中科云量安全综合管理平台 V1.0

操作手册

广东中科云量信息安全技术有限公司

免责条款

1、本文档是广东中科云量信息安全技术有限公司相关工作人员依据现有信息制作，在编写该文档时候已尽最大努力保证其内容准确可用，广东中科云量信息安全技术有限公司及其员工将不对本文档中任何内容直接或间接导致第三方的损失和损害承担任何责任。

2、本文档是用户实际安装过程中的指南和使用参考手册，本文档的部分内容可能随产品型号和规格的不同而略有区别，不会影响对本文档的理解。中科云量有权利在不通知用户的情况下对产品和手册进行修改。

目 录

第 1 章 引言

1.1 文档范围

本文档将详细介绍如何安装及使用中科云量安全综合管理平台 V1.0，用户可以通过文档的相关指导对中科云量安全综合管理平台 V1.0 进行有效的安装、配置、使用及管理。

通过阅读本文档，用户可以独立完成以下操作：

1、顺利安装及登录中科云量安全综合管理平台；

2、对安全设备进行集中管理；

3、接收并存储设备发过来的日志；

4、配置安全策略；

5、集中管理安全事件和告警；

1.2 用户对象

本文档适用于具有一定网络安全知识的人员使用，对以下几个方面的知识有一定的了解：

1、信息安全管理知识；

2、SYSLOG 日志采集方式；

3、BDSEC 管控操作和 SNMP 协议；

4、正则表达式规则；

1.3 格式约定

本文档使用以下格式约定进行描述图形界面的相关操作：

1、按钮名称或菜单名称的格式约定为：【XXX】

2、点击或选择一个菜单项的格式约定为：XXX>XXX > XXX

3、命令或关键字的格式约定为：***粗体且斜体的字词***

4、关于**建议**、**说明**、**重要信息**使用以下图标约定：

建议：  说明：  重要信息： 

第 2 章　产品综述

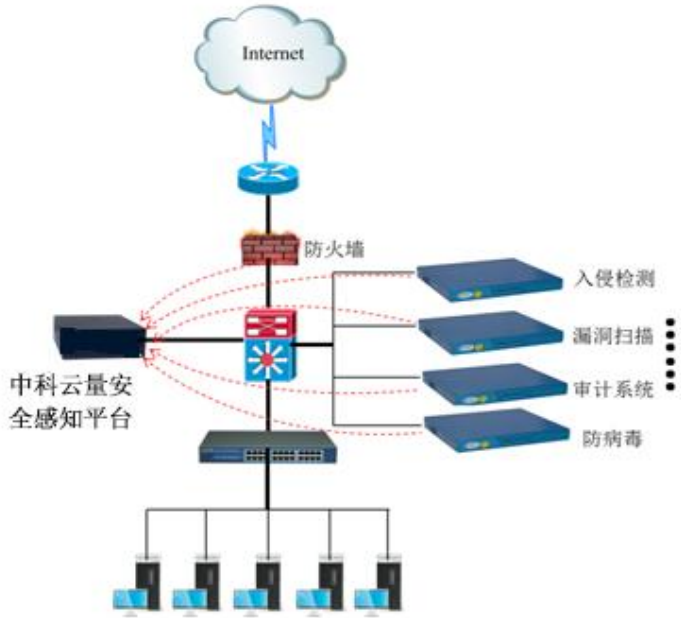
2.1 系统简介

中科云量安全综合管理平台 V1.0 是协助用户实现安全事件管理、安全策略管理、安全组织管理、安全运作管理和安全技术框架的中心枢纽。中科云量安全综合管理平台 V1.0 是一种安全管理的形式，它分为管理层面的职能和技术层面的职能，它能有效地将企业的策略管理、安全组织管理、安全运作管理和安全技术框架结合在一起，保持一致性。

2.2 部署方式

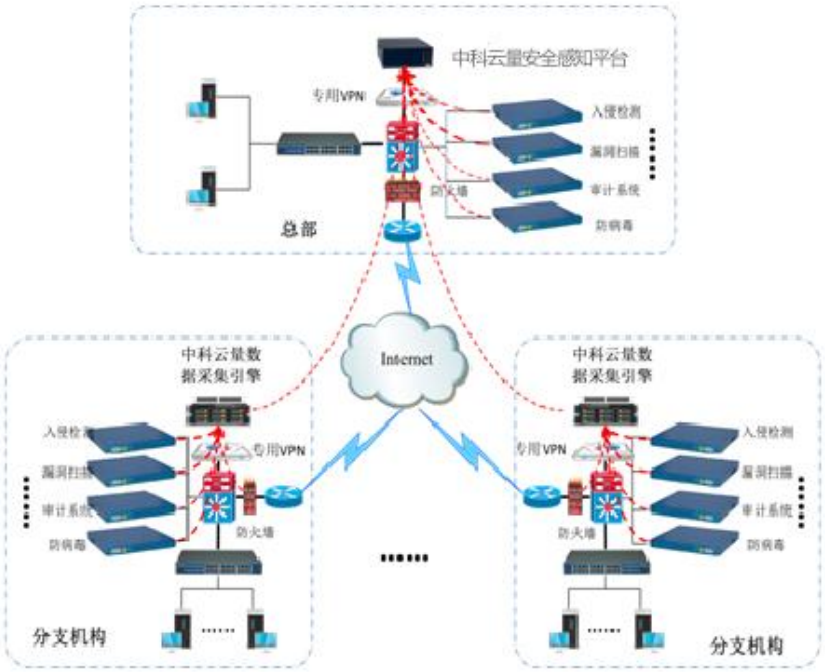
2.2.1 本地集中部署

在本地网络部署中科云量安全综合管理平台，系统自动实时接收来自本地网络内各类安全系统的安全威胁日志，通过在中科云量安全综合管理平台上制定的安全策略进行威胁分析，并结合信息资产的安全保护等级进行智能化的综合关联分析，科学合理的定义事件的性质和处理级别，具备网络监控防护和预警告警的能力，能够定时提供网络运维报告和安全分析报告。



2.2.2 分布式部署

在本地网络中部署一台中科云量安全综合管理平台，在分支端部署中科云量数据采集引擎，集中收集本地和远程的日志信息，做出综合分析、过滤和归纳，从而做出风险评估，判断是否发生网络安全事件，并发出报警和下发策略，最后以可视化的方式输出相关的报表信息。



第 3 章　登录注销

3.1 登录

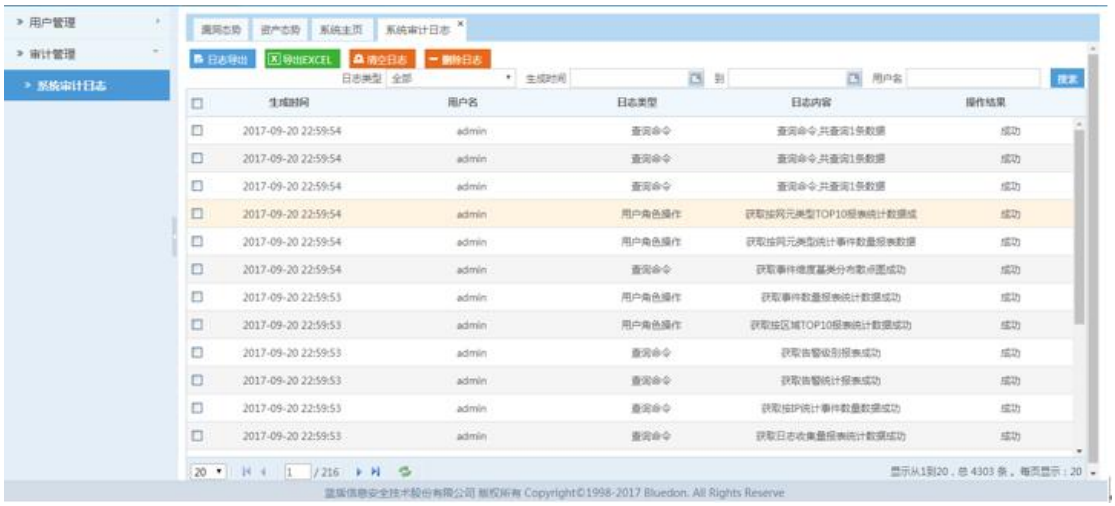
中科云量安全综合管理平台采用 B/S 架构，通过浏览器登录进行操作管理，为了获得最佳的页面浏览效果，建议您使用 Google Chrome 版本 53.0.2785.143 m 及以上版本的浏览器（安装最新的 Flash 插件），推荐显示分辨率 1440 × 900 以上效果最好。

网线接上 LAN1 口，在浏览器地址栏输入中科云量安全综合管理平台的 Web 服务器的 IP 地址 https://192.168.0.1，出现登录窗口，如上图所示，初始用户名：admin，密码：Admin_1234。

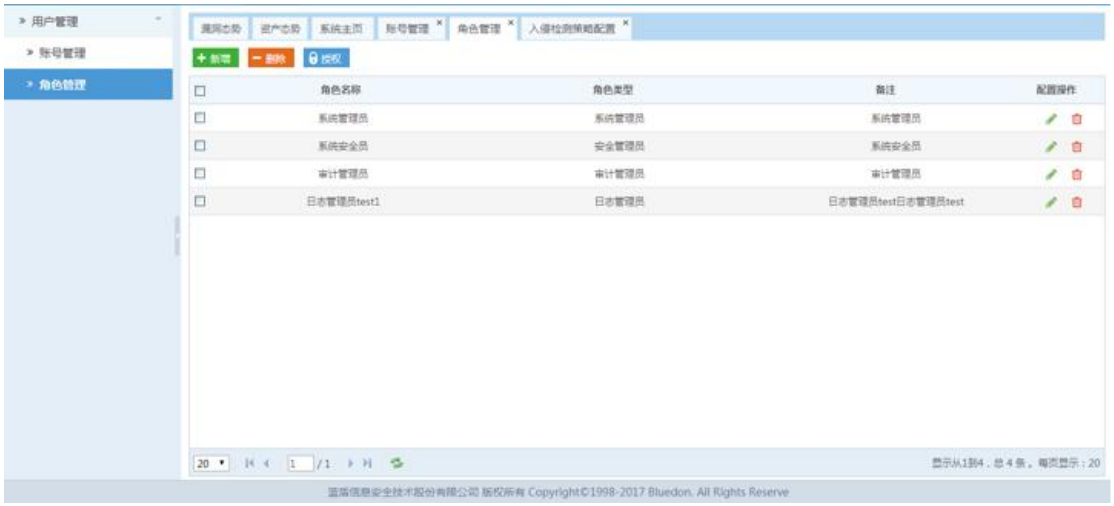
如果连续 5 次登录失败，则该登录 IP 地址将被锁定默认的 5 分钟。

一个密码连续使用 7 天及以上，会要求重置密码，输入新设置的密码才可登录。

安全审计员只能查看主页和系统审计日志而不能进行任何修改配置的操作，如下图：



安全管理员可以对用户进行账号管理和角色管理，如下图：



系统管理员登录成功后，进入管理界面：

1.整个界面划分为9个功能块，即左上侧的产品Logo图标，上方的功能菜单列表，右上方的登录信息，左侧的详细功能选项菜单，右侧中间、功能菜单列表下面的选项卡列表。

2.功能菜单列表：所有的操作管理页面都可以通过上方的功能菜单点击进入。

3.2 注销

点击右上侧  注销当前账户按钮，可以退出管理界面，退回登录界面。

3.3 管理员

中科云量安全综合管理平台采用三员分立的方式来管理系统：

安全审计员：账号--audit,密码--Admin_1234

系统管理员：账号--admin，密码--Admin_1234

安全管理员：账号--security，密码--Admin_1234

其中：

系统管理员:主要负责系统的各种配置，以确保系统能正常的运行；

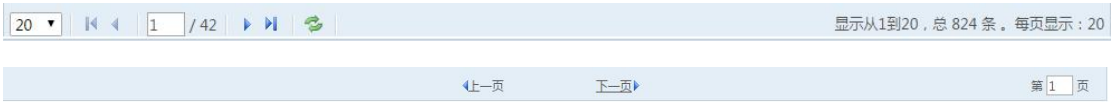
安全管理员:可以创建不同的系统管理员，并对系统管理员分配不同的权限和对设备进行策略配置；

安全审计员:可以审计各管理员的操作行为。

 按F11键可以让浏览器进入全屏浏览模式，提供更大的操作界面。

通用菜单、按钮介绍：

◆ **翻页功能**



如上两图所示，在以列表显示的页面中，当前的页数，可以通过以下操作进行页面选择：

1. 填写  页数，可直接跳转到指定页面；
2. 点击  表示跳到首页；
3. 点击  或者  上一页表示跳到上一页；
4. 点击  或者下一页  表示跳到下一页；
5. 点击  表示跳到末页。

第 4 章　系统主页

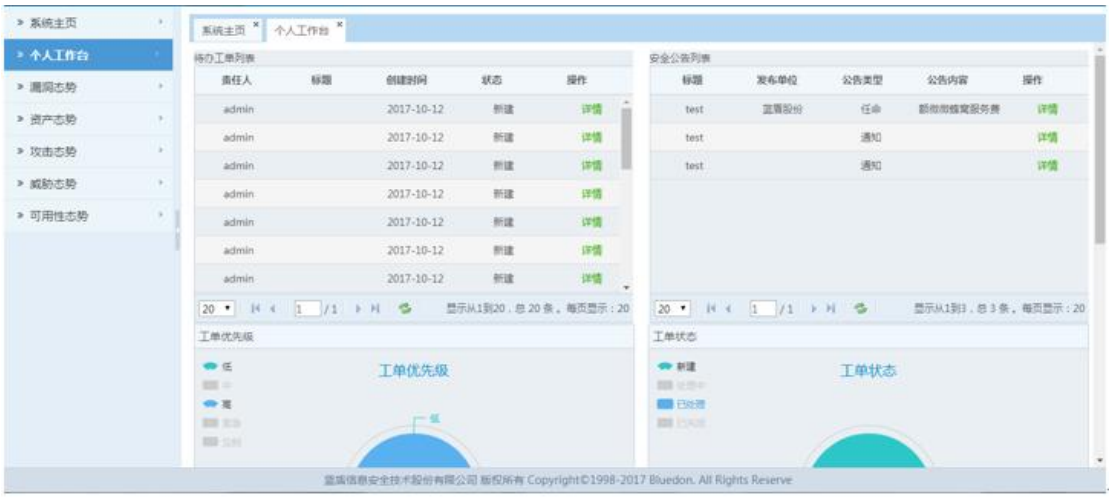
4.1 系统主页

用户登录成功后首先进入的页面就是中科云量安全综合管理平台的主页，该页面向用户展示了运维平台的各种情况，包括事件实时监控表，告警实时监控表，漏洞报表，工单分布图，事件数量统计报表，日志收集量统计报表，告警级别统计报表等。对于上述报表用户可以自由选择不同的统计方式，其中“每小时”统计从当天 00 点到当前时间的数据；“每天”统计本周一到当天的数据；“每周”统计本月第一周到当前周的数据；“每月”则是统计当年 1 月到本月的数据。

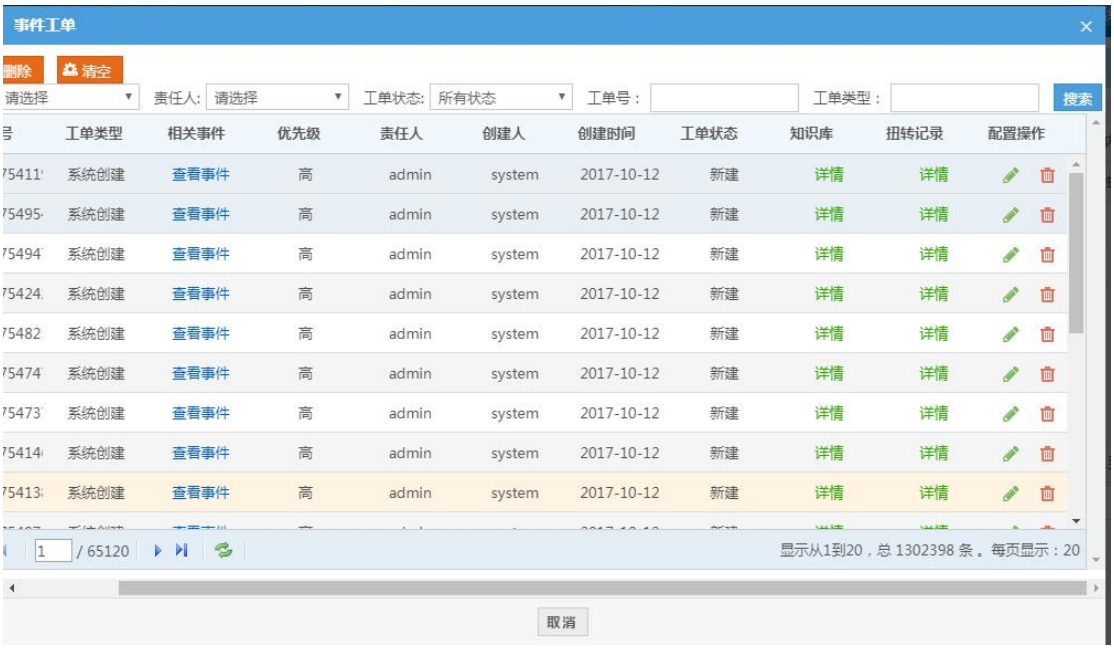
其中，报表可以手动拖动。

4.2 个人工作台

个人工作台主要是提醒该账户名下的工单任务和安全公告，让账户可以快速的处理工单，工作台主要包括待办工单列表、安全公告列表、工单优先级、工单状态和工单统计图。如下图：



在**待办工单列表**中点击**详情**可直接查看改工单的情况，如下图：



在配置操作列中点击  可编辑工单信息，包括修改工单状态、工单的优先级和指派给责任人。

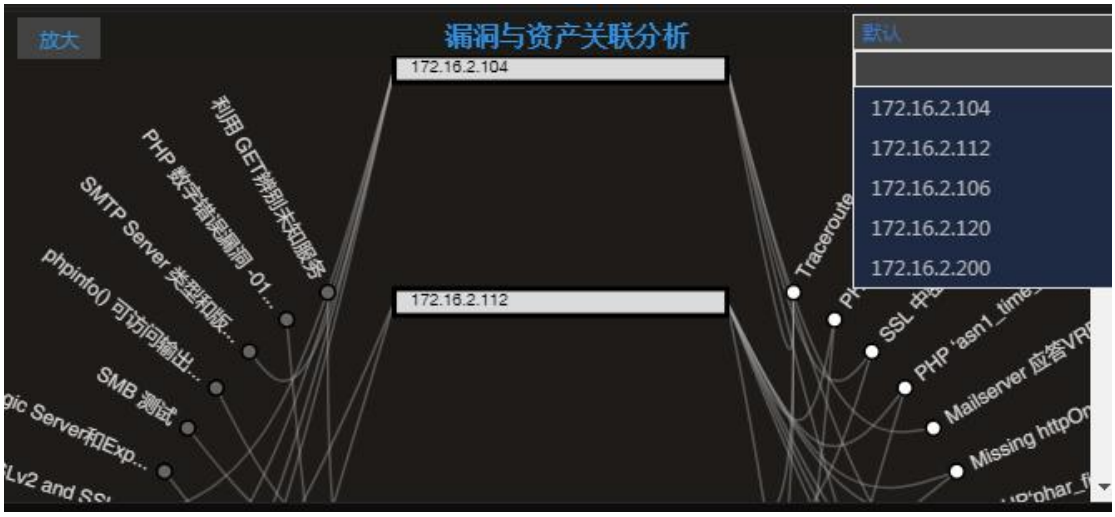
在**安全公告列表**中点击**详情**可直接查看该公告的情况，如下图：

在配置操作列中点击 可编辑公告信息，包括修改标题、发布单位、类型和公告内容。如下图：

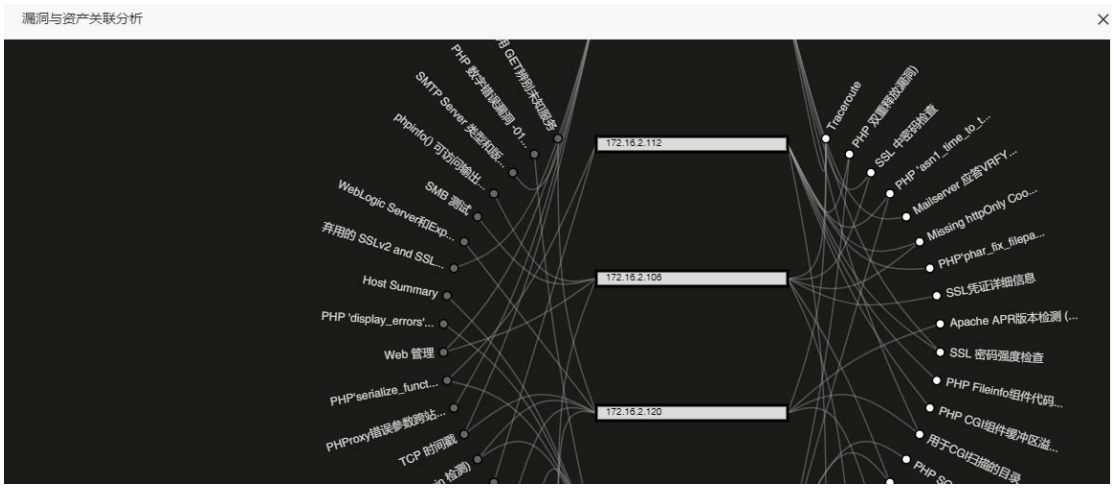
4.3 漏洞态势

漏洞态势是根据**安全分析>漏洞管理>资产漏洞分析**的文件提取出的信息。其中漏洞级别统计是将高风险漏洞、中风险漏洞、低风险漏洞和信息的统计结果，漏洞数量统计是根据时间先后顺序动态显示存在的漏洞信息，脆弱性分析是直接将单个网元存在的漏洞以图表的方式展示出来，漏洞与资产关联分析图则将所有的网元与所有的漏洞关联在一起展示。如下图：

脆弱性分析和漏洞与资产关联分析都可以选择对应的单个网元展示，如下图：



点击  按钮可以将图形放大展示，点击  可以退出放大的效果，如下图：



4.4 资产态势

资产态势可以将资产风险、威胁、端口分布情况依次排列，包括通过热力图

直观的显示资产的地理位置、个数、威胁程度，包括统计资产使用的端口分布、统计资产使用的协议分布、统计资产使用的操作系统分布，如下图：

4.5 攻击态势

攻击态势包括日志源和事件分析、攻击地球、以雷达图显示最近的攻击类型。其中，日志源和事件分析有：统计日志源数量和告警事件数量、通过列表显示最近的攻击事件、显示产生日志数量最多设备的日志量情况、按事件类型分别统计最近的事件数量；攻击地球有：基于 3D 地球，通过 IP 经纬度显示攻击事件、DDOS 攻击没有源地址，其他攻击显示源和目的、基于 3D 地球，显示攻击来源热力图、可以切换到中国地图显示攻击事件；雷达图显示最近的攻击类型主要是通过仪表盘显示整个系统资产风险的安全态势。如下图：

4.6 威胁态势

威胁态势主要按事件和漏洞展示变化，其中有事件列表、漏洞列表、威胁的总数和地图的展示，地图可变化为全球或者中国地图展示。如下图：

4.7 可用性态势

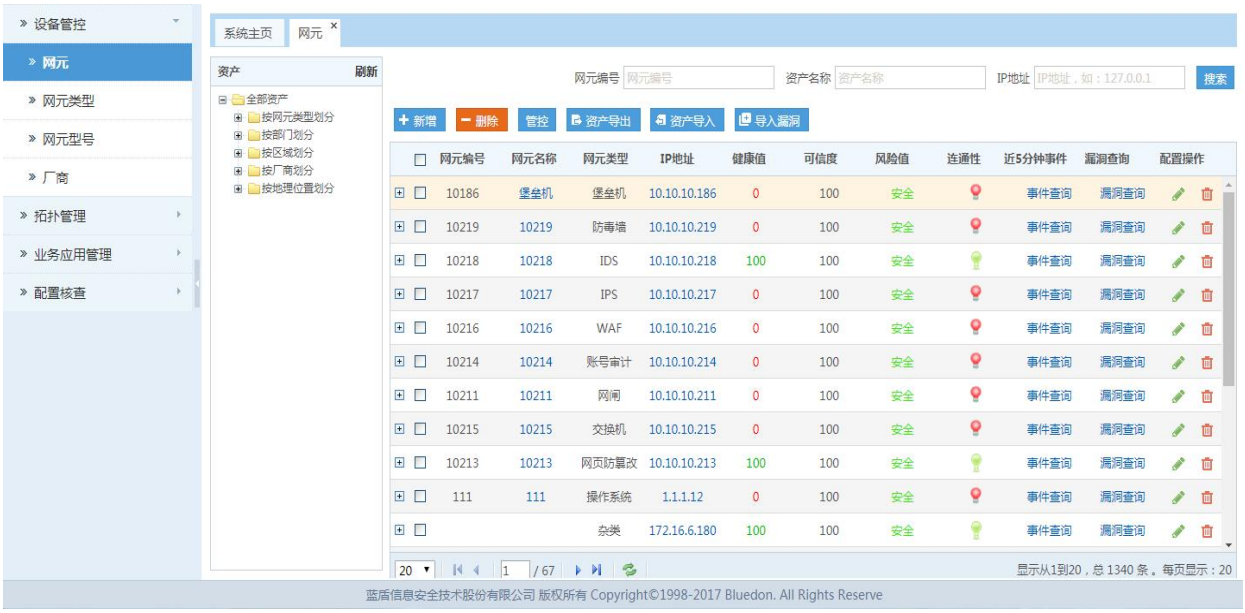
可用性态势主要包括：设备总数量、正常和故障设备数量。其中，设备故障率统计有：统计设备故障率最大的设备 TOP5、统计今日平均故障率、统计本月平均故障率、统计本年平均故障率；延时统计有：延时最大设备 TOP5、平均延时趋势；

第 5 章　资产管理

5.1 设备管控

5.1.1 网元

点击**设备管控>网元**进入网元界面，界面显示了资产的基本信息，用户可以根据自己的需求，新增、配置、删除、管控资产。左中侧的资产列表可以根据网元信息的网元类型、部门、区域、厂商、地理位置来划分，点开可查看详细信息，并根据详细信息可精确查找相应的网元。



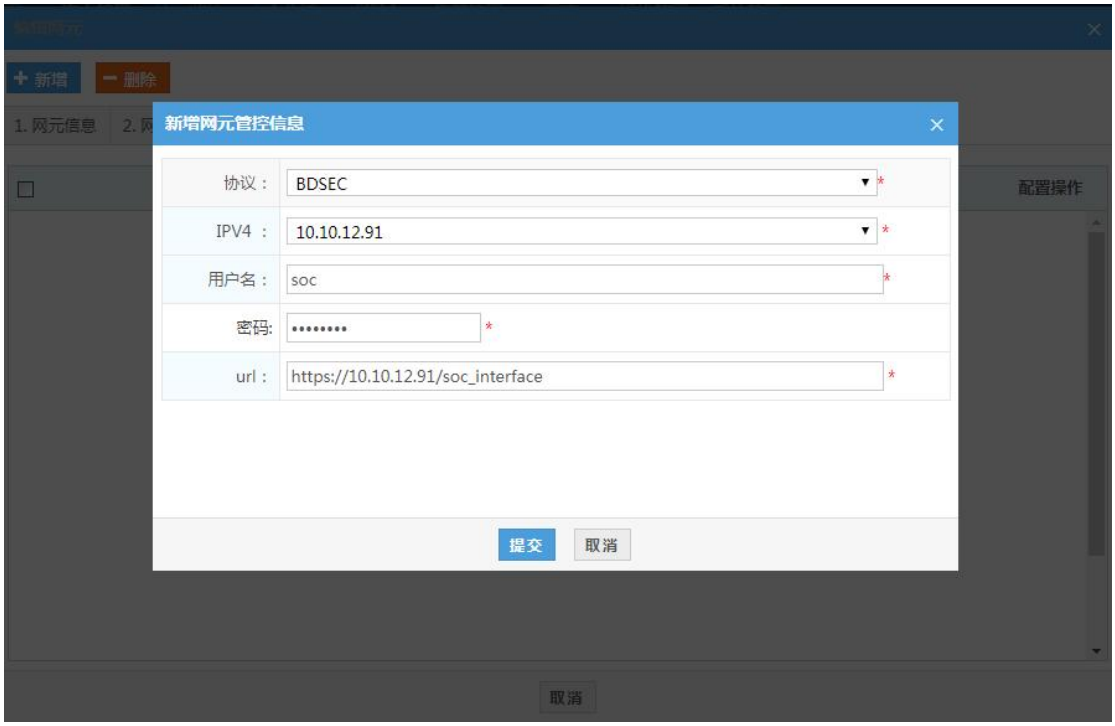
网元信息每 10 秒刷新一次，并将最新的情况呈现出来。

点击**设备管控>网元>新增**按钮，用户可以在弹出的新增网元页面中提交网元的信息（其中红色“*”号标记的为必填项），如下图：

对于提交过后或者已经存在网元编辑时，可以编辑或者删除网元 IP 信息、管控信息、监控信息与区域信息。对于传感器拓扑出来的网元，其网元 IP 信息一般会自动查找并显示，如果没有可以新增；管控信息，正确配置后可以对网元进行管控操作；监控信息，正确配置后配合**状态监控**采集插件可以查看网元的 CPU 使用率、内存使用率、服务列表和软件列表等信息；区域信息，可选择所属区域关联网元，若没有区域信息可在**系统管理>用户管理>区域管理**添加区域信息。添加后点击**网元>全部资产>按网元类型划分**可以精确查找资产。

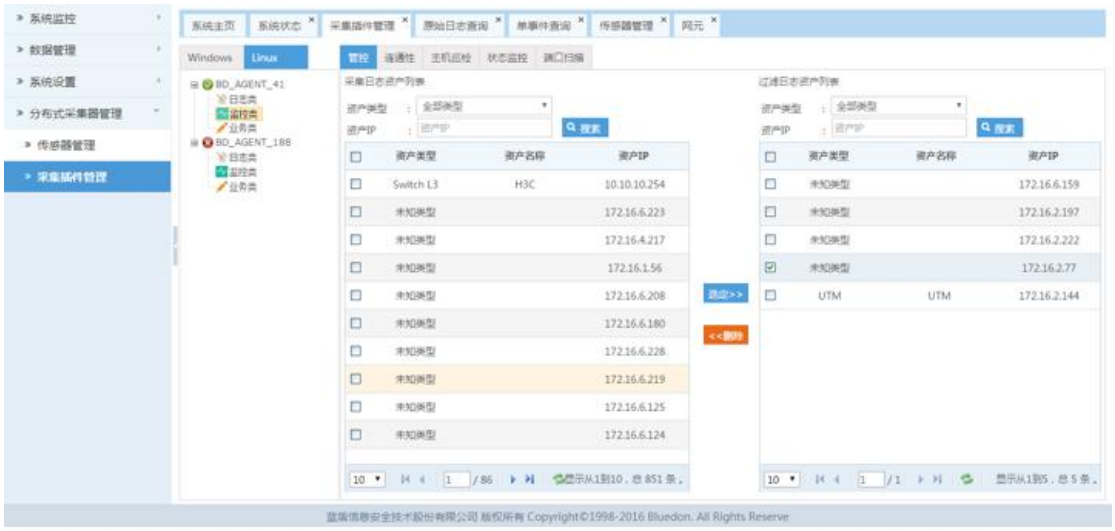
点击**设备管控>网元>删除**按钮可以删除选中的网元信息。

点击**设备管控>网元>管控**按钮可以管控选中的网元，目前管控主要涉及重启、关机、时间同步操作。管控之前首先需要配置好对应网元的管控信息，如下图：



其中管控信息中的 url 需要确认是否填写正确，确认方法为直接将 url 拷到浏览器的新窗口，若能进去则说明 url 信息填写正确。

对于早期系统的版本（如 v5.0、v5.0.1）还需要把管控的资产 IP 添加到启动的管控采集器上，如下图：



v5.1 版本默认均可管控，不用此操作。

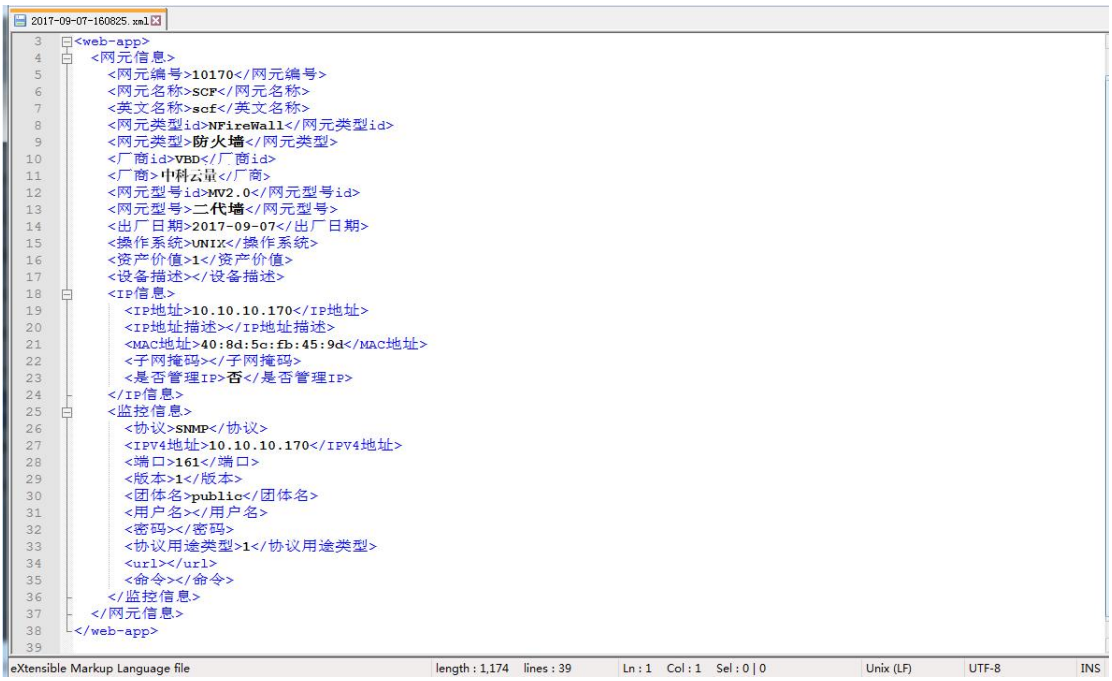
最后，可进行管控操作，如下图：

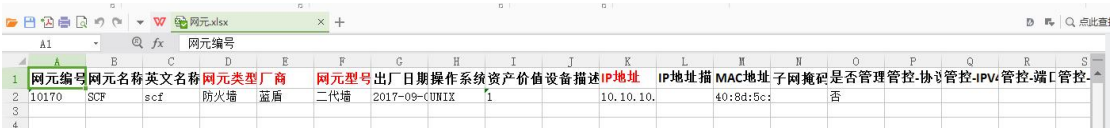
若被管控的网元在管控前可 PING 通，重启管控后不可 PING 通，过段时间又可 PING 通，则认为重启管控成功；若被管控的网元在管控前可 PING 通，关机管控后长时间不可 PING 通，且网元不运行，则认为关机管控成功；若网元时间为 A，SOC v5.1 管理服务器时间为 B，在时间同步操作后可输入要时间同步的 SOC 的 IP，网元的时间也变为 B，则认为时间同步管控成功。

关于管控信息的配置，不同的设备配置方式可能有所不通，其配置信息可参考下图：

设备名称	协议	用户名	密码	URL
IDS	YLSEC	admin	bd888888	https://10.10.12.179/cgi-bin/admin/bdsec_daemon
中科云量多功能防火墙一代墙	YLSEC	admin	bd888888	https://10.10.12.178:441/cgi-bin/admin/bdsec_daemon
UTM	YLSEC	root	bluedon	https://172.16.2.144:441/cgi-bin/admin/bdsec_daemon
漏洞扫描	YLSEC	soc	88888888	https://10.10.10.7/bdsec_daemon.php
中科云量多功能防火墙二代墙	YLSEC	soc	88888888	https://10.10.11.101:444/soc_interface
信息安全审计	YLSEC	soc	88888888	https://10.10.12.91/soc_interface
堡垒机	YLSEC	soc	88888888	https://10.10.13.107/bdsec
数据库审计	YLSEC	soc	88888888	https://10.10.12.170/soc_interface
WAF	YLSEC	soc	88888888	https://10.10.10.22:444/bdsec_daemon.php

点击**设备管控>网元>资产导出**按钮可以将网元以 xml 或者 excel 表格的形式导出来并查看，如下图：





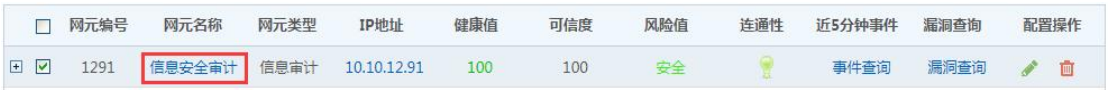
点击**设备管控>网元>资产导入**按钮可以将网元以 excel 表格的形式导入，对于已经存在的网元将导入失败并提示，如下图：

点击**设备管控>网元>导入漏洞**按钮可以将漏洞以 html 的形式导入，如下图：

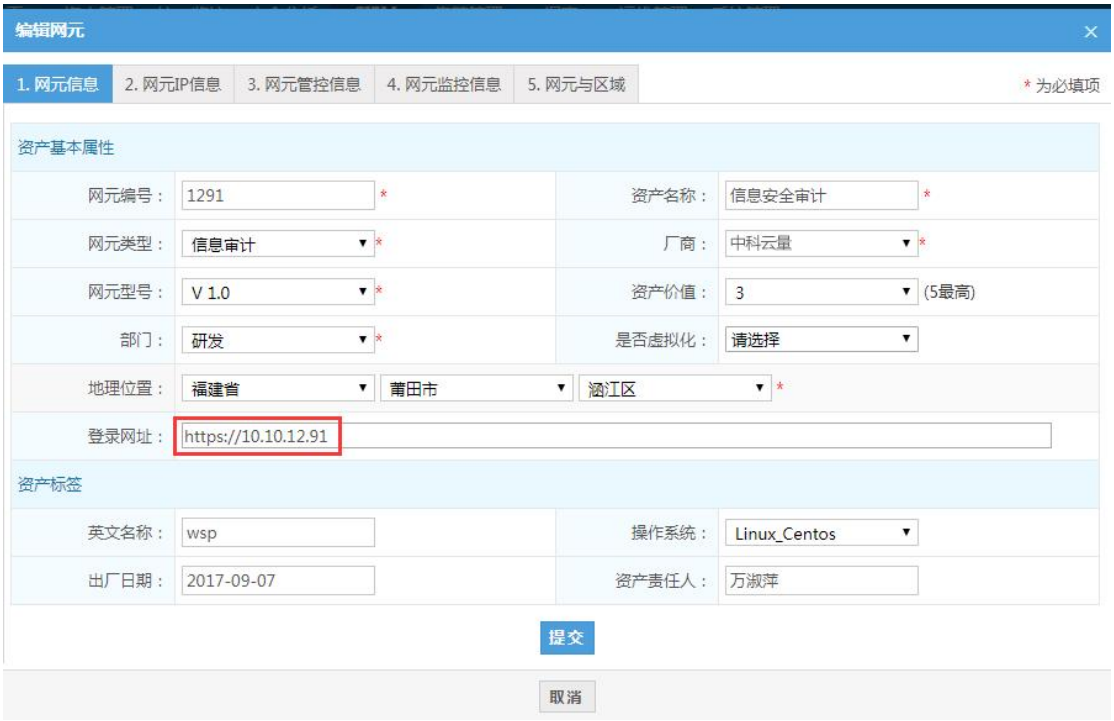
导入成功的漏洞在网元的漏洞查询中可查询到。在**安全分析>漏洞管理**中也可查询到。

设备的基本信息，可以展开以表格的形式说明，如下图：

点击**设备管控>网元>网元名称**按钮可以跳转到该网元的登录界面，如下图：

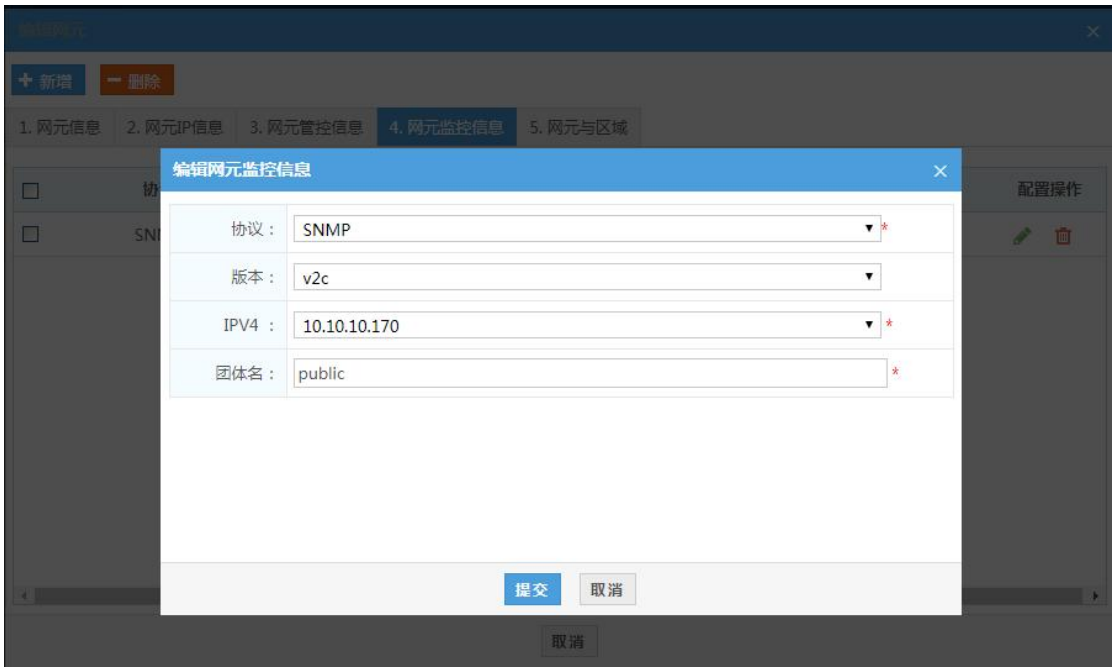


跳转需要设置登录网址，如下图：

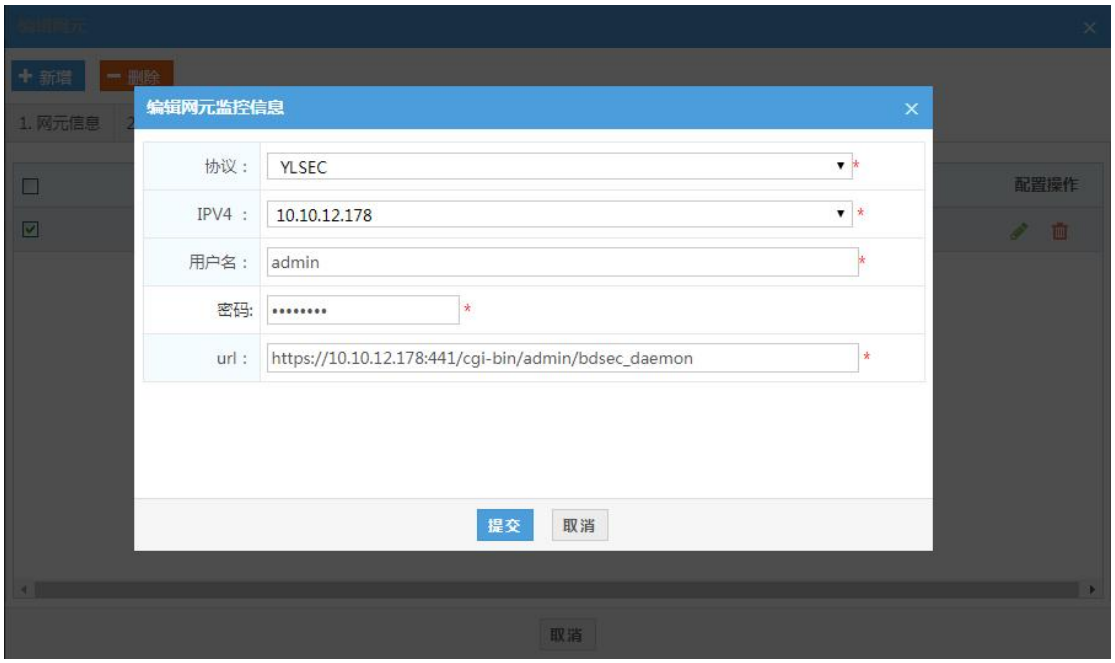


点击**设备管控>网元>IP 地址**按钮可以查看资产的 CPU、内存和硬盘的相关信息，如下图：

获取资产信息之前首先需要在网元信息中填写网元监控信息，监控信息可选 SNMP、BDSEC 两种协议。SNMP 协议如下图：

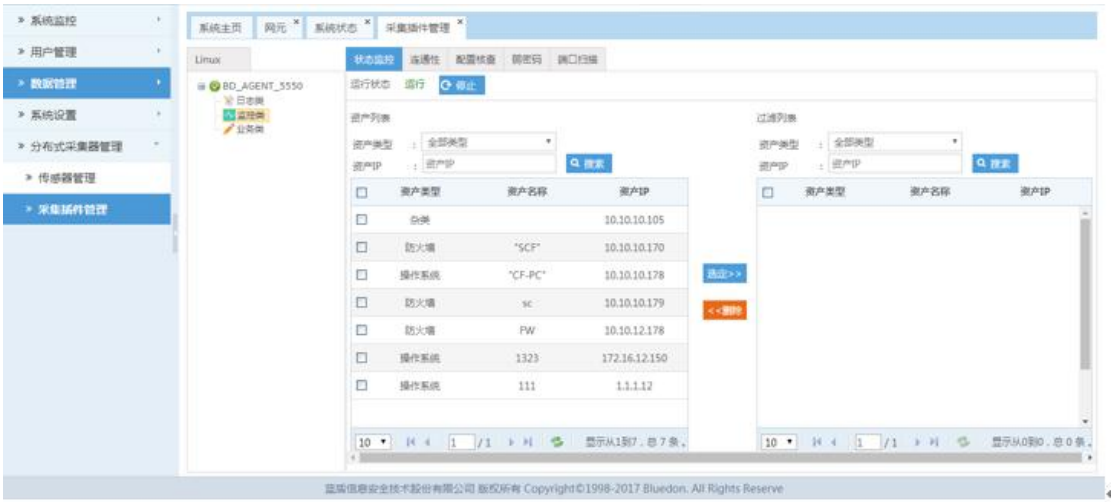


设置 SNMP 协议之后，需要用第三方工具（如 MIB Browser）确认下网元的 SNMP 服务器是否开启，如果没有这需要开启 SNMP 服务。BDSEC 协议如下图：



信息中的 url 需要确认是否填写正确，确认方法为直接将 url 拷到浏览器的新窗口，若能进去则说明 url 信息填写正确；若是网元可以被管控则可直接认为 url 信息填写正确。

还需要配合**状态监控**采集插件，如下图：



资产的***健康值***根据资产的状态告警指标扣分。设备健康度满分为 100 分。出现告警后扣分，告警清除后扣分清零。扣分规则如下：

扣分项	扣分值
链路通断	-100 分
每项指标严重告警	-10 分
每项指标重要告警	-5 分
每项指标次要告警	-3 分

资产的***可信度***。系统将资产的 IP 与事件的 3 个 IP 字段（源 IP，目的 IP，设备 IP）整合成一个 IP 地址库，这些 IP 地址根据漏洞扫描结果和告警事件评估该设备的可信度。当 IP 落在系统资产的范围内为资产的可信度，当落在用户终端的 IP，为用户信誉度。

可信度计算方式：

1. 计算周期为一周，满分为 100 分。周期到后，扣分清零。根据漏洞与告警扣分，漏洞扣分占 50，告警扣分占 50。

2. 提取漏洞扫描结果的 IP 以及受告警事件影响的主机 IP。

3. 漏洞等级分了 5 级，只取最高 3 级，同理，事件等级也只取最高 3 级。

4. 扣分方式：

漏洞等级	每个漏洞扣分值	告警等级	每次告警扣分值
紧急	5	严重	1.5
高危	2	高	1

中危	1	中	0.5

资产的***风险值***。资产风险的计算根据三个因子计算，资产价值，资产威胁，资产脆弱性。三个因子的取值为 1~5。风险值的统计周期为一小时。

资产价值为在资产基本属性配置。

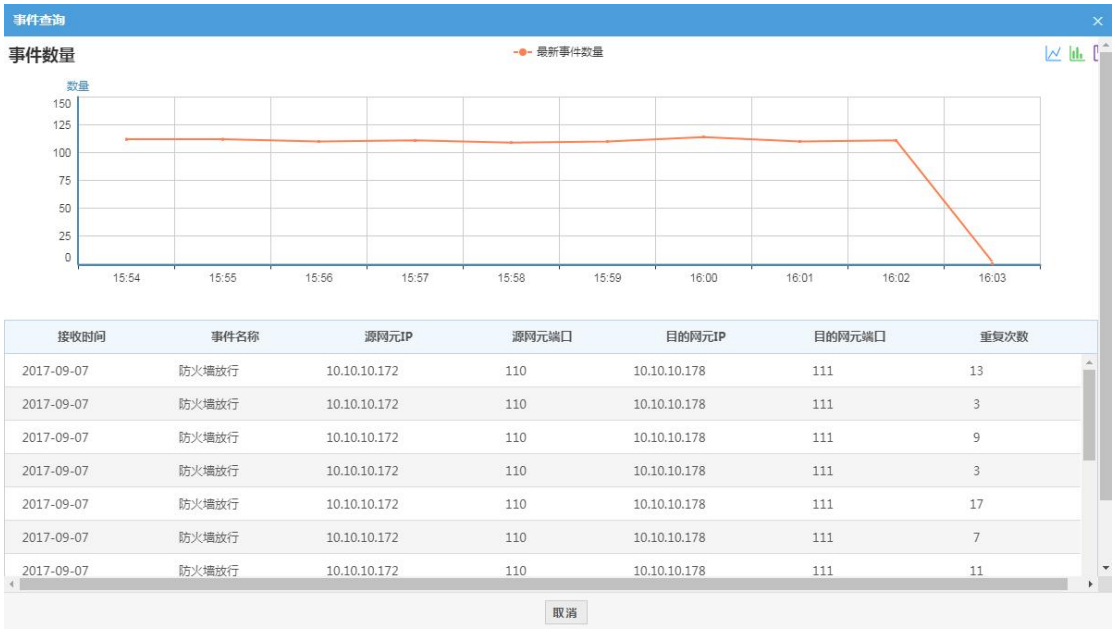
资产威胁根据事件等级与频率相关，关系如下：

等级频率	严重	高	中	低	轻微
200 以上	严重	严重	高	中	轻微
100~200	严重	高	高	低	轻微
50~100	严重	高	中	低	轻微
10~50	严重	高	中	低	轻微
10 次以下	严重	高	中	低	轻微

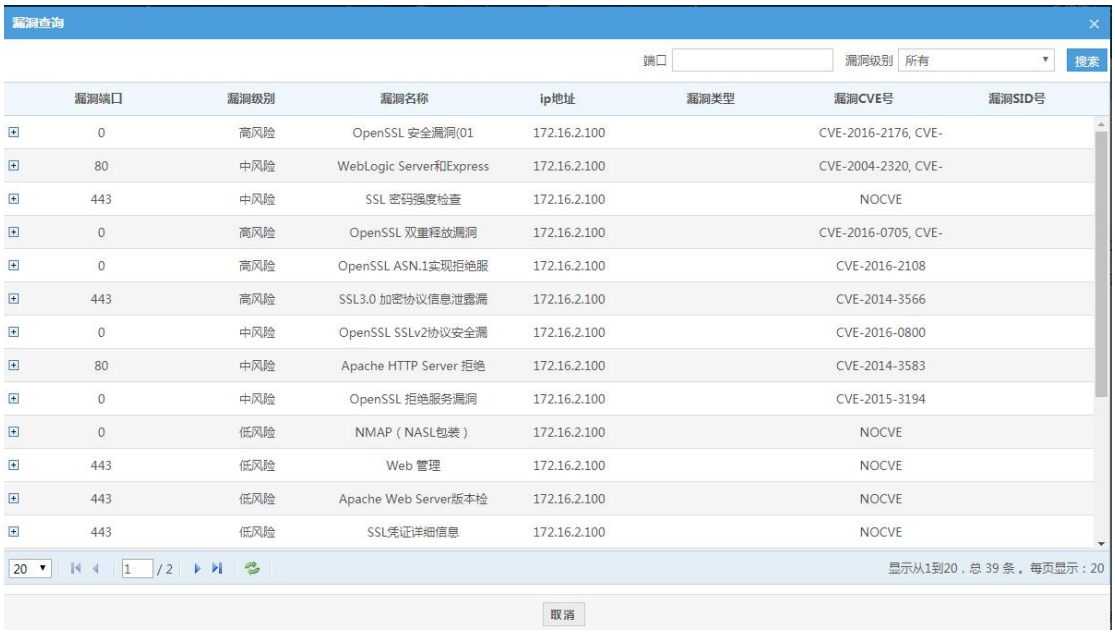
资产脆弱性与资产的漏洞与漏洞个数相关，关系如下：

等级个数	严重	高	中	低	轻微
20 个以上	严重	严重	高	中	轻微
15~20 个	严重	严重	高	低	轻微
10~15 个	严重	高	高	低	轻微
5~10 个	严重	高	中	低	轻微
5 个以下	严重	高	中	低	轻微

可以查询资产**最近 5 分钟事件**，点击**设备管控>网元>事件查询**可以得到最近 5 分钟产生的事件数及其具体信息，如下图：



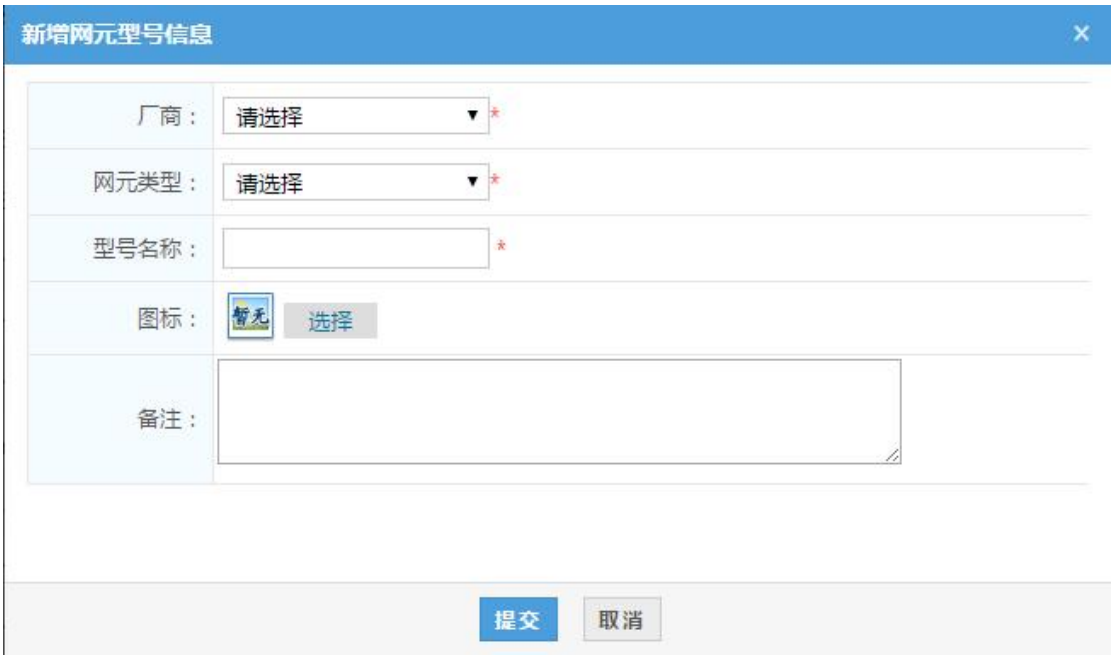
点击**设备管控>网元>漏洞查询**可以得该资产的漏洞信息，如下图：



5.1.2 网元型号

点击**设备管控>网元型号**进入网元型号界面，界面显示网元型号的信息，用户可以根据自己的实际需求，新增、编辑、删除选中的网元信息，也可以根据型号名称厂商、网元类型来查询（按型号名称排序），如下图：

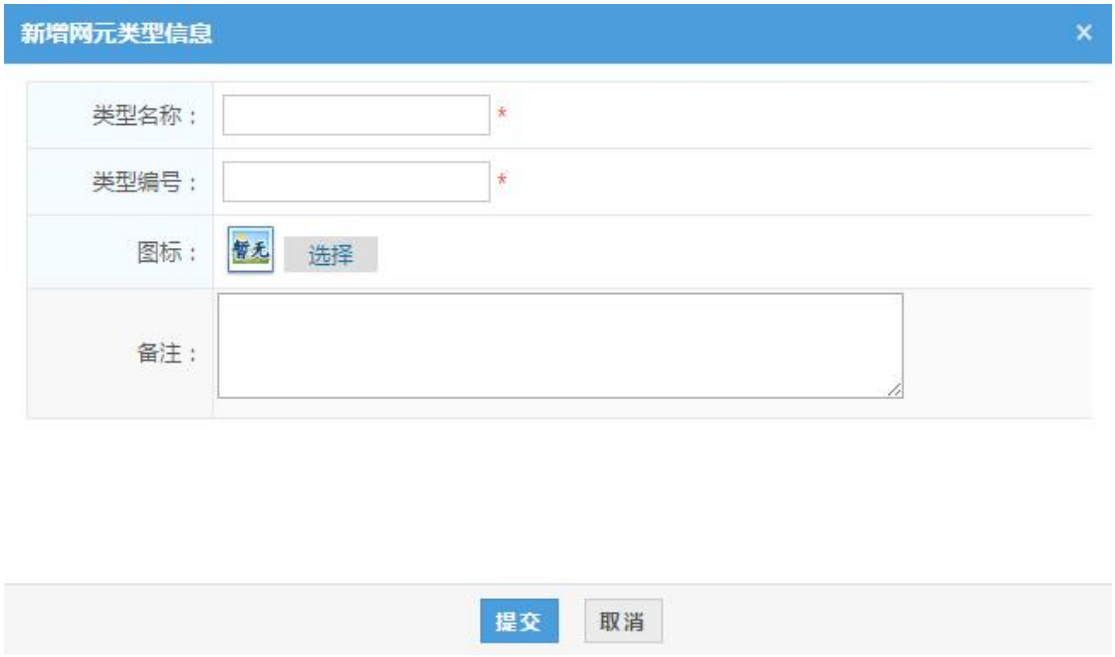
点击**新增**按钮，用户可以在弹出的页面中新增新的网元型号。如下图：



5.1.3 网元型号

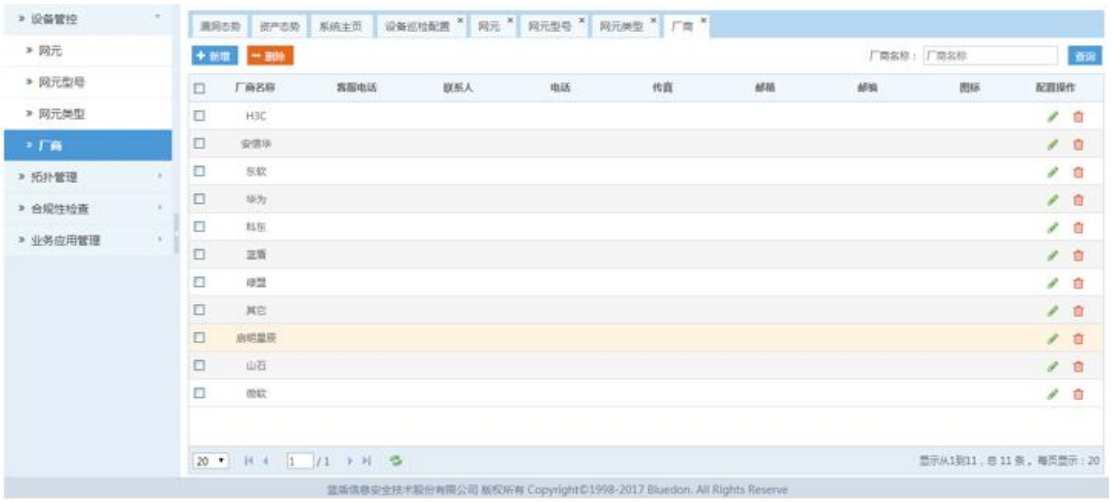
点击**设备管控>网元类型**进入网元类型界面，界面显示网元类型的信息，用户可以根据自己的实际需求，新增、编辑、删除选中的网元类型信息，也可以根据类型名称来查询（按类型名称排序），如下图：

点击**新增**按钮，用户可以在弹出的页面中新增新的网元类型。如下图：

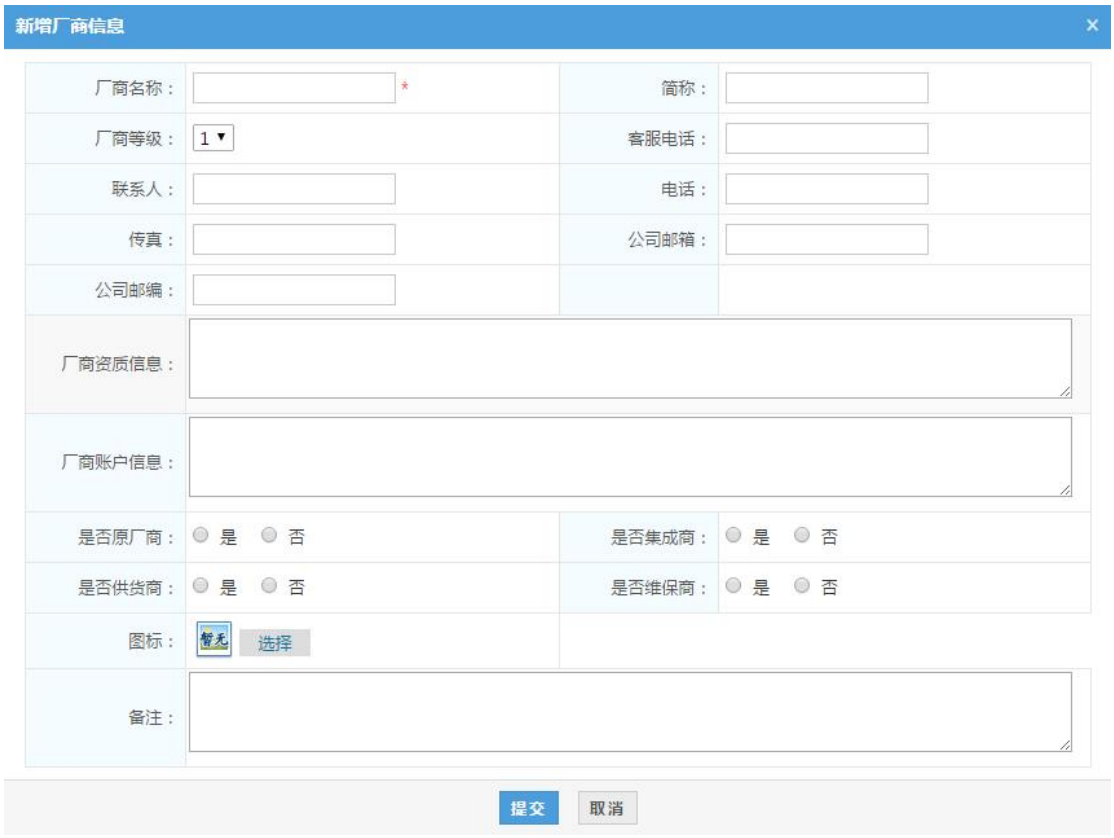


5.1.4 厂商

点击**设备管控>厂商**进入厂商界面，界面显示厂商的信息，用户可以根据自己的实际需求，新增、编辑、删除选中的厂商信息，也可以根据厂商名称来查询（按厂商名称排序），如下图：



点击**新增**按钮，用户可以在弹出的页面中新增新的厂商信息。如下图

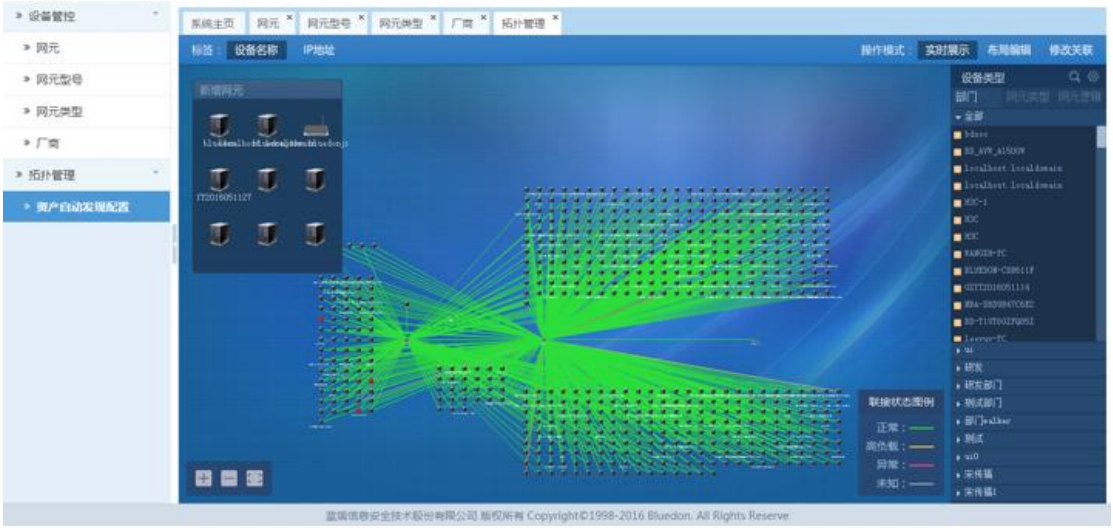


5.2 拓扑管理

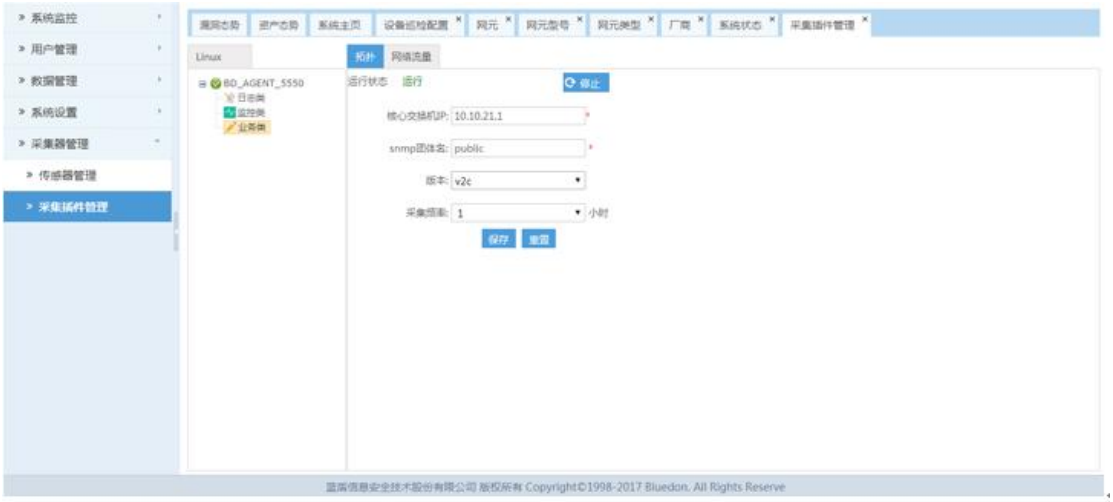
5.2.1 拓扑管理

点击**拓扑管理>拓扑管理**进入资产拓扑画面，画面中有资产的拓扑图。画面左上方有新增网元信息；右上方有三种操作模式可供选择，它们分别是实时展示、布局编辑和修改关联，其中实时展示可以选择显示资产的“设备名称”还是资产

的“IP 地址”，布局编辑有 7 种不同的排列方式可以选择，修改关联则可以更改资产之间的关联；左侧可以按部门、网元类型或者网元逻辑来显示设备类型。如下图：



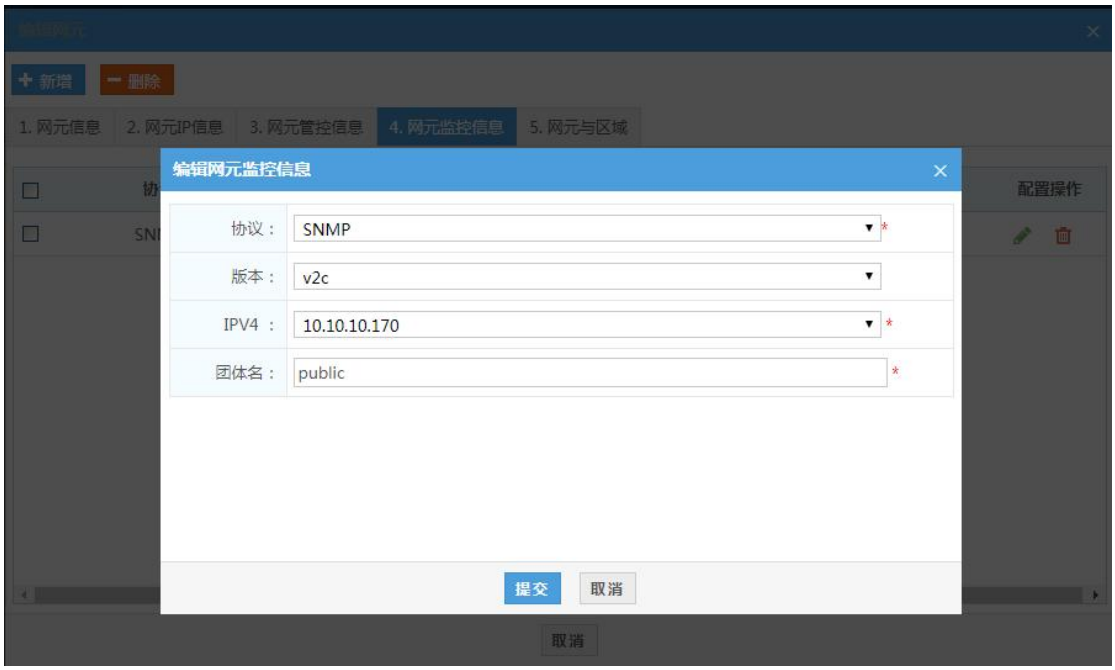
资产自动发现功能需要配合**拓扑**采集插件的设置、启动才能开启，采集器可以选择每 1 小时、每 3 小时、每 5 小时不同的频率来采集，以此发现新加入的资产设备。



拓扑要求交换机开启 SNMP 服务，且对应的团体名要一致。

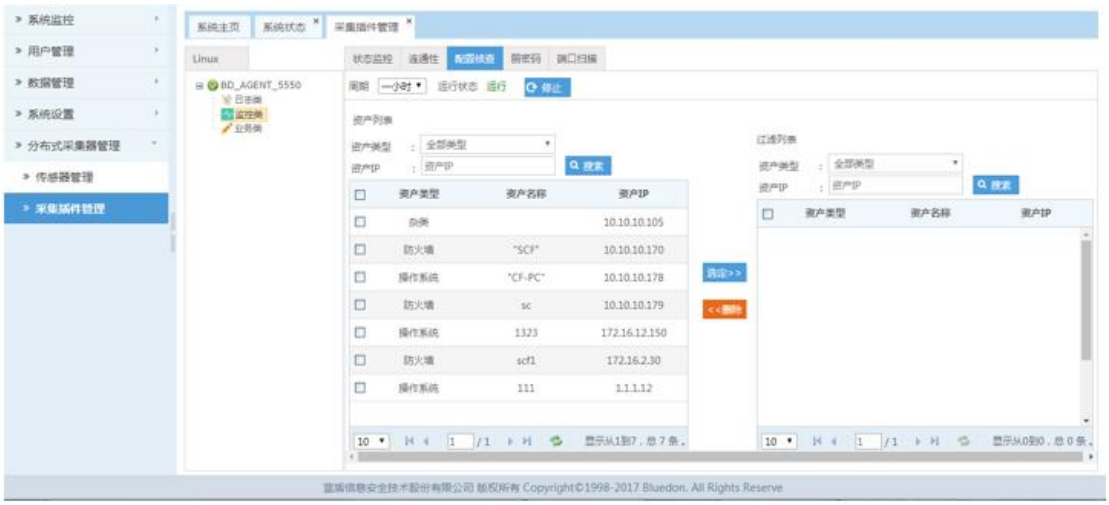
5.3 合规性检查

合规性检查功能需要网元填写网元监控信息，且仅支持 SNMP 协议。SNMP 协议如下图：



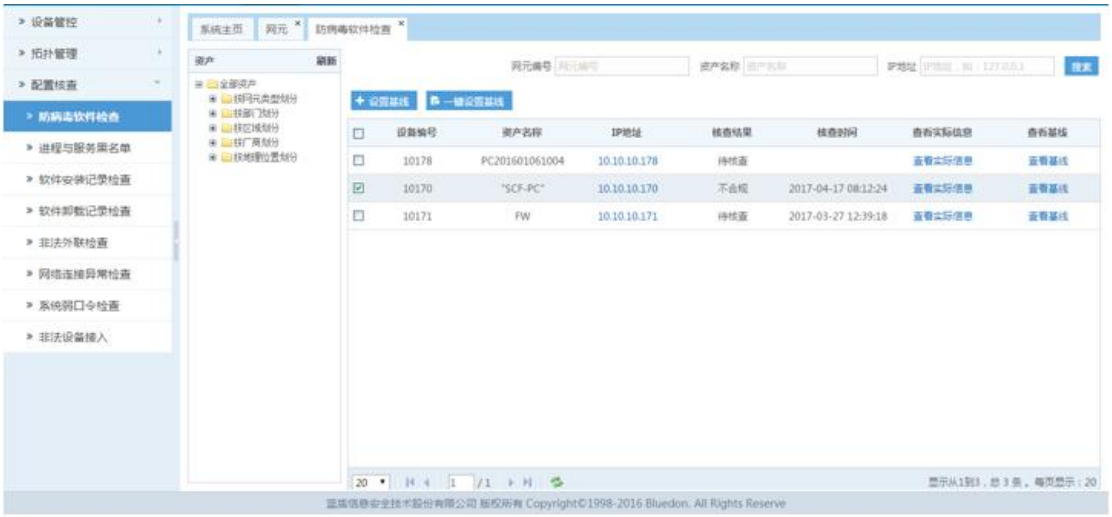
设置 SNMP 协议之后, 需要用第三方工具 (如 MIB Browser) 确认下网元的 SNMP 服务器是否开启，如果没有这需要开启 SNMP 服务。配置核查内容仅显示已配了 SNMP 协议的网元，对于没有配 SNMP 协议或者配的其他协议的网元不予显示。

同时需要配置核查插件处于开启状态，插件只核查资产列表中的网元，不核查过滤列表中的网元。核查的周期可手动选择，默认为一个小时。如下图:



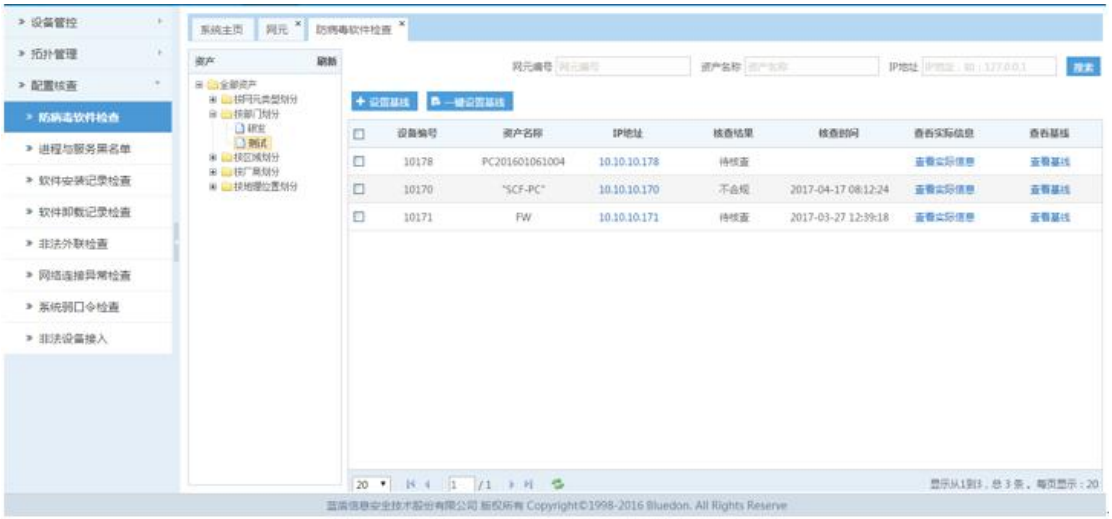
5.3.1 防病毒软件检查

点击**配置核查>防病毒软件检查**进入软件检查画面，系统可根据设置的防病毒软件基线，对资产进行防病毒软件检查，如下图:

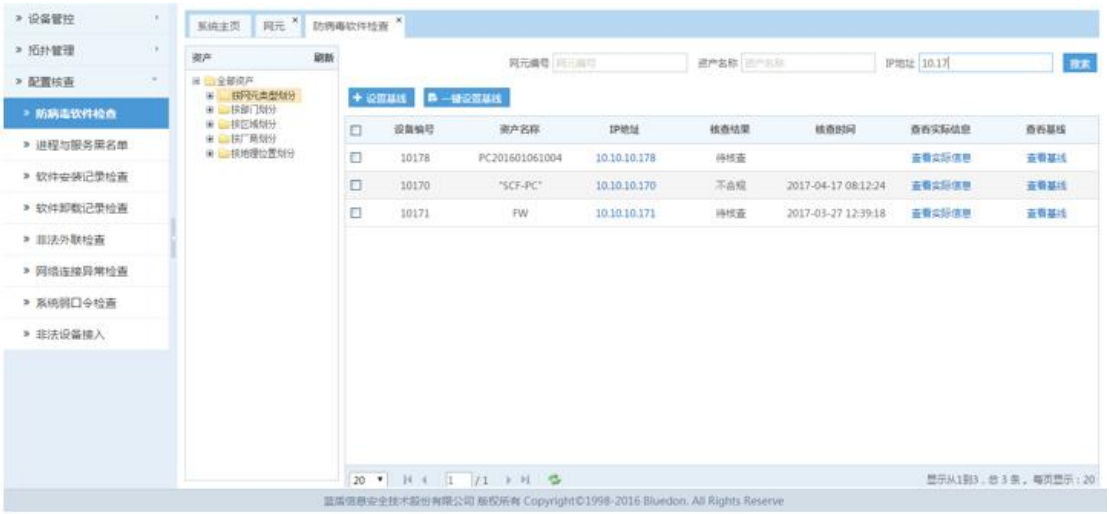


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：

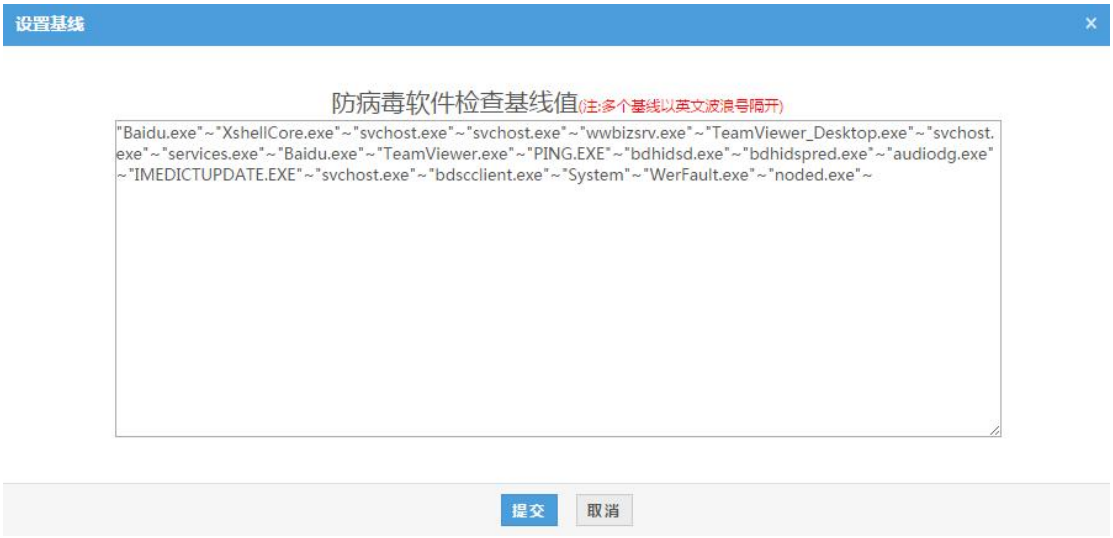


2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：



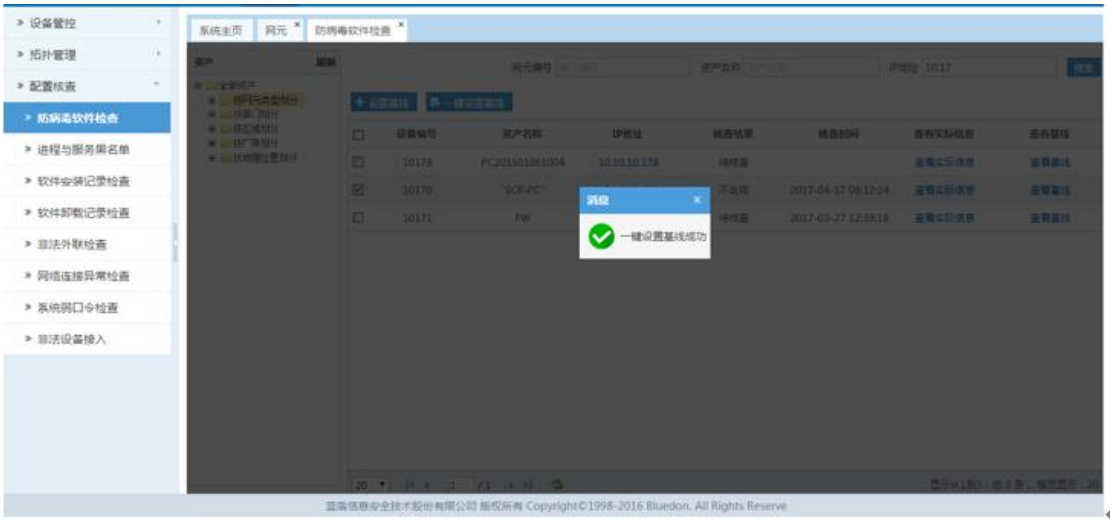
- 基线设置

1.手动设置防病毒软件基线，选择要设置基线的设备，点击**设置基线**，手动输入防病毒软件，点击**确认**如下图：

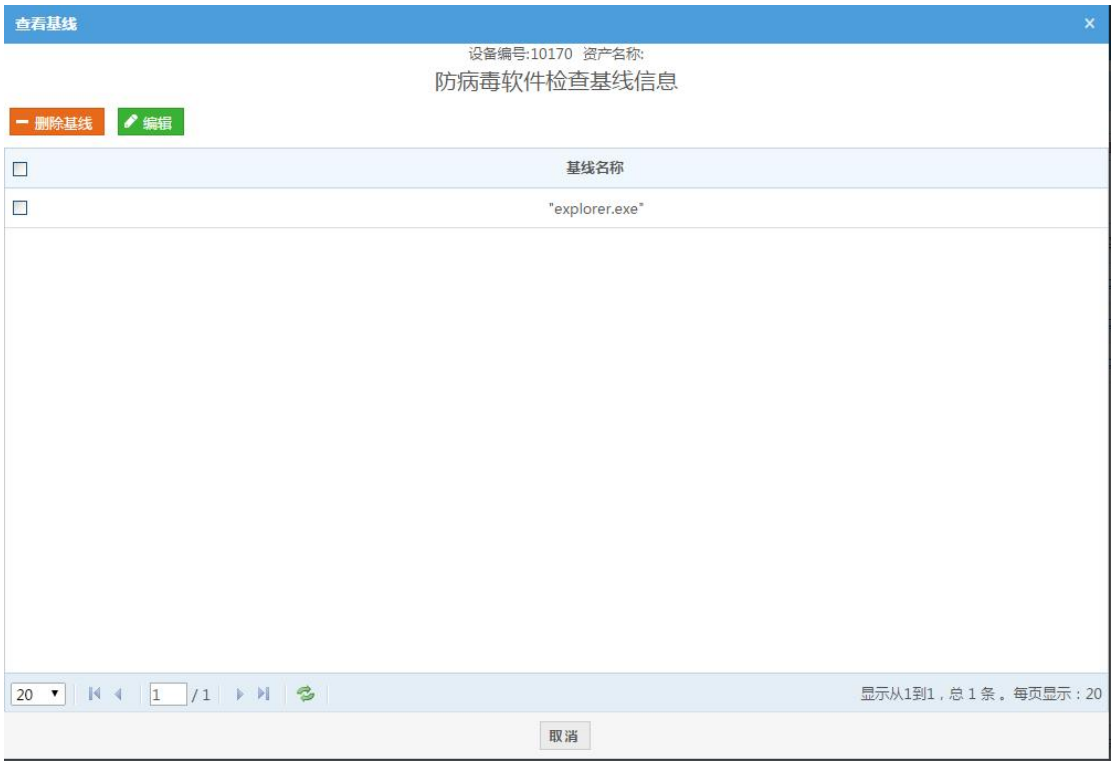


2.选择基线值设置基线，点击**查看实际信息**，勾选基线值，点击**将选中项设置为基线**，如下图：

3.一键设置基线。即选择一个基线，可以运用到所有设备，选择一个设备的基线，点击**一键设置基线**，如下图：



4.查看基线。点击右侧查看基线，可查看到所设置的基线，如下图：

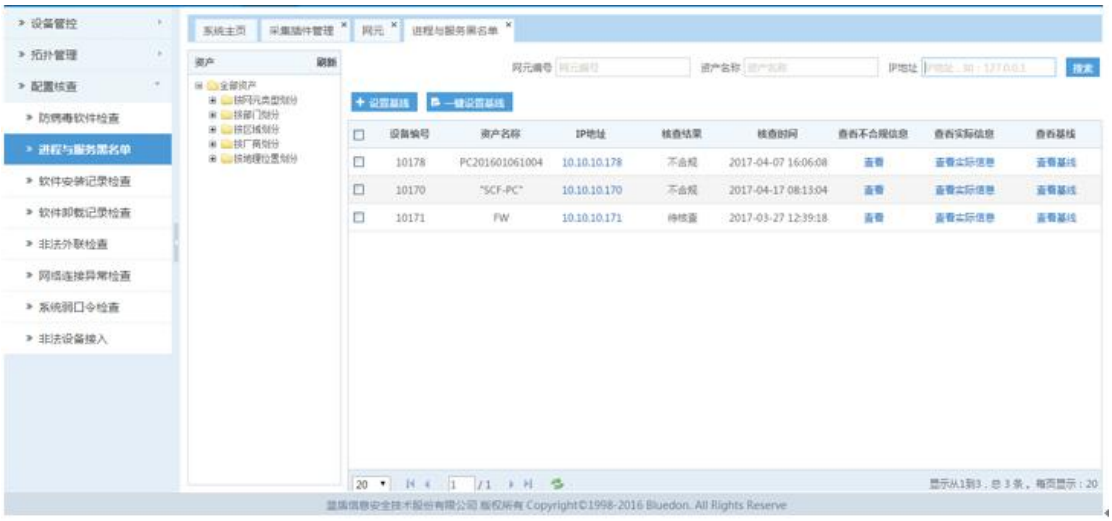


- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。其中系统对选定设备进行基线对比检测，符合基线返回为合规，不符合基线返回为不合规，并执行告警动作；没有做基线设置的，检测后返回无结果。

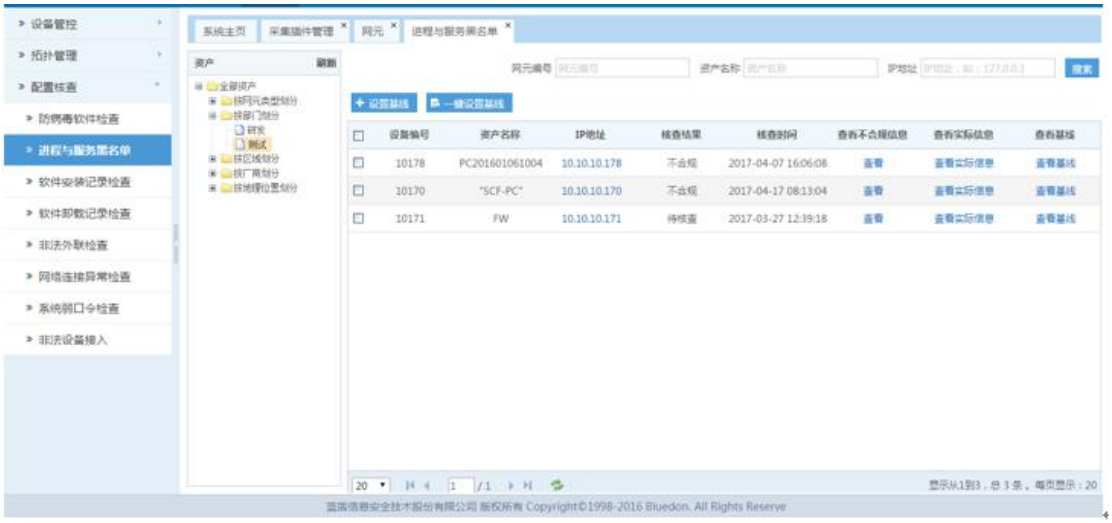
5.3.2 进程与服务黑名单

点击**配置核查>进程与服务黑名单**进入检查画面，系统可根据设置的进程与服务，对资产进行进程与服务核查，如下图:

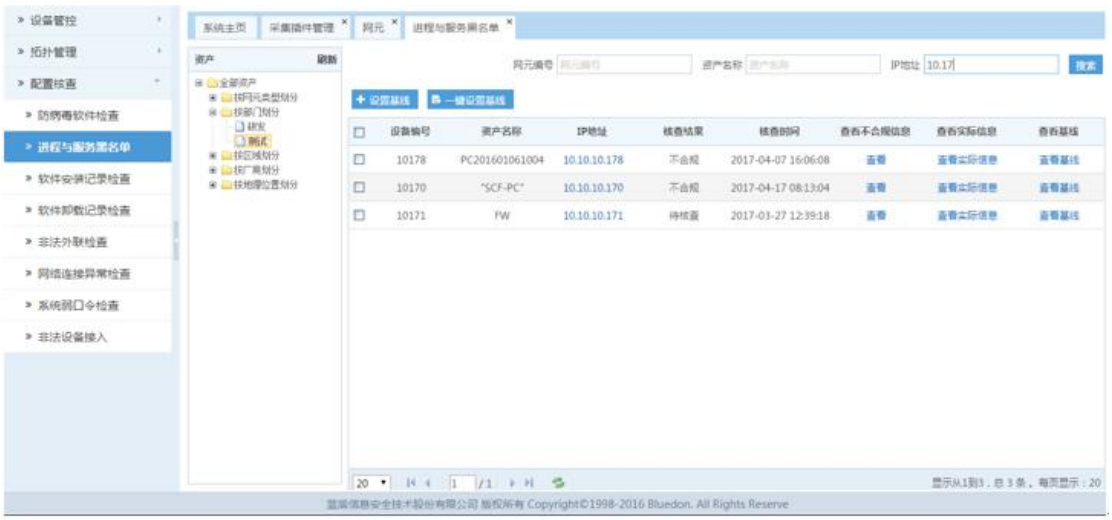


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：

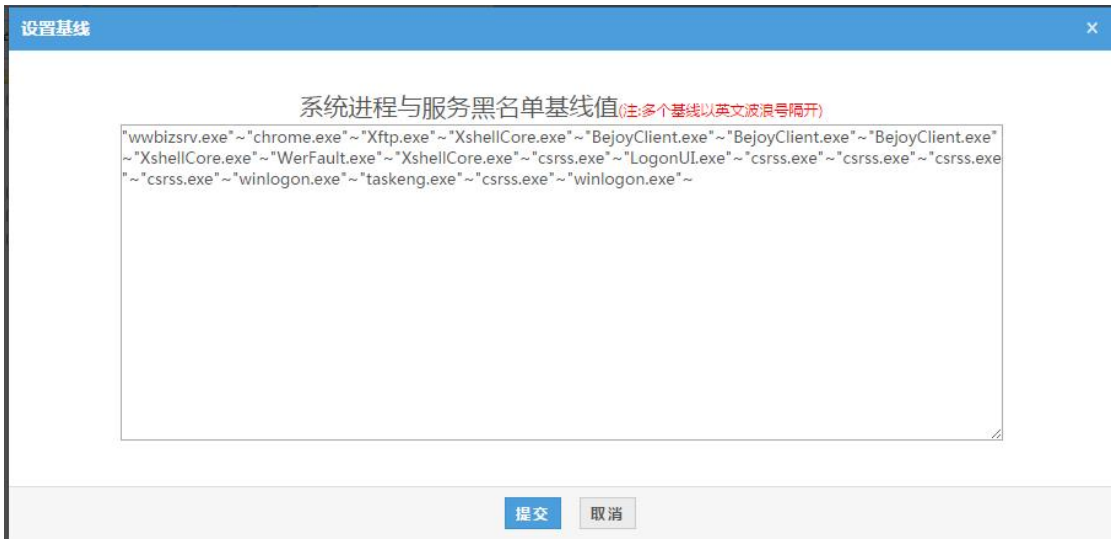


2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：



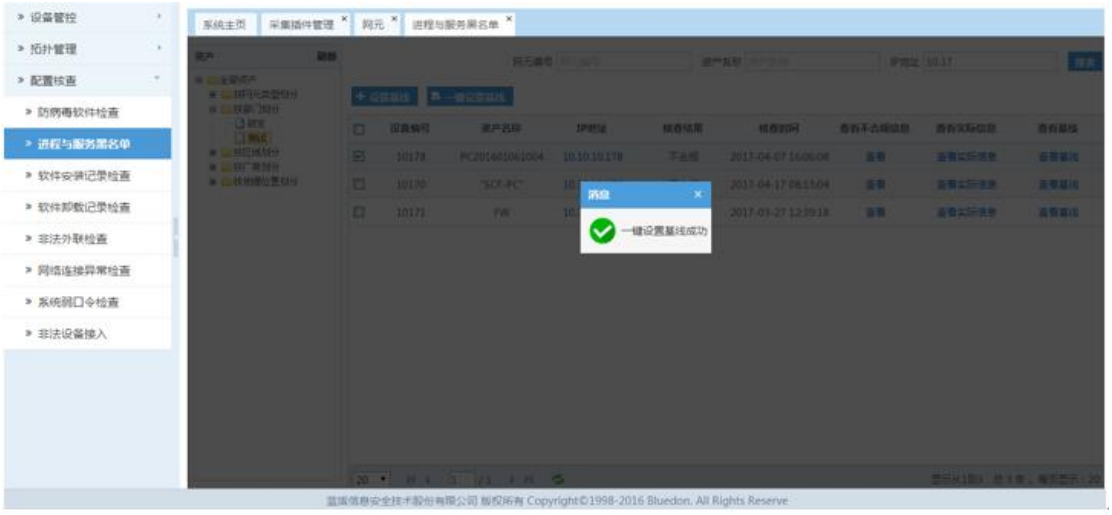
- 基线设置

1.手动设置进程与服务黑名单基线，选择要设置基线的设备，点击**设置基线**，手动输入进程与服务，点击**确认**如下图：



2.选择基线值设置基线，点击**查看实际信息**，勾选基线值，点击**将选中项设置为基线**，如下图：

3.一键设置基线。即选择一个基线，可以运用到所有设备，选择一个设备的基线，点击**一键设置基线**，如下图：



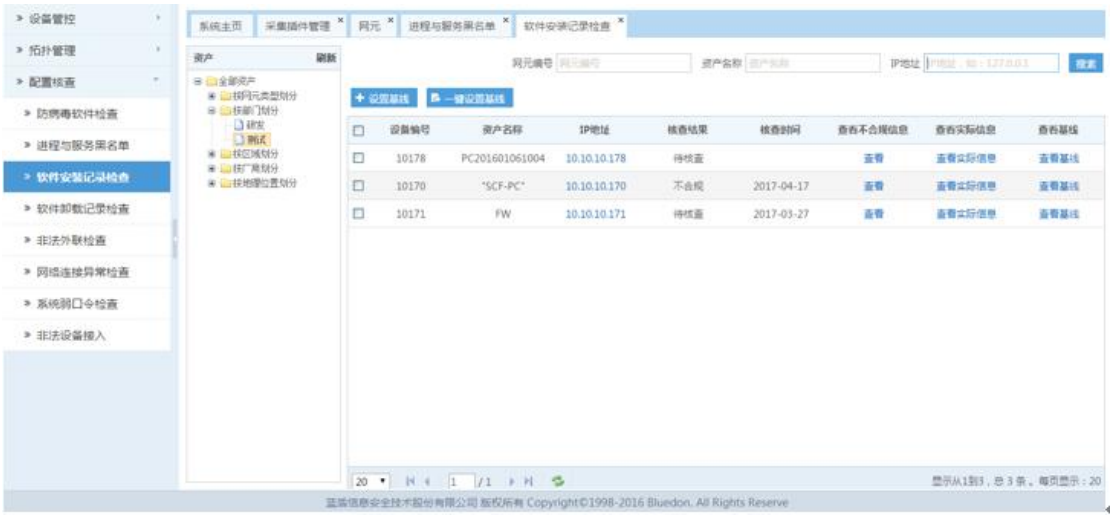
4.查看基线。点击右侧查看基线，可查看到所设置的基线，如下图：

- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。把进程与服务黑名单设置为基线，检测时，把设备开启的进程与服务跟基线进行对比，开启了基线里进程与服务的，返回不合规，并执行告警动作，没有开启的返回为合规；点击**查看**，可查看不合规信息，以便做出修改；没有做基线设置的，检测后返回无结果。

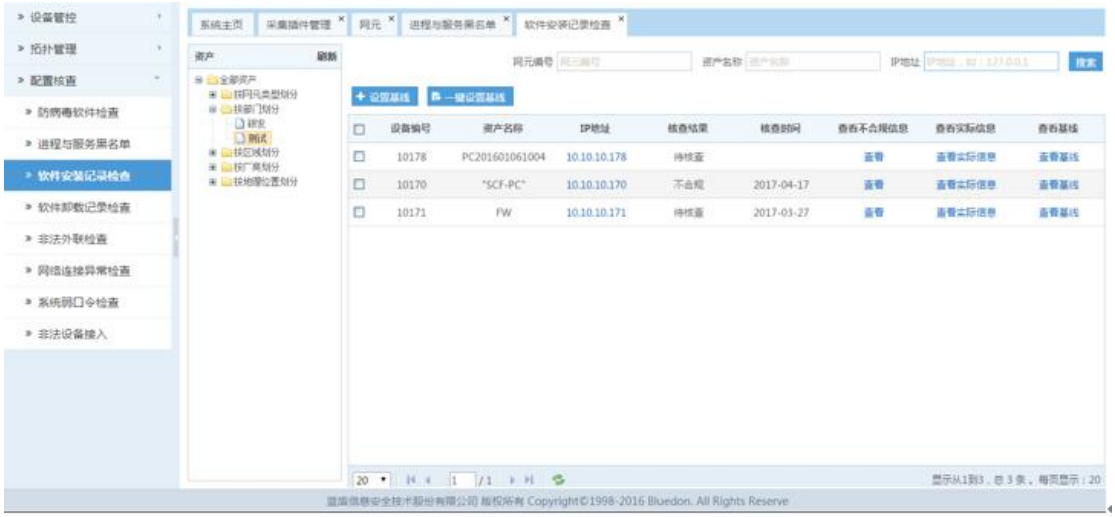
5.3.3 软件安装记录检查

点击**配置核查>软件安装记录检查**进入检查画面，系统可根据设置的基线，对资产进行软件安装核查，如下图:

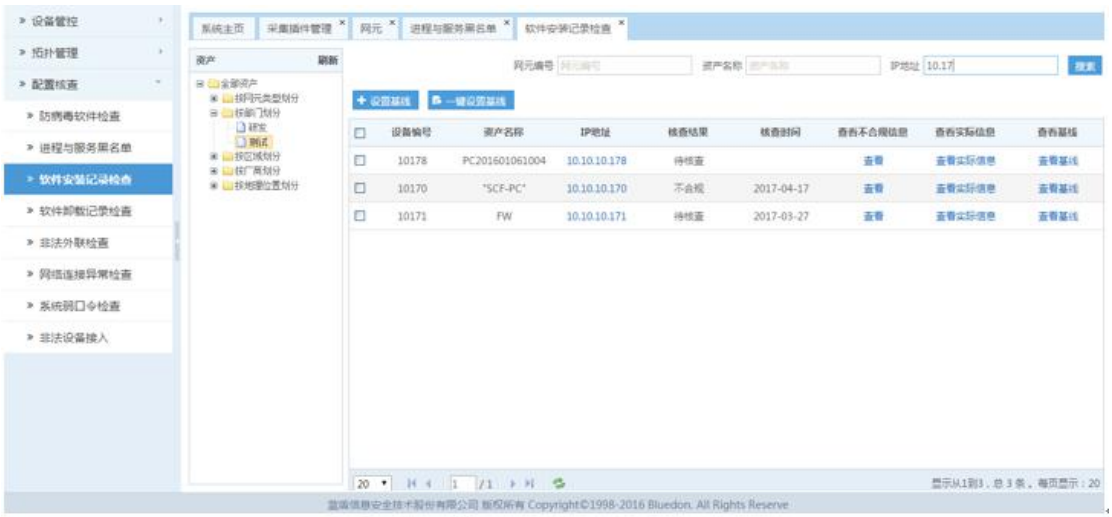


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：

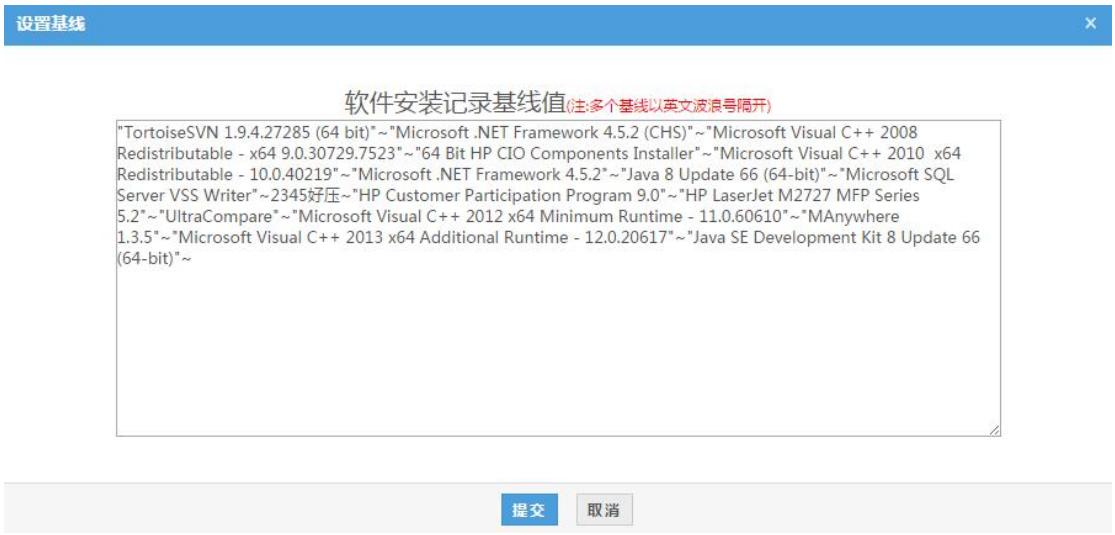


2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：



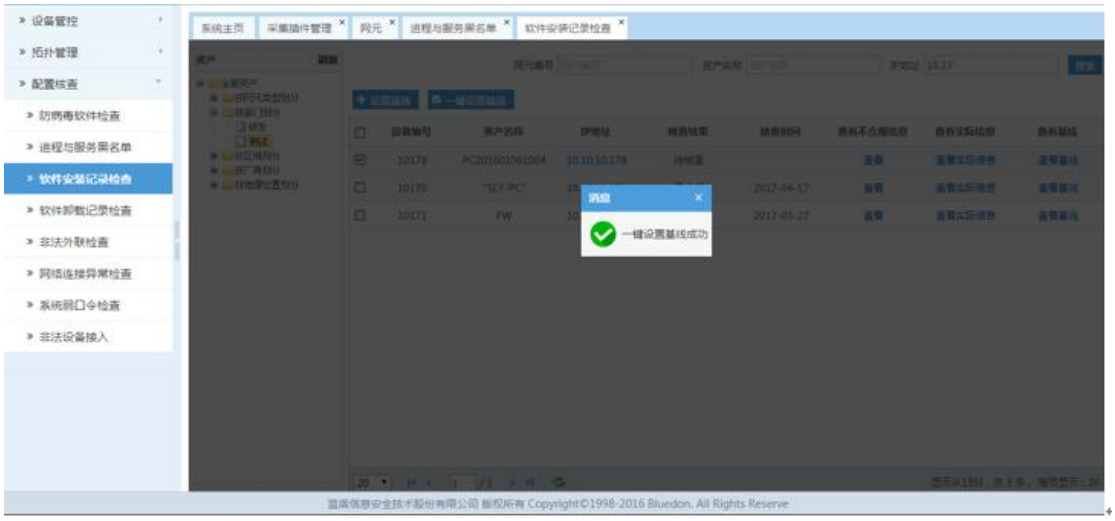
- 基线设置

1.手动设置软件安装记录黑名单基线，选择要设置基线的设备，点击**设置基线**，手动输入进程与服务，点击**提交**如下图：



2.选择基线值设置基线，点击**查看实际信息**，勾选基线值，点击**将选中项设置为基线**，如下图：

3.一键设置基线。即选择一个基线，可以运用到所有设备，选择一个设备的基线，点击**一键设置基线**，如下图：



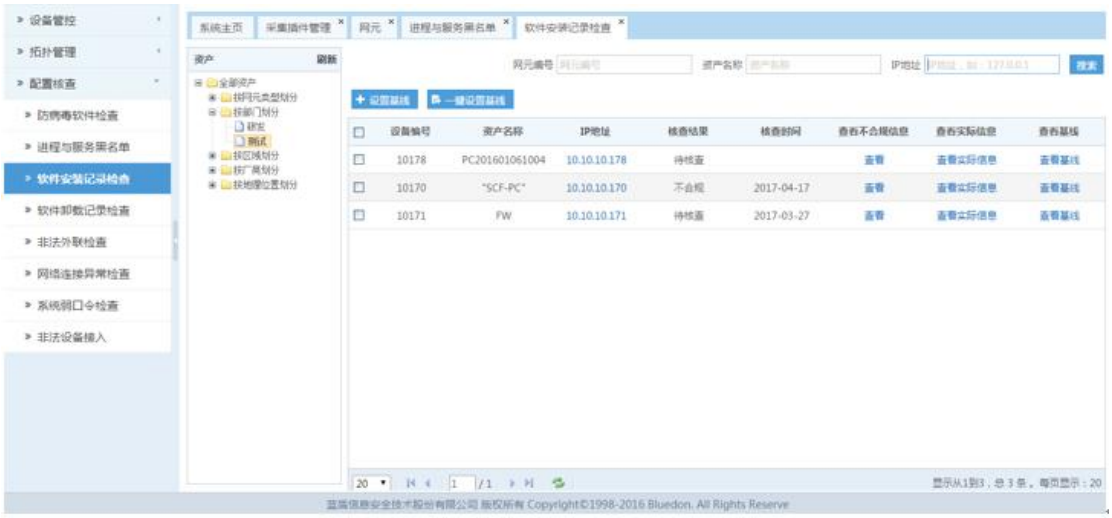
4.查看基线。点击右侧查看基线，可查看到所设置的基线，如下图：

- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。这里把设备最初安装的软件做为基线，检测时，把设备实时安装的软件与基线设置进行对比，如果软件列表比基线软件多，则设备非法安装了软件，返回不合规，并执行告警动作，与基线软件一样，返回合规；点击**查看**，可查看不合规信息，以便做出修改；没有做基线设置的，检测后返回无结果。

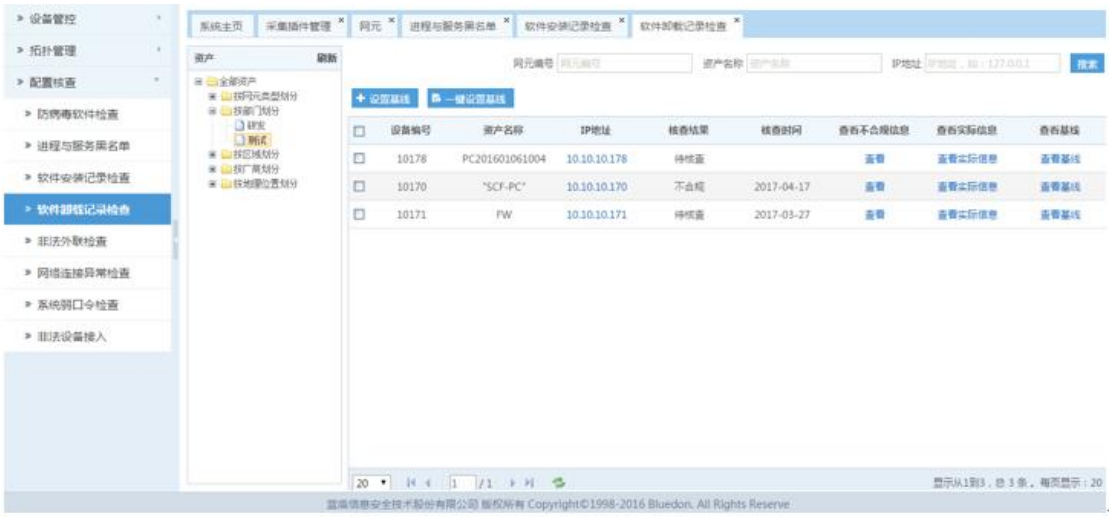
5.3.4 软件卸载记录检查

点击**配置核查>软件卸载记录检查**进入检查画面，系统可根据设置的基线，对资产进行软件卸载核查，如下图:

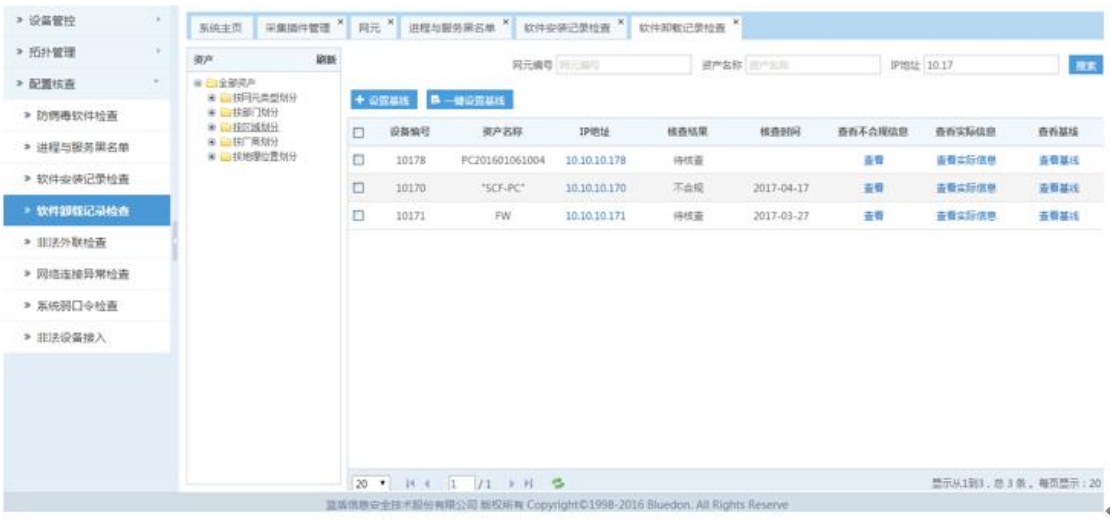


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：

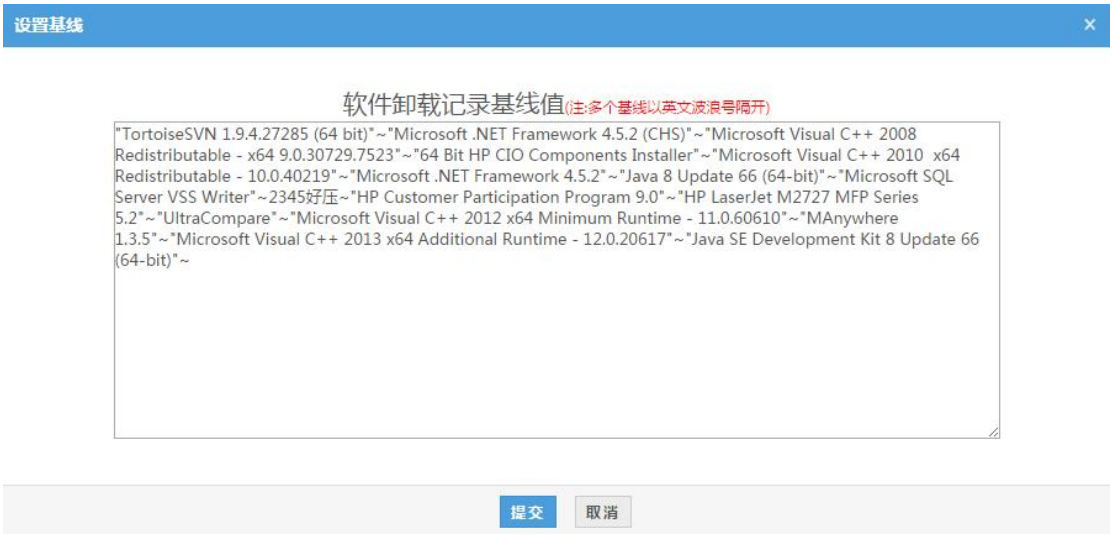


2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：



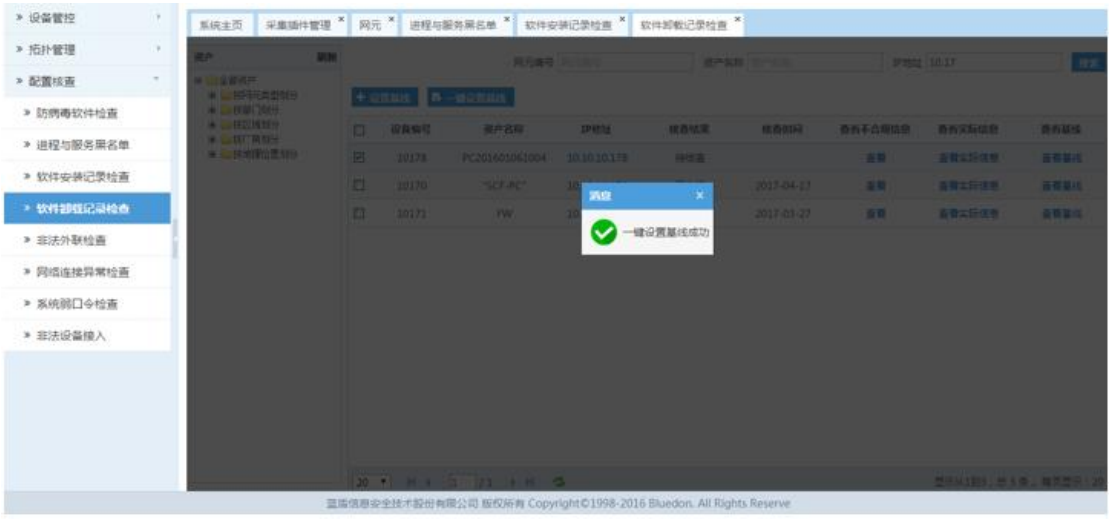
- 基线设置

1.手动设置软件卸载记录黑名单基线，选择要设置基线的设备，点击**设置基线**，手动输入进程与服务，点击**提交**如下图：

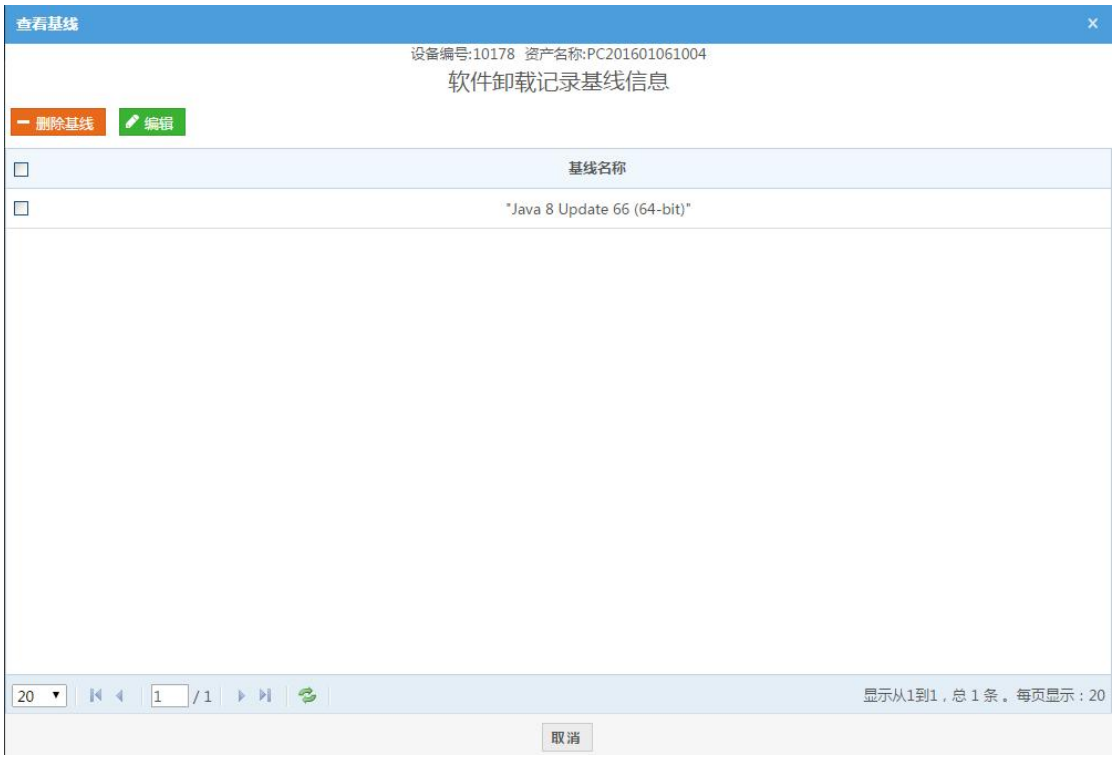


2.选择基线值设置基线，点击**查看实际信息**，勾选基线值，点击**将选中项设置为基线**，如下图：

3.一键设置基线。即选择一个基线，可以运用到所有设备，选择一个设备的基线，点击**一键设置基线**，如下图：



4.查看基线。点击右侧查看基线，可查看到所设置的基线，如下图：

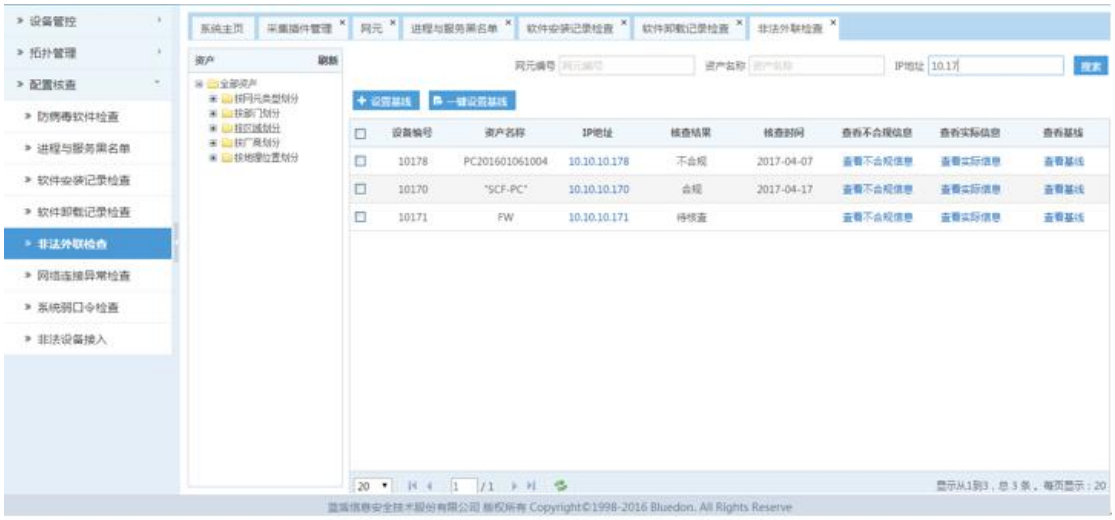


- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。这里把设备必要的软件做为基线，检测时，把设备实时安装的软件与基线设置进行对比，如果软件列表没有基线软件，则软件被非法卸载，返回不合规，并执行告警动作，如果软件列表有基线软件，返回合规；点击**查看**，可查看不合规信息，以便做出修改；没有做基线设置的，检测后返回无结果。

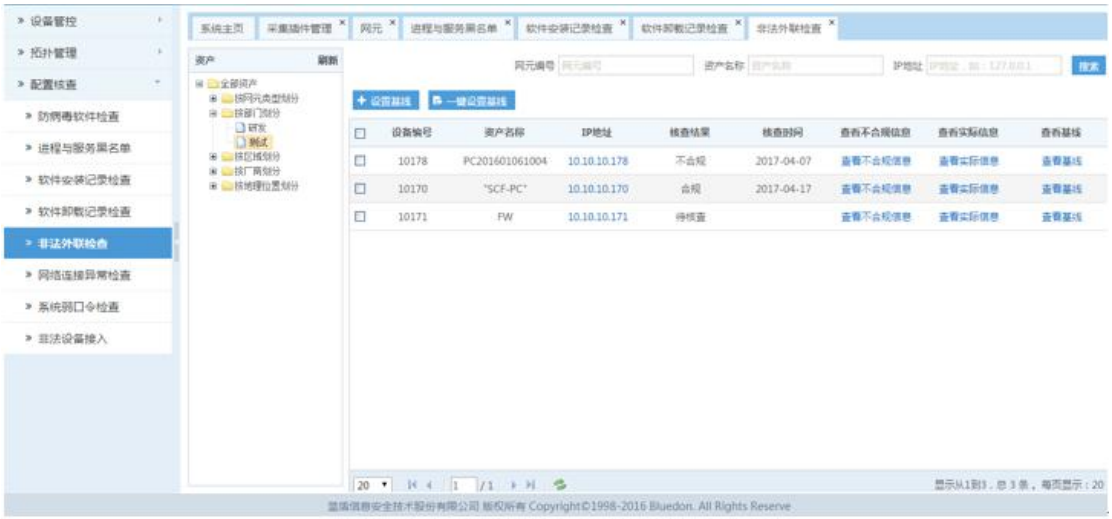
5.3.5 非法外联检查

点击**配置核查>非法外联检查**进入检查画面，系统可根据设置的基线，对资产进行非法外联核查，如下图：

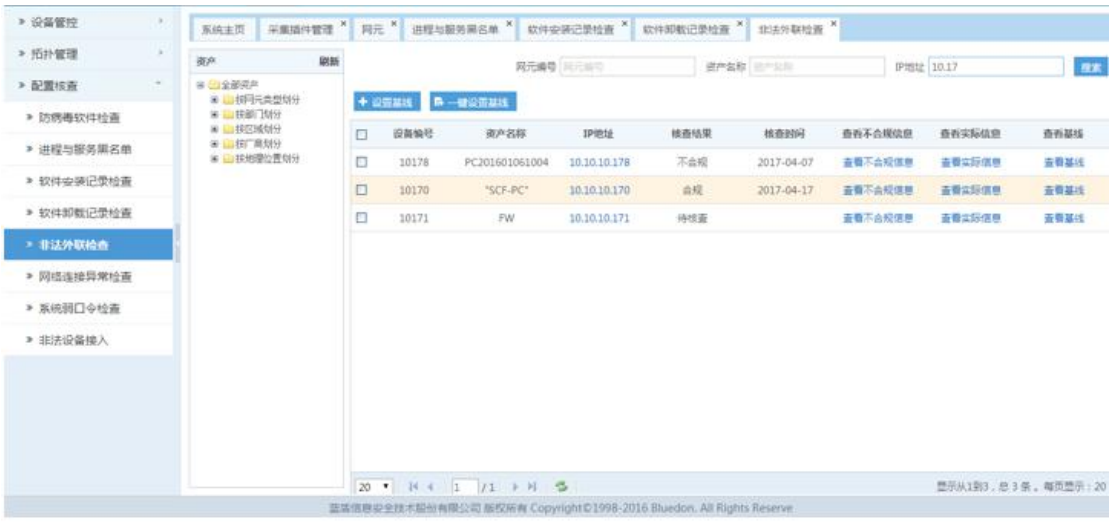


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：



2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：

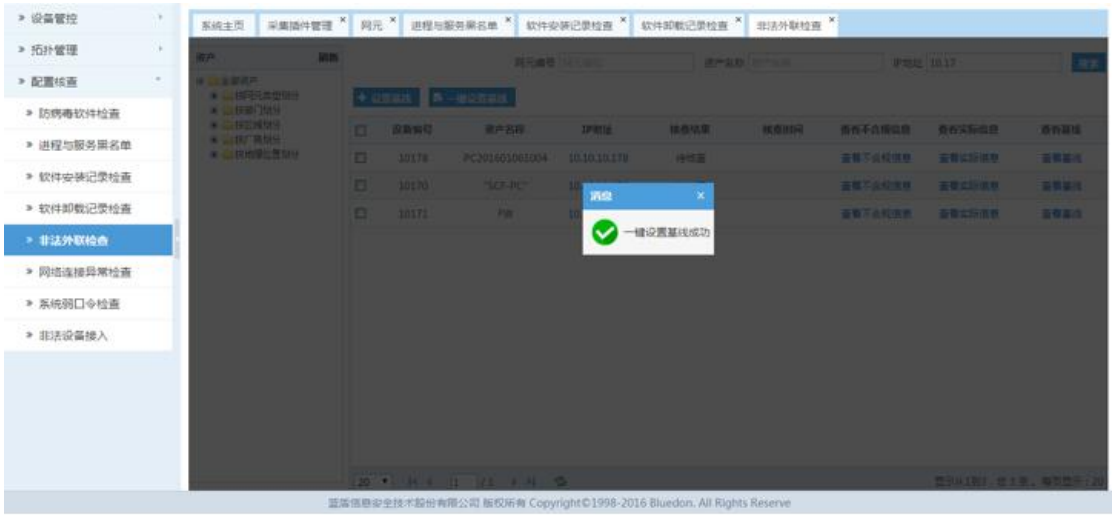


- 基线设置

1.手动设置外联检查基线，选择要设置基线的设备，点击**设置基线**，手动输入基线值，点击**提交**如下图：

2.选择基线值设置基线，点击**查看实际信息**，勾选基线值，点击**将选中项设置为基线**，如下图：

3.一键设置基线。即选择一个基线，可以运用到所有设备，选择一个设备的基线，点击**一键设置基线**，如下图：



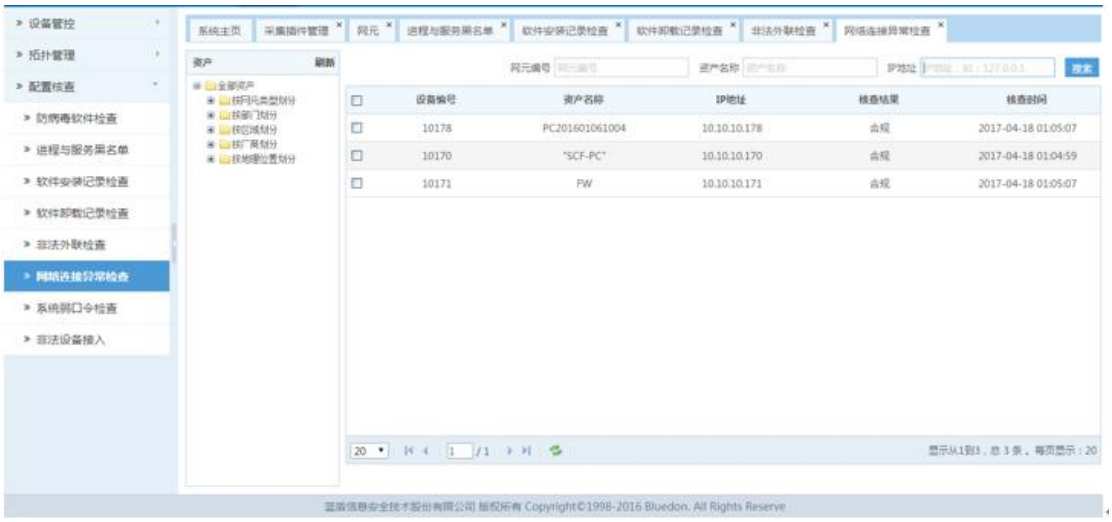
4.查看基线。点击右侧查看基线，可查看到所设置的基线，如下图：

- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。这里把设备必要的网口信息做为基线，检测时，把设备实际网口信息与基线设置进行对比，如果实际网口信息比基线数据不符，则设备有非法外联(非法接入的网络设备)，返回不合规，并执行告警动作，如果实际网口信息比基线数据一致，返回合规；没有做基线设置的，检测后返回无结果。

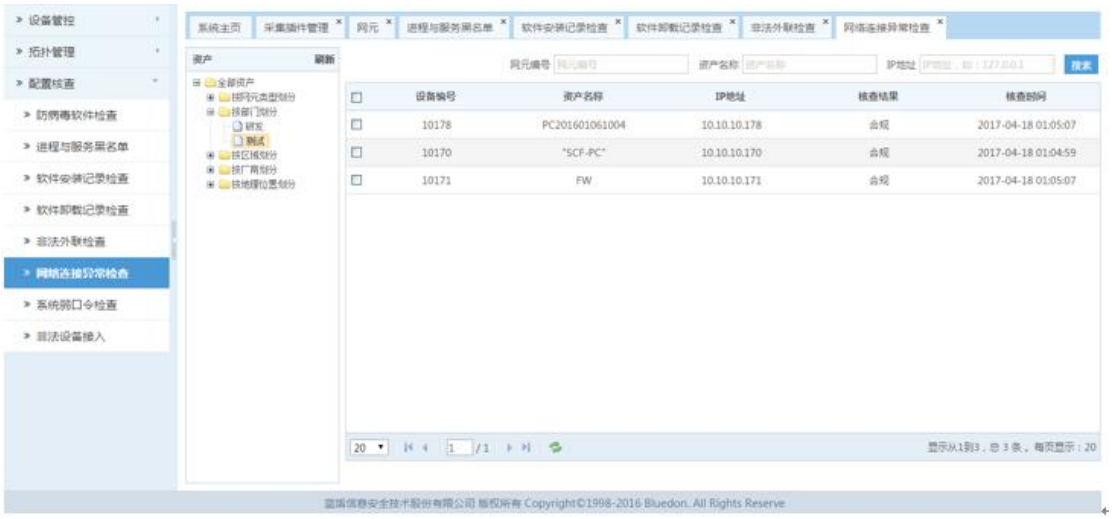
5.3.6 网络连接异常检查

点击**配置核查>网络连接异常检查**进入检查画面，系统可对资产进行核查，如下图：

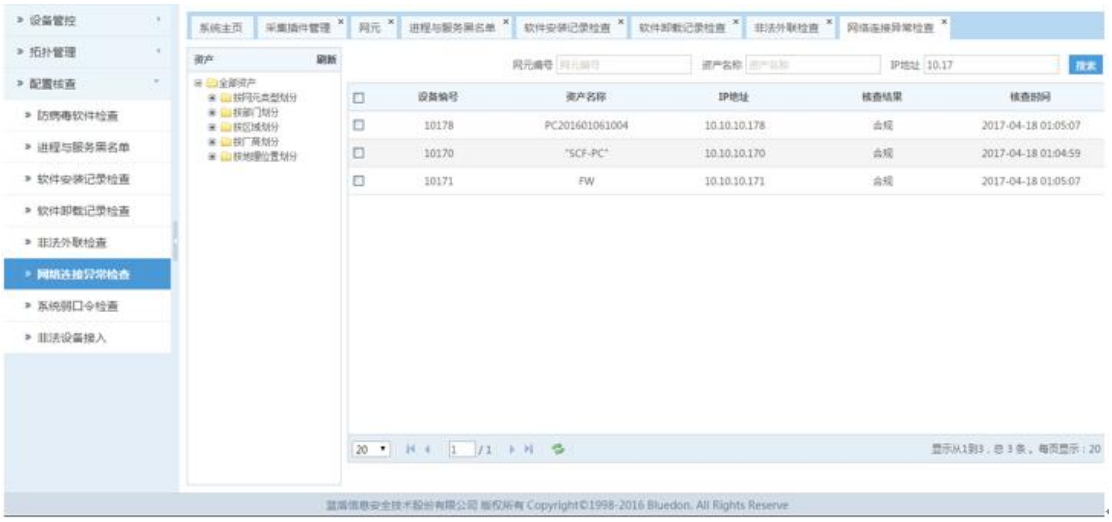


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：



2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：



- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。这里不用设置基线，可直接进行检测；点击**立即检查**，系统立即对选定设备的联通性进行检测，如网络连接异常（不通），则返回不合规，并执行告警动作；如可正常通信，则返回合规。

5.3.7 系统弱口令检查

点击**配置核查>系统弱口令检查**进入检查画面，系统可对资产进行核查，如下图：

- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：

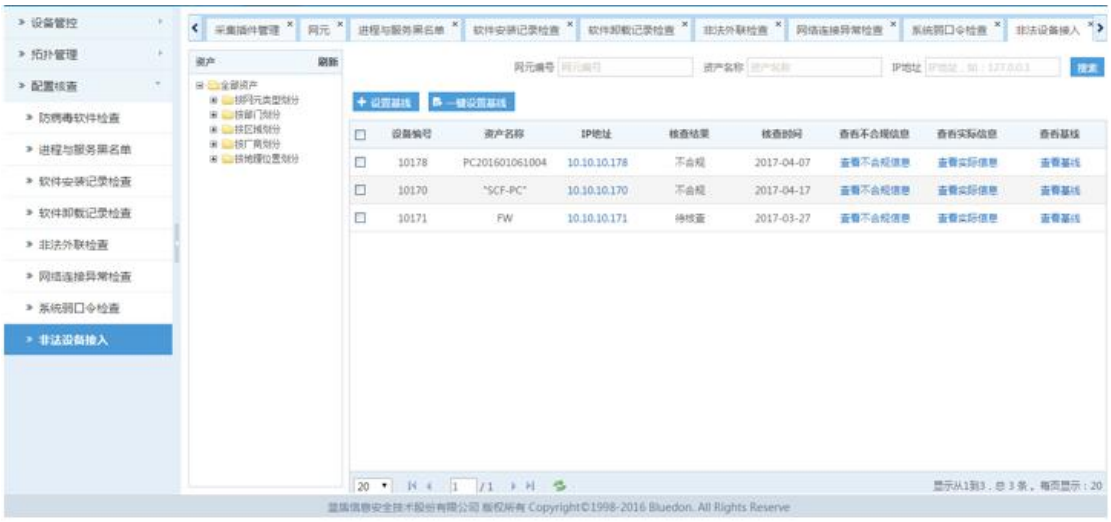
2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：

- 核查结果

在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。这里不用不用设置基线，可直接进行检测；点击**立即检查**，系统立即对选定设备的弱口令进行检测，如存在弱口令，则返回不合规，并执行告警动作；如无弱口令，则返回合规。

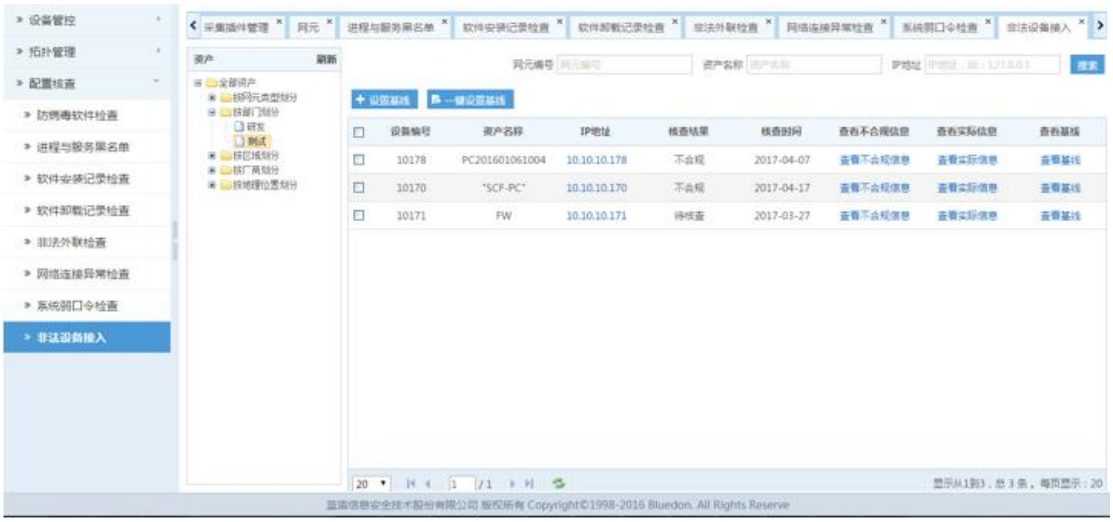
5.3.8 非法设备接入

点击**配置核查>非法设备接入**进入检查画面，系统可根据设置的基线，对资产进行非法外联核查，如下图：

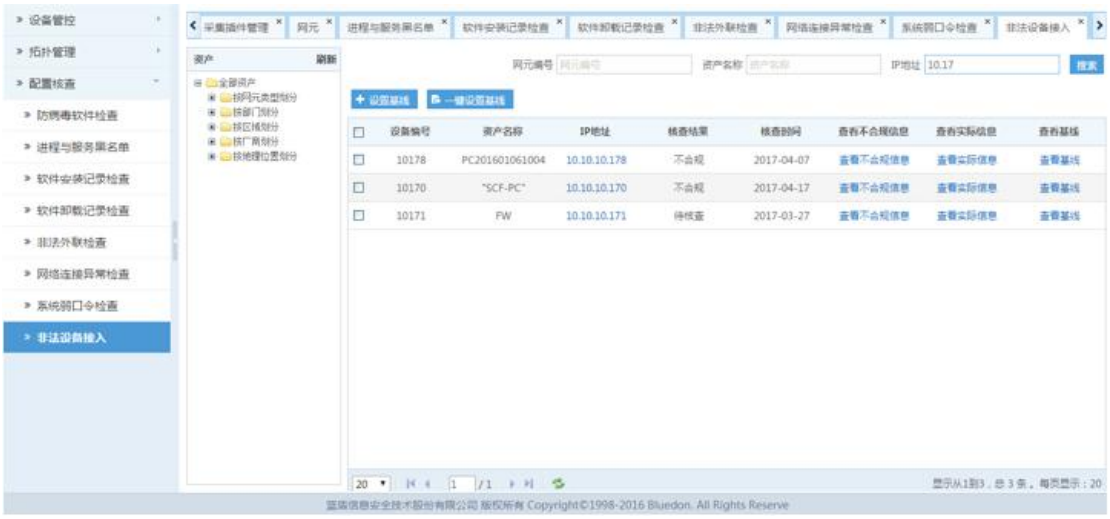


- 资产查询

1.点击左侧树型结构资产分部，选择对应的资产类型、部门、区域、厂商等，对资产进行检索，如选择按部门型划分>测试，如下图：

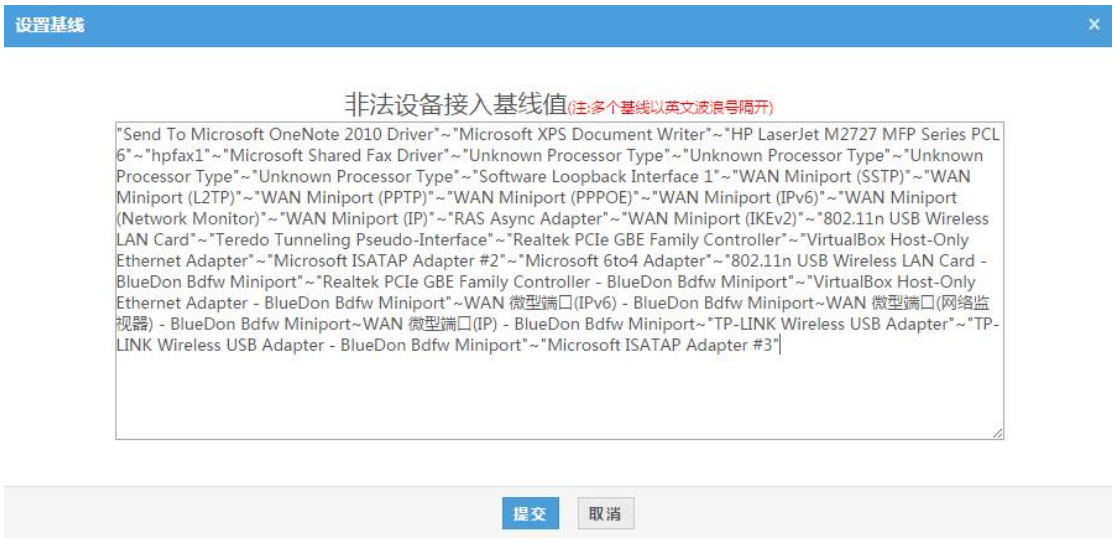


2.输入网元编号、资产名称、IP 地址，点击搜索，查询对应的资产，如下图：

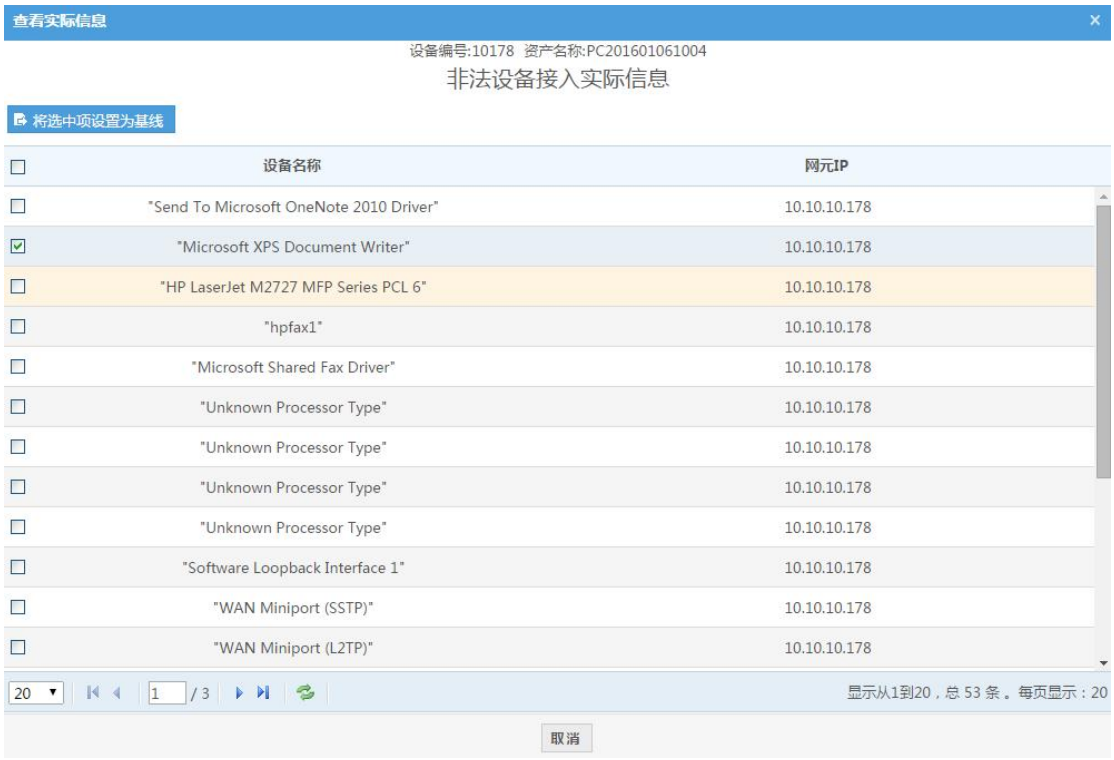


- 基线设置

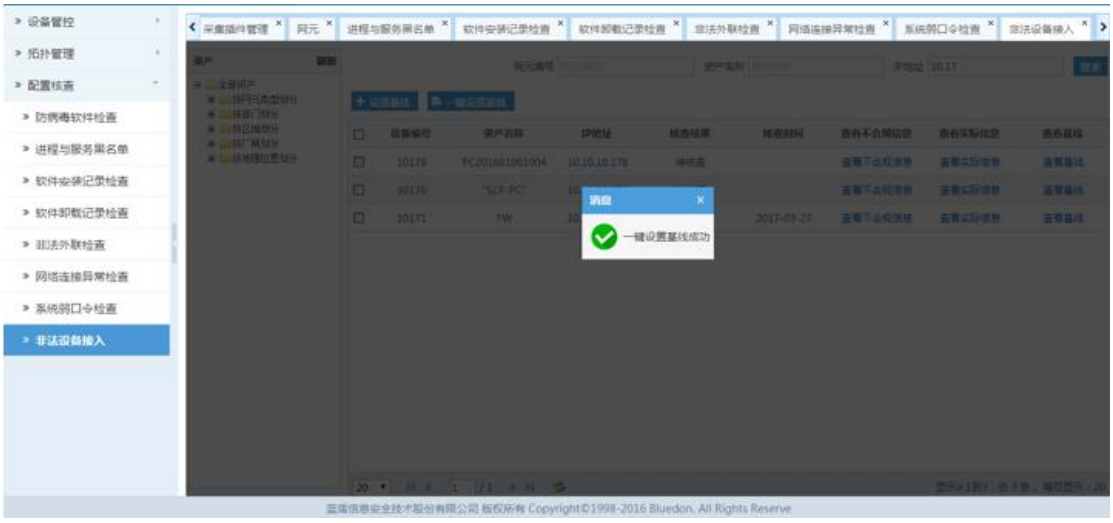
1.手动设置外联检查基线，选择要设置基线的设备，点击**设置基线**，手动输入基线值，点击**提交**如下图：



2.选择基线值设置基线，点击**查看实际信息**，勾选基线值，点击**将选中项设置为基线**，如下图：



3.一键设置基线。即选择一个基线，可以运用到所有设备，选择一个设备的基线，点击**一键设置基线**，如下图：



4.查看基线。点击右侧查看基线，可查看到所设置的基线，如下图：

- 核查结果

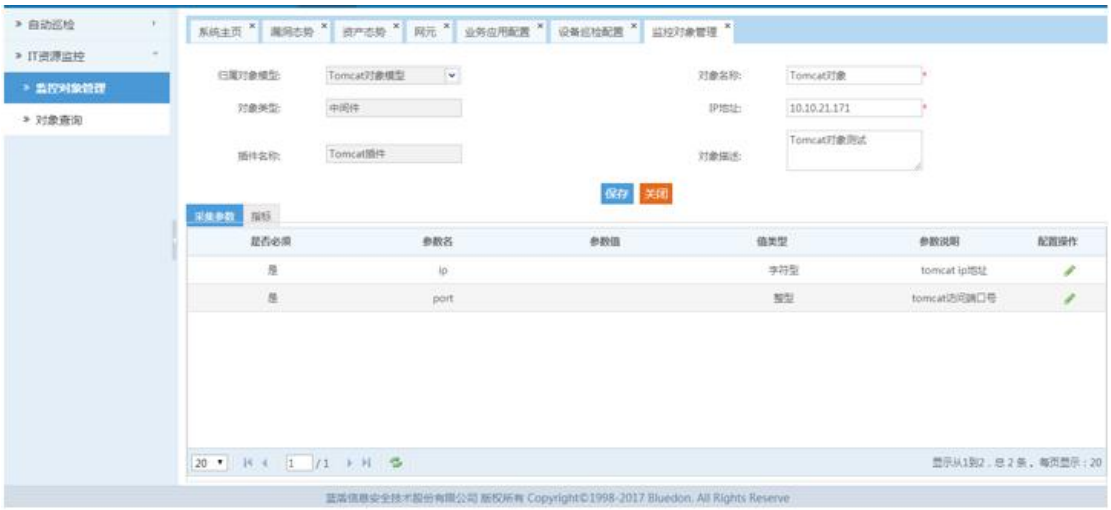
在**配置核查**插件中选择核查类型、核查周期和被核查的资产列表，启动**配置核查**插件，每过一个周期，系统会更新下核查结果，分别是待核查、核查完毕、合规与不合规。这里把设备必要的网口信息做为基线，检测时，把设备实际网口信息与基线设置进行对比，如果实际网口信息比基线数据不符，则设备有非法设备接入，返回不合规，并执行告警动作，如果实际网口信息比基线数据一致，返回合规；没有做基线设置的，检测后返回无结果。

5.4 业务应用管理

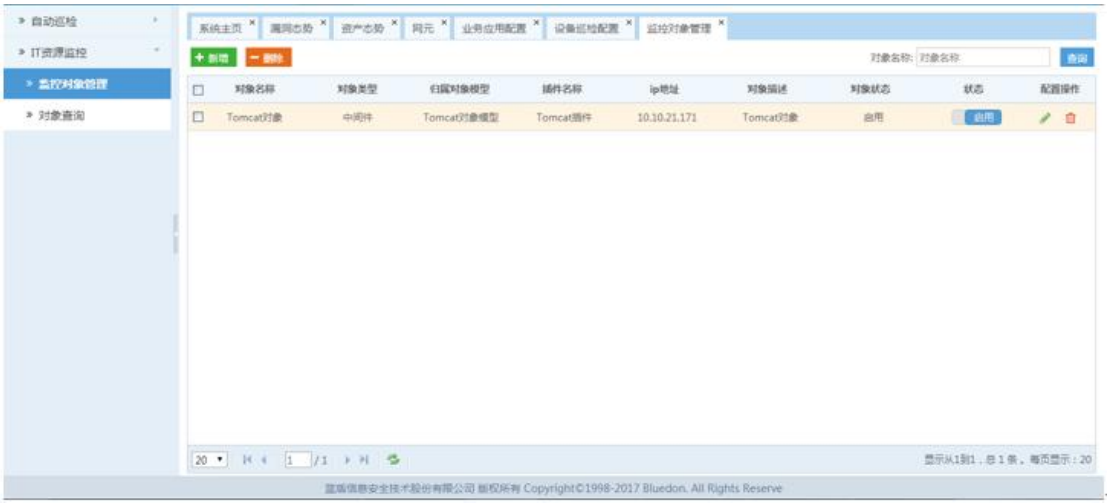
用户可以构建业务拓扑，反映业务支撑系统的资产构成。通过业务拓扑建立业务中各个管理对象的分布和联系，可以是实际的物理拓扑，也可以是业务相关的逻辑联系，方便用户了解和查看此业务相关对象的实际状况。

5.4.1 业务应用配置

用户在新增**业务应用配置**之前需要先在**统一监控>IT 资源监控>监控对象管理**中新增支撑对象，如下图：

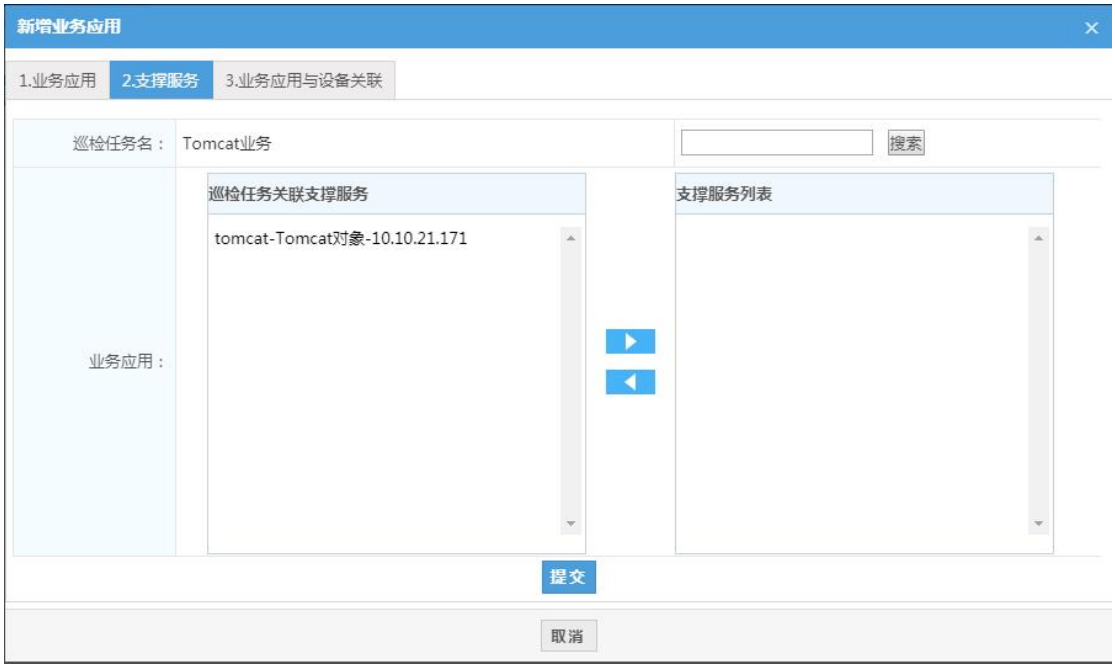


并开启状态，如下图：

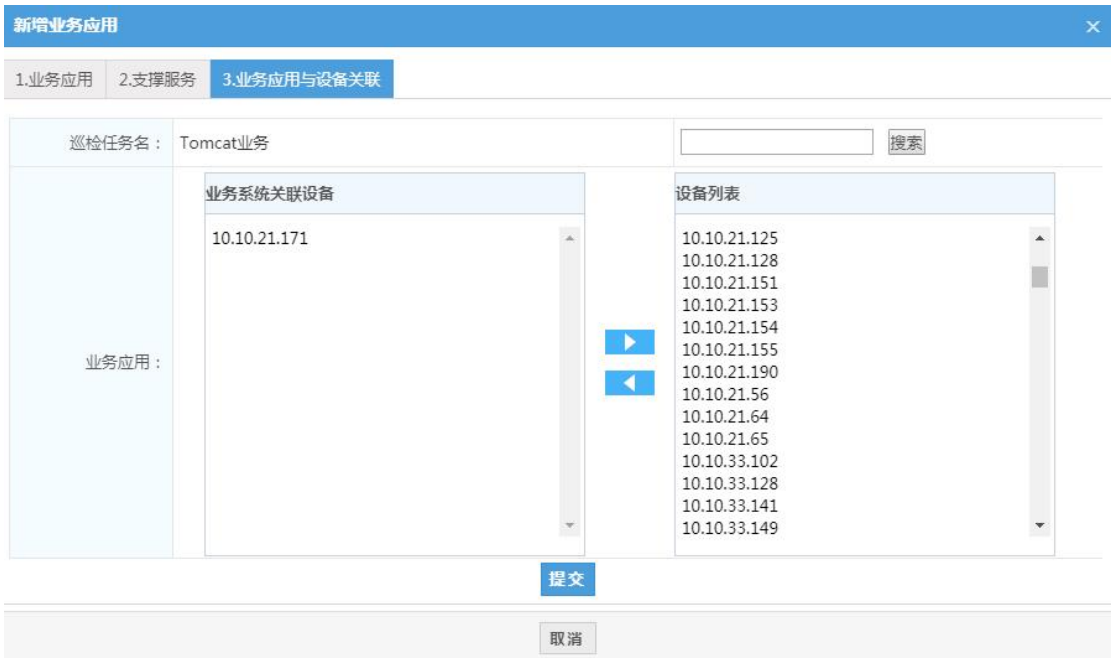


再点击**资产管理>业务应用管理>业务应用配置**进入页面，用户可以根据自己的需求新增、编辑和删除。新增如下图：

其中业务编号、业务系统名可自定义，url 为对应支撑服务的 IP 入口，点击提交。先前新增的监控对象出现在支撑服务列表中，将其左选入关联支撑服务中，如下图：



点击提交，进入 **3.业务应用与设备关联**界面，在设备列表中找到对象监控对应的 IP，如下图：



再点击提交，则完成业务配置的新增，如下图：

其中，一个设备可以对应多个支撑服务，点击**业务拓扑配置**可以查看其拓扑关心，如下图：

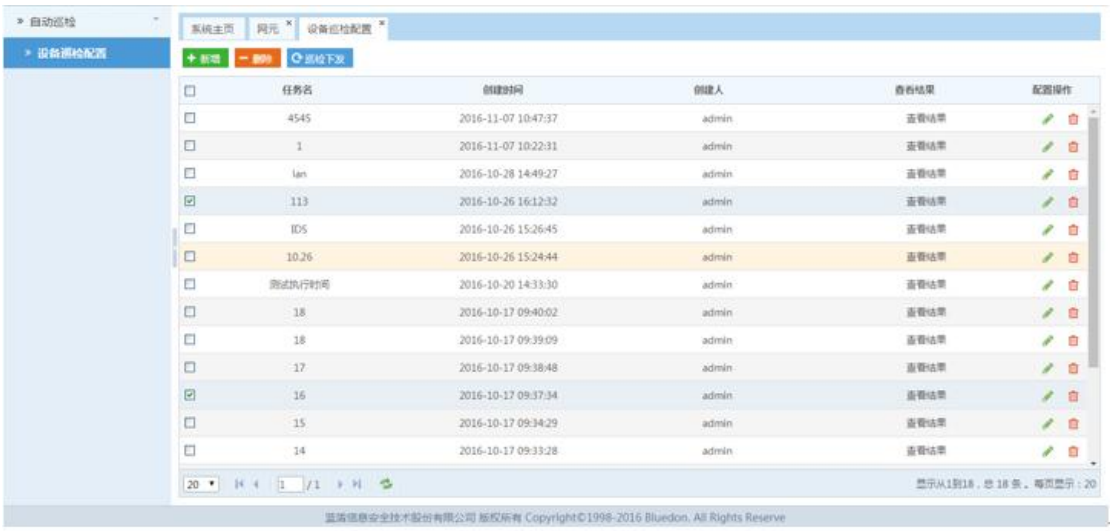
5.4.2 业务应用列表

点击**资产管理>业务应用管理>业务应用列表**进入页面，可看到新增的业务信息，如下图：

点击**故障定位**，可看到改业务的拓扑信息和关联设备的相关信息，如下图

5.4.3 业务应用巡检

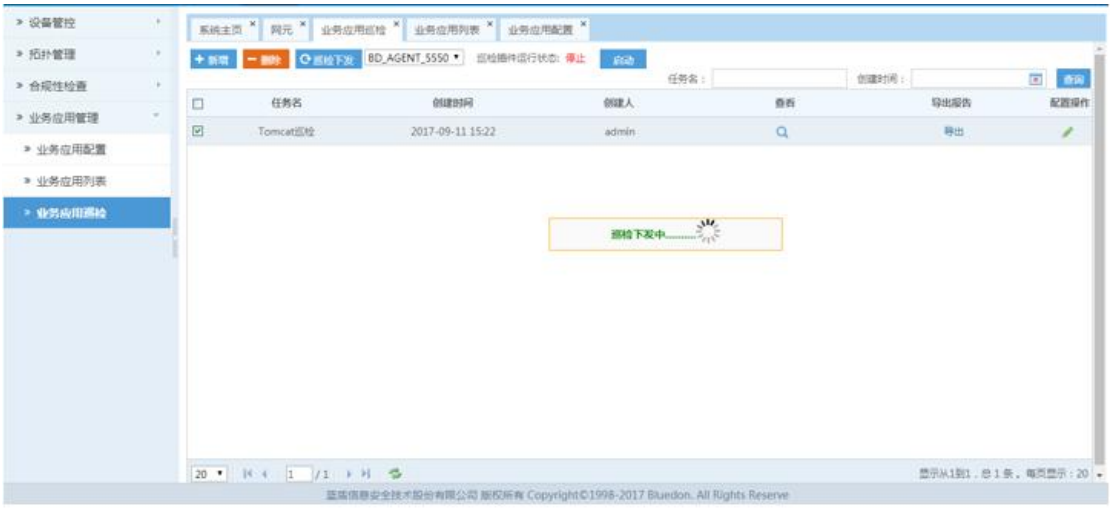
点击**资产管理>业务应用管理>业务应用巡检**进入相关界面。页面显示了任务名的基本信息，用户可以根据自己的需求，新增、配置、删除和下发任务，如下图：



点击**业务应用管理>业务应用巡检>新增**按钮，用户可以在弹出的新增任务页面中提交巡检任务信息，如下图：

提交成功后，业务应用列表中有**业务应用配置**新增的业务，选中左移至关联业务应用，点击提交，如下图：

选中巡检任务，选择传感器，再点击**巡检下发**按钮，如下图：



到了设置的任务开始时间，任务就会运行。点击查看图标，可看到结果，如下图：

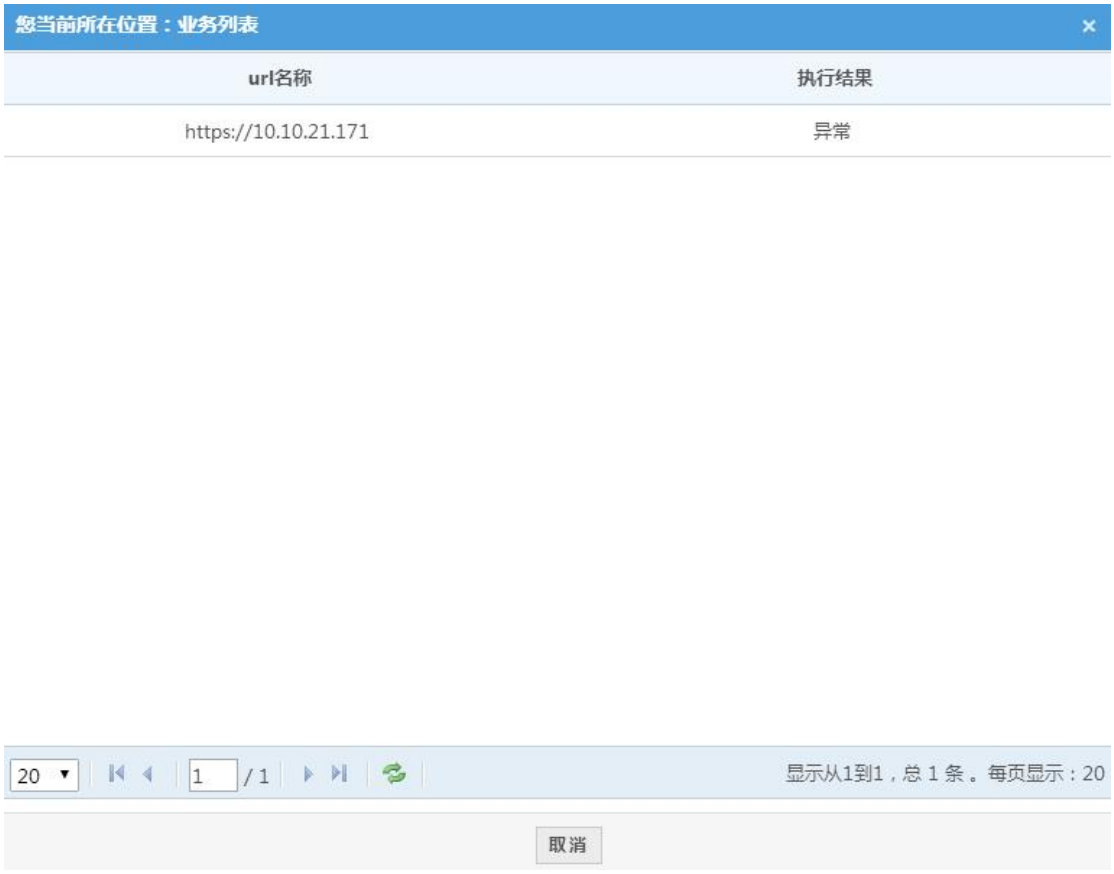
插件需要停止状态才可下发任务，且开始时间之后才有巡检结果。

对于结果可以导出报告，如下图：

	A	B	C	D	E	F	G
1	任务名称	创建时间	创建人	URL	状态	应时间(毫	备注
2	Tomcat巡检	2017-09-11 15:22:15	admin	https://10.10.21.171	不可用	75	Tomcat巡检备注

同时，对于状态为不可用的业务则认为异常，在**资产管理>业务应用管理>业务应用列表**中标红显示，如下图：

点击异常数，则显示异常的具体信息，如下图：



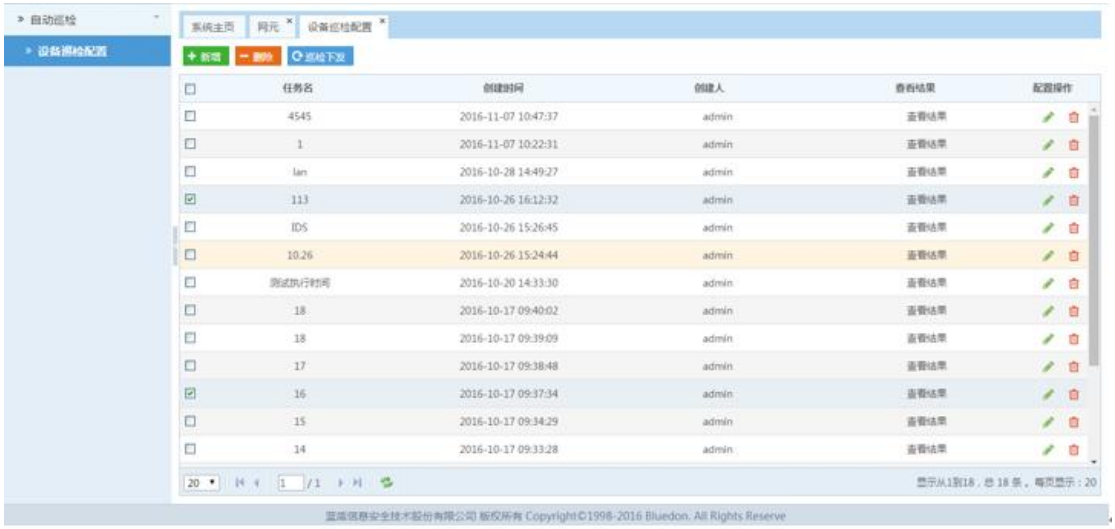
第 6 章　统一监控

6.1 自动巡检

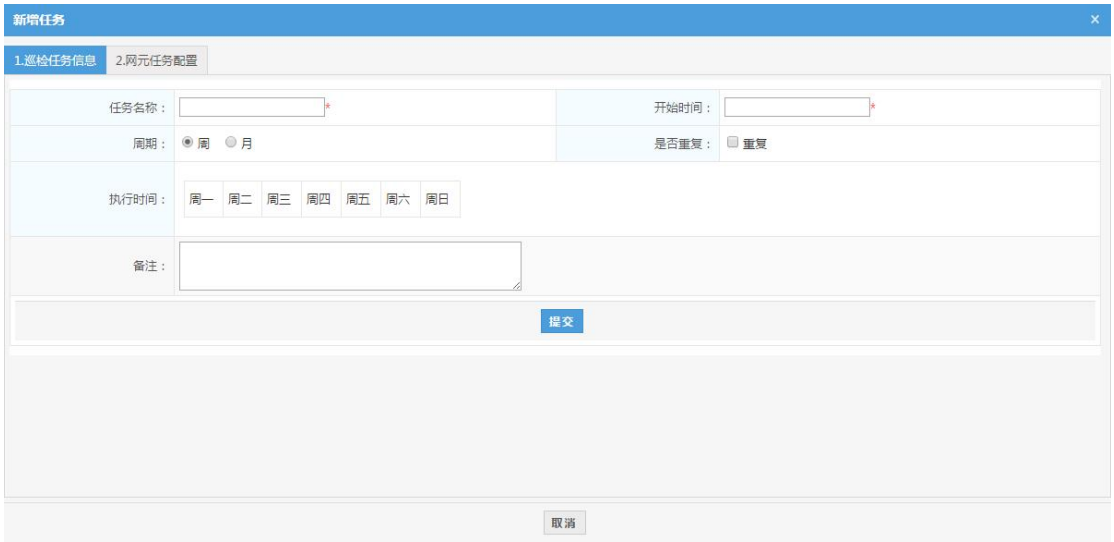
自动巡检是将各类选定的网元设备在选定的时间节点进行巡检，巡检的目的是对不同时间网元设备的运行状况进行整理，运行状态包括网元设备的 CPU 使用率类存使用率，硬盘使用率，网络情况和进程运行情况。

6.1.1 设备巡检配置

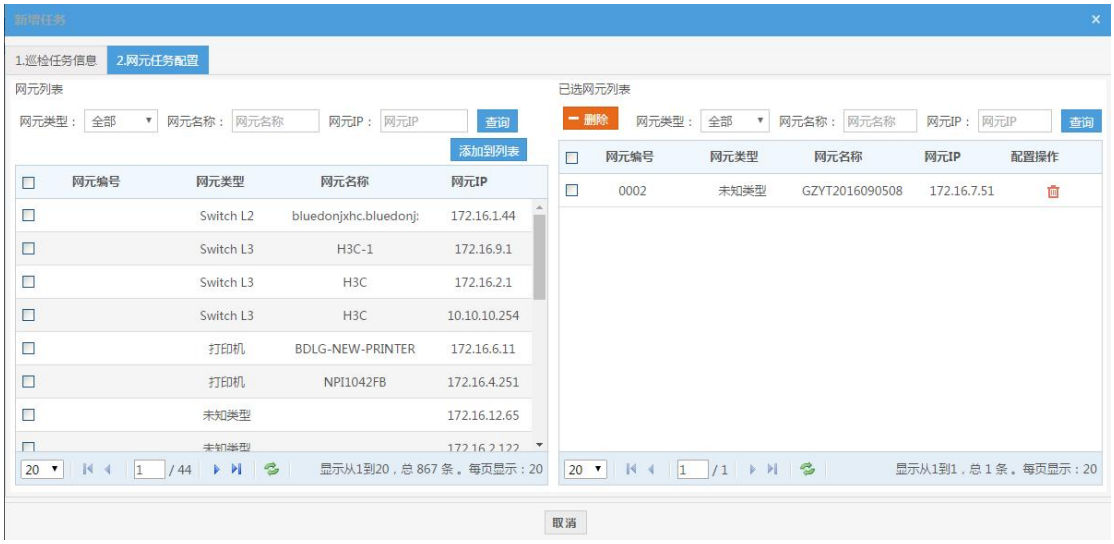
点击**自动巡检>设备巡检配置**进入页面，页面显示了任务名的基本信息，用户可以根据自己的需求，新增、配置、删除和下发任务，如下图：



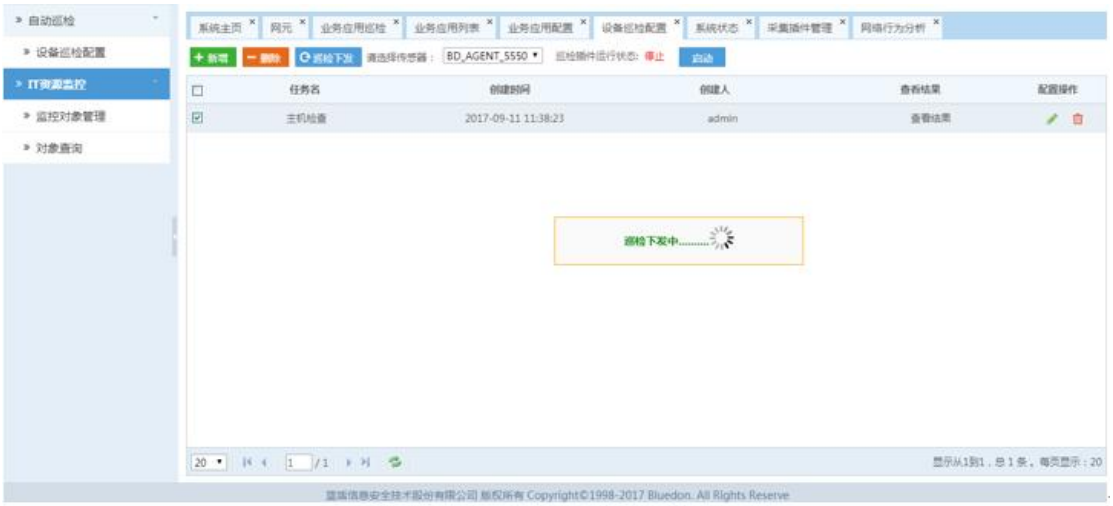
点击**自动巡检>设备巡检配置>新增**按钮，用户可以在弹出的新增任务页面中提交巡检任务信息，如下图：



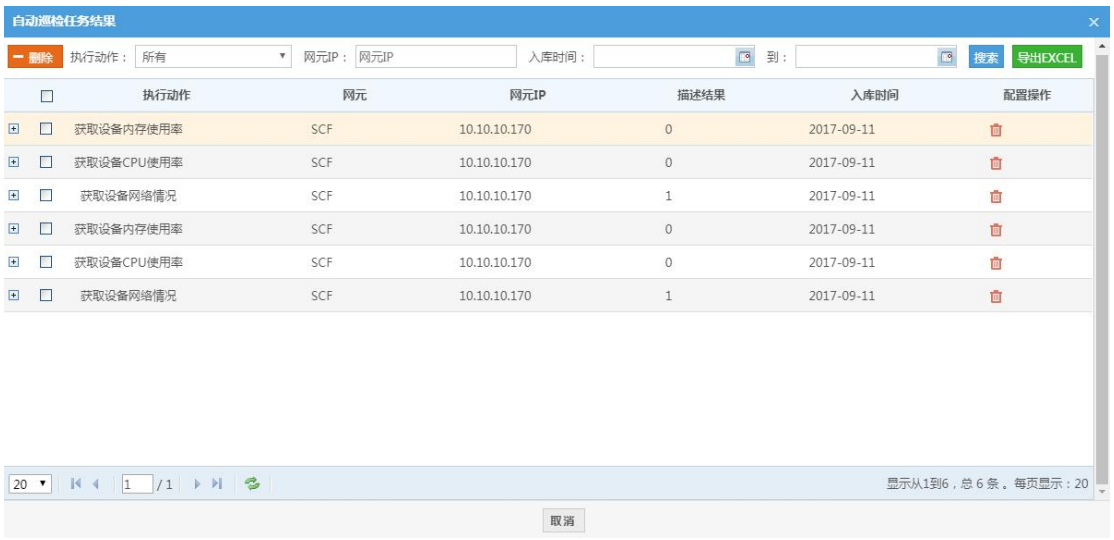
提交成功后，可以配置网元任务，如下图：



最后，需要选定该任务名，选择传感器，并点击**自动巡检>设备巡检配置>巡检下发**按钮，将该任务下发，如下图：



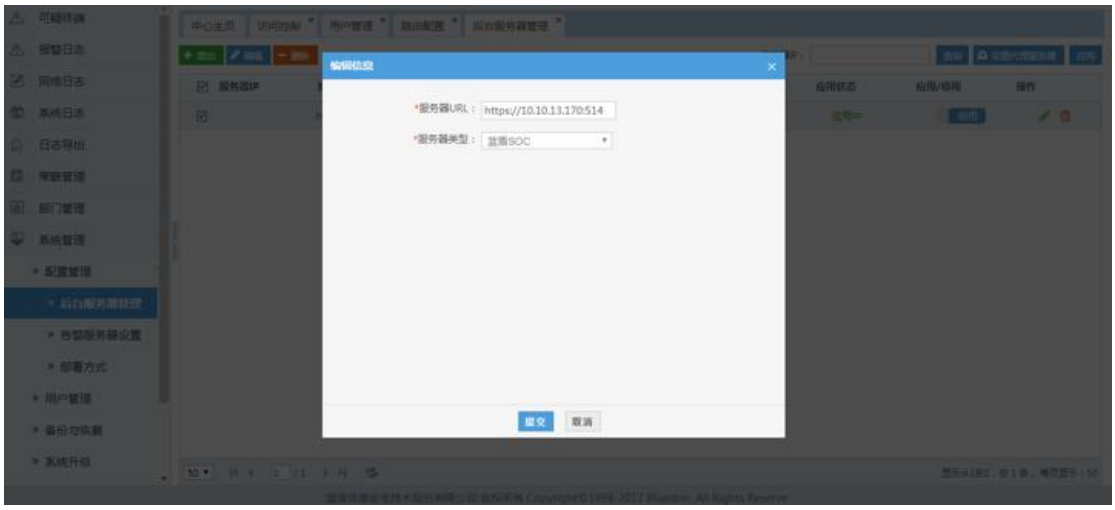
任务下发后，点击**自动巡检>设备巡检配置>查看结果**可以看到巡检任务后的结果，如下图：


自动巡检任务结果
删除
执行动作：
所有
网元IP：
网元IP
入库时间：
到：
搜索
导出EXCEL
执行动作
网元
网元IP
描述结果
入库时间
配置操作
获取设备内存使用率 SCF 10.10.10.170 0 2017-09-11
获取设备CPU使用率 SCF 10.10.10.170 0 2017-09-11
获取设备网络情况 SCF 10.10.10.170 1 2017-09-11
获取设备内存使用率 SCF 10.10.10.170 0 2017-09-11
获取设备CPU使用率 SCF 10.10.10.170 0 2017-09-11
获取设备网络情况 SCF 10.10.10.170 1 2017-09-11
20
1 / 1
显示从1到6，总 6 条。每页显示：20
取消

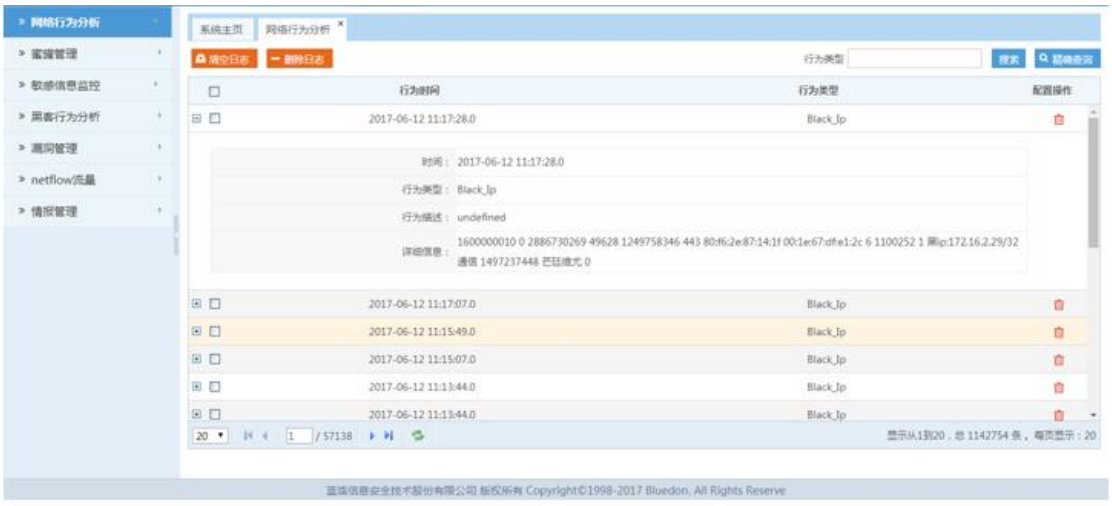
第 7 章　安全分析

7.1 网络行为分析

信息安全审计系统可设置为向 SOC 服务器发送日志，设置格式如下图：

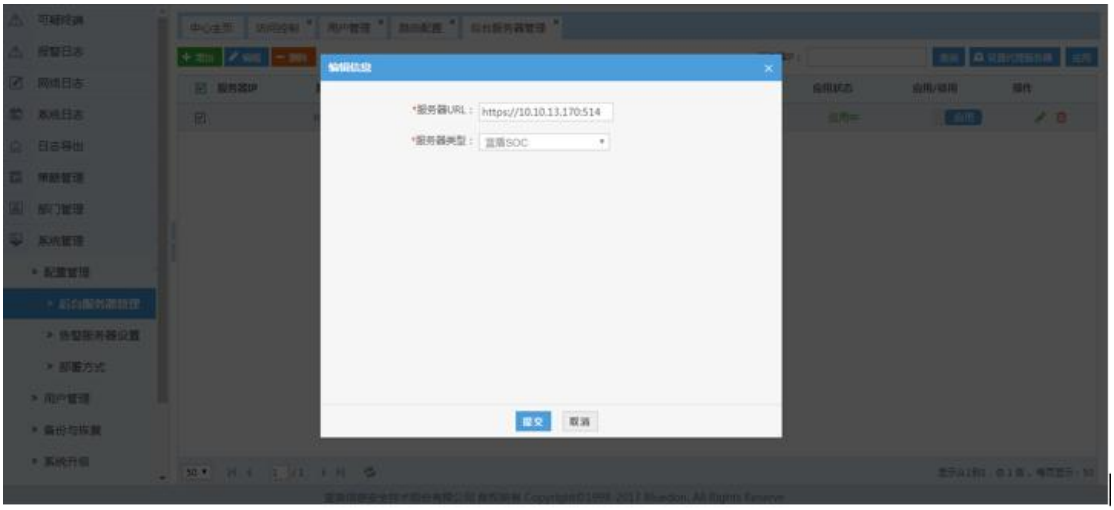


配好服务器 URL 之后需要将其状态设置为应用中，否则不予发送日志。SOC v5.1 对于接收到的日志会自动进行识别，如果收到的信息安全审计日志的内容含有字段 auditlog:agentlog:ABNORMAL-BEHAVIOUR，识别为行为分析，并在**网络行为分析体现出来**，如下图：

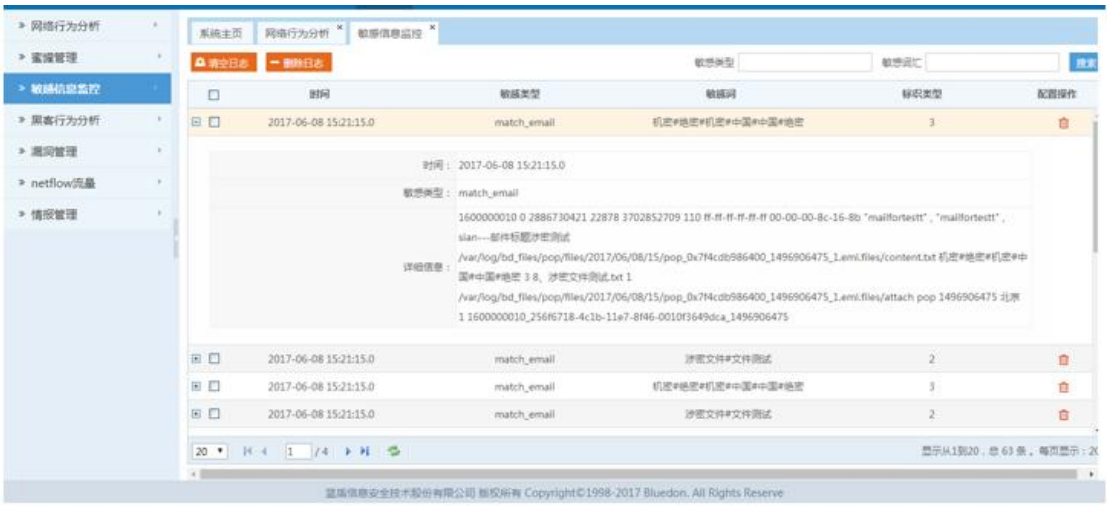


7.2 敏感信息监控

信息安全审计系统可设置为向 SOC 服务器发送日志，设置格式如下图：



如果收到的信息安全审计日志的内容含有字段 auditlog:agentlog:SENSITIVE，则识别为敏感信息，并在**敏感信息监控**中体现出来，如下图：



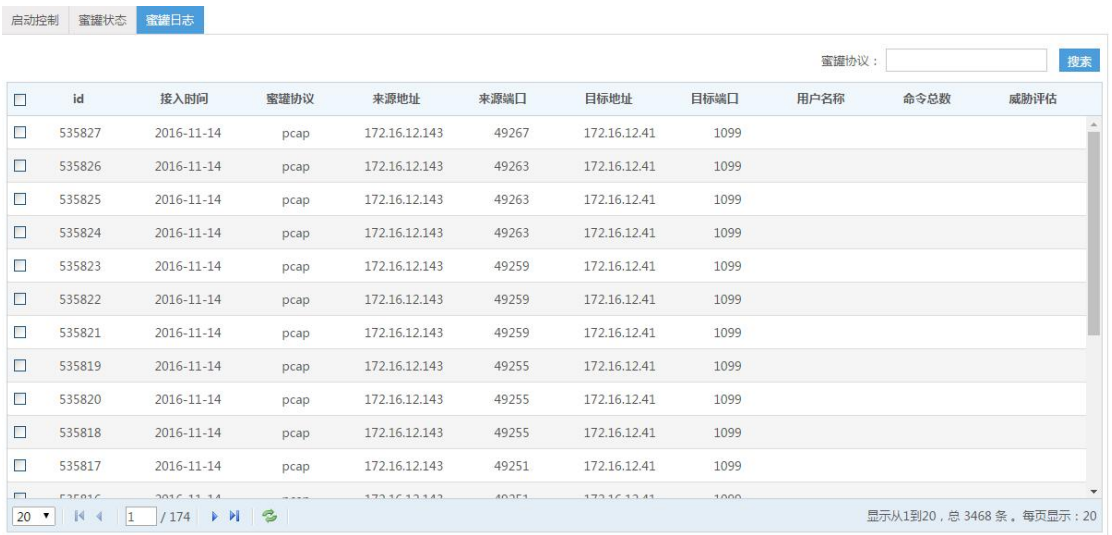
7.3 蜜罐管理

SOC 具备蜜罐管理，自动反扫描攻击源，扫描器自动发现，特种木马监控等功能，并生成对应日志，并对日志进行统计分析。

用户可以点击**蜜罐管理>启动控制**，对蜜罐进行启动、重启等操作，（系统默认蜜罐为“停止”状态）启动后如下图：

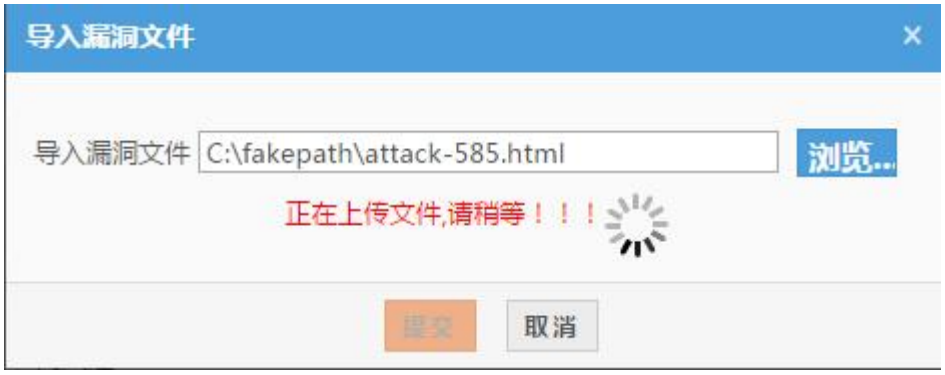
蜜罐管理>蜜罐状态包含了 id，接入时间，蜜罐协议，来源地址，来源端口，目标地址，目标端口等信息，用户可以根据协议名称来搜索。如下图：

蜜罐管理>蜜罐日志包含了 id，接入时间，蜜罐协议，来源地址，来源端口，目标地址，目标端口等信息，用户可以根据蜜罐协议来搜索。如下图：

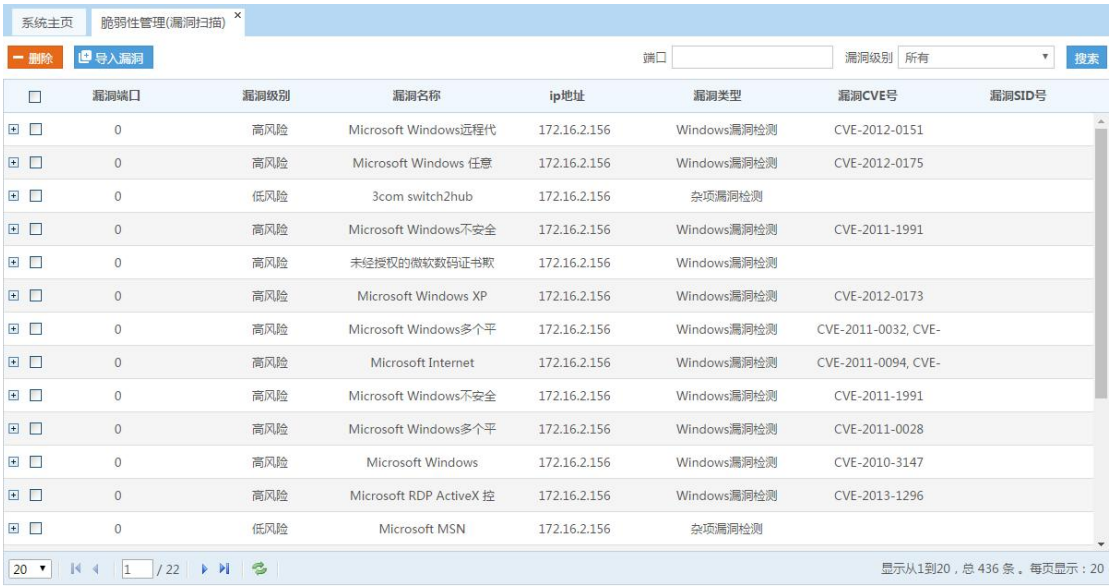


7.4 漏洞管理

用户可以点击**漏洞管理>导入漏洞**，导入.html 格式的漏洞文件，如下图：



导入成功后，显示漏洞信息，包括漏洞端口、漏洞级别、漏洞名称等信息。用户可以根据端口、漏洞级别来搜索，如下图：

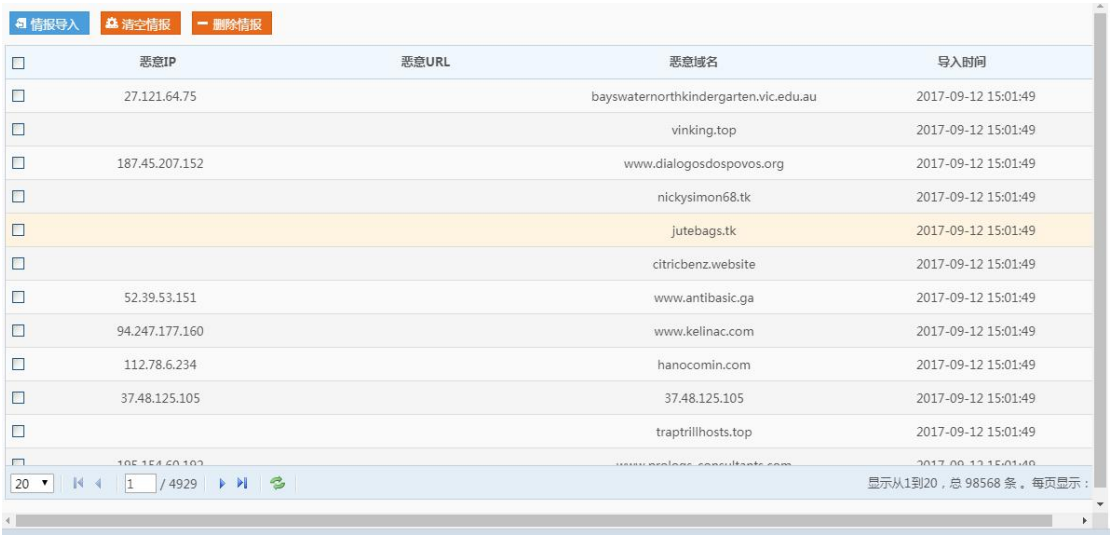


7.5 情报管理

7.5.1 情报导入

用户可以点击**安全分析>情报管理>情报导入**，点击 情报导入 导入 csv 格式的漏洞文件，如下图：

导入成功后，显示情报信息，包括恶意 IP、恶意 URL、恶意域名等信息，选中情报点击 删除情报 可以将该情报删除，点击 清空情报 可以将所有情报清空，如下图：



7.5.2 舆情病毒

用户可以点击**安全分析>情报管理>舆情病毒**，点击 舆情病毒导入 导入 csv 格式的舆情病毒文件，如下图：

导入成功后，显示病毒信息，包括病毒名称、病毒类型、严重级别等信息，选中情报点击 删除情报 可以将该情报删除，点击 清空情报 可以将所有情报清空，如下图：

7.5.3 漏洞情报

用户可以点击**安全分析>情报管理>漏洞情报**，点击 漏洞情报导入 导入 xml 或 xls 或 xlsx 格式的漏洞情报文件，如下图：

导入成功后，显示漏洞信息，包括漏洞级别、漏洞名称、漏洞类型等信息，选中情报点击 删除情报 可以将该情报删除，点击 清空情报 可以将所有情报清空，如下图：

第 8 章 SIEM

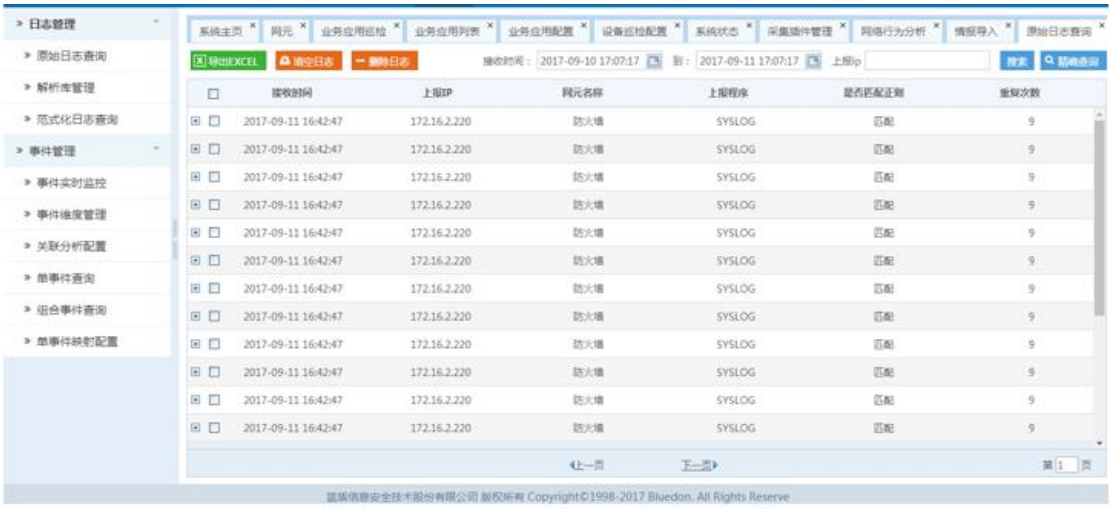
8.1 日志管理

8.1.1 原始日志查询

采集日志是中科云量安全综合管理平台的重要功能，目前支持采集

SYSLOG、WMI、SNMP TRAP、FTP 等格式的日志。日志采集到了之后，经过解析库解析入库，会形成范式化日志；范式化日志可以通过内置规则形成单事件，通过关联分析配置可以对生成的单事件形成组合事件；不同的事件会触发对应的告警策略；告警策略会形成实时告警；最后形成各自的报表。从原始日志到事件生成、触发告警、形成报表一系列流程是中科云量安全综合管理平台的主流程，也是该系统的重点所在。

用户在进入**日志管理>原始日志查询**后，可设置时间段或者上报 IP 搜索原始日志，也可以通过**日志管理>原始日志查询>精确查询**来添加**最近时间**进行精确搜索，如下图：

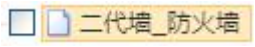


对于搜索出来的日志，用户可以删除、清空或者导出 EXCEL。选中日志后，点击**日志管理>原始日志查询>删除日志**，该日志会从数据库中删去；点击**日志管理>原始日志查询>清空日志**后，数据库中的原始日志表的数据将全部清除；点击**日志管理>原始日志查询>导出 EXCEL** 后，原始日志将以 excel 表的形式导出，如下图：

接收时间	上报ip	上报程序	是否匹配	重复次数	日志内容
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	4	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	5	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	8	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	10	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	7	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	5	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	8	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	7	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	7	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	6	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:
2017-09-11 16:42:47	172.16.2.220	SYSLOG	匹配	9	宋传福 j1500357641 2017/07/18 Tue 14:00:41 ipt_log=ACCEPT IN=vEth1 OUT=vEth3 MAC=00:90:0b:49:36:63:40:8d:5c:

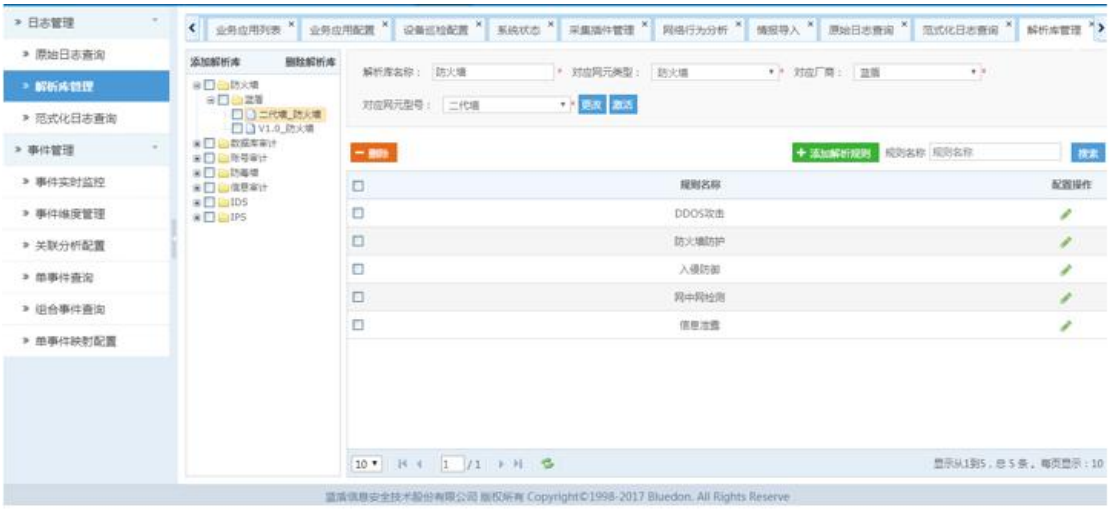
 导出所选择的日志内容，若没有选择日志则默认导出最近的 5 万条数据。

8.1.2 解析库管理

点击**日志管理>解析库管理**后，在点击具体的解析库，例如： 

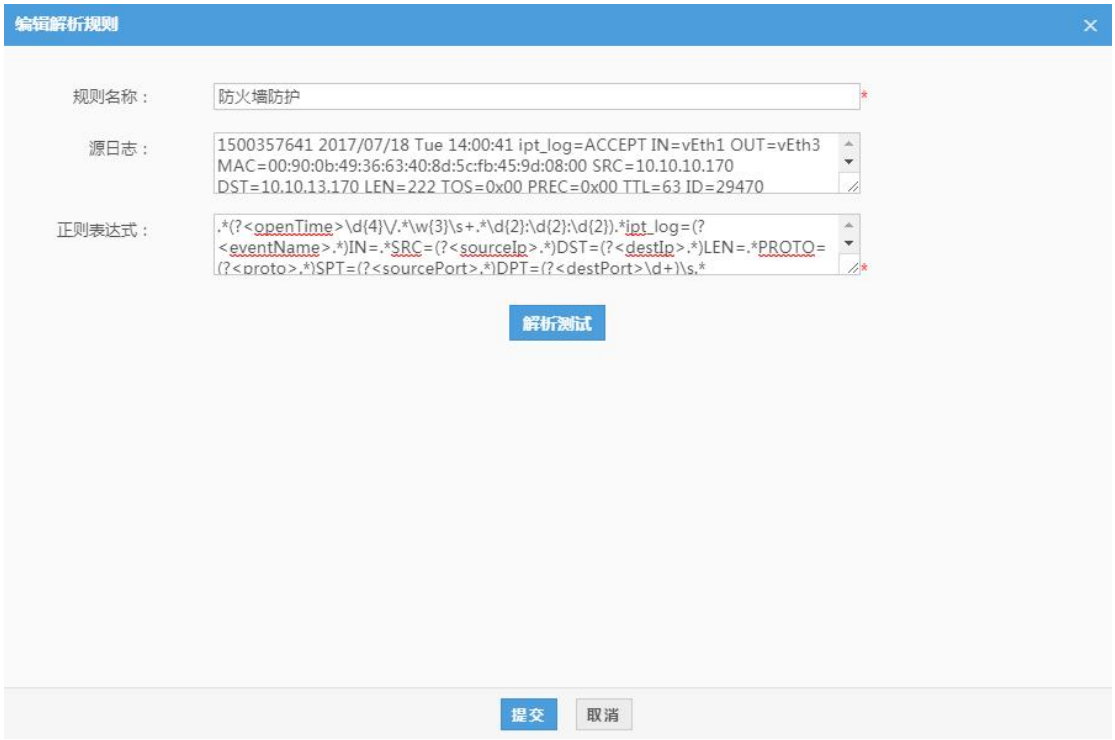
，可以看到**【二代墙_防火墙】**里面的解析规则。用户可以**【更改】**解析库名称、对应网元类型、对应厂商和对应网元型号；同时用户还可以添加、编辑、按规则名称搜索和删除解析规则。对于刚编辑的规则需要过一个小时之后才生效，或者点击 

按钮立马生效。如下图：



因为原始日志要通过解析库规则来产生范式化日志，所以用户可以自定义规则来产生想要的范式化日志。点击  来编辑解析库，在【正则表达式】的“内容”中输入正则表达式，点击 

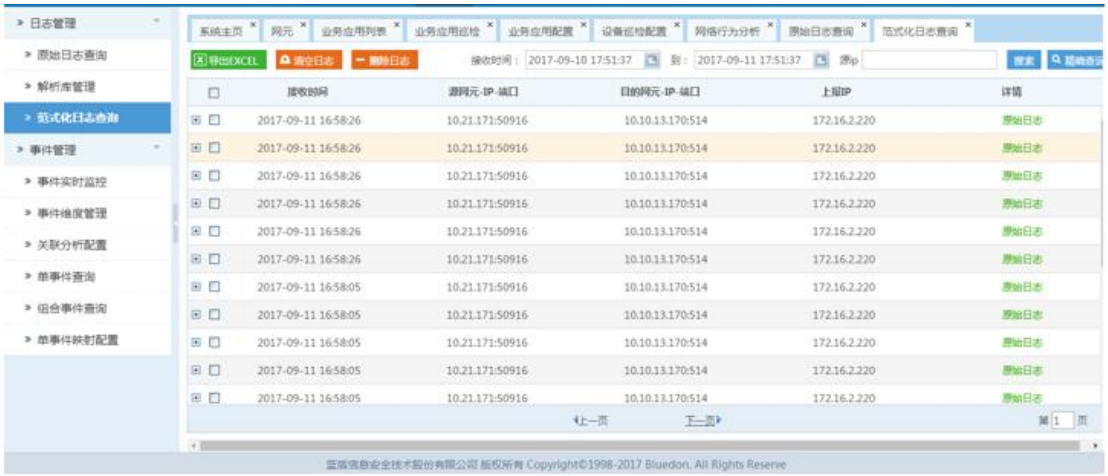
，系统会对内容进行匹配，并显示是否匹配。比如，下图为编辑解析库操作：



匹配日志前系统先识别该日志的上报 IP 网元的网元信息，如网元类型、网元型号、厂商是否与与解析库一致，若一致则进行规则匹配；若不一致，则直接判定为不匹配，这点在查看匹配结果前特别得注意。

8.1.3 范式化日志查询

点击**日志管理>范式化日志查询**，用户可设置时间段或者源 IP 搜索范式化日志，也可以通过**日志管理>范式化日志查询>精确查询**来添加**源 IP、目的 IP、关键字、厂商、网元、最近时间等条件**进行精确查询，如下图：

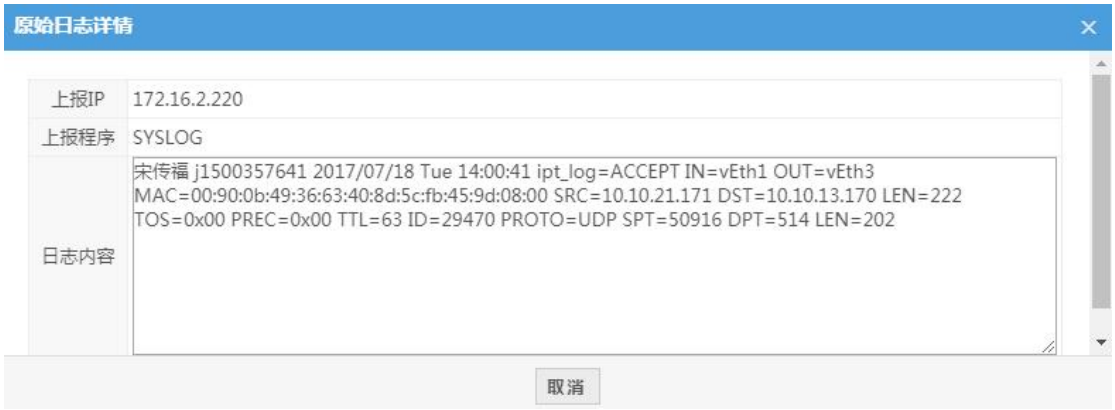


对于搜索出来的日志，用户可以删除、清空或者导出 EXCEL。选中日志后，点击**日志管理>范式化日志查询>删除日志**，该日志会从数据库中删去；点击**日**

志管理>范式化日志查询>清空日志后，数据库中的范式化日志表的数据将全部清除；点击**日志管理>原始日志查询>导出 EXCEL** 后，原始日志将以 excel 表的形式导出（默认导出最近的 5 万条数据），如下图：

	A	B	C	D	E
1	**接收时间**	**源网元-IP-端口**	**目的网元-IP-端口**	**上报IP**	
2	2017-09-11 16:58:26	10.21.171:50916	10.10.13.170:514	172.16.2.220	
3	2017-09-11 16:58:26	10.21.171:50916	10.10.13.170:514	172.16.2.220	
4	2017-09-11 16:58:26	10.21.171:50916	10.10.13.170:514	172.16.2.220	
5	2017-09-11 16:58:26	10.21.171:50916	10.10.13.170:514	172.16.2.220	
6	2017-09-11 16:58:26	10.21.171:50916	10.10.13.170:514	172.16.2.220	
7	2017-09-11 16:58:26	10.21.171:50916	10.10.13.170:514	172.16.2.220	
8	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
9	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
10	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
11	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
12	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
13	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
14	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
15	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
16	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
17	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
18	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
19	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
20	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
21	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	
22	2017-09-11 16:58:05	10.21.171:50916	10.10.13.170:514	172.16.2.220	

点击**原始日志**可以查看生成当条范式化日志对应的原始日志内容，如下图：



8.2 事件管理

8.2.1 事件实时监控

用户在进入**事件管理>事件实时监控**后，用户可看到当前时间段的事件数量，此时间段会随着当前系统时间的变化而变化，以此达到实时监控事件数量的目的。页面的的下方显示监控到的事件的接收时间、事件名称、源网元 IP、源网元端口等具体信息。如下图：

用户可以点击页面左侧的网元类型和事件维度，选中其中具体的一项，则事件实时监控只显示被选中项的事件数量和事件具体信息。如下图：

8.2.2 事件维度管理

用户点击**事件管理>事件维度管理**后，用户可看到事件基本类和事件子类等信息。用户可以根据事件类型来过滤查询，也可以删除或者添加事件类型，如下图：

点击 

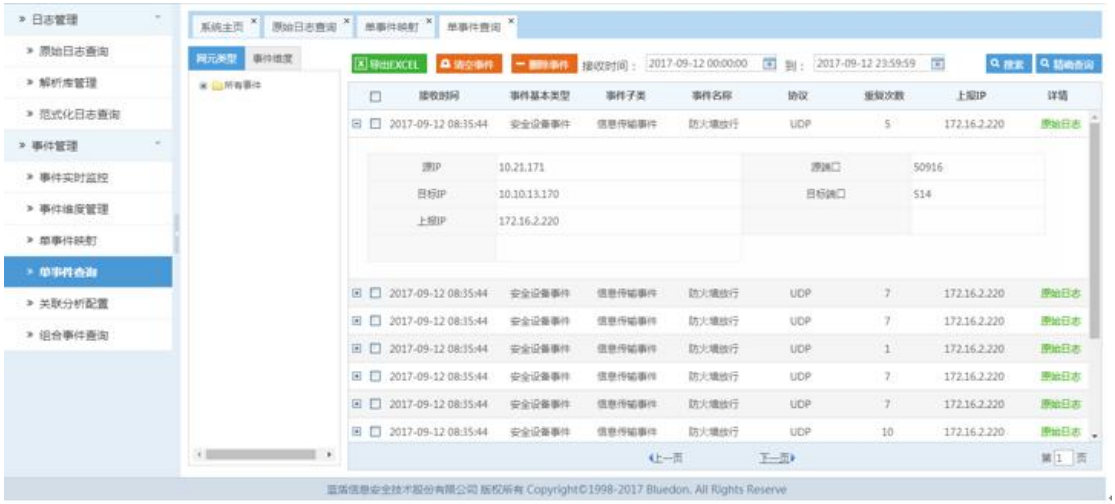
后可以选择添加基本类型事件还是添加子类事件，其中添加基本类型只需要添写类型名称、类型描述，如下图：

添加子类事件首先需要选择所属基本类型，然后再添写类型名称、类型描述，如下图：

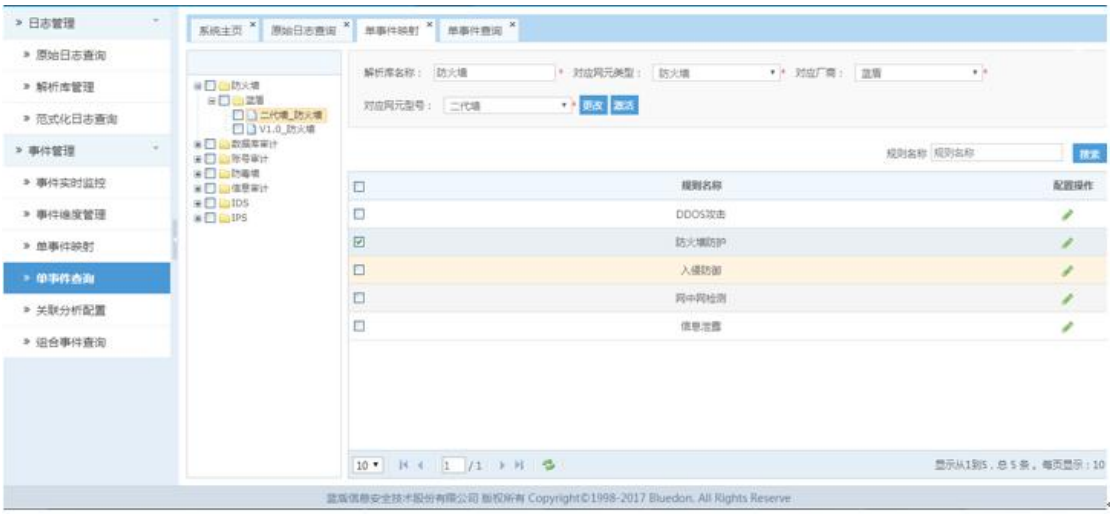
事件管理>事件维度管理的事件信息直接反应在**事件管理>事件实时监控**画面的***事件维度***里。

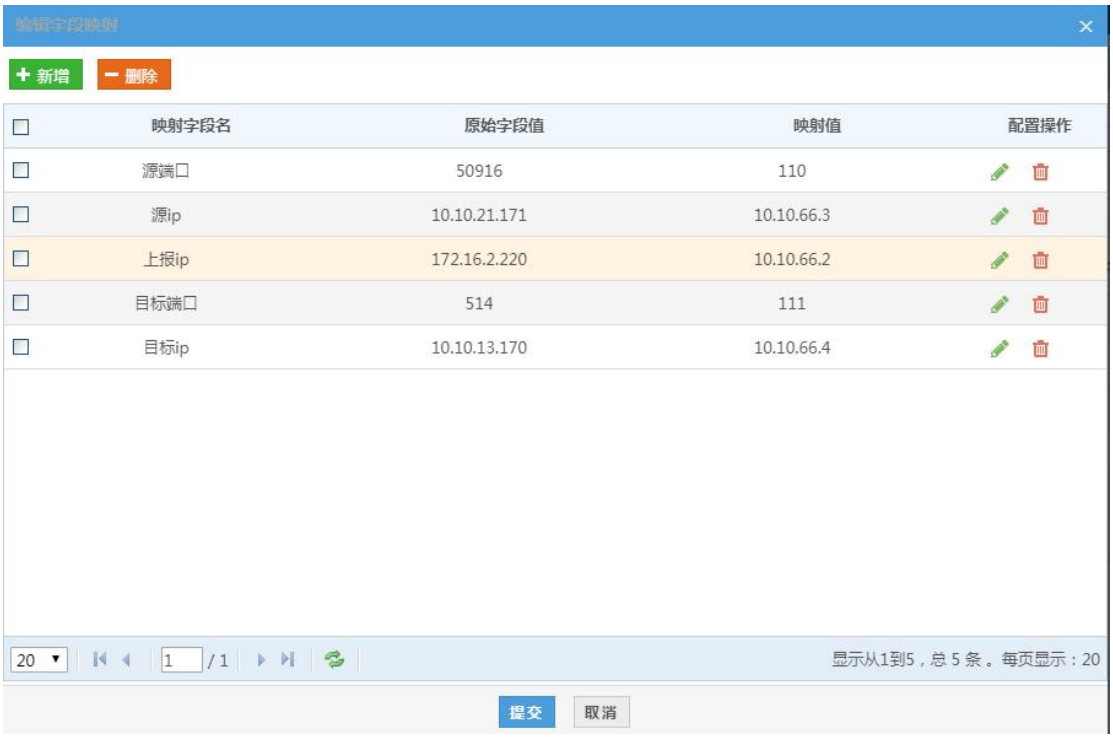
8.2.3 单事件映射

点击**事件管理>单事件映射**，可以将已经生成的事件信息映射成其他信息，如下图为已经生成的事件信息：

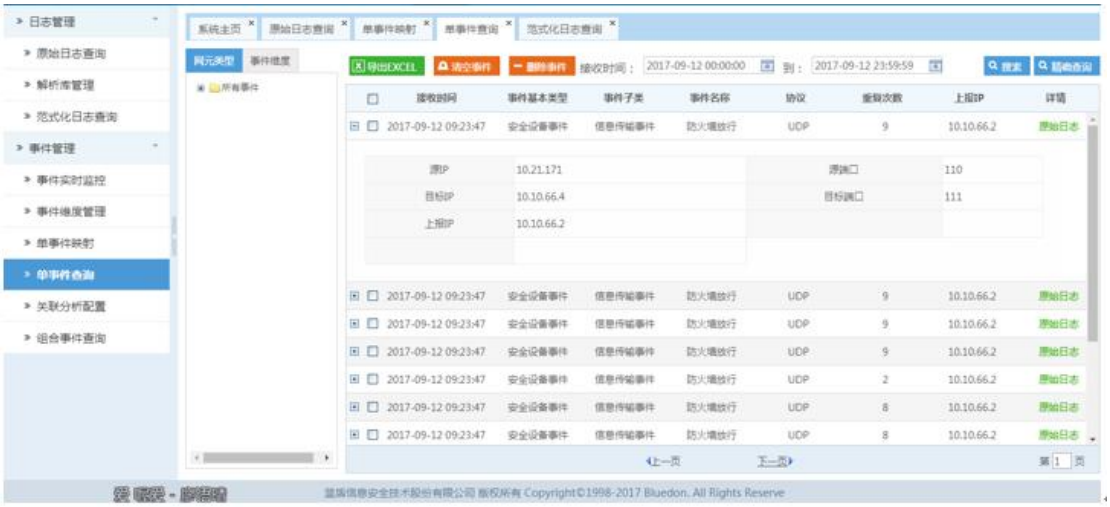


编辑规则提交，如下图：


日志管理
原始日志查询
解析库管理
范式化日志查询
事件管理
事件实时监控
事件维度管理
单事件映射
单事件查询
关联分析配置
组合事件查询
规则名称
配置操作
DDOS攻击
防火墙防护
入侵防御
网中网检测
信息泄露

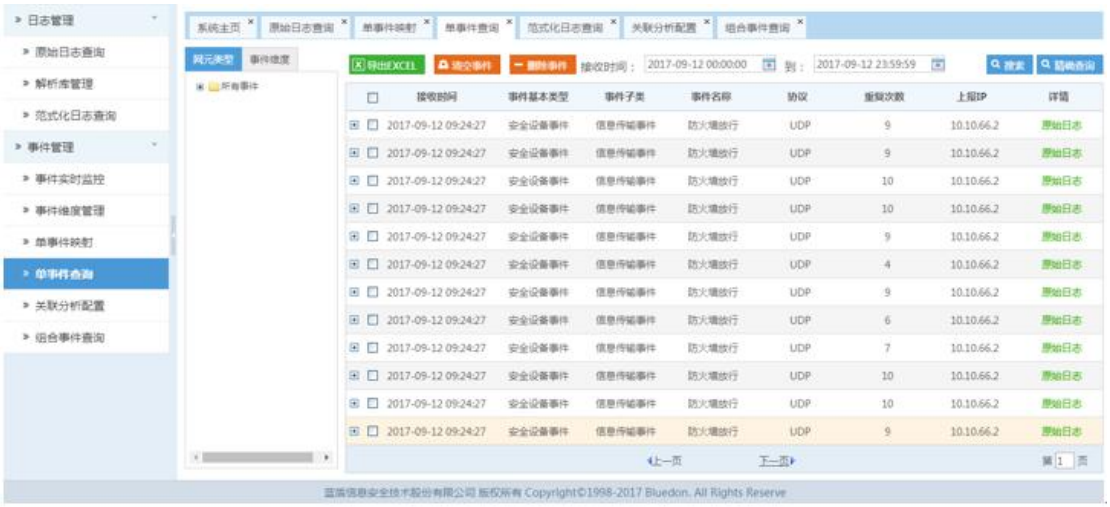

编辑字段映射
新增
删除
映射字段名
原始字段值
映射值
配置操作
源端口
50916
110
源ip
10.10.21.171
10.10.66.3
上报ip
172.16.2.220
10.10.66.2
目标端口
514
111
目标ip
10.10.13.170
10.10.66.4
显示从1到5，总 5 条。每页显示：20
提交
取消

事件信息被映射成如下：



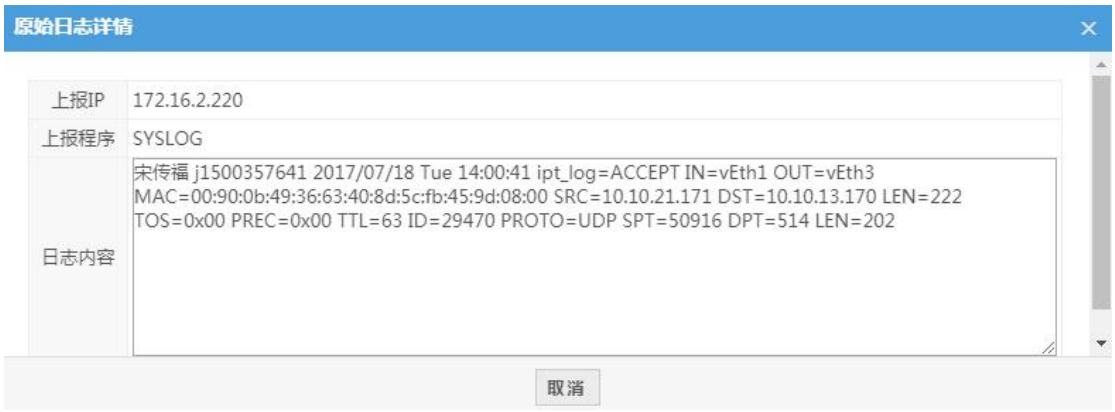
8.2.4 单事件查询

用户在进入**事件管理>单事件查询**后，用户可看到产生的单事件信息。用户可以搜索、删除、清空事件，点击 搜索 按钮通过设置时间段来搜索，选中事件点击 删除事件 按钮则删除数据库中单事件表中对应的数据，点击 清空事件 按钮则清空数据库中单事件表中的所有数据，如下图：



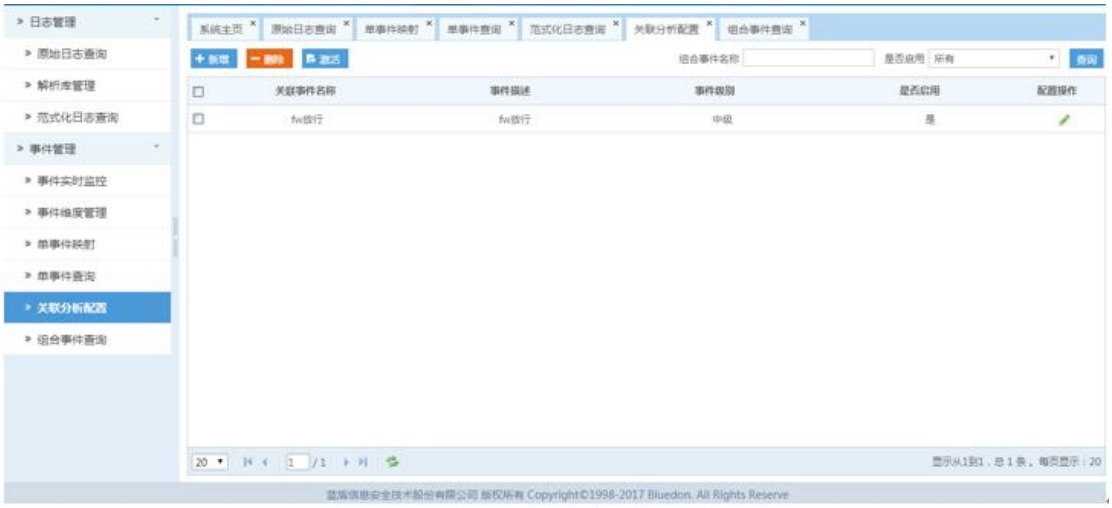
用户可以点击页面左侧的 网元类型 和 事件维度，选中其中具体的一项，则**事件管理>单事件查询**只显示被选中项的单事件信息。如下图：

点击**原始日志**可以查看生成当条事件对应的原始日志内容，如下图：

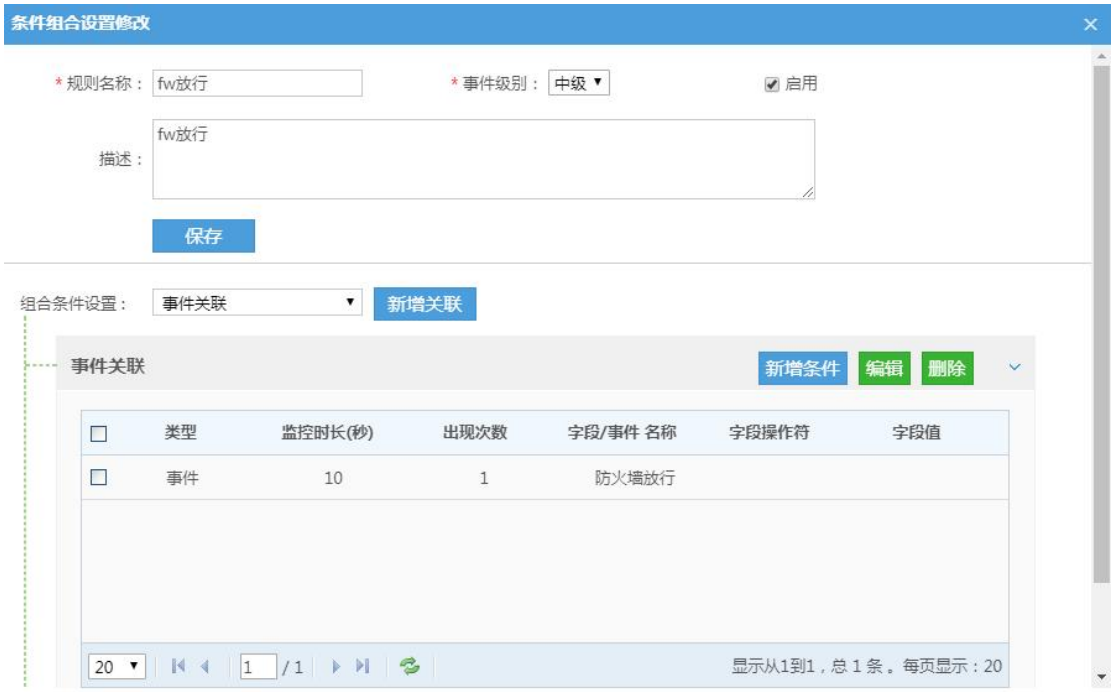


8.2.5 关联分析配置

点击**事件管理>关联分析配置**，用户可看到关联事件规则。用户可以根据组合事件名称来查询、删除、编辑、新增关联规则，如下图：



如下图 为已经添加、现在编辑的关联规则，用户可以更改规则名称、规则描述、事件级别和组合关系：

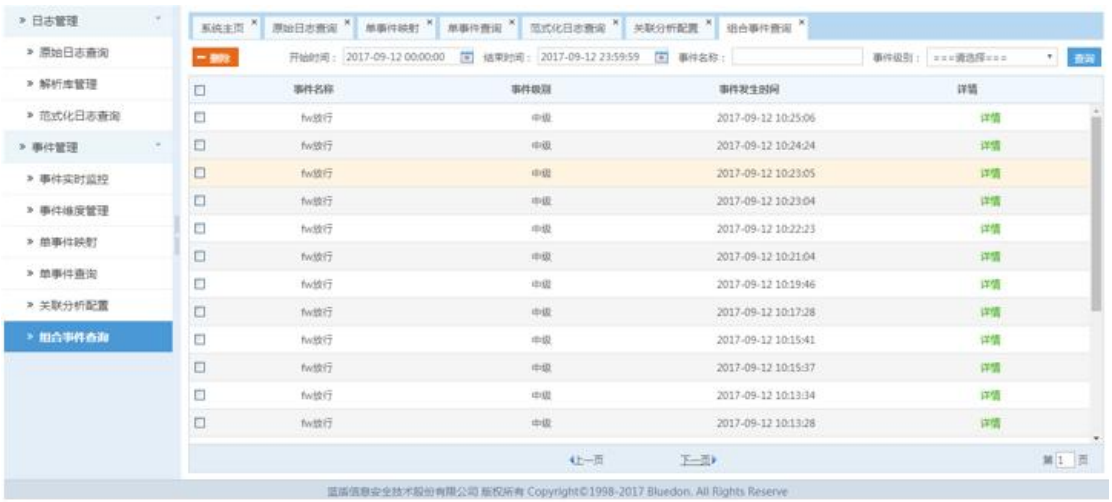


在更改组合关系的过程中，选中关联的事件可以点击 

来编辑关联的具体事件，如下图：

8.2.6 组合事件查询

点击**事件管理>组合事件查询**后，用户可看到产生的组合事件信息。用户可以搜索、删除组合事件，点击 查询 按钮通过设置时间段、事件名称、事件级别来查询，选中事件点击 删除 按钮则删除数据库中组合事件表中对应的数据，如下图：



点击**事件管理>组合事件查询>详情**，可看到该组合事件关联事件详情，用户可看到关联事件发生时间、事件名称、事件级别、源 IP、源端口、目的 IP、目的端口、协议等信息，如下图：


关联事件详情
发生时间
事件名称
事件级别
源IP
目标IP
2017-09-12 10:05:42 防火墙放行 10.10.66.3 10.10.66.4
上一页
下一页
第 1 页
取消

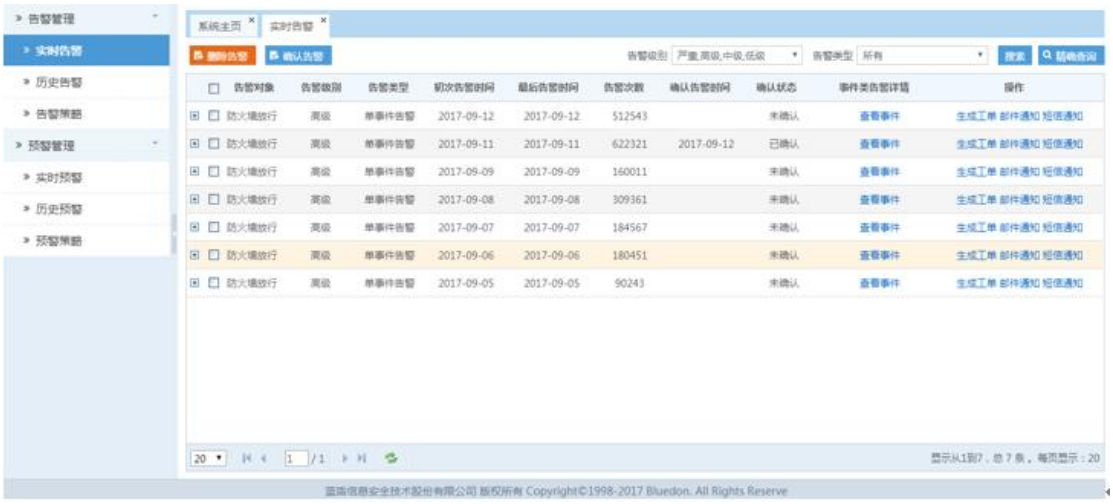
第 9 章　告警管理

9.1 告警管理

9.1.1 实时告警

事件经过告警策略之后会形成实时告警（关于告警策略的配置在 9.1.3 中有详细的说明），相同的实时告警多次发生会在***重复次数***上累加。

点击**告警管理>实时告警**，用户可看到产生的实时告警信息。用户可以搜索、删除、确认发生的告警，点击 搜索 按钮通过告警级别、告警类型来筛选，选中告警点击 删除 按钮则删除数据库中实时告警表中对应的数据，如下图：



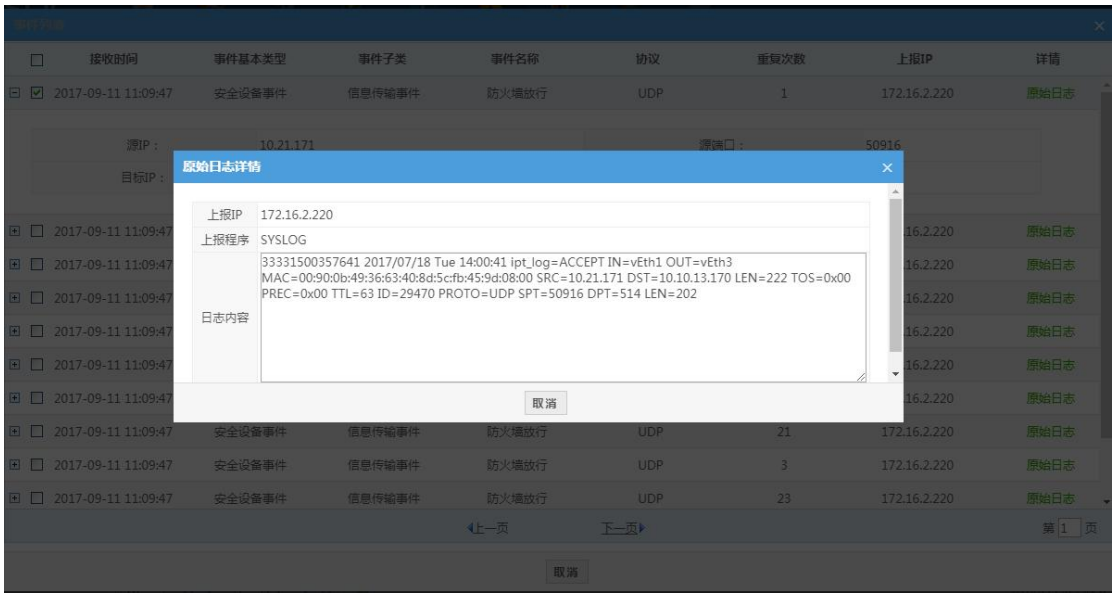
选中告警点击 确认告警 按钮则对产生的告警进行确认，如下图：

告警对象	告警级别	告警类型	初次告警时间	最后告警时间	告警次数	确认告警时间	确认状态	事件类告警详情	操作
防火墙放行	高级	单事件告警	2017-09-12	2017-09-12	644753		未确认	查看事件	生成工单 邮件通知 短信通知
防火墙放行	高级	单事件告警	2017-09-11	2017-09-11	622321	2017-09-12	已确认	查看事件	生成工单 邮件通知 短信通知
防火墙放行	高级	单事件告警	2017-09-08	2017-09-08	309361		未确认	查看事件	生成工单 邮件通知 短信通知
防火墙放行	高级	单事件告警	2017-09-07	2017-09-07	184567		未确认	查看事件	生成工单 邮件通知 短信通知
防火墙放行	高级	单事件告警	2017-09-06	2017-09-06	180451		未确认	查看事件	生成工单 邮件通知 短信通知
防火墙放行	高级	单事件告警	2017-09-05	2017-09-05	90243		未确认	查看事件	生成工单 邮件通知 短信通知

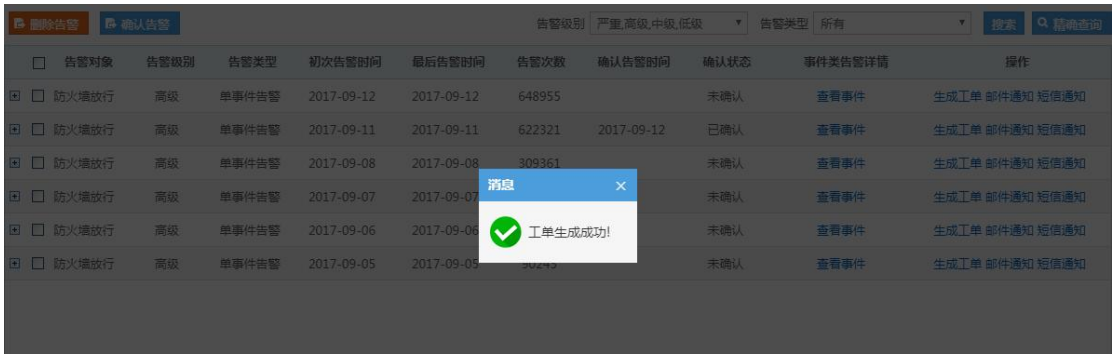
选中告警点击 删除告警 按钮则对产生的告警进行删除。

点击告警的**查看事件**按钮，则可查看当条告警对应的事件详情，如下图：

选中打开的事件中的**原始日志**，则可查看当条事件对应的原始日志内容，如下图：



点击告警的**生成工单**按钮，则可将该告警生成一个工单，如下图：



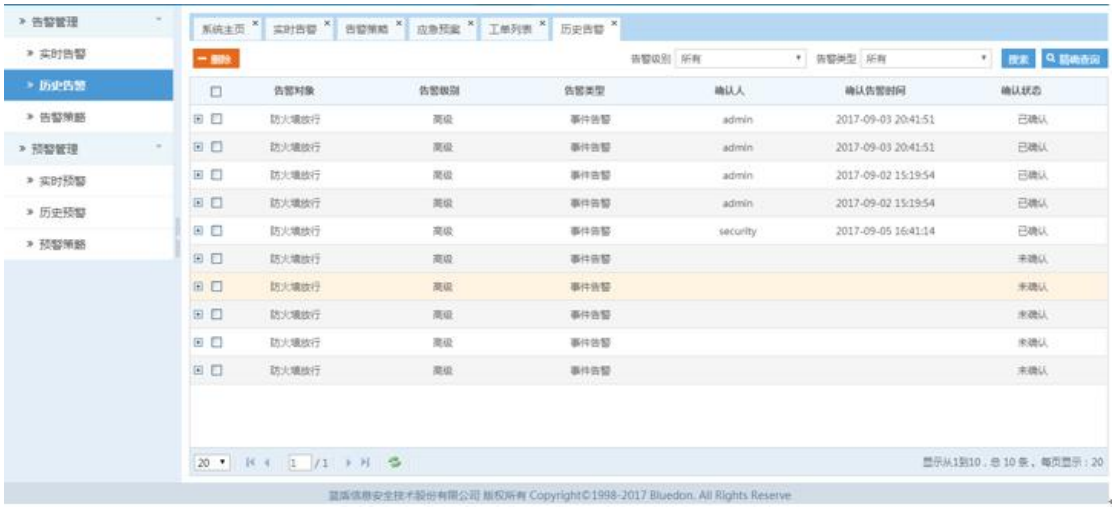
生成工单后在**运维管理>工单管理>工单列表**有该工单的记录，如下图：

9.1.2 历史告警

实时告警界面的告警被删除之后会在历史告警中显示，点击**告警管理>历史告警**，用户可看到被删除的告警信息即历史告警。用户可以搜索、删除、历史告警，点击 

按钮通过告警级别、告警类型来筛选，选中历史告警点击 

按钮则删除数据库中历史告警表中对应的数据，如下图：



9.1.3 告警策略

点击**告警管理>告警策略**，用户可看到产生的告警策略信息。用户可以搜索、删除、新增告警策略，点击 搜索 按钮通过告警策略名来搜索，选中告警策略点击 删除 按钮则删除数据库中告警策略表中对应的数据，如下图：

点击 可以编辑告警策略，用户可更改告警策略名、告警等级、告警类型、处理方式和告警描述等，其中告警类型有单事件告警、联合事件告警、状态告警、漏洞告警等类型选项，如下图：

9.2 预警管理

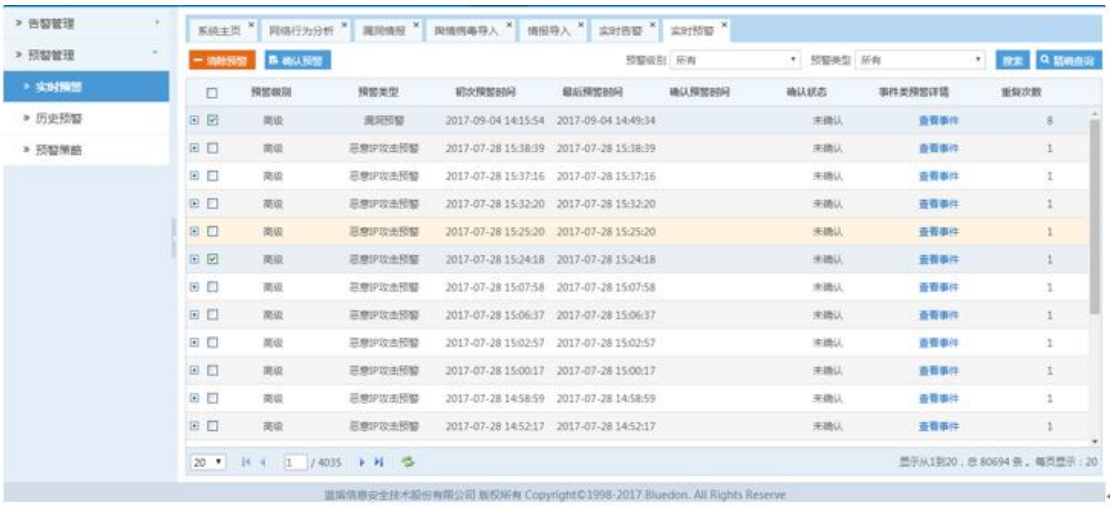
9.2.1 实时预警

根据原始日志的信息和**安全分析>情报管理>情报导入**中的情报，生成实时预警（关于预警策略的配置在 9.2.3 中有详细的说明），相同的实时预警多次发生会在***重复次数***上累加。

点击**预警管理>实时预警**，用户可看到产生的实时预警信息。用户可以搜索、删除、确认发生的告警，点击 

按钮通过预警级别、预警类型来筛选，选中预警点击 

按钮则删除数据库中实时告警表中对应的数据，如下图：



选中预警点击 

按钮则对产生的告警进行确认，如下图：

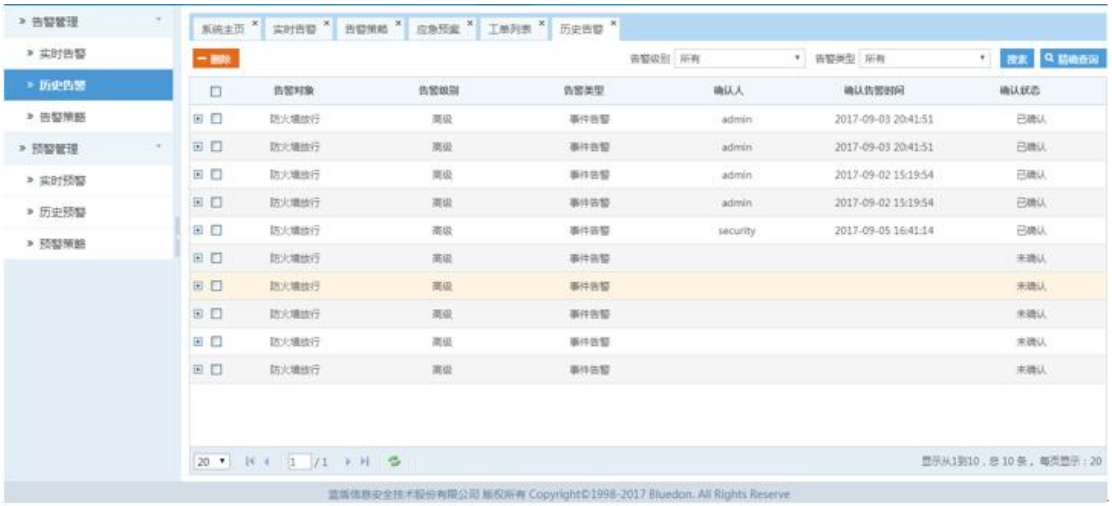
点击预警的**查看事件**按钮，则可查看当条预警对应的事件详情。

9.2.2 历史预警

实时预警界面的预警被删除之后会在历史预警中显示，点击**预警管理>历史预警**，用户可看到被删除的预警信息即历史预警。用户可以搜索、删除、历史告警，点击 

按钮通过预警级别、预警类型来筛选，选中历史告警点击 

按钮则删除数据库中历史预警表中对应的数据，如下图：



9.2.3 预警策略

点击**预警管理>告警策略**，用户可看到配置的预警策略信息。可以勾选策略类型和预警处理方式，如下图：

点击  可以将策略保存，点击  使策略马上生效，若不激活则要等一个小时后生效。

第 10 章 报表

中科云量安全综合管理平台提供了 6 大类 20 多个报表，涵盖日志类报表、事件安全类报表、告警类报表、资产管理类报表、系统审计类报表和工单类报表。点击**报表**，在左边菜单栏选择报表类型，进入报表种类选择界面，点击报表图标，

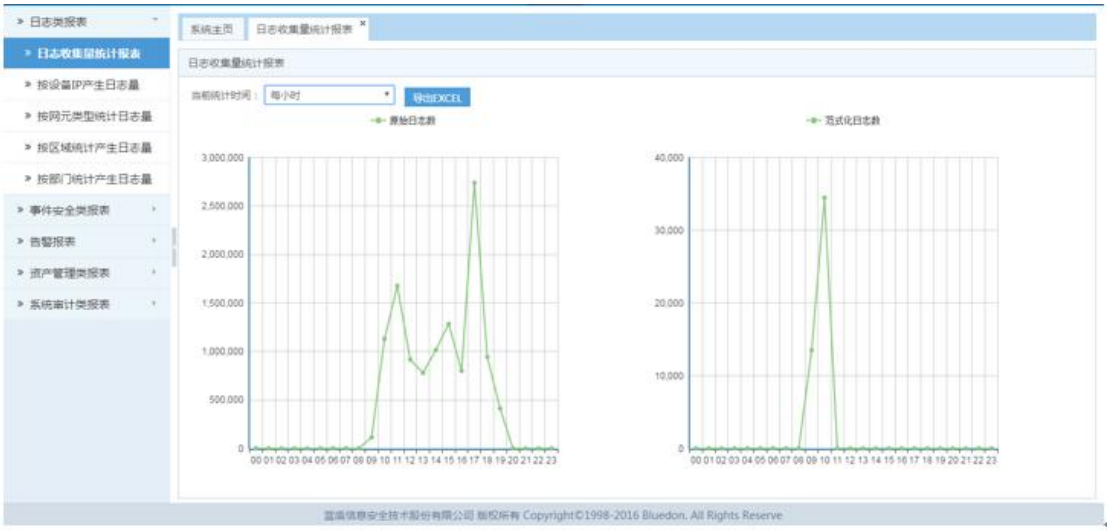
进入报表信息统计界面，用户选择报表信息统计的时间范围，将显示满足用户选择范围的报表信息。

10.1 日志类报表

10.1.1 日志收集量统计报表

原始日志和范式化日志在经过报表服务器处理之后，会在报表上进行数据统计，最终呈现在报表页面上。报表服务器中的数据会每小时更新一次，更新的结果反应在“每小时”统计、“每天”统计、“每周”统计和“每月”统计。“每小时”是在每时的 05 分更新，“每天”是在每时的 25 分更新，“每周”是在每时的 35 分更新，“每月”是在每时的 45 分更新。

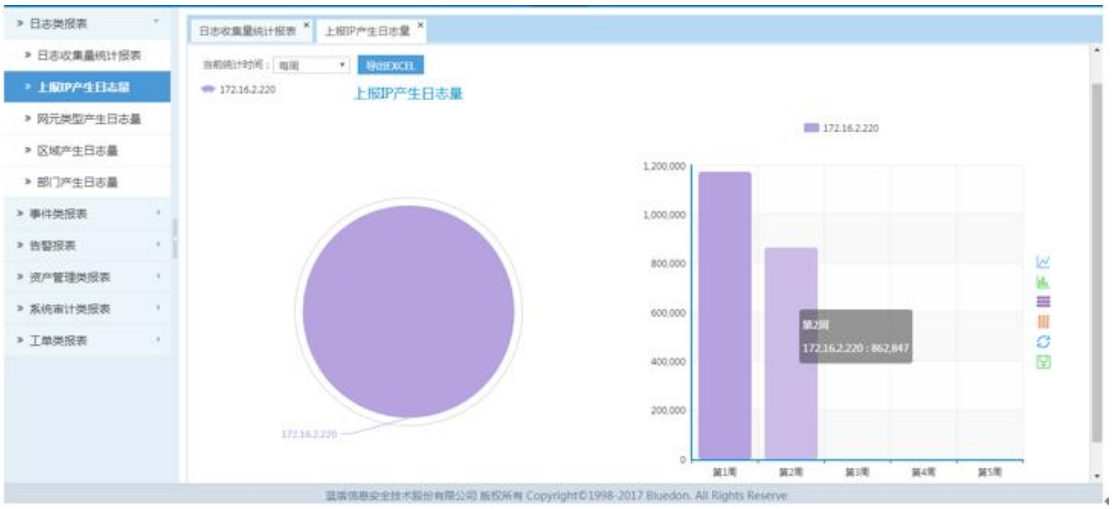
点击**日志类报表>日志收集量统计报表**，如下图为按“每小时”统计的原始日志和范式化日志：



10.1.2 上报 IP 产生日志量

不同的 IP 会产生不同的日志量，此界面将按上报的 IP 来统计日志量。从左到右依次递减，显示前 10 个 IP。

点击**日志类报表>上报 IP 产生日志量**，如下图为按“每周”统计的上报 IP 日志数：

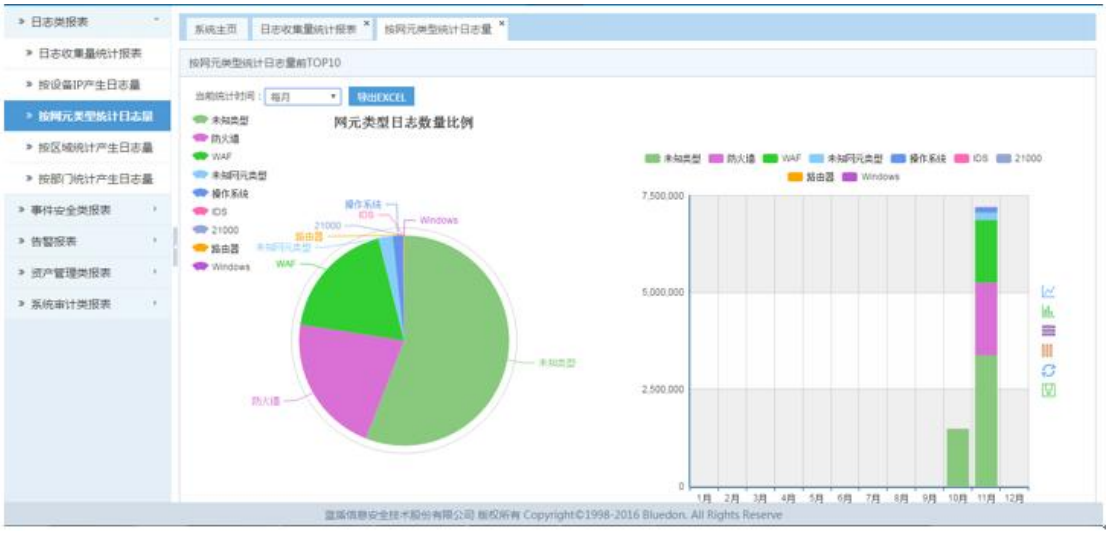


左边为饼图，右边为柱状图。右边的柱状图可以以堆积的方式表示，可以以平铺的方法表示，也可以切换成折线图。

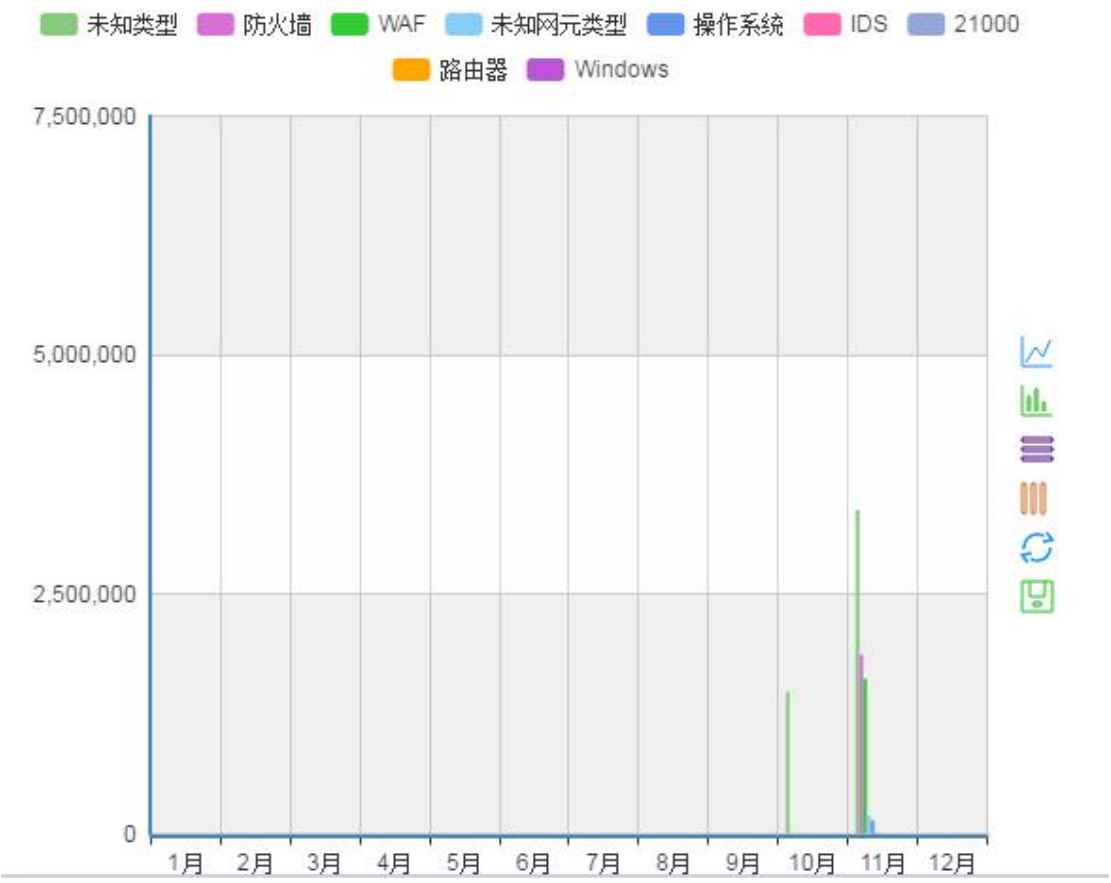
10.1.3 网元类型产生日志量

每个 IP 对应一台设备，设备属于各自的网元类型。不同的网元类型可能会产生不同的日志量，***网元类型产生日志量***界面将按网元的类型来统计日志量。

点击**日志类报表>网元类型产生日志量**，如下图为按“每月”统计的日志量及各个网元类型所占的百分比：



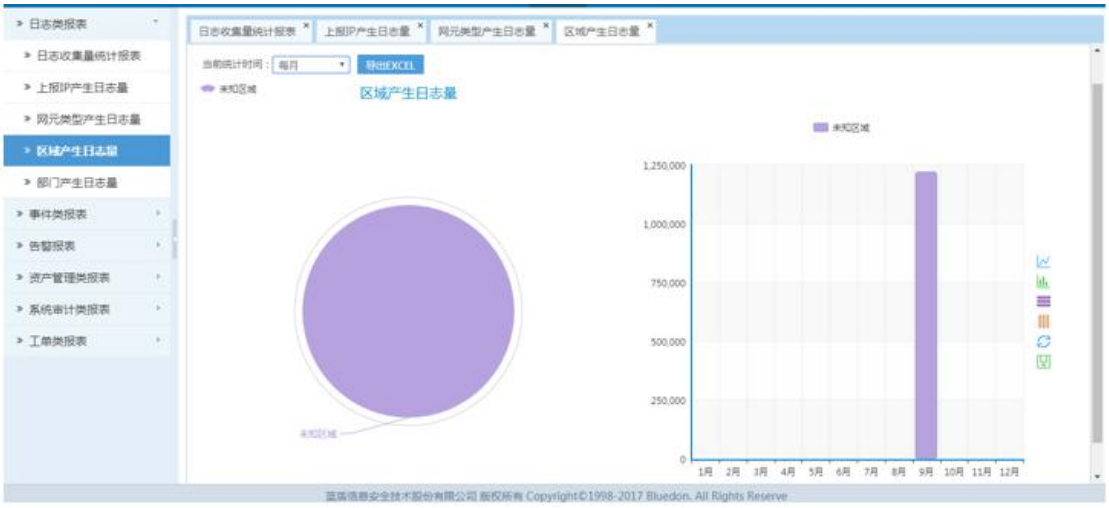
左边为饼图，右边为柱状图。右边的柱状图可以以堆积的方式表示，可以以平铺的方法表示，也可以切换成折线图。如下图：



10.1.4 区域产生日志量

编辑设备信息的时候，可以编辑设备所在的区域，***区域产生日志量***界面将以不同区域的形式来统计日志量。

点击**日志类报表>按区域统计产生日志量**，如下图为按“每月”统计的日志量及各个区域所占的百分比：



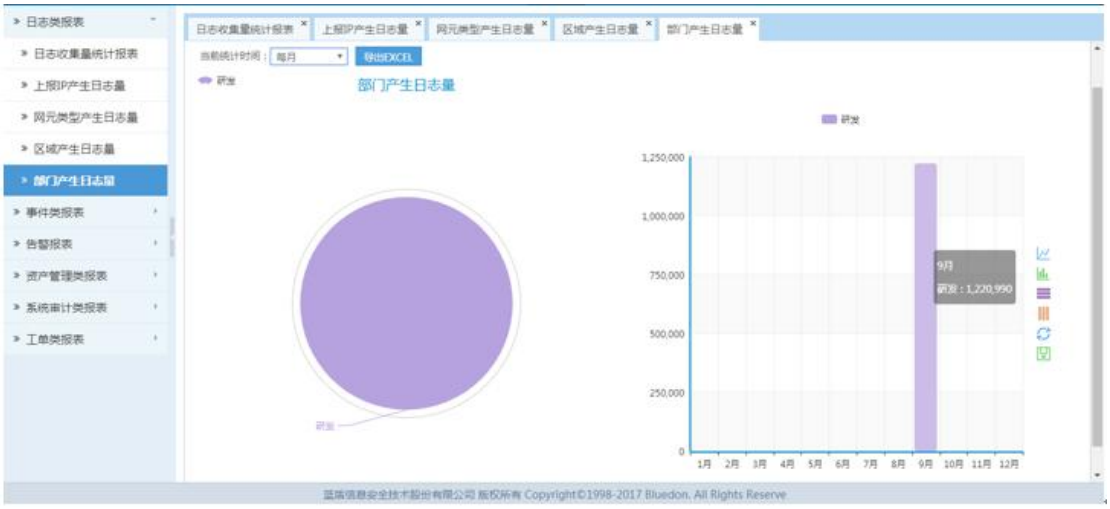
左边为饼图，右边为柱状图。右边的柱状图可以以堆积的方式表示，可以以

平铺的方法表示，也可以切换成折线图。

10.1.5 部门产生日志量

编辑设备信息的时候，可以编辑设备所属的部门，***部门产生日志量***界面将以不同部门的形式来统计日志量。

点击**日志类报表>部门产生日志量**，如下图为按“每月”统计的日志量及各个部门所占的百分比：

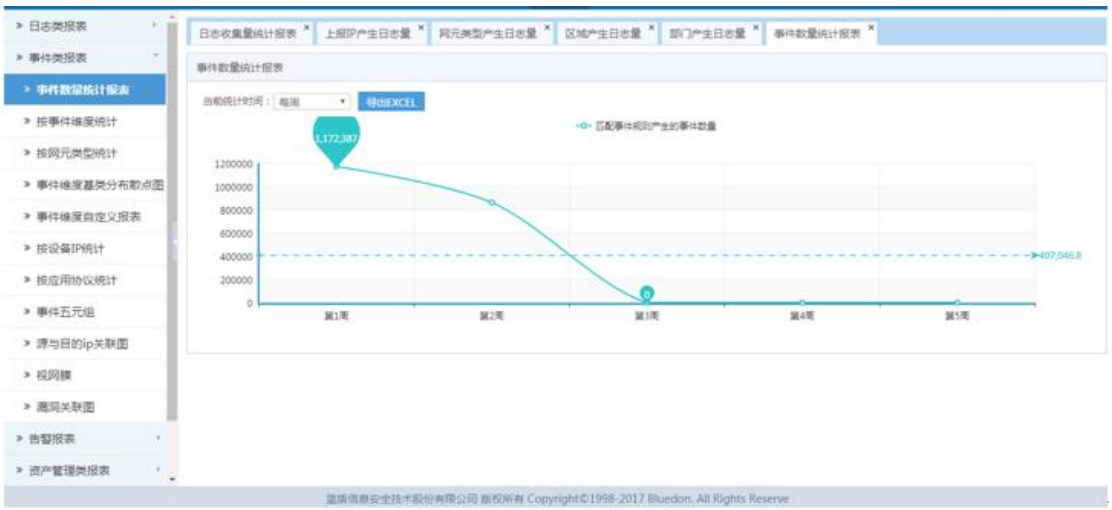


10.2 事件类报表

10.2.1 事件数量统计报表

事件数量统计报表界面将以选择的统计时间来显示产生的事件数量。

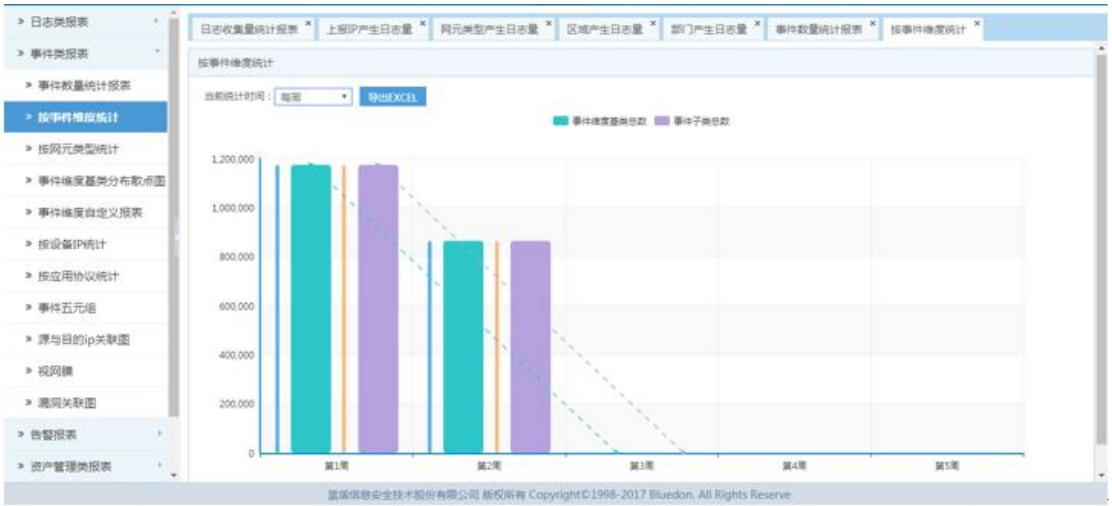
点击**事件类报表>事件数量统计报表**，如下图为按“每周”统计的事件数量（数据每小时更新一次）：



10.2.2 按事件维度统计

*按事件维度统计*界面将以选择的统计时间来显示基本类型的事件数和子类事件数。

点击**事件类报表>按事件维度统计**，如下图为　按“每周”统计的基类事件数量和子类事件数量（数据每小时更新一次）：



10.2.3 按网元类型统计

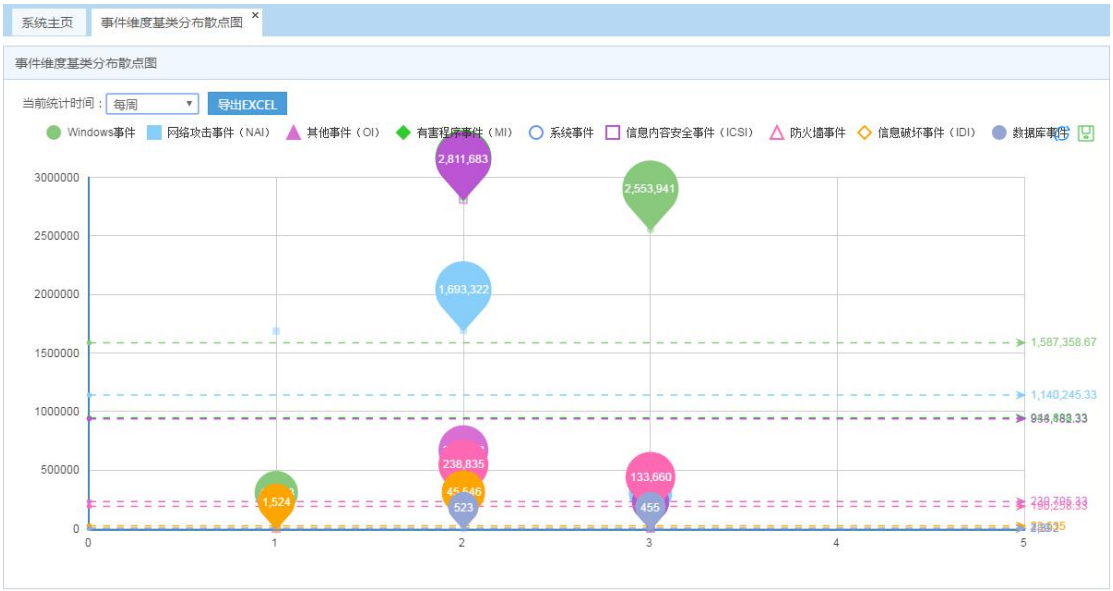
*按网元类型统计*界面将以选择的统计时间来显示不同网元类型产生的事件数。

点击**事件类报表>按网元类型统计**，如下图为　按“每周”统计的不同网元类型产生的事件数量及各自所占的百分比（数据每小时更新一次）：

10.2.4 事件维度基类分布散点图

事件维度基类分布散点图界面将以选择的统计时间来显示不同事件所形成的散点图。

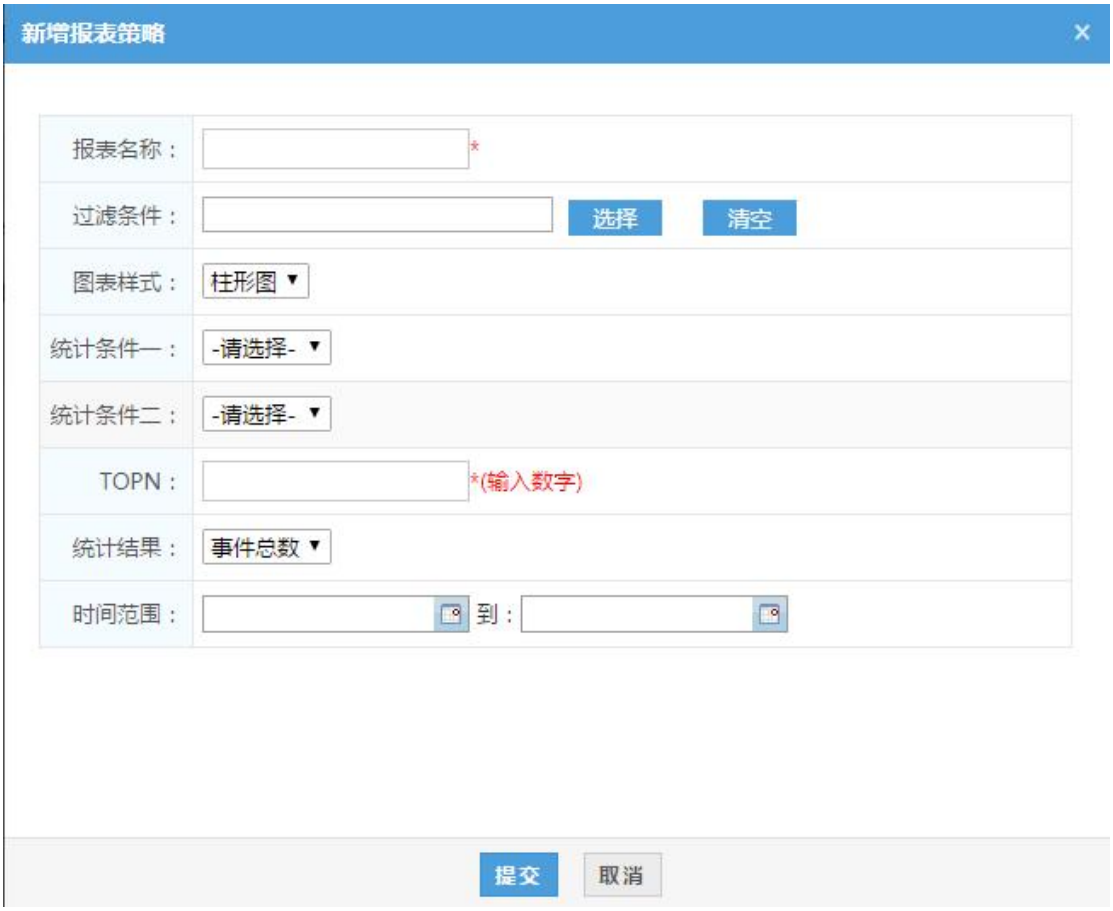
点击**事件类报表>事件维度基类分布散点图**，如下图为 按“每周”统计的不同事件所形成的散点图（数据每小时更新一次）：



10.2.5 事件维度自定义报表

点击**事件类报表>事件维度自定义报表**，进入自定义报表界面，界面显示了自定义报表的报表名称、过滤条件、图标样式等信息，用户可以根据自己的实际需求，新增不同统计条件的报表，同时可以编辑报表，删除报表（里面的基础数据不能删改）。如下图：

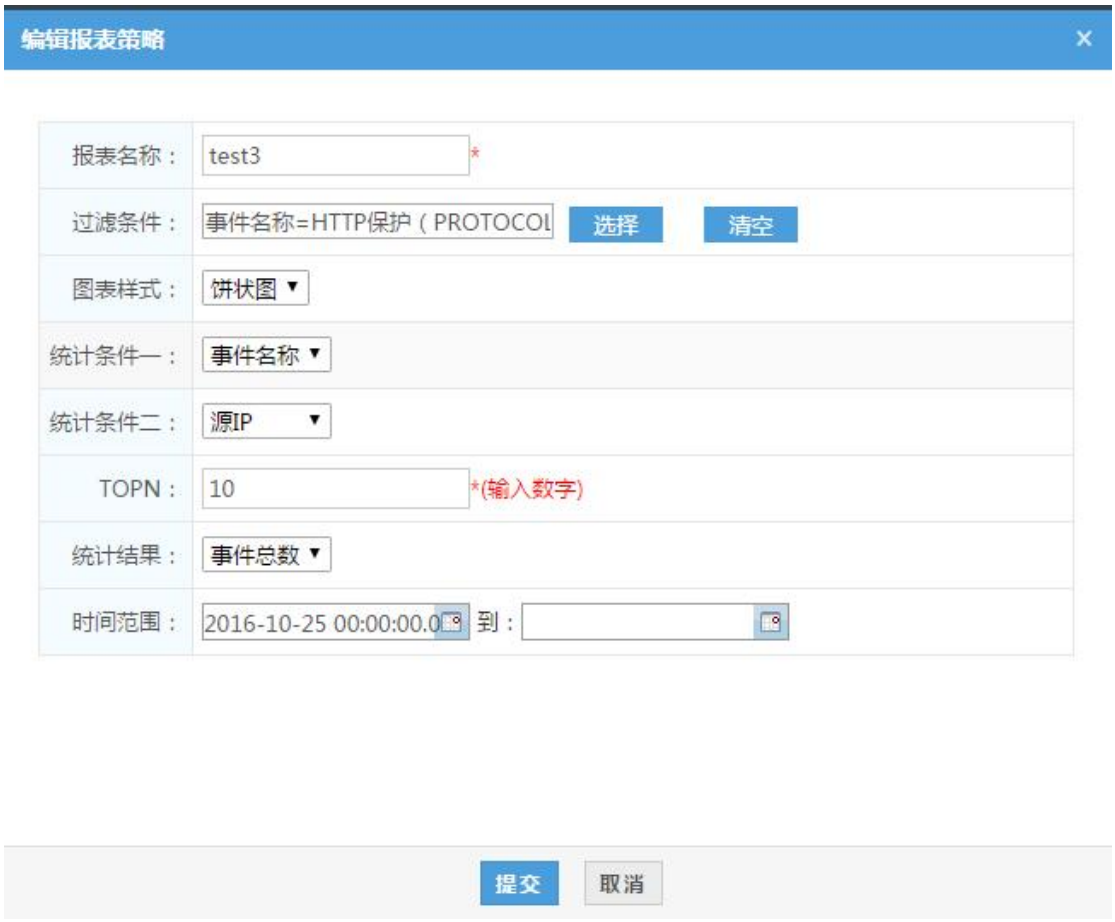
点击**新增**按钮，用户可以在弹出的新增页面中新增新的报表。如下图：



其中“*”为必填项，用户可以选择事件级别，事件名称，源 IP，目的 IP，上报网元 IP 等过滤条件，如下图：

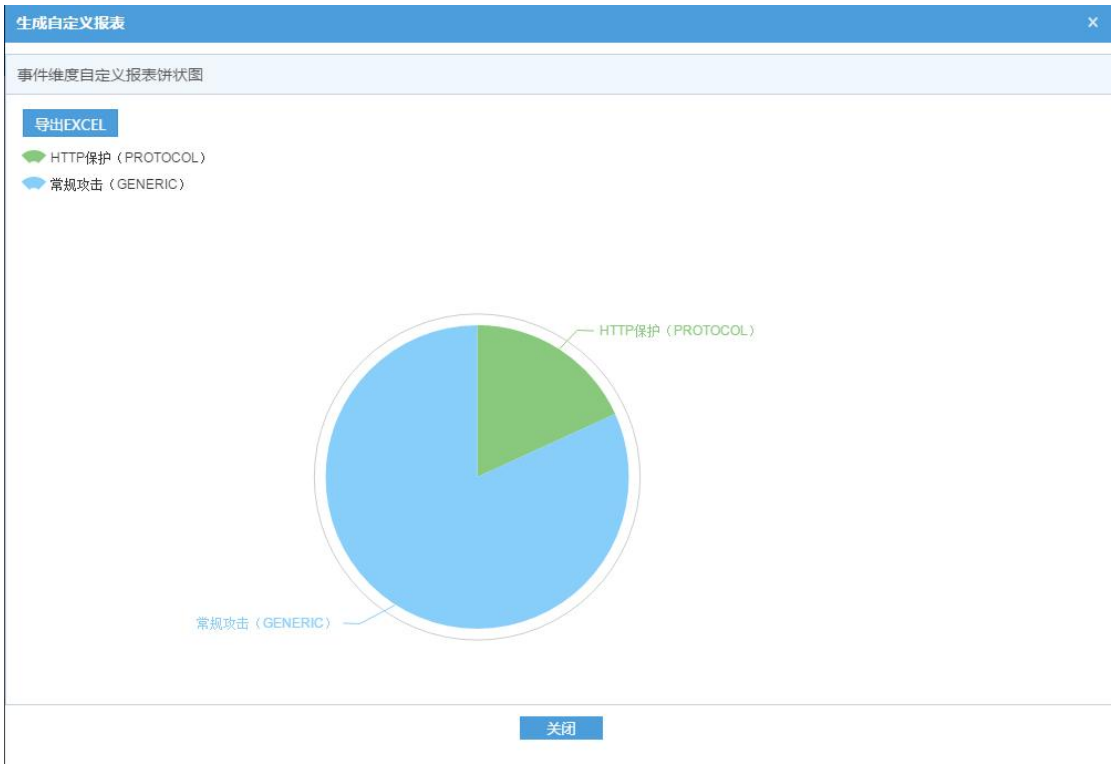
用户可以选择一个或多个过滤条件，当需要的过滤条件超过 2 个时，可以点击 添加条件，增加过滤条件；当选择的条件过多时可以点击 删除条件，逐个减少条件。

选择一个报表，点击 按钮，用户可以在弹出的编辑页面中对选中的报表重新进行编辑。如下图：



点击 删除 或者 按钮，用户可以对选中的报表进行删除操作。

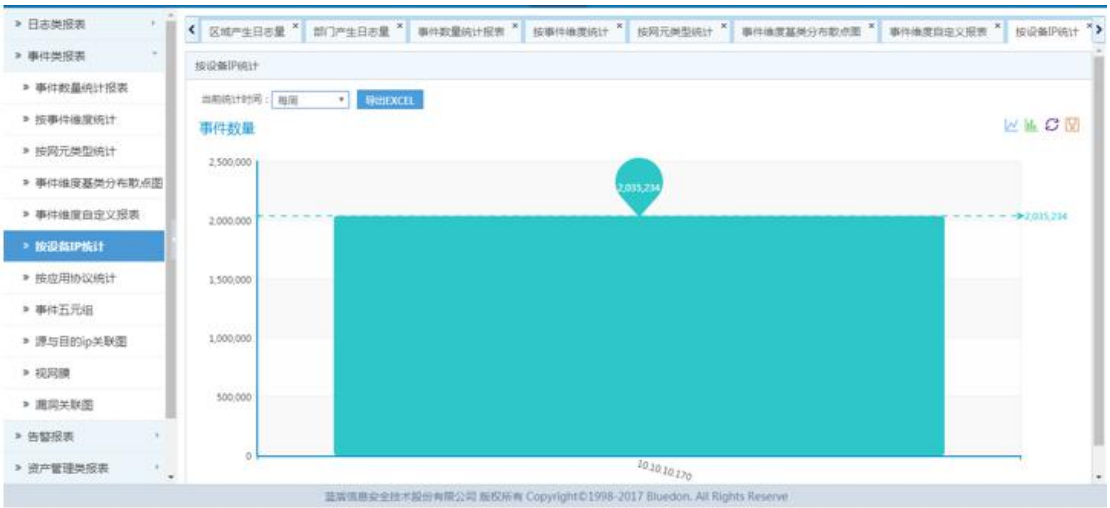
点击 生成报表 按钮，将生成自定义报表。



10.2.6 按设备 IP 统计

不同的 IP 会产生不同的事件，此界面将按 IP 统计事件数量。从左到右依次递减，显示前 10 个 IP。

点击**事件类报表>按设备 IP 统计**，如下图为按“每周”统计的事件数：



10.2.6 按应用协议统计

不同的协议会产生不同的事件，此界面将按应用协议来统计事件数量。

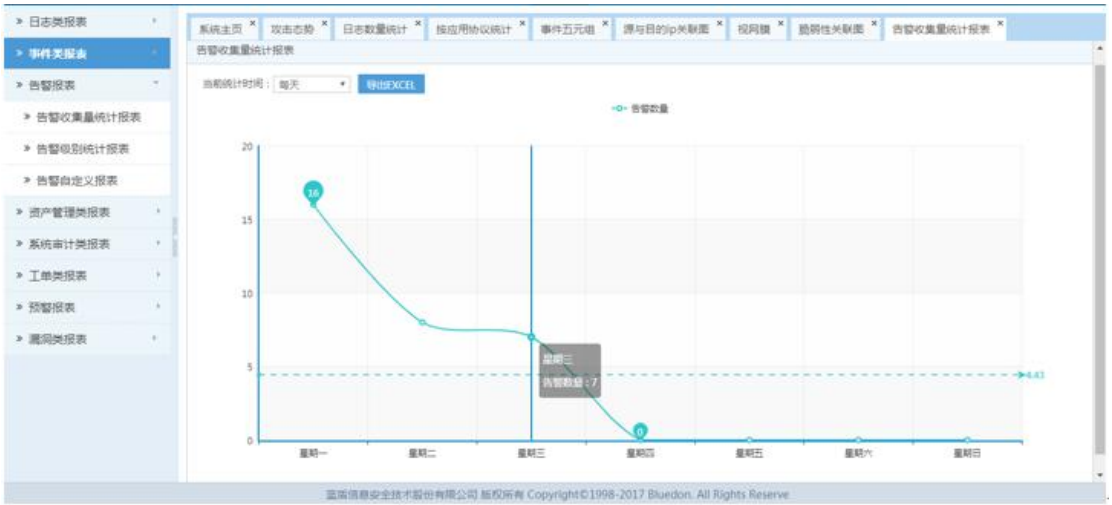
点击**事件类报表>按设备应用协议统计**，如下图为按“每周”统计的事件数：

10.3 告警报表

10.3.1 告警收集量统计报表

事件经过告警策略后会形成实时告警，实时告警最终呈现在***报表***页面上。报表服务器中的数据会每小时更新一次，更新的结果反应在“每小时”统计、“每天”统计、“每周”统计和“每月”统计。

点击**告警报表>告警收集量统计报表**，如下图为按“每小时”统计的告警情况：



10.3.2 告警级别统计报表

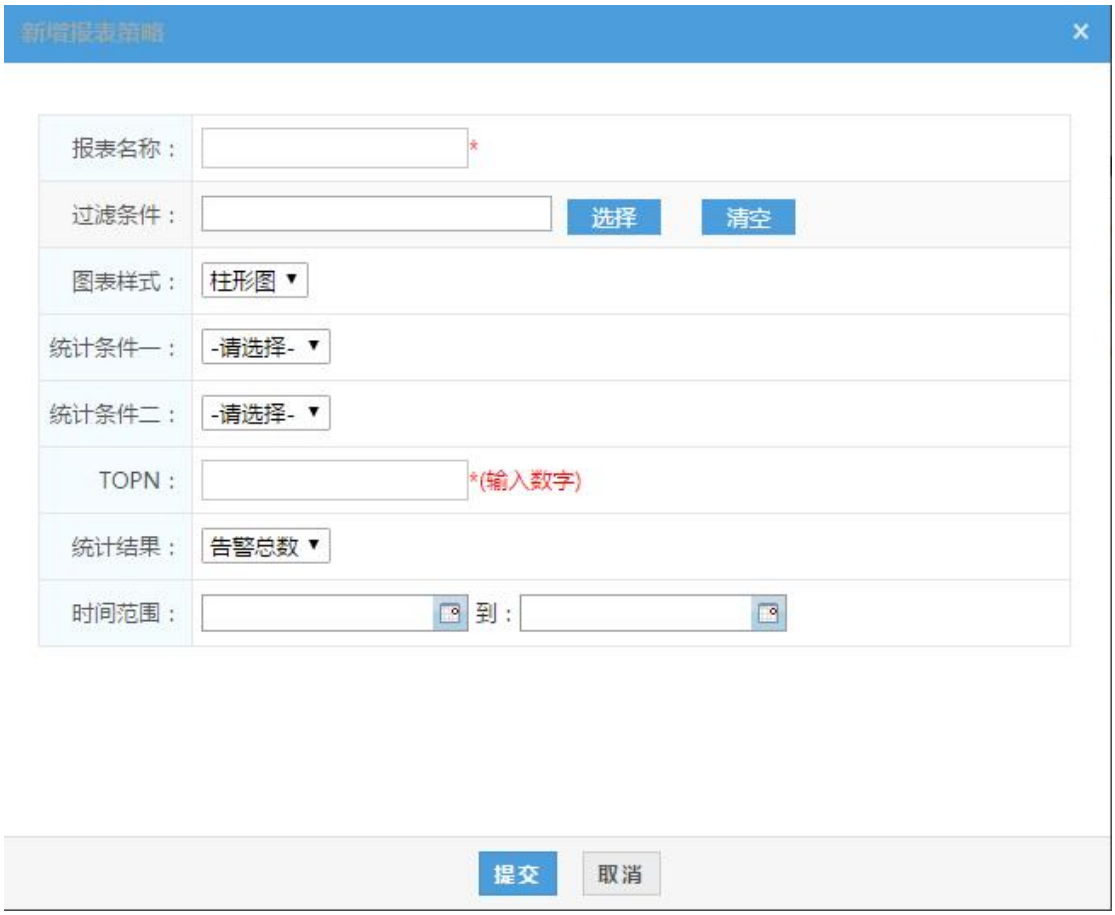
事件经过告警策略后会形成实时告警，每个实时告警都有对应的告警级别，此界面则是通过告警级别来统计。

点击**告警报表>告警级别统计报表**，如下图为按“每月”统计的告警情况：

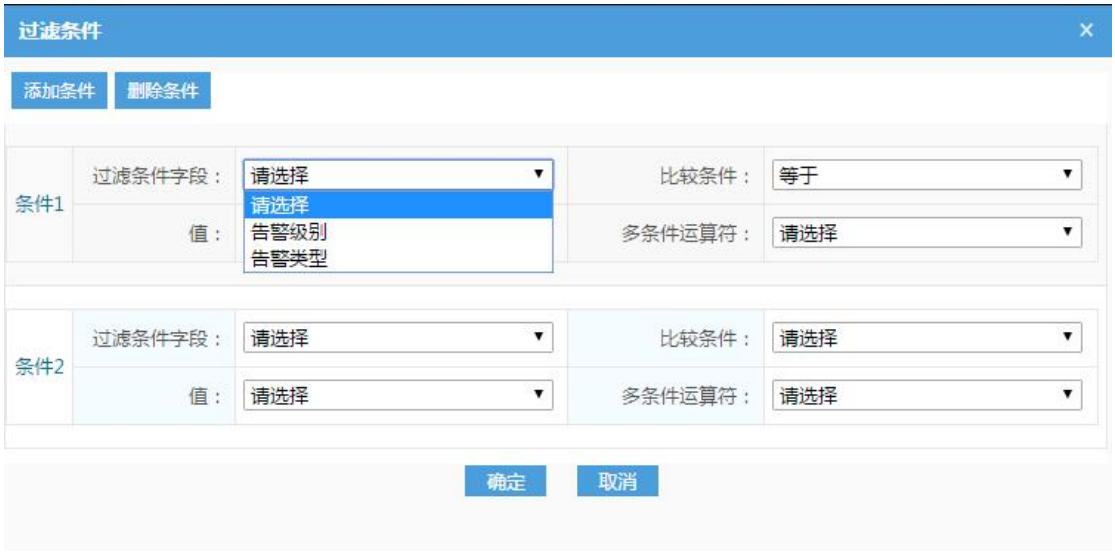
10.3.3 告警自定义报表

点击**告警报表>告警自定义报表**，进入自定义告警界面，其中内置了一些报表，用户可直接使用查看，用户也可以根据自己的实际需求，新增报表，编辑报表，删除报表（里面的基础数据不能删改）。如下图：

点击**新增**按钮，用户可以在弹出的新增页面中新增新的报表策略。如下图：

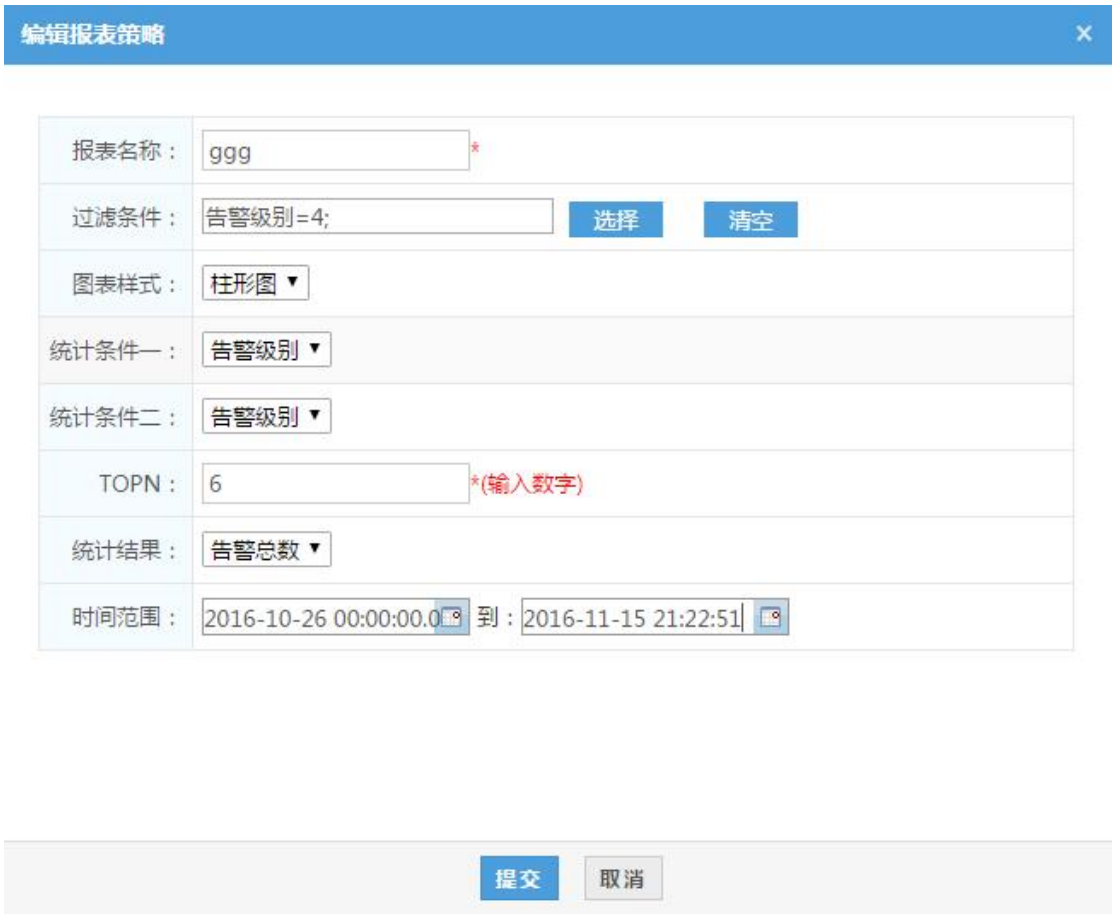


其中“*”为必填项，用户可以选择告警级别，告警类型等不同的过滤条件来对告警进行过滤，如下图：



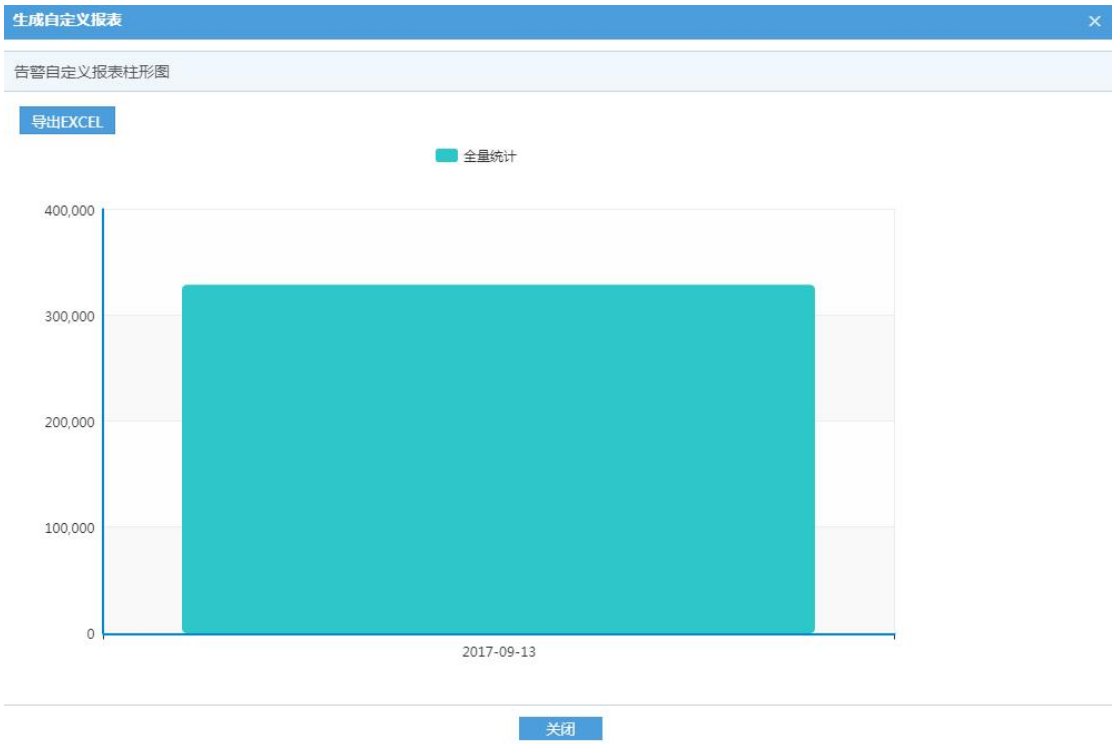
用户可以选择一个或多个过滤条件，当需要的过滤条件超过 2 个时，可以点击 添加条件，增加过滤条件；当选择的条件过多时可以点击 删除条件，逐个减少条件。

选择一个报表，点击 按钮，用户可以在弹出的编辑页面中对选中的报表重新进行编辑。如下图：



点击 删除 或者 按钮，用户可以对选中的报表进行删除操作。

点击 生成报表 按钮，将生成自定义报表。

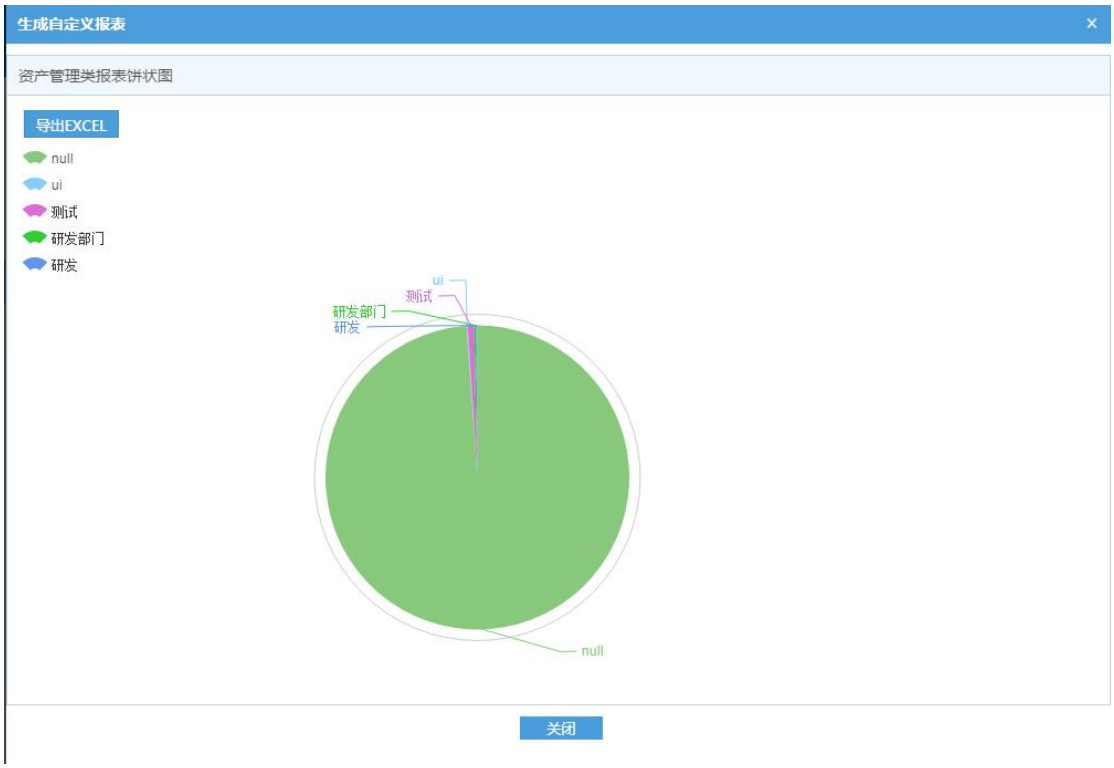


10.4 资产管理类报表

10.4.1 资产管理类报表

点击**资产管理类报表>资产管理类报表**，进入资产管理类报表中心。可以查看“资产按部门分布”，“资产风险等级分布”，“资产按类型分布”等报表。该报表类型系统已经内置，用户不可添加或修改。

点击 生成报表，可以查看被选中的报表，如资产按部门分布报表，如下图：



点击 导出EXCEL，如下图：

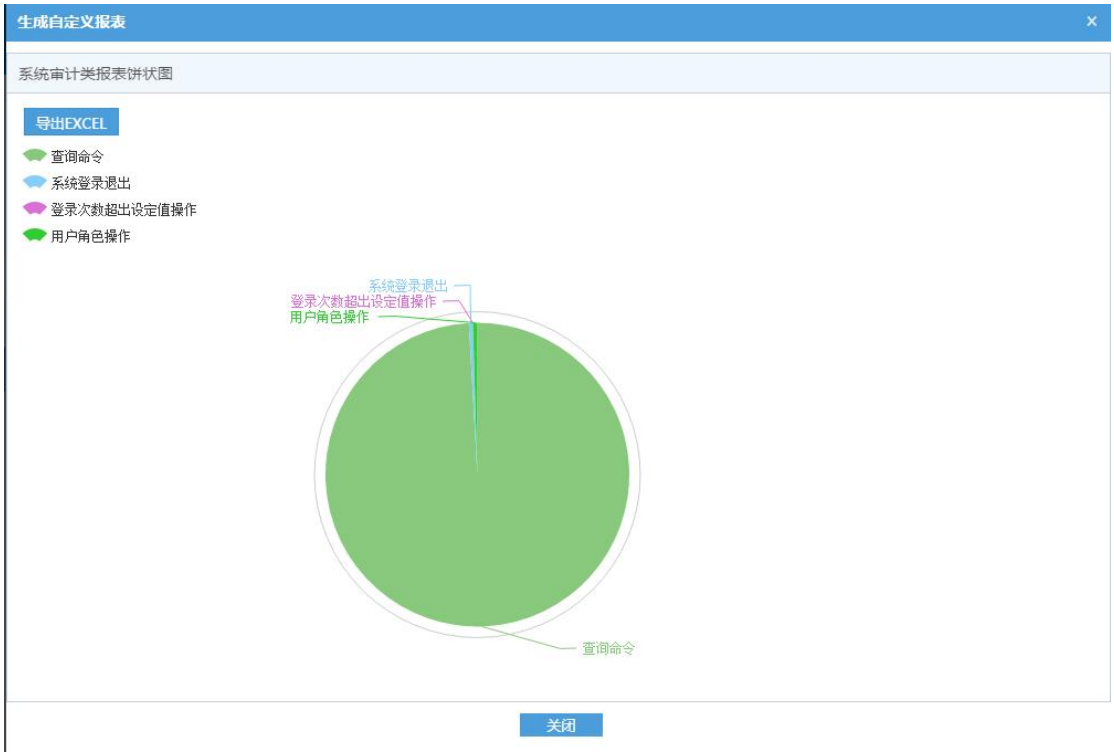
	A	B	C
1	名称	数量	
2	null	883	
3	ui	1	
4	测试	6	
5	研发部门	2	
6	研发	1	
7	总计	893	
8			

10.5 系统审计类报表

10.5.1 系统审计类报表

点击**系统审计类报表>系统审计类报表**，进入系统审计类报表中心，包括“系统日志类型分布”和“用户登录分布”两类报表。

点击 生成报表，可以查看被选中的报表，如系统日志类型分布报表，如下图：



点击 导出EXCEL，如下图：

	A	B	C
1	名称	数量	
2	查询命令	607001	
3	系统登录退出	2514	
4	登录次数超出设定值操作	36	
5	用户角色操作	2903	
6	总计	612454	
7			

10.6 工单类报表

10.6.1 工单报表

点击**工单类报表>工单报表**，可以查看工单的报表信息，如下图：

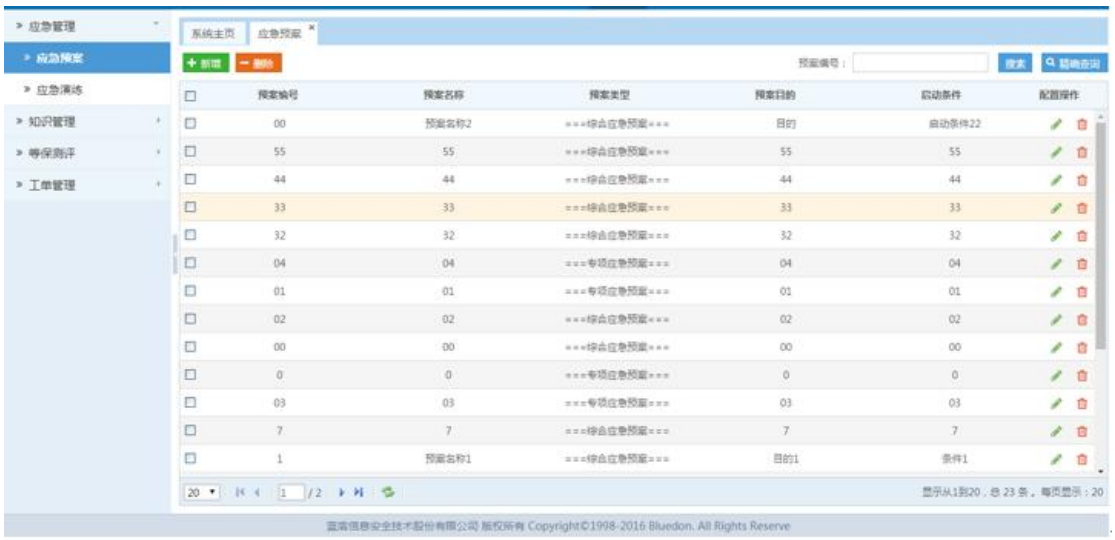

日志类报表
事件类报表
告警报表
告警收集量统计报表
告警级别统计报表
告警自定义报表
资产管理类报表
系统审计类报表
系统审计类报表
工单类报表
工单报表
预警报表
漏洞类报表
工单分布图
工单优先级
工单状态
紧急
新建

第 11 章 运维管理

11.1 应急管理

11.1.1 应急预案

点击**应急管理>应急预案**，用户可看到预案信息。用户可以搜索、删除、新增、配置预案，点击 搜索 按钮通过预案编号来搜索，选中预案后点击 删除 按钮或 按钮则删除数据库中预案表中对应的数据，如下图：



点击 新增 按钮，可以新增新的预案,如下图：

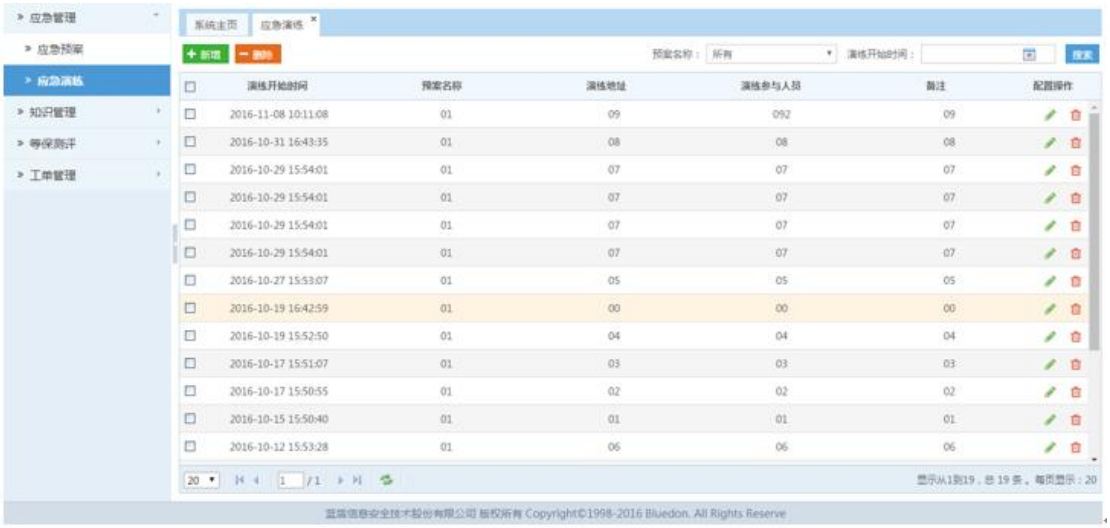
也可以点击 按钮编辑预案，如下图：

11.1.2 应急演练

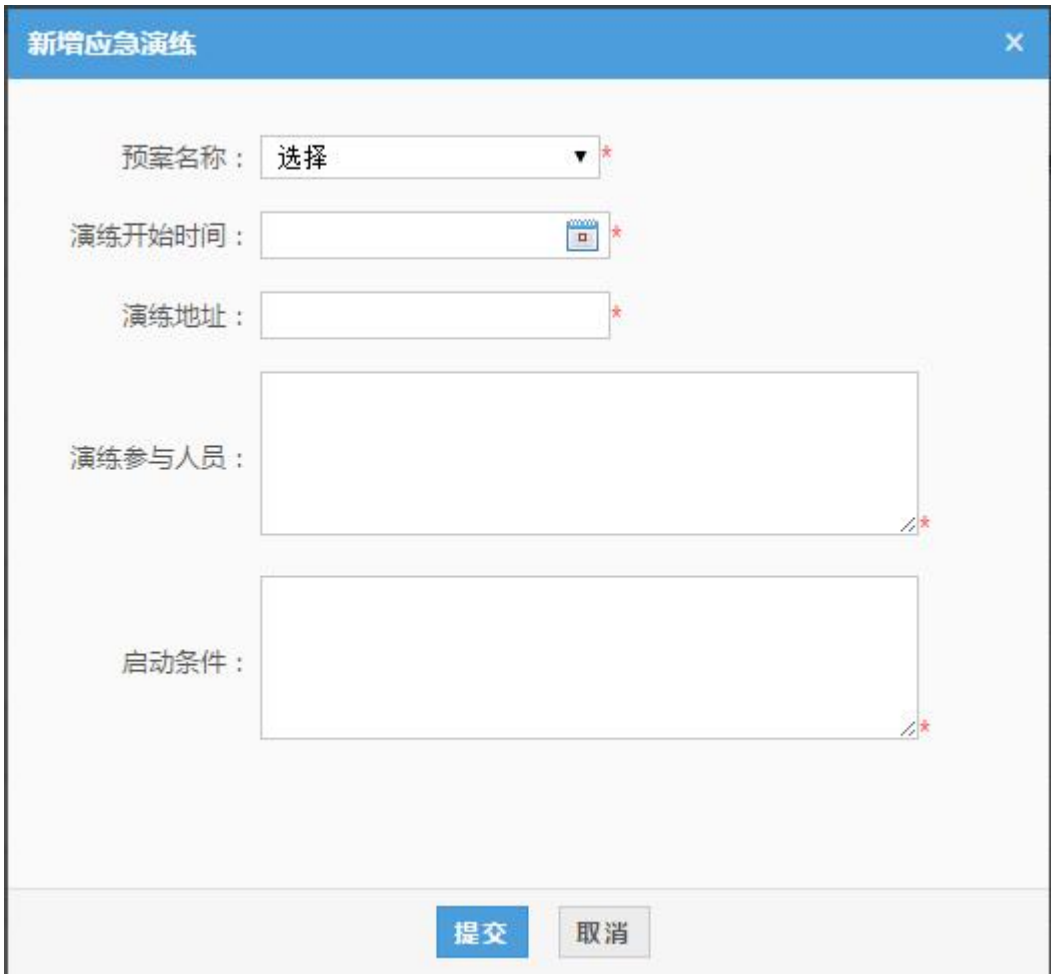
点击**应急管理>应急演练**，用户可看到演练的信息。用户可以搜索、删除、新增、配置演练，点击 

按钮通过预案名称、演练开始时间来搜索，选中演练后点击 

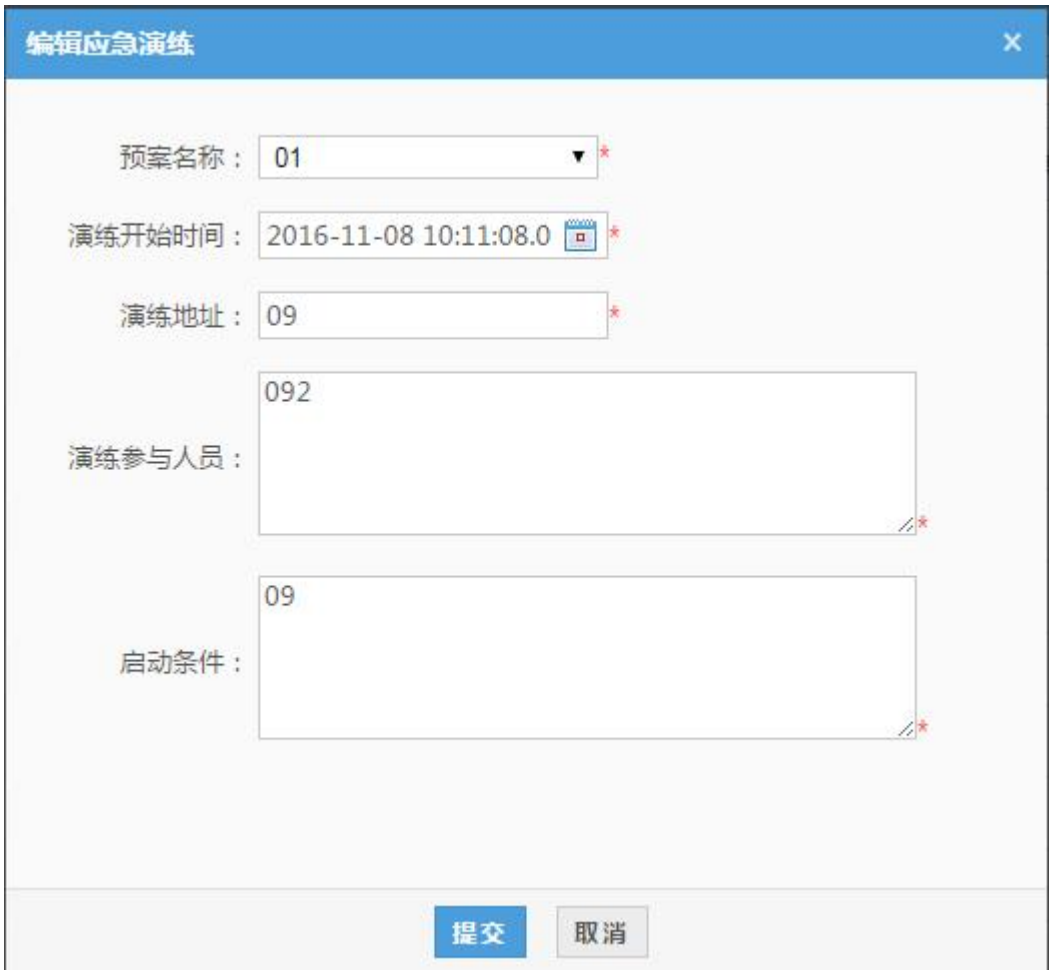
按钮或  按钮则删除数据库中演练表中对应的数据，如下图：



点击  按钮，可以新增新的应急演练，其中***演练开始时间***要大于当前时间，如下图：



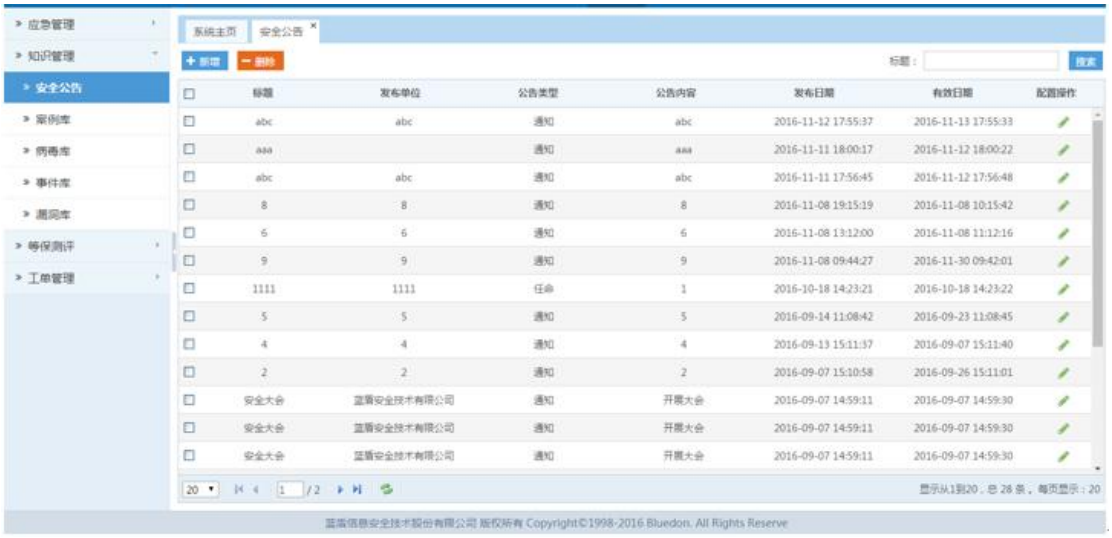
也可以点击  按钮编辑预案，其中***演练开始时间***要大于当前时间，如下图：



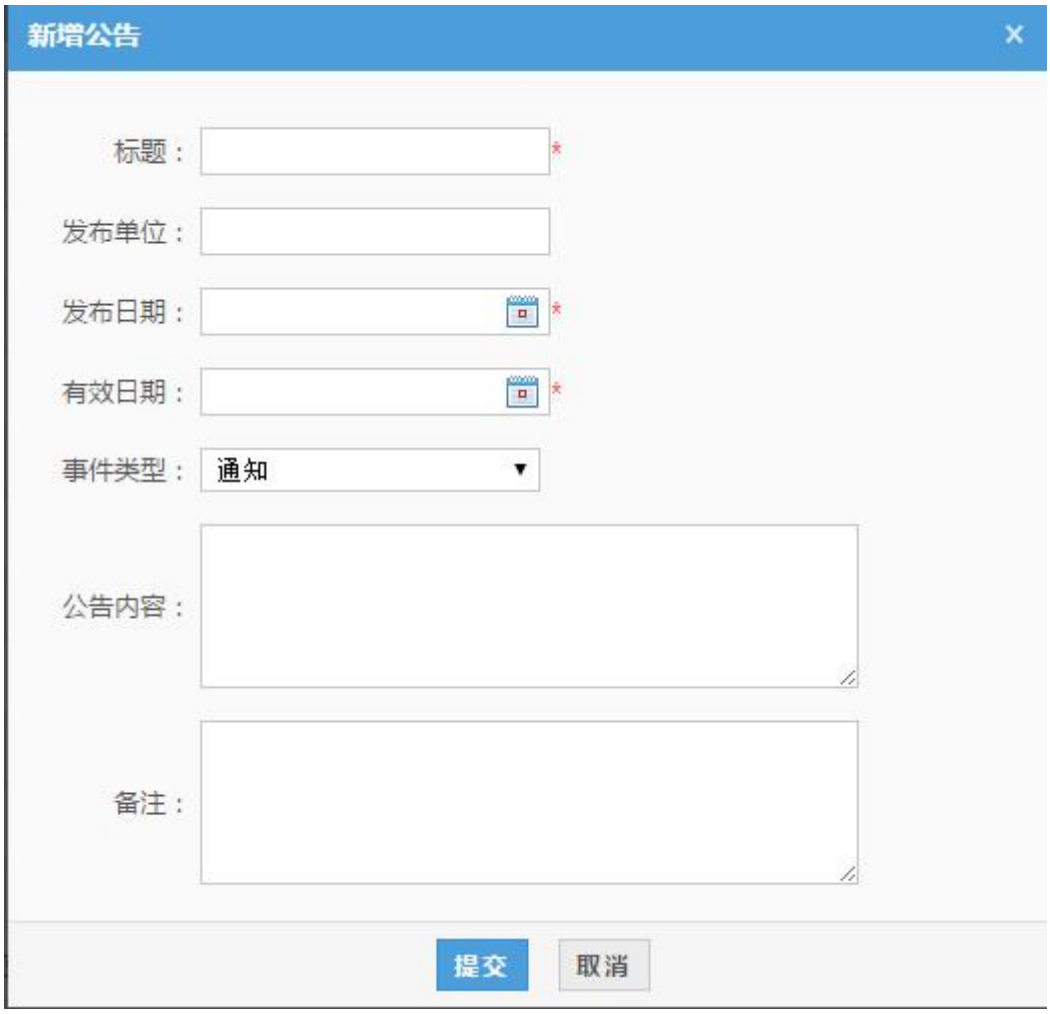
11.2 知识管理

11.2.1 安全公告

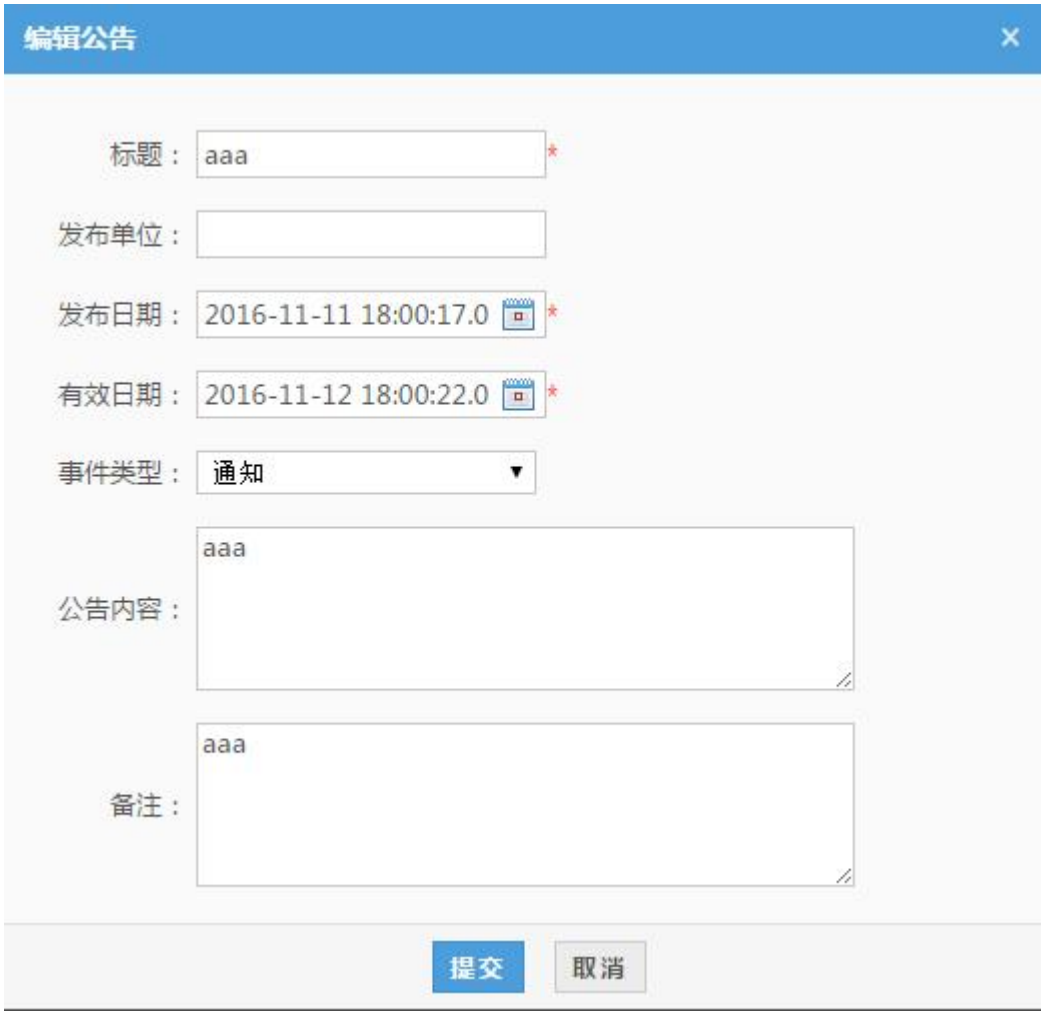
点击**知识管理>安全公告**，用户可看到公告信息。用户可以搜索、删除、新增、配置预案，点击 搜索 按钮通过标题来搜索，选中公告后点击 删除 按钮则删除数据库中公告表中对应的数据，如下图：



点击 新增 按钮，可以新增新的公告,其中发布日期要大于当前时间、有效日期要大于发布日期，如下图：

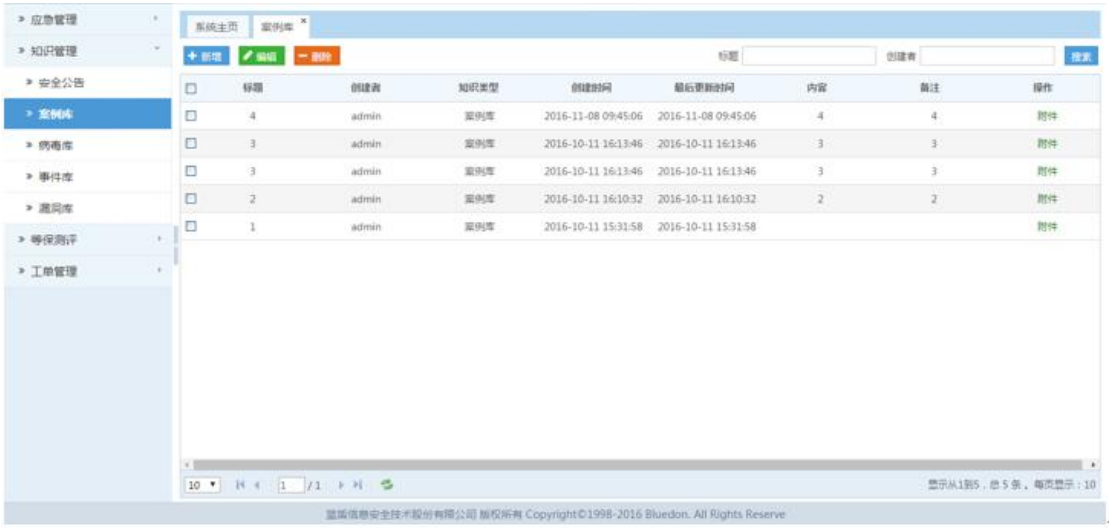


也可以点击 按钮编辑公告，如下图：

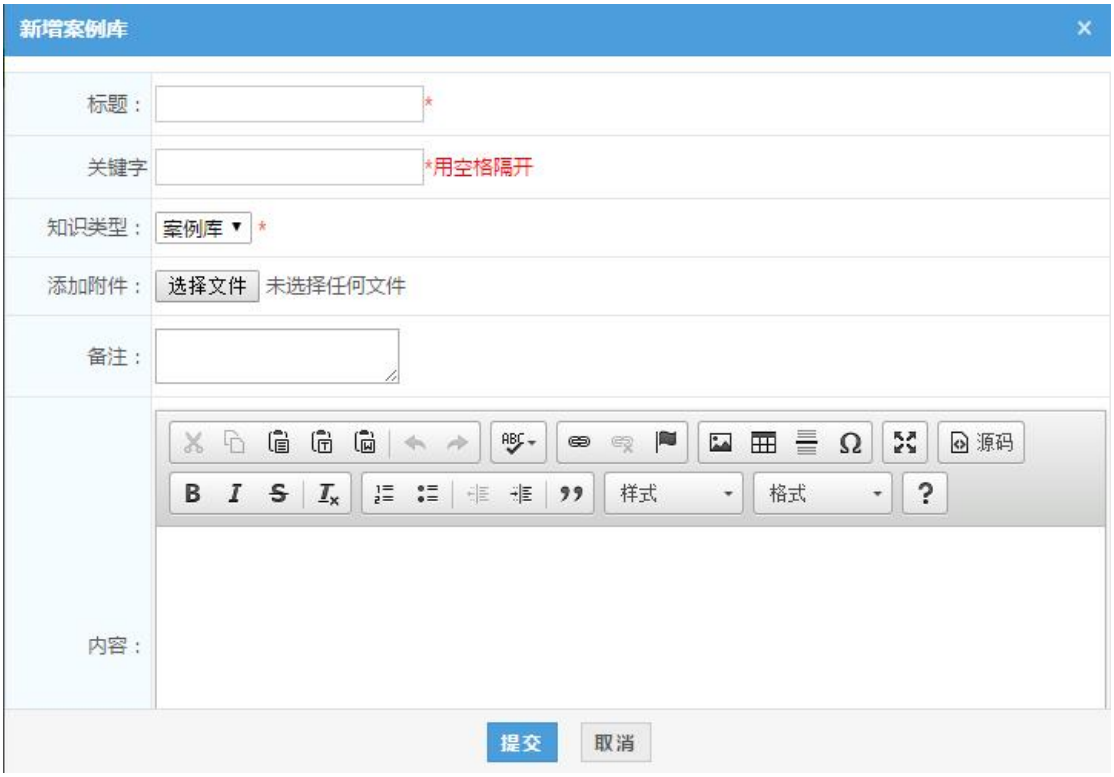


11.2.2 案例库

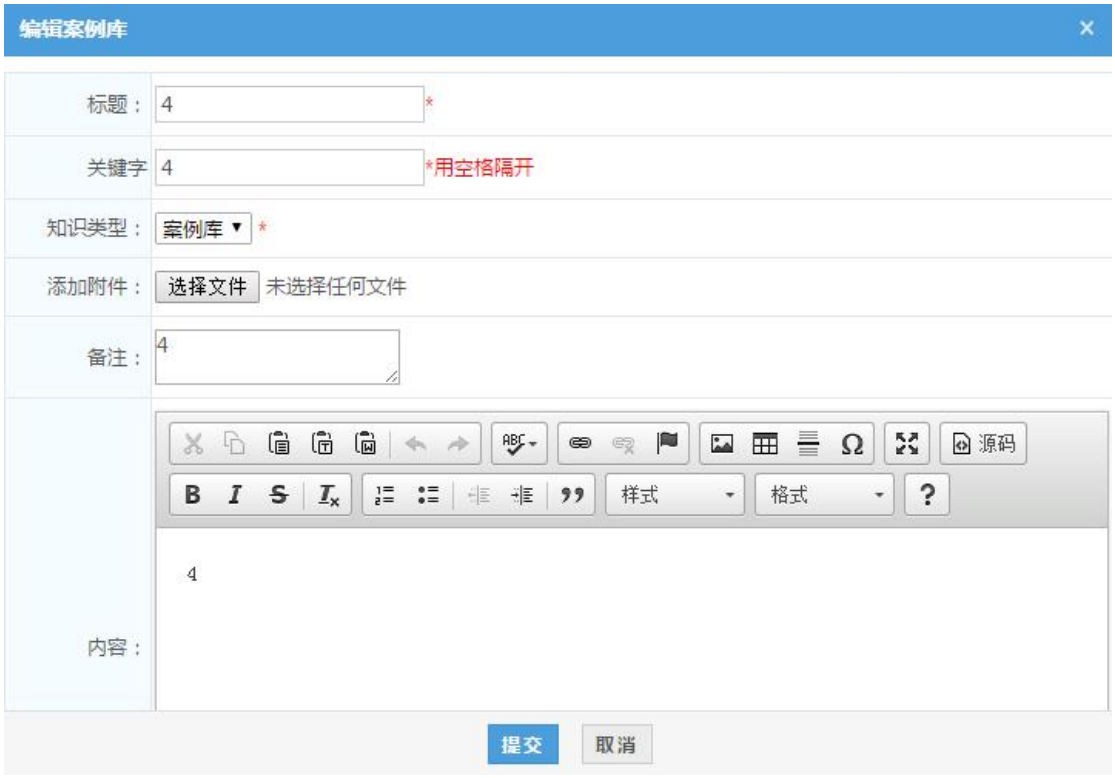
点击**知识管理>案例库**，进入案例库界面，该界面显示了详细的案例信息。用户可看到案例库信息，可以搜索、删除、新增、编辑预案，点击 搜索 按钮通过标题、创建者来搜索，选中案例后点击 删除 按钮则删除数据库中案例表中对应的数据，如下图：



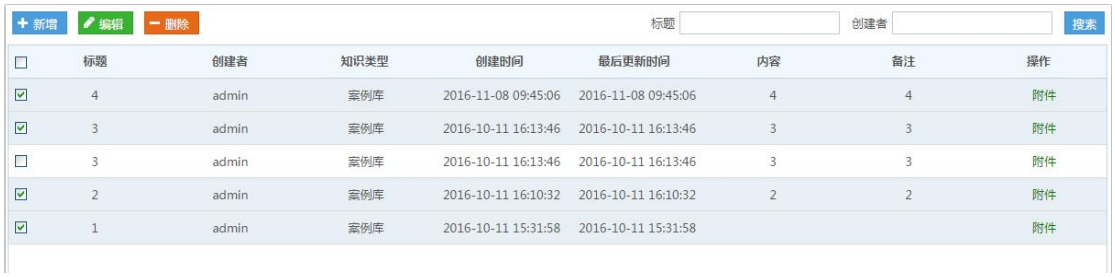
点击 新增 按钮，可以新增新的案例库，如下图：



也可以点击 编辑 按钮编辑案例库，如下图：

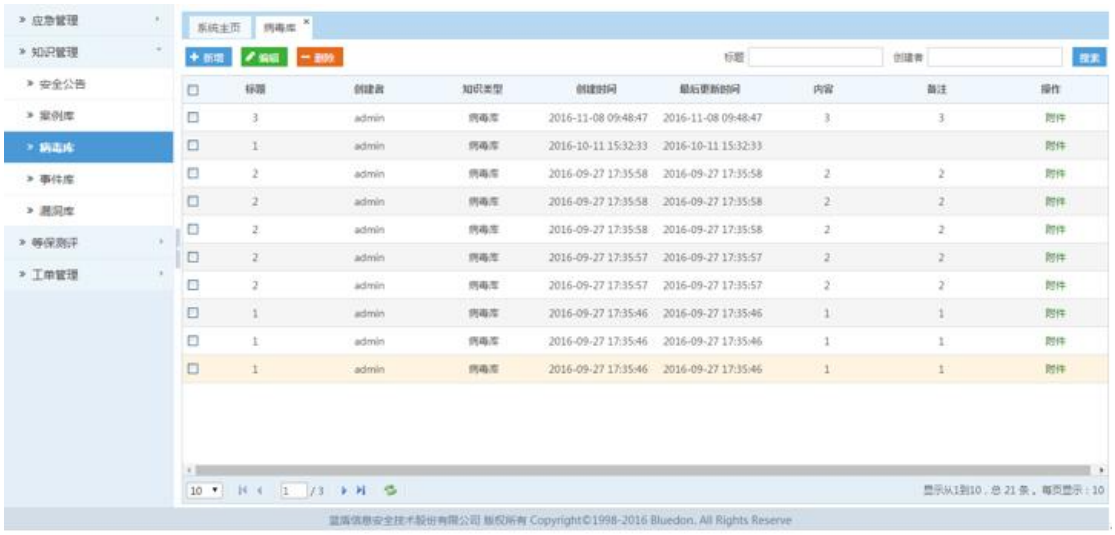


也可以点击 附件 按钮下载附件，如下图：

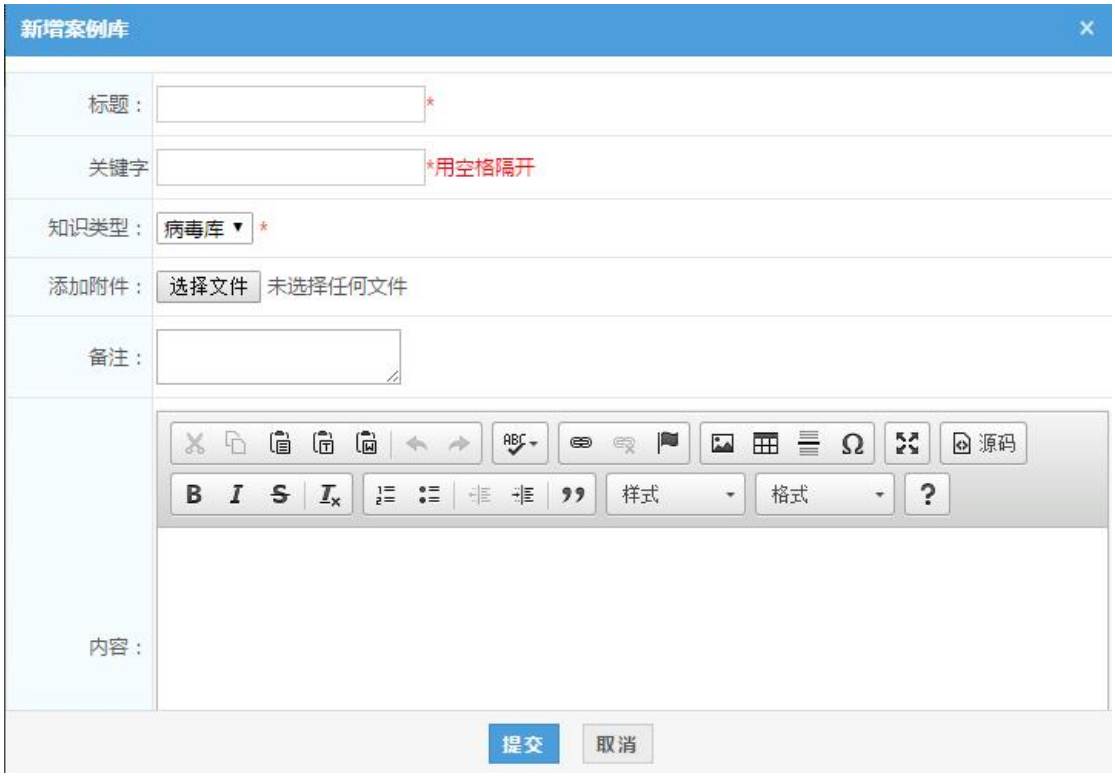


11.2.3 病毒库

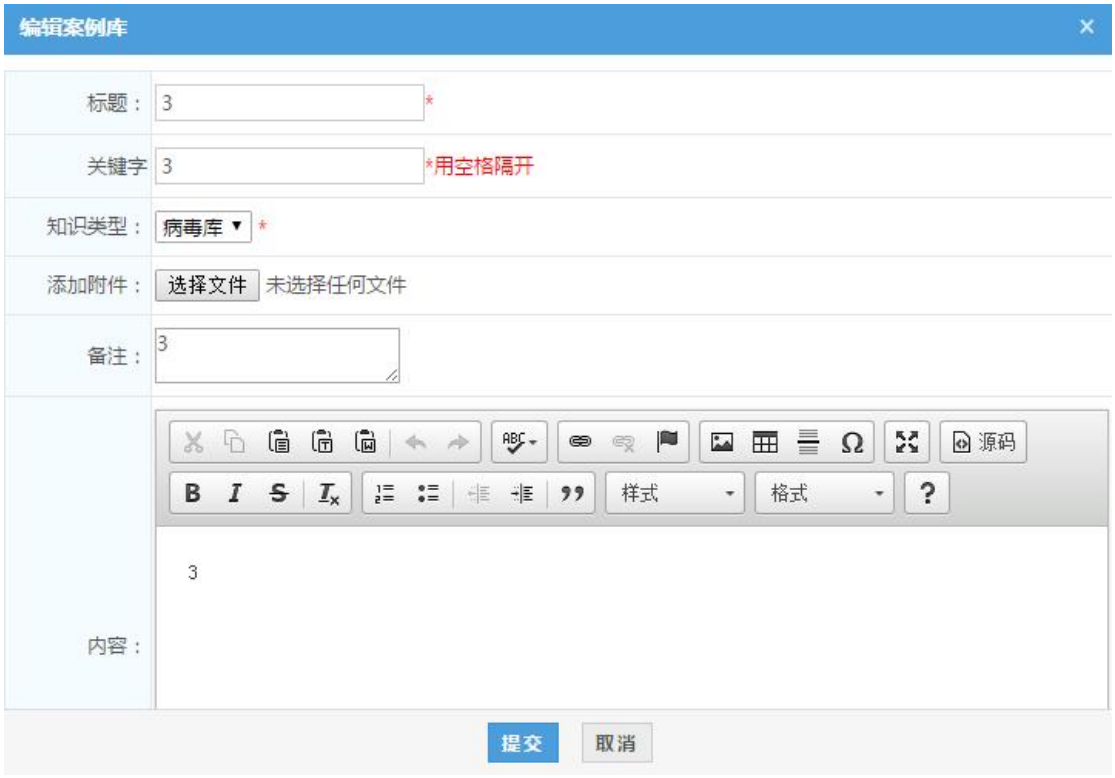
点击**知识管理>病毒库**，进入病毒库界面，该界面显示了详细的病毒库信息。用户可看到病毒库信息，可以搜索、删除、新增、编辑病毒库，点击 搜索 按钮通过标题、创建者来搜索，选中案例后点击 删除 按钮则删除数据库中病毒库表中对应的数据，如下图：



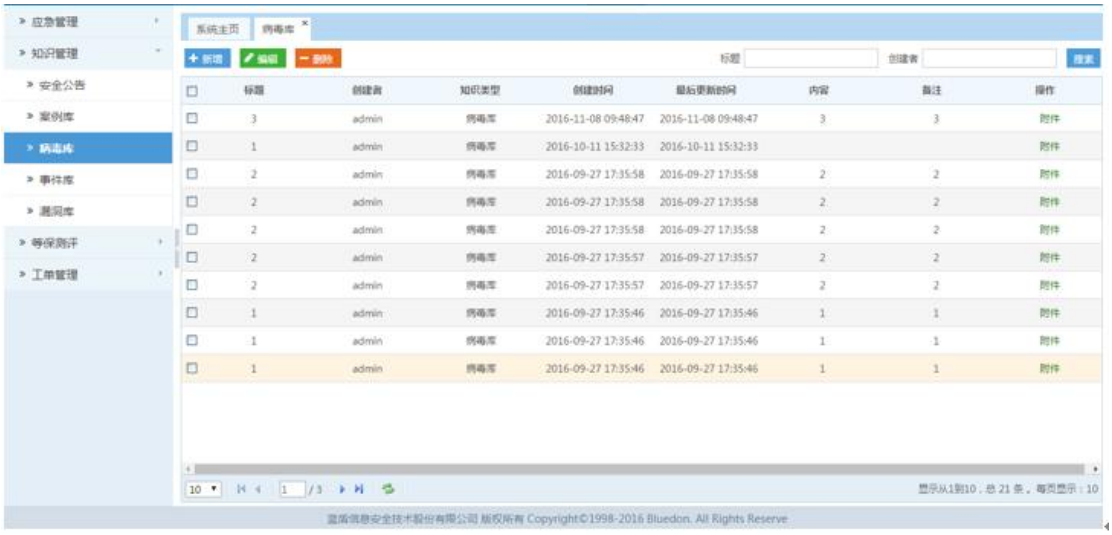
点击 新增 按钮，可以新增新的病毒库，如下图：



也可以点击 编辑 按钮编辑病毒库，如下图：

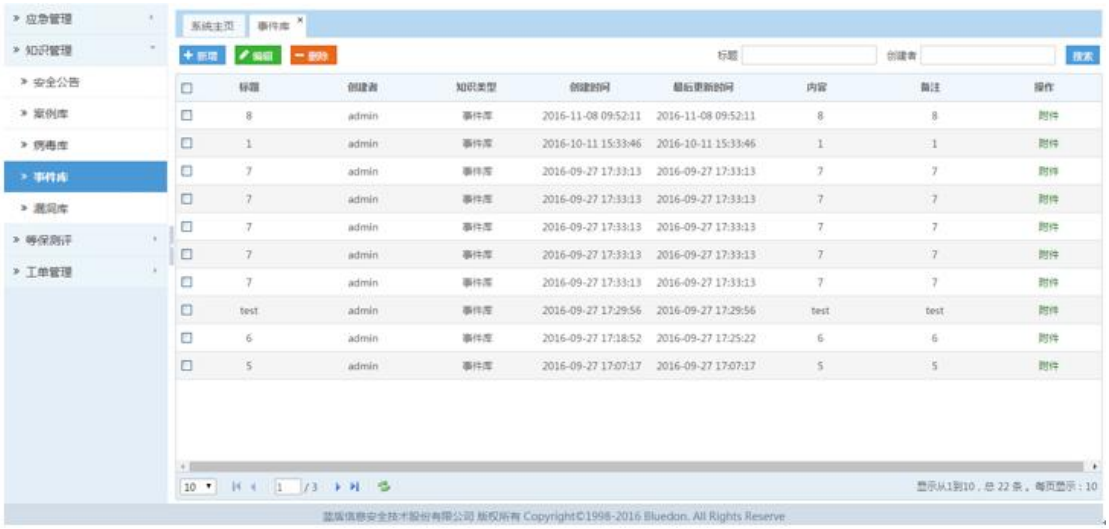


也可以点击 附件 按钮下载附件，如下图：

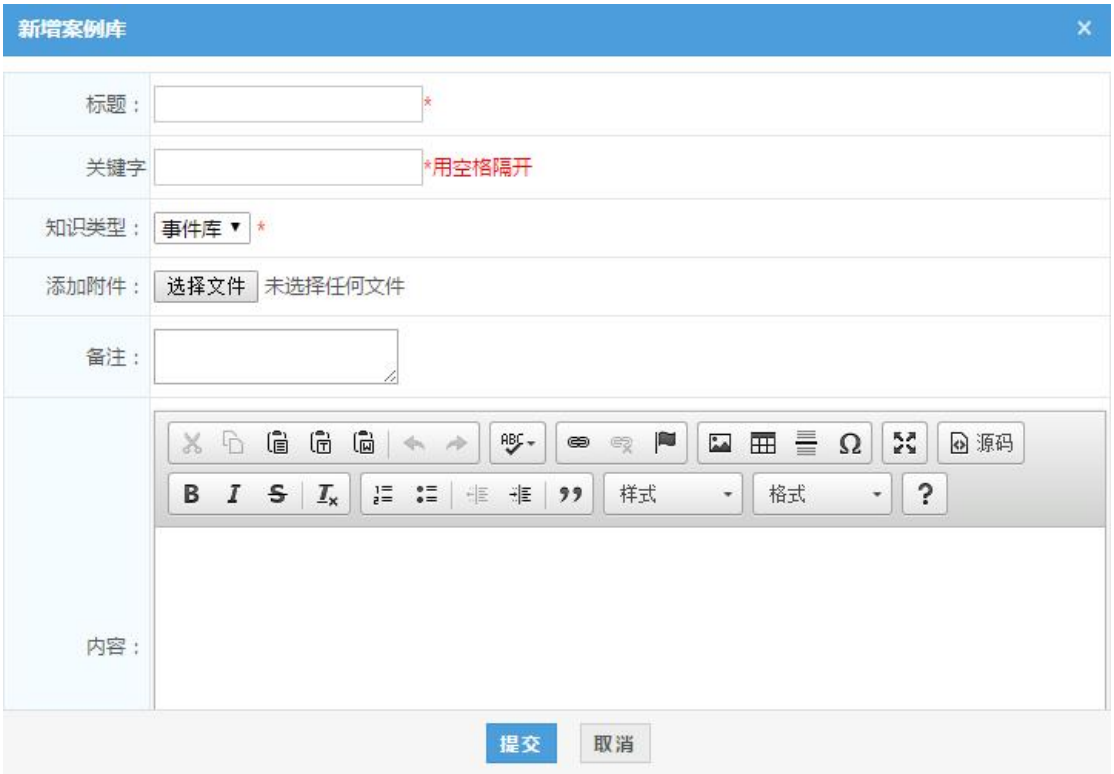


11.2.4 事件库

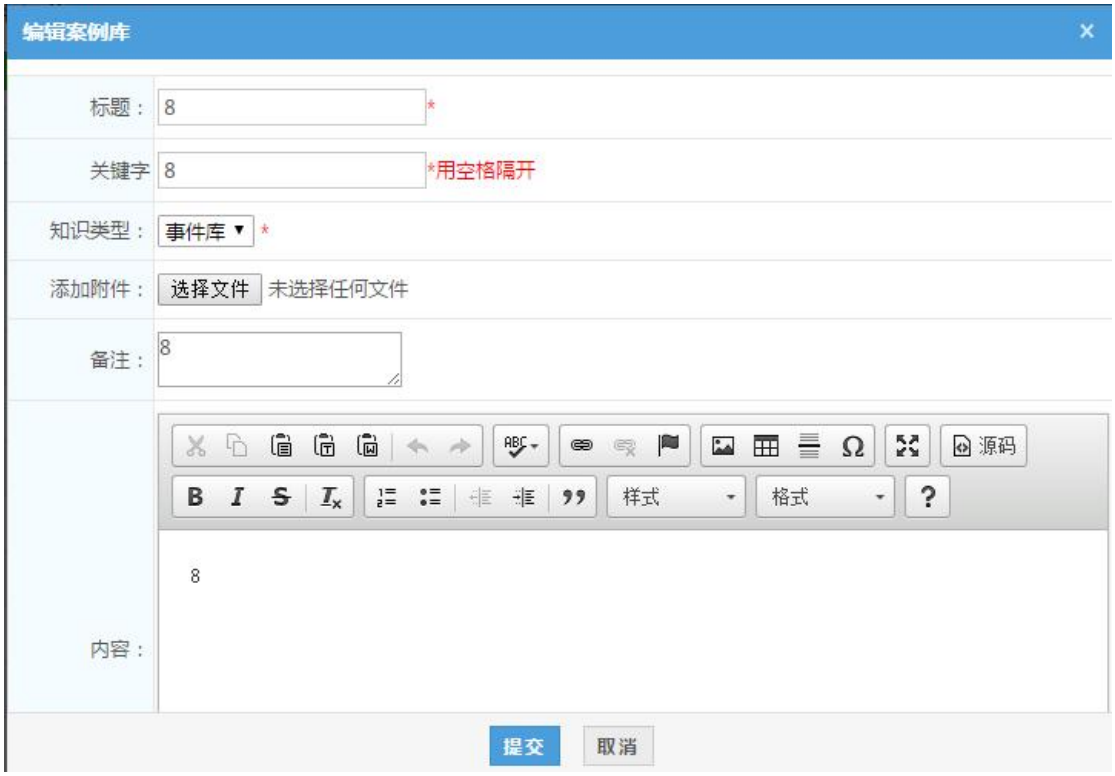
点击**知识管理>事件库**，进入事件库界面，该界面显示了详细的事件库信息。用户可看到事件库信息，可以搜索、删除、新增、编辑病毒库，点击 搜索 按钮通过标题、创建者来搜索，选中案例后点击 删除 按钮则删除数据库中事件库表中对应的数据，如下图：



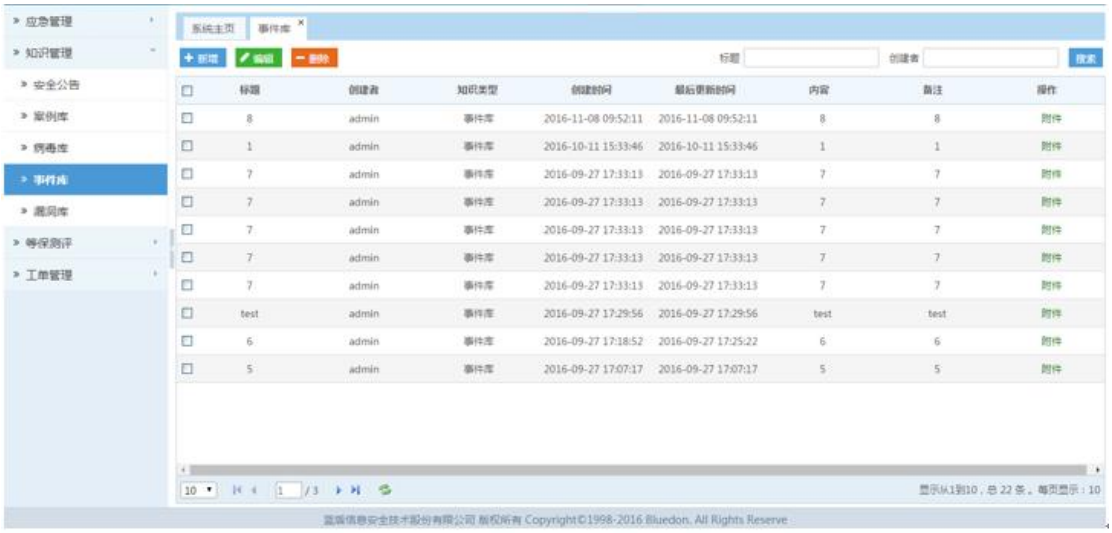
点击 新增 按钮，可以新增新的事件库，如下图：



也可以点击 编辑 按钮编辑事件库，如下图：

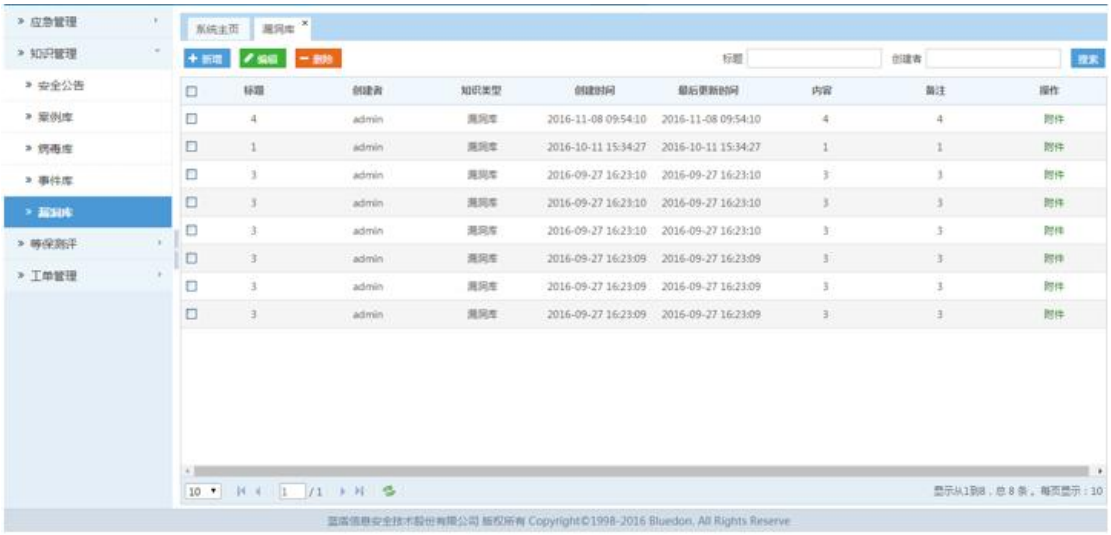


也可以点击 附件 按钮下载附件，如下图：

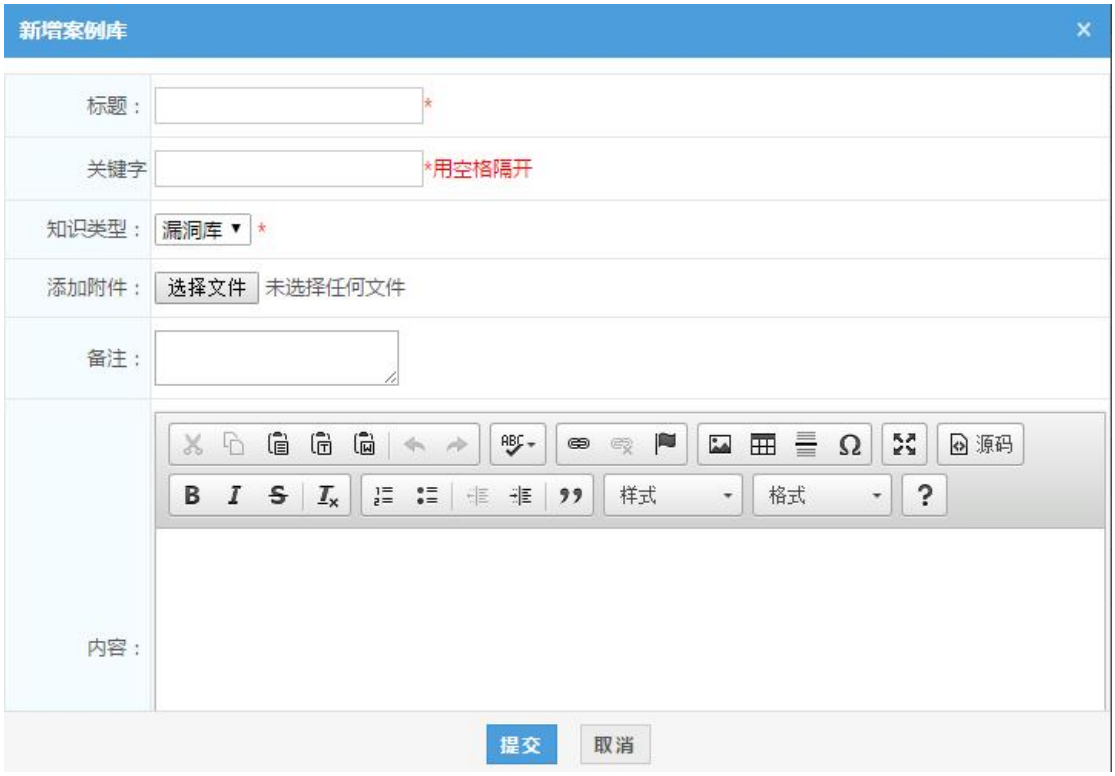


11.2.5 漏洞库

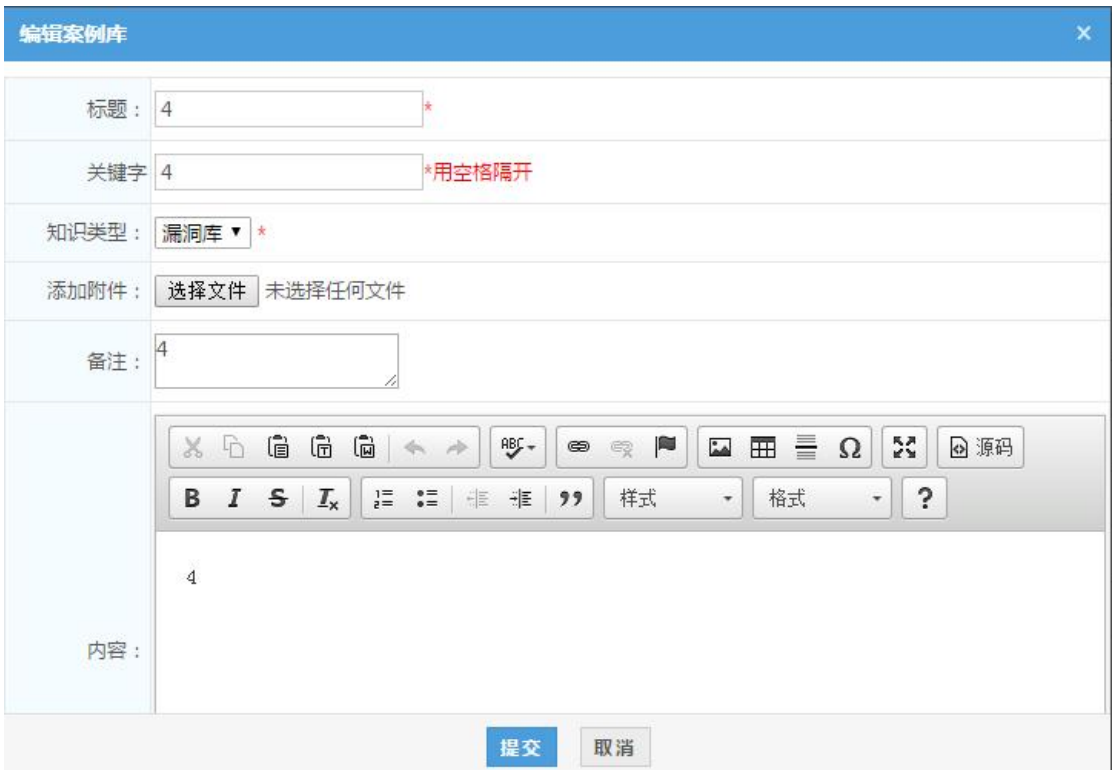
点击**知识管理>漏洞库**，进入漏洞库界面，该界面显示了详细的漏洞库信息。用户可看到漏洞库信息，可以搜索、删除、新增、编辑病毒库，点击 搜索 按钮通过标题、创建者来搜索，选中案例后点击 删除 按钮则删除数据库中漏洞库表中对应的数据，如下图：



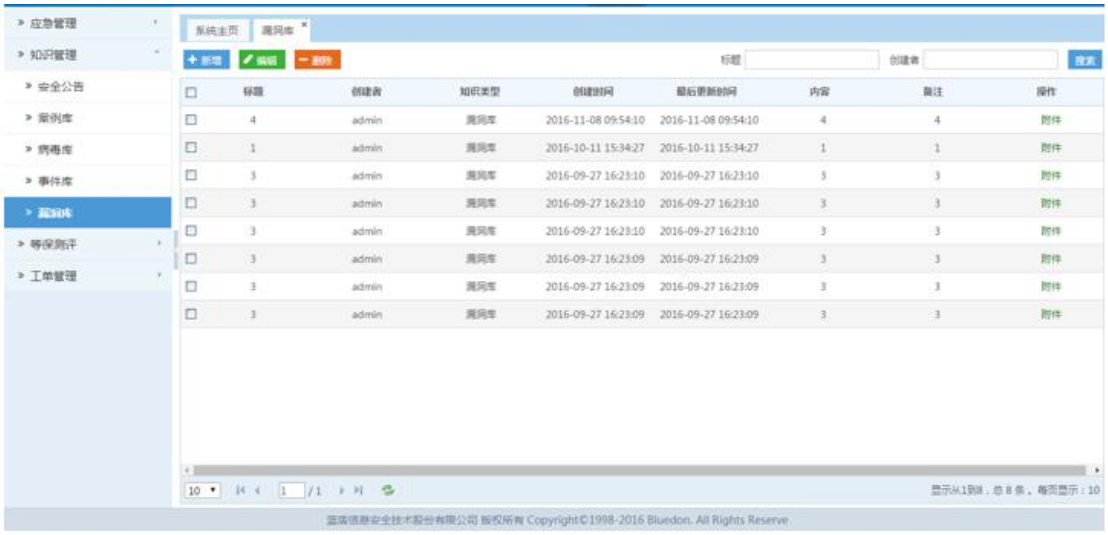
点击 新增 按钮，可以新增新的漏洞库，如下图：



也可以点击 编辑 按钮编辑漏洞库，如下图：



也可以点击 附件 按钮下载附件，如下图：



11.3 等保测评

11.3.1 测评配置

点击**等保测评>测评配置**，用户可看到测评选项和数据操作信息。用户可以选择不同的测评等级，如一级、二级、三级或者四级，也可以选择数据操作的具体测评项目，点击 确定 按钮后设定指标类型成功，如下图：

点击 全部清空 则清空所选测评项目的所有测评数据；

点击 清空测评 则清空所选测评项目的当前测评数据；

点击 反向清空 则清空所选测评项目的当前未测评数据。

11.3.2 测评项目

点击**等保测评>测评项目**，用户可看到物理安全、网络安全、主机安全等 10 个不同的测评项目。如下图：

每个测评项目有各自的指标分类和类别，需要添写符合情况、关联威胁、可能性、影响程度后点击 保存 按钮，全部项目添写完之后可以点击 全部保存 按钮。

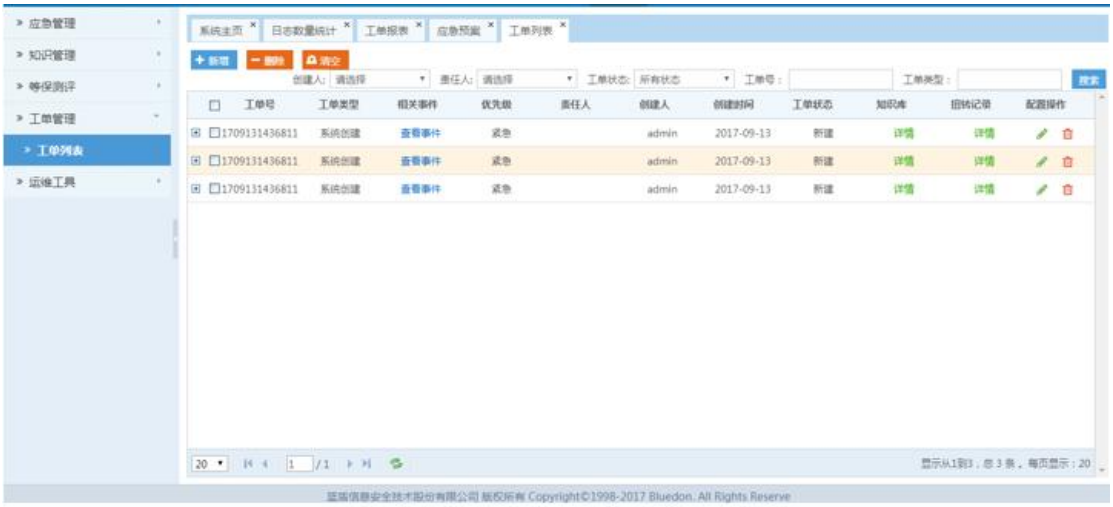
点击 测评统计 按钮，将弹出测评的结果统计列表，如下图：

点击 导出word 按钮，将导出测评项目的 word 文档。

11.4 工单管理

11.4.1 事件工单

点击**工单管理>事件工单**，用户可看到工单信息。工单主要由告警策略生成，用户可以搜索、删除、新增、配置工单，点击 搜索 按钮通过工单号、工单类型来搜索，选中公告后点击 删除 按钮或者 按钮删除数据库中工单表中对应的数据，如下图：



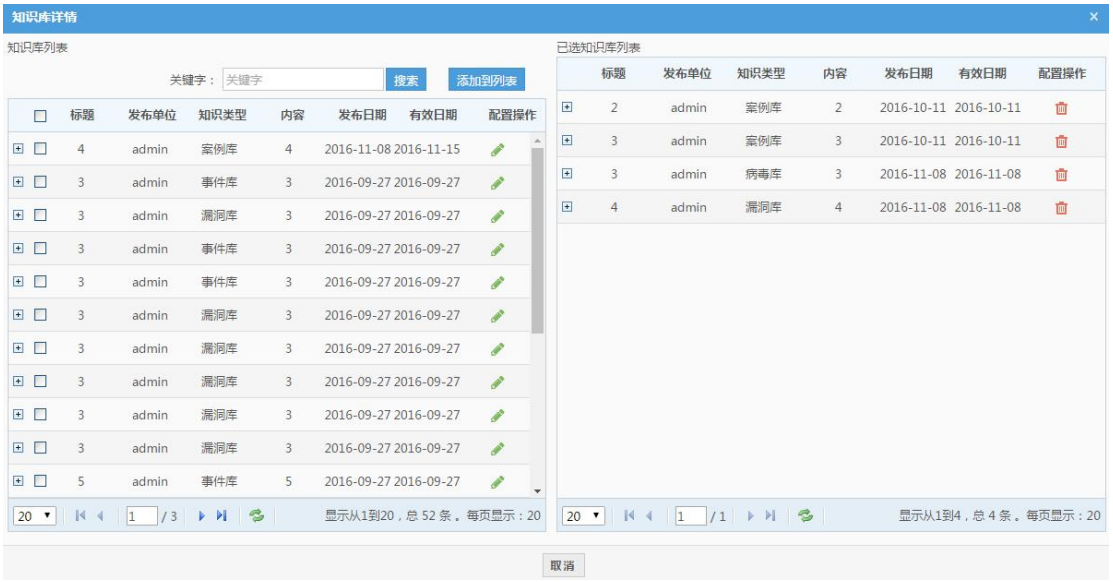
点击 

按钮，可以新增新的公告，如下图：

也可以点击  按钮编辑工单，如下图：

也可以点击 

按钮查看工单详情，如下图：



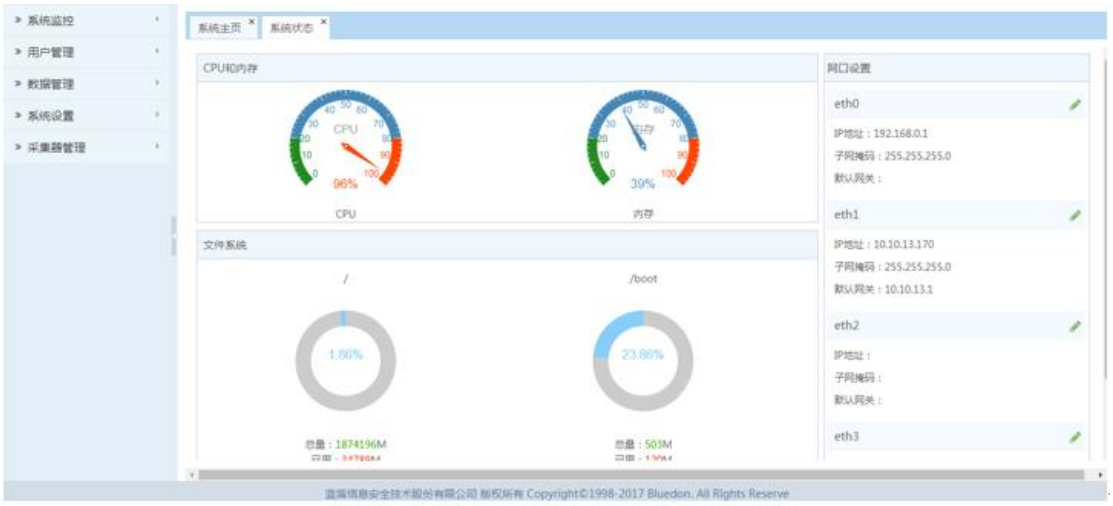
在详情中也可以将知识库列表中的数据选中添加到已选知识库列表中，已选知识库列表的数据也可以删除回到知识库列表中。

第 12 章 系统管理

12.1 系统监控

12.1.1 系统状态

点击**系统监控>系统状态**，用户可看到 Web 服务器所在系统的 CPU 使用率和内存使用率，页面还显示文件系统的使用情况。如下图:



点击  按钮可以设置网口信息（除了网口名称和 IP 地址），如下图:

12.1.2 系统各组件状态

点击**系统监控>系统各组件状态**，用户可看到系统版本信息、报表服务器信息、Web 服务器信息、管理服务器信息。如下图：

除此之外，还有分析引擎状态情况，传感器列表还有传感器的状态情况。其中系统信息右侧有关机、重启和设置时间按钮。点击  ，有弹框提示确认重

启；点击  ，有弹框提示确认关机；点击  ，有时间设置弹框，提交后可设置时间。

12.2 用户管理

12.2.1 账号管理

点击**用户管理>账号管理**，进入账号管理界面，该界面用户信息和登录设置信息。用户可以看到登录名、姓名、性别、角色名称等信息；也可以获知登录失败的次数设置，最高不能超过 5 次，登录失败时该 IP 会被锁定的时间，当用户无操作超过时间再操作时返回登录界面和更改密码的强度设置。点击 

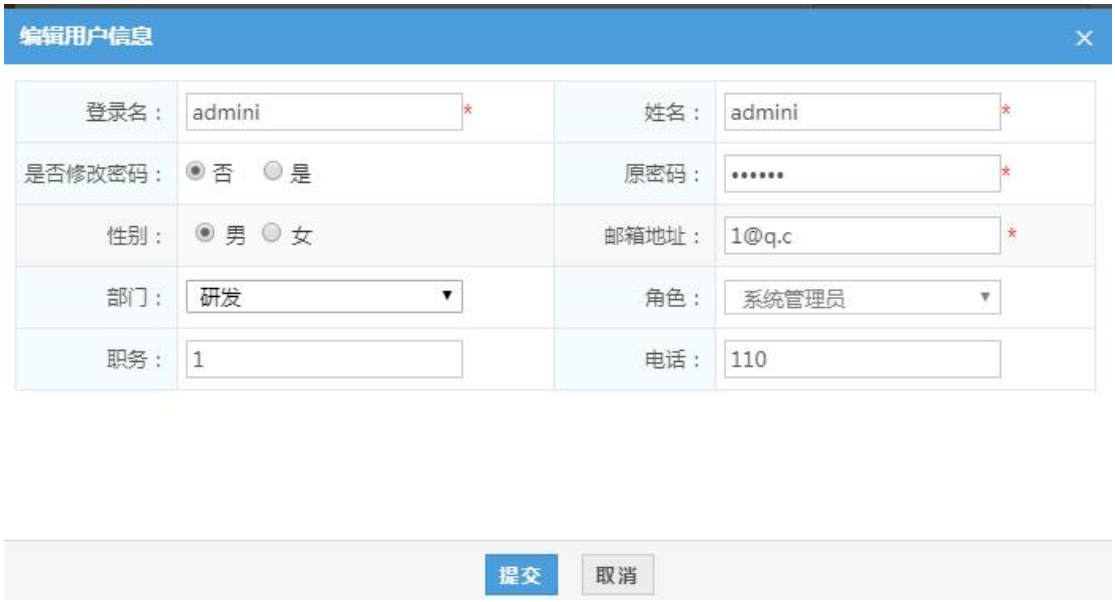
按钮通过登录名、姓名来搜索，选中账号后点击 

按钮则删除数据库中对应的数据，如下图：

点击 

按钮，可以新增新的账号信息，如下图：

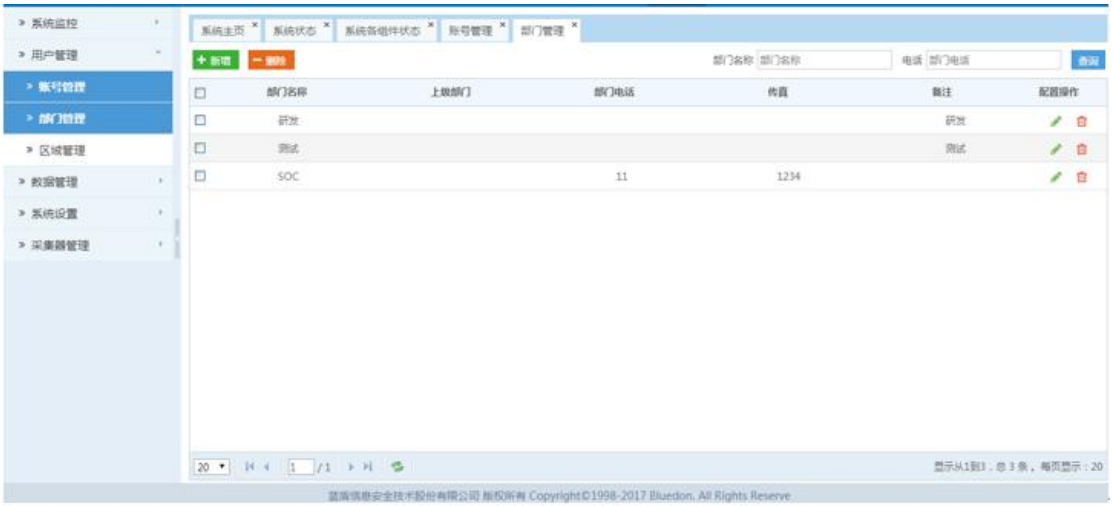
也可以点击 按钮编辑账号信息，如下图：



同一个角色只能创建、编辑同种角色，不能跨角色处理。

12.2.2 部门管理

点击**用户管理>部门管理**，进入部门管理界面，该界面显示了详细的部门信息。用户可看到部门名称、上级部门、部门电话、传真等信息，可以搜索、删除、新增、编辑各部门信息，点击 查询 按钮通过部门名称、电话来搜索，选中部门后点击 删除 按钮则删除数据库中案例表中对应的数据，如下图：



点击 

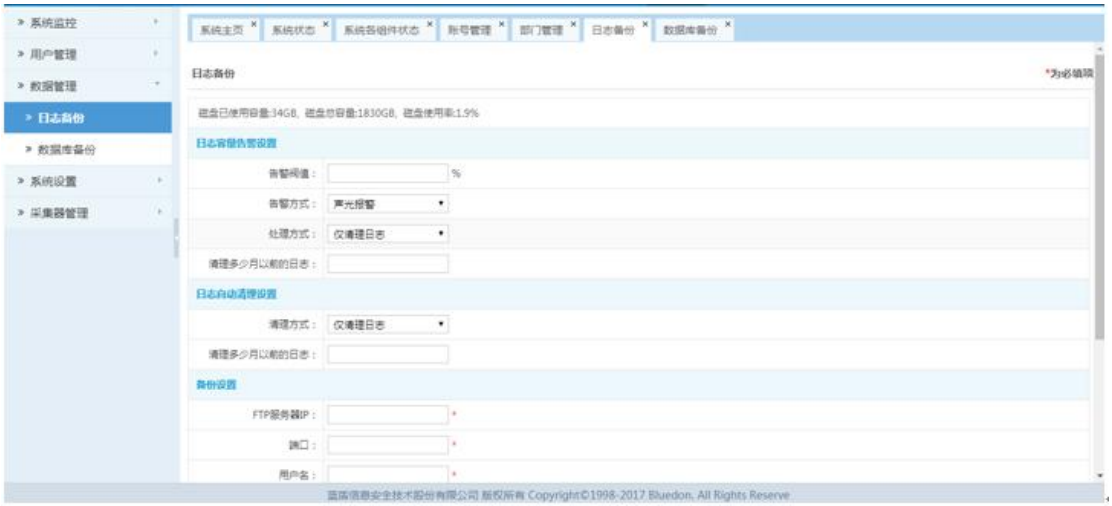
按钮，可以新增新的部门信息，如下图：

也可以点击 
按钮编辑部门信息，如下图：

12.3 数据管理

12.3.1 日志备份

点击**数据管理>日志备份**，用户可在该界面中设置日志告警和备份时间策略。如下图：



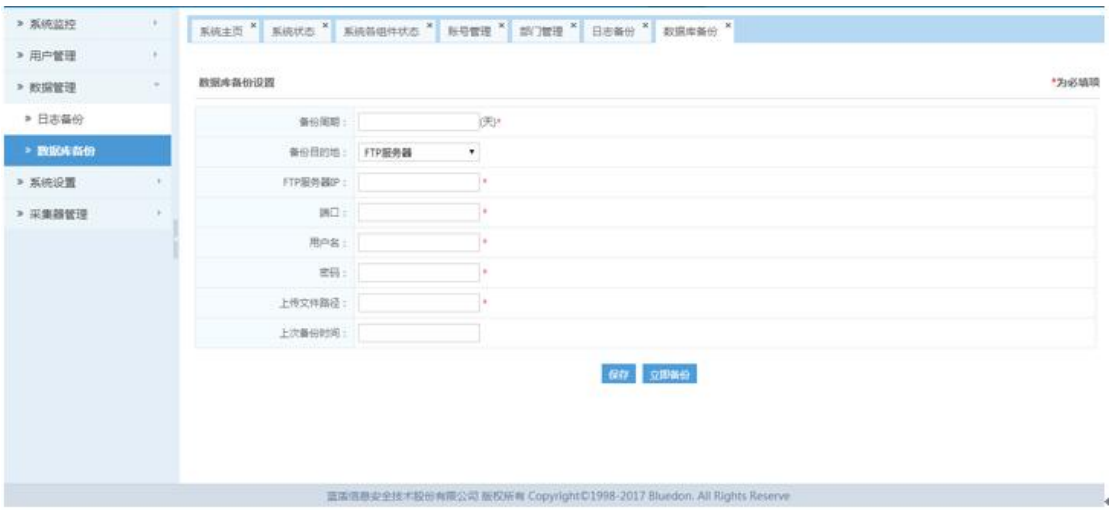
日志容量告警设置，设置告警阀值后，可以以声光告警或者邮件告警并进行告警处理动作（清理日志或者清理并备份日志）。

备份设置，正确设置 FTP 服务器之后，可将日志备份到 FTP 服务器上。

手动清理/备份，设置后可以选择时间段的日志马上进行清理或者备份。

12.3.2 数据库备份

点击**数据管理>数据库备份**，用户可看到数据库 ftp 备份界面。如下图：



用户输入以下信息，点击 保存 可完成数据库 FTP 备份设置的操作，点击

立即备份可将数据库备份到所输入的 FTP 服务器上。

备份周期：以天为单位的备份周期

FTP 服务器 IP：FTP 服务器 IP 地址

端口：FTP 服务器端口

用户名：FTP 服务器用户名称

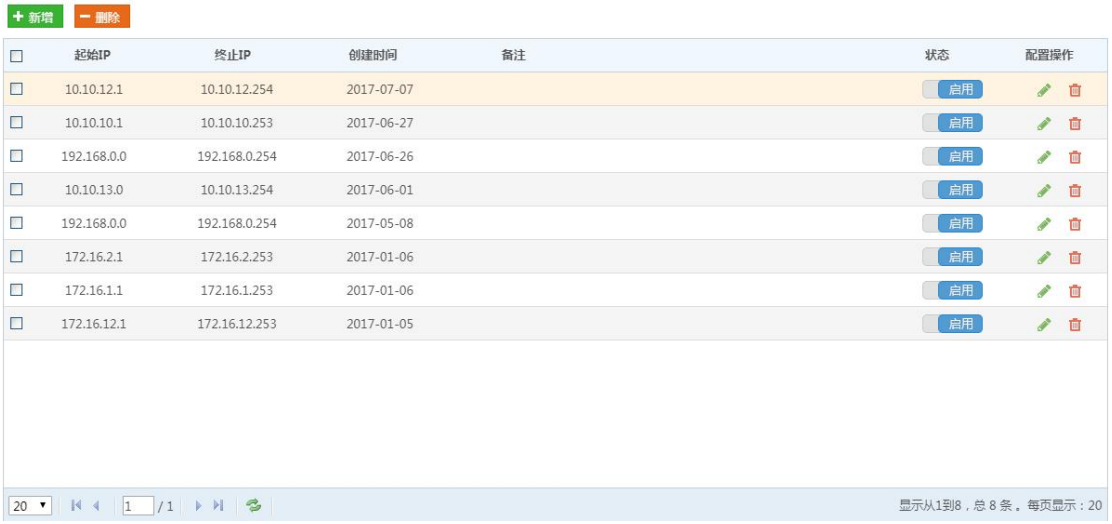
密码：FTP 服务器密码

上传文件路径：上传到 FTP 服务器的文件路径

12.4 系统设置

12.4.1 登陆可信 IP 设置

点击**系统设置>登陆可信 IP 设置**，用户可看到 IP 信息。用户可以删除、新增、配置 IP，选中 IP 后点击 删除 按钮或 按钮则删除 IP，如下图：



点击 新增 按钮，可以新增新的可信 IP，如下图：

对于 IP 的状态可以点击 

使其状态为 

。这样该段 IP 不可再登陆系统，直至状态改回 

。

12.4.2 邮件设置

点击**系统设置>邮件设置**，用户可添写发送者姓名、邮箱地址、邮箱密码、邮件主题、SMTP 服务器、收件人邮箱。用户点击 

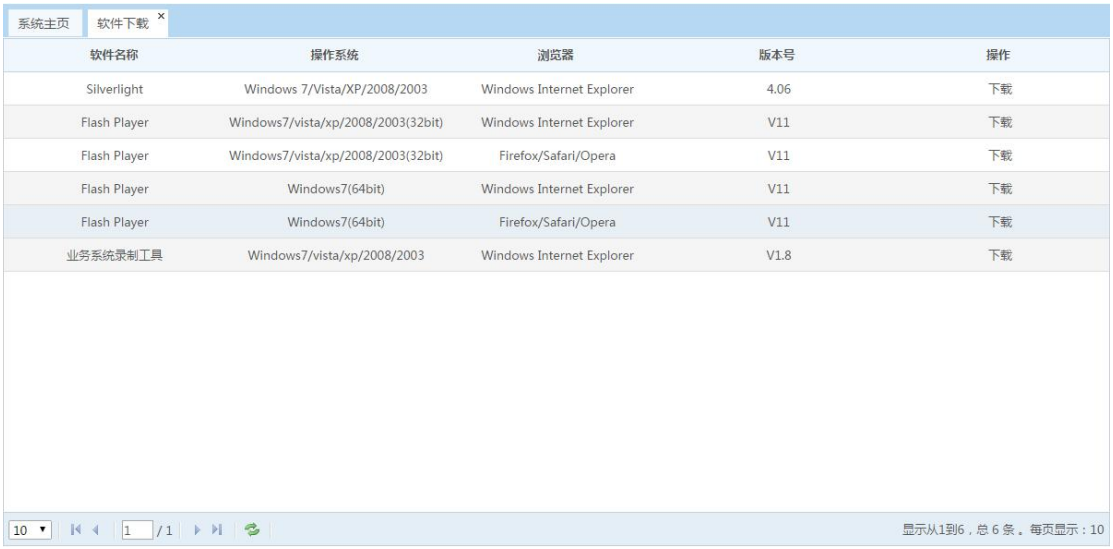
按钮或者 

按钮来操作正确添写后对于触发邮件设置的操作会发送邮件提醒，如下图：

12.4.3 软件下载

点击**系统设置>软件下载**，用户可看到软件信息，如软件名称、操作系统、浏览器、版本号和操作。用户点击 

按钮可以下载对应的软件，如下图：

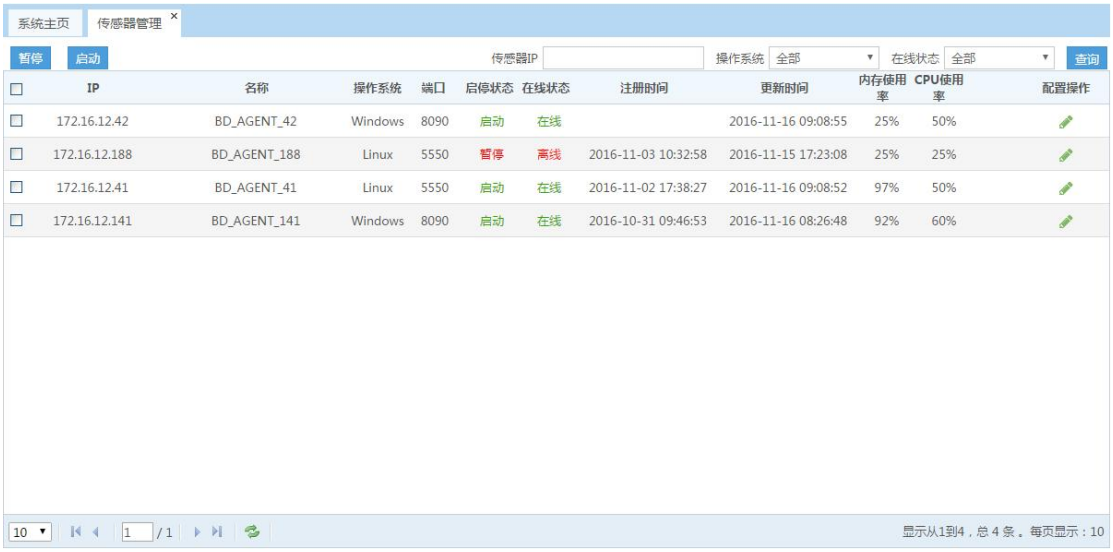


12.5 采集器管理

12.5.1 传感器管理

点击**采集器管理>传感器管理**，用户可看到当前各个采集器的情况。用户可以查询、启动、暂停、编辑传感器，点击 

按钮通过传感器 IP、操作系统、在线状态来搜索，如下图：



选中传感器，点击 

按钮，可以将启动状态的传感器状态改为暂停；

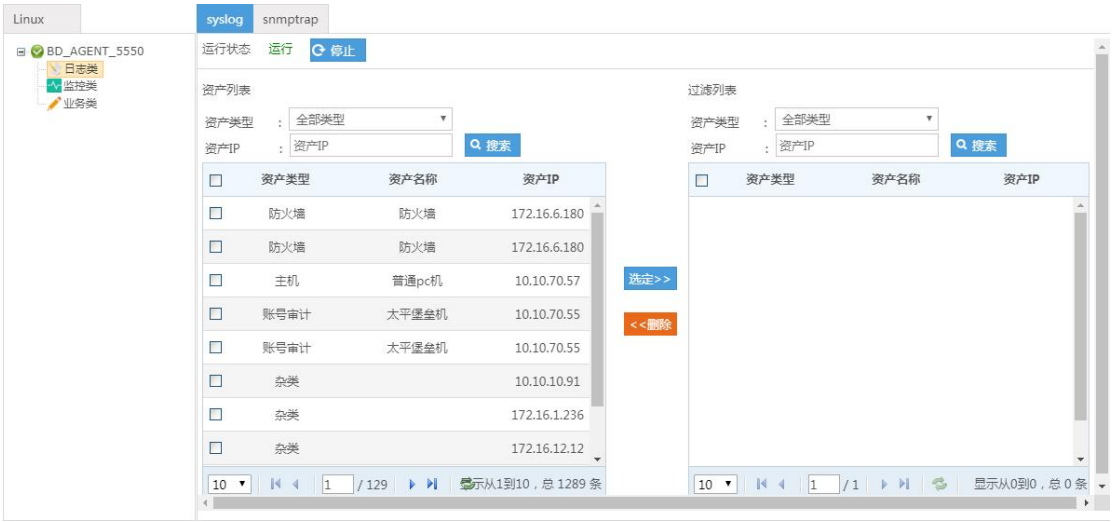
选中传感器，点击 

按钮，可以将暂停状态的传感器状态改为启动。

点击  按钮，可以进入采集器配置来配置采集器，如下图：

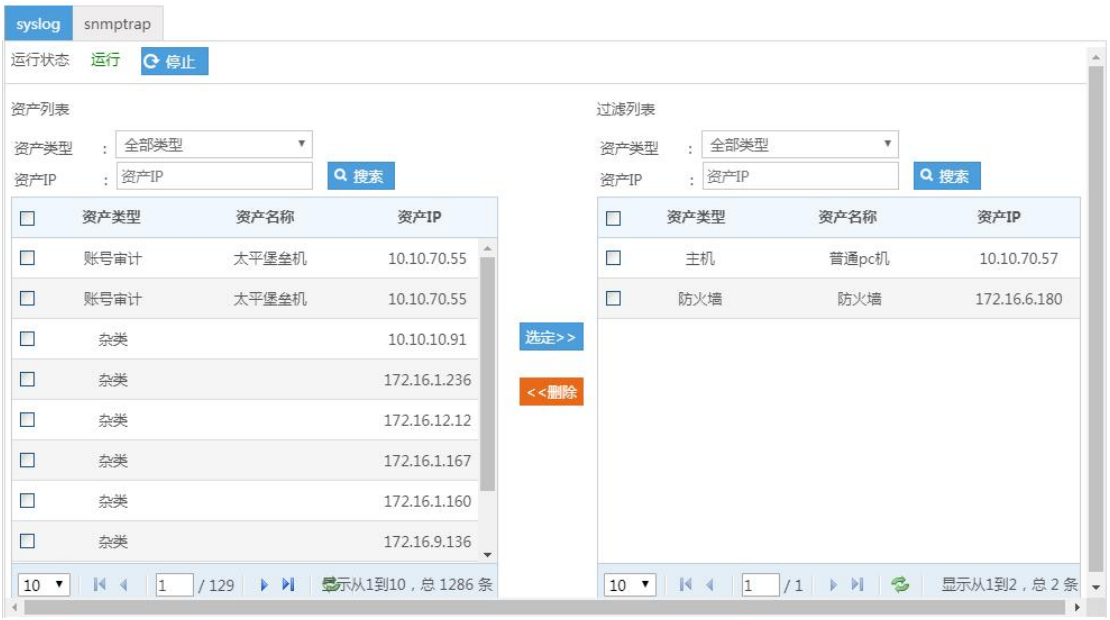
12.5.2 采集插件管理

点击**采集器管理>采集插件管理**，用户可选中传感器中采集器的类别，如下图：

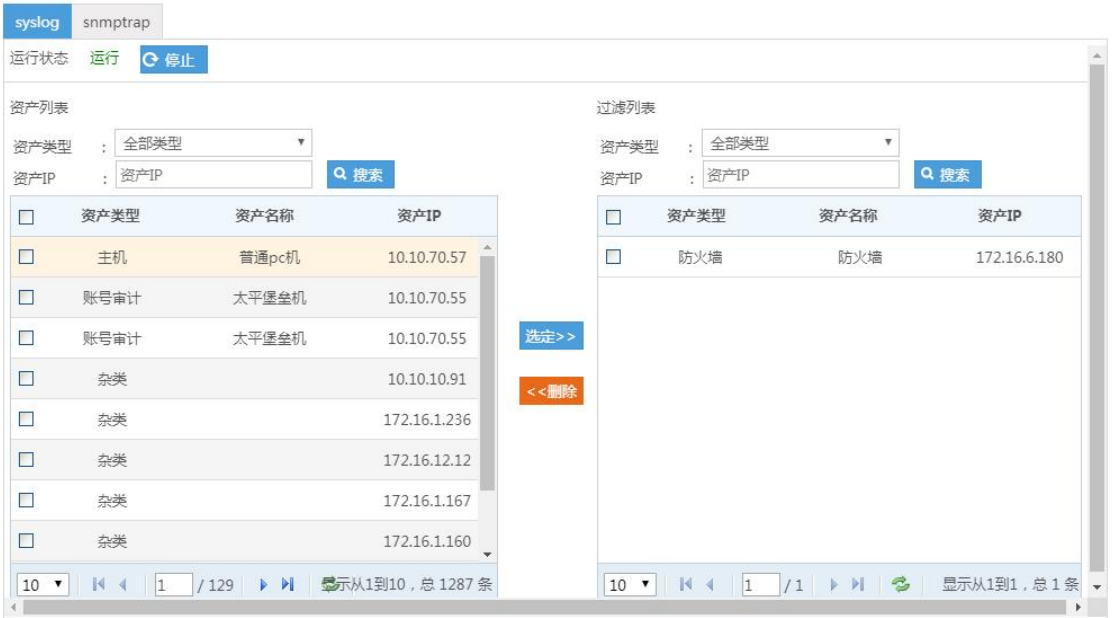


对于启动的传感器，用户点击 启动 按钮或者点击 停止 按钮变动采集

器运行的状态，在采集日志资产列表中可以对资产类型进行筛选，点击 搜索 对资产 IP 进行搜索，选中资产后点击 选定>> 可以将资产列表的资产转移到过滤列表中，如下图：



在过滤列表中选中资产后点击 <<删除 可以将过滤列表的资产转移到资产列表中，如下图：



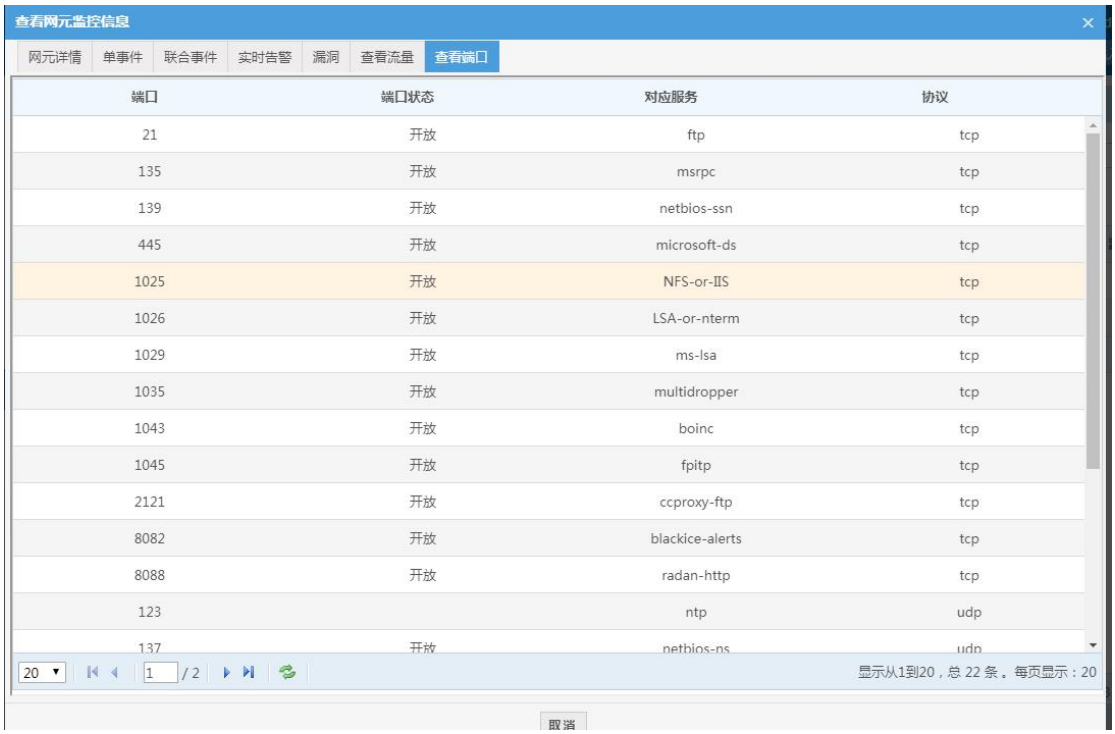
在过滤日志资产列表中也可以对资产类型进行筛选，点击 搜索 对资产 IP 进行搜索。

Windows 系统日志类插件的 wmi 能够采集选定资产的 WMI 日志，采集日志

之前需要配置资产。点击  按钮进入修改 WMI 日志源界面，添写正确的用户名、密码，选择采集日志类型，和采集频率（采集频率可选择 1 小时、3、小时、5 小时），如下图：

Linux 系统监控类***连通性***插件启动后，将对列表中的资产确定与 SOC 是否连通，若通，则网元的连通性为  ，同时**资产管理>合规性检查>网络连接异常检查**为合规。

Linux 系统监控类***端口扫描***插件启动后，将对列表中的资产的端口进行扫描，并将结果同步到网元的监控信息中，如下图：



Linux 系统业务类插件的拓扑启动后配置好核心交换机 IP、snmp 团体名和采集频率后，点击 保存 按钮可以对资产进行自动发现，新发现的资产会在**设备管控>网元**显示，如下图：

点击 重置 按钮，则重新配置核心交换机 IP、snmp 团体名和采集频率。

第 13 章 附录

附录 A:常见问题解答

1、系统提示登录超时。

解答：请重新退出登录。

2、无法获取设备状态值。

解答：检查设备配置参数的查询用户用户名和密码是否正确。

3、无法对设备进行管控。

解答：检查设备配置参数的管控用户用户名和密码是否正确，检查设备类型配置文件是否正确。

4、用户无法进行操作，提示用户权限不够

解答：检查用户组权限配置。