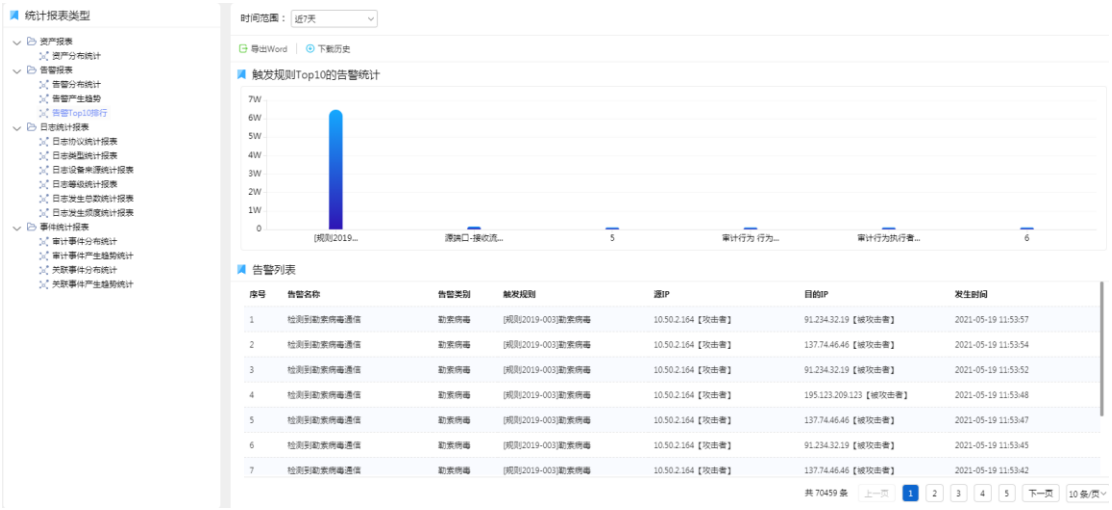
选择告警分布统计报表



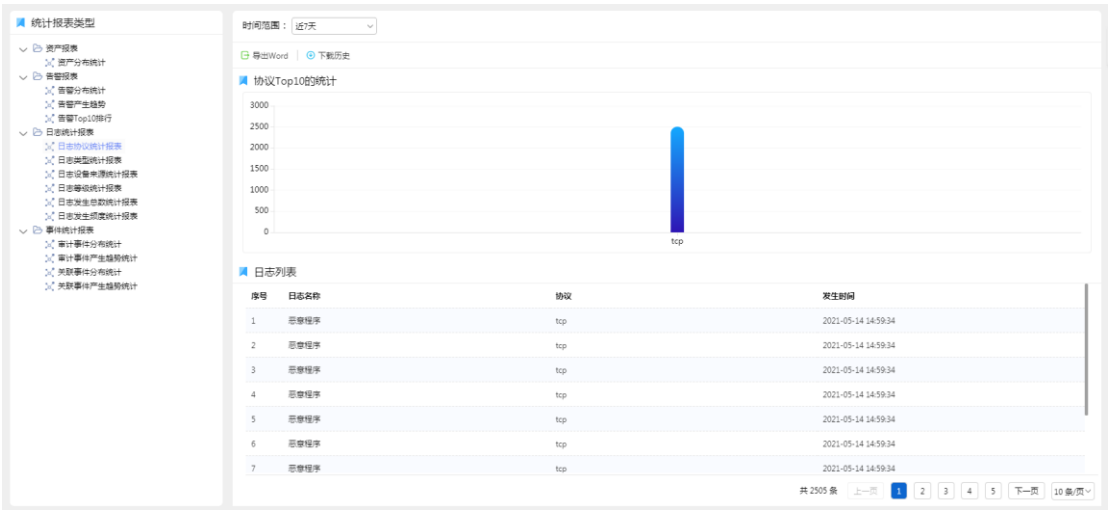
选择告警产生趋势报表



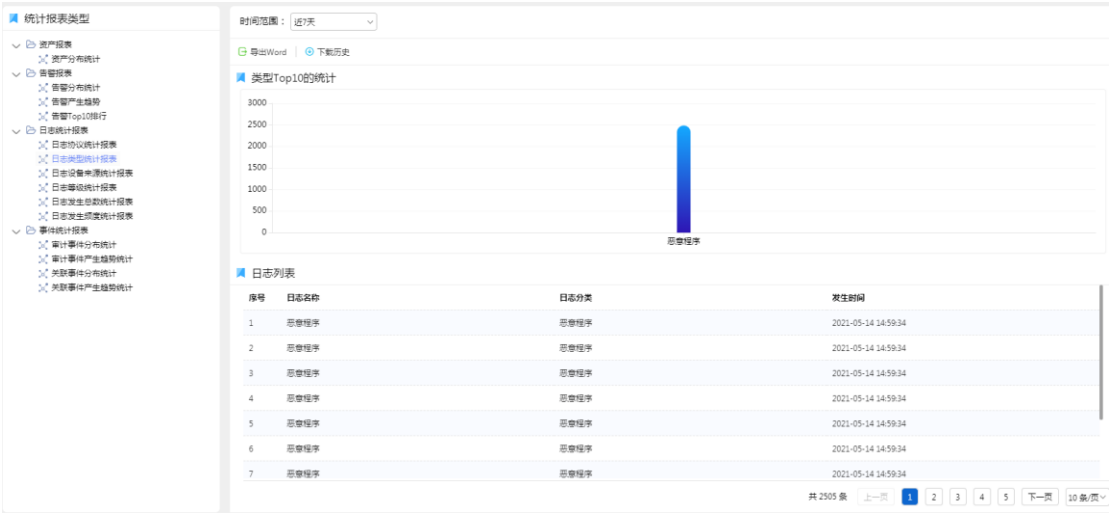
选择告警 TOP10 排行报表



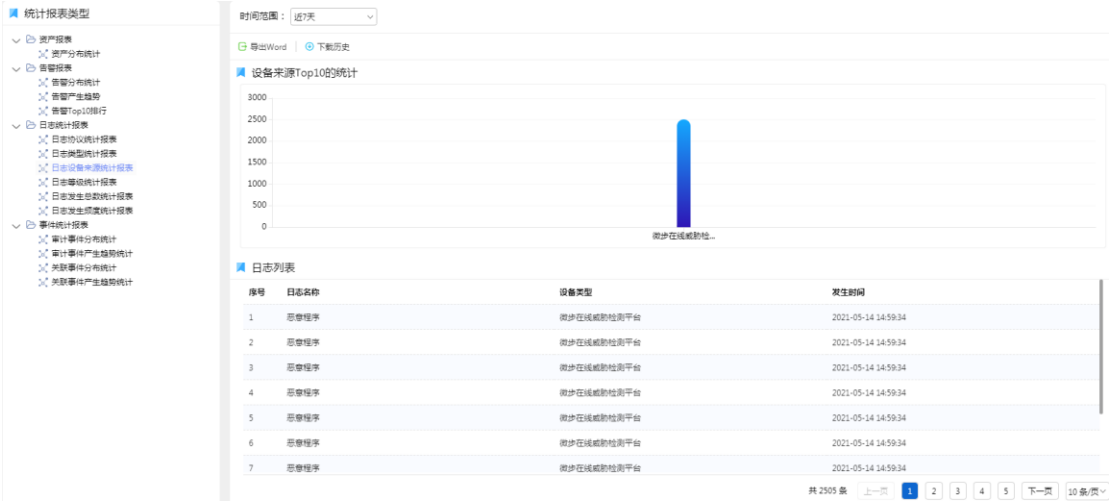
选择日志协议统计报表



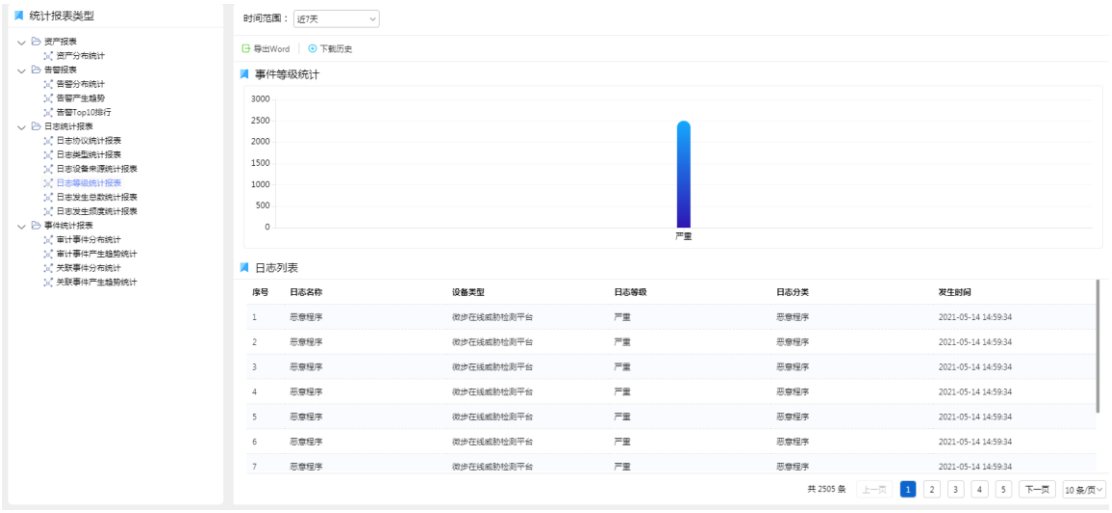
选择日志类型统计报表



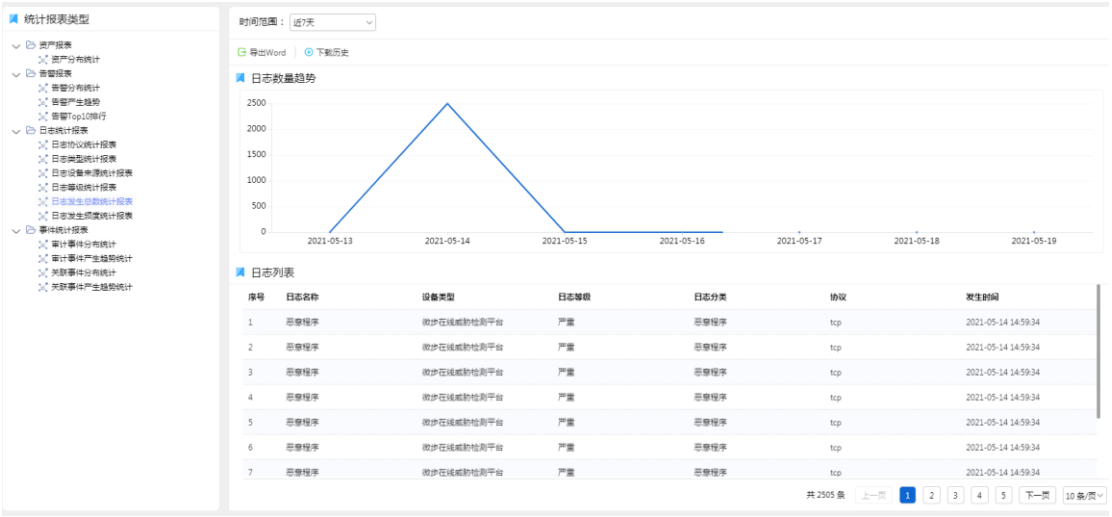
选择日志设备来源统计报表



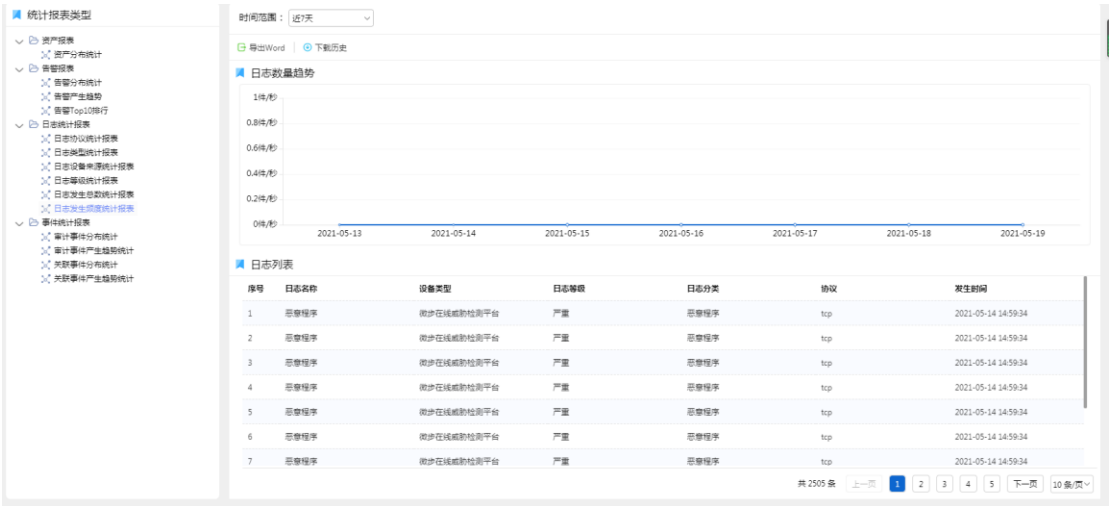
选择日志等级统计报表



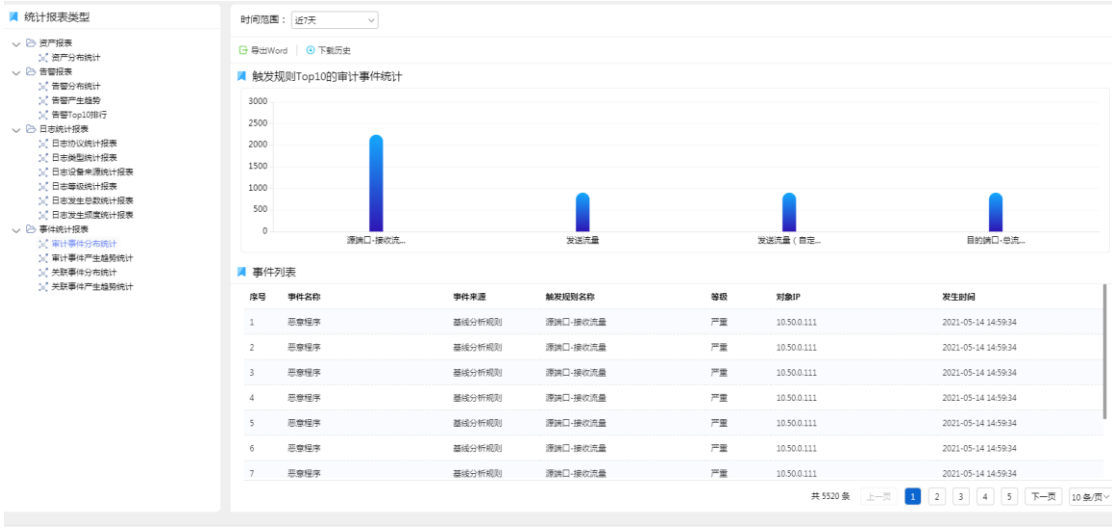
选择日志发生总数统计报表



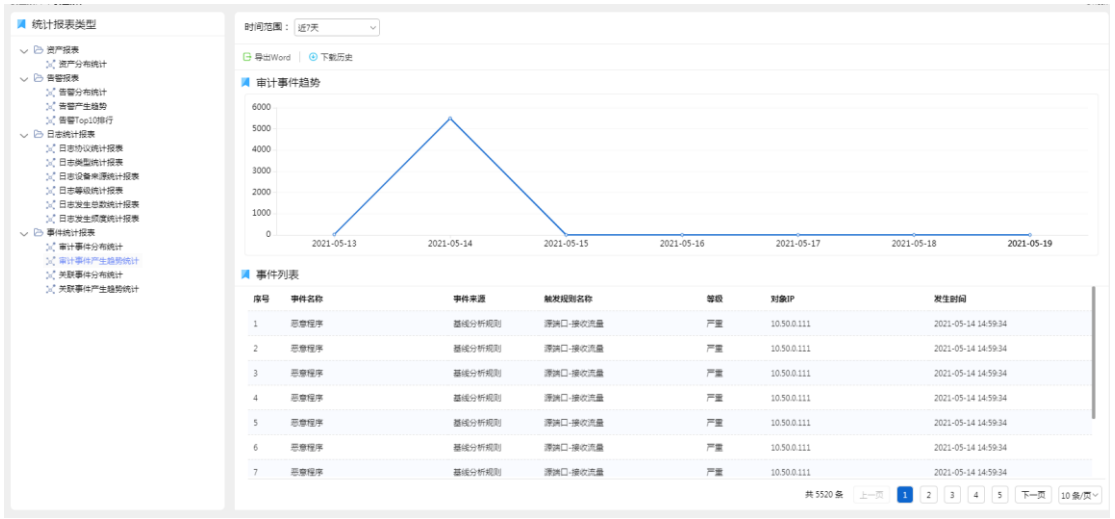
选择日志发生频度统计报表



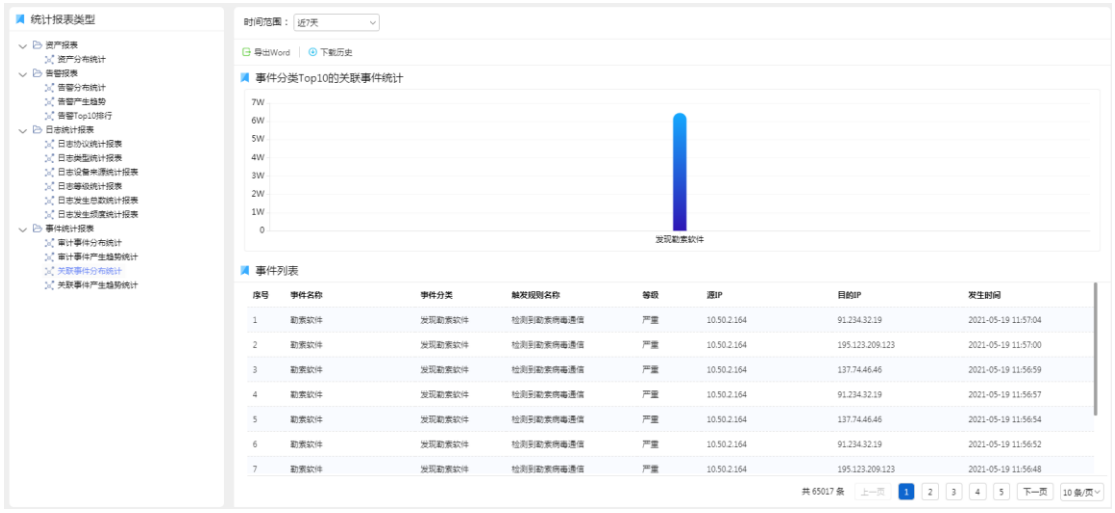
选择审计事件分布统计报表



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



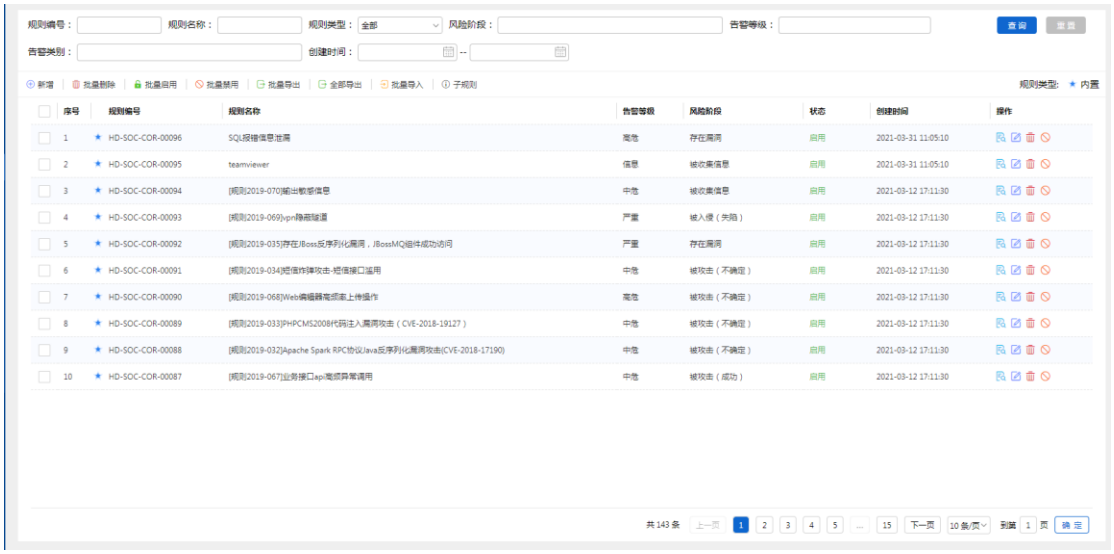
选择关联事件产生趋势统计报表

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。

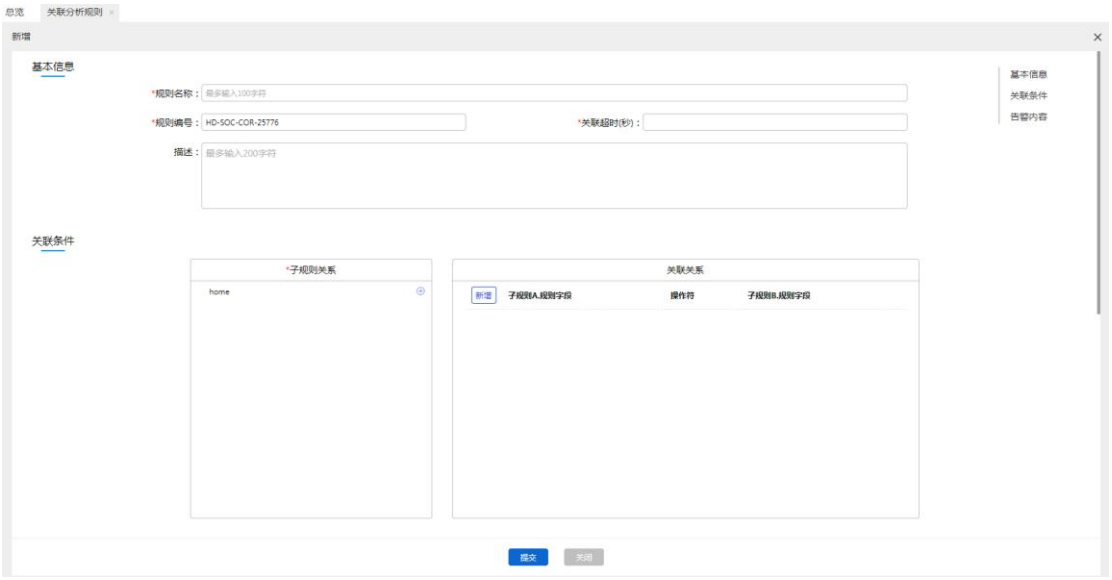
2.6 策略管理

2.6.1 关联分析规则

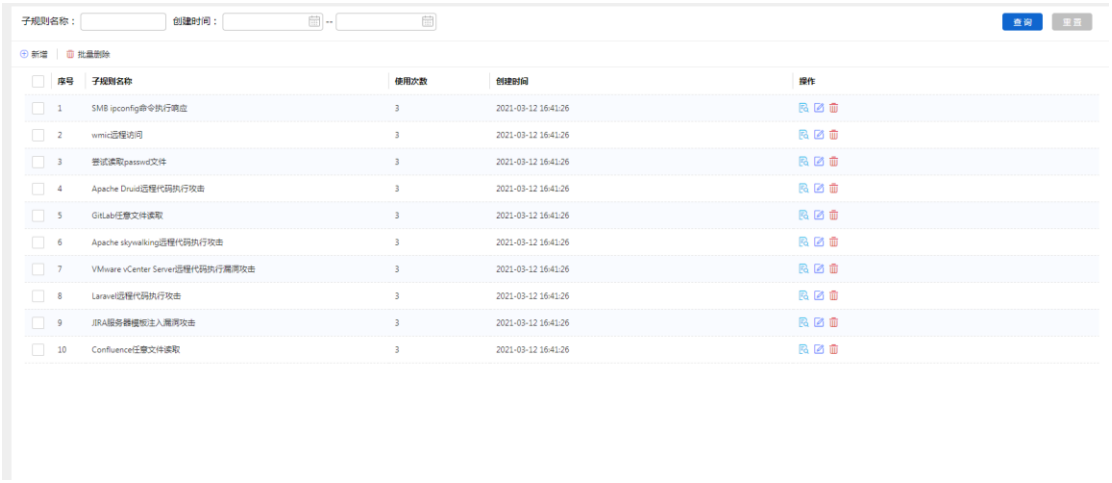
路径：策略管理->关联分析规则。



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。

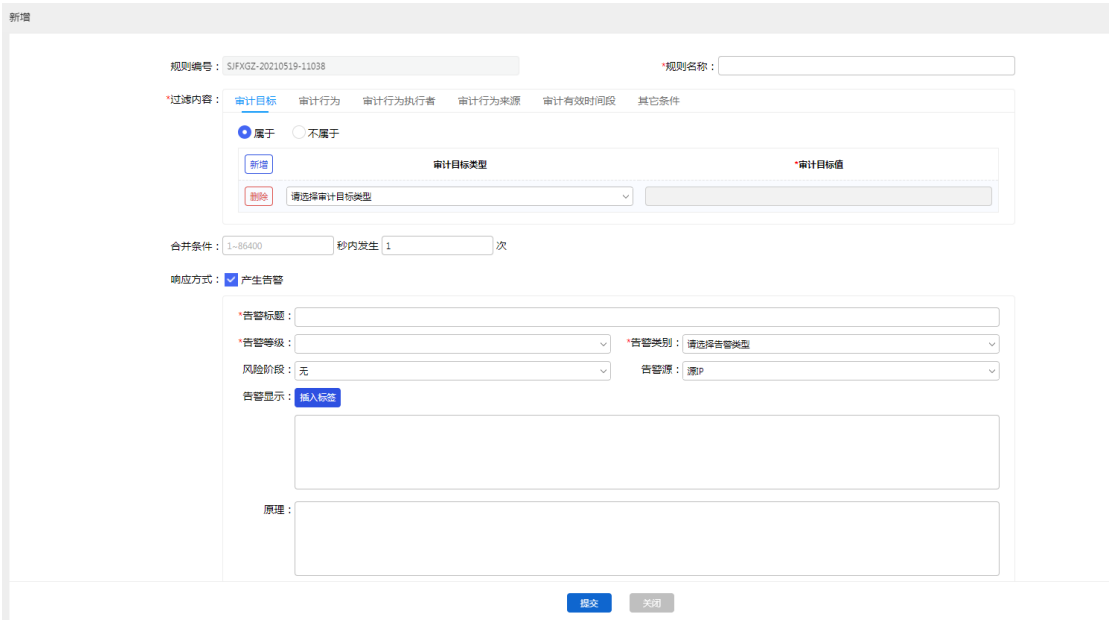
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。
点击【新增】，进入添加规则页面

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



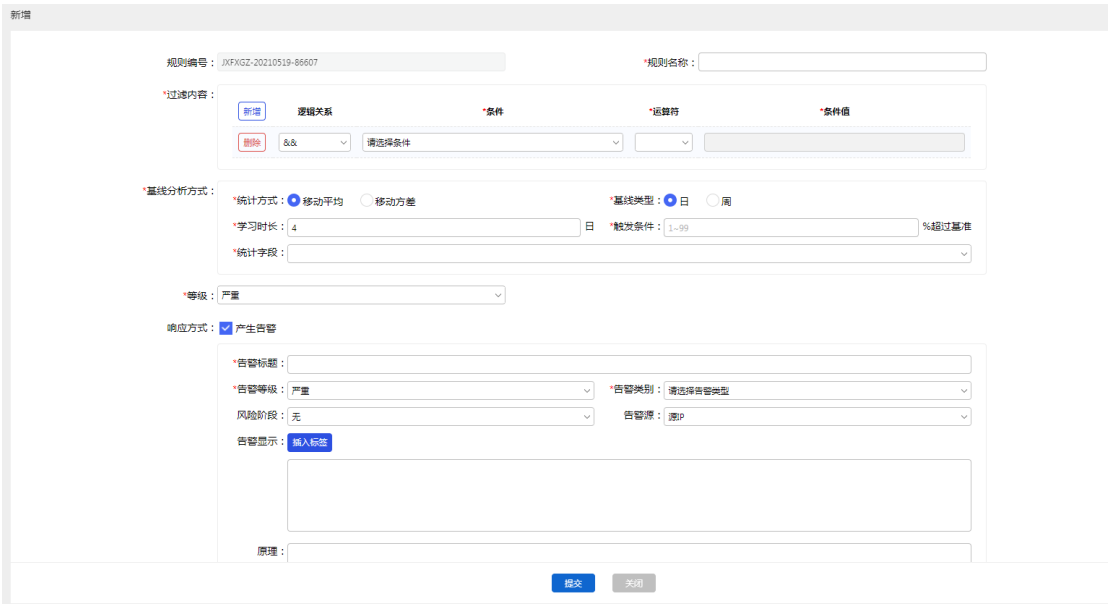
填写相关信息，点击提交，新增规则完成。
左边勾选框勾选多项，点击【批量删除】，可以批量删除选中规则。
左边勾选框勾选多项，点击【批量启用】，可以批量启用选中规则。
左边勾选框勾选多项，点击【批量禁用】，可以批量禁用选中规则。
左边勾选框勾选多项，点击【批量导出】，可以批量导出选中规则。
点击【批量导入】，可导入规则。
点击【调整规则处理顺序】，进入调整规则处理顺序页面

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。

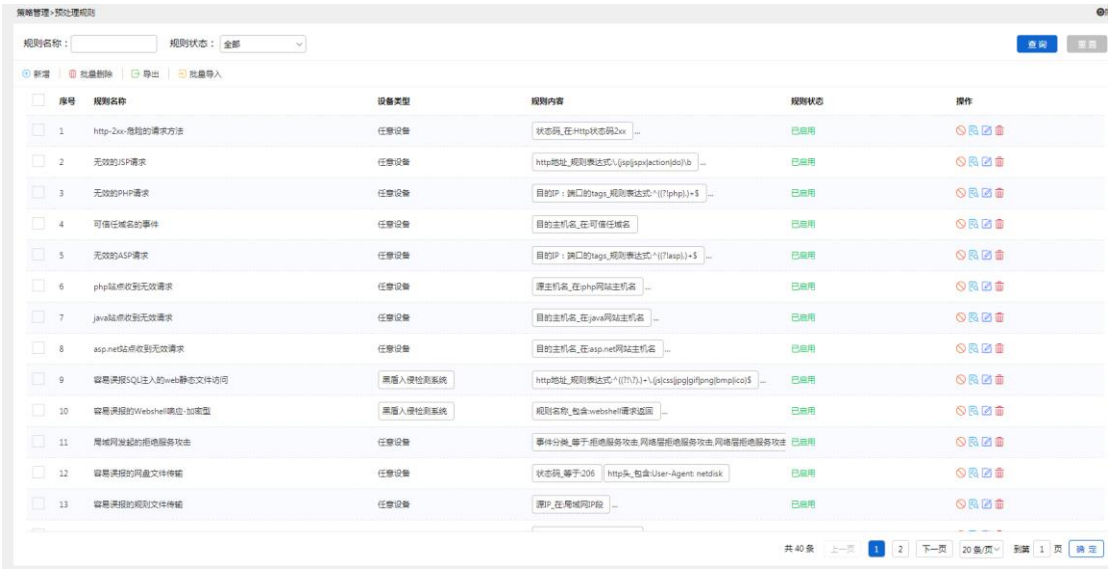
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。
点击【新增】，进入新增规则页面



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。

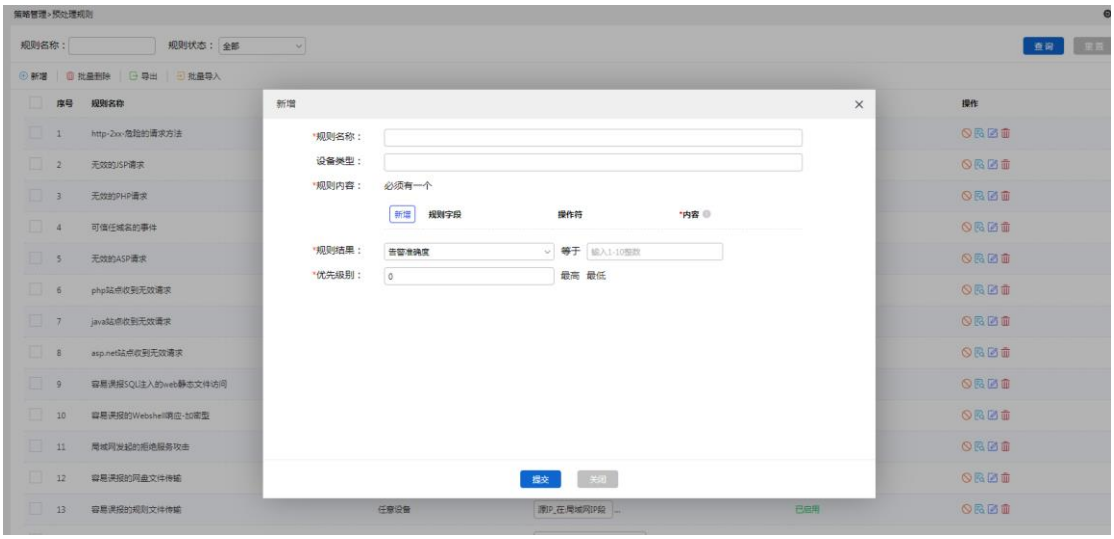
2.6.5 预处理规则

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。

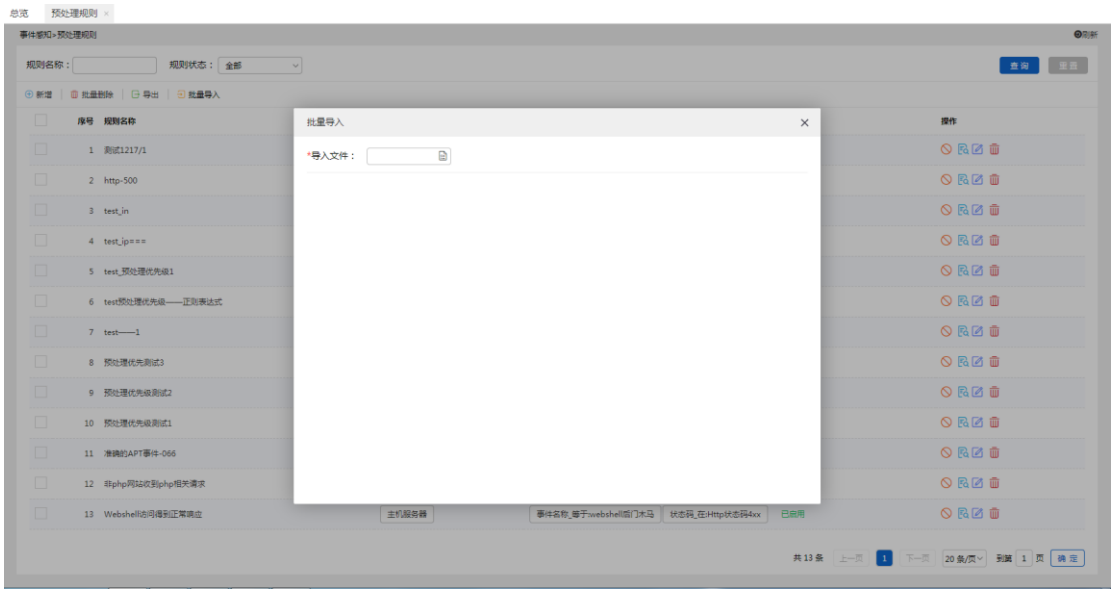
点击【新增】，进入新增页面



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

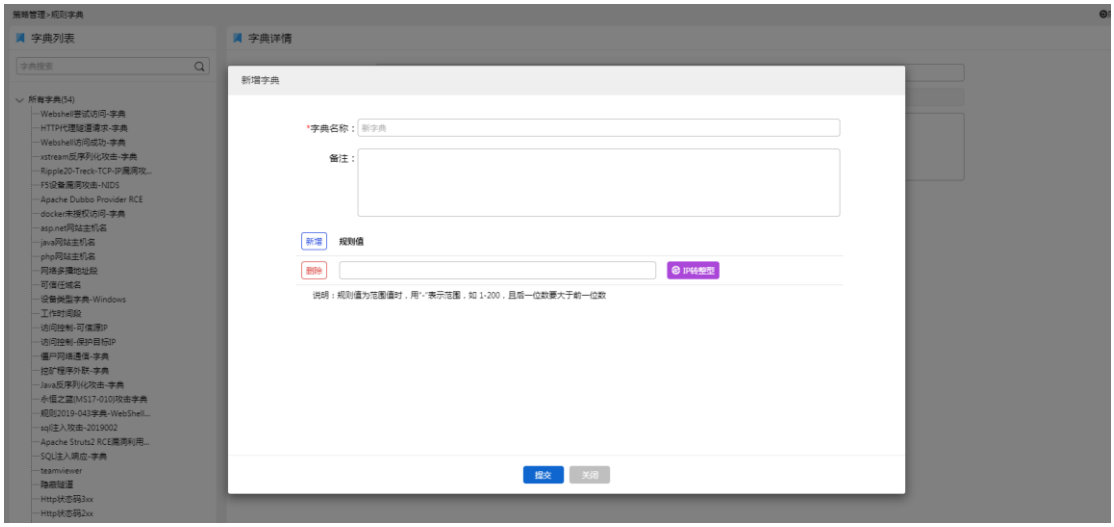


点击【导出】，可以导出规则。
点击操作中的【查看】，进入查看规则页面。
点击操作中的【编辑】进入编辑页面。
点击操作中的【禁用】，禁用规则。
点击操作中的【启用】，启用规则。
点击操作中的【删除】，删除规则。

2.6.6 规则字典

路径：策略管理->规则字典。

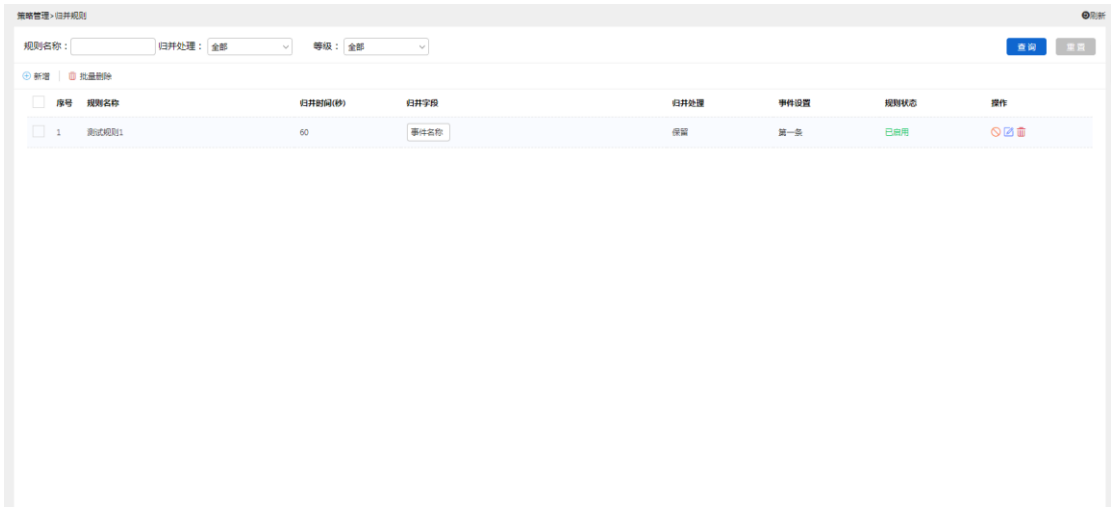
鼠标移至“所有字典”，出现【新增】，点击【新增】进入新增字典页面



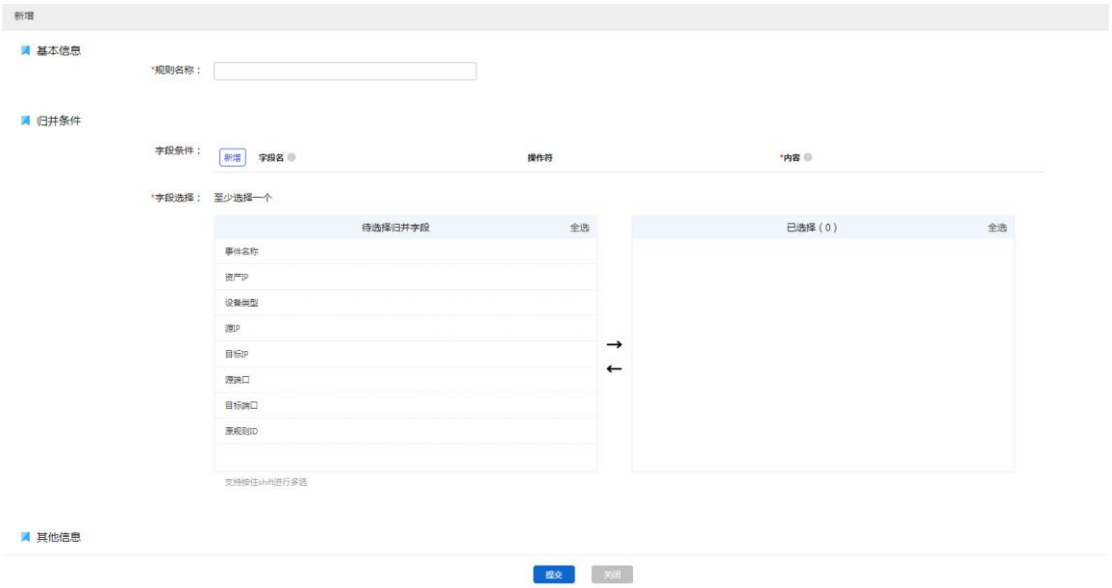
填写相关信息，点击【提交】，添加字典完成。
点击【编辑】，进入编辑页面。
点击字典名称，右边显示字典信息。
点击【删除】，删除字典。

2.6.7 归并规则

路径：策略管理->归并规则。



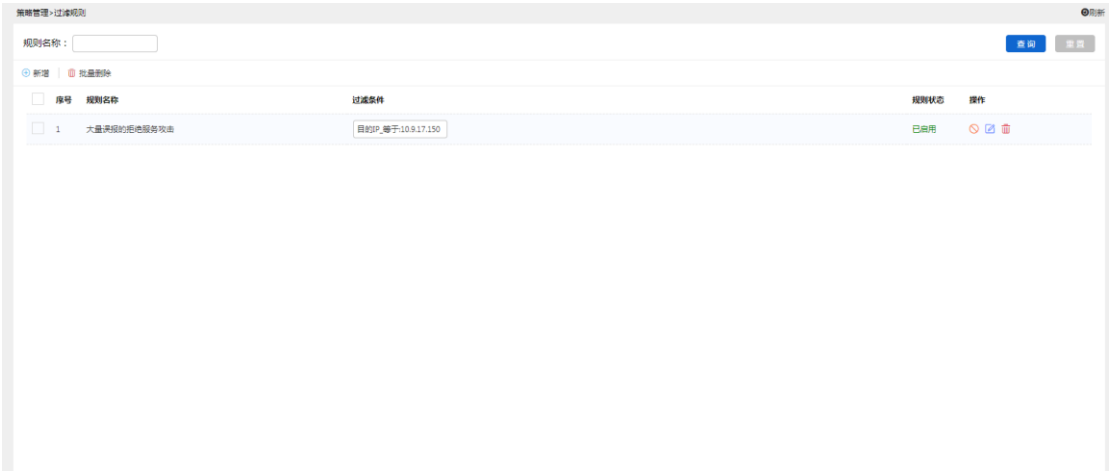
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。
点击【新增】，进入新增页面



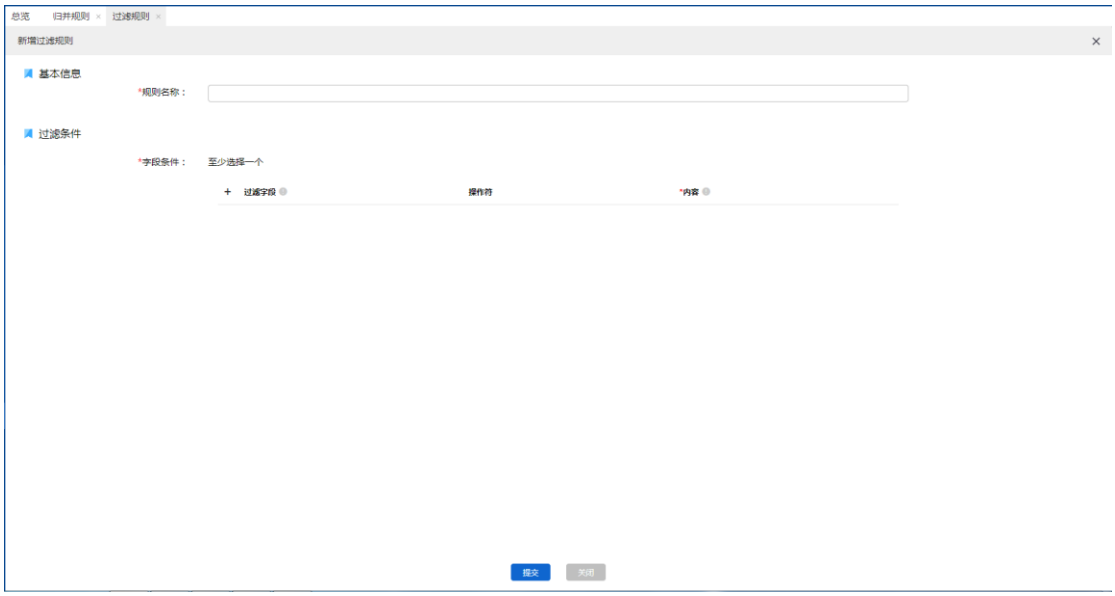
填写相关信息，点击【提交】，添加归并规则完成。
左边勾选框勾选多项，点击【批量删除】，可以批量删除规则。
点击操作中的【编辑】，进入编辑页面。
点击操作中的【禁用】，禁用规则。
点击操作中的【启用】，启用规则。
点击操作中的【删除】，删除规则。

2.6.8 过滤规则

路径：策略管理->过滤规则。



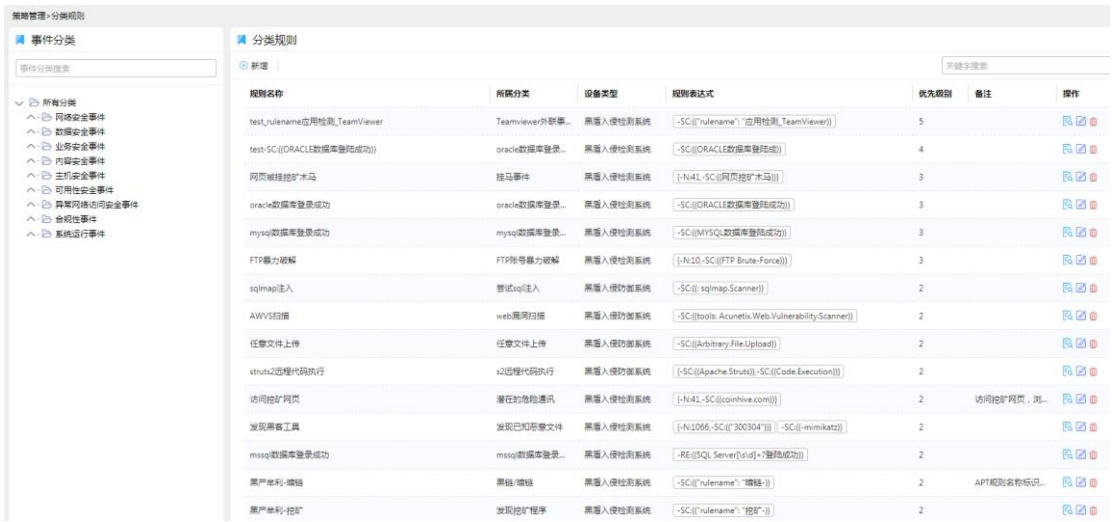
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。
点击【新增】，进入新增页面



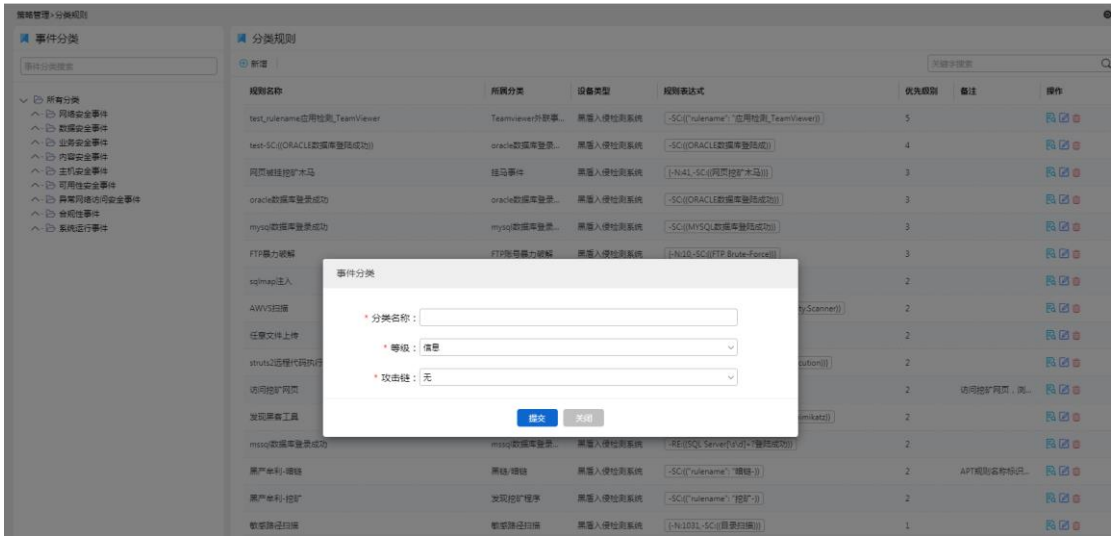
填写相关信息，点击【提交】，添加过滤规则完成。
左边勾选框勾选多项，点击【批量删除】，可以批量删除规则。
点击操作中的【编辑】，进入编辑页面。
点击操作中的【禁用】，禁用规则。
点击操作中的【启用】，启用规则。
点击操作中的【删除】，删除规则。

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



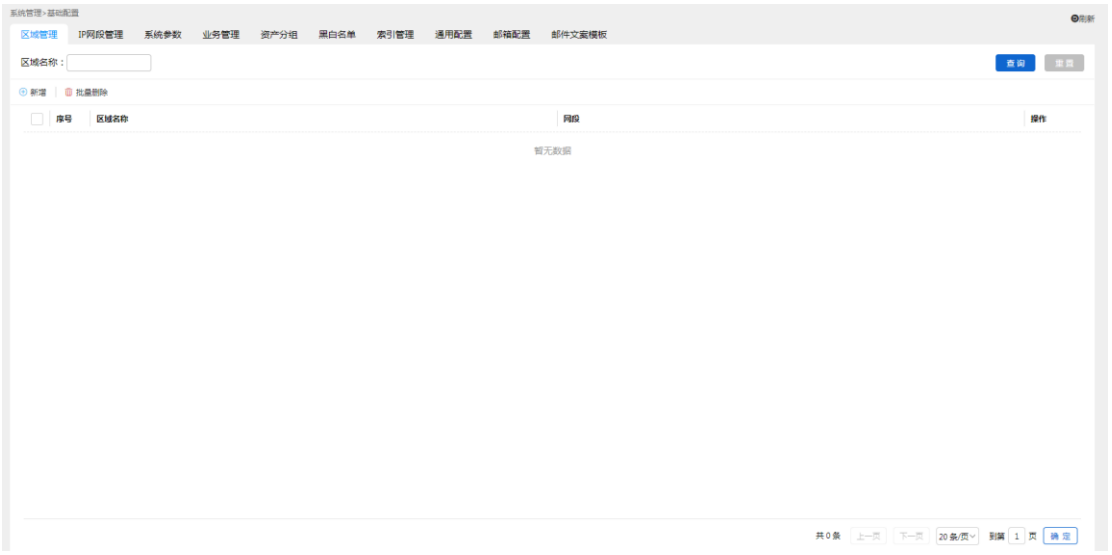
点击【编辑】，跳出事件分类编辑弹框。
点击【删除】，可删除菜单中事件分类。
点击分类规则中的【新增】，进入新增规则页面

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

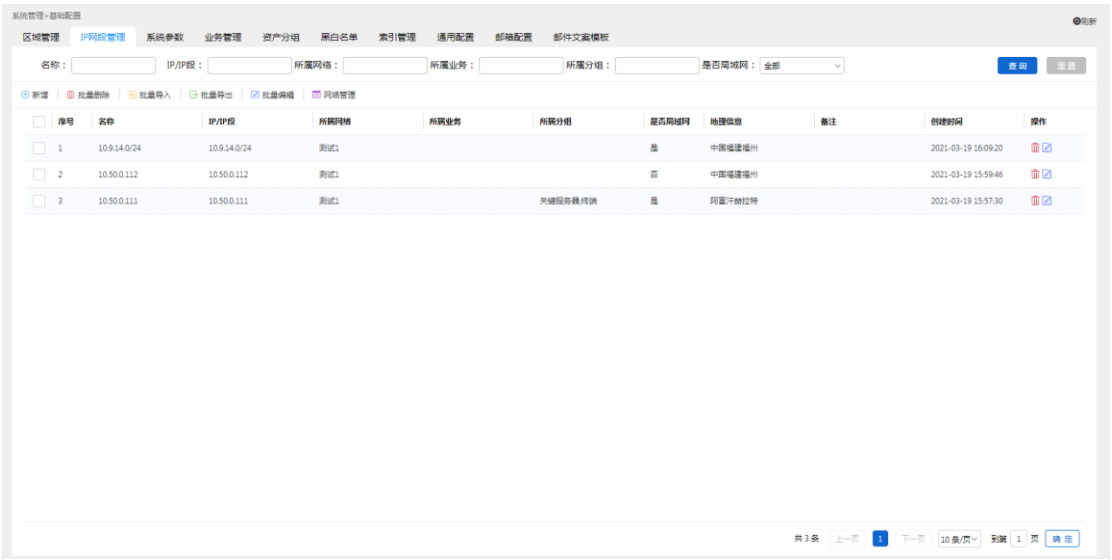
2.7.1 基础配置

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。



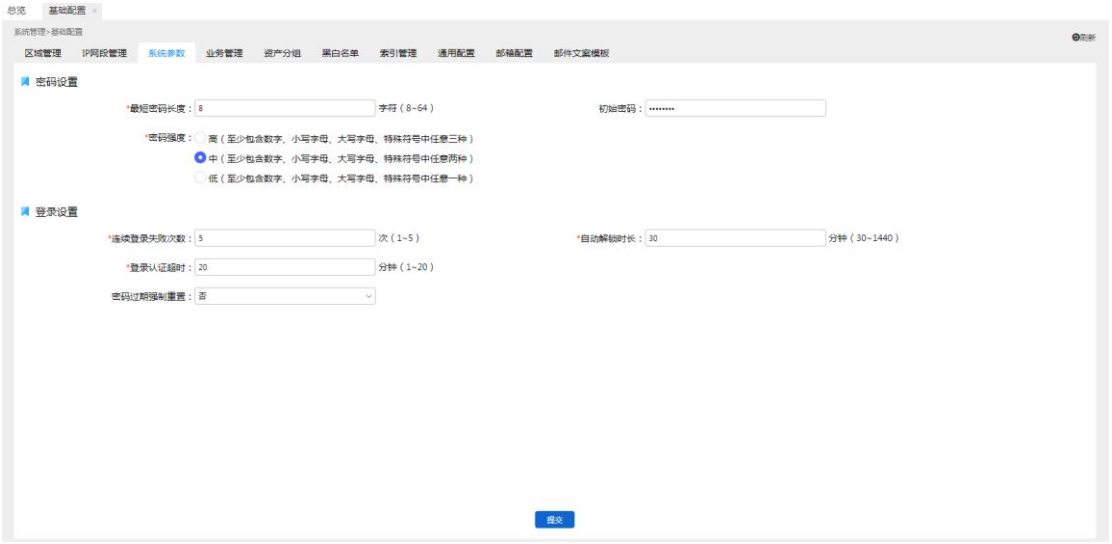
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行增删查改操作。

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。

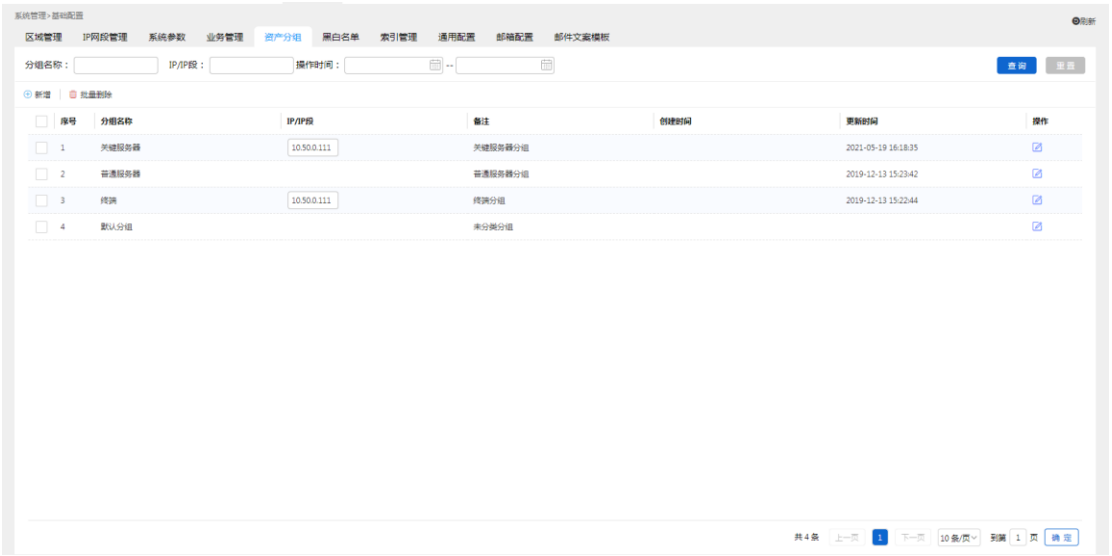


可修改系统参数，点击提交，保存信息。

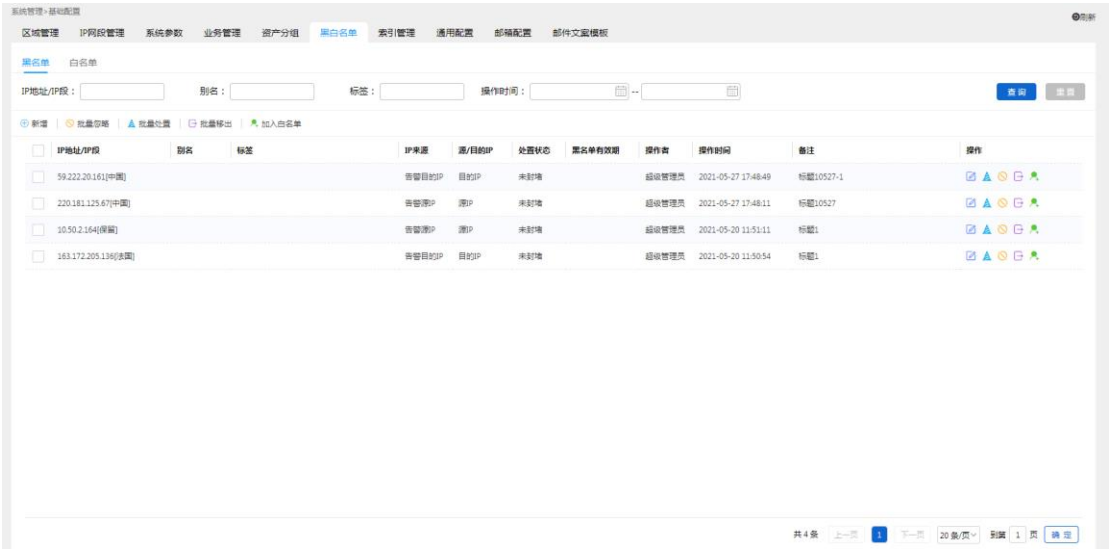
点击‘业务管理’，进入业务管理页面。

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。

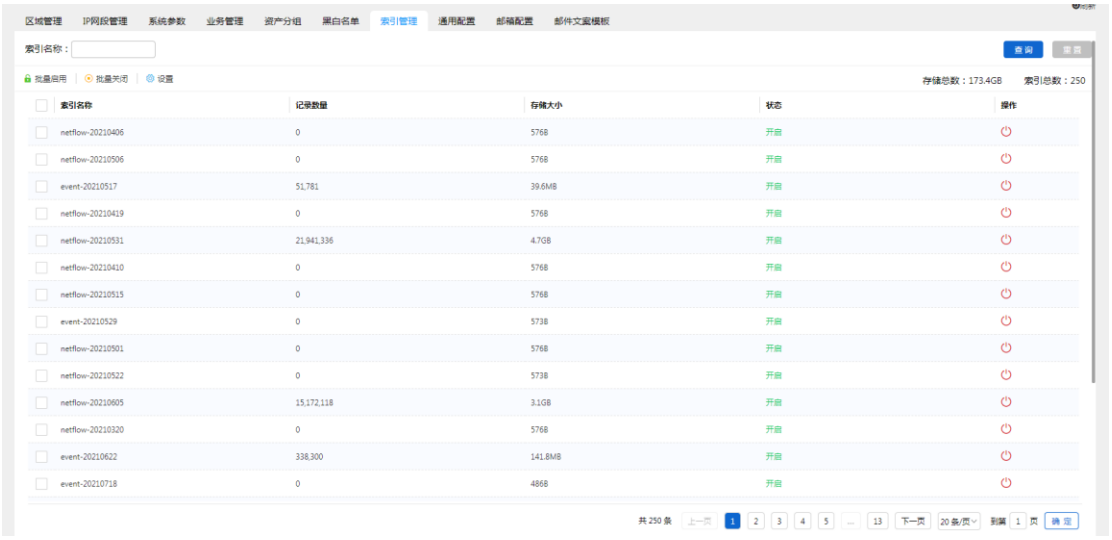
点击‘资产分组’，进入资产分组页面。



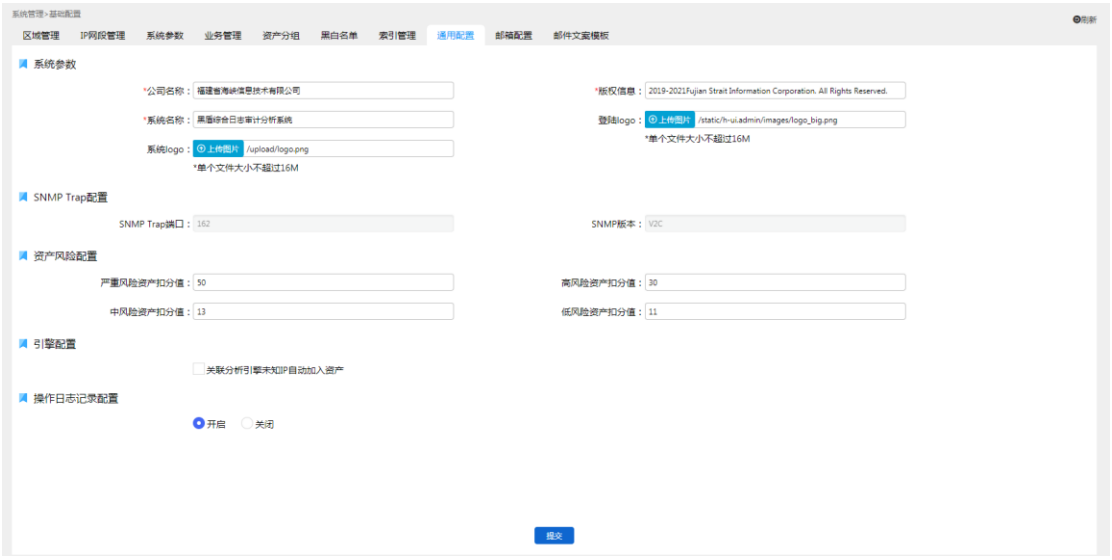
通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行增删查改操作。
点击‘黑白名单’，进入黑白名单页面。



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。

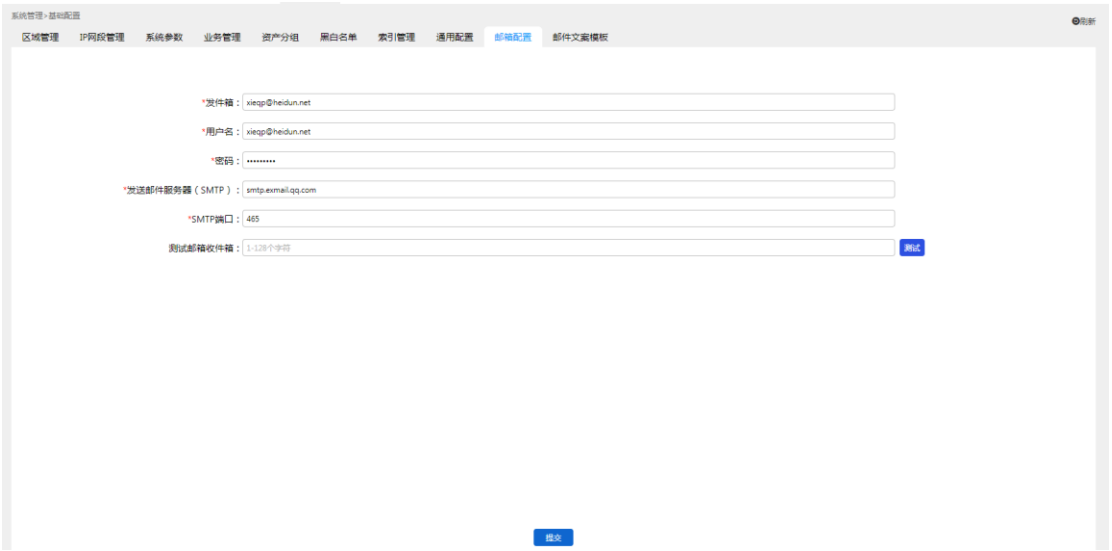


通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可进行启用、关闭及设置操作。
点击‘通用配置’，进入通用配置页面。



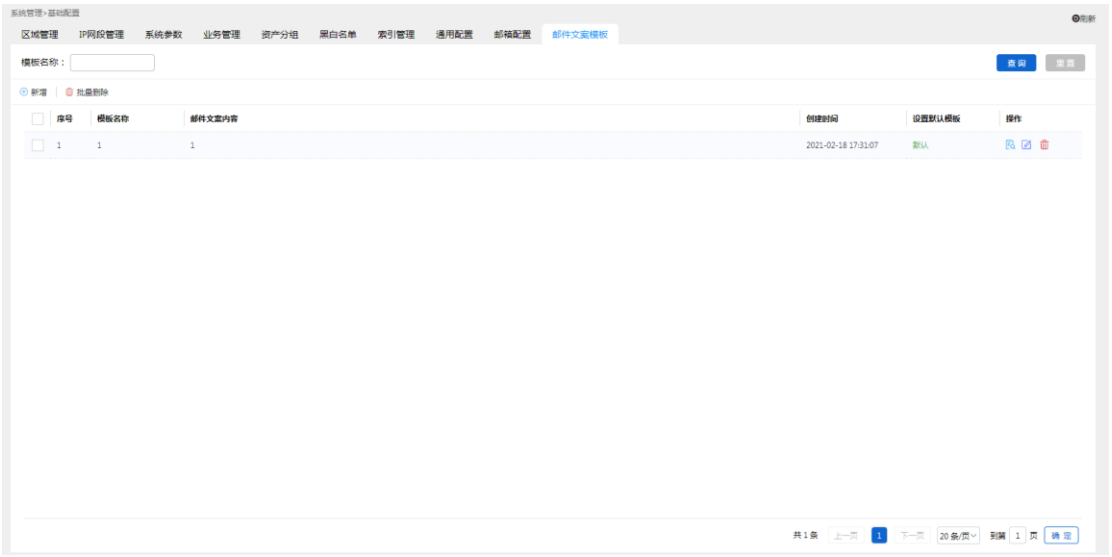
可修改通用配置，点击提交，保存信息。

点击‘邮箱配置’，进入邮箱配置页面。



可进行邮箱配置操作。

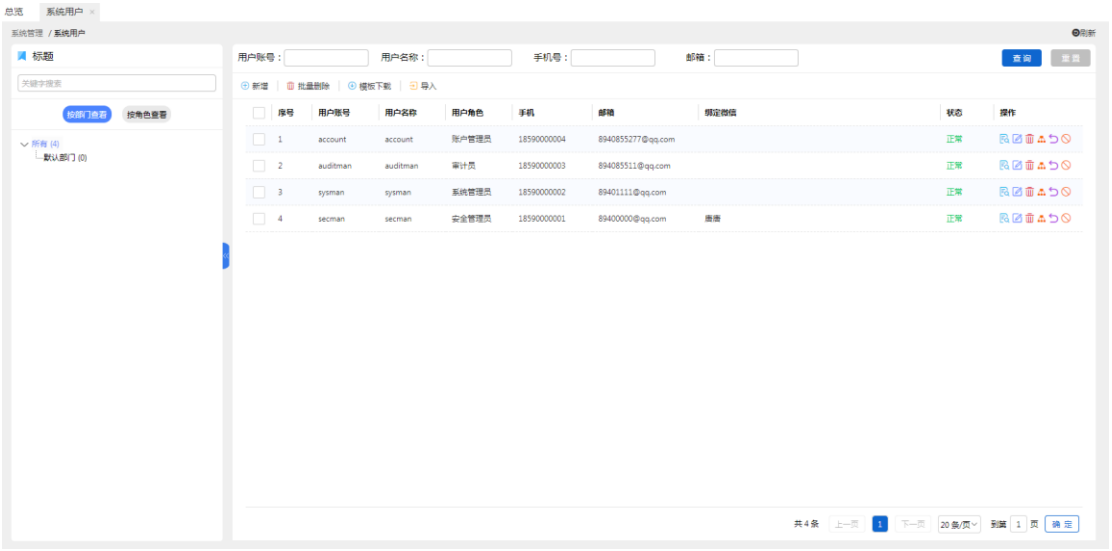
点击‘邮件文案模板’，进入邮件文案模板页面。



可进行邮件文案模板的增删查改。

2.7.2 系统用户

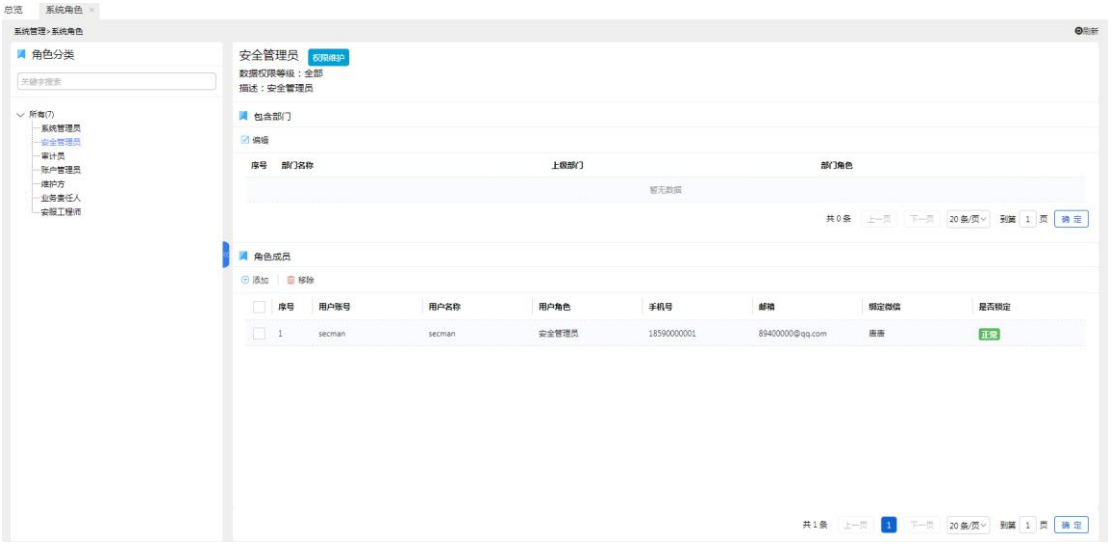
路径：系统管理->系统用户。



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

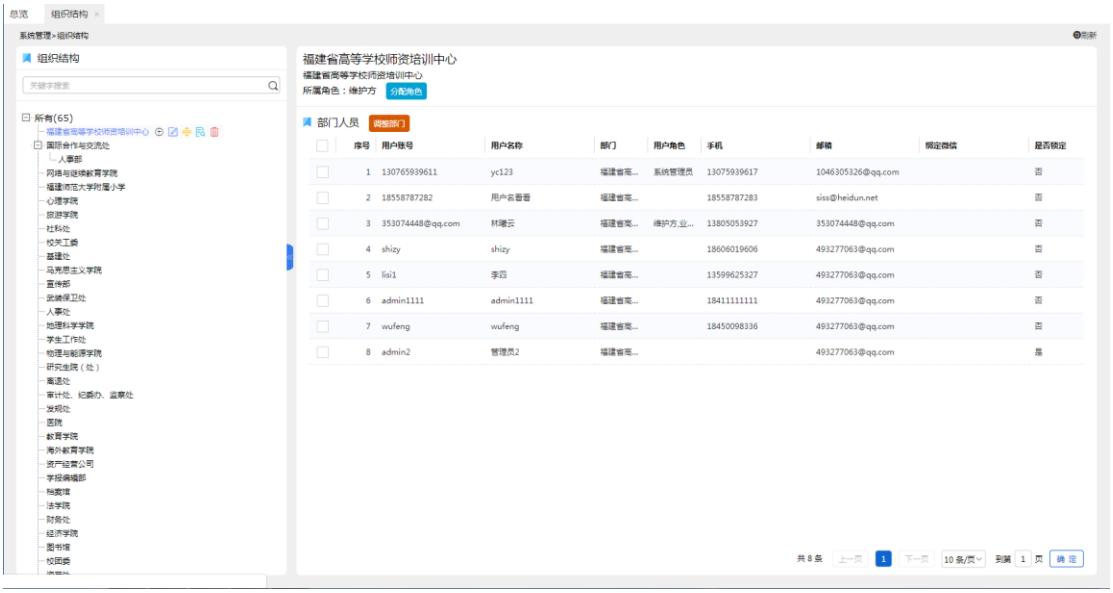
路径：系统管理->系统角色。



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

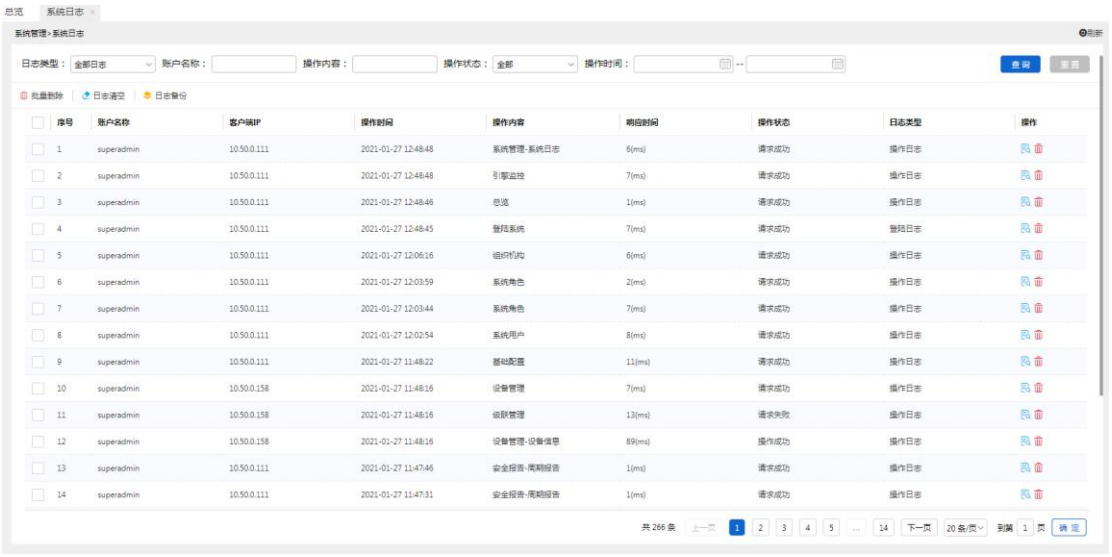
路径：系统管理->组织结构。



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

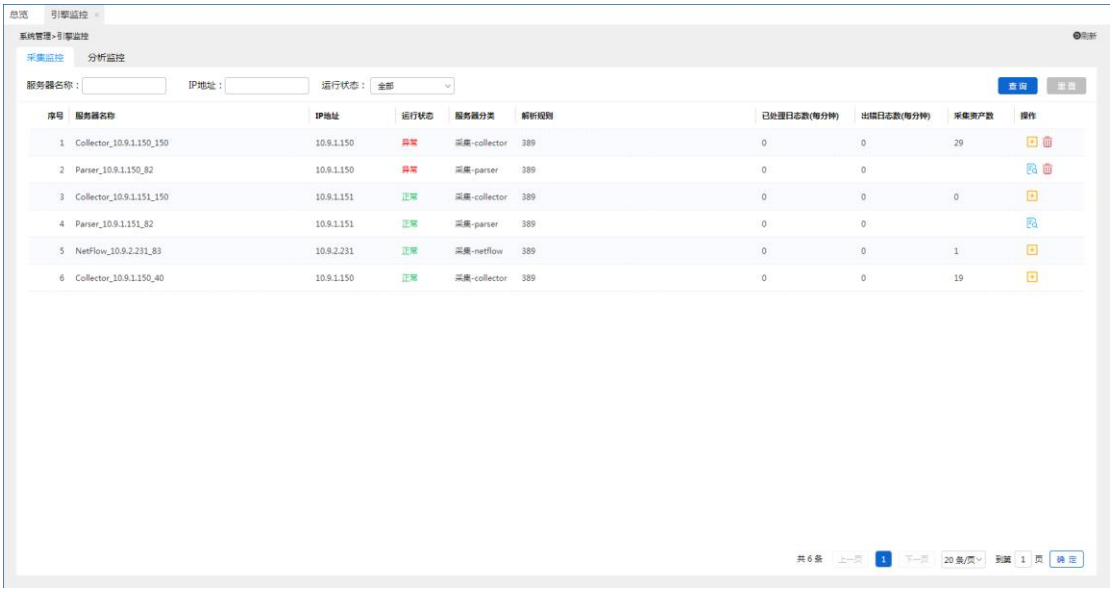
路径：系统管理->系统日志。



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。

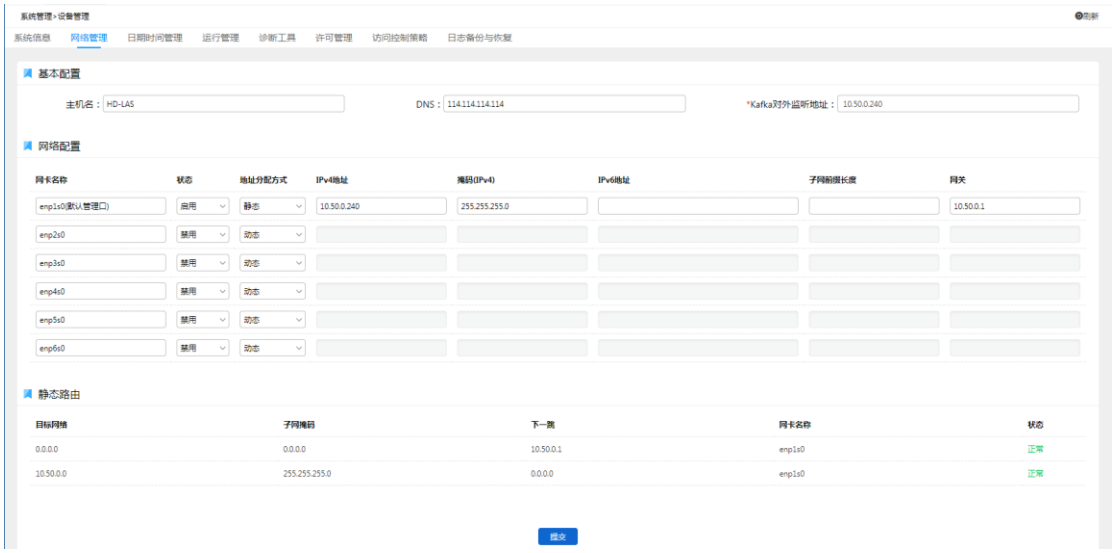


通过填写相关查询条件，点击【查询】，出现相关查询结果；点击【重置】，查询条件内容清空。可在此进行添加、查看及删除操作。

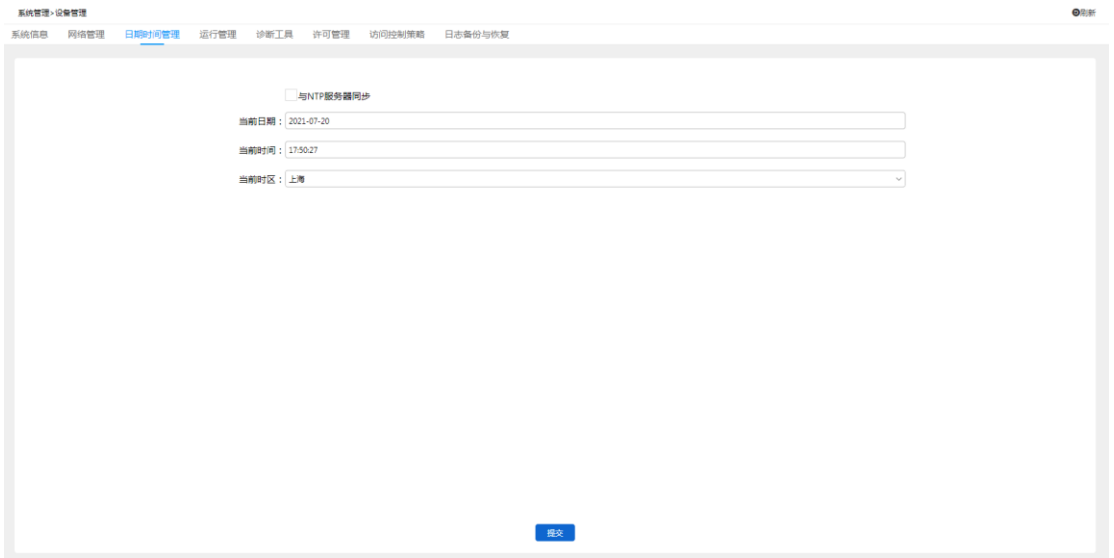
2.7.7 设备管理

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。

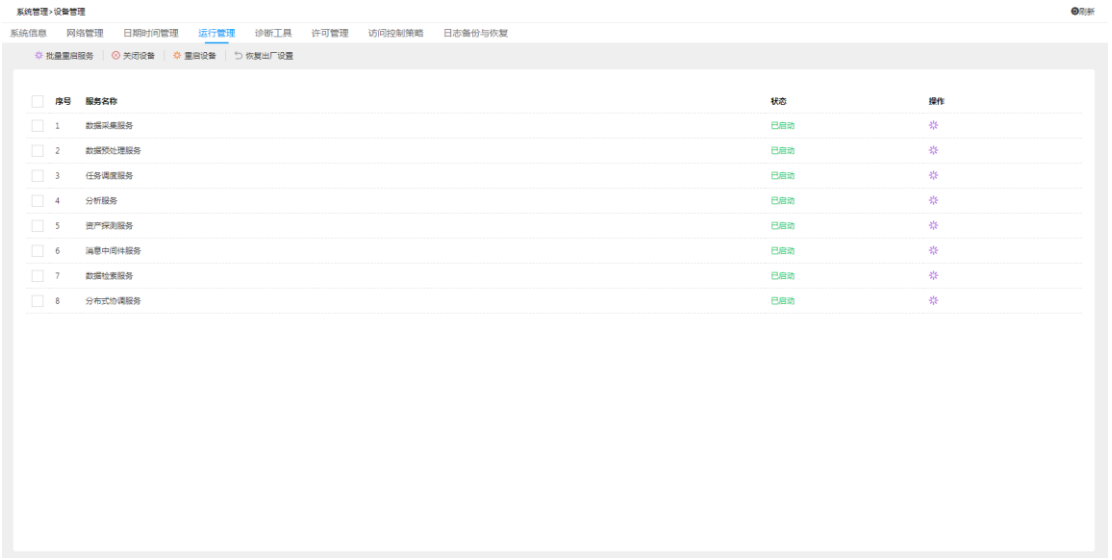
点击‘网络管理’，进入网络管理页面，可继续网络配置和查看路由信息。



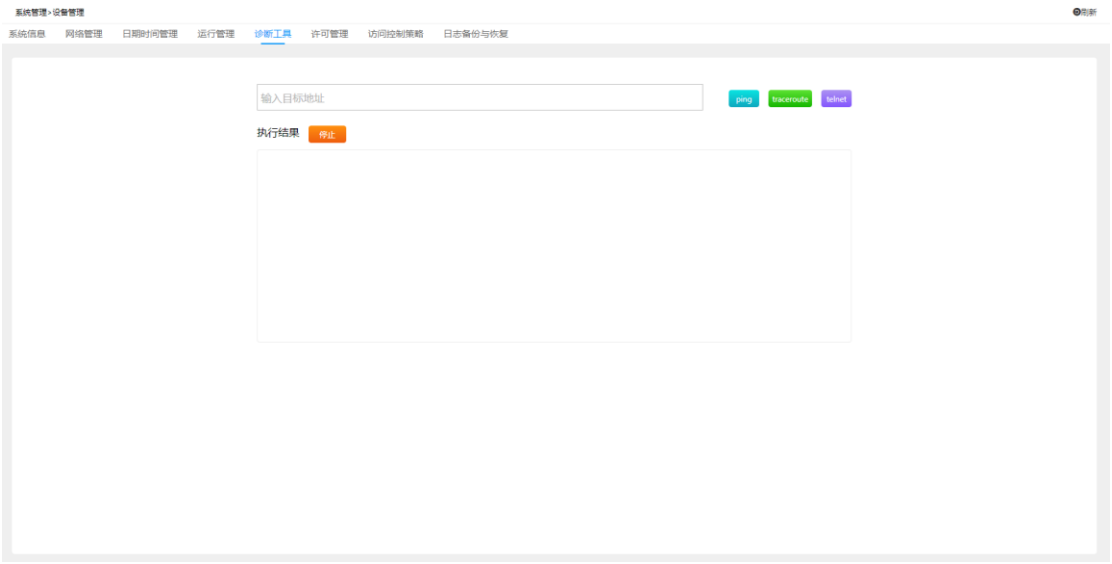
点击‘日期时间管理’，进入日期时间管理页面，填写内容，点击【提交】，日期时间设置完成。



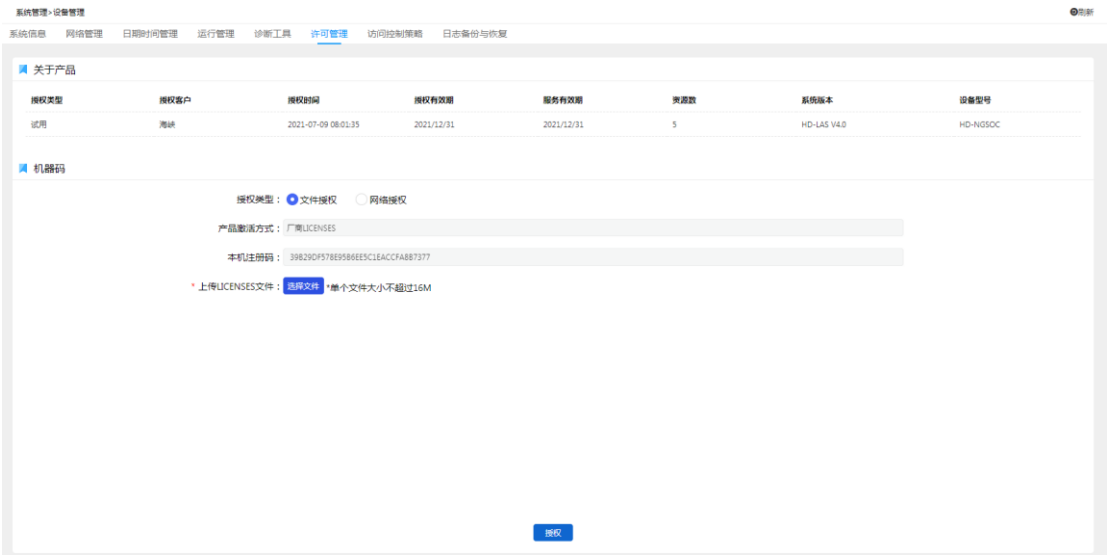
点击‘运行管理’，进入运行管理页面，可查看服务信息，并进行重启服务、重启设备及恢复出厂设置等操作。



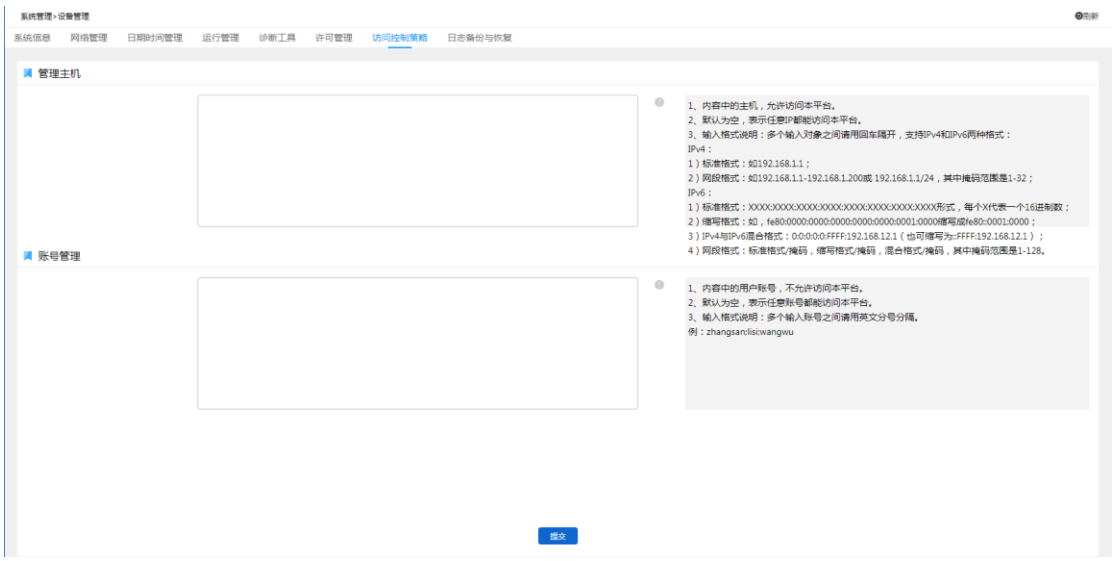
点击‘诊断工具’，进入诊断工具页面。



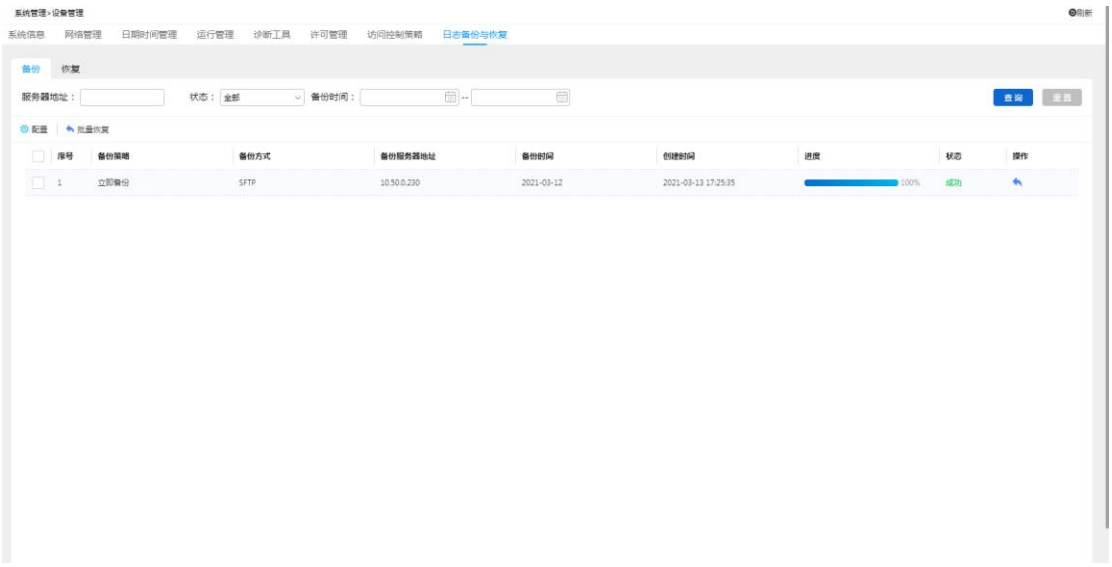
点击‘许可管理’，进入许可管理页面，可查看产品相关内容，并进行本地授权或网络授权。



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
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
1
立即备份
SFTP
10.50.0.230
2021-03-12
2021-03-13 17:25:35
100%
成功