对外公开

东软 NetEye 日志审计系统用户手册

东软公司

Neusoft

目录

一、 概述

1.1 日志审计的必要性

随着信息技术持续地发展，各类组织、企业对信息系统的运用也不断深入，为了在复杂条件下应付各类安全情况（如黑客的攻击、内部员工的有意或无意地进行越权或违规操作），企业部署了大量的、不同种类、形态各异的信息安全产品：

- 为了监控黑客的攻击控制，部署了各种入侵检测或入侵防御设备
- 为了控制内部员工的非法接入，部署了网络终端管理、网络准入等系统
- 为了控制数据的非法泄露或重要数据被修改，部署了防泄漏系统、数据库审计系统
- …

另外，除了这些专用安全设备或系统每日会产生各种日志，组织或企业日常使用的业务系统、主机系统、网络设备等也会生成许多和安全相关的日志，这存在如下问题：

- 它们格式差异巨大，没有统一标准
- 它们数量巨大，用户无法进行重点分析
- 难以挖掘各类日志之间的关联关系，从而难以审计

上述这些原因均会导致日志审计工作难以开展，所以各组织或企业需要部署集中的日志分析系统；另外，各组织或企业部署集中日志分析系统的意义在于：

- 它是信息安全管理的需要：因为日志审计是日常信息安全管理中最为重要的环节之一；能从纷繁复杂的日志中萃取出具有价值的部分是各类信息安全管理者、参与者、相关者最大的诉求，故选择一款高可靠、高性能、具备强大功能的日志集中审计系统就成为必须；
- 它是安全技术保障体系建设要求的需要：一个完整的信息安全技术保障体系应由检测、保护和响应三部分组成，而日志审计是检测、分析安全事件的不可或缺的重要手段之一。目前，大部分信息系统所依赖的 IDS/IPS 只能检测部分来自网络的攻击事件，对运维人员的违规操作、系统运行异常、设备故障等安全事件缺乏监控能力，而这些异常事件恰恰是对内部信息系统安全威胁最大的来源之一。日志分析系统通过分析各设备、系统、应用、数据库产生的运行日志，能够及时发现入侵检测系统检测不到的各类安全隐患及合规审计违规情况，并及时给予告警，从而在安全事件发生前做出积极防御；
- 它是各种规范符合性要求的需要：如：《信息安全等级保护》（几乎各级均要求提供审计功能）、《信息安全风险管理规范》、《基于互联网电子政务信息安全指南》、《银行业金融机构信息系统管理指引》等等。此外，国际上的相关标准、规范也均明确提出信息安全审计系统的重要性，如萨班斯法案、ISO27001 等均要求企业对重要系统、设备的运行日志进行保留，并且周期性地进行第三方审计。

1.2 日志审计系统

东软 NetEye 日志审计系统（简称日志审计系统）通过集中采集各类系统中的安全事件（如网络攻击、病毒攻击等）、用户访问记录、系统运行日志、系统运行状态、网络存取日志等各类信息，经过规范化、过滤、归并和分析后，以统一格式进行集中存储和管理。

日志分析系统能够对信息系统中各类主机、数据库、应用和设备的安全事件进行实时采集、实时分析、异常报警、集中存储和分析审计，支持分布式部署，具备对各类网络设备、安全设备、操作系统、中间件服务器、通用服务、数据库和其它应用进行全面的日志安全审计能力。

通过日志分析系统，相关人员可以随时了解系统的整体运行情况，及时发现系统异常事件及审计违规行为；通过事后分析和丰富的报表系统，管理员可以方便高效地对信息系统进行有针对性的安全审计。遇到特殊安全事件和系统故障，日志审计系统可以确保日志完整性和可用性，协助管理员进行故障快速定位，并提供客观依据进行追查和恢复。

因此，日志审计系统可以帮助用户有效降低业务系统故障率，减少潜在的经济损失，降低运维成本和管理的复杂度，显著提高系统整体的安全性、可靠性和运行效率，保证信息系统 7*24 小时的正常、持续、稳定运行，从而降低信息系统的整体安全风险。

二、 日志审计系统架构和运行环境

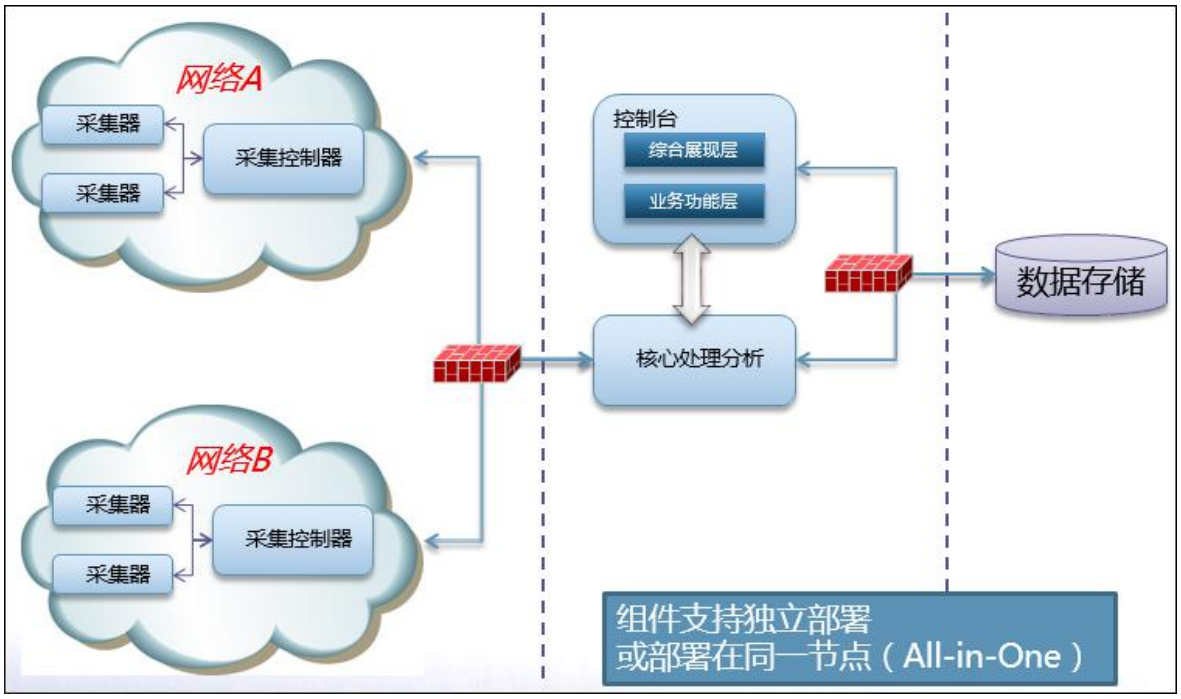
2.1 总体架构

总体而言，日志审计系统包括数据存储、管理控制（控制台）、核心处理分析和采集控制四大组件群。

其中，数据存储部分负责存储系统内所有数据，它不仅包括一般的关系式数据库还包括了一个可分布的原始数据存储器和查询器；管理控制组件主要指一个基于 Web 的控制台；核心处理分析组件群主要包含各类安全数据分析、风险计算、任务调度、响应处理的组件；而采集控制组件群包含了一个到多个可分级部署的数据采集控制器/采集器，它是日志审计系统的主要数据来源。

根据实施规模的大小，上述四个组件群均可分开部署，也可以进行不同的组合。

上述关系如下图所示：



本文主要描述的是管理控制（控制台）的相关主要功能。

2.2 运行环境

日志审计系统的数据存储、管理控制、采集控制及核心处理分析均运行于 CentOS 系统（x86 64 位）上。

建议采用 FireFox、谷歌或 IE11（含）以上浏览器查看系统。

三、 硬件配置平台

平台说明：该平台主要负责设备基本配置，完成设备上架运行前各准备工作。

3.1 初始状态说明：

默认 IP 地址	eth0	192.168.1.100
	eth5（或 eth3 设备最后一个电口）	1.1.1.1（该地址不能修改）

设备登录方式	设备应用	https://ip
	设备硬件管理平台	https://ip:8082
默认用户名密码	admin	neteye

3.2 网络配置

修改设备访问地址，在设备运行过程中，需要设备与网络中各资产路由可达。

选择对应网络接口，配置 ip 地址，并保存，更改完端口 ip，设备会提示重启，设备重启之后会完成系统中各组件的相关配置，该 ip 地址才可正常使用。

路由配置：

3.3 时间调整

为了正确反映收集到的日志及网络中各个行为，需要调整设备时间与网络中各资产时间一致。

3.4 数据备份

系统支持手动备份，定时备份及周期备份，同时支持多种备份方式，可以将设备日志备份到第三方存储设备。

四、 主要业务及流程

4.1 采集管理

采集管理是系统进行事件分析的第一步，用户通过指定需要采集的目标、相关采集参数（Syslog、SNMP Trap 等被动方式无需指定）、相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。采集管理包括采集策略管理和采集器管理。

4.2 资产管理

安全资产是系统基础的管理对象、是风险分析的依据；与 ISO27001 的关于资产的定义略有不同，日志审计系统中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务和应用。

资产管理支持用户录入、导入或自动发现资产。为了处理不同网络的资产具有相同 IP 的问题，系统还支持对于网络和 IP 地址段的管理。为了用户便于集中、灵活地管理所辖范围内的资产，日志审计系统支持用户自定义资产管理视图。

日志分析系统中的关联、审计策略都是针对资产上产生的事件而触发的，而实时事件监控以及事件查询不受资产的影响，是针对设备产生的事件。

4.3 事件分析

日志审计系统的事件分析功能是系统中的核心功能，对于分析所产生的结果，如果符合关联策略，将在关联事件中呈现，如果用户配置了产生告警，将以告警的形式在安全监控模块呈现给用户，用户可以对告警进行相关的处理。

创建关联策略时，系统支持基于规则和基于统计两种方式进行事件关联，同时，还支持短时间或长时间的事件关联，最长可达 30 天。

4.4 审计管理

日志审计系统的审计管理功能是系统中的又一核心功能，审计管理侧重于发现日志中相关要素是否和预定的审计策略相符，如时间、地点、人员、方式等，对于相符合的结果，系统将以审计事件的形式呈现给用户，用户可以根据审计类型、审计策略、审计人员、审计目标地址四个维度对审计事件进行查看；对于关心的审计事件，用户可以在审计策略中配置告警相关信息，系统将在安全监控菜单下以告警的形式呈现给用户，用户可以对告警进行相关的处理，也可以通过邮件提醒，或转发外部系统的方式进行处理。

审计管理为安全管理员提供了一个统一的审计工具，减少人、财、物的投入，降低了综合审计成本。

审计管理能够方便的自定义审计人员、审计对象、审计类型、审计策略等基本配置；并能够自定义审计策略模板，审计管理内置了大量审计模板，涵盖了常见的、对企业非常实用的审计策略模板，如主机、防火墙、数据库、等级保护、萨班斯审计策略模板等；审计策略管理允许用户在创建审计策略时自定义审计对象，也可以预定义审计对象作持久化对象使用。

4.5 安全监控

安全监控包括告警监控和实时监控。

告警是指用户特别需要关注的安全问题，这些问题来源于关联事件分析、审计事件分析的结果。

告警监控中包括了如下功能：

- 监控系统内存在的各种告警；用户可以通过定义过滤器以监控需要特别关注的告警信息；用户也可以根据个人需求，设置告警的提示音、界面显示方式等；
- 告警处理：处理监控列表中相关告警；针对告警，用户可以清除、确认（不能确定是否需要处理）；

实时监控是指对当前接入的事件日志逐条、实时显示，显示的日志内容是可以根据用户的需求进行设

置过滤条件来定制的。

实时监控中包括了如下功能：

- 设置监控过滤规则：根据用户需要或分析过程的需要设定显示过滤条件，便于观察日志实时接收情况
- 开始或暂停监控：根据过滤条件开始监控或暂停监控
- 导出当前监控显示的内容：当暂停监控时，用户可以导出当前显示的日志内容，便于后续分析、挖掘或追溯异常安全事件日志。

4.6 报表管理

报表管理的作用为展示系统安全工作的结果。报表内容包含各种信息的统计情况，包括：告警报表、资产报表、安全事件报表、审计报表等。

用户可以定义相关条件以生成报表，它们均可以导出为 PDF、Word、Excel、HTML 等格式。

五、 基础功能

用户在使用日志审计系统前，应通过相关正规渠道获取许可证，再将许可证导入到系统后方可正常使用。

5.1 功能概述

在日志审计系统，Web 主要由采集管理、资产管理、事件分析、审计管理、报表管理、安全监控、拓扑管理、系统管理等子系统组成。

5.1.1 什么是日志

从各类设备或系统中产生、能代表其运行状态、配置状态及报警等数据，如用户登入/登出、系统启动/停止等。

一般日志均有不同的等级，例如 Syslog 就包含有 8 个等级，分别从 0 到 7，级别越高数值越小，另外，Syslog 中还包含有可以表示其日志产生模块或类型的 facility 属性，这在分析日志时也经常会被用到；而对于 Windows 的 EventLog 则是另外一种形式，其级别包括错误、警告、信息、成功审核或失败审核，其日志的类别包括系统、安全和应用类型。

5.1.2 日志是如何采集的

日志审计系统对各类日志的采集一般是通过如下几种方式：

1. Syslog：这是一种最为常见的形式，一般 Linux/Unix 主机、各类网络设备、安全设备等均支持将自身日志通过 Syslog 形式发送出来
2. SNMP Trap：这也是一种较为常见的形式，一般网络设备和部分安全类设备可以发送此类日志
3. 数据库：不是特别常见，有些防毒类产品、VPN 设备仅支持这种类型，它需要设置若干参数

方可获取，如数据库的类型、IP 地址、服务监听端口、实例名称、日志表名、序列字段等；日志分析系统是主动获取此类日志的

4. Socket：直接连接到相关的设备服务，设备通过双方约定的格式传递日志信息；OPSEC 也是一类特殊的 Socket 日志接入方式，目前仅针对 CheckPoint 防火墙

5. 文件：从外部的文件中逐行（有时候也支持将多行合并为一行）获取日志，它一般用于无法直接或实时获取设备、系统日志的场合（用户需将日志单独导出成文件，传送到综合日志分析系统指定的目录或自行设置的目录下）

6. SMB：这是一类基于文件共享（SAMBA）的日志接入方式

7. WMI：Windows 系统日志的主要接入方式

5.1.3 什么是安全事件

能表达或反映某种安全问题的日志或数据，包括攻击类、恶意代码类、异常行为、敏感行为类等。

5.1.4 标准化

鉴于各类设备或系统产生的日志、安全事件格式五花八门、形式不一而足，故在综合日志分析系统进行分析之前需要进行标准化，如下列不同设备的日志：

SUN Solaris

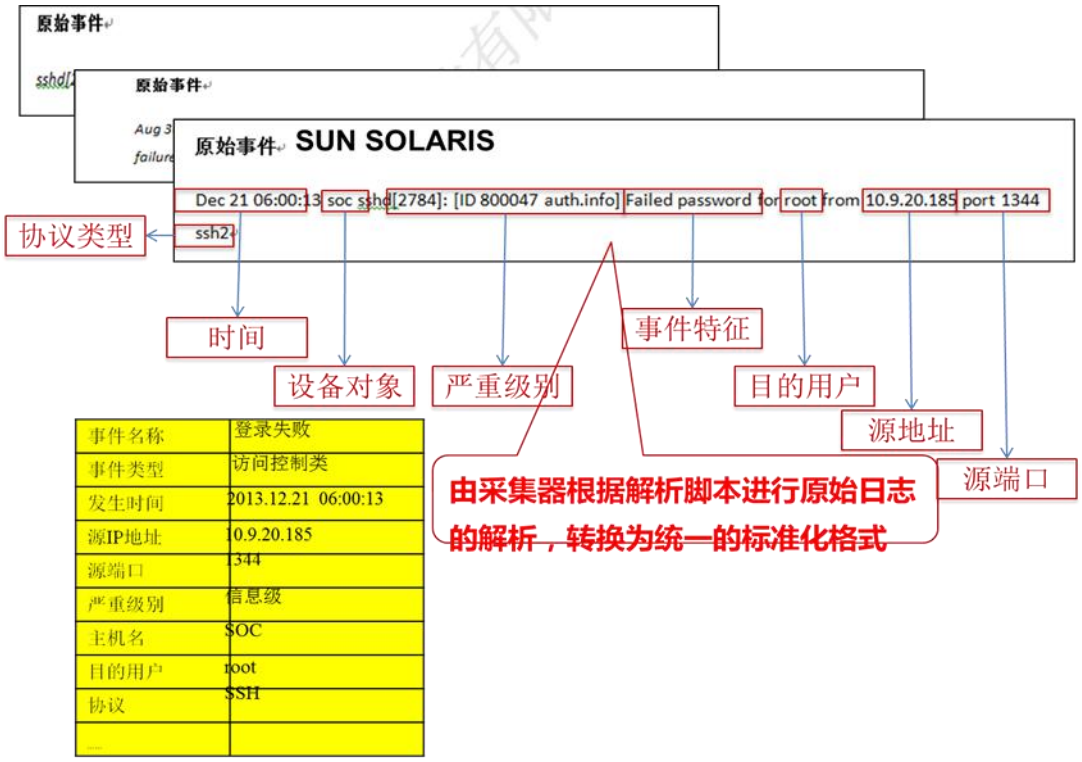
Aug 27 13:04:09 sshd[3228]: [ID 70112 auth.info] Failed password for root from 79.16.133.71 port 4489 ssh2

Cisco 路由器

4066: Aug 17 20:04:31.388: %SEC-6-IPACCESSLOGP: list ZJ_MPLSLINK_IN permitted tcp 129.9.11.247(9801) -> 10.34.14.200(1067), 203 packets

标准化的目的实际上就是将类似上述不同的日志进行规格化，然后存储为内部格式。例如，我们会将第一条日志的名称转换为“root 用户登录失败”，将源地址转换为“79.16.133.71”；而第二条的名称则会转换为“连接”，源地址、源端口、目的地址和目的端口分别转换为“129.9.11.247”、“9801”、“10.34.14.200”和“1067”。

下图为一个日志标准化的示例：



至于，如何编写标准化脚本，则会在“日志审计系统产品用户手册（事件标准化脚本语法和接入指南）”文档中进行详细介绍，本文不再涉及。

5.1.5 什么是过滤和归并

有时，为了使用户集中查看他所需要关注的相关日志或事件，或者有时我们并不需要保存所有的原始日志或事件，那么我们可以设置一个或多个过滤或归并策略。

其中，过滤与归并策略的不同点在于，过滤策略既可以丢弃被过滤的原始日志或事件，也可以保留这些原始日志或事件，而如命中归并规则，则采集器将根据规则归并一个到多个字段。

在后面的操作中可以看出，过滤或归并策略是应用在采集器上的，而且一个采集器可以包含多个过滤策略。

5.2 采集管理

采集管理是使用日志分析系统的第一步，用户通过指定需要采集的目标、相关采集参数（Syslog、SNMP Trap 等被动方式无需指定）、相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。采集器管理模块包括采集策略管理和采集器管理。

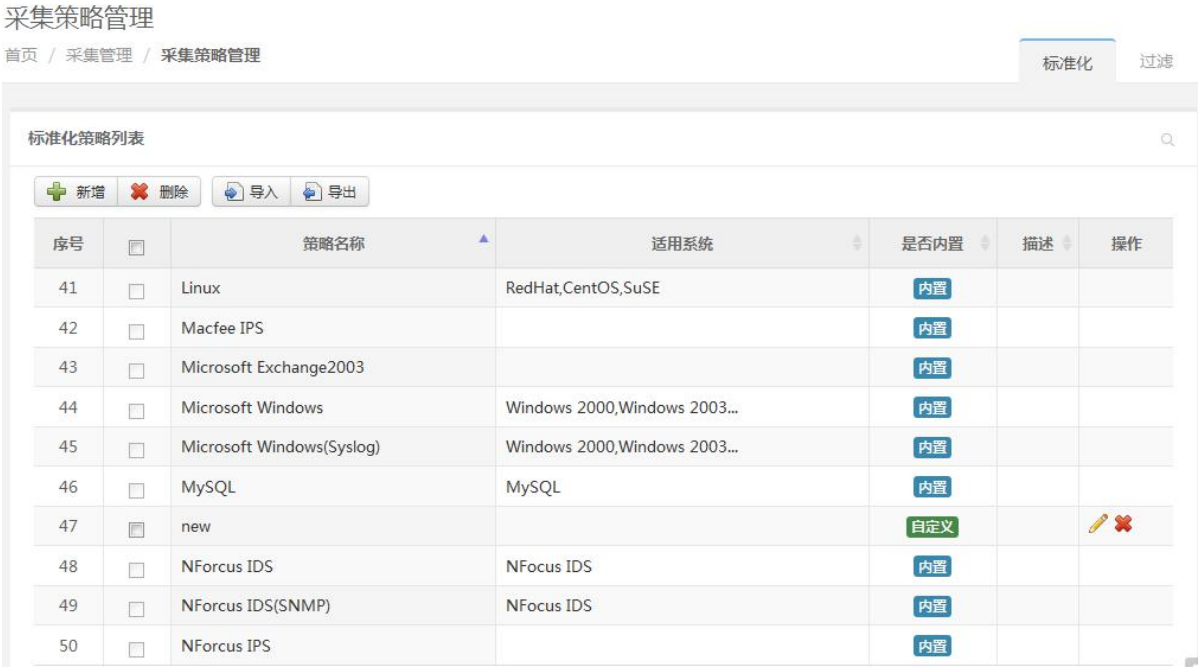
5.2.1 相关操作

5.2.1.1 标准化策略

标准化策略功能包括如下内容：

1. 查看标准化策略列表：系统内置了一些标准化策略，内置标准化策略是不允许修改和删除的，且内容是

加密的。如下图所示：

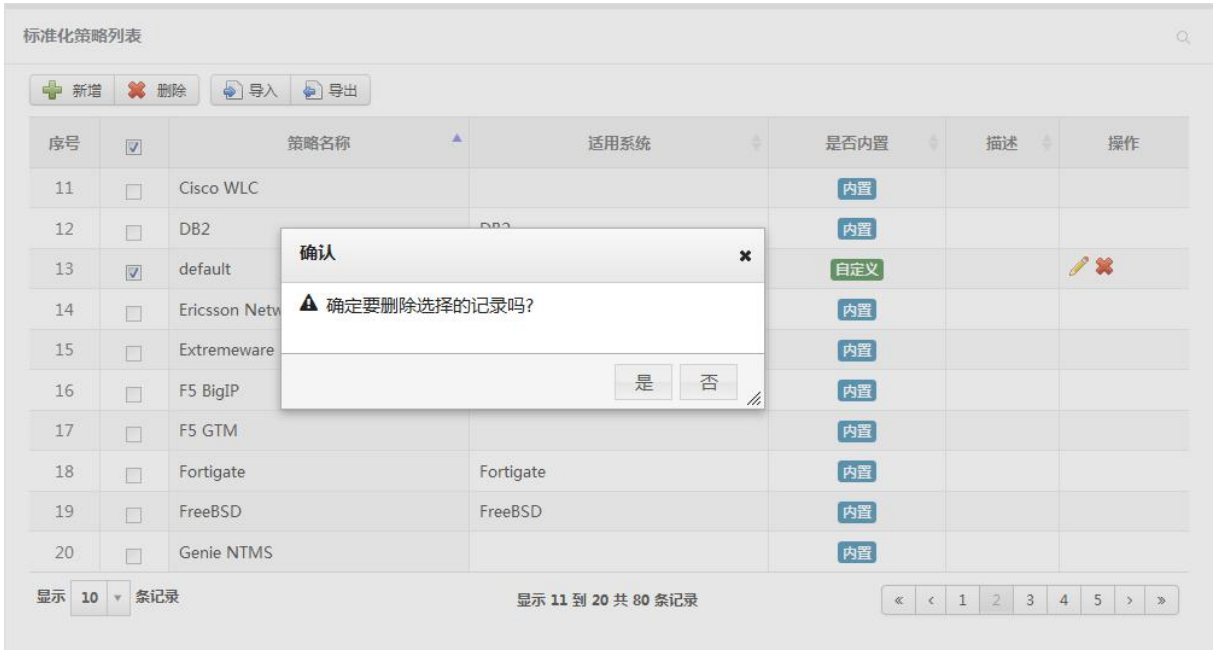


2. 新增标准化策略：点击新增，输入策略名称、使用系统（可填）、标准化策略（录入的标准化策略必须是 UTF-8 格式，而不要使用 GB 系列的编码，否则会出现乱码）、描述（可填）；点击保存。如下图所示：

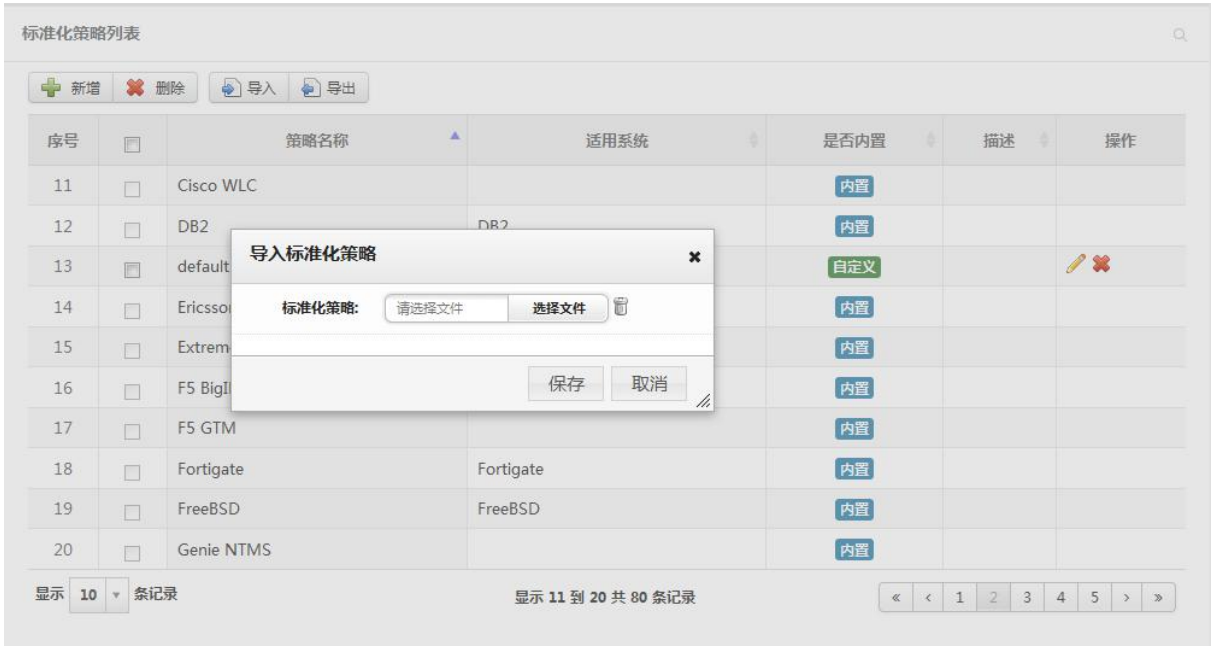
3. 修改标准化策略：修改标准化策略相关属性，点击保存。内置标准化策略是不允许修改的，只允许修改自定义的标准化策略。如下图所示：

4. 删除标准化策略：删除用户选定的一个或多个标准化策略；内置标准化策略是不允许删除的，只允许删

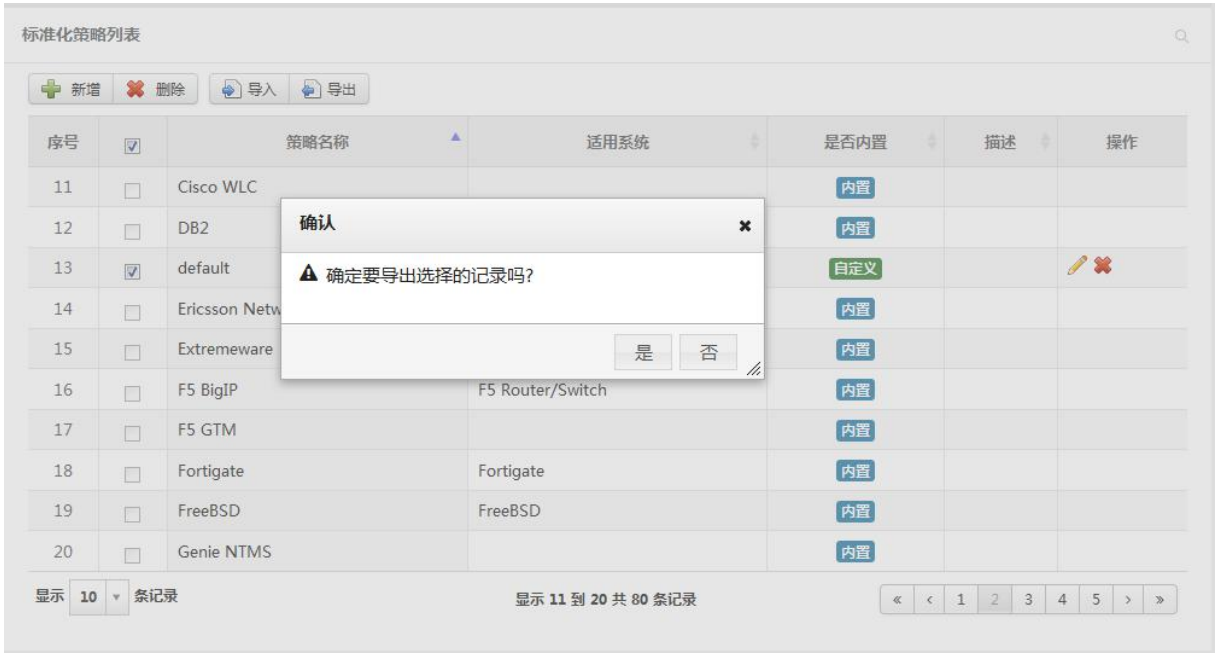
除自定义的标准化策略。如下图所示：



5. 导入标准化策略：根据系统约定格式从外部文件导入标准化策略。如下图所示：



6. 导出标准化策略：用户选择一个或多个需要导出的标准化策略，点击导出按钮。内置策略不支持导出，只允许导出自定义标准化策略。如下图所示：

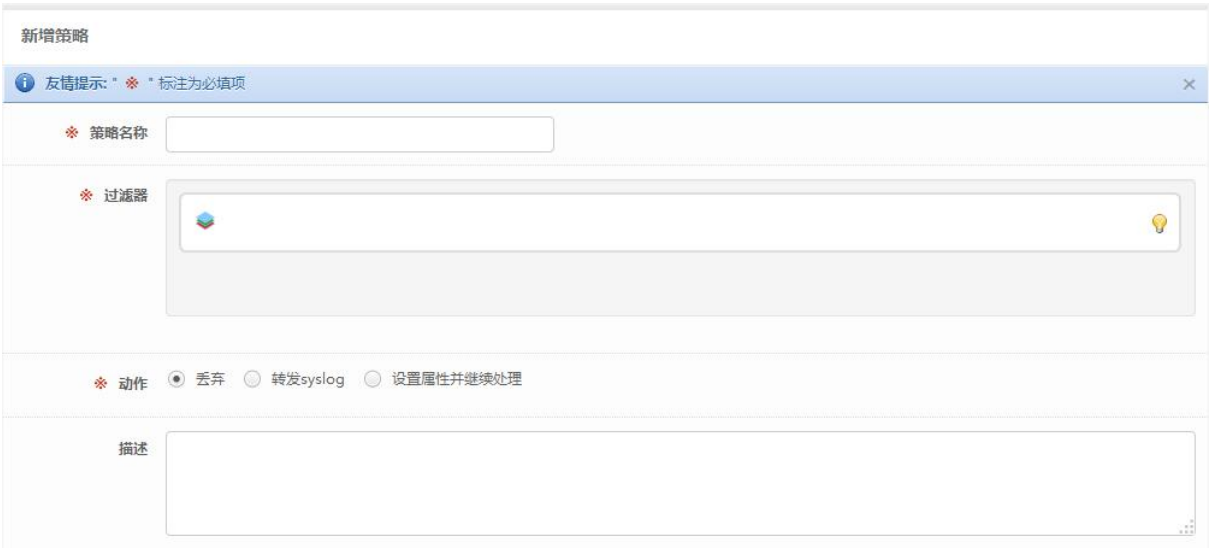


5.2.1.2 事件过滤策略

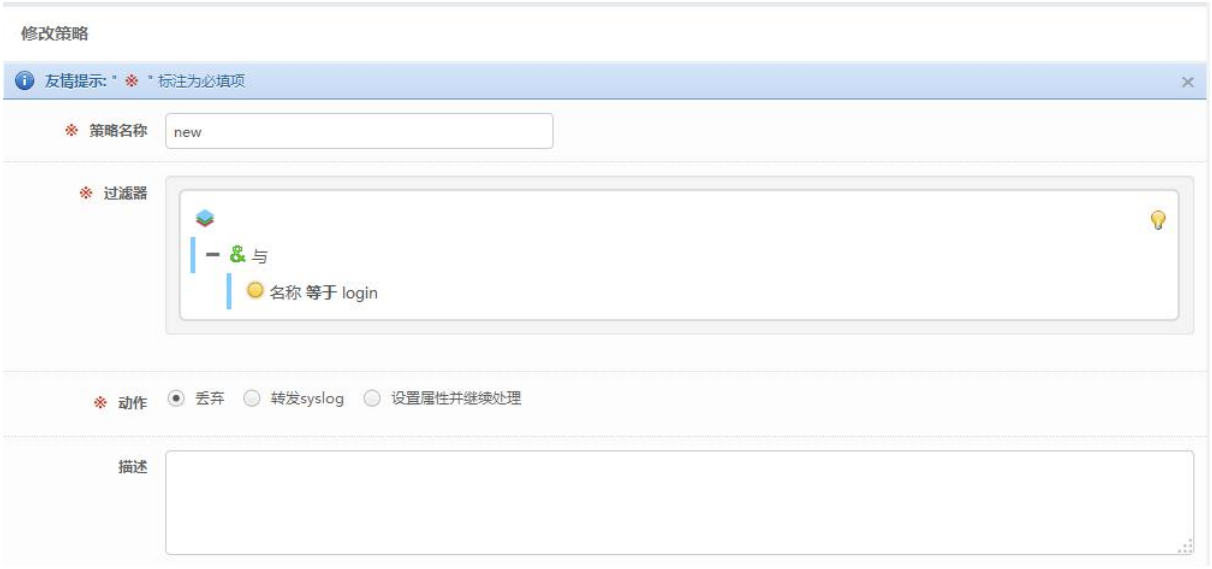
1. 查看事件过滤策略列表：如下图所示：

2. 新增事件过滤策略：点击新增，输入策略名称、过滤器、动作、描述（可填）；点击保存。
事件过滤策略支持以下动作：
   - 丢弃
   - 转发 syslog：可以将命中事件通过 Syslog 方式（系统管理中定义的 Syslog 服务器或者直接指定 1 到 2 个 Syslog 服务器地址）转发到外部系统。
   - 设置属性并继续处理：修改命中过滤器事件的属性。

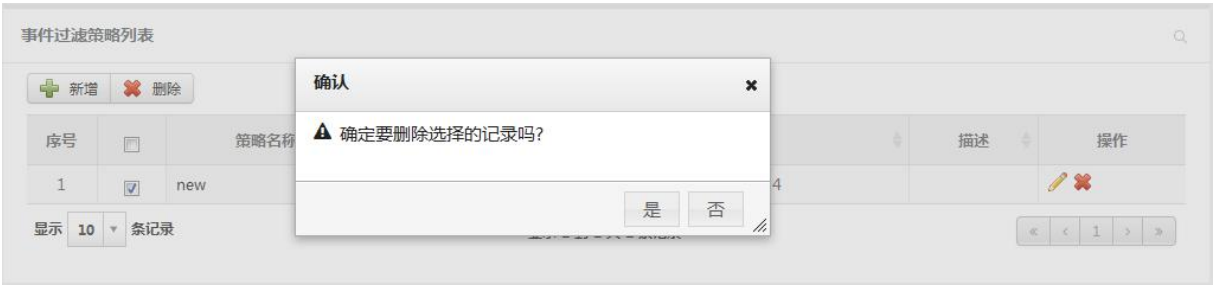
   如下图所示：



3. 修改事件过滤策略：修改事件过滤策略相关属性，点击保存。如下图所示：

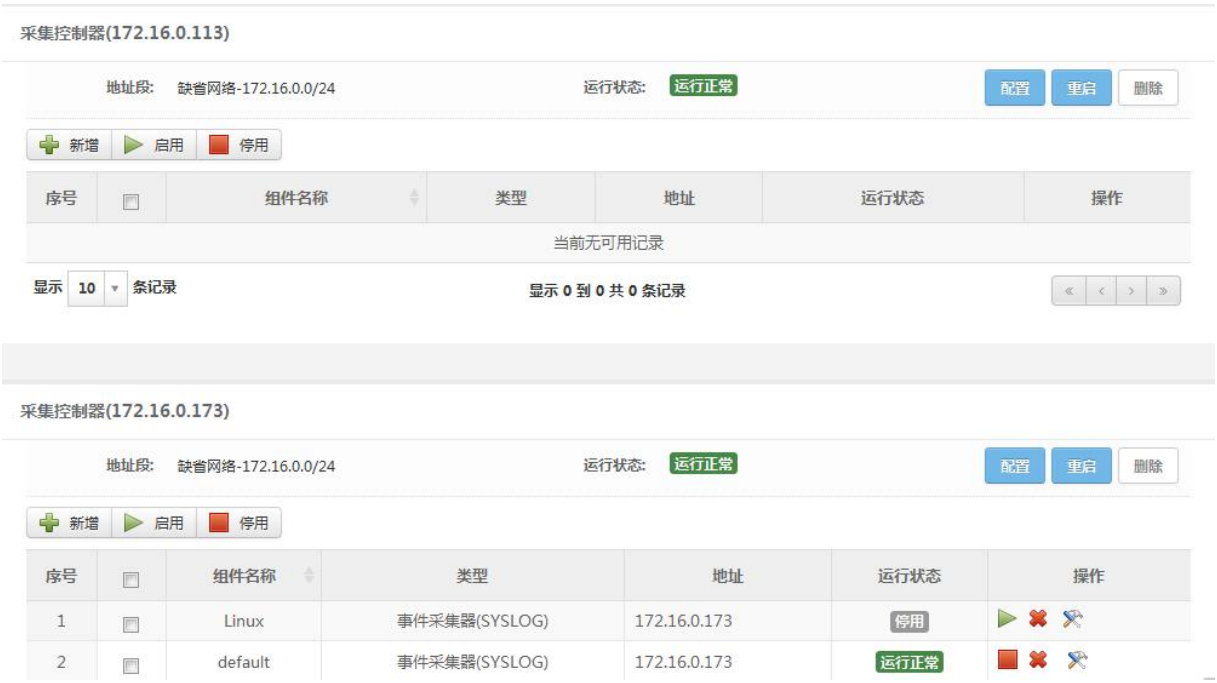


4. 删除事件过滤策略：用户选定的一个或多个需要删除的事件过滤策略，点击删除，如果事件过滤策略正在被采集器使用则无法删除。如下图所示：



5.2.1.3 采集器管理

1. 查看采集控制器列表：系统支持多个采集控制器，每个采集控制器允许存在多个组件。如下图所示：

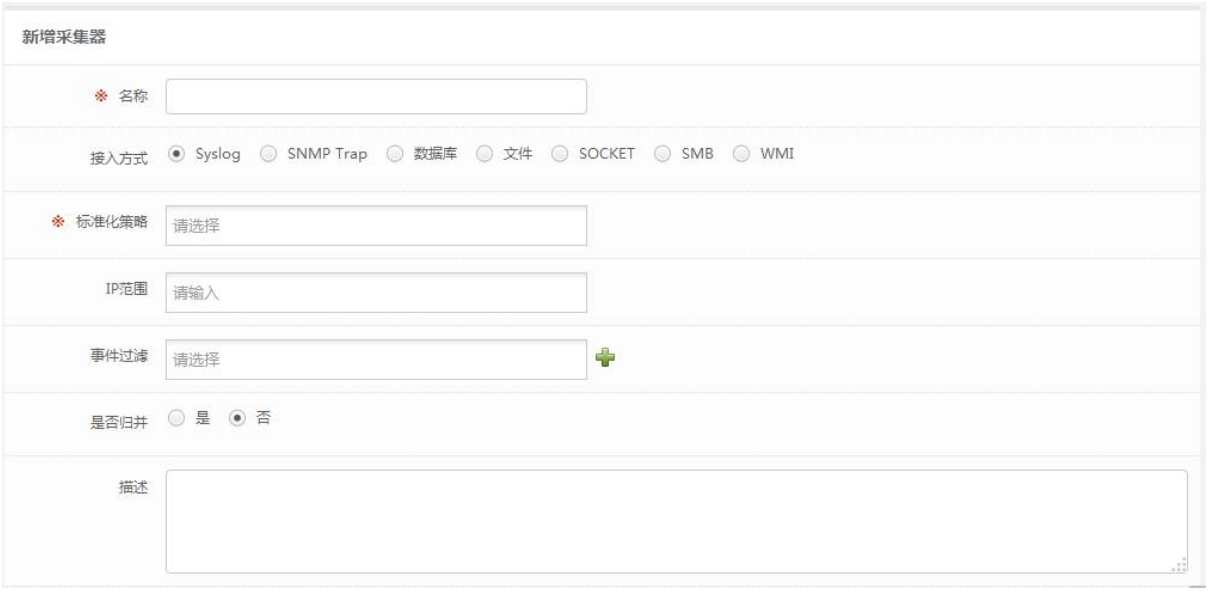


2. 配置采集控制器：点击配置，修改采集控制器名称、地址段；点击保存。如下图所示：

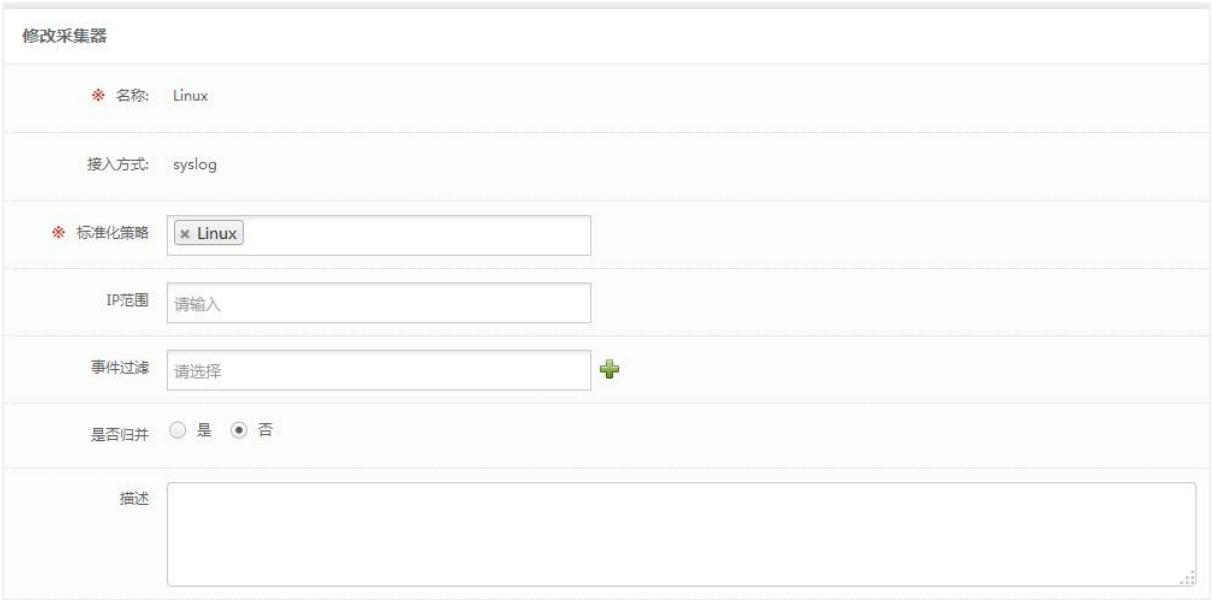
3. 重启采集控制器：点击重启，可以重新启动采集控制器。如下图所示：

4. 删除采集控制器：点击删除，可以删除采集控制器，采集控制器删除后只能通过后台脚本重新启动进程触发注册。如下图所示：

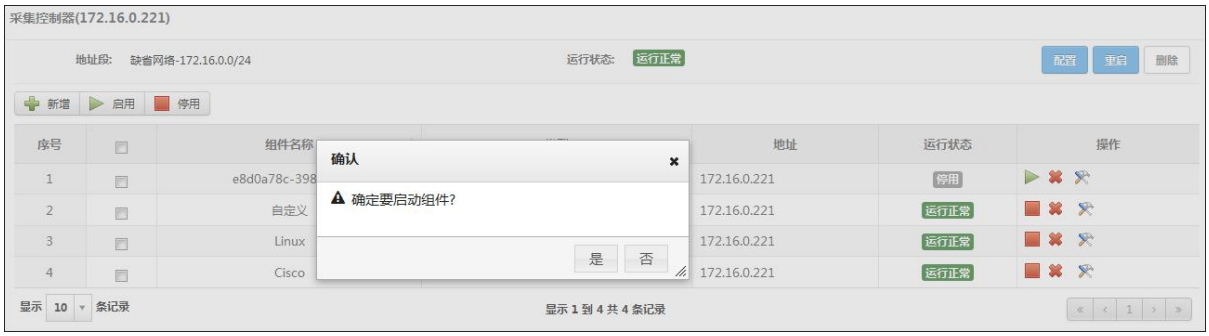
5. 新增采集器：点击新增，输入名称、接入方式、标准化策略、IP 范围（可填）、事件过滤（可填）、是否归并、描述（可填）；系统支持在指定 IP 范围的情况下可选择相同的标准化策略，不指定 IP 范围的话是不允许的，点击保存。如下图所示：



6. 配置采集器：点击操作列下面的配置图标，修改采集器相关属性，点击保存。如下图所示：



7. 启用采集器：点击操作列或列表上面的启用图标，点击确认。如下图所示：



8. 停用采集器：点击操作列或列表上面的停用图标，点击确认。如下图所示：

9. 删除采集器：删除用户选定的采集器。如下图所示：

5.3 资产管理

5.3.1 什么是安全资产

安全资产是日志审计系统的核心管理对象。与 ISO27001 的关于资产的定义略有不同，东软网络安全管理中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务或应用。

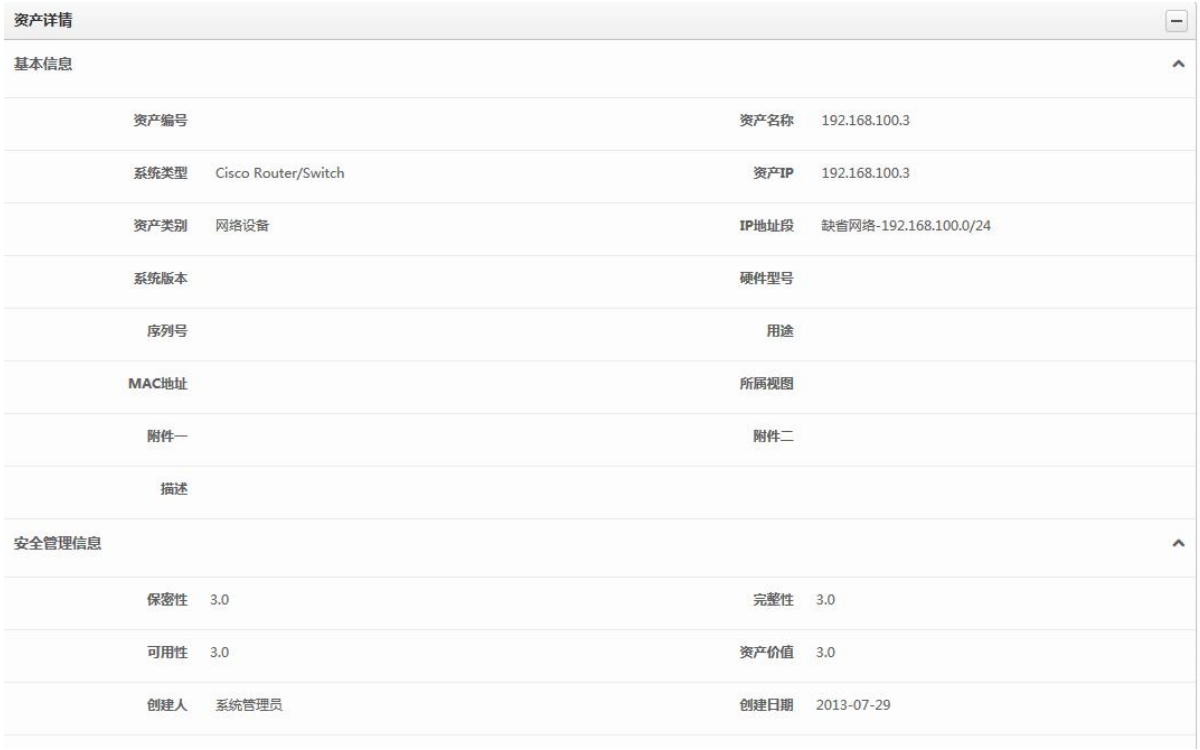
5.3.2 安全资产的属性

一般而言，安全管理中的资产具备如下两类属性：

1. 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 和 IPv6 格式）、责任人（出现安全问题应由何人处理）、上架信息等；

2. 安全属性：完整性、可用性、保密性、风险信息、告警、安全事件等。

如下图所示：



为了提供一定的扩展性和灵活性，系统支持用户定义多个自定义属性，属性的类型包括数值型、日期型、字符型等。

如前所述，日志审计系统的资产管理支持用户录入、导入或自动发现资产。

5.3.3 什么是网络

与普通定义的网络不同，日志审计系统的网络是为了处理不同网络（初始安装后系统存在一个所谓的默认网络）的资产同 IP 问题；网络中包括若干网段。

日志审计系统支持对于网络和 IP 地址段的管理；网段可以通过手工录入或自动发现获得；系统发现的新资产也可在此功能模块中列出，用户可以将它们纳入或归并到已存在的资产中。

5.3.4 什么是资产视图

为了便于用户集中、灵活地管理所辖范围内的资产，日志审计系统支持用户自定义资产管理视图；所谓资产视图就是用户对于资产的组织形式。

5.3.5 相关操作

5.3.5.1 资产管理

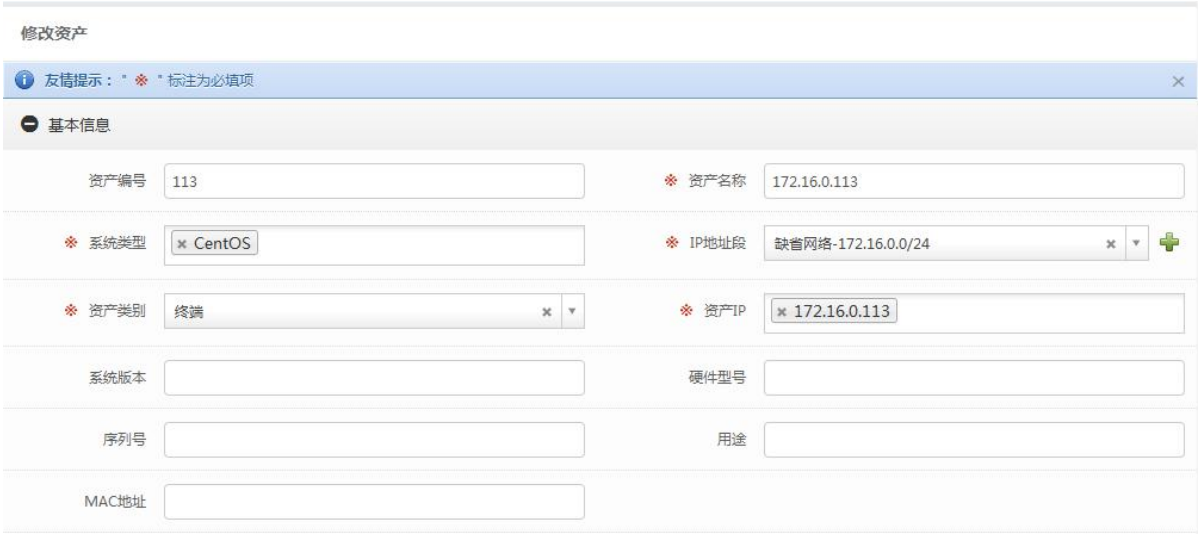
资产管理功能包括如下内容：

1. 资产查看：用户根据各自权限（含角色中的授权以及资产创建人）查看资产列表，列表查看

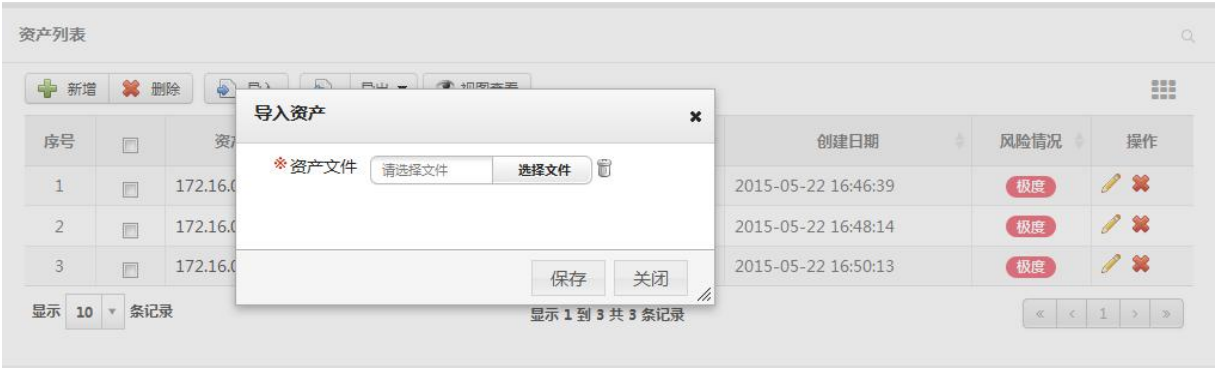
时可以依据选中的视图（和用户个人相关），也可不选择任何视图查看；用户点击某资产链接可查看资产详情，如下图所示：

2. 资产查询：在资产列表中输入相关字段的查询条件（可查询字段参看属性列表），点击查询；查询结果可导出成报告；报告可以另存为 PDF、Word、Excel 和 csv 格式，如下图所示：

3. 资产维护：资产的增加、修改和删除操作；在新增资产时系统可自动将资产的 IP 地址添加到网络中（导入资产类似），如下图所示：



4. 导入资产：根据系统约定格式从外部文件导入资产，如下图所示：



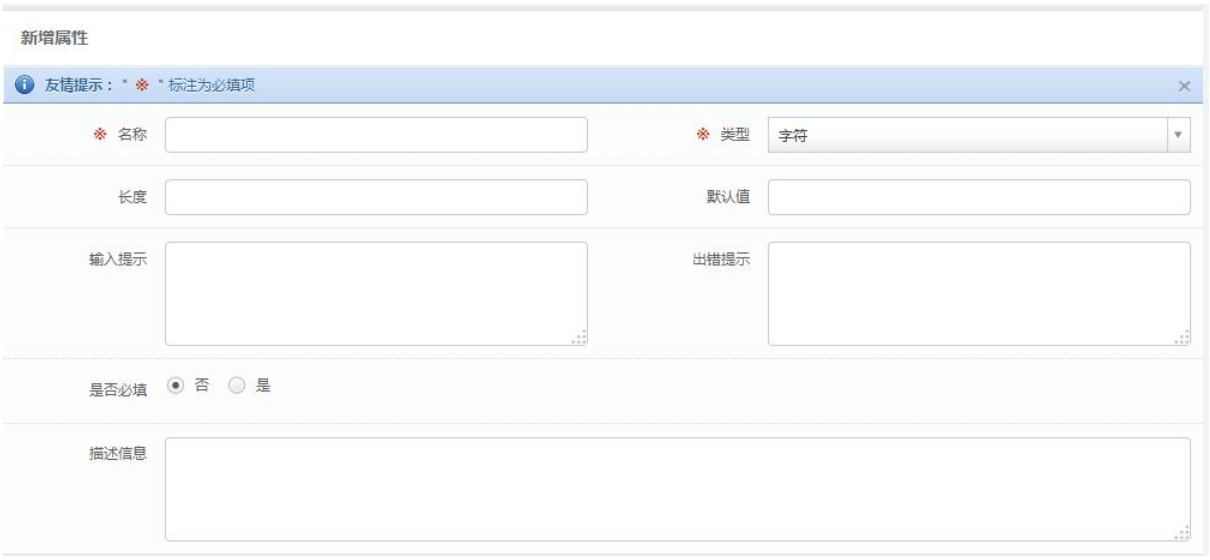
5. 导出资产：根据用户需要，将所选择的或全部资产导出到外部文件，如下图所示：

5.3.5.2 资产自定义属性

资产自定义属性支持：文本、数值（包括整型、浮点型）、日期等类型；可设置字段名称、长度、输入提示（可选）、出错提示。

用户可以定义、修改和删除自定义属性。

界面如下图所示：



5.3.5.3 资产视图管理

资产视图是用户对于所管理资产的组织形式，系统可以使用地理位置、安全域、系统类型等创建资产视图，用户也可以定义其它相关视图并关联资产 。

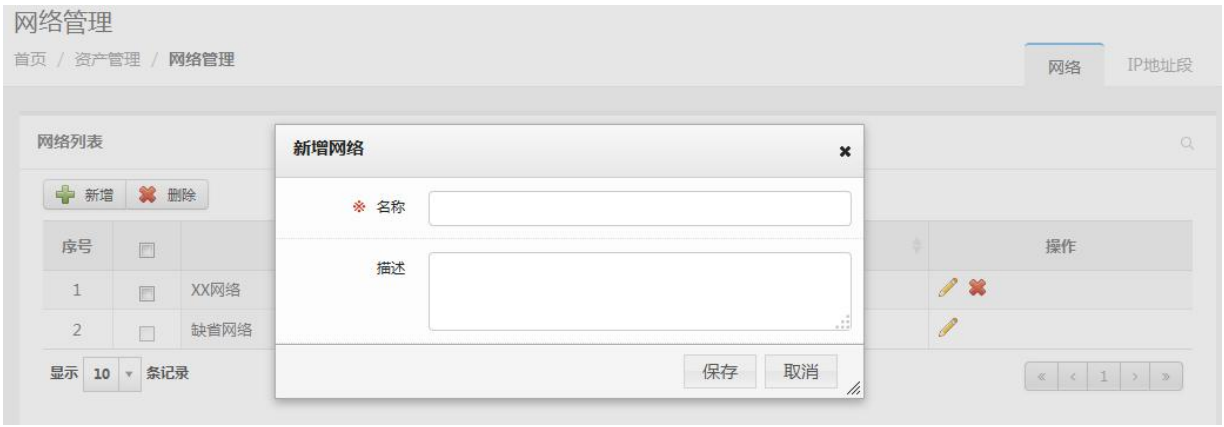
界面如下图所示：

5.3.5.4 网络管理

网络管理：为解决不同局域网中存在相同 IP 地址，以定义不同网络；系统在事件采集、扫描、安全基线检查等会使用此属性；默认可以不增加网络。

网段管理：对网段进行维护，系统仅支持 IP 地址和前缀码形式；系统支持 IPv6 形式的地址段。

界面如下图所示：



5.3.5.5 资产发现管理

资产发现的目的除了发现网络中存活的真实设备，还能尽量地发现其运行操作系统的类型、版本。资产发现的结果不直接添加到资产中，需过滤已经存在资产。

在定义资产发现任务时，用户可以给出需发现的 IP 地址段或系统可以采集器安装的情况进行自动发现；资产发现功能不支持 IPv6 设备的发现。

用户可以将系统发现的 IP 设备加入为资产或者删除，若发现的 IP 设备被删除，再次进行资产发现时此 IP 设备将不会再被发现。

界面如下图所示：

注意：如果系统内部署多个采集控制器，则既可以全部进行发现，也可以选择其中几个进行。

5.4 事件分析

5.4.1 安全事件的关联

为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了关联功能，该功能的具体使用方法见下。

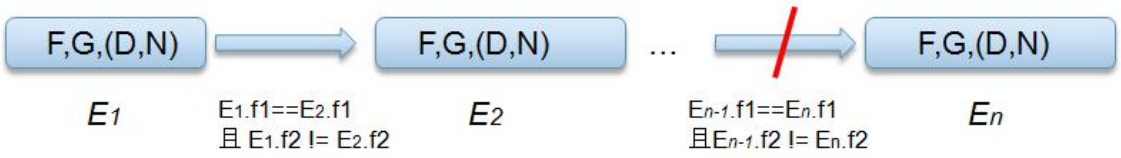
关联的类型包括基于规则的和基于统计的。

基于规则

基于规则的关联条件是一个状态机，它包括若干个状态及关联运算符，且每两个状态之间均有一个关联运算符（即它是一个二元算子）；但与一般的关系运算不同的是，它有两种属性：

1. 时序：后续发生或后续不发生
2. 关联过滤条件：可选；前后状态之间的关联关系定义

其形式类似下图：



其中，F,G,(D,N)为一状态，F 表示过滤器，G 表示分组字段（支持多个），而 D 表示持续时间（以秒为单位，必须设置），而 N 为重复次数（可不设）。

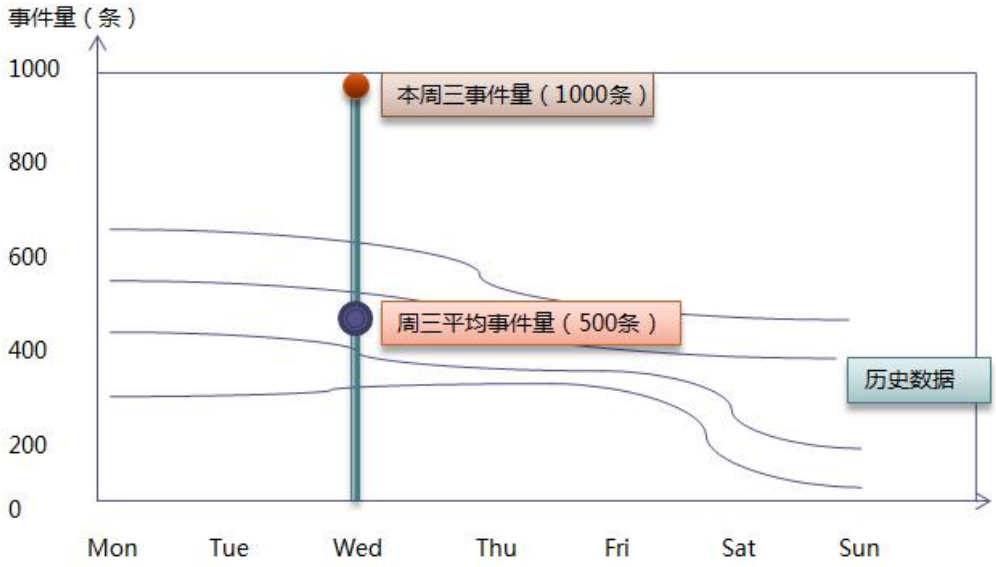
需要注意如下几点约束：

1. 关联过滤条件不是必须的，但如果设置，则其左操作数和右操作数分别为相邻事件集的事件属性（属性类型必须相同），不能为常量且必须加入到各自状态的分组条件中（系统应提示并自动添加），例如：*E1[事件名称==”登录失败”,”源地址”,(60,3)] 后续发生[E1.源地址==E2.源地址] E2[事件名称==”登录成功”,”源地址”,(60,1)]* 为合法，而
   *E1[事件名称==”登录失败”,”源地址”,(60,3)] 后续发生[E1.源地址==E2.源地址 且 E1.目标地址==E2.目标地址] E2[事件名称==”登录成功”,”源地址”,(60,1)]*为非法，因为它没有将目标地址加入到分组条件中
2. 对于关联条件中的过滤条件，其关系运算仅支持等于和不等于
3. 如果关联条件中的时序类型为后续不发生，则它必须是整个状态序列的最后一个（如上图所示），否则错误

基于统计

基于统计的关联需要有基线数据；基线类型包括日基线和周基线；其中日基线包含最近若干天，每个时段（以小时为单位）的基于指定聚合字段的统计数据，而周基线包括最近若干周每周几的基于指定聚合字段的统计数据。

下图周基线为例（假定学习了最近 4 周的数据），而过去一天为周三，则：



从上图可以看出，过去最近四周，周三的平均事件量为 500 条，而刚过去的一日为 1000 条，与基线相比，超出了 100%，如触发条件设定为 100，则触发响应。

响应的类型包括如产生告警、转发外部系统和执行程序。

5.4.2 相关操作

5.4.2.1 事件列表

1. 设备事件量排名列表：系统支持按照设备类型视图对事件进行查看，可通过选择日期查看某一天的事件，也可通过点击 IP 地址、事件级别跳转到查询页面查看事件列表。如下图所示：

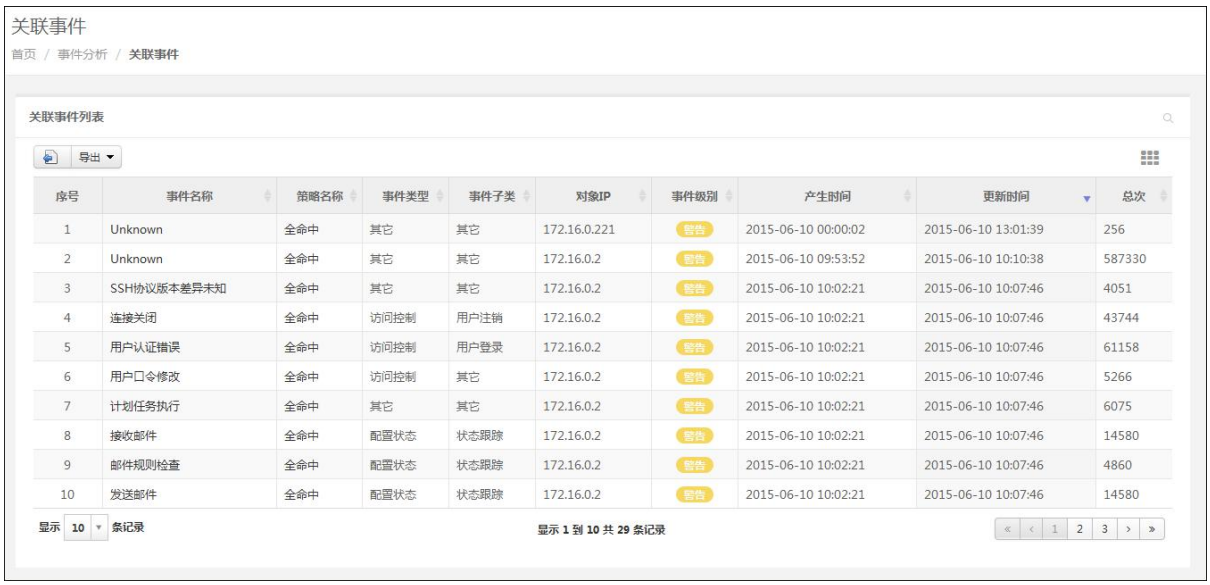
2. 事件列表：在事件列表中输入相关字段的查询条件（系统支持普通模式和专家模式两种查询模式，查询条件中必须包含事件时间属性），点击查询按钮；默认为查询当日事件，用户可以选择查询某个时间段的事件，若用户选择的时间段跨周，系统将按自然周以页签形式显示。如下图所示：

3. 事件详情：点击事件名称可查看事件详情。如下图所示：

4. 事件导出：系统支持导出查询出的事件，导出的格式为 xls，如遇有事件中含有逗号，则将其转义。如下图所示：

5.4.2.2 关联事件

1. 关联事件列表：关联事件列表显示通过关联策略产生的事件。如下图所示：

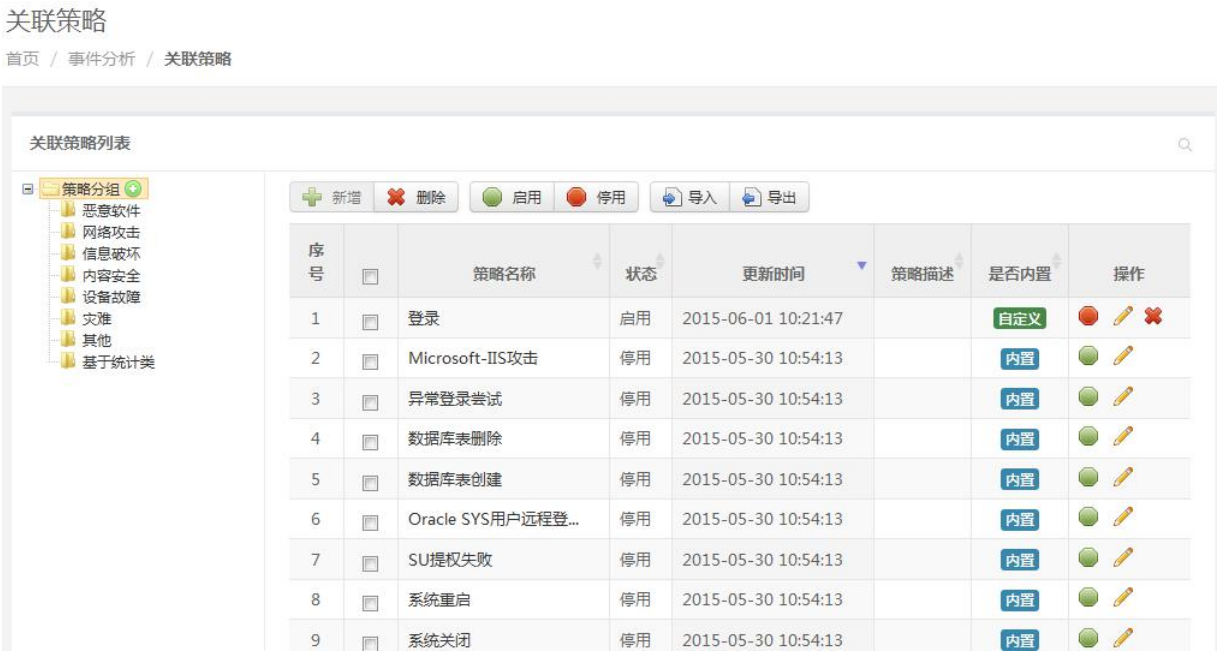


2. 关联事件详情：点击事件名称，显示关联事件详情（包括原始事件列表），在详情页面中可通过点击事件列表下的事件名称可查看原始事件详情。如下图所示：

3. 事件导出：系统支持导出通过查询条件查询出的事件，导出格式支持 PDF、Excel、Word、CSV 四种格式。如下图所示：

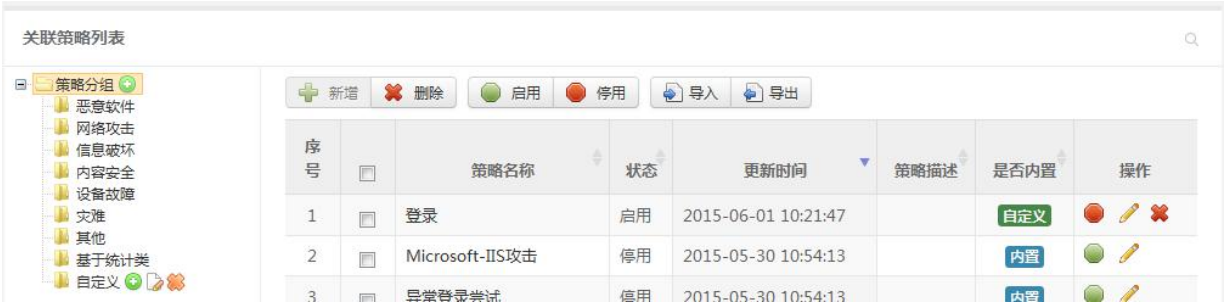
5.4.2.3 关联策略

1. 关联策略列表：系统支持按照策略分组维度查看关联策略，策略分组是可管理的。系统内置了一些关联策略，内置关联策略允许修改，但不允许删除。如下图所示：



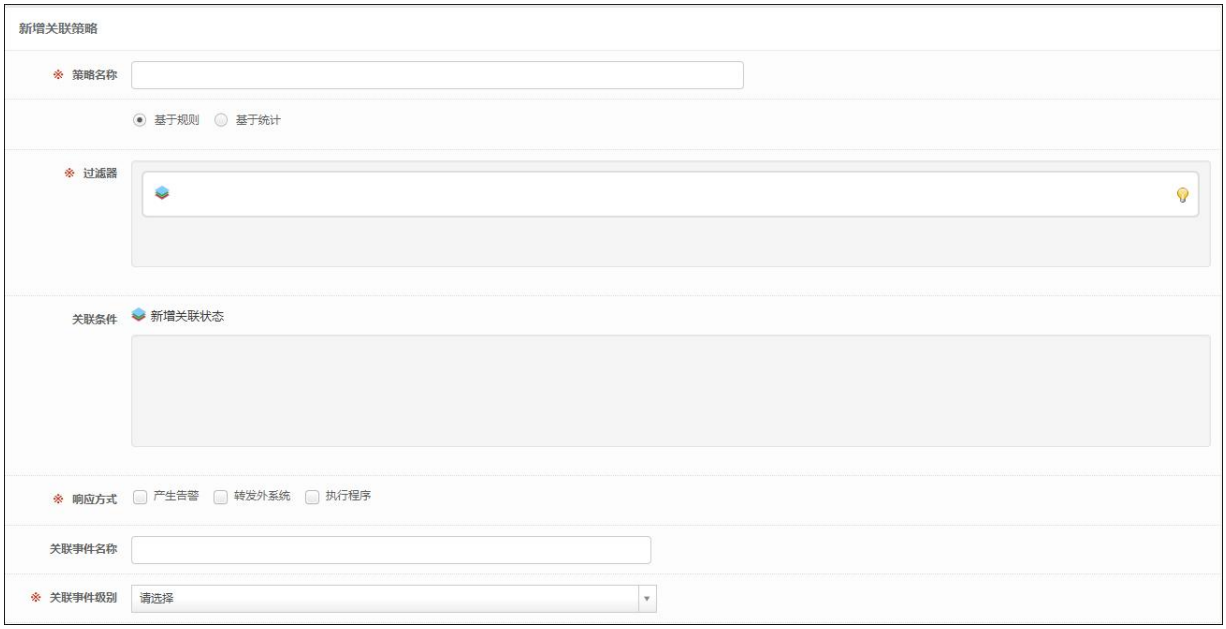
2. 关联策略详情：通过点击策略名称可查看策略详情：

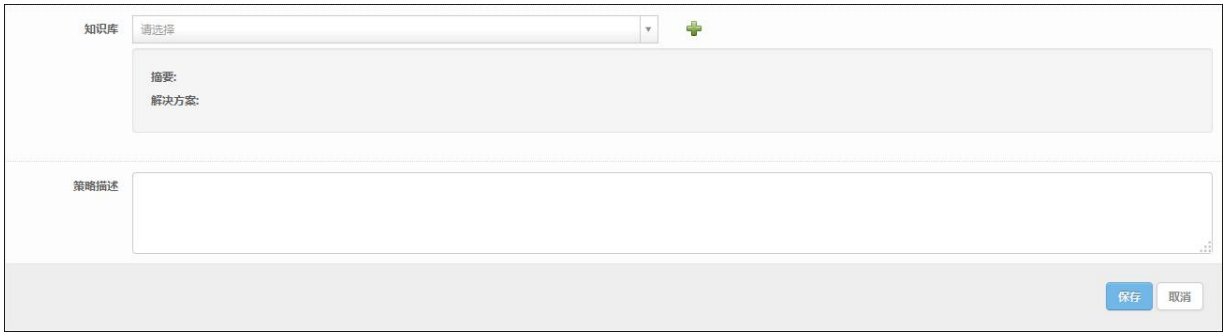
3. 策略分组管理：可以对自定义的策略分组进行增删改操作，内置策略分组不允许进行编辑操作。如下图所示：



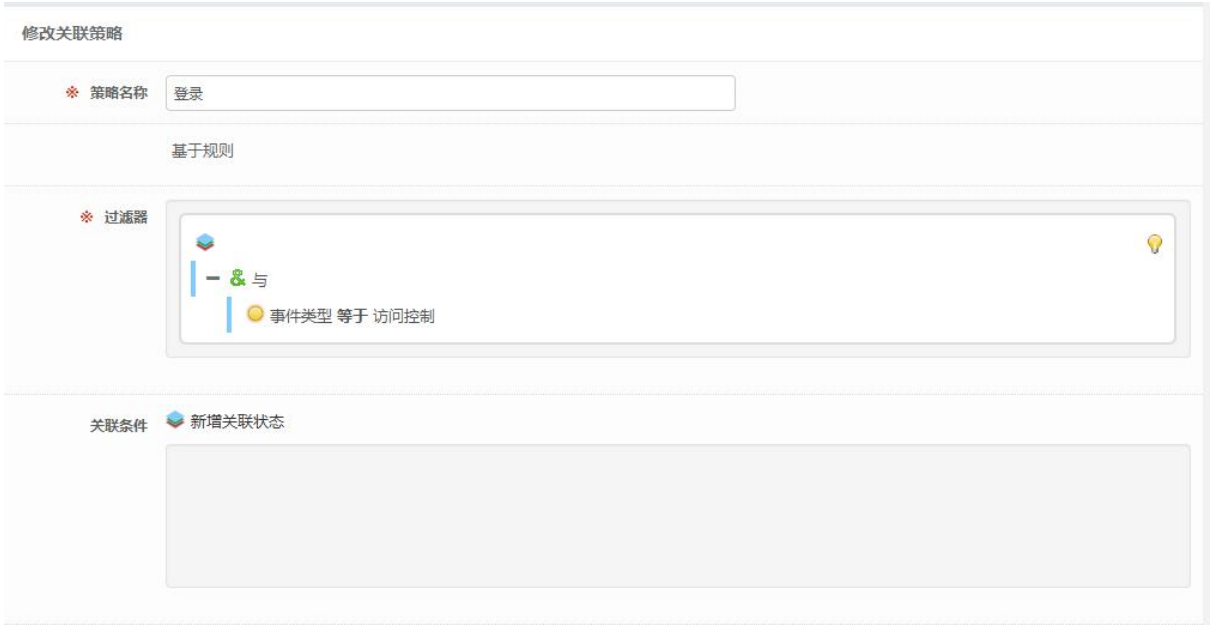
4. 新增关联策略：选择策略分组，点击列表上方的新增按钮，用户填写策略名称、过滤器、关联条件（选

填)、响应方式、关联事件名称（选填，如果为空，则使用原始事件名称)、关联事件级别、知识库（选填)、策略描述（选填)，点击保存。如下图所示：

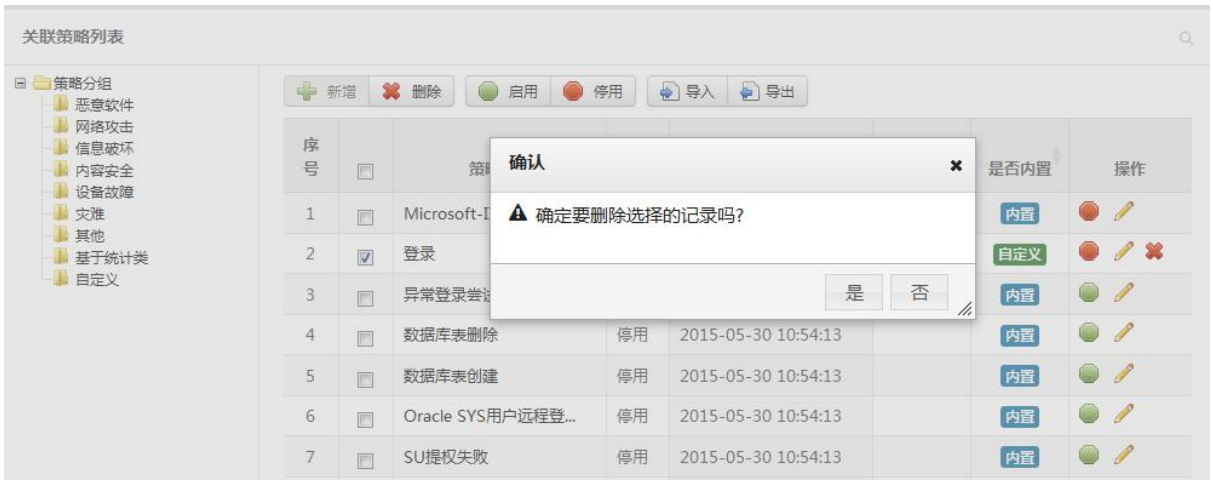




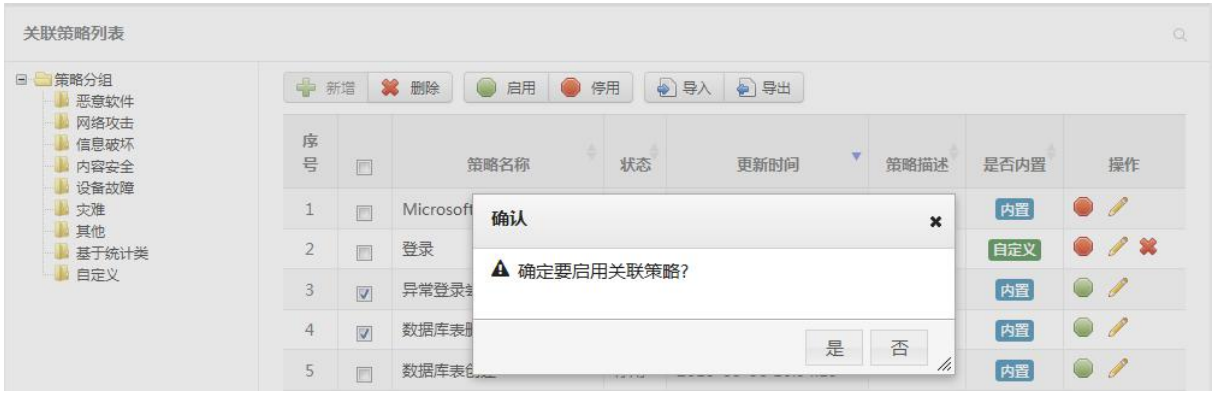
5. 修改关联策略：修改关联策略相关属性，点击保存。如下图所示：



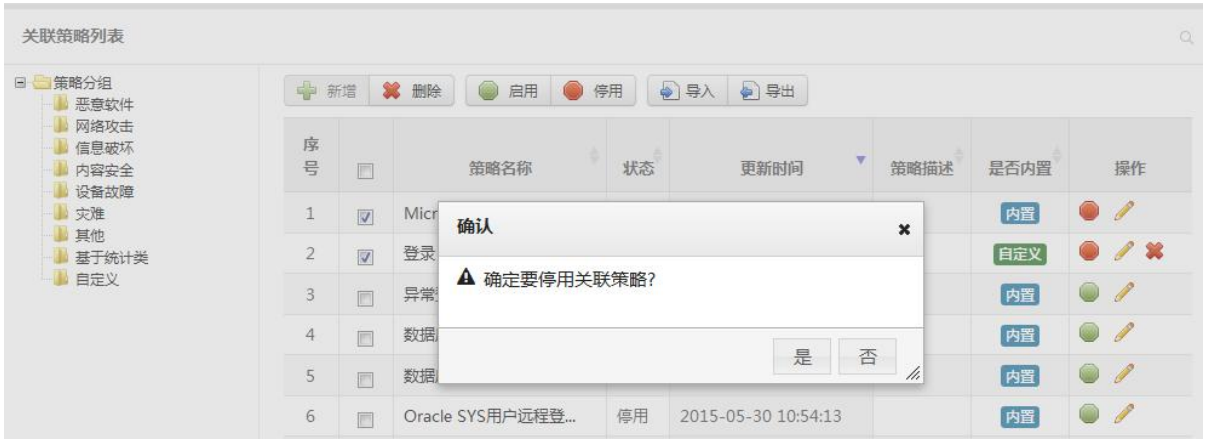
6. 删除关联策略：选择一个或多个要删除的关联策略，点击删除按钮，内置策略不允许删除。如下图所示：



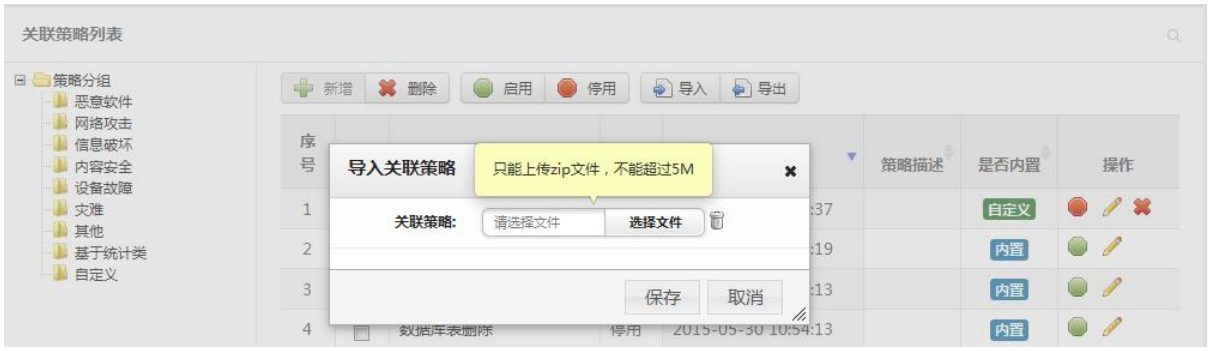
7. 启用关联策略：选择一个或多个要启用的关联策略，点击启用按钮，只有停用状态的关联策略才允许被启用。如下图所示：



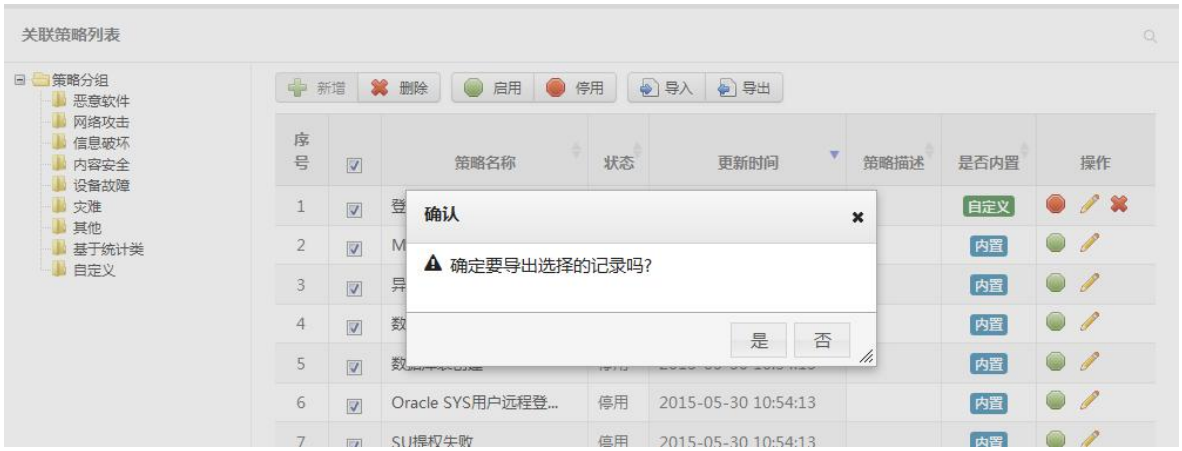
8. 停用关联策略：选择一个或多个要停用的关联策略，点击停用按钮，只有启用状态的关联策略才允许被停用。如下图所示：



9. 导入关联策略：点击导入，可通过导入功能批量将关联策略导入进系统中，文件格式必须满足系统要求。如下图所示：



10. 导出关联策略：选择要导出的多个安全策略，点击导出按钮，可将选中的策略导出成文件。如下图所示：



5.5 审计管理

5.5.1 什么是审计

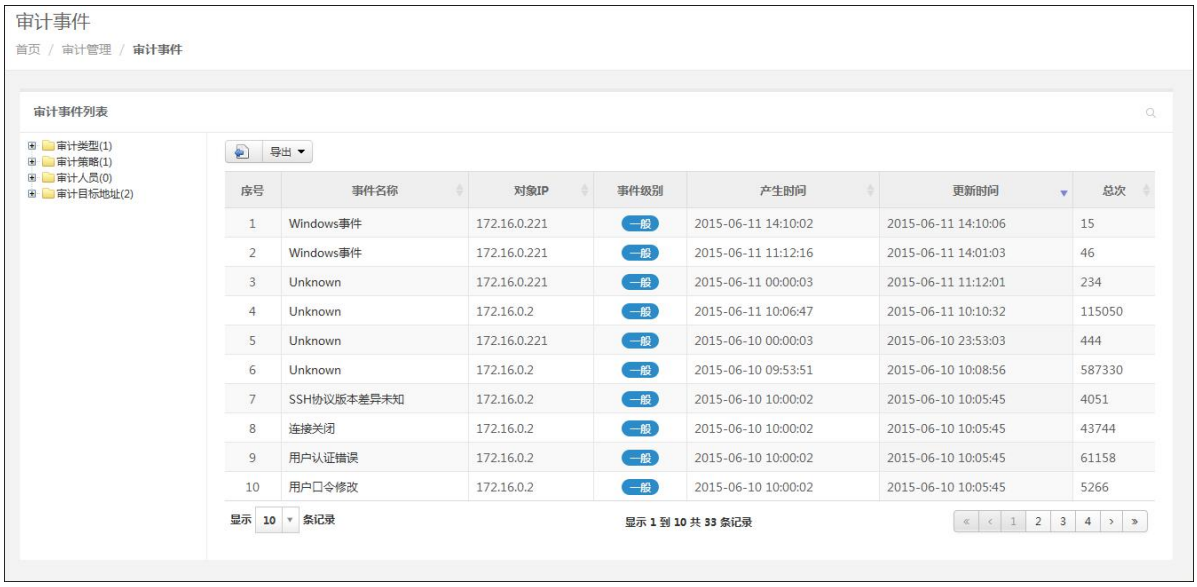
日志审计平台通过集中采集信息系统中的系统安全事件、用户访问记录、系统运行日志、系统运行状态等各类信息，经过标准化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统日志的全面审计。

通过日志分析系统，企业管理员随时了解整个 IT 系统的运行情况，及时发现系统异常事件；另一方面，通过事后分析和丰富的报表系统，管理员可以方便高效地对信息系统进行有针对性的安全审计。遇到特殊安全事件和系统故障，日志分析系统可以帮助管理员进行故障快速定位，并提供客观依据进行追查和恢复。

5.5.2 相关操作

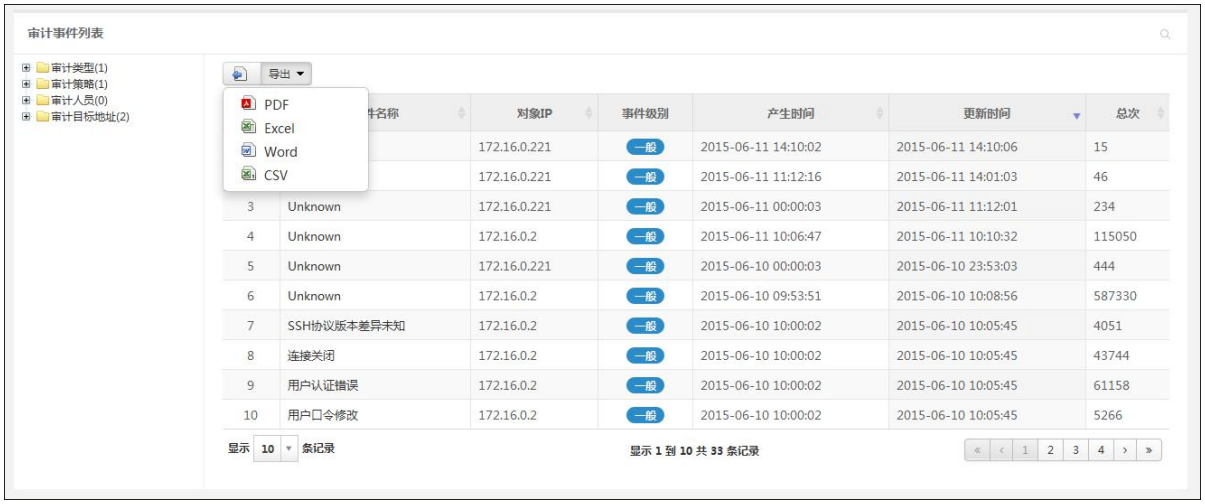
5.5.2.1 审计事件

1. 审计事件列表：审计事件列表显示通过审计策略产生的事件，可通过审计类型、审计策略、审计人员、审计目标地址四个维度查看审计事件。如下图所示：



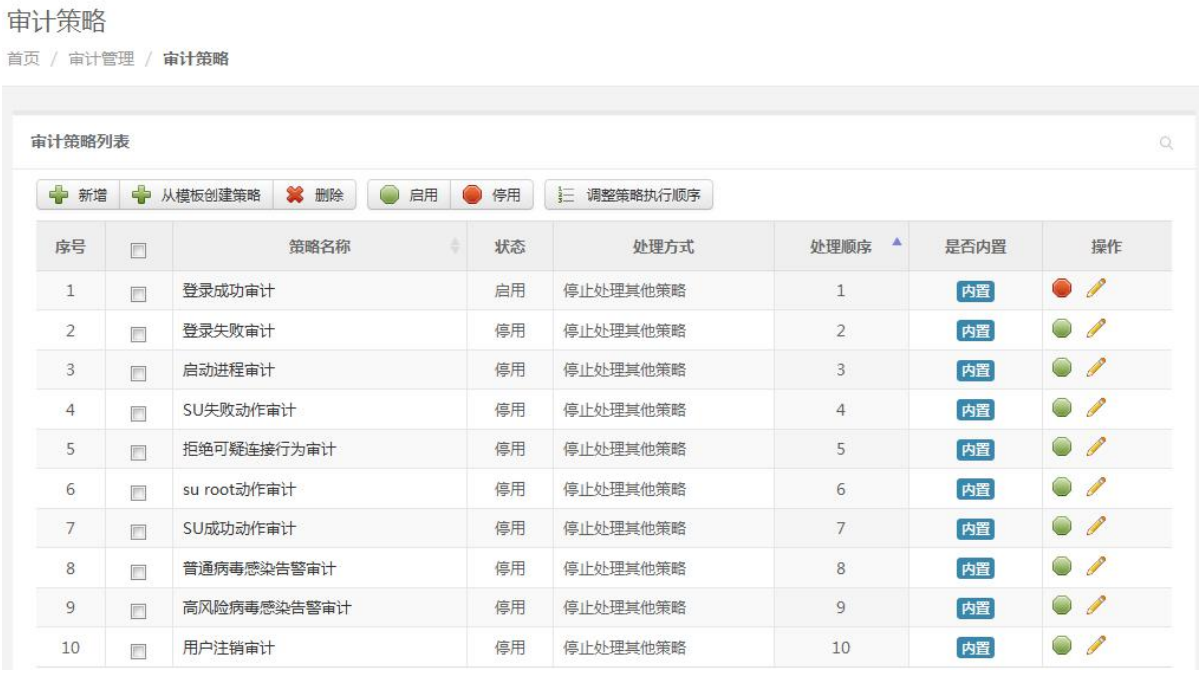
2. 审计事件详情：点击事件名称，显示审计事件详情（包括原始事件列表），在详情页面中可通过点击事件列表下的事件名称可查看原始事件详情。如下图所示：

3. 事件导出：系统支持导出通过查询条件查询出的事件，导出格式支持 PDF、Excel、Word、CSV 四种格式。如下图所示：

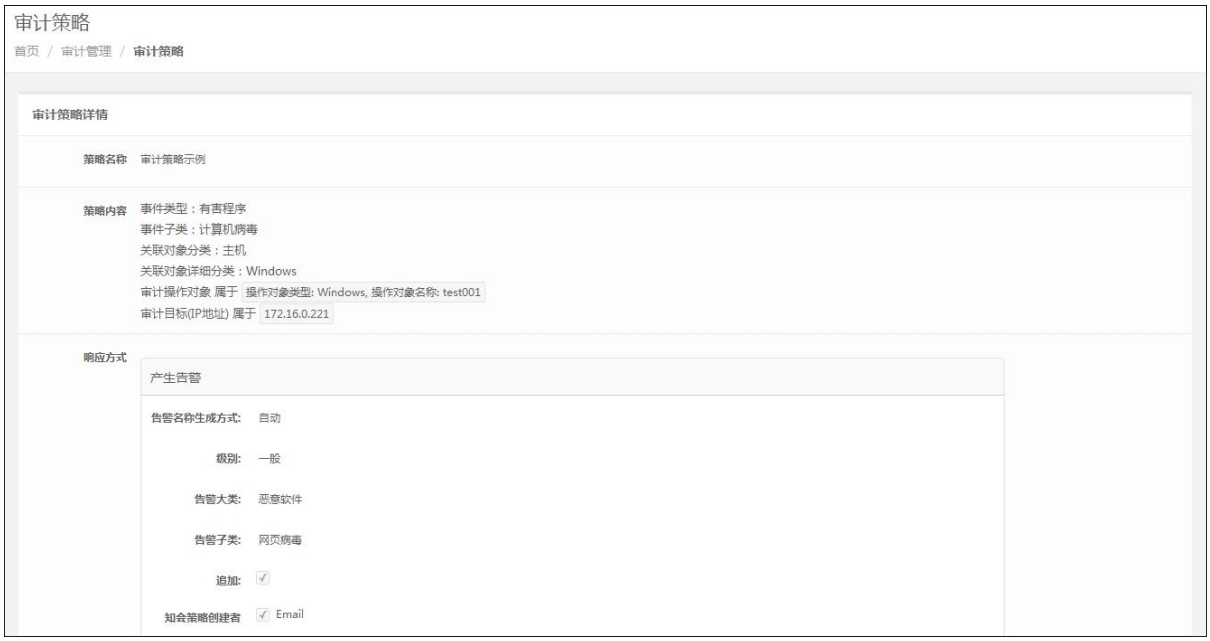


5.5.2.2 审计策略

1. 审计策略列表：系统内置一些审计策略，内置审计策略允许修改，但不允许删除。如下图所示：

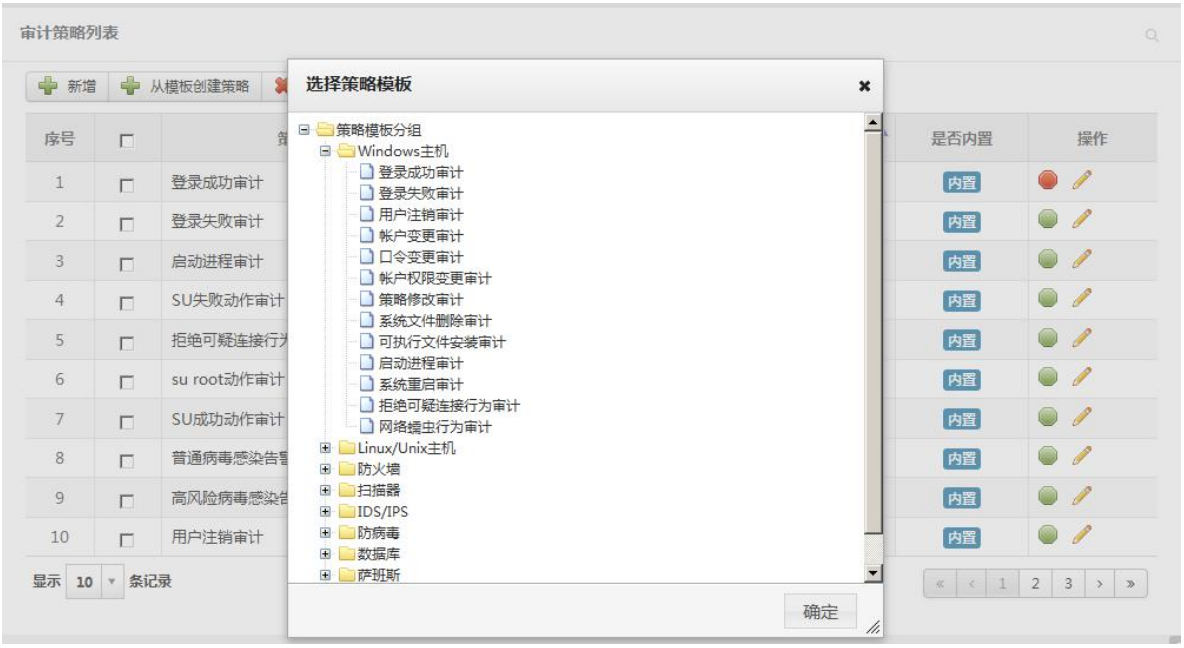


2. 审计策略详情：点击审计策略名称，查看审计策略详情。如下图所示：



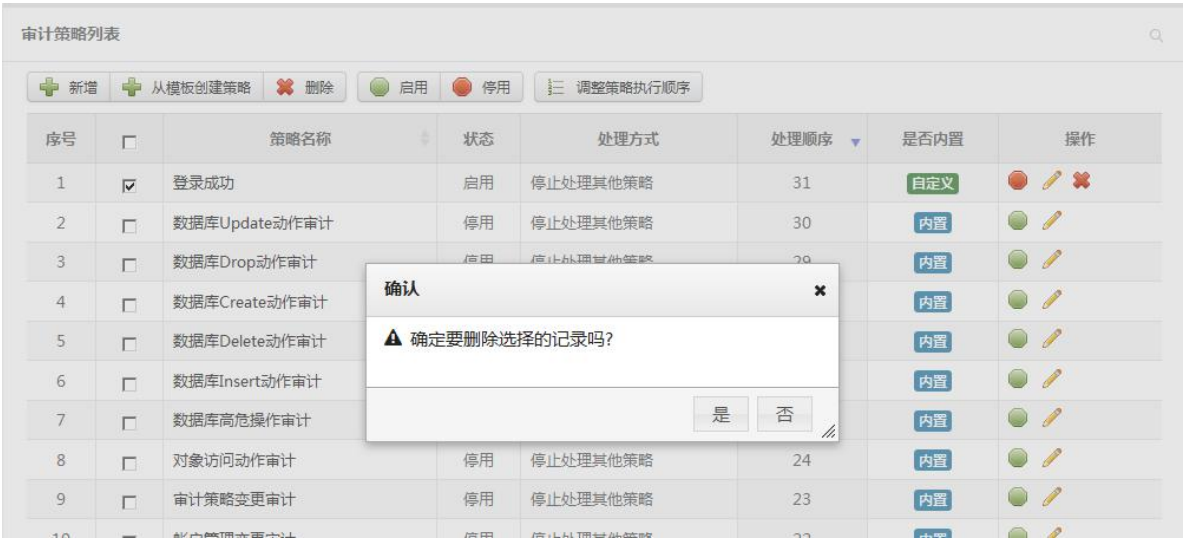
3. 新增审计策略：点击新增按钮，用户需要填写策略名称、过滤器（包括事件类型、事件子类、关联对象分类、关联对象详细分类、审计对象，审计对象分为自定义及预定义，预定义可参考 4.7.2.5~4.7.2.10 章节）、合并条件（选填）、响应方式（选填）、命中后继续（选填）、审计名称（选填）、审计类型、审计级别、描述（选填），点击保存。如下图所示：

4. 从模板创建审计策略：点击从模板创建策略，选择审计策略模板，修改审计策略属性，点击保存。如下图所示：

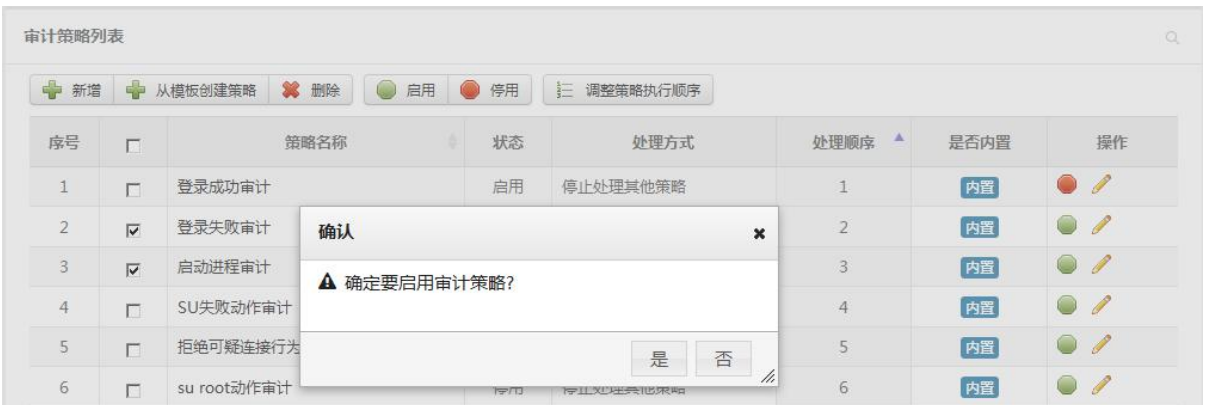


5. 修改审计策略：修改审计策略基础属性，点击保存。如下图所示：

6. 删除审计策略：选择一个或多个需要删除的审计策略，点击删除。内置策略不允许删除。如下图所示：

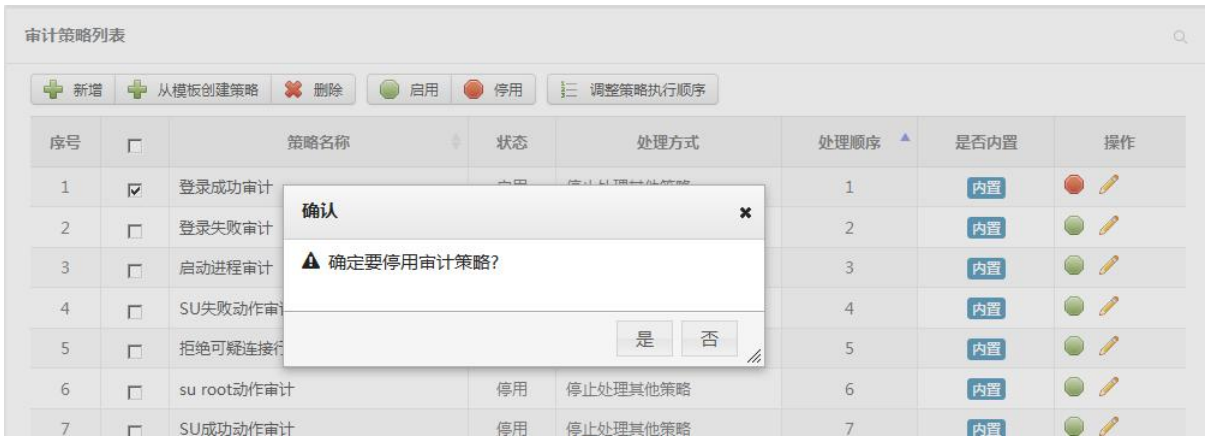


7. 启用审计策略：选择一个或多个需要启用的审计策略，点击启用。只有停用状态的审计策略才允许被启用。如下图所示：

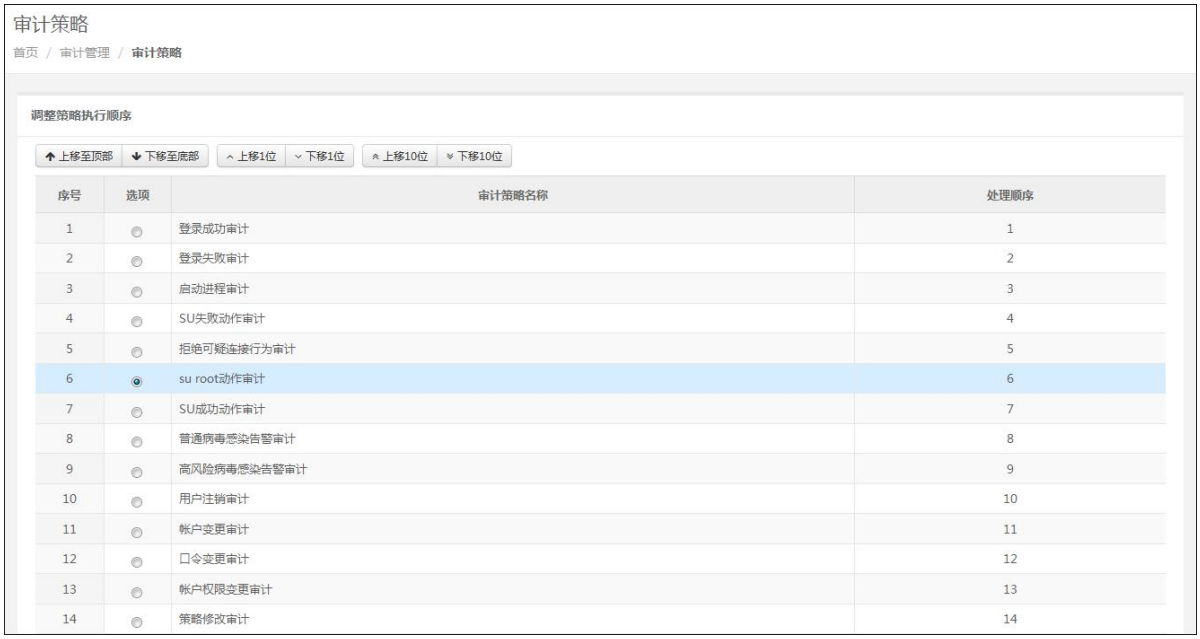


8. 停用审计策略：选择一个或多个需要停用的审计策略，点击停用。只有启用状态的审计策略才允许被

停用。如下图所示：

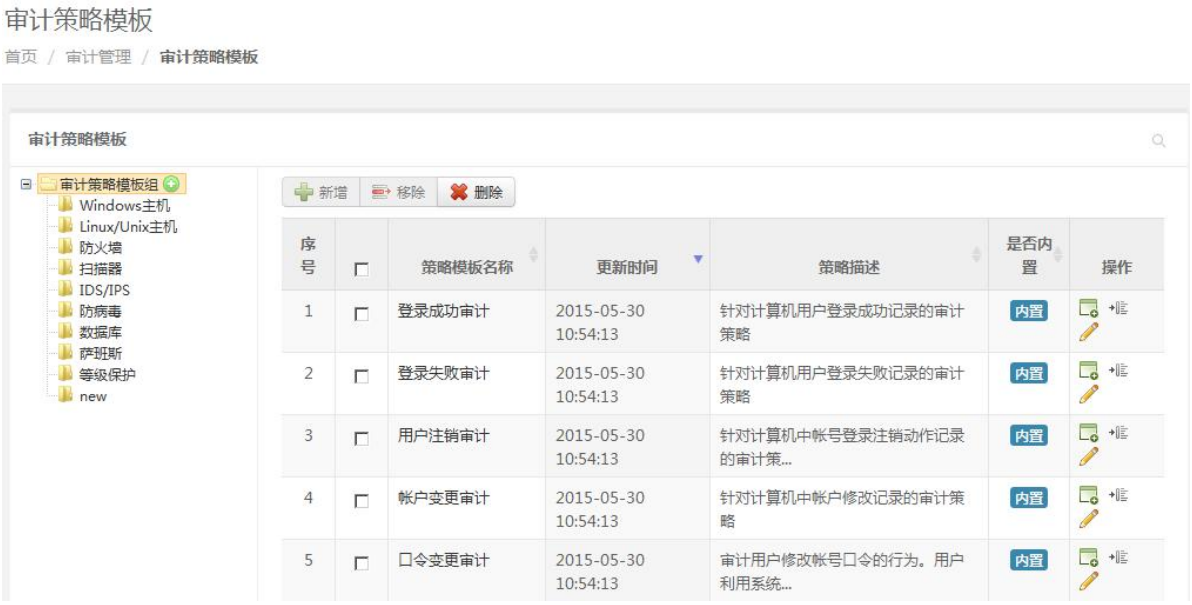


9. 调整审计策略执行顺序：点击调整策略执行顺序，选中需要调整的策略，通过点击上移至顶部、下移至底部、上移 1 位、下移 1 位、上移 10 位、下移 10 位，完成策略位置的调整。如下图所示：



5.5.2.3 审计策略模板

1. 审计策略模板列表：系统支持按照审计策略模板分组维度查看审计策略模板，审计策略模板分组是可管理的。系统内置了一些审计策略模板，内置审计策略模板允许修改，但不允许删除。如下图所示：



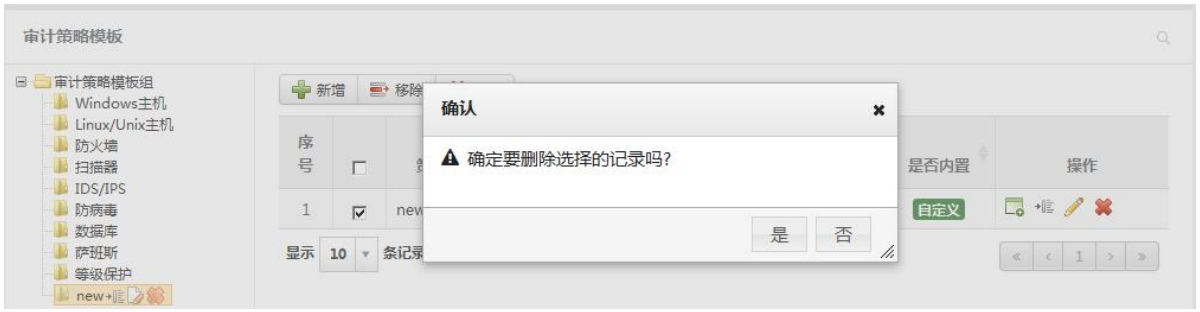
2. 审计策略模板详情：点击策略模板名称可查看审计策略模板详情。如下图所示：

3. 审计策略模板组管理：可以对自定义的策略模板分组进行增删改操作，内置策略模板分组不允许进行编辑操作。如下图所示：

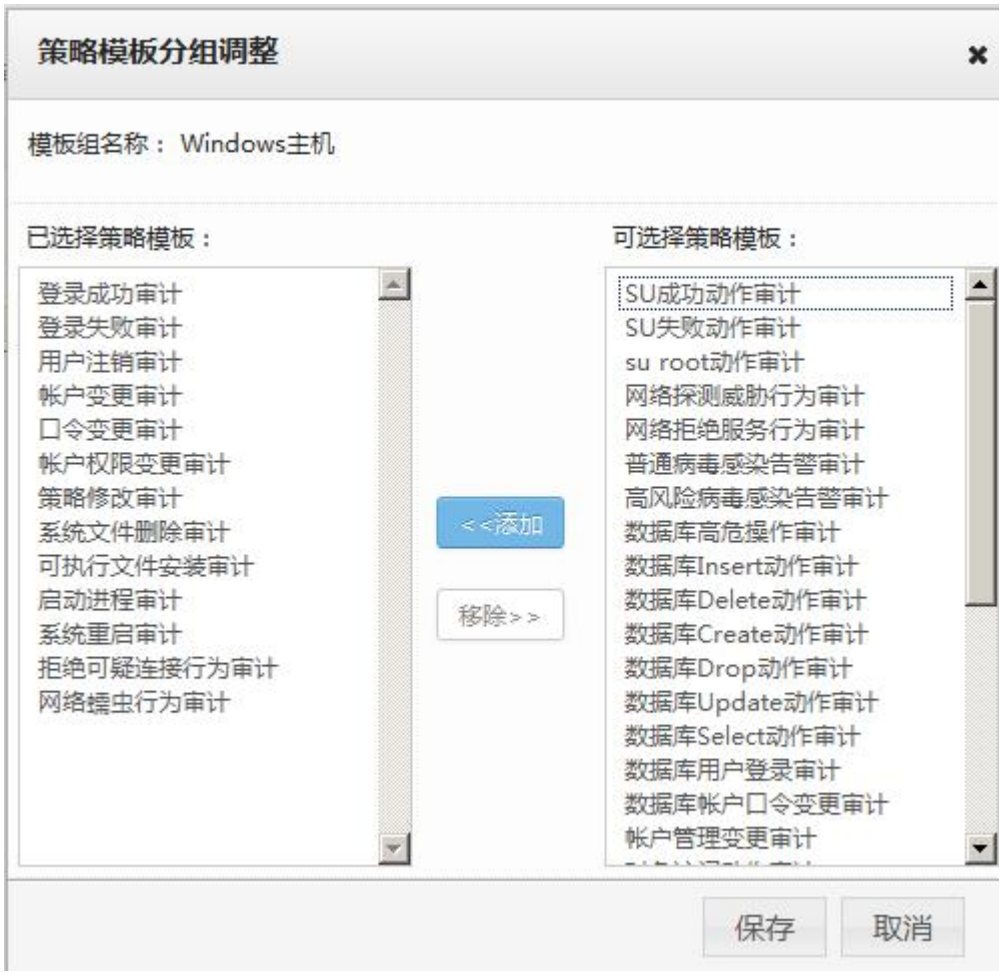
4. 新增审计策略模板：选择策略模板分组，点击新增按钮，用户填写策略模板名称、过滤器（包括事件类型、事件子类、关联对象分类、关联对象详细分类、审计对象，审计对象分为自定义及预定义，预定义可参考 4.7.2.5~4.7.2.10 章节）、合并条件（选填）、描述（选填），点击保存。如下图所示：

5. 修改审计策略模板：修改审计策略模板相关属性，点击保存。如下图所示：

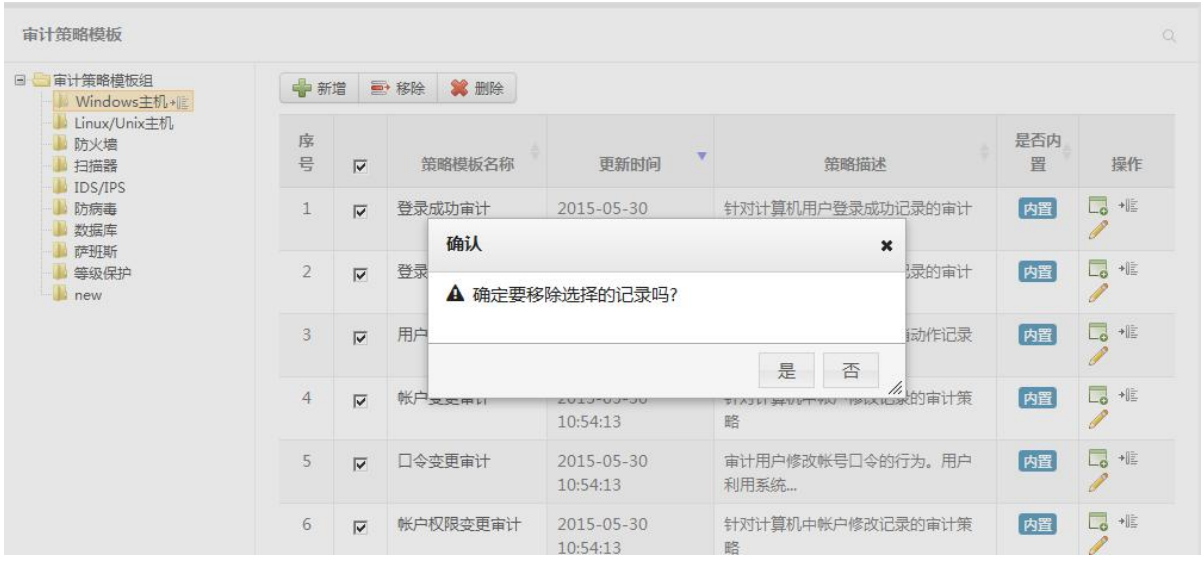
6. 删除审计策略模板：选择一个或多个要删除的审计策略模板，点击删除按钮，内置审计策略模板不允许删除。如下图所示：



7. 审计策略模板分组：点击分组按钮（审计模板组及模板数据后面均有分组按钮），对审计策略模板组或审计策略进行分组，点击保存。如下图所示：



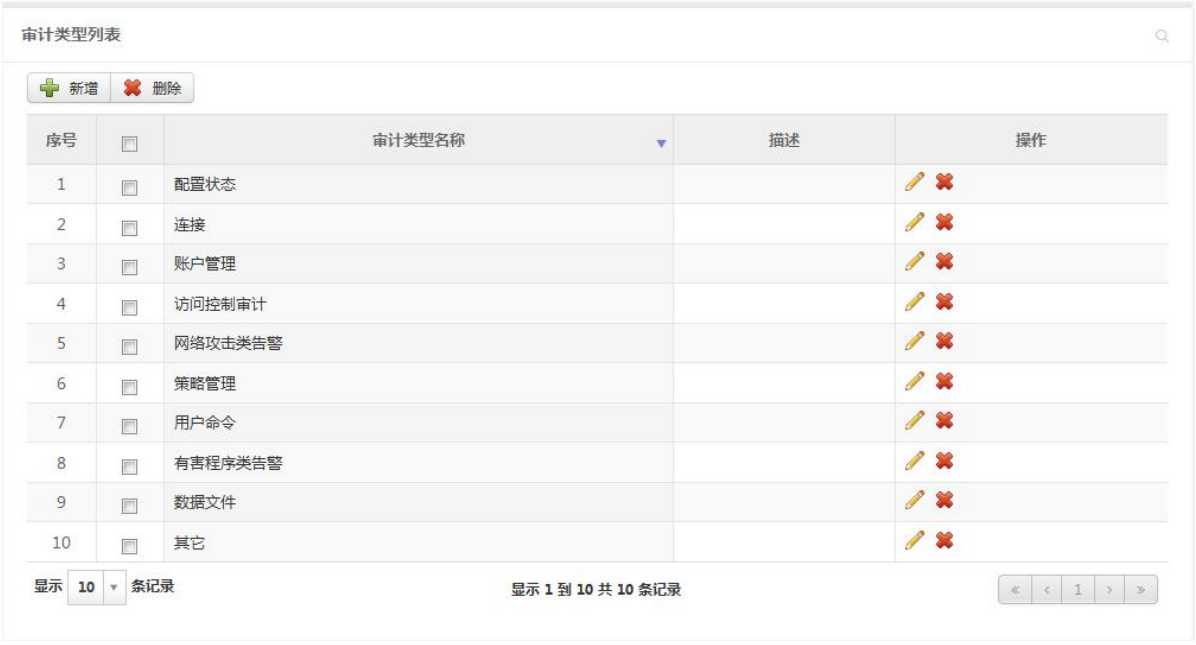
8. 审计策略模板移除：选择策略模板分组，选择一个或多个要移除的审计策略模板，点击移除按钮，系统将选择的审计模板从审计分组中移除出去，但不会删除审计模板。如下图所示：



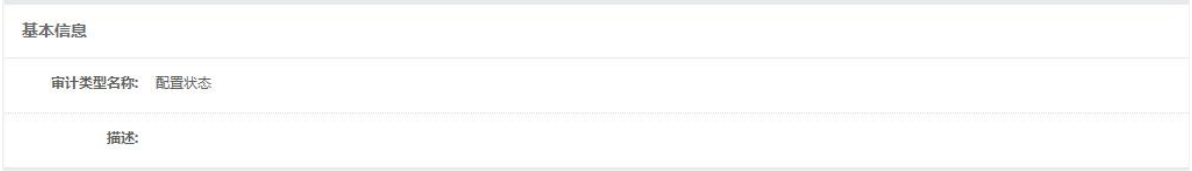
9. 从审计策略模板创建审计策略：点击从模板创建策略图标，用户修改审计策略基础属性（具体可参考4.7.2.2 章节），点击保存，完成创建审计策略。如下图所示：

5.5.2.4 审计类型

1. 审计类型列表：系统内置了一些审计类型，内置审计类型允许修改和删除。如下图所示：



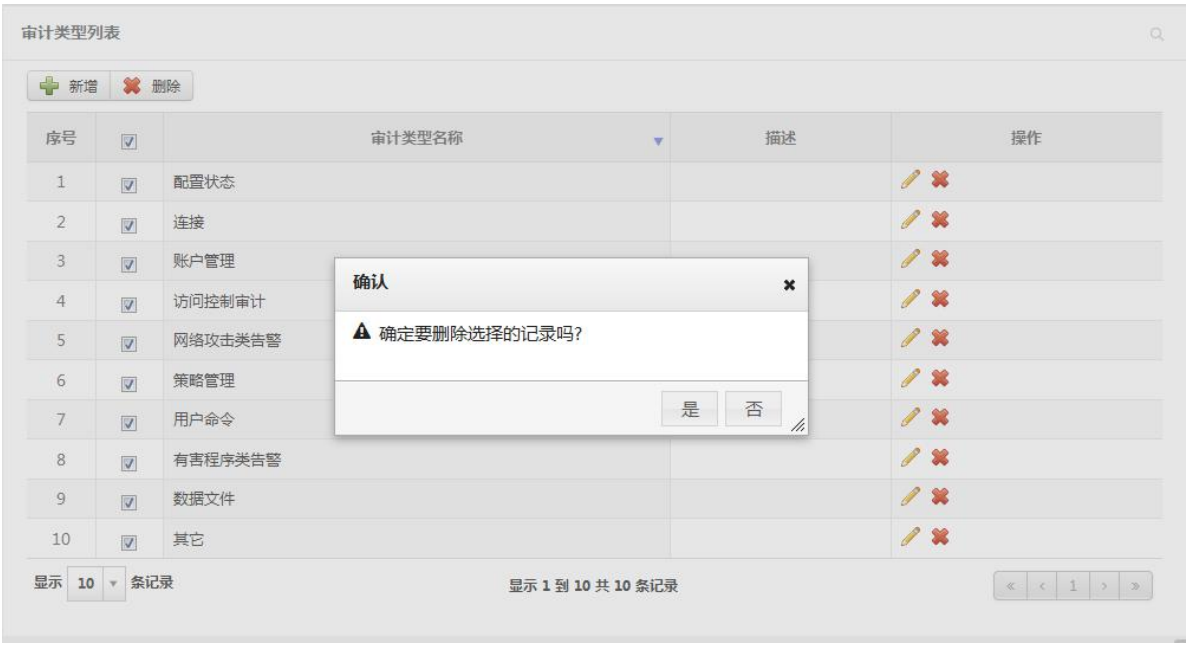
2. 审计类型详情：点击审计类型名称，可查看审计类型详情。如下图所示：



3. 审计类型新增：点击新增按钮，用于输入审计类型名称、描述（选填），点击保存。如下图所示：

4. 审计类型修改：修改审计类型相关属性，点击保存。如下图所示：

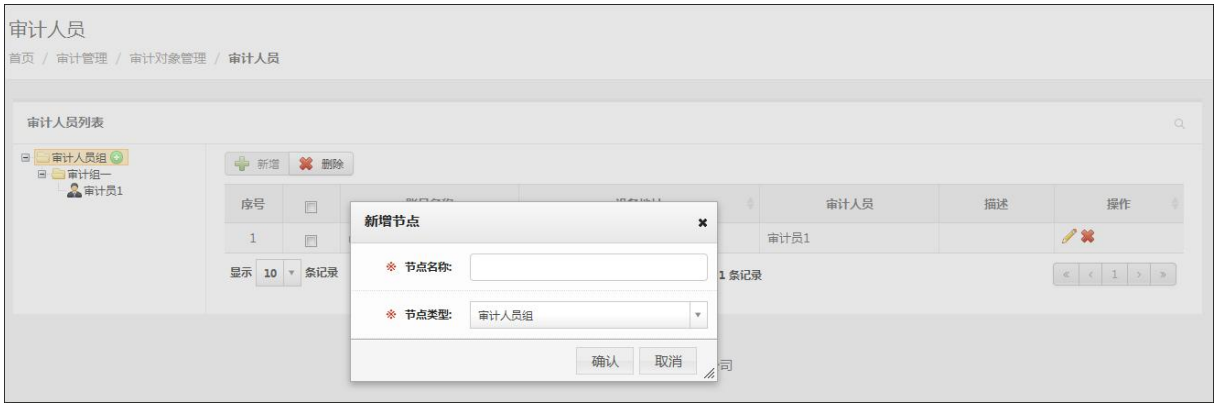
5. 审计类型删除：选择一个或多个需要删除的审计类型，点击删除。被审计策略使用的审计类型无法删除。如下图所示：



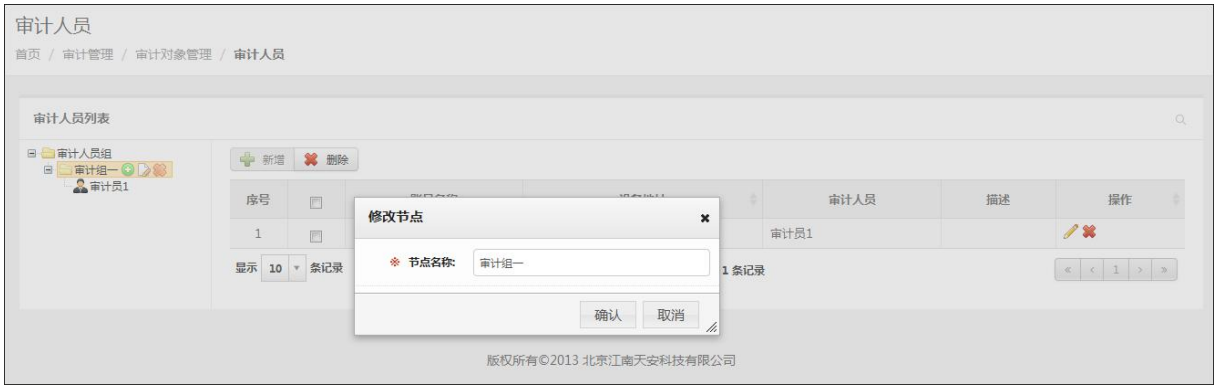
5.5.2.5 审计人员

1. 审计人员列表：左边树结构展示的是审计人员组及其下的审计人员（文件夹图标代表的是审计人员组，人员图标代表的是审计人员），右边列表展示的是审计人员组或审计人员下的审计账号。如下图所示：

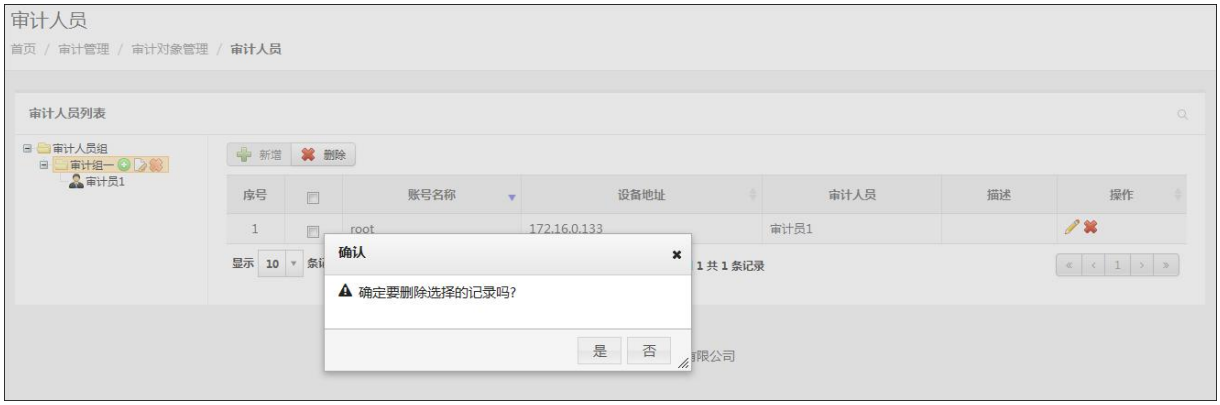
2. 新增节点：点击添加节点（只有审计人员组下允许添加节点），用户需要填写节点名称和节点类型（分为审计人员组和审计人员两种类型），点击确认，完成审计人员组或审计人员的新增。如下图所示：



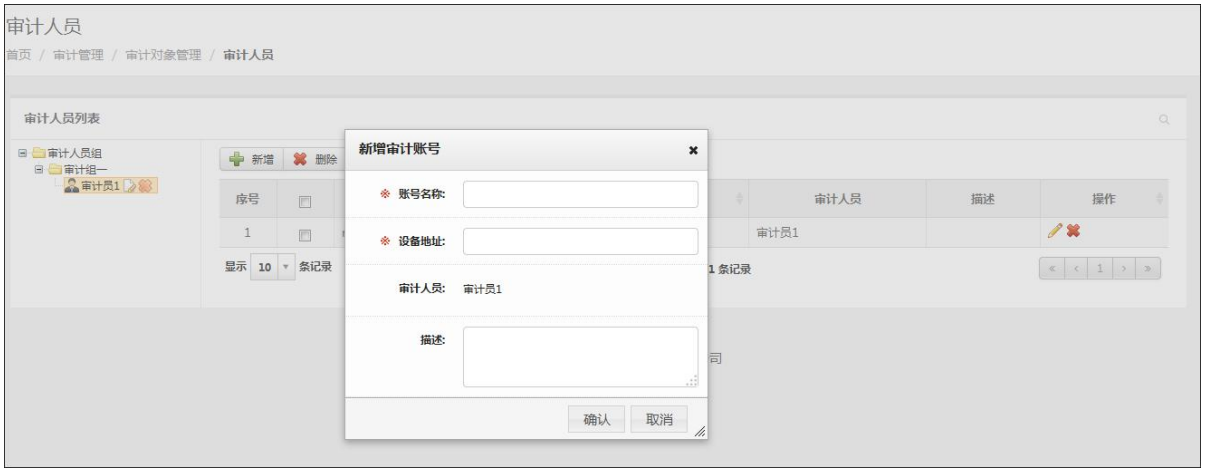
3. 修改节点：选择需要修改的节点，点击其旁边重命名图标，修改审计人员组或审计人员的基本属性，点击确认。如下图所示：



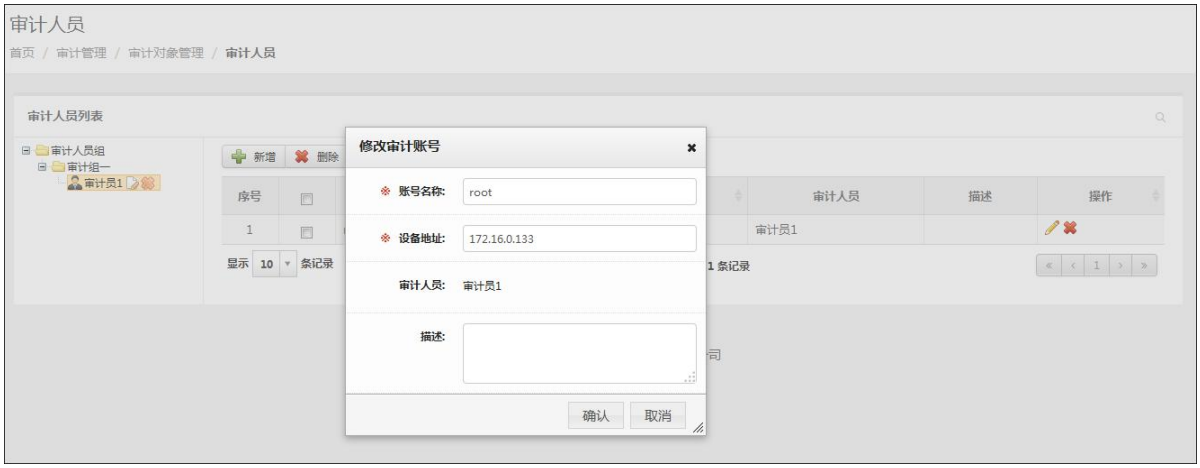
4. 删除节点：选择需要删除的节点，点击其旁边删除图标。如果审计人员组及其子节点下面存在审计人员，审计人员正在被审计策略或审计执行者对象引用，则不允许删除该节点。如下图所示：



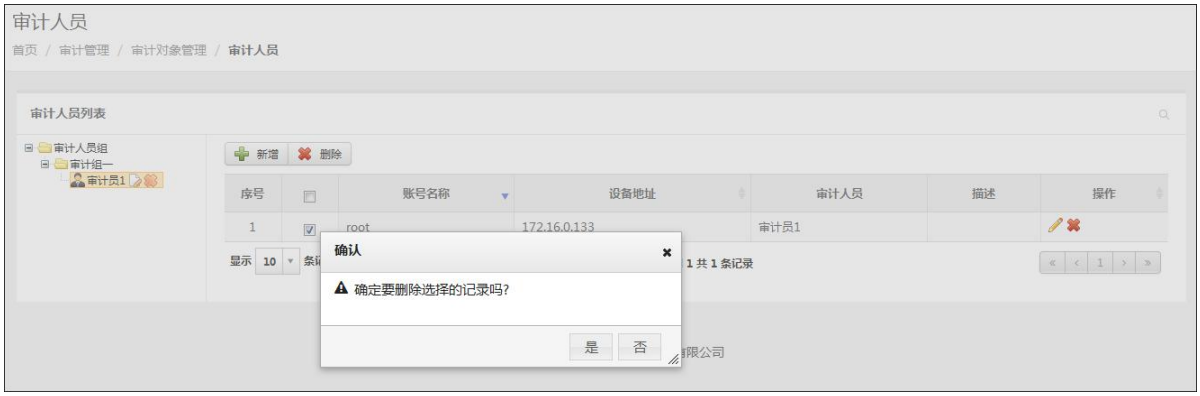
5. 新增审计账号：选择审计人员，点击新增按钮，用户需要输入账号名称、设备地址、描述（选填），点击确认。如下图所示：



6. 修改审计账号：点击修改按钮，修改审计账号基本属性，点击确认。如下图所示：



7. 删除审计账号：选择一个或多个需要删除的审计账号，点击删除。如下图所示：

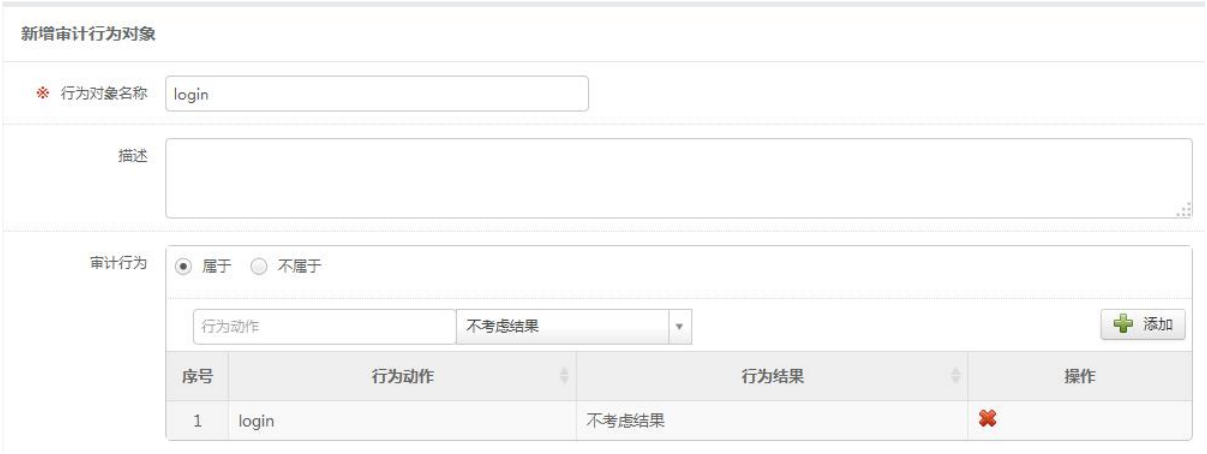


5.5.2.6 审计行为对象

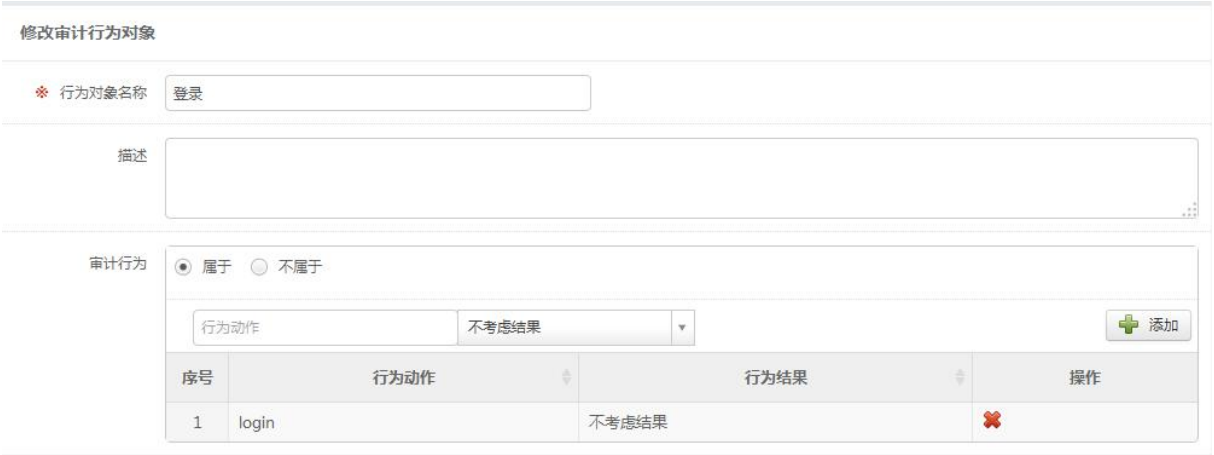
1. 审计行为对象列表：如下图所示：

2. 审计行为对象详情：点击行为对象名称，可查看行为对象详情。如下图所示：

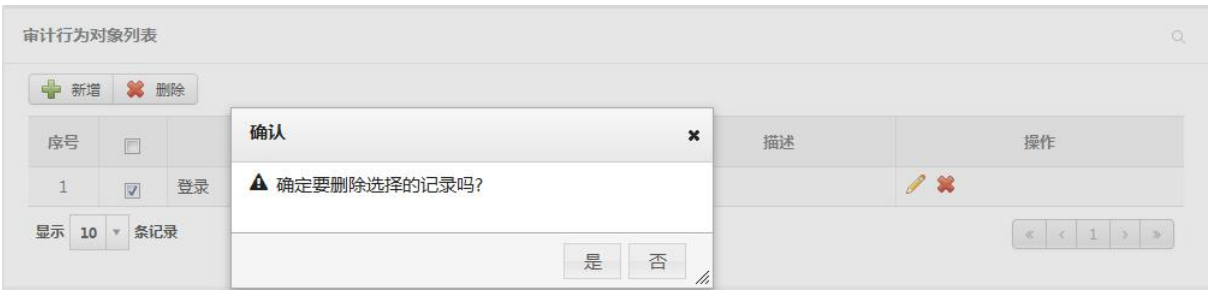
3. 审计行为对象新增：点击新增按钮，用于输入行为对象名称、审计行为、描述（选填），点击保存。如下图所示：



4. 审计行为对象修改：修改审计行为对象相关属性，点击保存。如下图所示：



5. 审计行为对象删除：选择一个或多个需要删除的审计行为对象，点击删除。被审计策略使用的审计行为对象无法删除。如下图所示：



5.5.2.7 审计行为执行者对象

1. 审计行为执行者对象列表：如下图所示：

2. 审计行为执行者对象详情：点击行为执行者对象名称，可查看行为执行者对象详情。如下图所示：

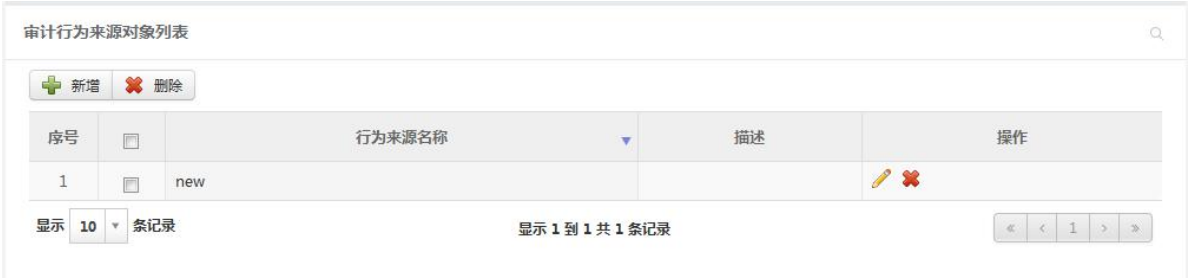
3. 审计行为执行者对象新增：点击新增按钮，用于输入行为执行者对象名称、审计行为执行者（可以添加账号，也可以选择审计人员）、描述（选填），点击保存。如下图所示：

4. 审计行为执行者对象修改：修改审计行为执行者对象相关属性，点击保存。如下图所示：

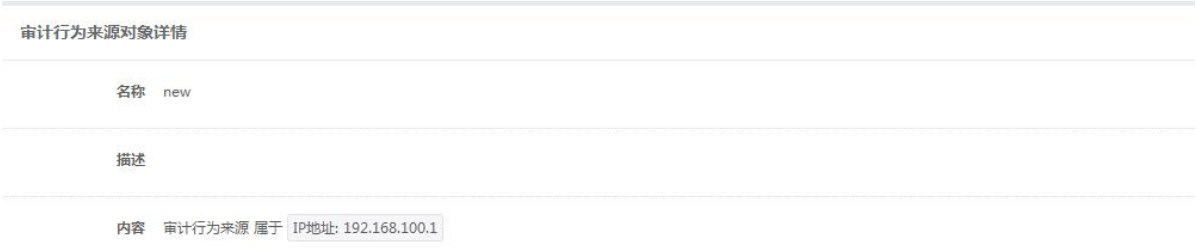
5. 审计行为执行者对象删除：选择一个或多个需要删除的审计行为执行者对象，点击删除。被审计策略使用的审计行为执行者对象无法删除。如下图所示：

5.5.2.8 审计行为来源对象

1. 审计行为来源对象列表：如下图所示：



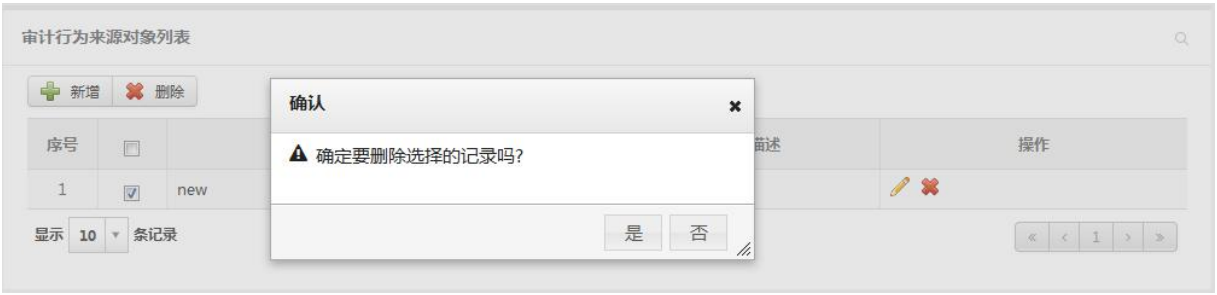
2. 审计行为来源对象详情：点击行为来源名称，可查看行为来源对象详情。如下图所示：



3. 审计行为来源对象新增：点击新增按钮，用于输入名称、行为来源、描述（选填），点击保存。如下图所示：

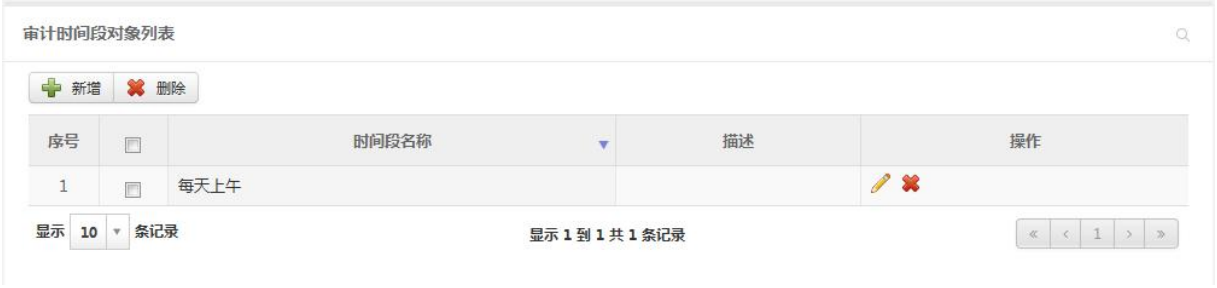
4. 审计行为来源对象修改：修改审计行为来源对象相关属性，点击保存。如下图所示：

5. 审计行为来源对象删除：选择一个或多个需要删除的审计行为来源对象，点击删除。被审计策略使用的审计行为来源对象无法删除。如下图所示：

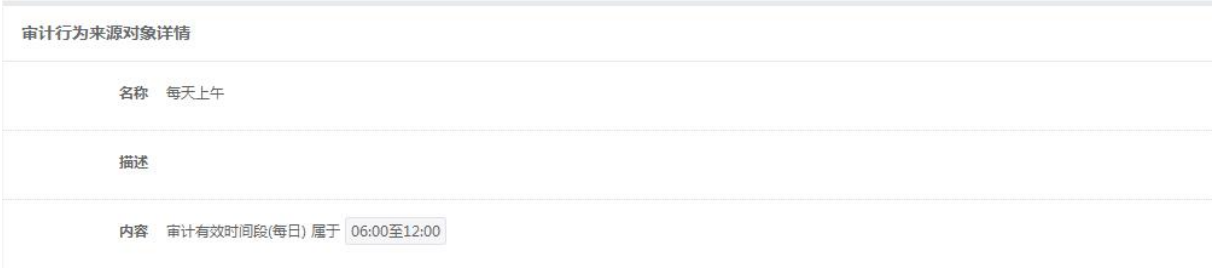


5.5.2.9 审计时间段对象

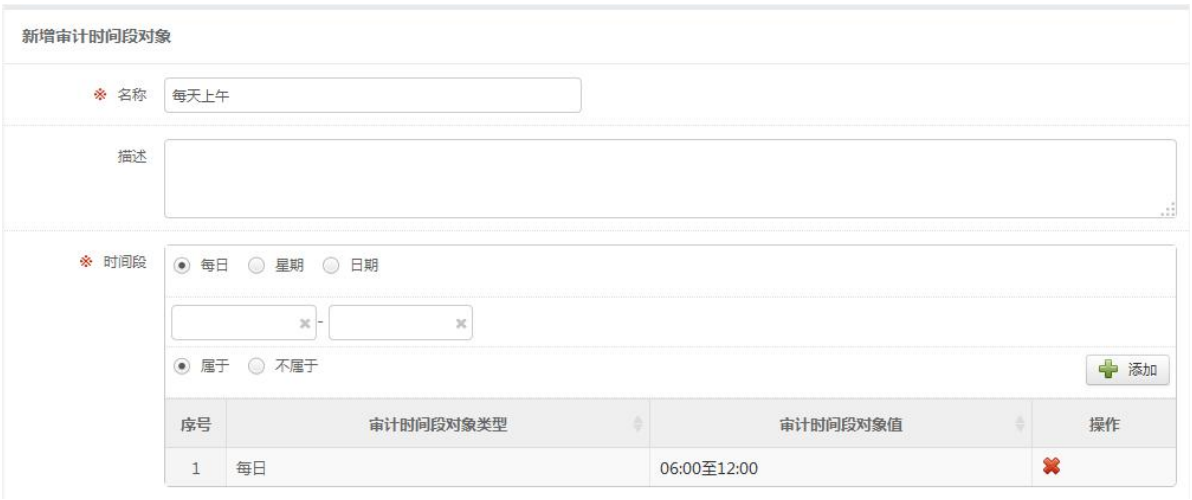
1. 审计时间段对象列表：如下图所示：



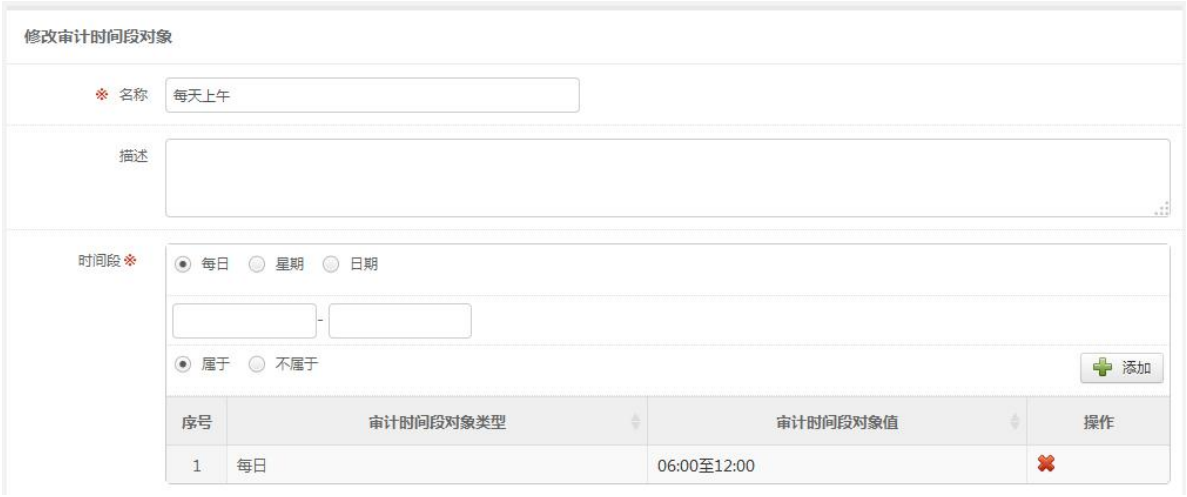
2. 审计时间段对象详情：点击时间段对象名称，可查看时间段对象详情。如下图所示：



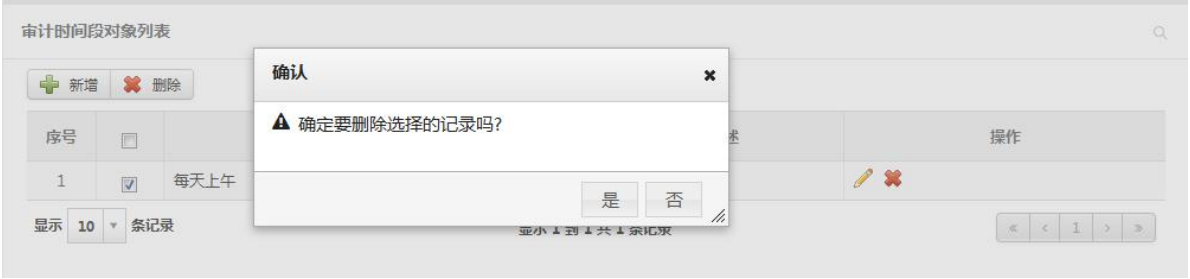
3. 审计时间段对象新增：点击新增按钮，用于输入名称、时间段（支持每日、星期、日期三种模式）、描述（选填），点击保存。如下图所示：



4. 审计时间段修改：修改审计时间段对象相关属性，点击保存。如下图所示：

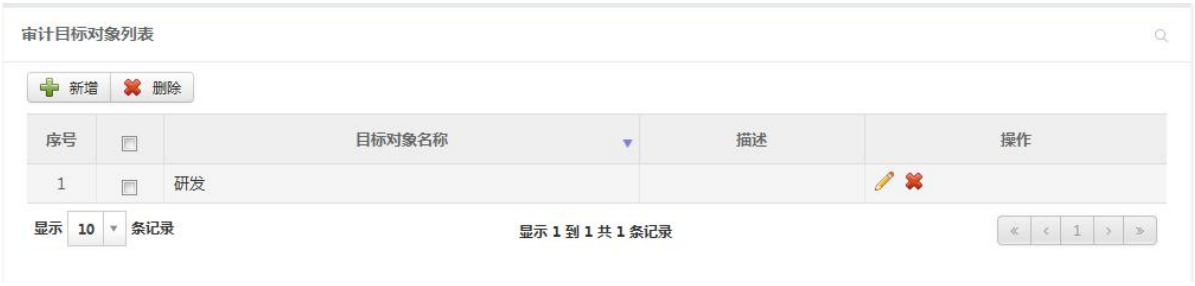


5. 审计时间段对象删除：选择一个或多个需要删除的审计时间段对象，点击删除。被审计策略使用的审计时间段对象无法删除。如下图所示：



5.5.2.10 审计目标对象

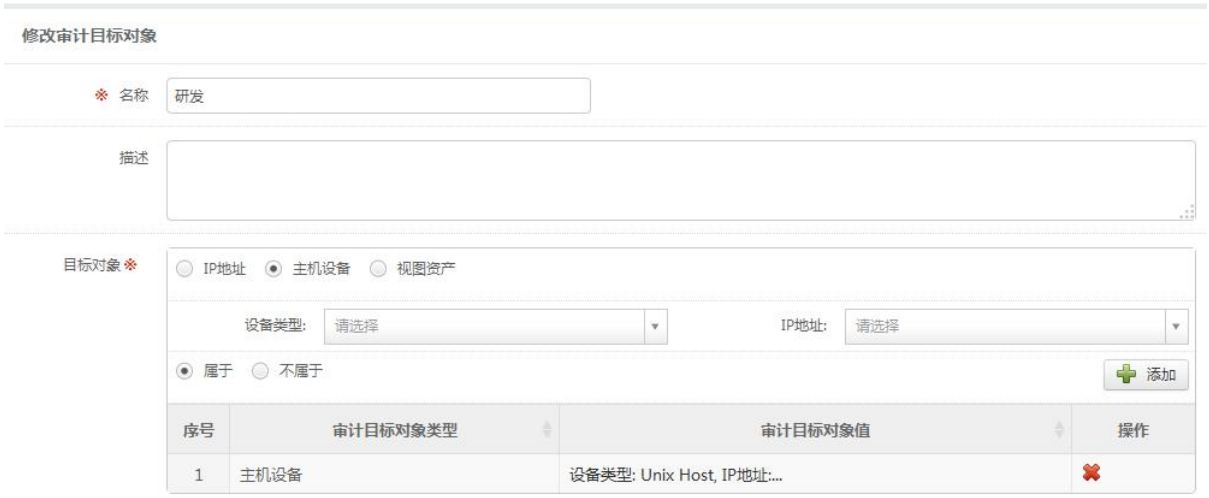
1. 审计目标对象列表：如下图所示：



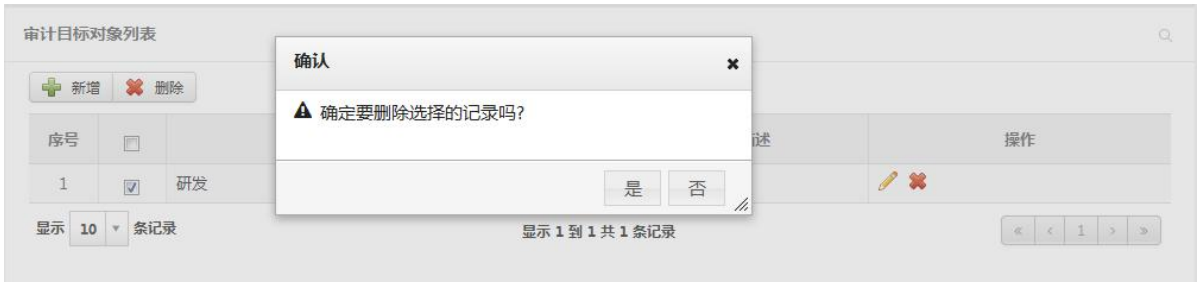
2. 审计目标对象详情：点击目标对象名称，可查看目标对象详情。如下图所示：

3. 审计目标对象新增：点击新增按钮，用于输入名称、目标对象（支持 IP 地址、主机设备、视图资产三种模式）、描述（选填），点击保存。如下图所示：

4. 审计目标对象修改：修改审计目标对象相关属性，点击保存。如下图所示：



5. 审计目标对象删除：选择一个或多个需要删除的审计目标对象，点击删除。被审计策略使用的审计目标对象无法删除。如下图所示：



5.6 安全监控

5.6.1 什么是告警

与普通的安全事件不同，告警是特别需要关注的安全问题，这些问题来源于关联事件或审计事件。

5.6.2 告警的级别

告警被分为如下级别：

级别	级别名称
1	一般
2	警告
3	严重
4	极度严重

5.6.3 告警的处理

对于告警的处理主要包括确认（认为可能是问题）、清除（认为不是问题或问题已解决）。

5.6.4 什么是实时监控

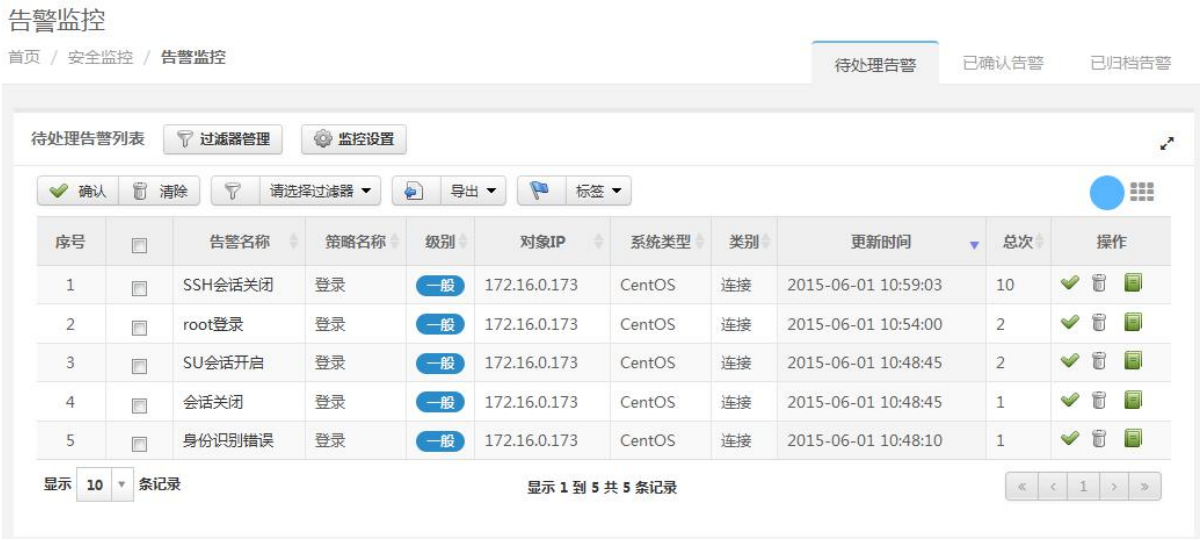
实时监控能够实时动态、逐条、滚动显示当前系统所接收到的事件日志，并且能够通过定制过滤规则，逐步缩小监控范围，有效及时发现安全异常问题。

5.6.5 相关操作

5.6.5.1 告警监控

1. 告警列表：以列表的方式展示告警，已 Tab 页的形式展示不同阶段的告警：
   - 待处理告警：展示等待处理的告警，该阶段可进行以下操作：过滤器管理、监控设置、确认、清除、选择过滤器、导出、标签。
   - 已确认告警：展示已确认的告警，该阶段可进行以下操作：过滤器管理、清除、选择过滤器、导出。
   - 已归档告警：展示已归档的告警，该阶段可进行以下操作：导出。

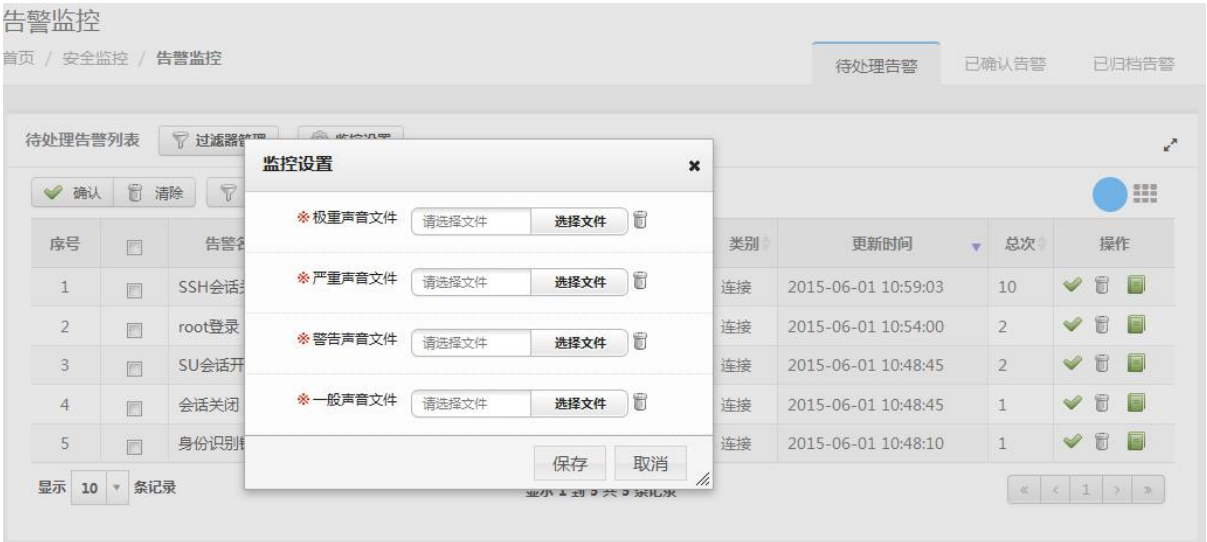
   如下图所示：



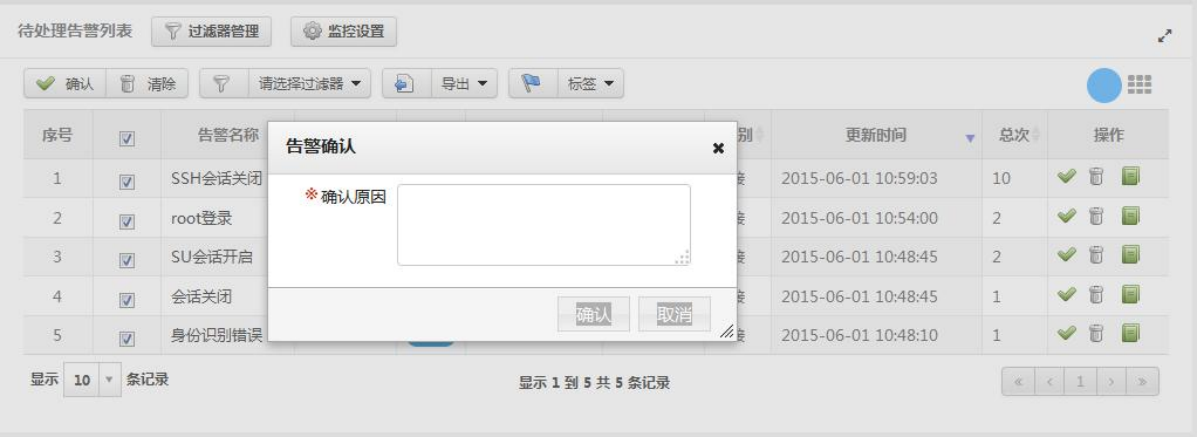
2. 告警详情：点击告警名称，进入告警详情页面，详情页面中包含告警详细信息以及原始事件列表，可通过点击原始事件名称进入原始事件详情页面。如下图所示：

3. 过滤器管理：点击过滤器管理，进入到过滤器管理页面，可以对过滤器进行增加、删除、修改操作。如下图所示：

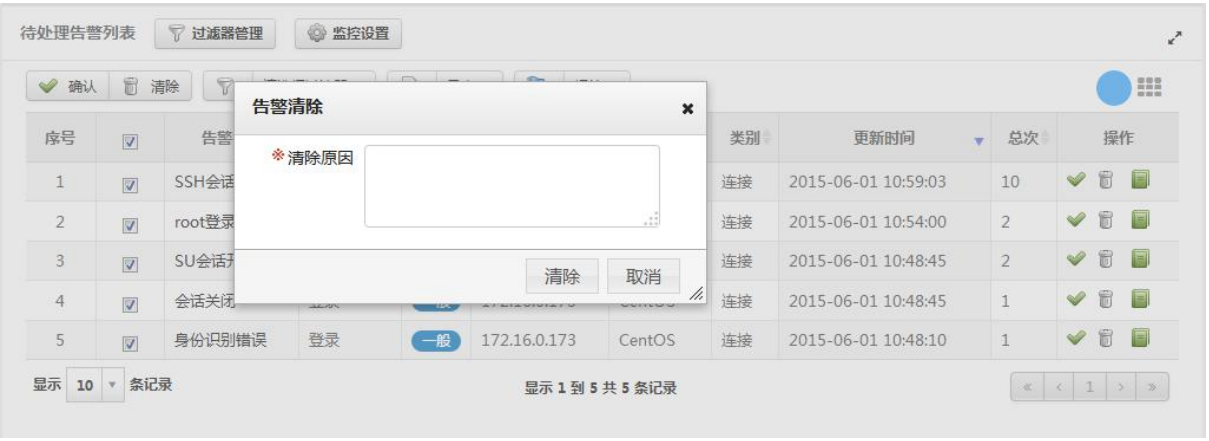
4. 监控设置：点击监控设置，上传声音文件，点击保存，可对不同严重级别告警的声音进行设置。如下图所示：



5. 确认：选择一条或多条需要确认的告警，点击确认，填写确认原因。如下图所示：

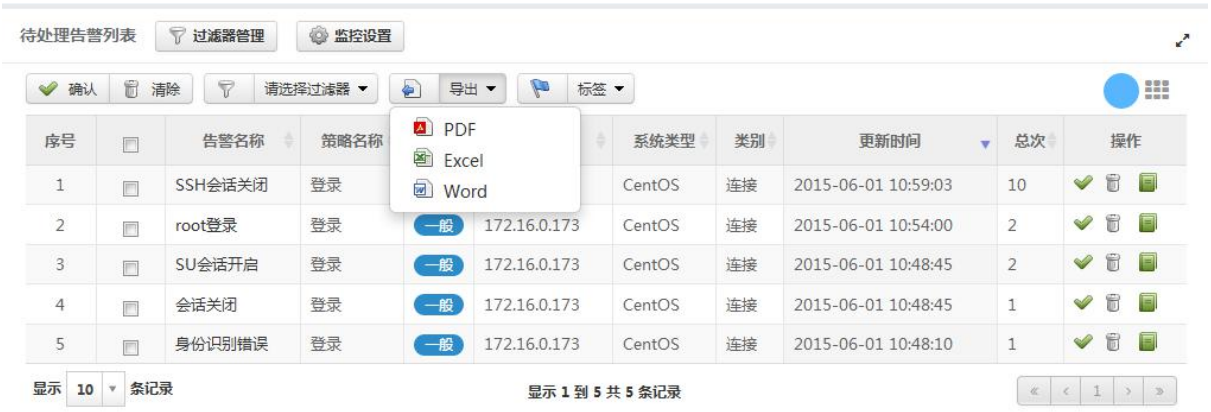


6. 清除：选择一条或多条需要清除的告警，点击清除，填写清除原因。如下图所示：



7. 选择过滤器：单击选择过滤器，选择已创建的过滤器（可在过滤器管理中对过滤器进行管理），列表会根据选择的过滤器进行事件过滤。如下图所示：

8. 导出：点击导出按钮，可将查询出的告警保存成文件，文件格式支持 PDF、Excel、Word。如下图所示：



9. 标签：选择一个或多个需要标签的告警，选择已创建的标签（标签可通过编辑标签进行管理），对告警进行标记。如下图所示：

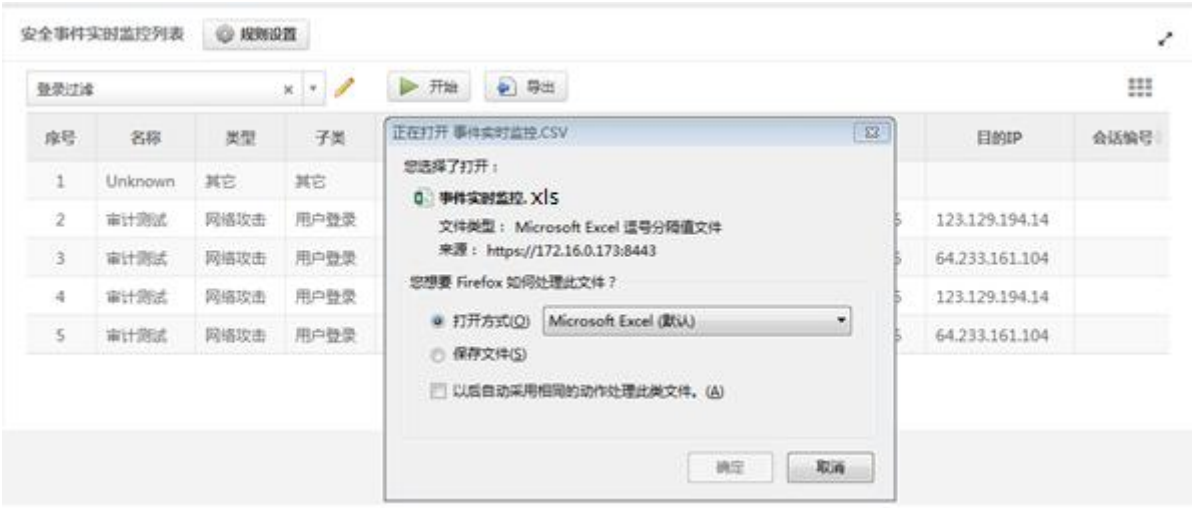
5.6.5.2 实时监控

1. 规则设置：点击规则设置，进入到规则管理页面，可以对规则进行增加、删除、修改操作。如下图所示：

2. 开始：选择已创建的规则（规则可在规则设置中进行管理，也可以通过点击“+”图标，进行快速创建），点击开始，可以对事件进行实时监控。如下图所示：

3. 暂停：点击暂停，可以暂停对事件的监控。如下图所示：

4. 导出：点击导出按钮，可以将已经监控到的事件保存为文件（监控开启时不允许导出文件），文件格式为 XLS。如下图所示：



5.7 报表管理

5.7.1 相关操作

5.7.1.1 报表实例

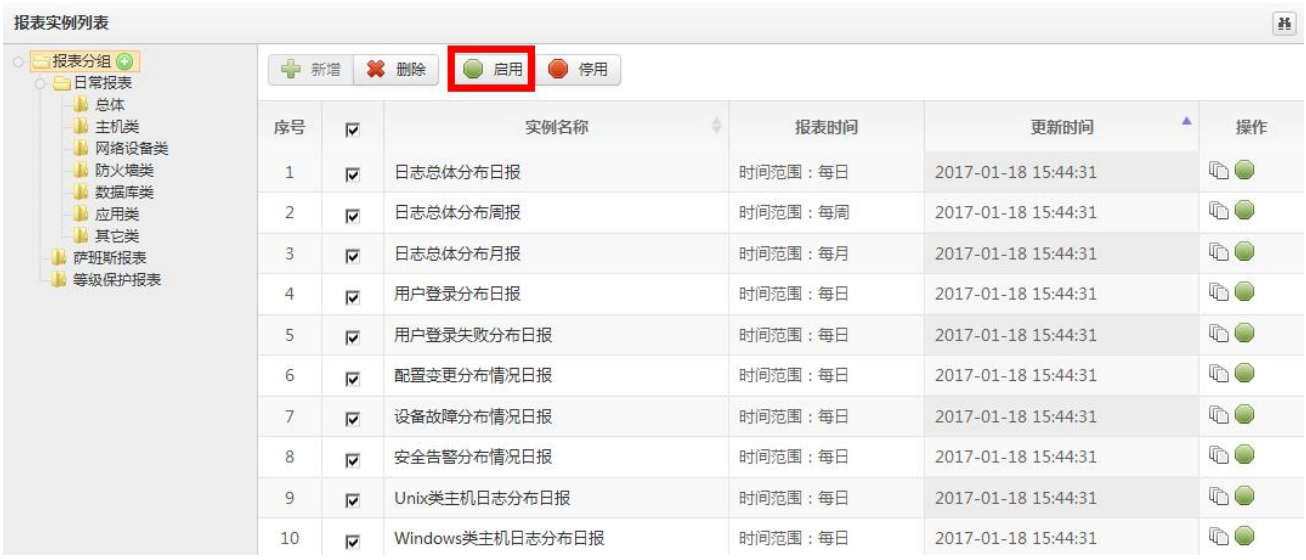
1. 报表实例列表：系统支持按照报表分组维度查看报表实例，报表分组是可管理的。系统内置了一些报

表实例，内置报表实例允许修改，但不允许删除。如下图所示：

2. 报表实例启用、停用：

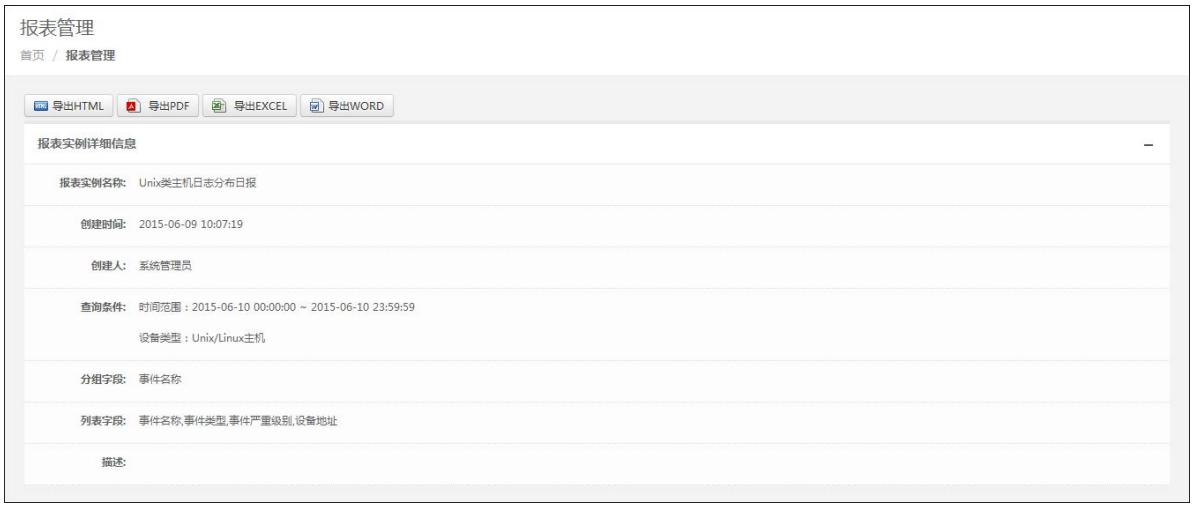
启用状态的实例可以停用

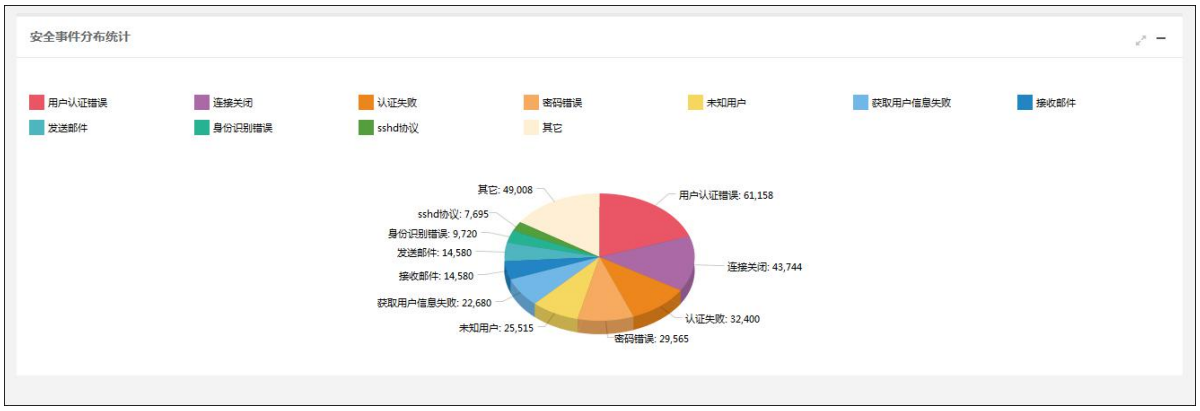
停用状态的实例可以启用



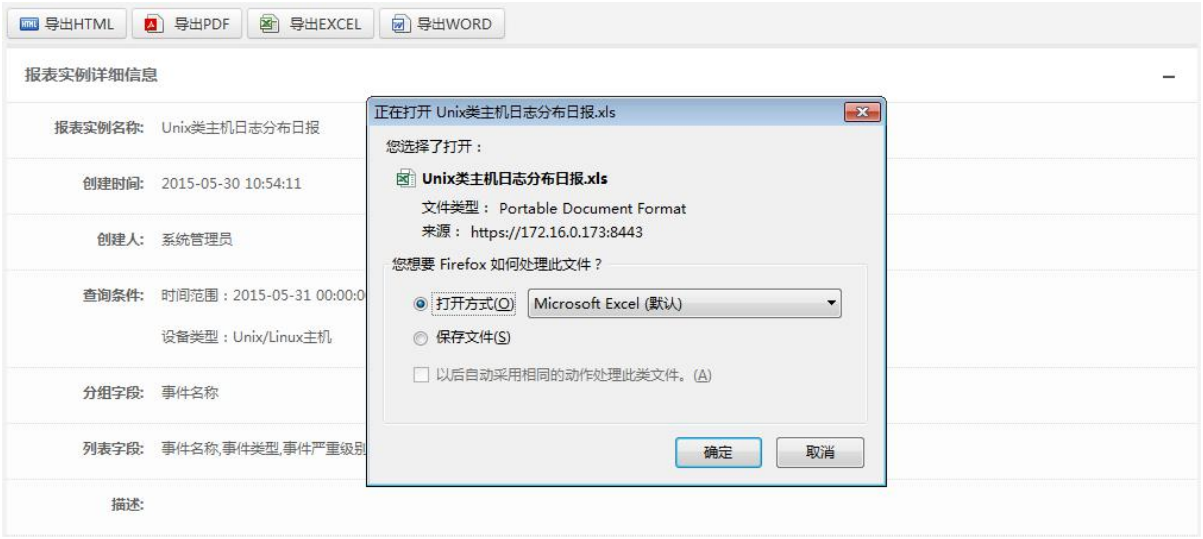
3. 报表分组管理：可以对自定义的报表分组进行增删改操作，内置报表分组不允许进行编辑操作。如下图所示：

4. 报表实例详情：点击查看按钮可查看报表实例详情。详情页面包含详细信息、安全事件分布统计图或趋势图、详细列表。如下图所示：



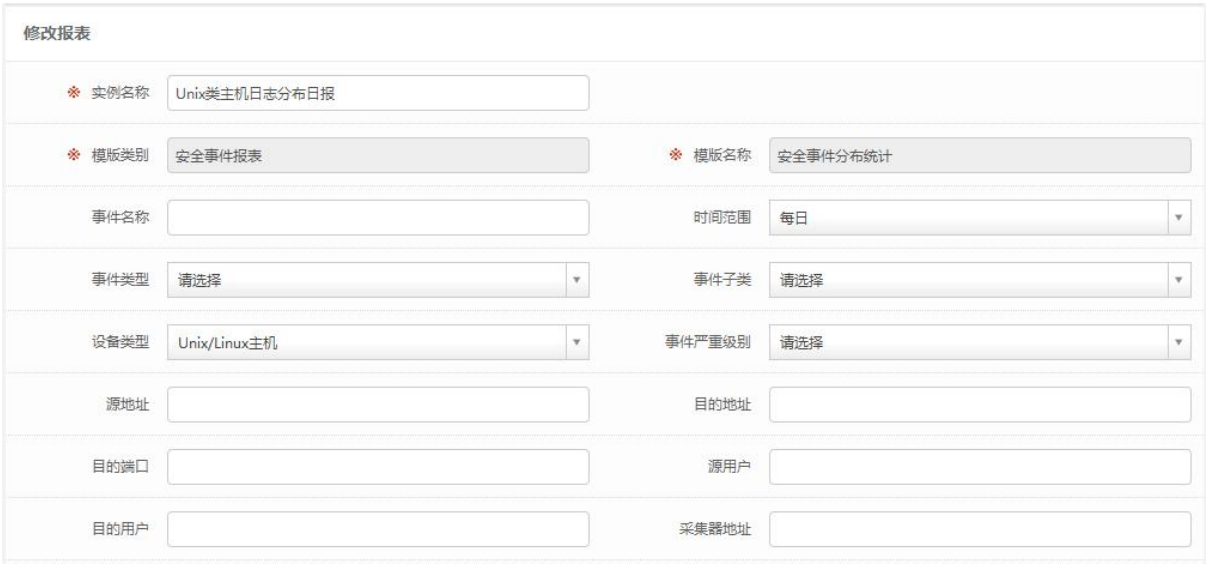


5. 报表实例导出：点击查看按钮进入到详情页面，根据文件类型点击导出按钮可以将报表实例详情保存为文件，文件类型支持 HTML、PDF、EXCEL、WORD。如下图所示：



6. 报表实例新增：选择报表分组，点击列表上方的新增按钮，用户填写实例名称、模板类别、模板名称、实例详细信息（根据选择的模板生成不同的详细信息）、描述（选填），点击保存。如下图所示：

7. 报表实例修改：修改报表实例相关属性，点击保存。如下图所示：

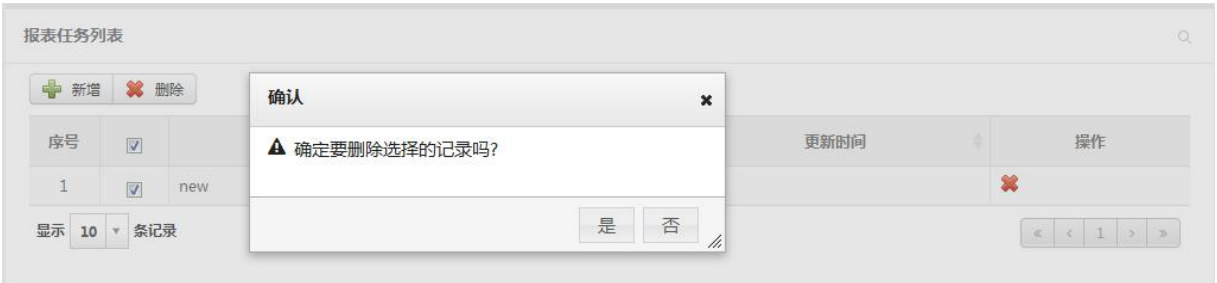


5.7.1.2 报表任务

1. 报表任务列表：显示报表任务，可以将鼠标放置在任务名称显示报表详情。如下图所示：

2. 报表任务新增：点击新增按钮，弹出输入框，用户输入任务名称、实例选择、任务类型、发送类型、收件人、附加收件人（选填）、描述（选填），点击保存。如下图所示：

3. 报表任务删除：选择一个或多个要删除的任务，点击删除按钮。如下图所示：



5.8 知识库管理

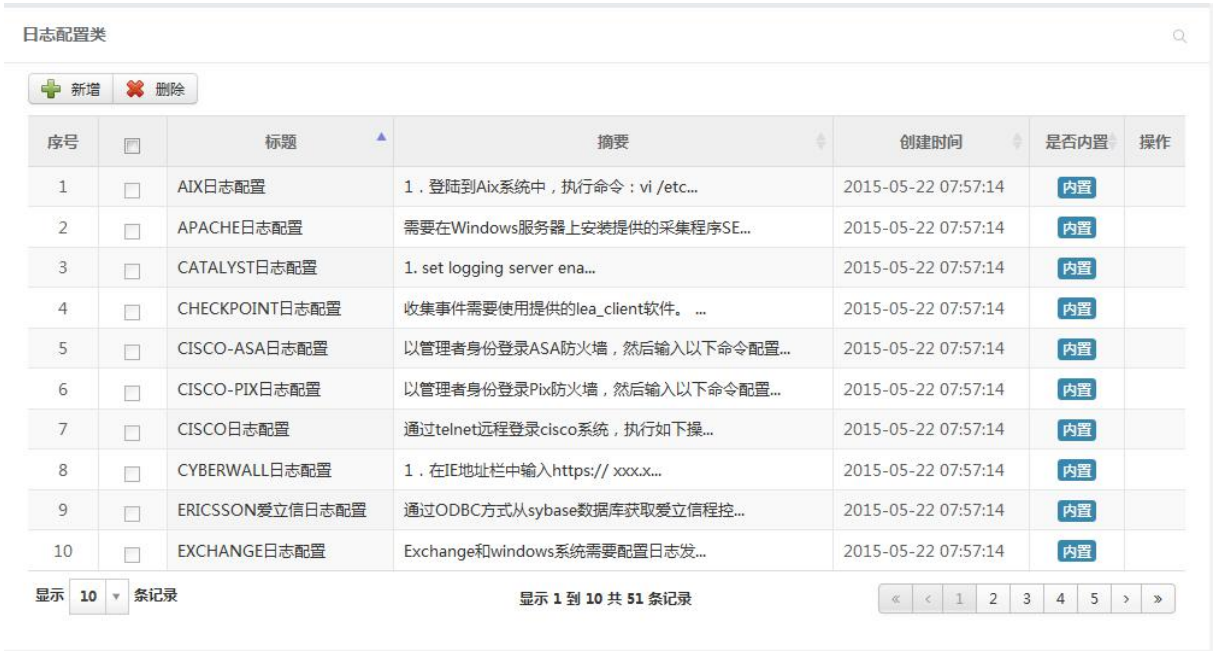
5.8.1 知识库有哪些分类

知识库管理为系统运行和维护提供了知识来源以及安全问题的处理依据、方法或参考，包括如下几类：

1. 日志配置类（各种操作系统、网络设备、应用系统及数据库等接入日志审计系统日志的配置收集方法）
2. 日志类（各种操作系统、网络设备、服务器及数据库的日志信息；反映系统运行/状态、安全问题、用户行为等的计算机记录或日志）
3. 安全经验类（基于系统安全事件、配置问题等信息综合生成的安全警示信息的描述、告警触发建议及解决方案等）

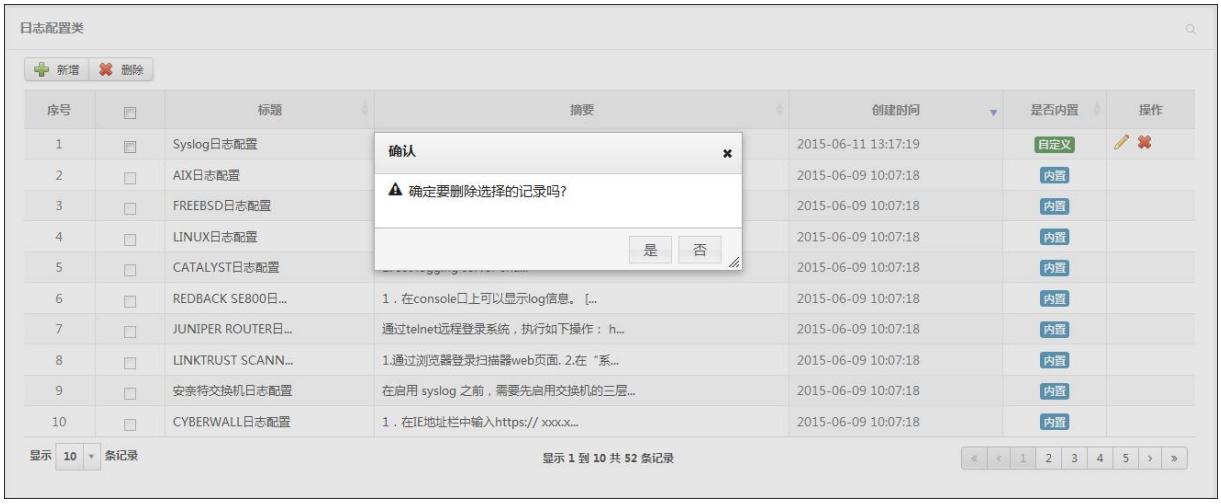
5.8.2 相关操作

1. 查看知识库列表：用户可以通过显示的类别查看各分类的知识库信息，可过滤显示自己要看的类别的知识库信息。如下图所示：



2. 查看知识库详情：查看知识库的详细内容。如下图所示：

3. 知识库维护：用户可以增加、修改（不能修改系统内置知识）、删除知识库（不能删除系统内置知识）。如下图所示：

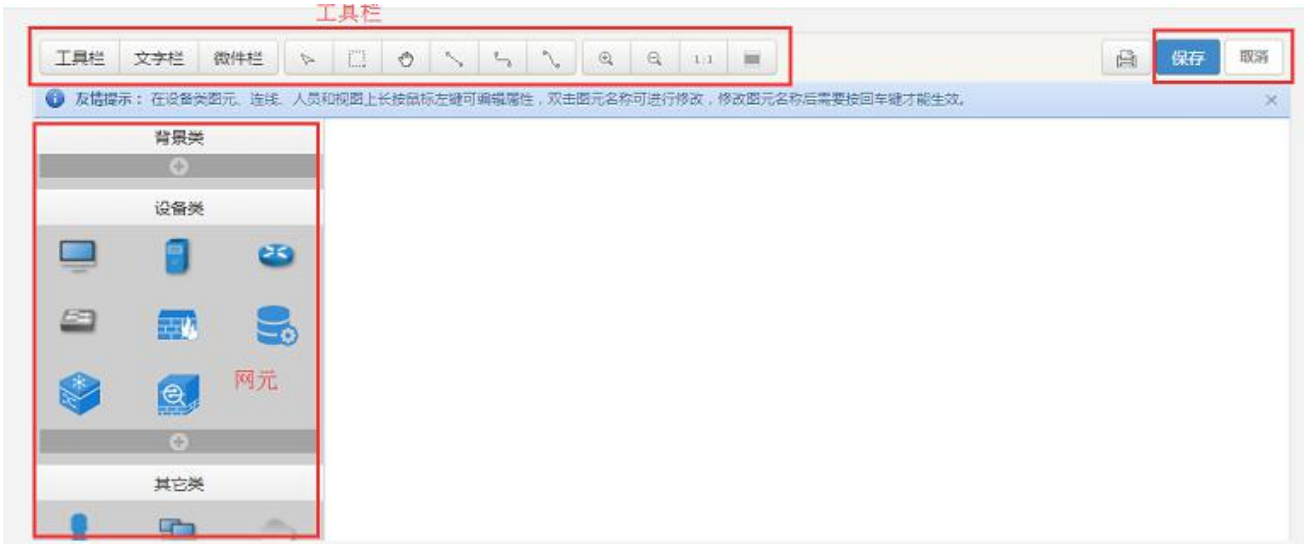


5.9 拓扑管理

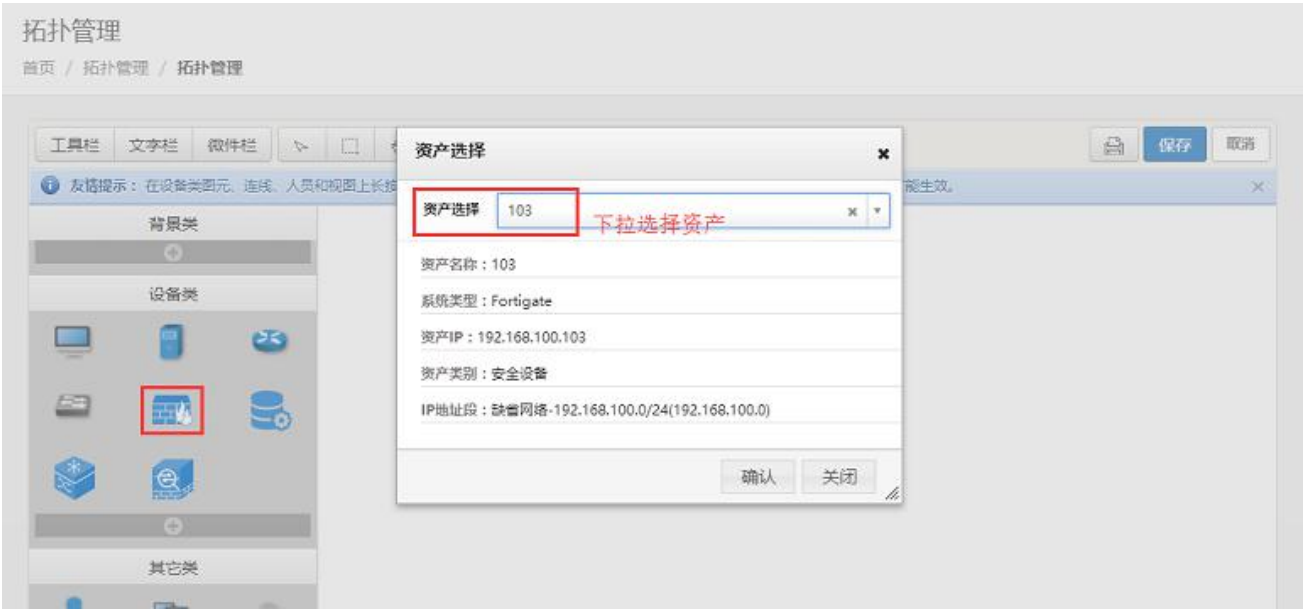
5.9.1 相关操作

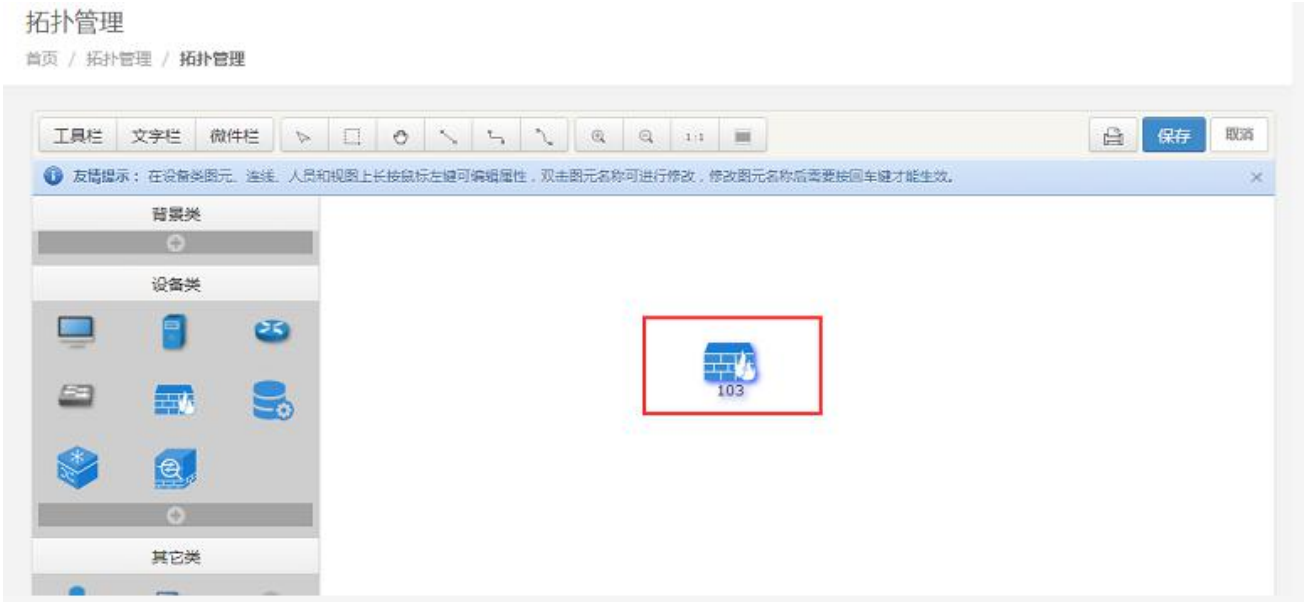
（1） 进入日志审计系统-》拓扑管理-》拓扑管理

（2） 点击“新增”按钮，进入拓扑图编辑页面



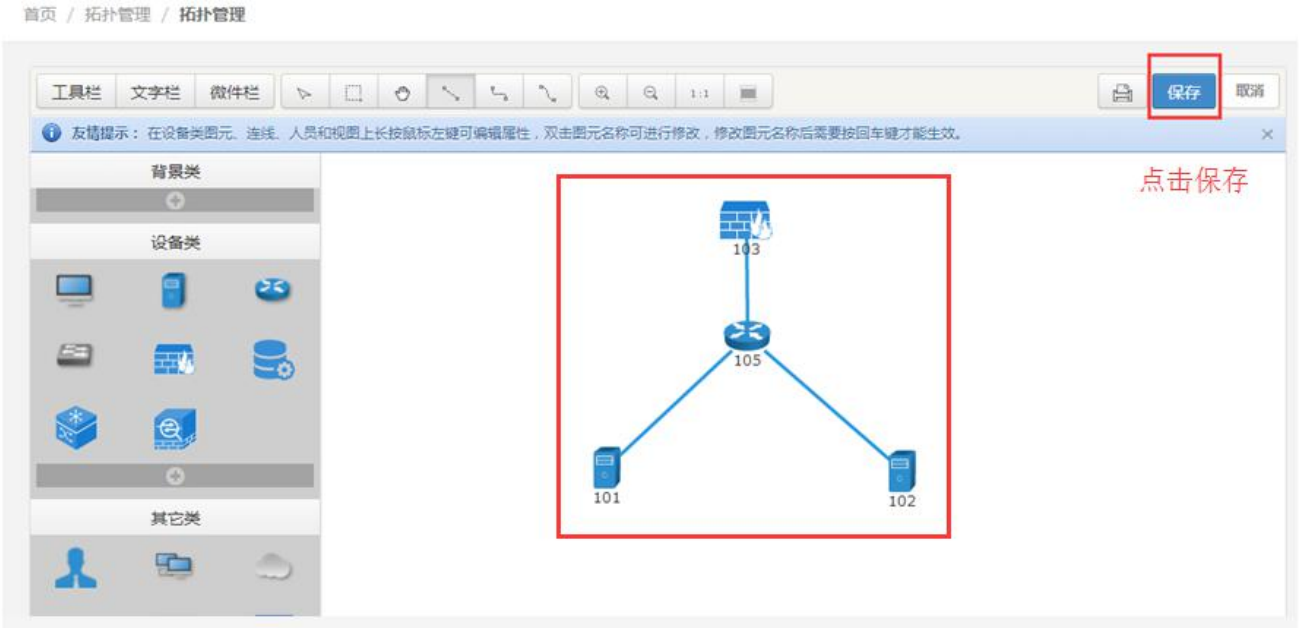
（3） 从左边网元里拖拽一个防火墙进入右边空白区域





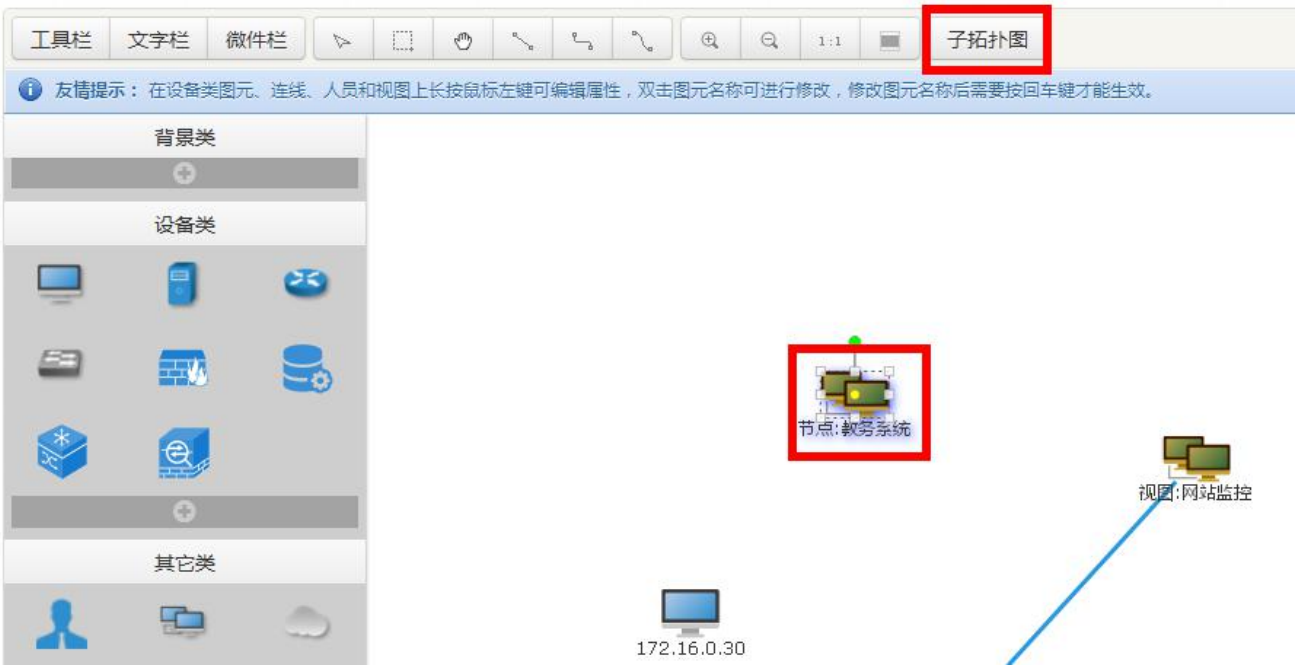
（4） 重复以上的方法，将 Linux 服务器、Tomcat、路由器创建出来

（5） 创建个设备间的关系

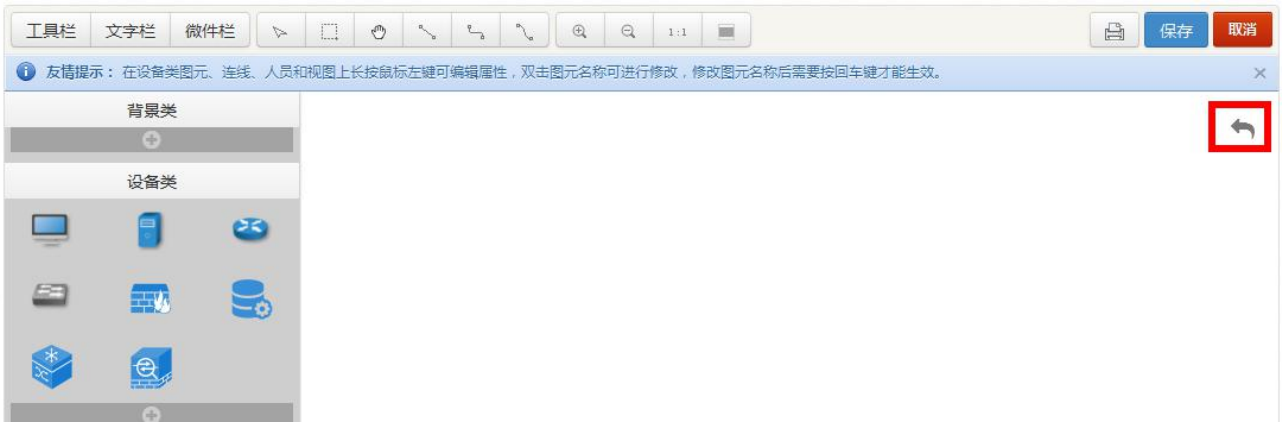


创建子拓扑

选择某个节点，单击，工具栏出现“子拓扑图”按钮

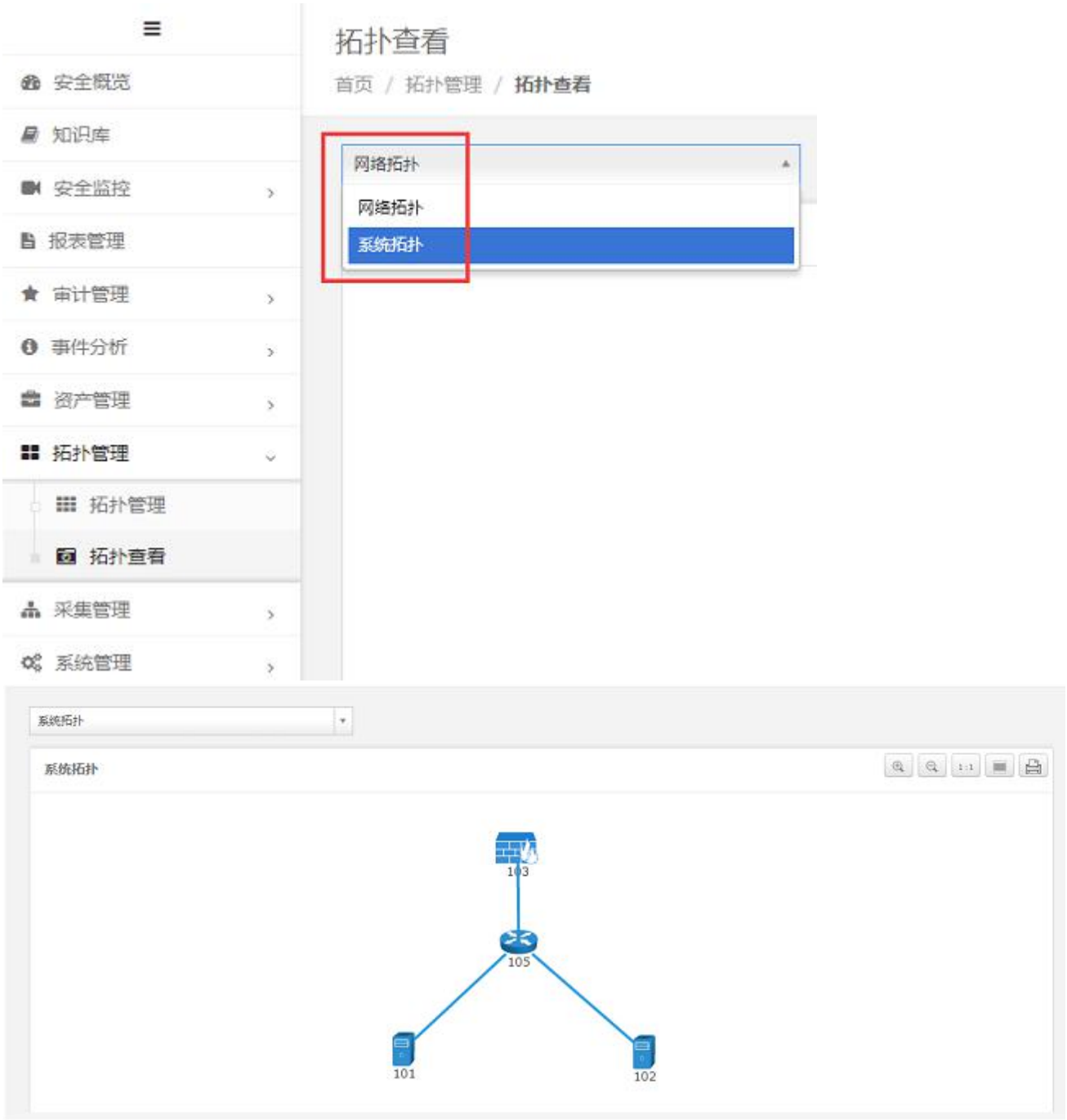


点击“子拓扑图”按钮，进入编辑页面，编辑方法参照之前流程；
子拓扑图右上角箭头为返回上一级。



（6） 拓扑查看

点击拓扑管理-》拓扑查看，选择创建的“系统拓扑”

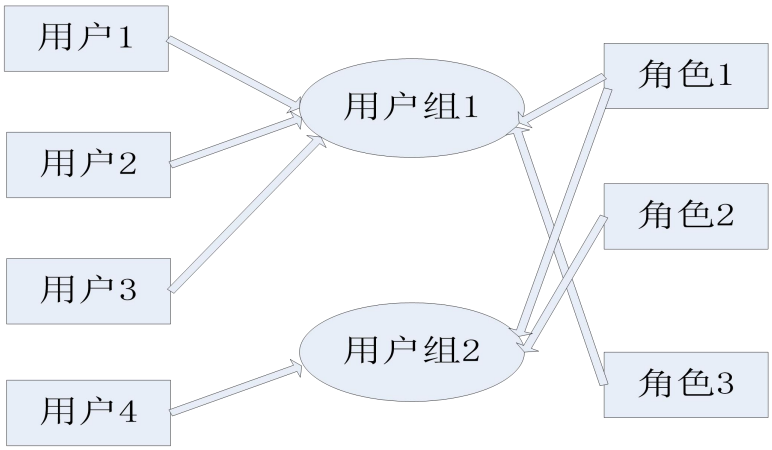


5.10 系统管理

日志审计系统的系统管理包括了各类系统自身管理的模块，包括用户管理、日志管理、系统参数、内置对象管理、升级管理、许可证管理。

5.10.1 用户管理

用户管理中包含用户管理、用户组管理、角色管理。一个用户只能属于一个用户组，一个用户组可以拥有多个角色。用户组与角色之间是多对多的关系。下图是一个权限的示意图：



5.10.1.1 角色管理

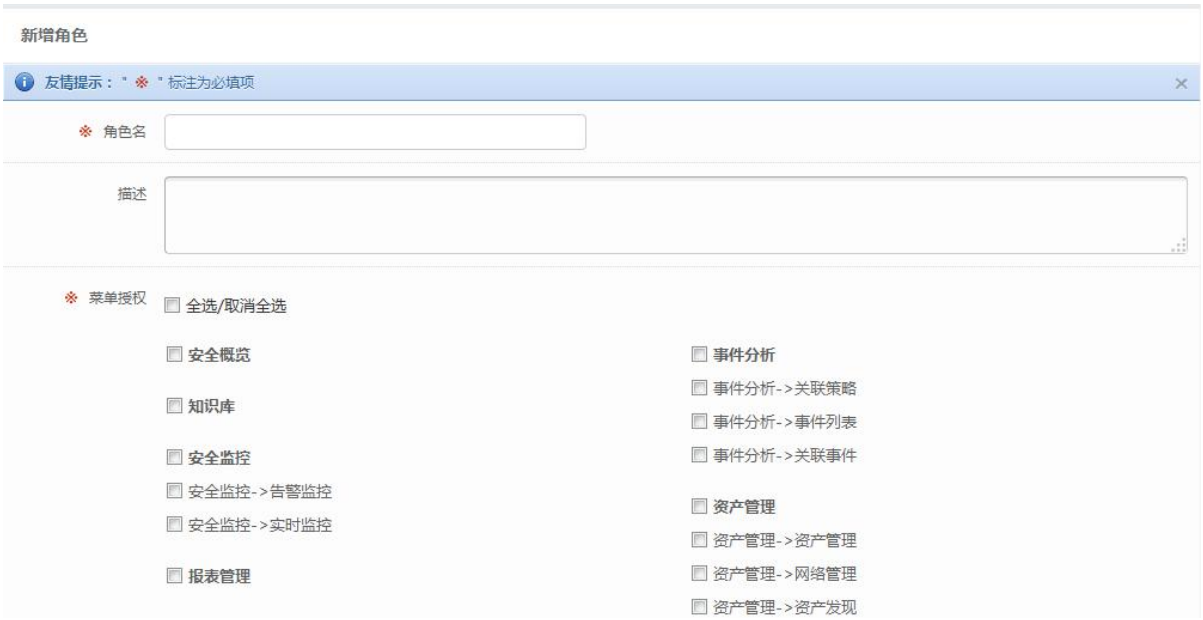
1. 列表查看：系统内置三个角色：安全管理员、安全审计员、系统管理员。

安全管理员对除了系统管理以外的所有菜单进行了功能授权。

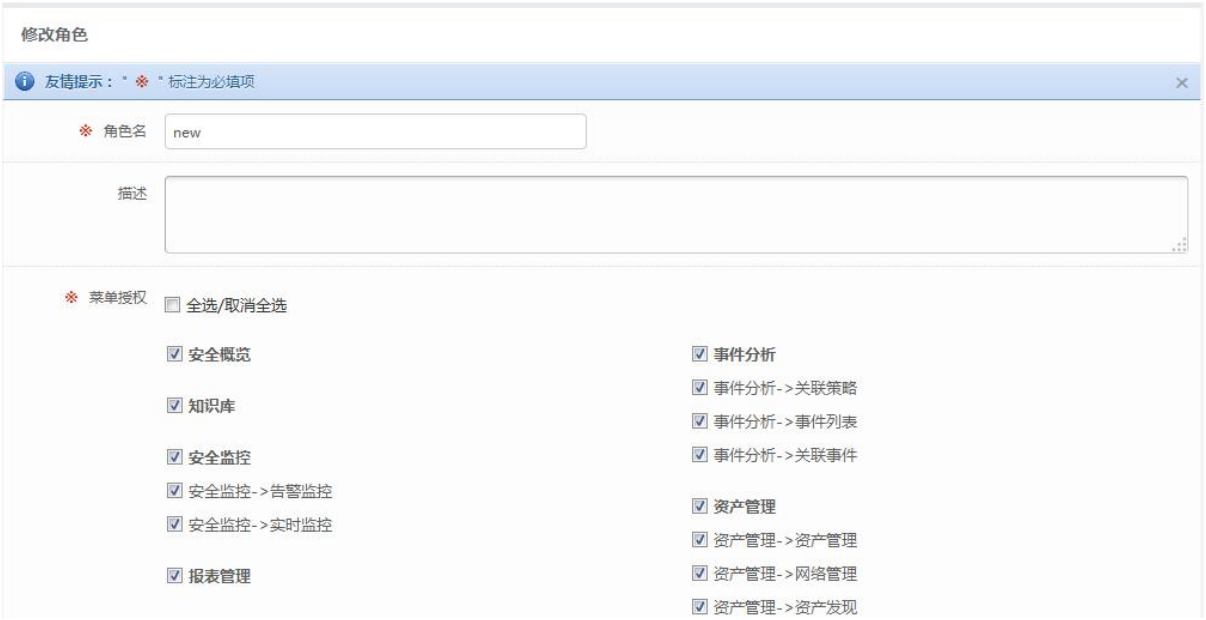
安全审计员只对日志管理菜单予以授权。

系统管理员仅对系统管理菜单下除日志管理以外的菜单予以授权。如下图所示：

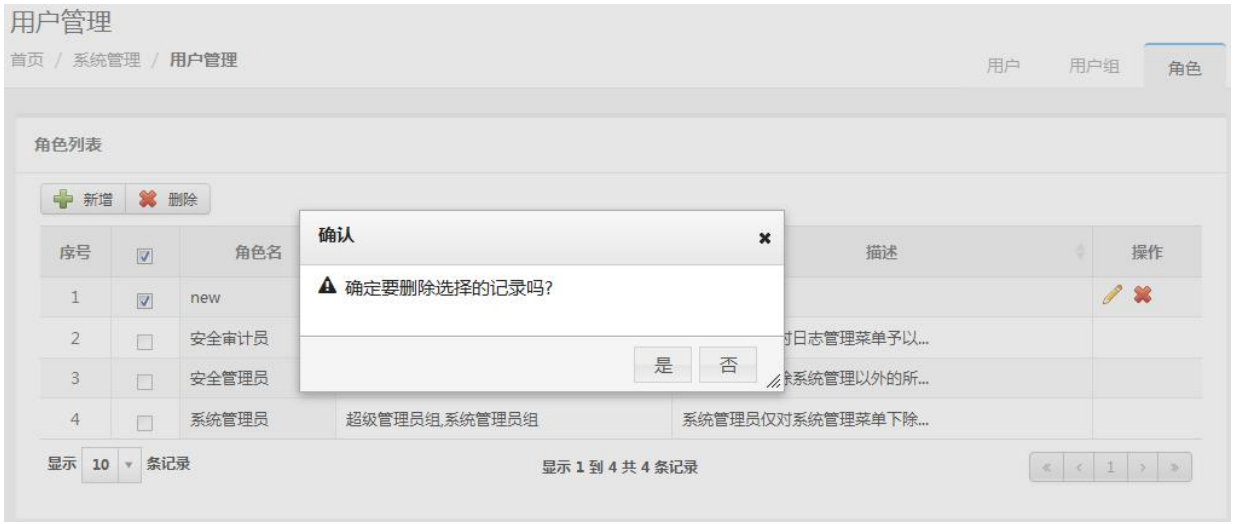
2. 新建角色：在新建角色页面中，输入角色名称，在菜单授权中勾选授权的项目，填写描述（可选）。菜单授权：以树状结构列出各个菜单及其下一级菜单。如下图所示：



3. 修改角色：用户可以修改角色的相关属性及授权定义。如下图所示：



4. 删除角色：用户可以选择删除一个或多个角色（系统正在使用的角色及系统内置的角色不可以被删除）。如下图所示：



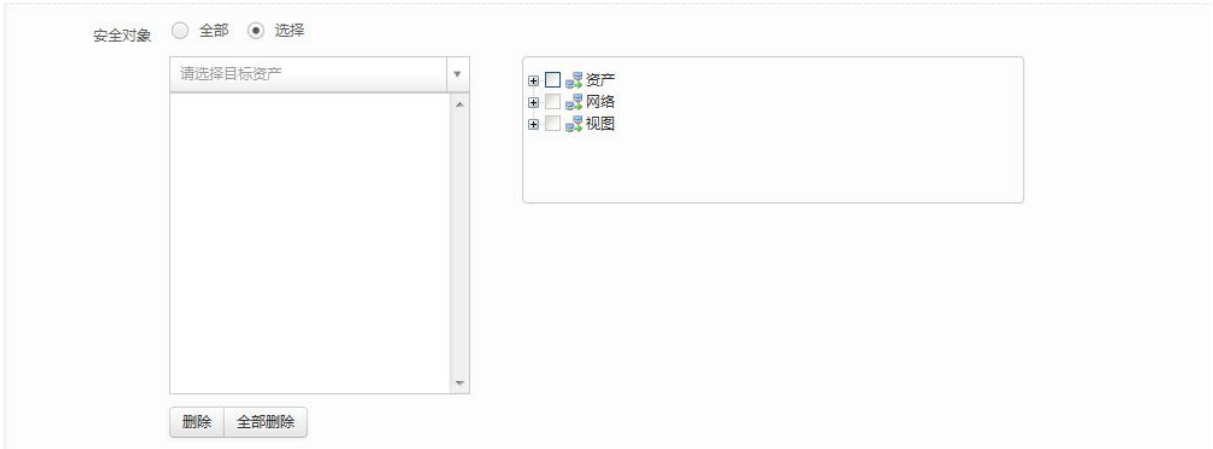
5.10.1.2 用户组管理

1. 用户组列表查看：系统内置四个用户组：超级管理员组（包含角色：安全管理员、安全审计员、系统管理员）、安全管理员组（包含角色：安全管理员）、安全审计员组（包含角色：安全审计员）、系统管理员组（包含角色：系统管理员）。如下图所示：

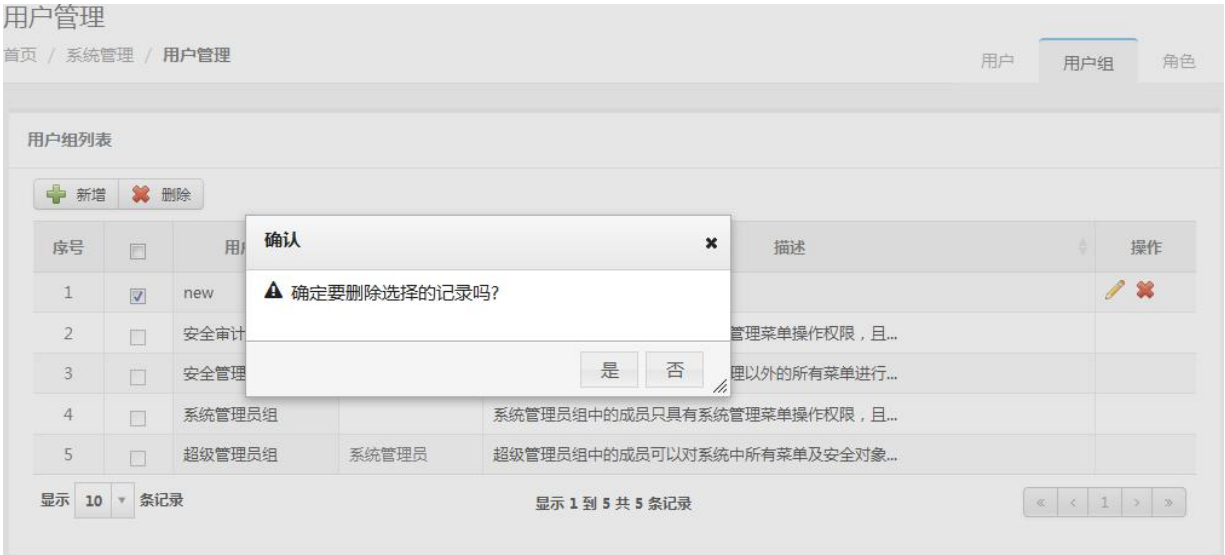
2. 新建用户组：输入用户组名称、描述（可填）、选择本系统角色授权（至少选一个，可以多选）；点击提交。如下图所示：

3. 修改用户组：修改用户组相关属性。如下图所示：

4. 安全对象授权：选择资产（根据视图选资产），可以具体到某一个具体的资产。如下图所示：



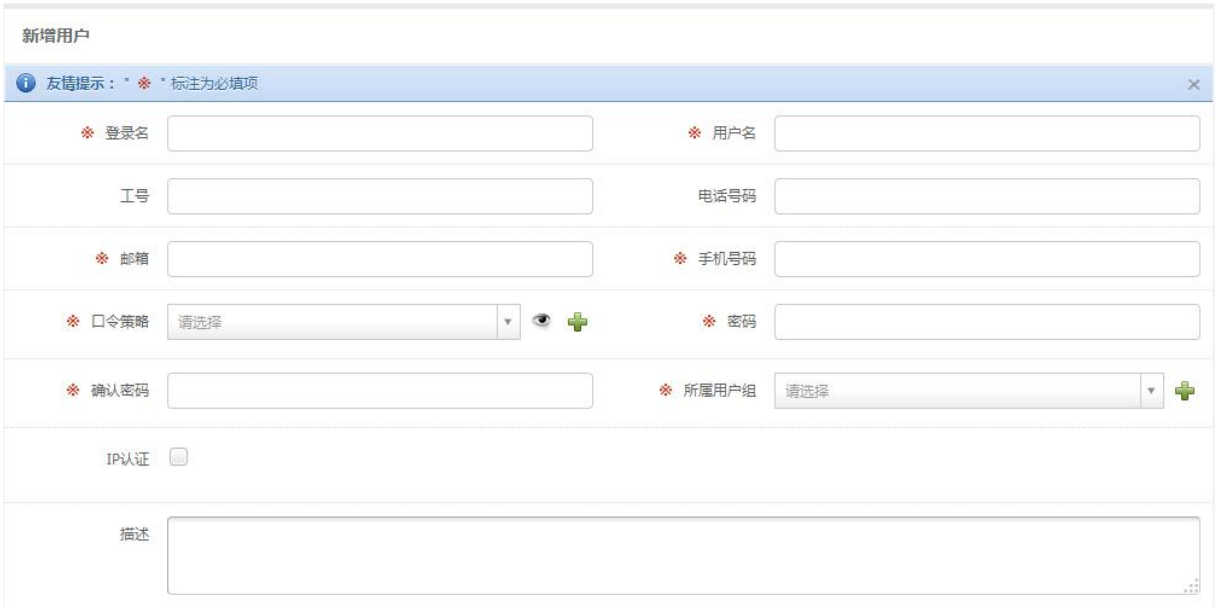
5. 删除用户组：删除用户选定的一个或多个用户组；如用户组中包含了用户则应提示用户先删除。如下图所示：



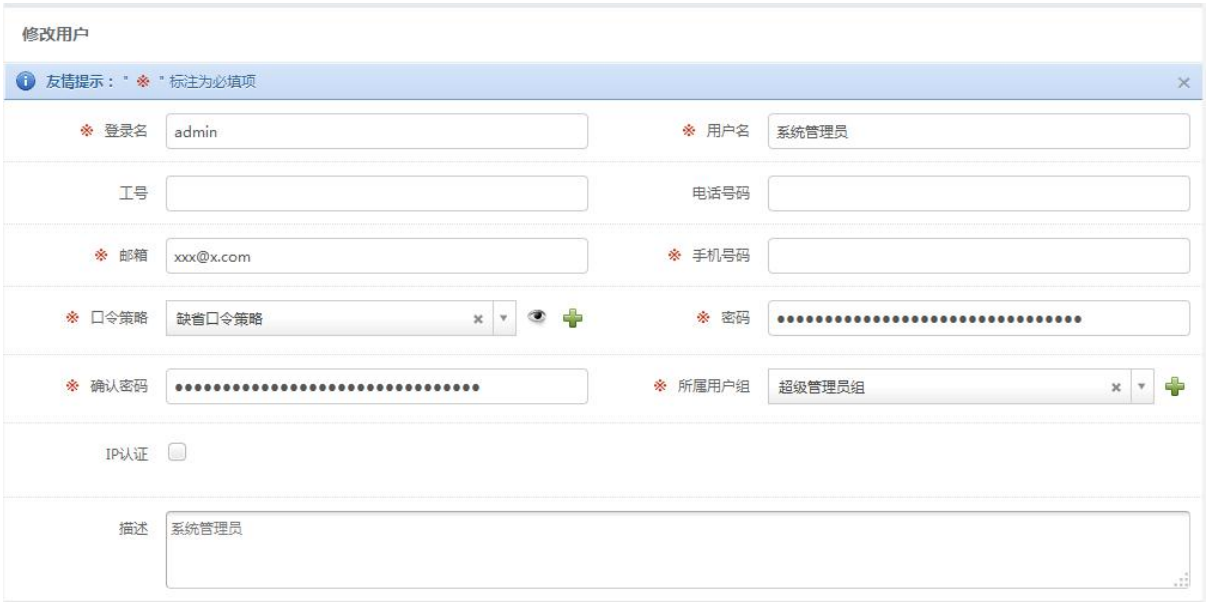
5.10.1.3 用户管理

1. 用户列表：点击用户管理系统默认显示用户列表页面，用户列表下显示系统内置用户（该用户属于超级管理员组）。用户列表上方显示新建、删除、解锁、查询操作按钮。如下图所示：

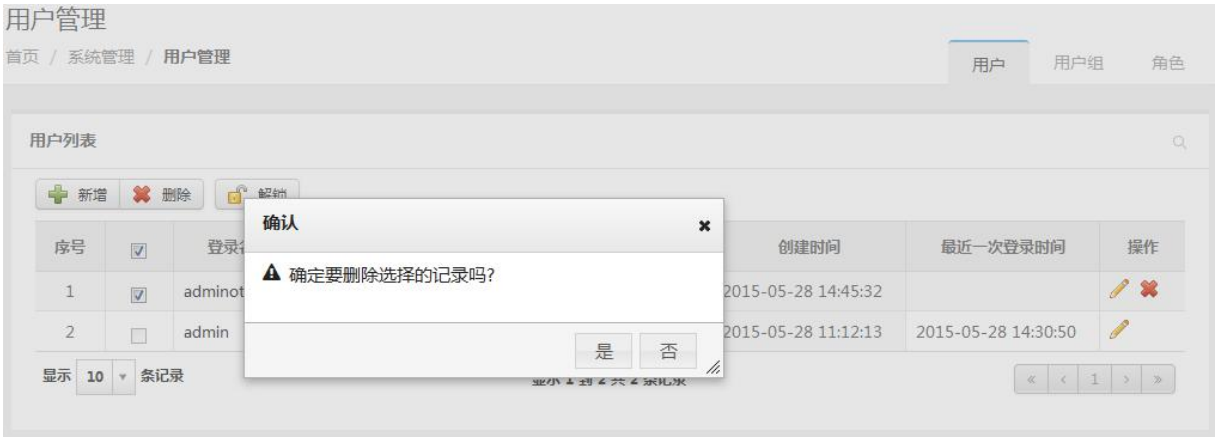
2. 新增用户：在新增用户页面，输入登录名、用户名、工号、电子邮箱、电话号码（可填可不填）、手机号码、IP 范围（可填可不填）、密码、确认密码（**如果系统设置为用户密码通过邮件发送则不显示上述两个输入**）、描述（可填可不填），选择口令策略、所属用户组（只能选一个）；用户只能属于一个用户组。用户密码的设置方式可以在系统参数菜单的用户密码获取方式中进行设置，设置方式有两种。一种是在新建用户页面设置，另一种是系统自动生成密码发送给用户（发送至用户新建时设置的邮箱地址）。如下图所示：



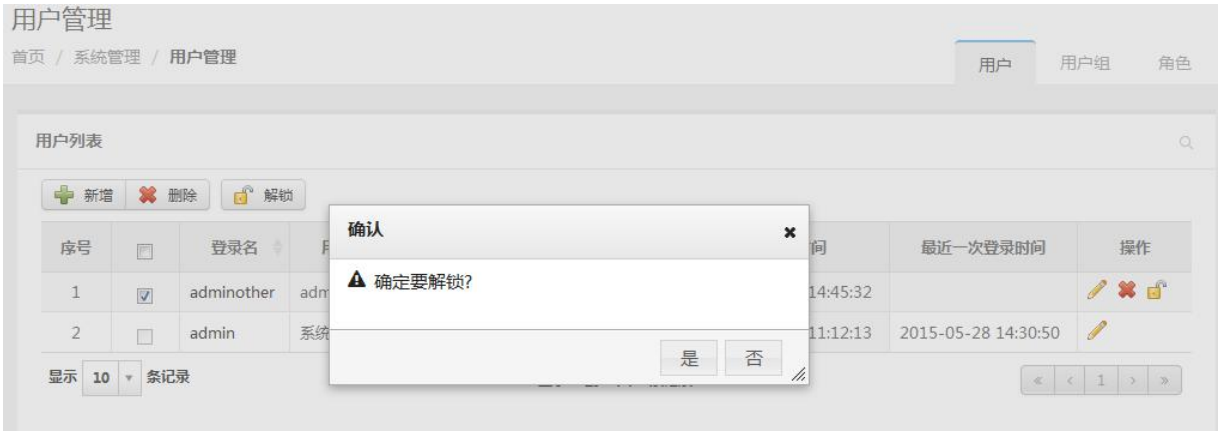
3. 修改用户：在修改用户页面，修改用户的相关属性。登录名、用户名、工号、电子邮箱、电话号码、手机号码、IP 范围、密码、确认密码、描述、口令策略、所属用户组。如下图所示：



4. 删除用户：删除用户选定的一个或多个用户，系统内置的用户不可以删除（admin）。如下图所示：



5. 用户解锁：在用户列表中，勾选需要解锁（锁定的原因是用户多次输错密码）的一条或多条用户信息点击“解锁”；要解锁用户的用户状态必须是锁定。如下图所示：

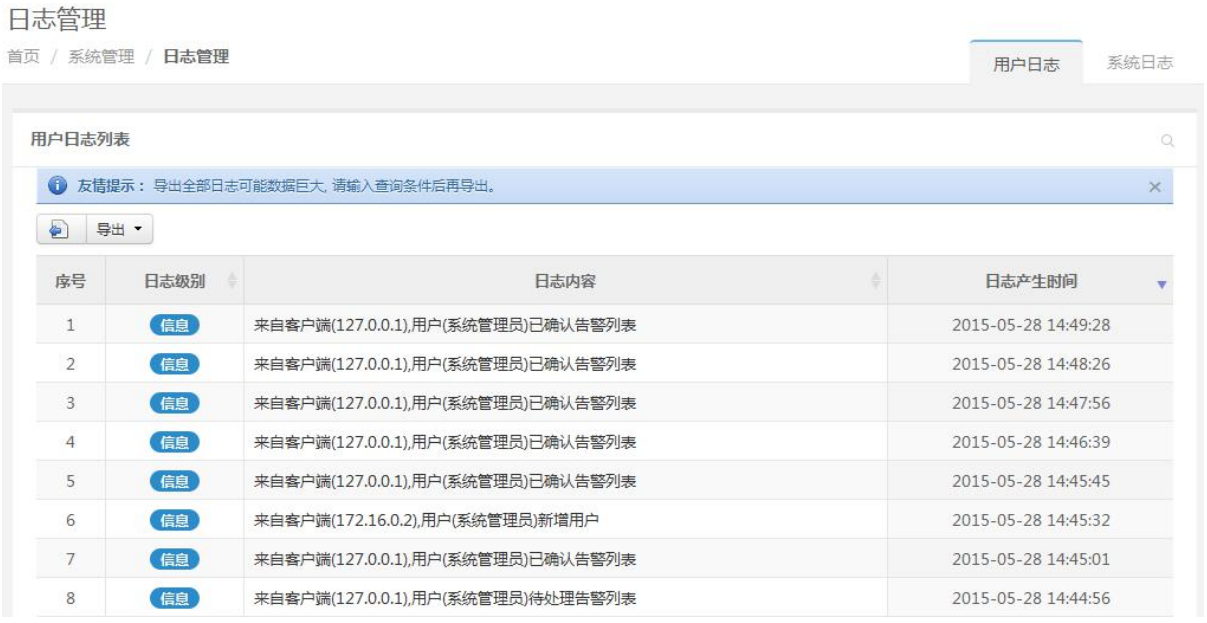


5.10.2 日志管理

日志审计系统中的日志管理是提供给用户查看、导出系统自身运行和操作日志的模块。

5.10.2.1 用户日志管理

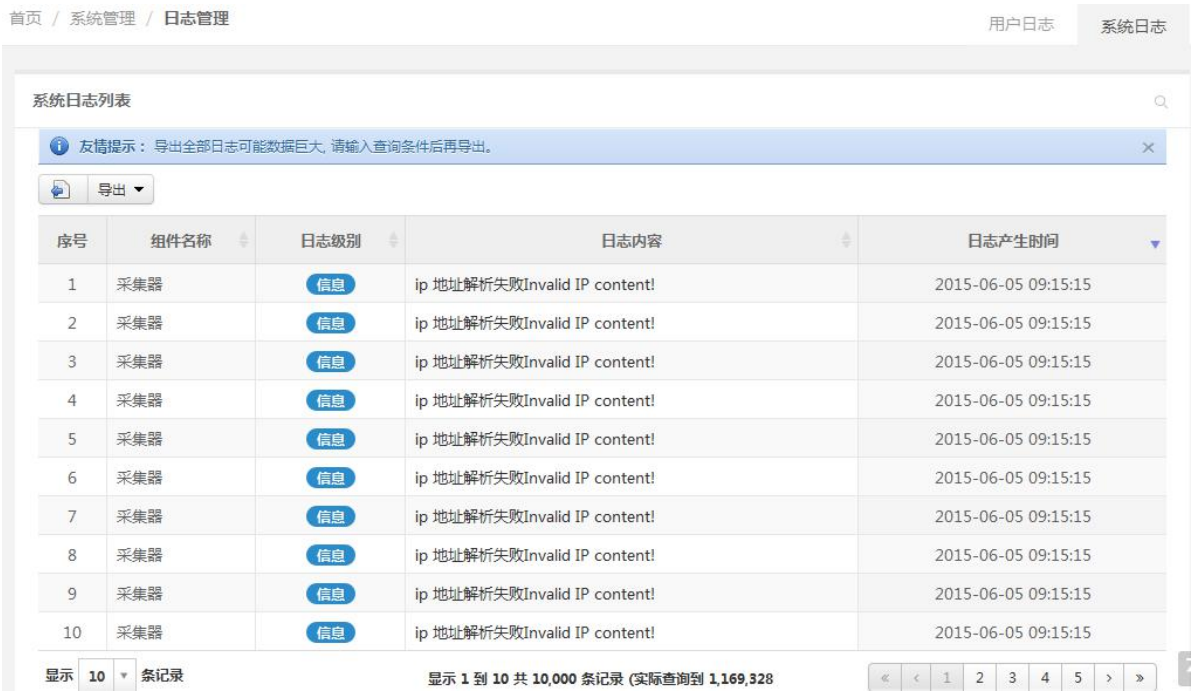
1. 用户日志查看和查询：查看和查询用户指定的日志，查询的条件包括客户端 IP、日志级别、日志产生时间。如下图所示：



2. 用户日志导出：用户可以将查询出的日志导出成文件，文件格式包括 PDF、Excel、Word；文件内容包括日志级别、日志内容、日志产生时间。如下图所示：

5.10.2.2 系统日志管理

1. 系统日志查看和查询：查看和查询用户指定的系统日志，查询的条件包括组件名称、日志级别、日志产生时间。如下图所示：



2. 用户日志导出：用户可以将查询出的日志导出成文件，文件格式包括 PDF、Excel、Word；文件内容包括组件名称、日志级别、日志内容、日志产生时间。如下图所示：

5.10.2.3 日志清理参数设置

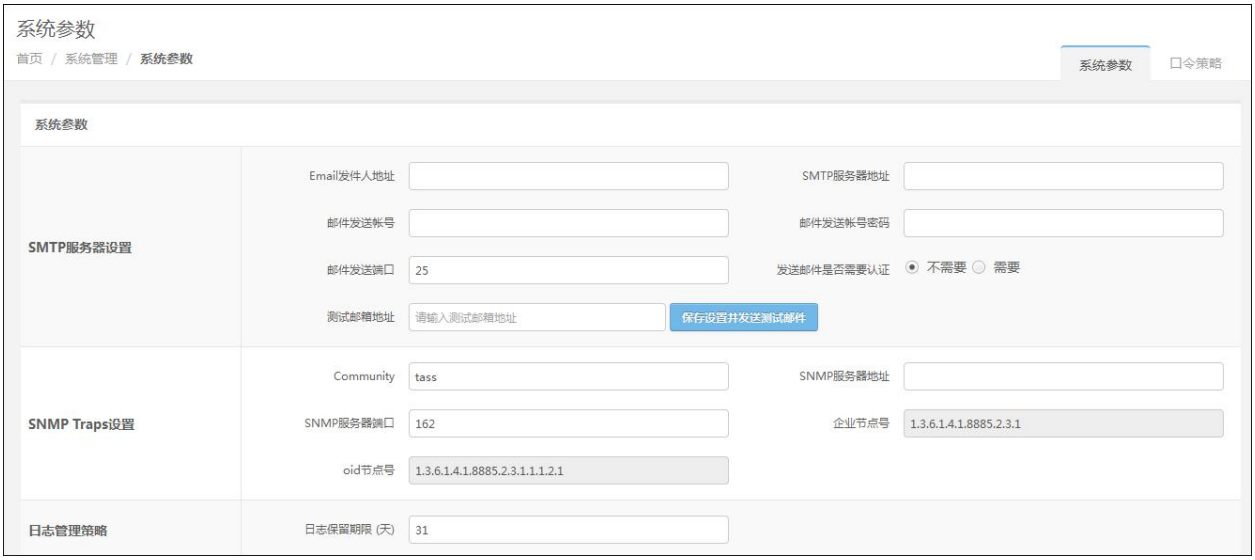
设置用户日志和系统日志保留天数（在系统参数管理中），默认为 31 天，即系统仅保留最近 31 天的日志，而会将 31 天之前的日志清除。如下图所示：

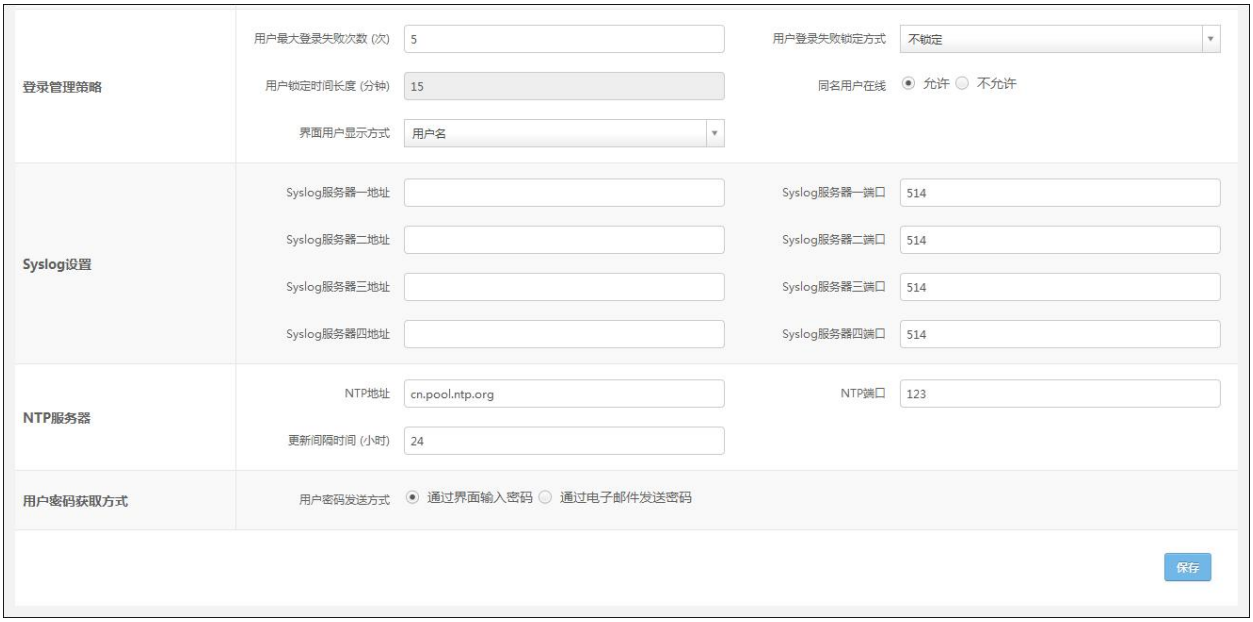
5.10.3 系统参数管理

5.10.3.1 系统参数

系统参数管理中包含了日志审计系统在运行中需要设置的一些参数。

系统参数中可以设定邮件服务器参数（IP 地址、端口等）、SNMP Trap 参数、Syslog 服务器（服务器地址、端口，支持 4 个）、NTP 服务器（地址、端口等）、登录密码允许错误次数（如 3 ~ 5 次）、锁定时间（如 5、15、30 分钟，即重鉴别功能）、是否允许同名用户在线（**即如一个用户已在线，那么同名的用户则不允许登录，直到前面的用户注销**）、用户密码获取方式（邮件还是界面设置）等，如下图所示：



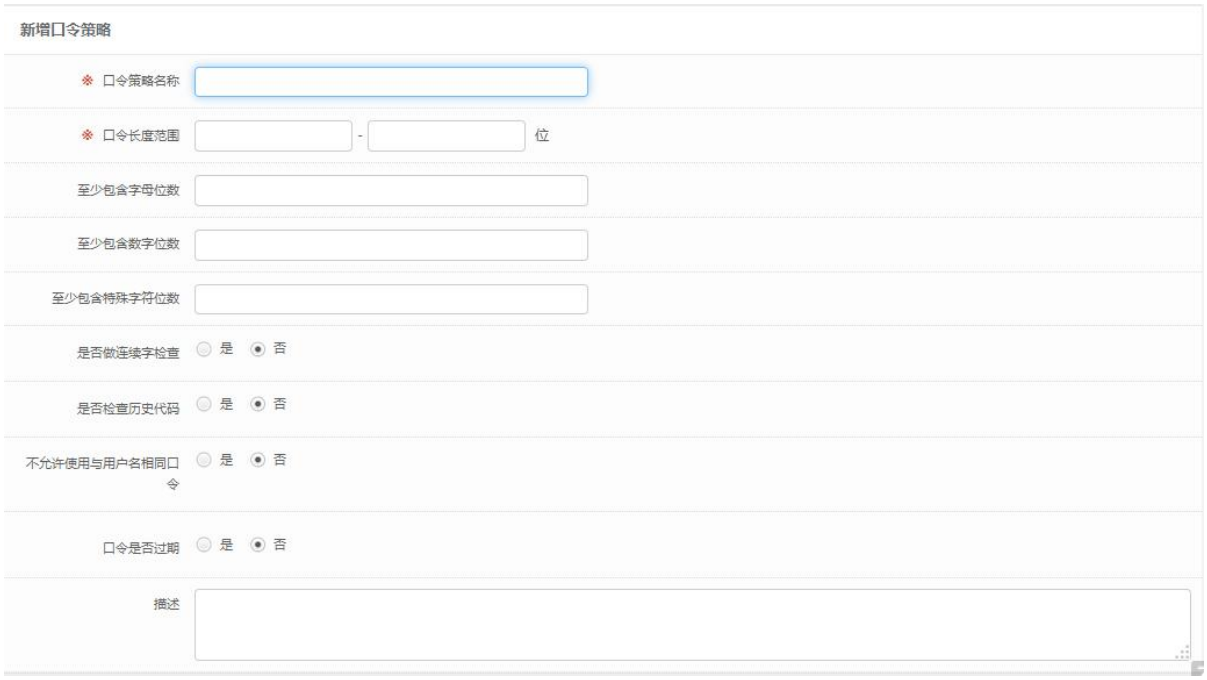


5.10.3.2 口令策略

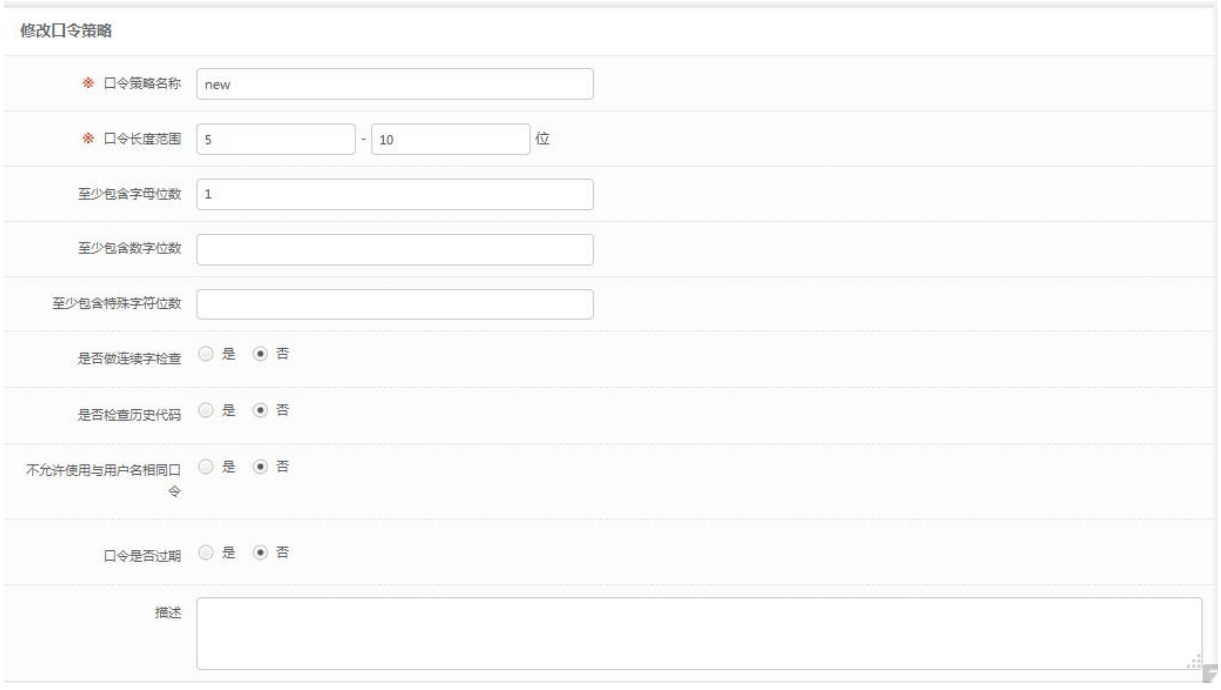
系统可以设定口令策略，用于在创建用户时针对不同的用户设置不同的口令策略。

1. 口令策略管理列表，系统内置了口令策略，如下图所示：

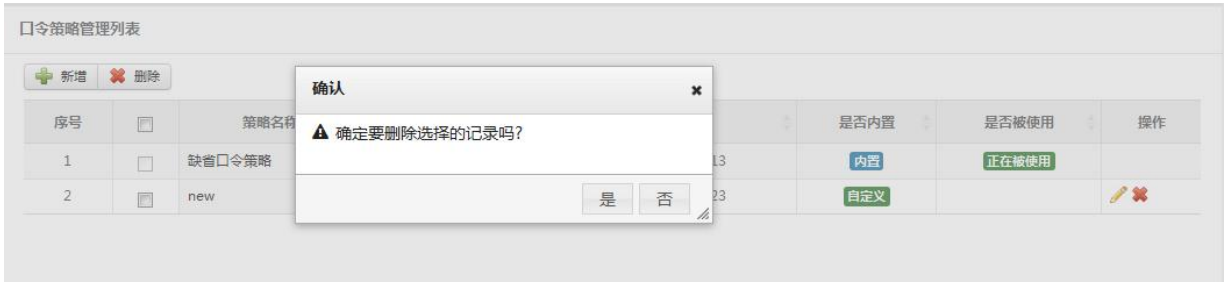
2. 新增口令策略：在新增页面，输入口令策略名称、口令长度范围、至少包含字母位数、至少包含数字位数、至少包含特殊字符位数、是否做连续字检查、是否检查历史代码、不允许使用与用户名相同的口令、口令是否过期、描述。如下图所示：



3. 修改口令策略：在修改页面，修改口令策略的相关属性，系统内置的口令策略不允许修改。口令策略名称、口令长度范围、至少包含字母位数、至少包含数字位数、至少包含特殊字符位数、是否做连续字检查、是否检查历史代码、不允许使用与用户名相同的口令、口令是否过期、描述。如下图所示：



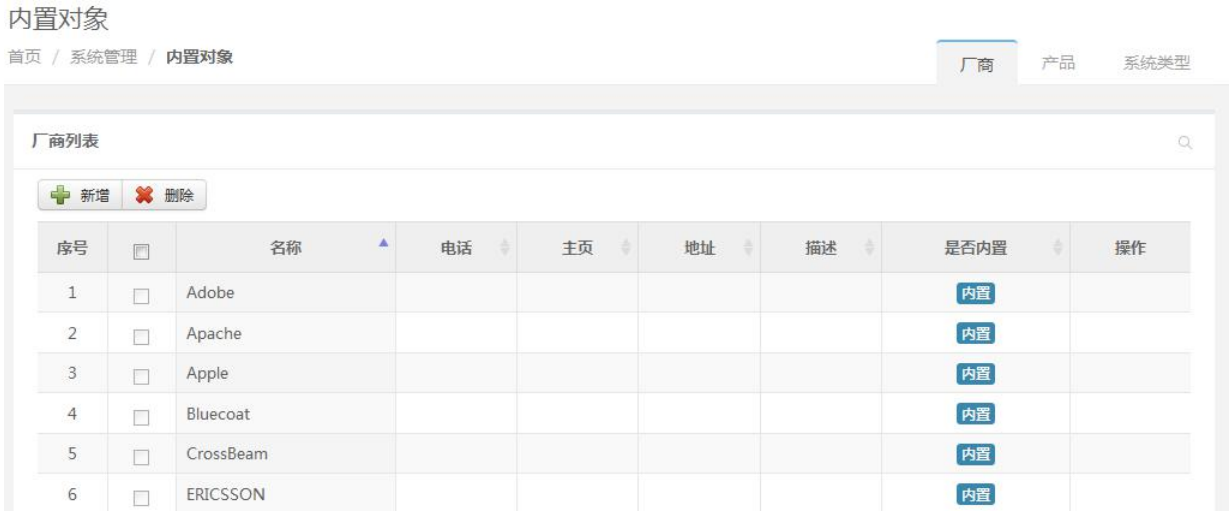
4. 删除口令策略：删除口令策略选定的一个或多个口令策略，系统内置的口令策略和被引用的口令策略都不可以删除。如下图所示：



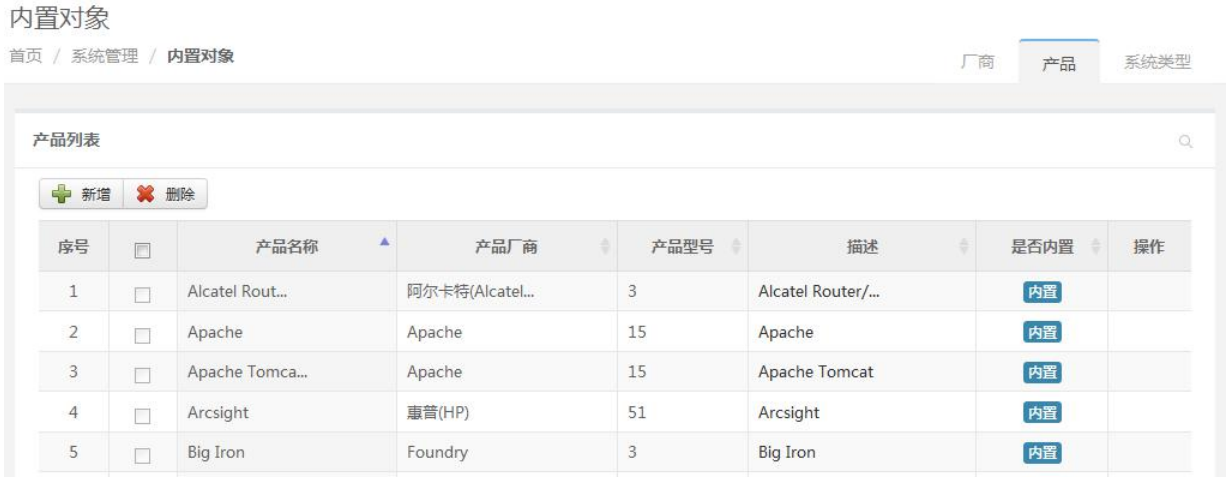
5.10.4 内置对象管理

内置对象管理包括：

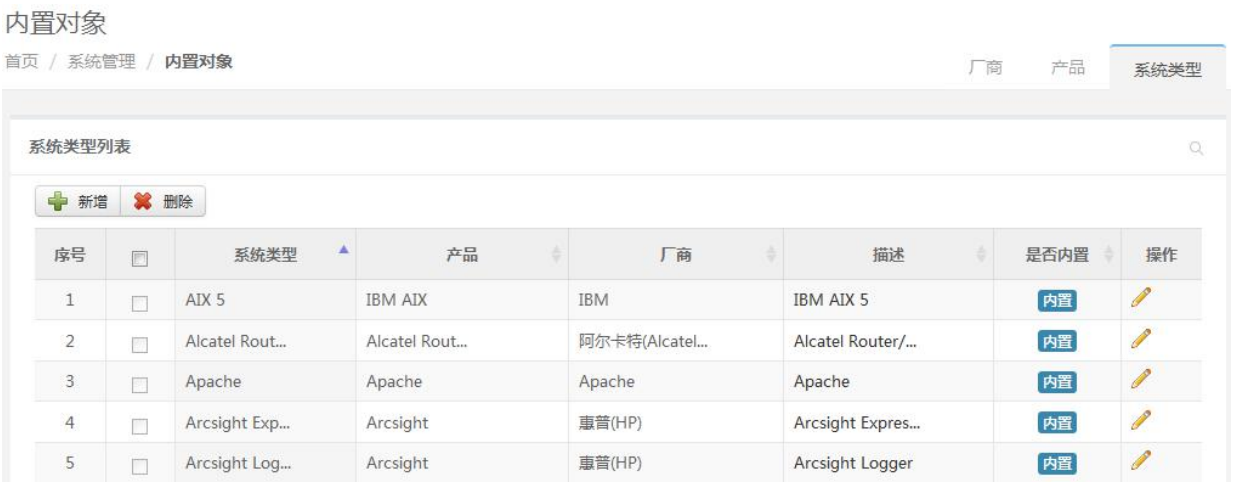
1. 厂商管理：维护厂商信息，如 Oracle、微软等，如下图所示：



2. 产品管理：维护产品信息，它和厂商之间有关联关系；产品如 Windows（厂商是微软）、AIX（厂商是 IBM）等，如下图所示：



3. 系统类型管理：维护某种产品的不同系统版本，如 Windows7、AIX 5.2，如下图所示：



5.10.5 升级管理

用户可以从正规渠道获得系统升级包，然后在日志审计系统的系统管理->升级管理中导入升级包，系统会记录升级的记录。升级管理如下图所示：

5.10.6 许可证管理

用户可以查看和升级系统许可证；许可证包括客户名称、主机标识码、有效期、设备数（包括资产和非资产）、采集控制器数量、性能参数，如下图所示：

5.11 其它

5.11.1 安全概览

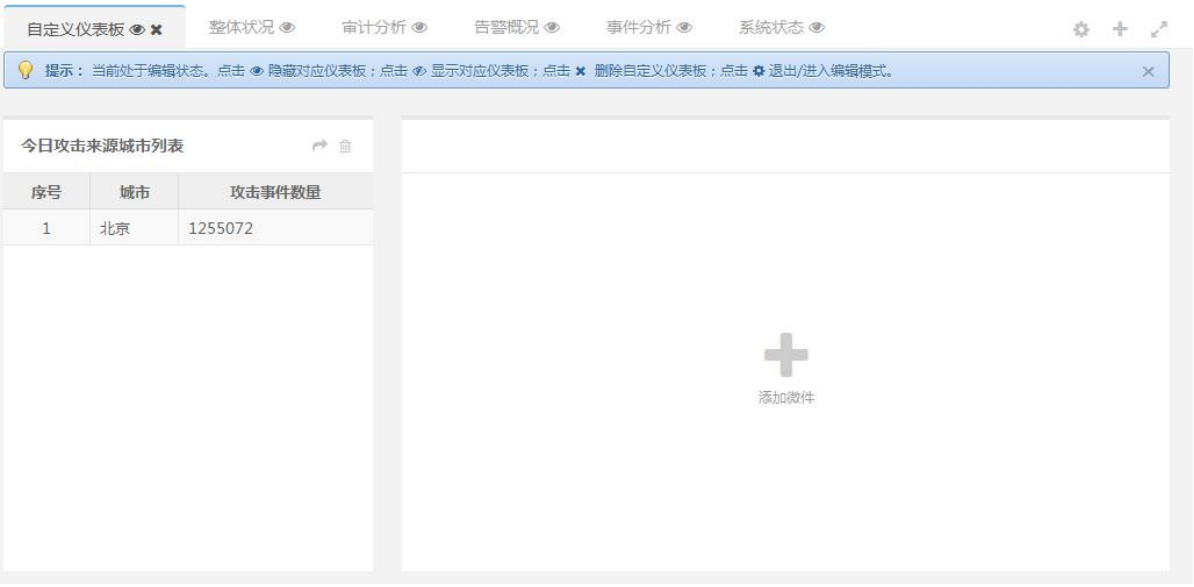
安全概览是日志审计系统风险的集中展示区域，也是日志审计系统展现给用户的第一个视觉界面；它支持以 TAB 页及微件（Widget）形式展现，用户也可对仪表的布局和内容进行调整。

Tab 页面，主要指一级菜单下的 web 分类页面，不需要刷新整个页面而分别显示不同内容。

微件（Widget），主要指 Tab 页面中，用来显示的各种仪表、图表等。

安全概览应能支持用户自定义布局和展现内容。仪表板应根据权限和许可证情况进行展示；仪表板提供 TAB 管理功能，管理的内容主要有：

1. TAB 的添加、删除、排序、全屏显示，排序是调整 TAB 的先后顺序。
2. TAB 中微件的添加、删除、隐藏，如下图所示：

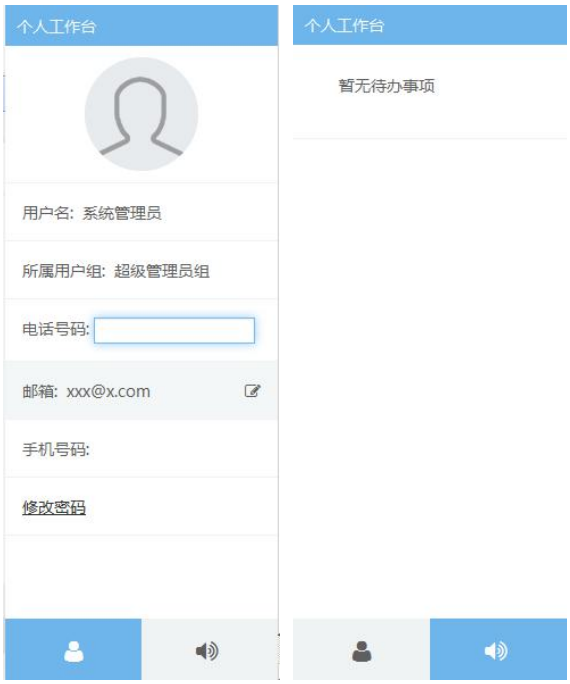


5.11.2 个人工作台

个人工作台是登录用户用于便捷操作的窗口，可以通过点击登录用户头像打开，主要包含了与登录用户相关的一些信息，其功能主要包括：

1. 个人信息的显示及修改。
2. 个人待办事宜：需处理的告警。

如下图所示：



5.11.3 全文检索

由于日志审计系统涉及到的安全数据或安全问题较多，为了便于操作，系统提供了一个全文检索功能。能对系统内的对象提供全文检索功能，对于海量数据的检索可限定检索时间段（主要针对安全事件）。

全文检索的检索范围主要有：

1. 资产
2. 告警
3. 事件
4. 知识库
5. 用户

如下图所示：

附录 1 专家模式查询语法

安全事件的专家模式查询语法比较类似于逻辑表达式（安全事件字段参见上表），如下：

1. 字符型的字段：关键字或*匹配，以”“括起（建议不要使用*，这样会显著降低查询效率），

   如：*EventName: “complication error”*

2. 数值型的字段：数字或区间（开区间：{}，闭区间:[]），查询多个以逗号隔开，如：

   DeviceAddress: [TO 5} AND Severity:[3,4]*

3. 可以设置权重来显示优先搜索结果（权重范围 1-2，默认是 1，建议保留小数，权重越大，

   越优先显示）：*EventName: complication^1.6*

4. 与（AND）、或（OR）和非（NOT）的联合查询：

   DeviceAddress:”192.168.100.2” OR EventName:“complication” NOT message:”error”

示例 1：搜索详细信息字段的“close failed”并且可信度字段的“>50”。

*Message: close failed AND Reliability：{50 TO *}*

示例 2：搜索严重级别字段的值为“1”（低级）并且详细信息字段为“close failed”或者产品名称为“Windows”的所有信息。

Severity:1 AND Message:“close failed” OR ProductName:”Windows”