

铱迅日志审计系统

管理员手册



南京铱迅信息技术股份有限公司

Nanjing YXLink Information Technology Co. Ltd.

注意

- 未经南京铱迅信息技术股份有限公司 (Nanjing Yxlink Information Technology Co.,Ltd., 简称: 铱迅信息) 的事先书面许可, 对本产品附属的相关手册之所有内容, 不得以任何方式进行翻版、传播、转录或存储在可检索系统内, 或者翻译成其他语言。
- 本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其所提到之产品信息, 所引起直接或间接的数据流失、利益损失或事业终止, 铱迅信息不承担任何责任。
- 铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利, 而无须事先通知。
- 本公司已竭尽全力来确保手册内载信息的准确性和完善性。如果您发现任何错误或遗漏, 请向铱迅信息反映。对此, 我们深表感谢。

商标信息

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一一列明。

目录

目录.....	3
1. 概述.....	6
1.1. 日志审计的必要性.....	6
1.2. 日志审计系统.....	7
2. 日志审计系统架构和运行环境.....	7
2.1. 总体架构.....	7
2.2. 运行环境.....	8
3. 主要业务及流程.....	8
3.1. 采集管理.....	9
3.2. 资产管理.....	9
3.3. 事件分析.....	9
3.4. 审计管理.....	10
3.5. 安全监控.....	10
3.6. 报表管理.....	10
4. 基础功能.....	11
4.1. 功能概述.....	11
4.1.1. 什么是日志.....	11
4.1.2. 日志是如何采集的.....	11
4.1.3. 什么是安全事件.....	12
4.1.4. 标准化.....	12
4.1.5. 什么是过滤和归并.....	13
4.2. 初次使用.....	13
4.3. 向导.....	14
4.4. 采集管理.....	15
4.4.1. 相关操作.....	15
4.5. 资产管理.....	23
4.5.1. 什么是安全资产.....	23
4.5.2. 安全资产的属性.....	23
4.5.3. 什么是网络.....	24
4.5.4. 什么是资产视图.....	24
4.5.5. 相关操作.....	24

4.6. 事件分析.....	28
4.6.1. 安全事件的关联.....	28
4.6.2. 相关操作.....	30
4.7. 审计管理.....	38
4.7.1. 什么是审计.....	38
4.7.2. 相关操作.....	38
4.8. 安全监控.....	62
4.8.1. 什么是告警.....	62
4.8.2. 告警的级别.....	62
4.8.3. 告警的处理.....	63
4.8.4. 什么是实时监控.....	63
4.8.5. 相关操作.....	63
4.9. 报表管理.....	68
4.9.1. 相关操作.....	68
4.10. 知识库管理.....	73
4.10.1. 知识库有哪些分类.....	73
4.10.2. 相关操作.....	74
4.11. 系统管理.....	76
4.11.1. 用户管理.....	76
4.11.2. 日志管理.....	84
4.11.3. 系统参数管理.....	86
4.11.4. 内置对象管理.....	89
4.11.5. 升级管理.....	91
4.11.6. 许可证管理.....	91
4.12. 其它.....	92
4.12.1. 安全概览.....	92
4.12.2. 个人工作台.....	93
4.12.3. 全文检索.....	93

获得帮助

获取网络安全相关资料可以访问铱迅信息网站：<http://www.yxlink.com>

获取铱迅日志审计系统的最新相关信息可以访问网址：

<http://www.yxlink.com/products-waf.html>

如需获取更详尽的铱迅信息网络安全专业服务信息、商务信息，您可通过如下方式和我们取得联系：

地址：江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

邮编：210012

服务热线：400-097-5557

电话：025-83235296, 025-83235396, 025-58722055

传真：025-83235296, 025-83235396 转 601

网站：<http://www.yxlink.com>

Email：info@yxlink.com

格式与名词约定

设备、产品、系统——除非特指，本手册中均表示铱迅日志审计系统。

1. 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审计系统；另外，各组织或企业部署集中日志审计系统的意义在于：

- 它是信息安全管理需要：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。日志审计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，并且周期性地地进行第三方审计。

1.2. 日志审计系统

日志审计系统是南京铨迅信息技术股份有限公司独立研制的、拥有自主知识产权的新一代日志处理和分析的系统。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。

日志审计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。

通过日志审计系统，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。

2. 日志审计系统架构和运行环境

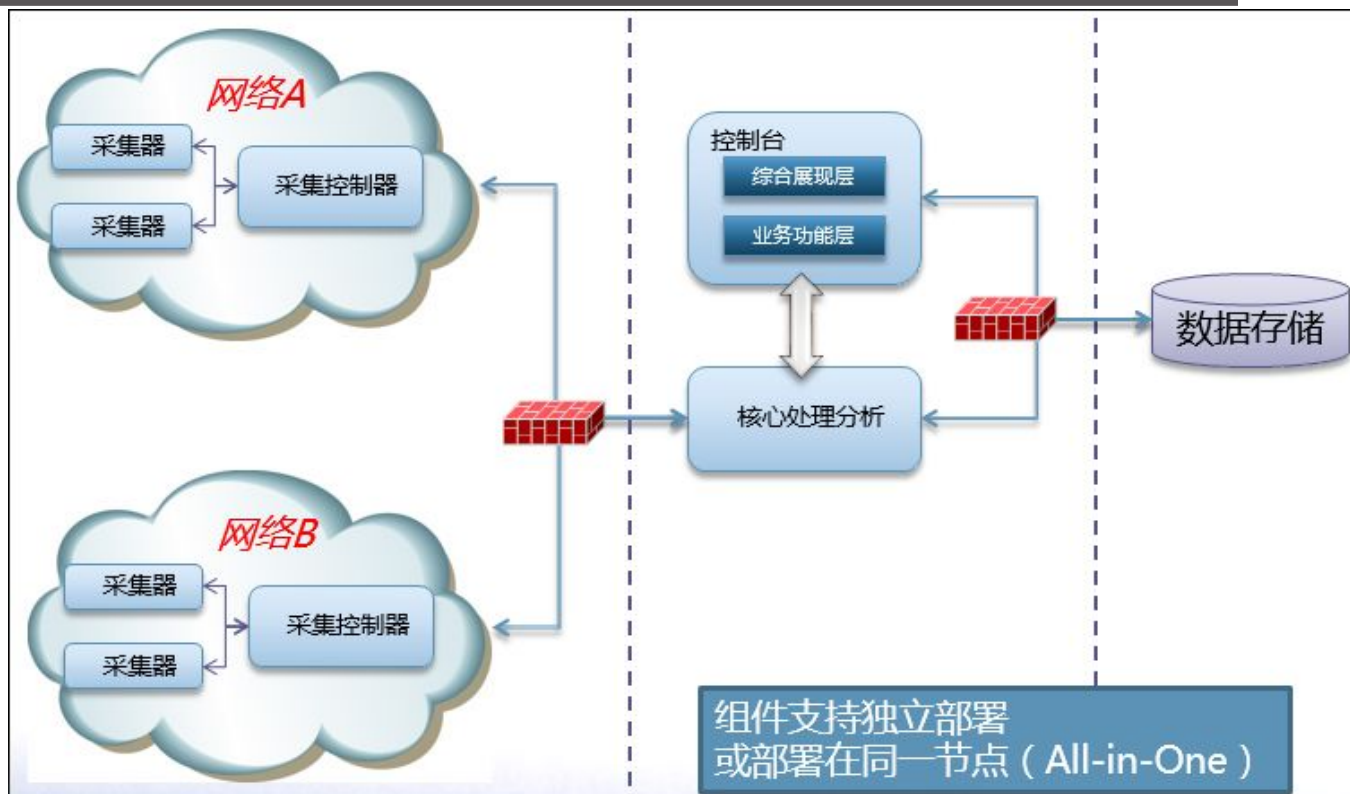
2.1. 总体架构

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：



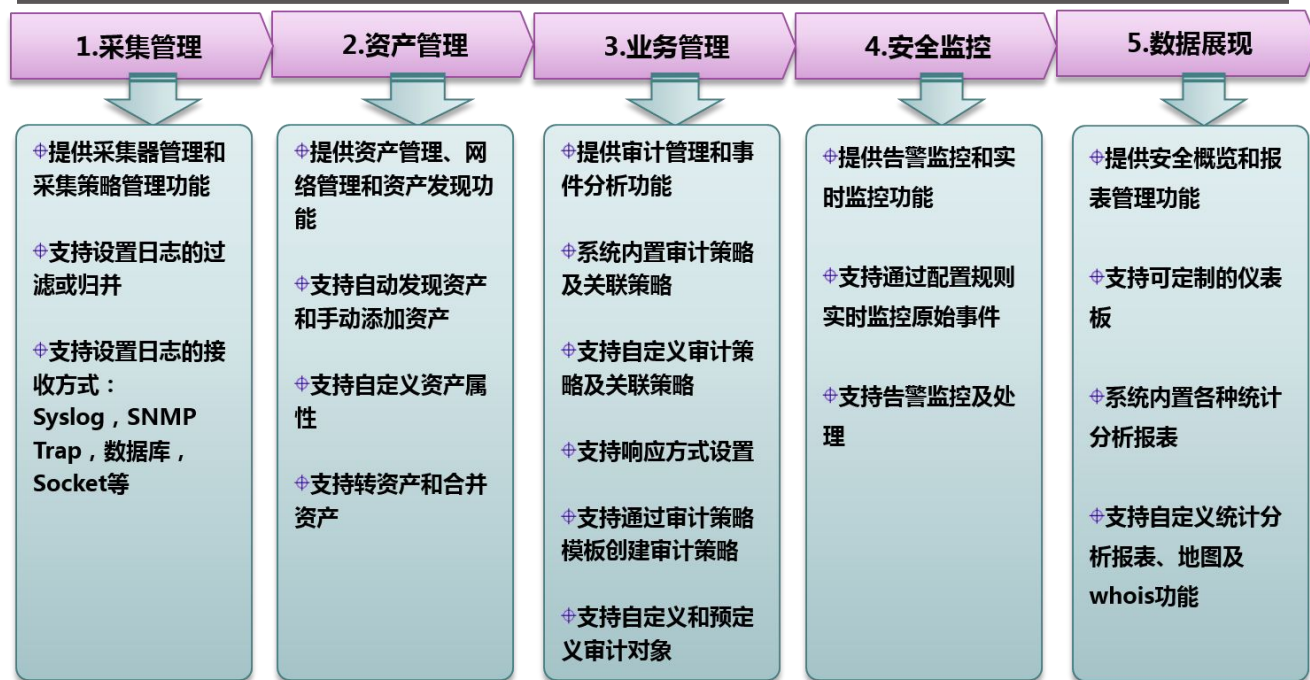
本文主要描述的是管理控制（控制台）的相关主要功能，关于系统的安装部署、核心处理分析及采集控制部分请参看“日志审计系统 V2 产品安装手册 V1.0”、“日志审计系统 V2 产品管理员手册 V1.0”。

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 IE10（含）以上浏览器查看系统。

3. 主要业务及流程



3.1. 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。

3.2. 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。

日志审计系统中的关联、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。

3.3. 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。

3.4. 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。

3.5. 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。

3.6. 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。

4. 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。

4.1. 功能概述

在铱迅信息日志审计系统，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、系统管理等子系统组成。

4.1.1. 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。

4.1.2. 日志是如何采集的

铱迅信息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；日志审计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，传送到安全运营中心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

4.1.3. 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。

4.1.4. 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，故在安全运营中心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

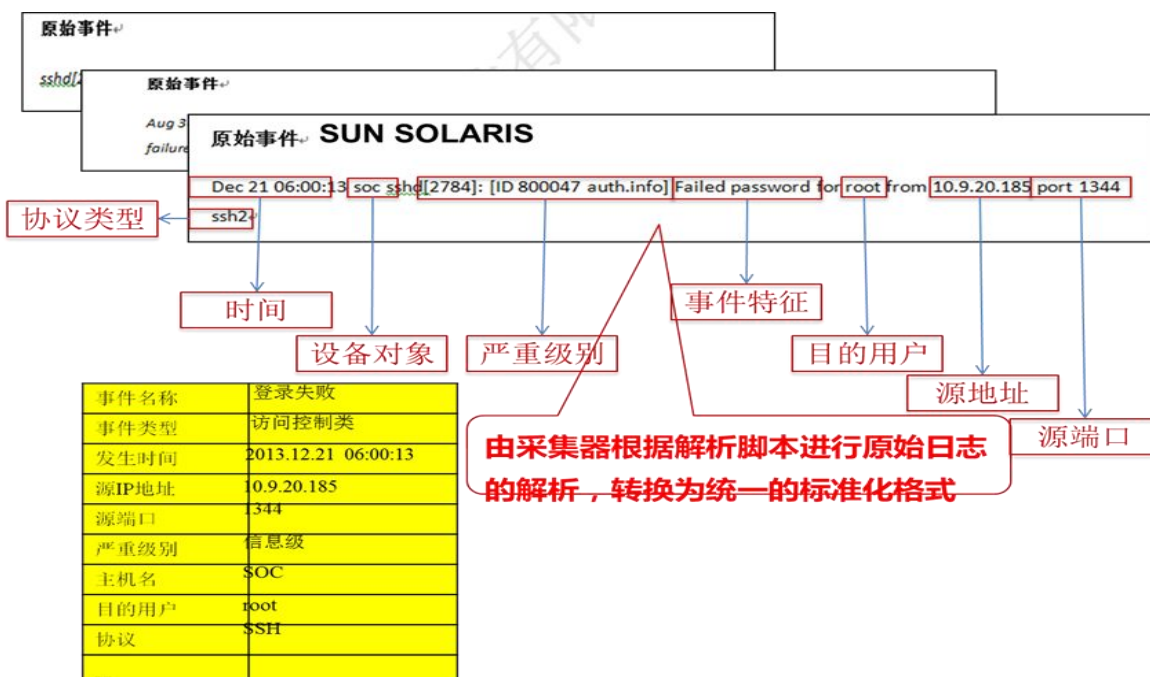
Aug 27 13:04:09 sshd[3228]: [ID 70112 auth.info] Failed password for root from 79.16.133.71 port 4489 ssh2

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 V2 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。

4.1.5. 什么是过滤和归并

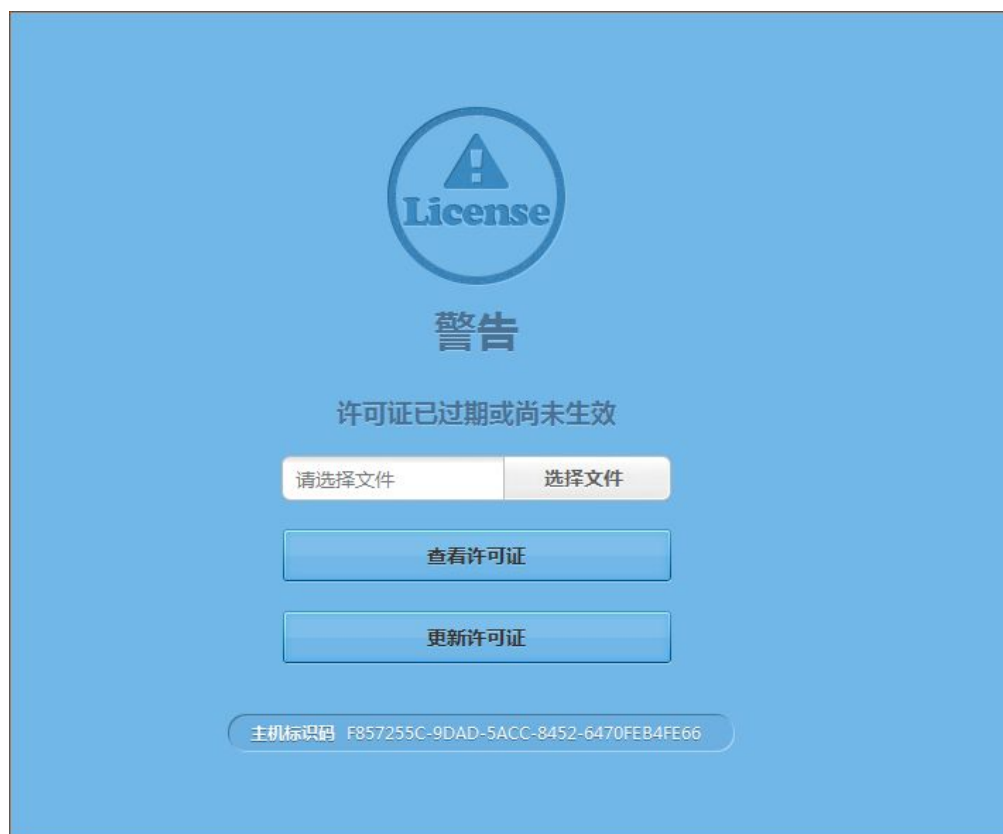
有时，为了使用户集中查看他所需要关注的相关日志或事件，或者有时我们并不需要保存所有的原始日志或事件，那么我们可以设置一个或多个过滤或归并策略。

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。

4.2. 初次使用

用户在初次使用日志审计系统时，需要导入许可证信息（License），在获取许可证之前，需要将界面上显示的主机标识码告知许可证提供方。



许可证信息注册成功后，使用帐号/口令（admin/admin）登录系统，系统会要求用户修改口令并添加管理员邮箱：



4.3. 向导

向导是用户第一次使用日志审计系统时，系统给出的相关使用步骤指引，它主要包括以下几个部分：

1. 设置采集器：由于日志审计系统默认不会建立事件采集器，故需要用户设置事件采集器；事件采集器需要根据实际情况配置。上述操作如下图所示：



2. 资产发现：自动发现采集管理器所在网络的相关主机、网络设备、安全设备、应用的存活情况；需要注意的一点是发现的资产系统类型不一定非常准确，用户可能还需进行调整。上述操作如下图所示：

快速入门

1 欢迎界面

2 采集器配置

3 资产管理

4 完成向导

提示：发现资产可能时间较长，请耐心等待。或者你可以点击“下一步”，跳过此步骤，稍后可以到“资产管理”页面查看执行的详细结果。

序号	IP地址段	进度
1	教育网-172.16.0.0/24(172.16.0.0/24)	

开始

完成

下一步

一般，用户通过系统的向导指引，就可以完成初始化工作和基本管理操作。

4.4. 采集管理

采集管理是使用日志审计系统的第一步，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。

4.4.1. 相关操作

4.4.1.1. 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：

采集策略管理

首页 / 采集管理 / 采集策略管理

标准化 过滤

标准化策略列表

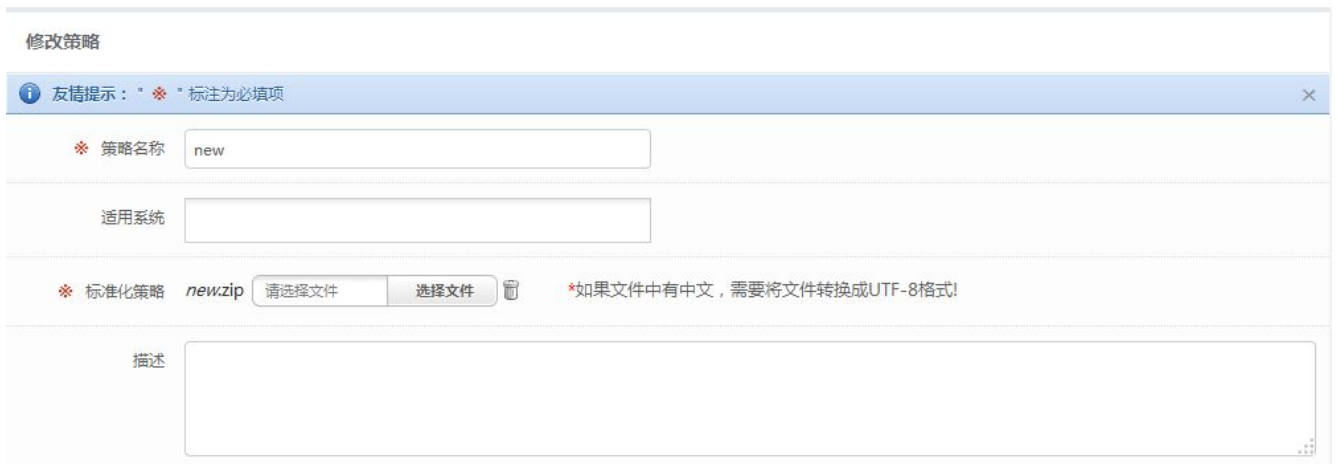
新增 删除 导入 导出

序号		策略名称	适用系统	是否内置	描述	操作
41	☐	Linux	RedHat,CentOS,SuSE	内置		
42	☐	Macfee IPS		内置		
43	☐	Microsoft Exchange2003		内置		
44	☐	Microsoft Windows	Windows 2000,Windows 2003...	内置		
45	☐	Microsoft Windows(Syslog)	Windows 2000,Windows 2003...	内置		
46	☐	MySQL	MySQL	内置		
47	☒	new		自定义		 
48	☐	NFocus IDS	NFocus IDS	内置		
49	☐	NFocus IDS(SNMP)	NFocus IDS	内置		
50	☐	NFocus IPS		内置		

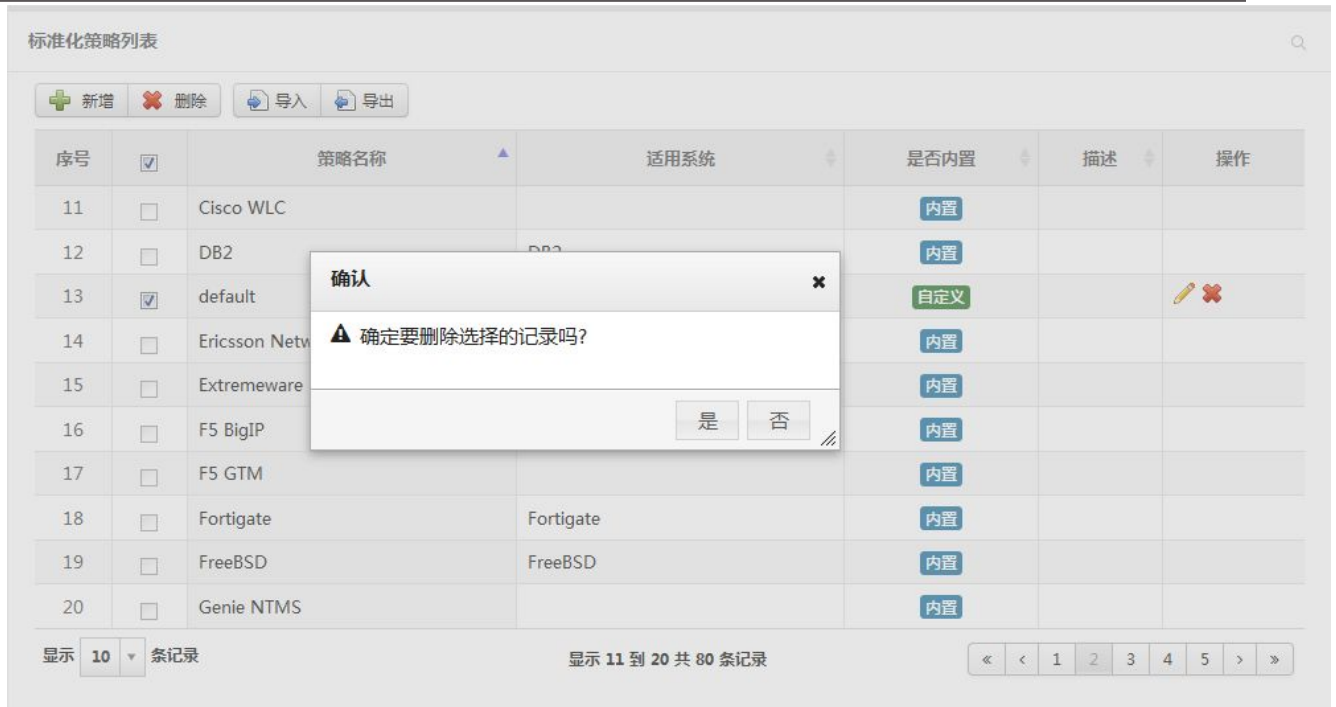
2. 新增标准化策略：点击新增，输入策略名称、使用系统（可填）、标准化策略（录入的标准化策略必须是 UTF-8 格式，而不要使用 GB 系列的编码，否则会出现乱码）、描述（可填）；点击保存。如下图所示：



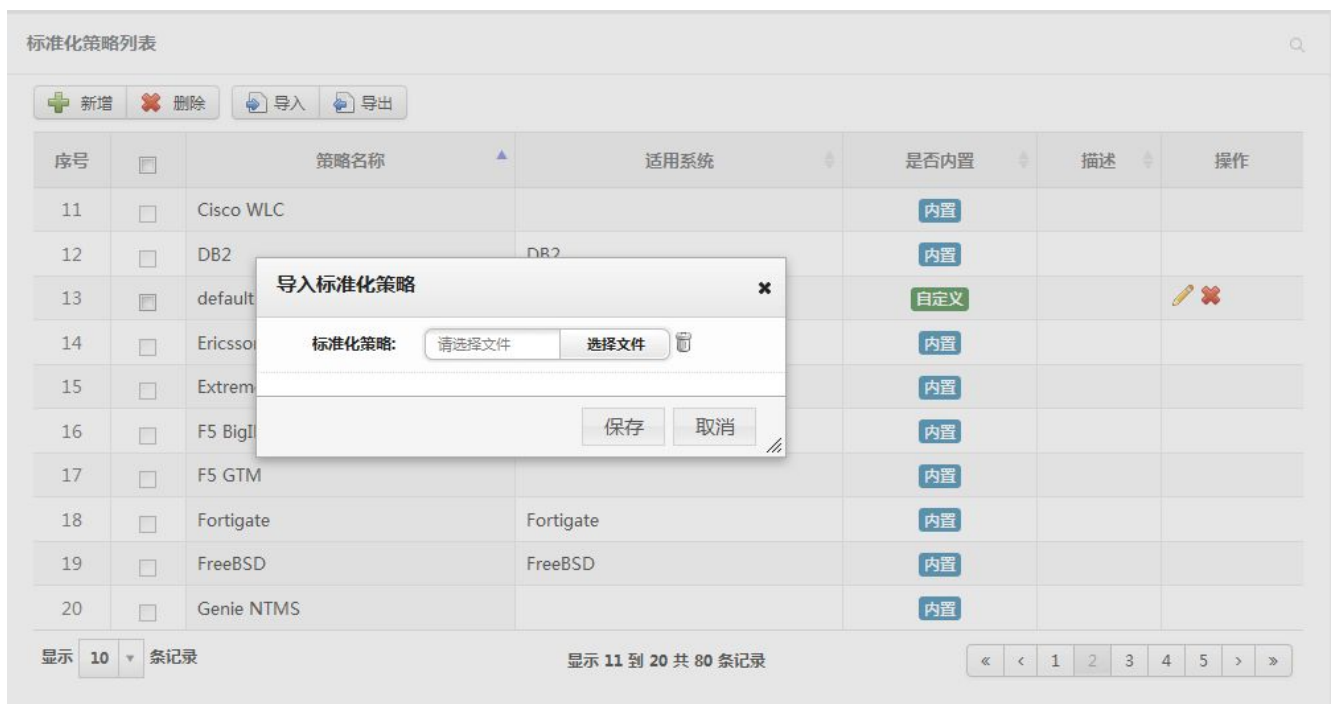
3. 修改标准化策略：修改标准化策略相关属性，点击保存。内置标准化策略是不允许修改的，只允许修改自定义的标准化策略。如下图所示：



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：

标准化策略列表

[+ 新增](#)
[✖ 删除](#)
[📄 导入](#)
[📄 导出](#)

序号	☒	策略名称	适用系统	是否内置	描述	操作
11	☐	Cisco WLC		内置		
12	☐	DB2		内置		
13	☒	default		自定义		✎ ✖
14	☐	Ericsson Netw		内置		
15	☐	Extremeware		内置		
16	☐	F5 BigIP	F5 Router/Switch	内置		
17	☐	F5 GTM		内置		
18	☐	Fortigate	Fortigate	内置		
19	☐	FreeBSD	FreeBSD	内置		
20	☐	Genie NTMS		内置		

显示 10 条记录 显示 11 到 20 共 80 条记录 « < 1 2 3 4 5 > »

确认

⚠ 确定要导出选择的记录吗?

是 否

4.4.1.2. 事件过滤策略

- 查看事件过滤策略列表：如下图所示：

采集策略管理

首页 / 采集管理 / 采集策略管理

标准化 过滤

事件过滤策略列表

[+ 新增](#)
[✖ 删除](#)

序号	☐	策略名称	动作	最后修改时间	描述	操作
1	☐	new	丢弃	2015-05-29 09:39:24		✎ ✖

显示 10 条记录 显示 1 到 1 共 1 条记录 « < 1 > »

- 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：

新增策略

友情提示: " * " 标注为必填项

* 策略名称

* 过滤器

* 动作 ☒ 丢弃 ☐ 转发syslog ☐ 设置属性并继续处理

描述

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：

修改策略

友情提示: " * " 标注为必填项

* 策略名称

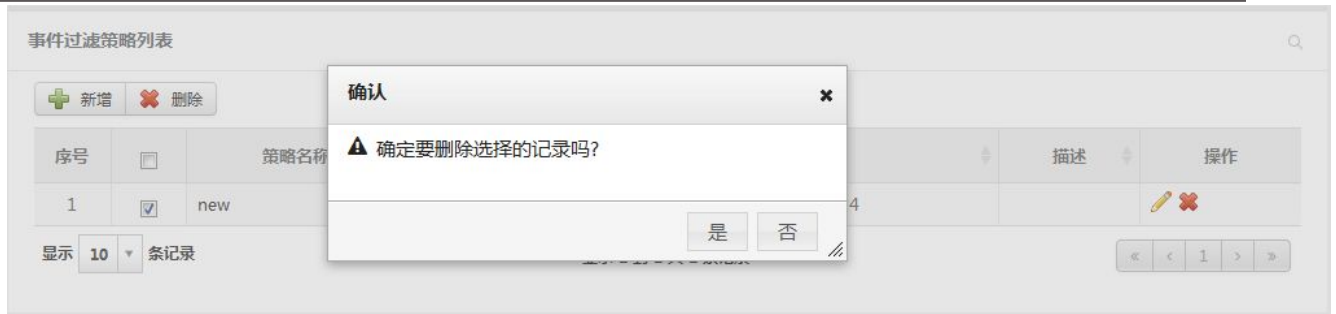
* 过滤器

  与  名称 等于 login 

* 动作 ☒ 丢弃 ☐ 转发syslog ☐ 设置属性并继续处理

描述

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：

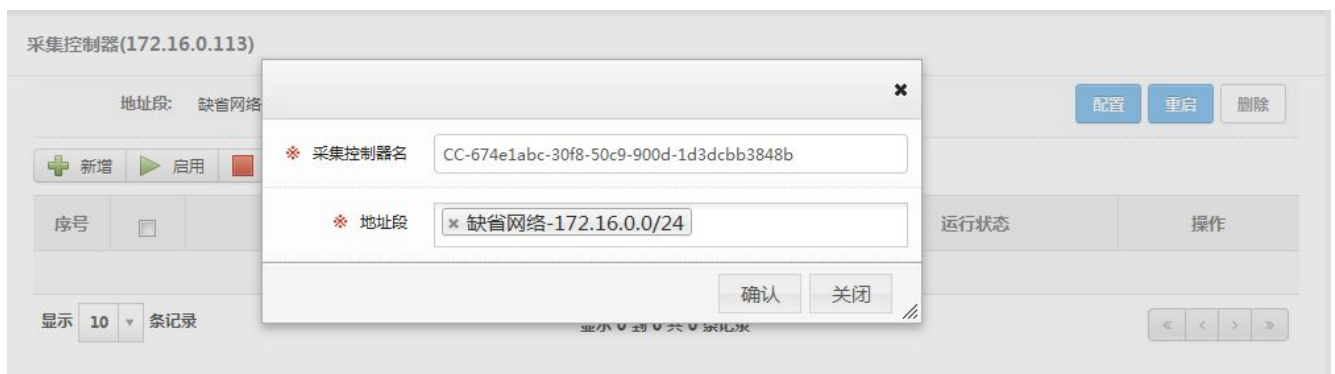


4.4.1.3. 采集器管理

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：



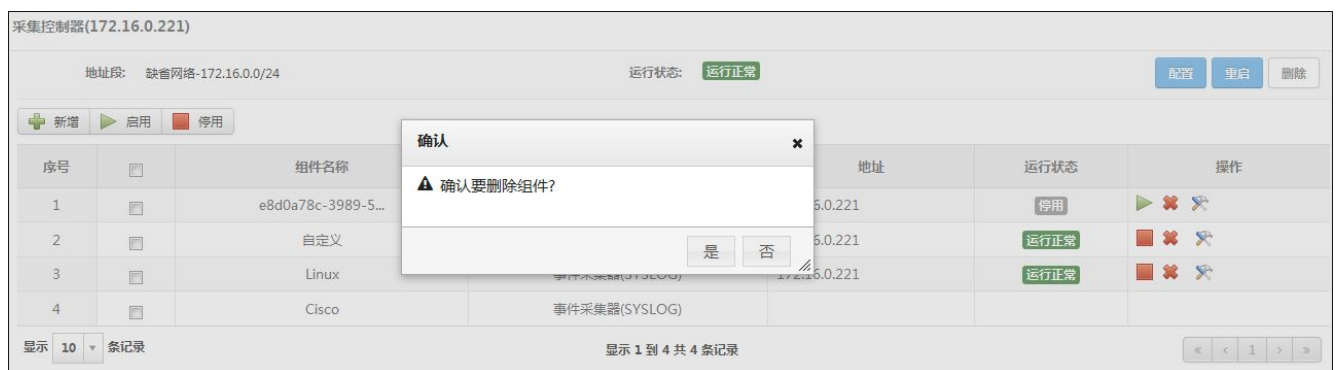
2. 配置采集控制器：点击配置，修改采集控制器名称、地址段；点击保存。如下图所示：



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：

新增采集器

✱ 名称

接入方式
 ☒ Syslog
 ☐ SNMP Trap
 ☐ 数据库
 ☐ 文件
 ☐ SOCKET
 ☐ SMB
 ☐ WMI

✱ 标准化策略

IP范围

事件过滤

+

是否归并
 ☐ 是
 ☒ 否

描述

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：

修改采集器

✱ 名称

接入方式
 ☒ syslog

✱ 标准化策略

IP范围

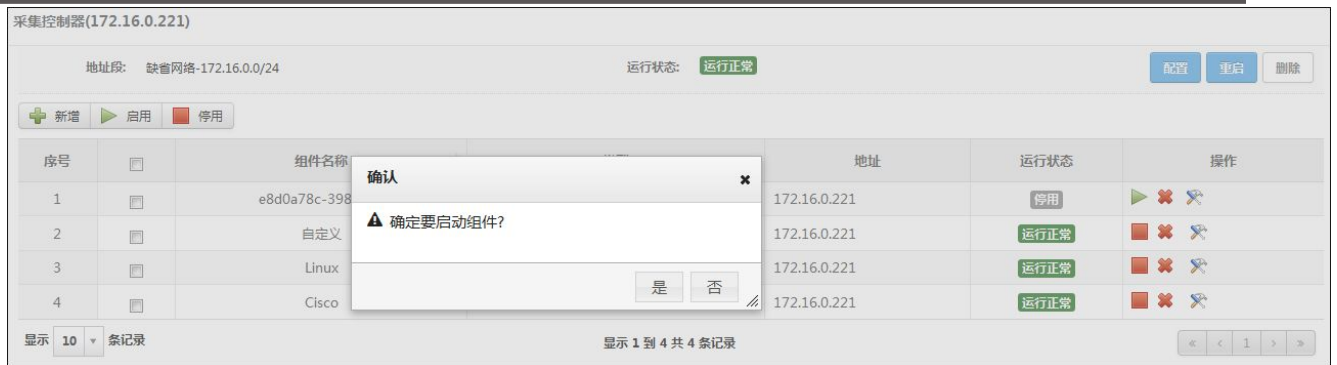
事件过滤

+

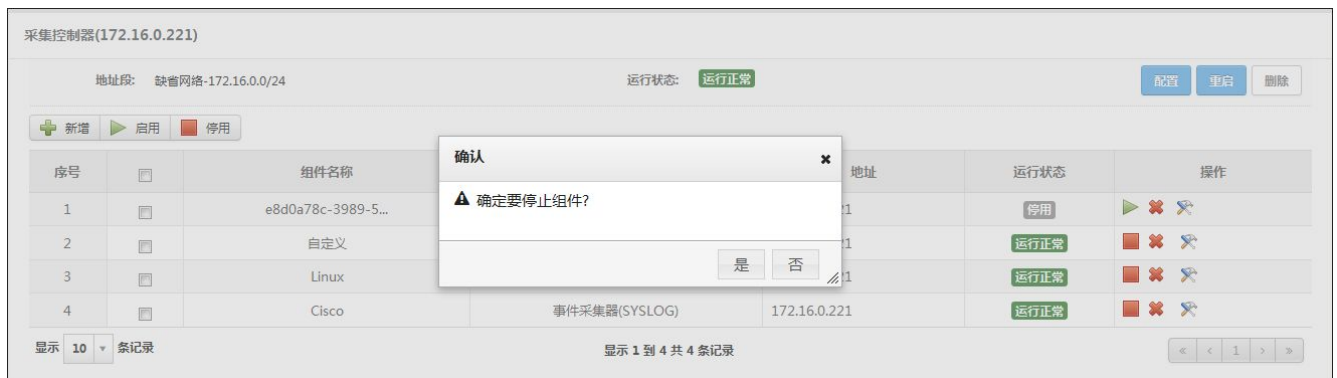
是否归并
 ☐ 是
 ☒ 否

描述

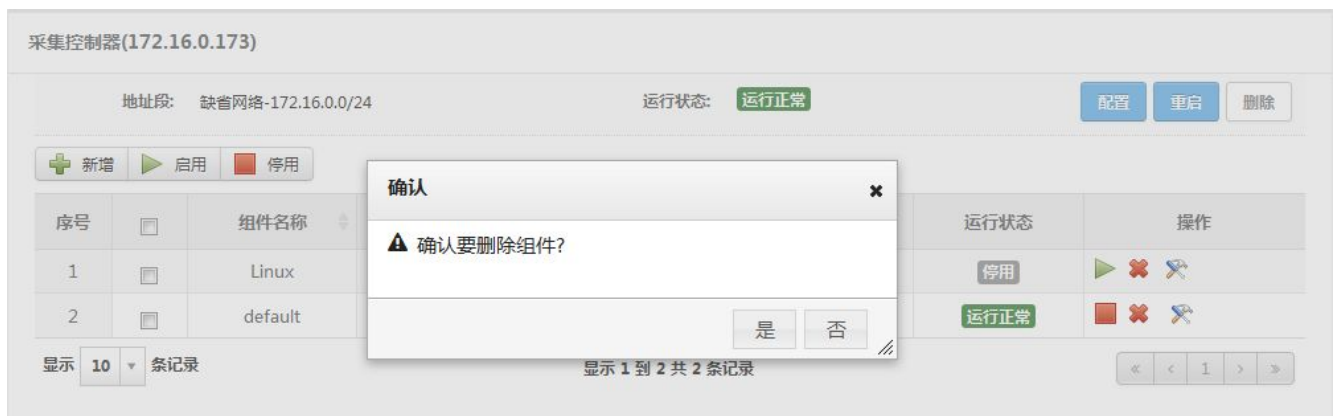
7. 启用采集器：点击操作列或列表上面的启用图标，点击确认。如下图所示：



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：



4.5. 资产管理

4.5.1. 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，铱迅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。

4.5.2. 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：

资产详情			
基本信息			
资产编号		资产名称	192.168.100.3
系统类型	Cisco Router/Switch	资产IP	192.168.100.3
资产类别	网络设备	IP地址段	缺省网络-192.168.100.0/24
系统版本		硬件型号	
序列号		用途	
MAC地址		所属视图	
附件一		附件二	
描述			
安全管理信息			
保密性	3.0	完整性	3.0
可用性	3.0	资产价值	3.0
创建人	系统管理员	创建日期	2013-07-29

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。

4.5.3. 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。

铨迅信息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。

4.5.4. 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。

4.5.5. 相关操作

4.5.5.1. 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：



The screenshot shows the 'Asset Detail' (资产详情) page. It features a tabbed interface with 'Basic Information' (基本信息) selected. The details are organized into two columns:

资产编号: 113	资产名称: 113
系统类型: CentOS	资产IP: 172.16.0.113
资产类别: 终端	IP地址段: 缺省网络-172.16.0.0/24
系统版本:	硬件型号:
序列号:	用途:
MAC地址:	所属视图:
附件一:	附件二:
描述:	

Below the details is a section for 'Security Management Information' (安全管理信息) and a 'Warning Status' (告警情况) tab at the bottom.

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：



The screenshot shows the 'Asset List' (资产列表) page. It includes a search bar at the top right and a query form with the following fields:

- 资产名称: [Text Input]
- 资产IP: [Text Input]
- 系统类型: [Dropdown Menu]
- 资产类别: [Dropdown Menu]
- 创建日期: [Date Range Picker]
- 责任人: [Text Input]
- 风险情况: [Dropdown Menu]

Buttons for 'Query' (查询) and 'Clear' (清空) are located below the form. At the bottom, there is a toolbar with icons for 'Add' (新增), 'Delete' (删除), 'Import' (导入), 'Export' (导出), and 'View' (视图查看). Below the toolbar is a table header with columns: 序号, 资产名称, 资产IP, 系统类型, 资产类别, 创建日期, 风险情况, and 操作.

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：

修改资产

友情提示：* 标注为必填项

基本信息

资产编号 113

资产名称 172.16.0.113

系统类型 CentOS

IP地址段 缺省网络-172.16.0.0/24

资产类别 终端

资产IP 172.16.0.113

系统版本

硬件型号

序列号

用途

MAC地址

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：

资产列表

新增 删除 导入 导出 视图查看

导入资产

资产文件 请选择文件 选择文件

保存 关闭

序号	资产名称	创建日期	风险情况	操作
1	172.16.0.2	2015-05-22 16:46:39	极度	编辑 删除
2	172.16.0.113	2015-05-22 16:48:14	极度	编辑 删除
3	172.16.0.173	2015-05-22 16:50:13	极度	编辑 删除

显示 10 条记录 显示 1 到 3 共 3 条记录

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：

资产列表

新增 删除 导入 导出 视图查看

PDF Excel Word CSV

序号	资产名称	系统类型	资产类别	创建日期	风险情况	操作
1	172.16.0.2	CentOS	终端	2015-05-22 16:46:39	极度	编辑 删除
2	172.16.0.113	CentOS	终端	2015-05-22 16:48:14	极度	编辑 删除
3	172.16.0.173	CentOS	服务器	2015-05-22 16:50:13	极度	编辑 删除

显示 10 条记录 显示 1 到 3 共 3 条记录

4.5.5.2. 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：

新增属性

友情提示：* 标注为必填项

* 名称

* 类型 字符

长度

默认值

输入提示

出错提示

是否必填 ☒ 否 ☐ 是

描述信息

4.5.5.3. 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：

视图列表

+ 新增 - 删除

序号 描述信息 操作

新增视图

* 视图名称

显示风险值 ☒ 否 ☐ 是

描述信息

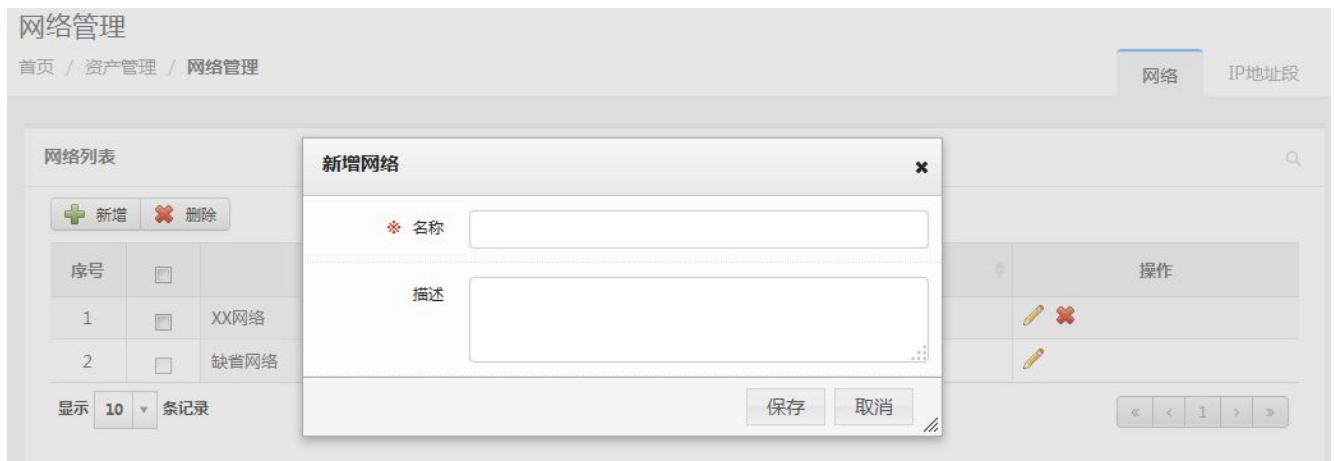
保存 取消

4.5.5.4. 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：



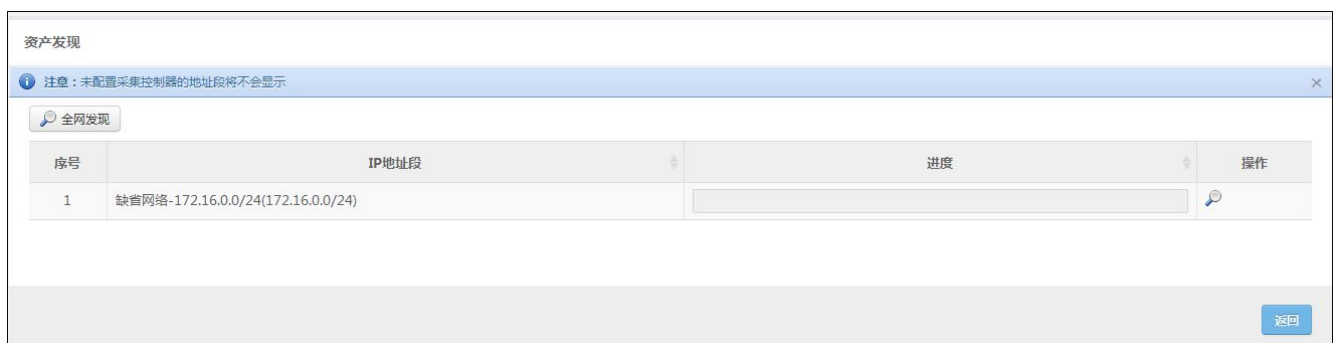
4.5.5.5. 资产发现管理

资产发现的目的除了发现网络中存活真实设备，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。

4.6. 事件分析

4.6.1. 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。

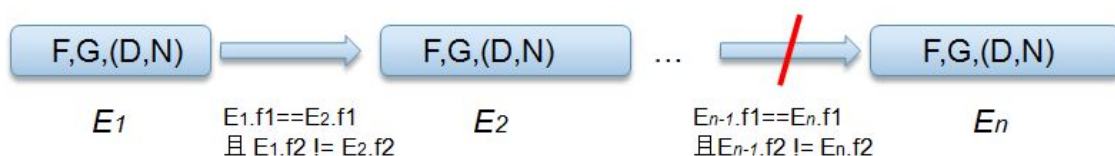
关联的类型包括基于规则的和基于统计的。

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

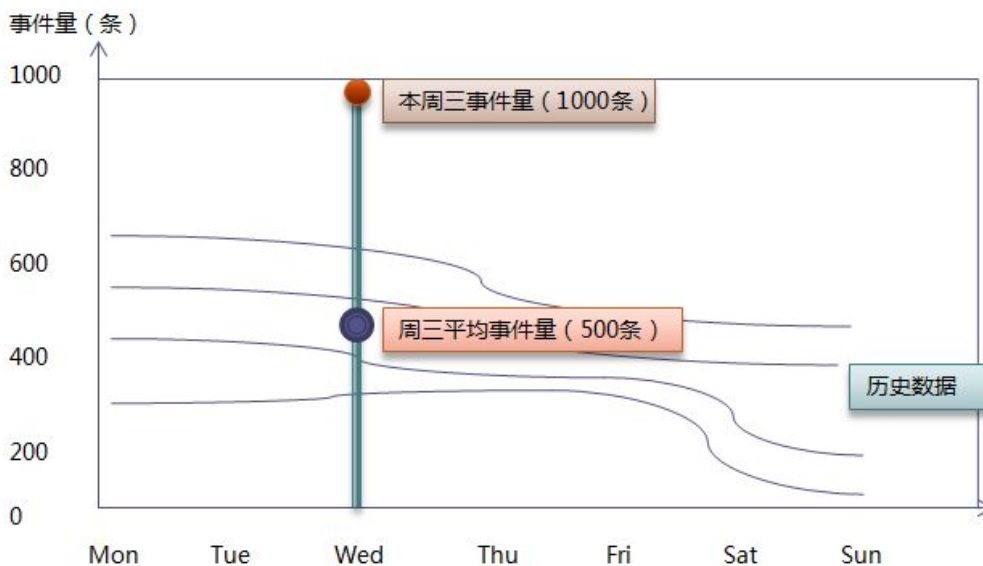
$E1[事件名称=="登录失败", "源地址", (60, 3)]$ 后续发生 $[E1.源地址==E2.源地址 \text{ 且 } E1.目标地址==E2.目标地址]$ $E2[事件名称=="登录成功", "源地址", (60, 1)]$ 为非法，因为它没有将目标地址加入到分组条件中

- 对于关联条件中的过滤条件，其关系运算仅支持等于和不同于
- 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，而周基线包含最近若干周每**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。

4.6.2. 相关操作

4.6.2.1. 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：

事件列表

[首页](#) / [事件分析](#) / [事件列表](#)

概览

查询

设备事件量排名列表								
日期选择： 2015-06-01								
设备类型 - Unix/Linux主机(3) - Windows主机(0) - 网络设备(0) - 防火墙(0) - 统一威胁管理(0) - 入侵检测系统(0) - 入侵防御系统(0) - 扫描器(0) - VPN (0) - 防病毒(0) - 数据库(0) - Web中间件(0) - 堡垒机(0) - 应用系统(0) - 其它(0)								
序号	IP地址	设备名称	严重	高级	中级	低级	信息	总数
1	172.16.0.221		0	0	0	0	199	199
2	172.16.0.173		0	0	0	0	195	195
3	172.16.0.113		0	0	0	0	195	195
显示 10 条记录			显示 1 到 3 共 3 条记录				« < 1 > »	

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：

事件列表

 友情提示: 请尽量输入精确查询条件, 查询或导出时系统将返回前100,000条记录.

普通模式

专家模式

查询条件: 请选择

时间段类型: 最近2小时

采集器: 请选择

设备IP:

设备类型: 请选择

名称:

源IP:

严重级别: 请选择

目的IP:

高级查询

查询

清空

保存查询条件

2015年23周

导出

序号	名称	类型	子类	严重级别	设备IP	时间	源IP	目的IP
1	计划任务执行	其它	其它	信息	172.16.0.221	2015-06-01 09:41:12		172.16.0.221

3. 事件详情：点击事件名称可查看事件详情。如下图所示：

事件列表

[首页](#) / [事件分析](#) / [事件列表](#)

详细信息			
基本信息			
名称:	计划任务执行	标准事件编号:	JNTA_General-LINUX_00016
事件编号:	a87dea35-ef03-555a-bead-1bf3dc8d2b08		
详细信息:	Jun 1 09:40:01 SMC-0424 CROND[422]: (root) CMD (/usr/lib64/sa/sa1 1 1)		
类型:	其它	子类:	其它
级别:	信息		
原始级别:			
设备类型:	Unix/Linux主机	设备地址:	172.16.0.221
设备名称:	172.16.0.221	产品名称:	LINUX
产品版本:			
接收时间:	2015-06-01 09:41:12		

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

2015年23周

导出

CSV

		类型	子类	严重级别	设备IP	时间	源IP	目的IP
1	SSH会话关闭	访问控制	用户注销	信息	172.16.0.221	2015-06-01 09:52:22		172.16.0.221
2	计划任务执行	其它	其它	信息	172.16.0.221	2015-06-01 09:51:12		172.16.0.221
3	计划任务执行	其它	其它	信息	172.16.0.113	2015-06-01 09:50:04		172.16.0.113
4	计划任务执行	其它	其它	信息	172.16.0.173	2015-06-01 09:50:04		172.16.0.173
5	特权命令执行	用户命令	用户命令	信息	172.16.0.221	2015-06-01 09:44:23		172.16.0.221
6	计划任务执行	其它	其它	信息	172.16.0.221	2015-06-01 09:41:12		172.16.0.221
7	SSH会话关闭	访问控制	用户注销	信息	172.16.0.221	2015-06-01 09:40:45		172.16.0.221
8	计划任务执行	其它	其它	信息	172.16.0.173	2015-06-01 09:40:04		172.16.0.173
9	计划任务执行	其它	其它	信息	172.16.0.113	2015-06-01 09:40:03		172.16.0.113
10	sftp传输	配置状态	状态变更	信息	172.16.0.221	2015-06-01 09:39:33		172.16.0.221

显示 10 条记录

显示 1 到 10 共 118 条记录 (实际查询到 118 条)

« < 1 2 3 4 5 > »

4.6.2.2. 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：

关联事件

首页 / 事件分析 / 关联事件

关联事件列表

导出

序号	事件名称	策略名称	事件类型	事件子类	对象IP	事件级别	产生时间	更新时间	总次
1	Unknown	全命中	其它	其它	172.16.0.221	警告	2015-06-10 00:00:02	2015-06-10 13:01:39	256
2	Unknown	全命中	其它	其它	172.16.0.2	警告	2015-06-10 09:53:52	2015-06-10 10:10:38	587330
3	SSH协议版本差异未知	全命中	其它	其它	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	4051
4	连接关闭	全命中	访问控制	用户注销	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	43744
5	用户认证错误	全命中	访问控制	用户登录	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	61158
6	用户口令修改	全命中	访问控制	其它	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	5266
7	计划任务执行	全命中	其它	其它	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	6075
8	接收邮件	全命中	配置状态	状态跟踪	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	14580
9	邮件规则检查	全命中	配置状态	状态跟踪	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	4860
10	发送邮件	全命中	配置状态	状态跟踪	172.16.0.2	警告	2015-06-10 10:02:21	2015-06-10 10:07:46	14580

显示 10 条记录

显示 1 到 10 共 29 条记录

« < 1 2 3 > »

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：

关联事件

首页 / 事件分析 / 关联事件

关联事件详情

事件名称: 登录事件

策略名称: 登录

事件类型: 访问控制

事件子类: 用户注销

事件级别: 一般

创建时间: 2015-06-01 10:22:49

原始事件内容: Jun 1 10:22:47 SMC-3144 sshd[17914]: pam_unix(sshd:session): session closed for user root

事件列表

序号	名称	类型	子类	严重级别	设备地址	时间	源地址	目的地址
1	SSH会话关闭	访问控制	用户注销	信息	172.16.0.173	2015-06-01 10:22:48		172.16.0.173

显示 10 条记录
显示 1 到 1 共 1 条记录

- 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：

关联事件列表

导出

PDF
Excel
Word
CSV

策略名称	事件类型	事件子类	对象IP	事件级别	产生时间	
登录	访问控制	用户注销	172.16.0.173	一般	2015-06-01 10:22:49	
登录	访问控制	用户注销	172.16.0.173	一般	2015-06-01 10:22:49	
3 登录事件	登录	访问控制	用户登录	172.16.0.173	一般	2015-06-01 10:19:46

显示 10 条记录
显示 1 到 3 共 3 条记录

4.6.2.3. 关联策略

- 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：

关联策略

首页 / 事件分析 / 关联策略

关联策略列表							
策略分组 - 恶意软件 - 网络攻击 - 信息破坏 - 内容安全 - 设备故障 - 灾难 - 其他 - 基于统计类 新增 删除 启用 停用 导入 导出							
序号		策略名称	状态	更新时间	策略描述	是否内置	操作
1	☐	登录	启用	2015-06-01 10:21:47		自定义	  
2	☐	Microsoft-IIS攻击	停用	2015-05-30 10:54:13		内置	
3	☐	异常登录尝试	停用	2015-05-30 10:54:13		内置	
4	☐	数据库表删除	停用	2015-05-30 10:54:13		内置	
5	☐	数据库表创建	停用	2015-05-30 10:54:13		内置	
6	☐	Oracle SYS用户远程登...	停用	2015-05-30 10:54:13		内置	
7	☐	SU提权失败	停用	2015-05-30 10:54:13		内置	
8	☐	系统重启	停用	2015-05-30 10:54:13		内置	
9	☐	系统关闭	停用	2015-05-30 10:54:13		内置	

2. 关联策略详情：通过点击策略名称可查看策略详情：

关联策略详情

策略名称: Microsoft-IIS攻击

基于规则

过滤器:

与

- 事件类型 等于 有害程序
- 动作对象名称 等于 IIS

关联条件:

状态1

在 60 秒内发生 1 次

归并字段 :

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：

关联策略列表							
策略分组 - 恶意软件 - 网络攻击 - 信息破坏 - 内容安全 - 设备故障 - 灾难 - 其他 - 基于统计类 - 自定义		新增 删除 启用 停用 导入 导出					
序号		策略名称	状态	更新时间	策略描述	是否内置	操作
1		登录	启用	2015-06-01 10:21:47		自定义	  
2		Microsoft-IIS攻击	停用	2015-05-30 10:54:13		内置	
3		异常登录尝试	停用	2015-05-30 10:54:13		内置	

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：

新增关联策略

策略名称

☒ 基于规则
☐ 基于统计

过滤器

关联条件
新增关联状态

响应方式
☐ 产生告警
☐ 转发外系统
☐ 执行程序

关联事件名称

关联事件级别
请选择

知识库
请选择

摘要:
解决方案:

策略描述

保存
取消

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：

修改关联策略

策略名称

基于规则

过滤器

与

事件类型 等于 访问控制

关联条件 新增关联状态

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：

关联策略列表

策略分组

- 恶意软件
- 网络攻击
- 信息破坏
- 内容安全
- 设备故障
- 灾难
- 其他
- 基于统计类
- 自定义

新增 删除 启用 停用 导入 导出

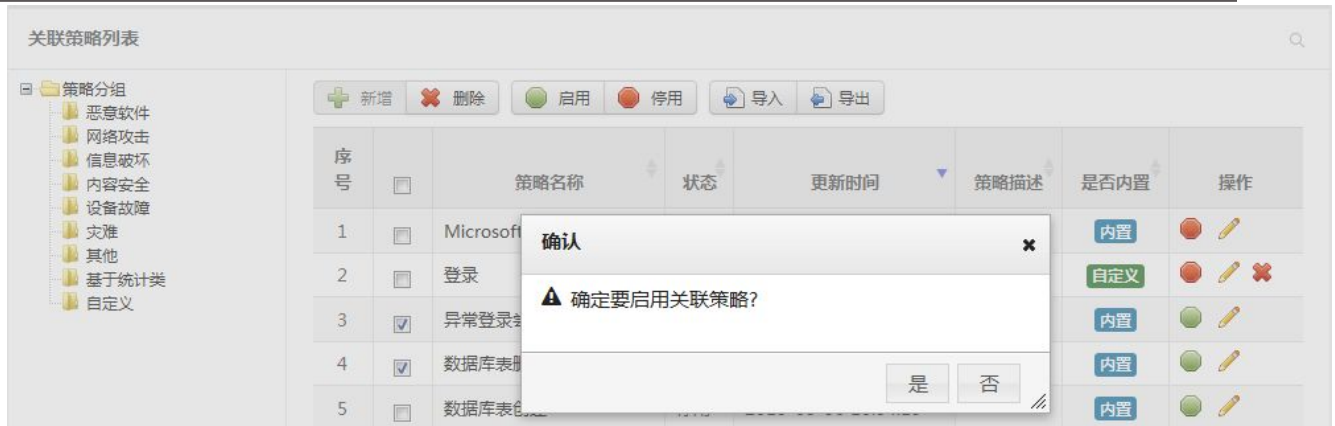
序号	策略名称	策略描述	策略状态	策略时间	策略来源	是否内置	操作
1	Microsoft-IIS		启用	2015-05-30 10:54:13	内置	内置	编辑
2	登录		启用	2015-05-30 10:54:13	自定义	自定义	编辑 删除
3	异常登录尝试		启用	2015-05-30 10:54:13	内置	内置	编辑
4	数据库表删除		停用	2015-05-30 10:54:13	内置	内置	编辑
5	数据库表创建		停用	2015-05-30 10:54:13	内置	内置	编辑
6	Oracle SYS用户远程登...		停用	2015-05-30 10:54:13	内置	内置	编辑
7	SU提权失败		停用	2015-05-30 10:54:13	内置	内置	编辑

确认

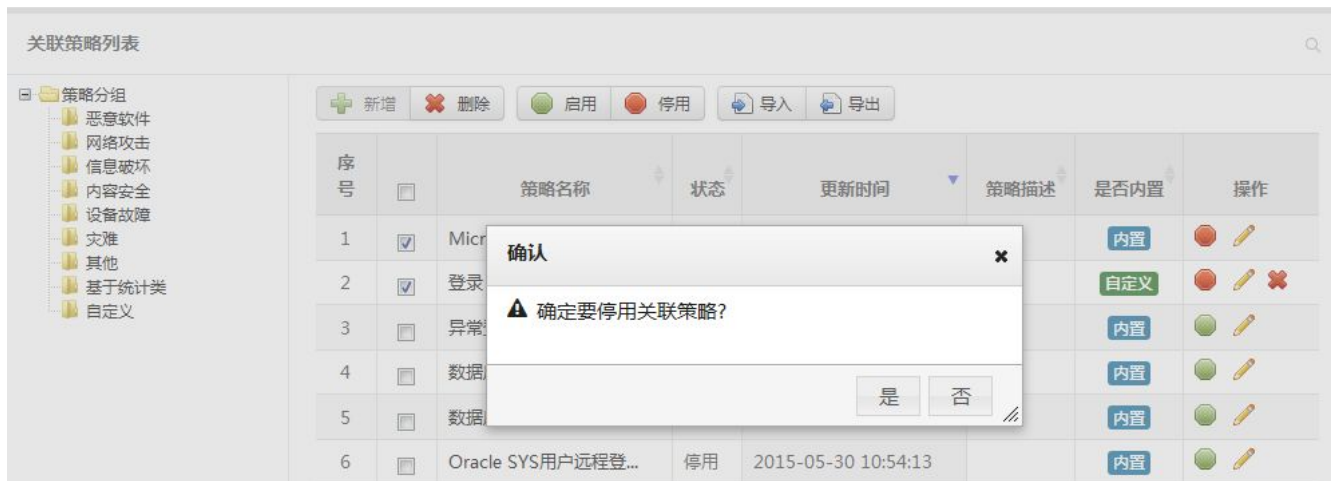
确定要删除选择的记录吗?

是 否

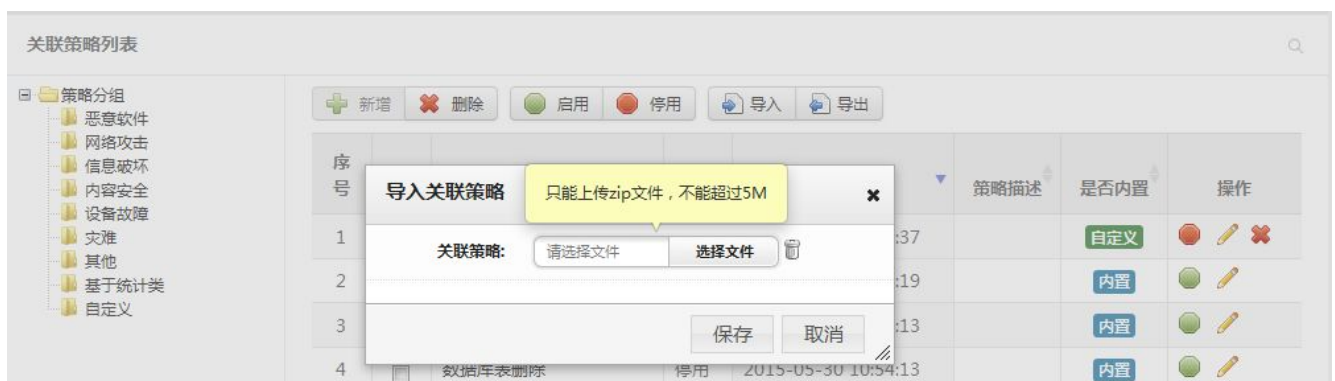
7. 启用关联策略：选择一个或多个要启用的关联策略，点击启用按钮，只有停用状态的关联策略才允许被启用。如下图所示：



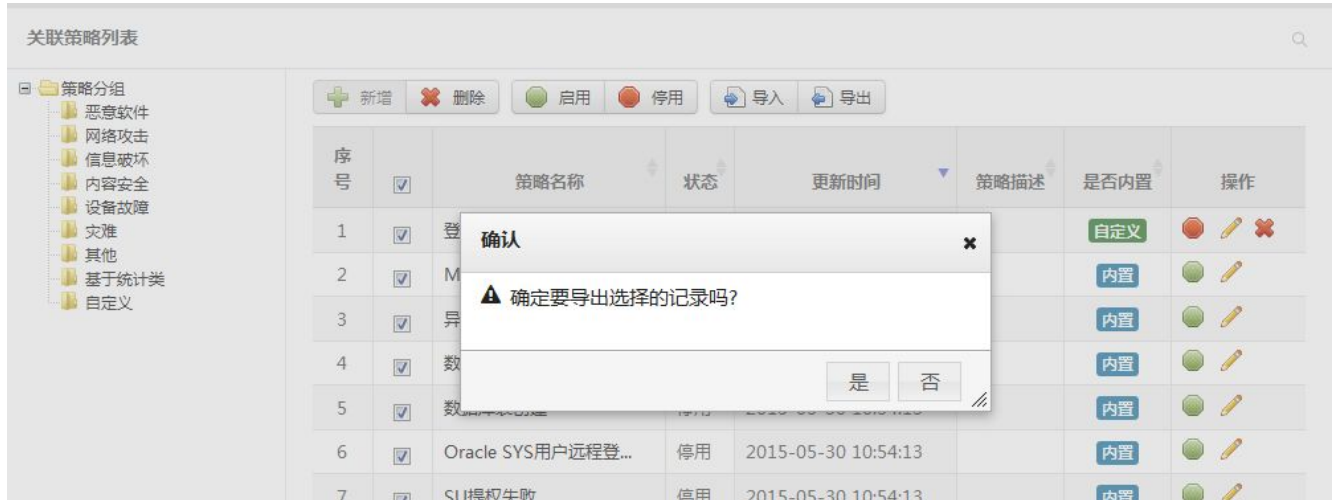
8. 停用关联策略：选择一个或多个要停用的关联策略，点击停用按钮，只有启用状态的关联策略才允许被停用。如下图所示：



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：



4.7. 审计管理

4.7.1. 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。

通过日志审计系统，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，日志审计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。

4.7.2. 相关操作

4.7.2.1. 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：

审计事件

首页 / 审计管理 / 审计事件

审计事件列表

导出

序号	事件名称	对象IP	事件级别	产生时间	更新时间	总次
1	Windows事件	172.16.0.221	一般	2015-06-11 14:10:02	2015-06-11 14:10:06	15
2	Windows事件	172.16.0.221	一般	2015-06-11 11:12:16	2015-06-11 14:01:03	46
3	Unknown	172.16.0.221	一般	2015-06-11 00:00:03	2015-06-11 11:12:01	234
4	Unknown	172.16.0.2	一般	2015-06-11 10:06:47	2015-06-11 10:10:32	115050
5	Unknown	172.16.0.221	一般	2015-06-10 00:00:03	2015-06-10 23:53:03	444
6	Unknown	172.16.0.2	一般	2015-06-10 09:53:51	2015-06-10 10:08:56	587330
7	SSH协议版本差异未知	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	4051
8	连接关闭	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	43744
9	用户认证错误	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	61158
10	用户口令修改	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	5266

显示 10 条记录 显示 1 到 10 共 33 条记录

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：

基本信息

事件名称: root登录

审计类型: 访问控制审计

事件级别: 一般

产生时间: 2015-06-01 15:42:34

审计策略: 登录成功审计

事件会话编号:

执行者账号: root

执行者地址: 172.16.0.2

操作对象名称:

操作对象类型:

审计行为: login

审计行为结果: 成功

审计行为来源: 172.16.0.2

审计目标地址: 172.16.0.173

审计行为详细信息: root

事件列表

序号	名称	类型	子类	严重级别	设备地址	时间	源地址	目的地址
1	root登录	访问控制	用户登录	信息	172.16.0.173	2015-06-01 15:42:33	172.16.0.2	172.16.0.173

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：

审计事件列表

导出 PDF Excel Word CSV

事件名称	对象IP	事件级别	产生时间	更新时间	总次
	172.16.0.221	一般	2015-06-11 14:10:02	2015-06-11 14:10:06	15
	172.16.0.221	一般	2015-06-11 11:12:16	2015-06-11 14:01:03	46
3 Unknown	172.16.0.221	一般	2015-06-11 00:00:03	2015-06-11 11:12:01	234
4 Unknown	172.16.0.2	一般	2015-06-11 10:06:47	2015-06-11 10:10:32	115050
5 Unknown	172.16.0.221	一般	2015-06-10 00:00:03	2015-06-10 23:53:03	444
6 Unknown	172.16.0.2	一般	2015-06-10 09:53:51	2015-06-10 10:08:56	587330
7 SSH协议版本差异未知	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	4051
8 连接关闭	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	43744
9 用户认证错误	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	61158
10 用户口令修改	172.16.0.2	一般	2015-06-10 10:00:02	2015-06-10 10:05:45	5266

显示 10 条记录 显示 1 到 10 共 33 条记录

4.7.2.2. 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：

审计策略

首页 / 审计管理 / 审计策略

审计策略列表

新增 从模板创建策略 删除 启用 停用 调整策略执行顺序

序号	策略名称	状态	处理方式	处理顺序	是否内置	操作
1	登录成功审计	启用	停止处理其他策略	1	内置	 
2	登录失败审计	停用	停止处理其他策略	2	内置	 
3	启动进程审计	停用	停止处理其他策略	3	内置	 
4	SU失败动作审计	停用	停止处理其他策略	4	内置	 
5	拒绝可疑连接行为审计	停用	停止处理其他策略	5	内置	 
6	su root动作审计	停用	停止处理其他策略	6	内置	 
7	SU成功动作审计	停用	停止处理其他策略	7	内置	 
8	普通病毒感染告警审计	停用	停止处理其他策略	8	内置	 
9	高风险病毒感染告警审计	停用	停止处理其他策略	9	内置	 
10	用户注销审计	停用	停止处理其他策略	10	内置	 

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：

审计策略

首页 / 审计管理 / 审计策略

审计策略详情

策略名称 审计策略示例

策略内容
事件类型: 有害程序
事件子类: 计算机病毒
关联对象分类: 主机
关联对象详细分类: Windows
审计操作对象 属于 操作对象类型: Windows, 操作对象名称: test001
审计目标(IP地址) 属于 172.16.0.221

响应方式

产生告警

告警名称生成方式: 自动

级别: 一般

告警大类: 恶意软件

告警子类: 网页病毒

追加: ☒

知会策略创建者 ☒ Email

其他邮箱 test@163.com

命中后继续 ☒

合并条件 事件类型 在60秒内发生3次

审计名称 审计策略示例

审计类型 有害程序类告警

审计级别 一般

描述 这是一个审计策略示例

返回

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：

新增审计策略

✳ 策略名称

策略内容

✳ 过滤器 事件类型 事件子类

关联对象分类 关联对象详细分类

审计操作对象 审计目标 审计行为 审计行为执行者 审计行为来源 审计有效时间段 其他条件

☐ 自定义 ☒ 预定义

合并条件 在 秒内发生 次

响应方式 ☐ 产生告警 ☐ 转发外系统

命中后继续 ☐

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：

审计策略列表

[+ 新增](#) [+ 从模板创建策略](#) [✳ 选择策略模板](#)

序号	☐	策略名称	是否内置	操作
1	☐	登录成功审计	内置	
2	☐	登录失败审计	内置	
3	☐	启动进程审计	内置	
4	☐	SU失败动作审计	内置	
5	☐	拒绝可疑连接行为审计	内置	
6	☐	su root动作审计	内置	
7	☐	SU成功动作审计	内置	
8	☐	普通病毒感染告警	内置	
9	☐	高风险病毒感染告警	内置	
10	☐	用户注销审计	内置	

显示 条记录

选择策略模板

- 策略模板分组
 - Windows主机
 - 登录成功审计
 - 登录失败审计
 - 用户注销审计
 - 帐户变更审计
 - 口令变更审计
 - 帐户权限变更审计
 - 策略修改审计
 - 系统文件删除审计
 - 可执行文件安装审计
 - 启动进程审计
 - 系统重启审计
 - 拒绝可疑连接行为审计
 - 网络蠕虫行为审计
 - Linux/Unix主机
 - 防火墙
 - 扫描器
 - IDS/IPS
 - 防病毒
 - 数据库
 - 萨班斯

确定

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：

修改审计策略

❖ 策略名称: 登录成功审计

策略内容: 事件大类: 访问控制
事件子类: 用户登录
审计行为 属于: 行为动作: login, 行为结果: 成功

❖ 过滤器: 事件类型: 访问控制 x v 事件子类: 用户登录 x v

关联对象分类: 关联对象详细分类:

审计操作对象: 审计目标: 审计行为: 审计行为执行者: 审计行为来源: 审计有效时间段: 其他条件:

☒ 属于 ☐ 不属于

操作对象类型: 操作对象名称: + 添加

序号	操作对象类型	操作对象名称	操作
当前无可用记录			

合并条件: 请选择 在 秒内发生 次

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:

审计策略列表

+ 新增 + 从模板创建策略 - 删除 启用 停用 调整策略执行顺序

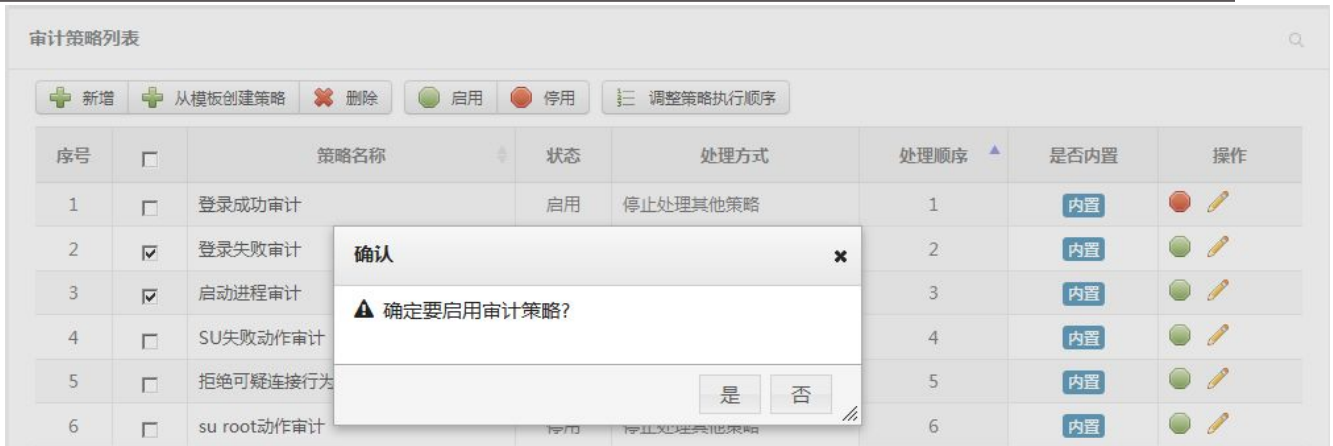
序号	☐	策略名称	状态	处理方式	处理顺序	是否内置	操作
1	☒	登录成功	启用	停止处理其他策略	31	自定义	删除
2	☐	数据库Update动作审计	停用	停止处理其他策略	30	内置	启用/停用/删除
3	☐	数据库Drop动作审计	停用	停止处理其他策略	29	内置	启用/停用/删除
4	☐	数据库Create动作审计	停用	停止处理其他策略	28	内置	启用/停用/删除
5	☐	数据库Delete动作审计	停用	停止处理其他策略	27	内置	启用/停用/删除
6	☐	数据库Insert动作审计	停用	停止处理其他策略	26	内置	启用/停用/删除
7	☐	数据库高危操作审计	停用	停止处理其他策略	25	内置	启用/停用/删除
8	☐	对象访问动作审计	停用	停止处理其他策略	24	内置	启用/停用/删除
9	☐	审计策略变更审计	停用	停止处理其他策略	23	内置	启用/停用/删除
10	☐	审计策略变更审计	停用	停止处理其他策略	22	内置	启用/停用/删除

确认

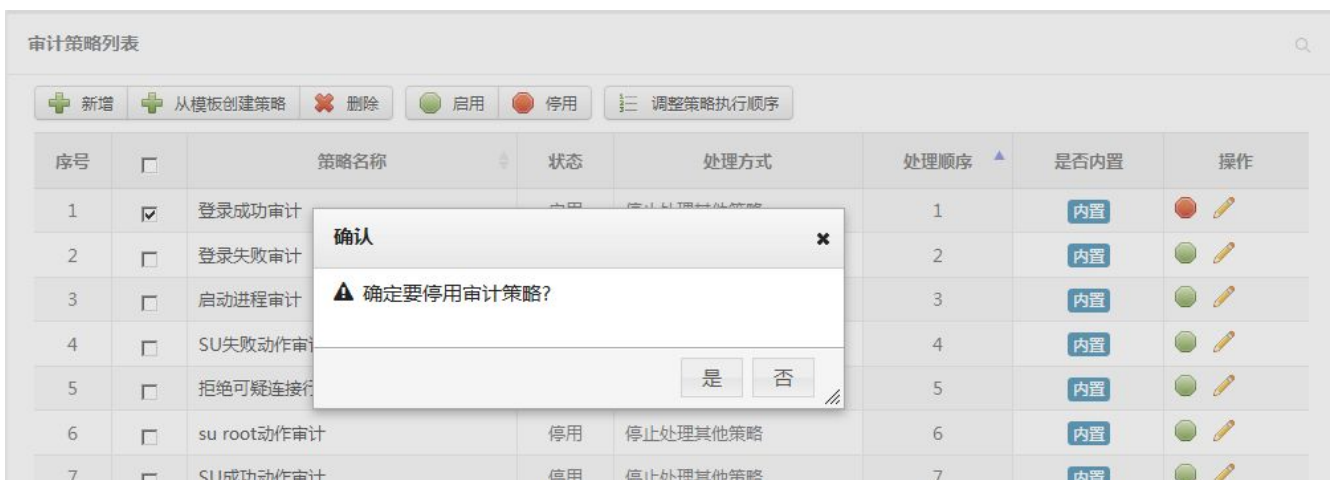
⚠ 确定要删除选择的记录吗?

是 否

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：

审计策略

首页 / 审计管理 / 审计策略

调整策略执行顺序

[↑ 上移至顶部](#)
[↓ 下移至底部](#)
[^ 上移1位](#)
[v 下移1位](#)
[^ 上移10位](#)
[v 下移10位](#)

序号	选项	审计策略名称	处理顺序
1	☐	登录成功审计	1
2	☐	登录失败审计	2
3	☐	启动进程审计	3
4	☐	SU失败动作审计	4
5	☐	拒绝可疑连接行为审计	5
6	☒	su root动作审计	6
7	☐	SU成功动作审计	7
8	☐	普通病毒感染告警审计	8
9	☐	高风险病毒感染告警审计	9
10	☐	用户注销审计	10
11	☐	帐户变更审计	11
12	☐	口令变更审计	12
13	☐	帐户权限变更审计	13
14	☐	策略修改审计	14

4.7.2.3. 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：

审计策略模板

首页 / 审计管理 / 审计策略模板

审计策略模板						
+ 新增 - 移除 ✖ 删除						
序号	☐	策略模板名称	更新时间	策略描述	是否内置	操作
1	☐	登录成功审计	2015-05-30 10:54:13	针对计算机用户登录成功记录的审计策略	内置	+ 编辑
2	☐	登录失败审计	2015-05-30 10:54:13	针对计算机用户登录失败记录的审计策略	内置	+ 编辑
3	☐	用户注销审计	2015-05-30 10:54:13	针对计算机中帐号登录注销动作记录的审计策...	内置	+ 编辑
4	☐	帐户变更审计	2015-05-30 10:54:13	针对计算机中帐户修改记录的审计策略	内置	+ 编辑
5	☐	口令变更审计	2015-05-30 10:54:13	审计用户修改帐号口令的行为。用户利用系统...	内置	+ 编辑

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：

审计策略模板详情

策略名称 登录成功审计

策略内容 事件大类：访问控制
事件子类：用户登录
审计行为 属于 行为动作: login, 行为结果: 成功

合并条件

描述 针对计算机用户登录成功记录的审计策略

所属策略模板组 Windows主机 Linux/Unix主机 防火墙 萨班斯

返回

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：

审计策略模板

新增 移除 删除

序号	☐	策略模板名称	更新时间	策略描述	是否内置	操作
1	☐	登录成功审计	2015-05-30 10:54:13	针对计算机用户登录成功记录的审计策略	内置	+ 编辑
2	☐	登录失败审计	2015-05-30 10:54:13	针对计算机用户登录失败记录的审计策略	内置	+ 编辑
3	☐	用户注销审计	2015-05-30 10:54:13	针对计算机中帐号登录注销动作记录的审计策略	内置	+ 编辑

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：

新增审计策略模板

✱ 策略模板名称

策略内容

过滤器 事件类型 事件子类

关联对象分类 关联对象详细分类

审计操作对象 审计行为 审计有效时间段 其他条件

☒ 属于 ☐ 不属于

操作对象类型 操作对象名称 + 添加

序号	操作对象类型	操作对象名称	操作
当前无可用记录			

合并条件 在 秒内发生 次

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：

新增审计策略模板

✱ 策略模板名称

策略内容 事件大类：访问控制
事件子类：用户登录
审计行为 属于 行为动作：login, 行为结果：成功

过滤器 事件类型 事件子类

关联对象分类 关联对象详细分类

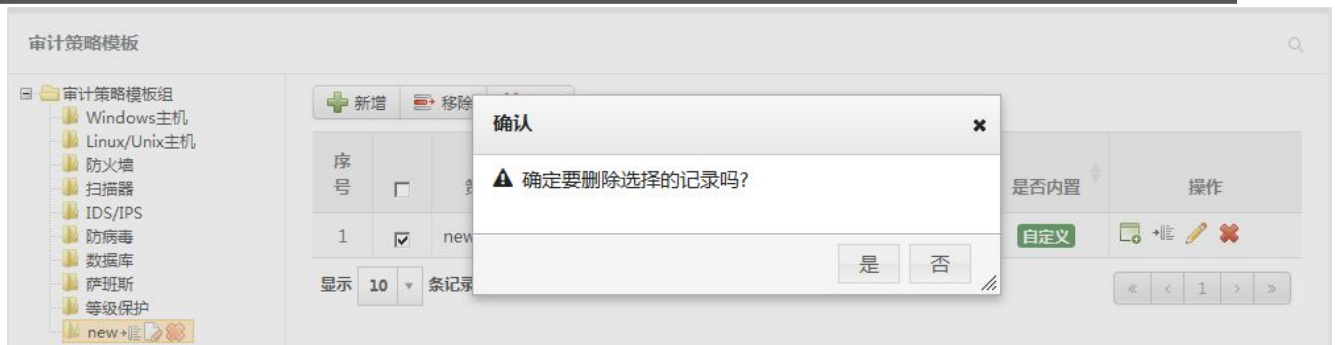
审计操作对象 审计行为 审计有效时间段 其他条件

☒ 属于 ☐ 不属于

操作对象类型 操作对象名称 + 添加

序号	操作对象类型	操作对象名称	操作
当前无可用记录			

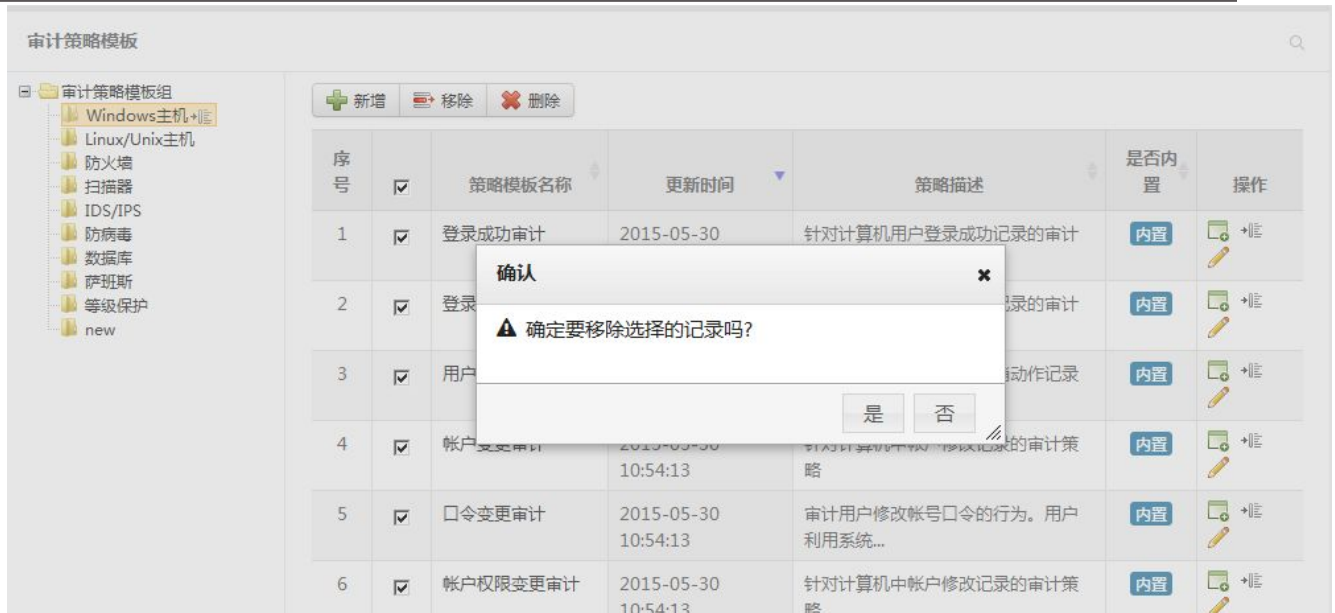
6. 删除审计策略模板：选择一个或多个要删除的审计策略模板，点击删除按钮，内置审计策略模板不允许删除。如下图所示：



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：

新增审计策略

策略名称: 登录成功审计

策略内容: 事件大类: 访问控制
事件子类: 用户登录
审计行为 属于 行为动作: login, 行为结果: 成功

过滤器: 事件类型: 访问控制 事件子类: 用户登录

关联对象分类: 关联对象详细分类:

审计操作对象: 审计目标: 审计行为: 审计行为执行者: 审计行为来源: 审计有效时间段: 其他条件:

☒ 属于 ☐ 不属于

操作对象类型: 操作对象名称: + 添加

序号	操作对象类型	操作对象名称	操作
当前无可用记录			

4.7.2.4. 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：

序号	☐	审计类型名称	描述	操作
1	☐	配置状态		 
2	☐	连接		 
3	☐	账户管理		 
4	☐	访问控制审计		 
5	☐	网络攻击类告警		 
6	☐	策略管理		 
7	☐	用户命令		 
8	☐	有害程序类告警		 
9	☐	数据文件		 
10	☐	其它		 

显示 10 条记录 显示 1 到 10 共 10 条记录

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：

基本信息	
审计类型名称：	配置状态
描述：	

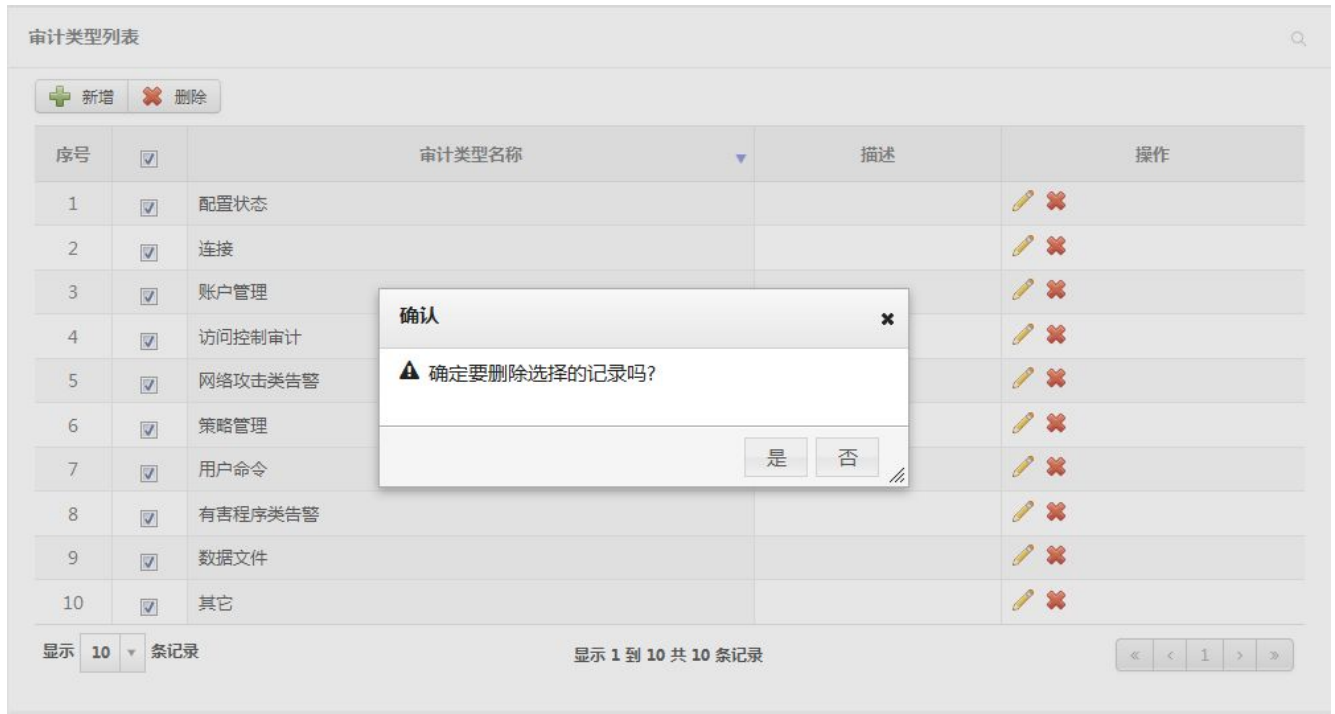
3. 审计类型新增：点击新增按钮，用于输入审计类型名称、描述（选填），点击保存。如下图所示：

新增审计类型	
* 审计类型名称	
描述	

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：

修改审计类型	
* 审计类型名称	配置状态
描述	

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：



4.7.2.5. 审计人员

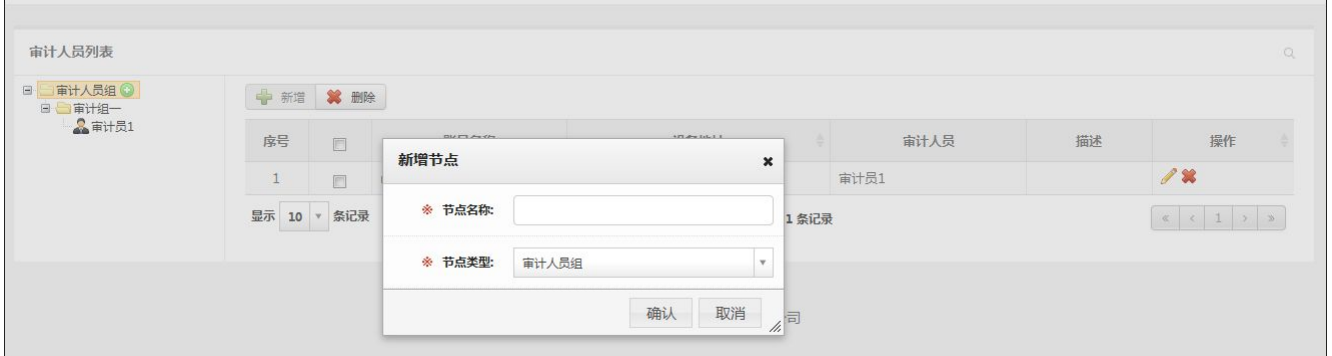
1. 审计人员列表：左边树结构展示的是审计人员组及其下的审计人员（文件夹图标代表的是审计人员组，人员图标代表的是审计人员），右边列表展示的是审计人员组或审计人员下的审计账号。如下图所示：



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：

审计人员

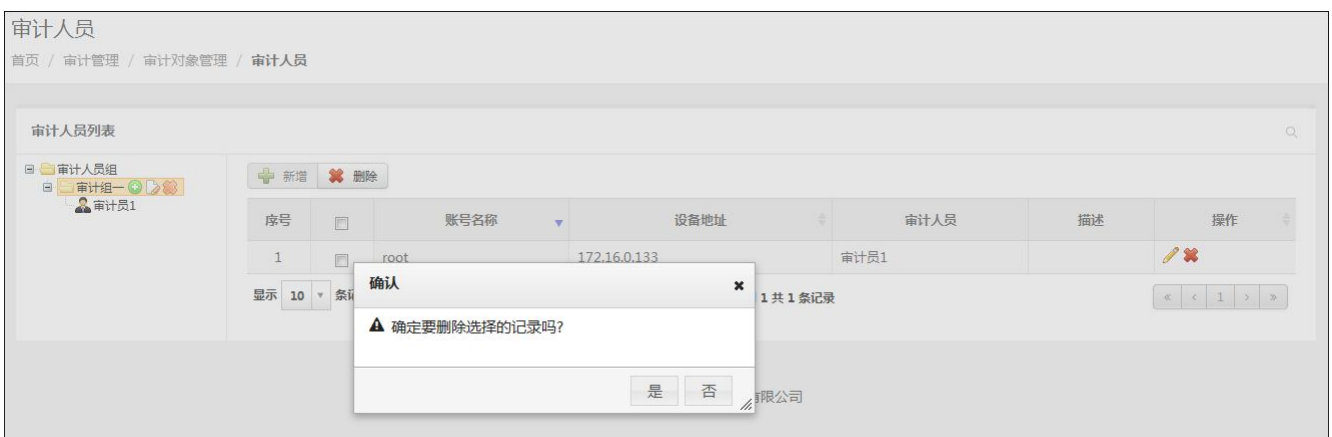
首页 / 审计管理 / 审计对象管理 / 审计人员



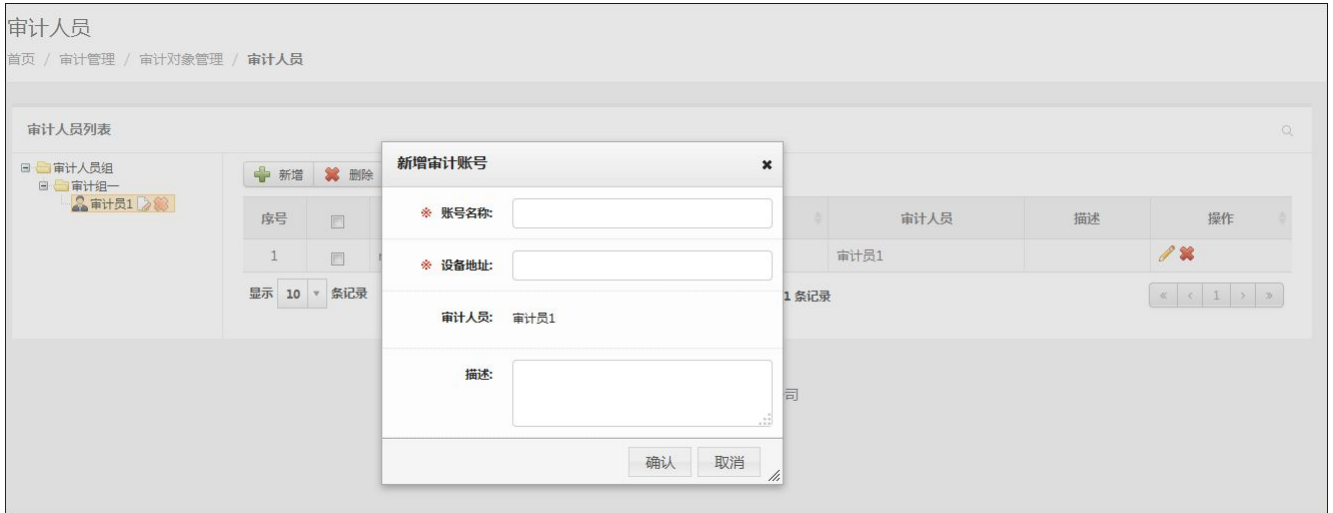
- 修改节点：选择需要修改的节点，点击其旁边重命名图标，修改审计人员组或审计人员的基本属性，点击确认。如下图所示：



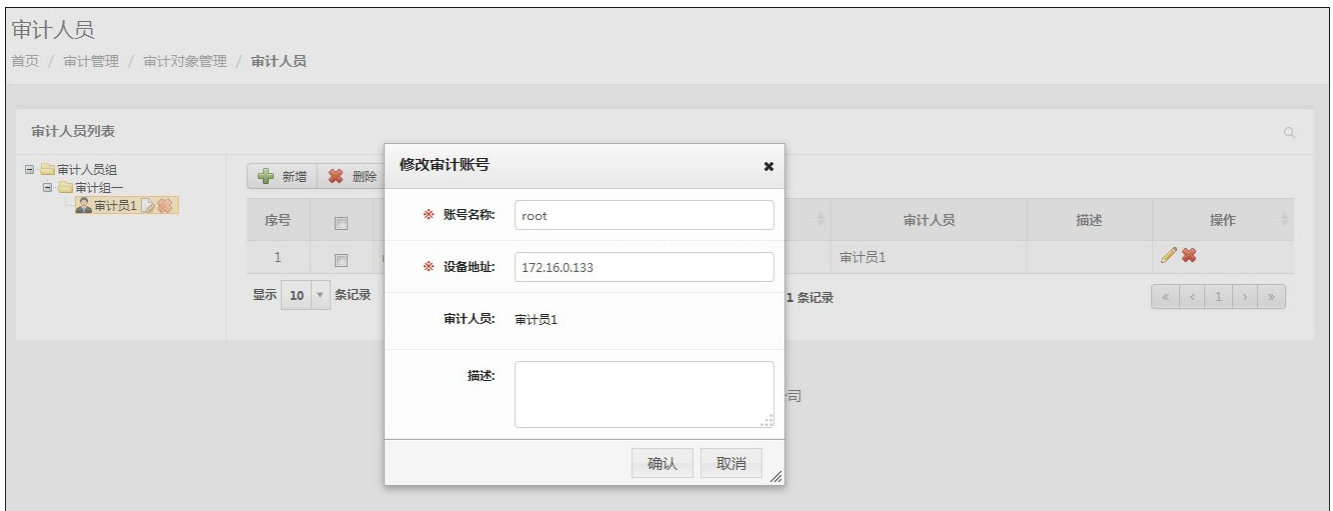
- 删除节点：选择需要删除的节点，点击其旁边删除图标。如果审计人员组及其子节点下面存在审计人员，审计人员正在被审计策略或审计执行者对象引用，则不允许删除该节点。如下图所示：



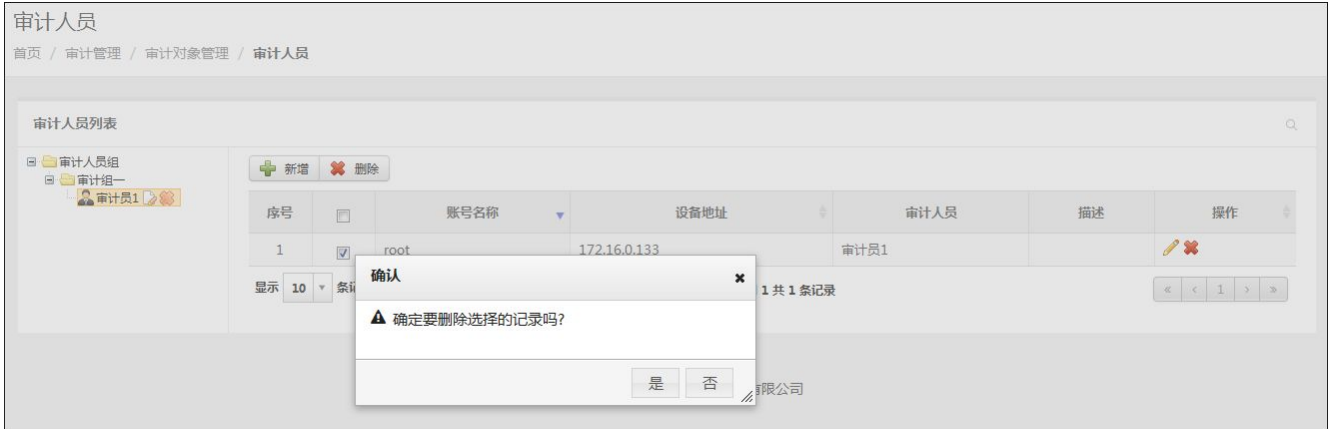
5. 新增审计账号：选择审计人员，点击新增按钮，用户需要输入账号名称、设备地址、描述（选填），点击确认。如下图所示：



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：

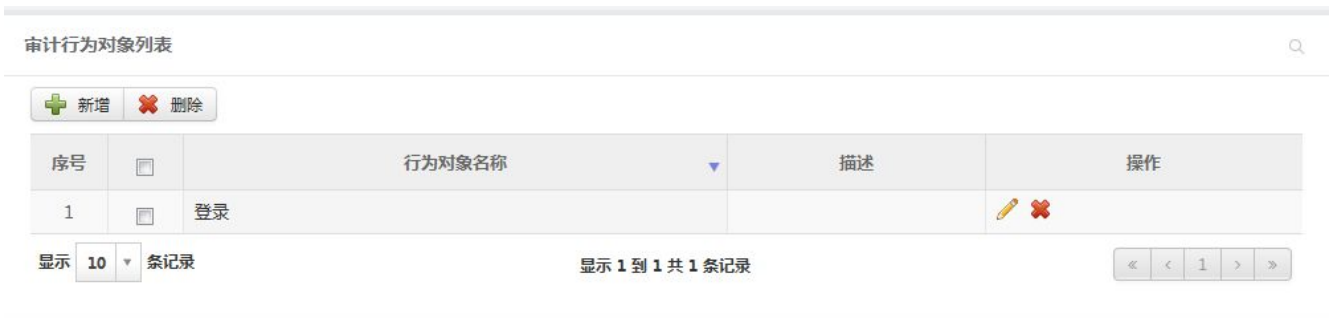


7. 删除审计账号：选择一个或多个需要删除的审计账号，点击删除。如下图所示：



4.7.2.6 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：

新增审计行为对象

✱ 行为对象名称

描述

审计行为 ☒ 属于 ☐ 不属于

行为动作 行为结果 + 添加

序号	行为动作	行为结果	操作
1	login	不考虑结果	✖

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：

修改审计行为对象

✱ 行为对象名称

描述

审计行为 ☒ 属于 ☐ 不属于

行为动作 行为结果 + 添加

序号	行为动作	行为结果	操作
1	login	不考虑结果	✖

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：

审计行为对象列表

+ 新增 ✖ 删除

序号	☐	描述	操作
1	☒	登录	✏ ✖

显示 条记录

确认

⚠ 确定要删除选择的记录吗?

4.7.2.7. 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：

审计行为执行者对象

首页 / 审计管理 / 审计对象管理 / 审计行为执行者对象

审计行为执行者对象列表				
+ 新增 ✖ 删除				
序号		行为执行者对象名称	描述	操作
1		管理员		✎ ✖
显示 10 条记录 显示 1 到 1 共 1 条记录				

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：

审计行为执行者对象详情	
名称	管理员
描述	
内容	审计行为执行者 属于 账号名称: root, 设备地址: 127.0.0.1

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：

新增审计行为执行者对象									
名称									
描述									
审计行为执行者	账号 ☒ 属于 ☐ 不属于 设备地址 账号名称 + 添加 <table> <tr> <th>序号</th><th>设备地址</th><th>账号名称</th><th>操作</th></tr> <tr> <td colspan="4">当前无可用记录</td></tr> </table>	序号	设备地址	账号名称	操作	当前无可用记录			
序号	设备地址	账号名称	操作						
当前无可用记录									

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：

修改审计行为执行者对象

名称

描述

审计行为执行者

账号

☒ 属于 ☐ 不属于

设备地址 账号名称 + 添加

序号	设备地址	账号名称	操作
1	127.0.0.1	root	✖

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：

审计行为执行者对象列表

+ 新增 ✖ 删除

序号	☐	描述	操作
1	☒	管理员	✏ ✖

显示 10 条记录

确认

⚠ 确定要删除选择的记录吗？

是 否

4.7.2.8. 审计行为来源对象

1. 审计行为来源对象列表：如下图所示：

审计行为来源对象列表

+ 新增 ✖ 删除

序号	☐	行为来源名称	描述	操作
1	☐	new		✏ ✖

显示 10 条记录

显示 1 到 1 共 1 条记录

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：

审计行为来源对象详情

名称	new
描述	
内容	审计行为来源 属于 IP地址: 192.168.100.1

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：

新增审计行为来源对象

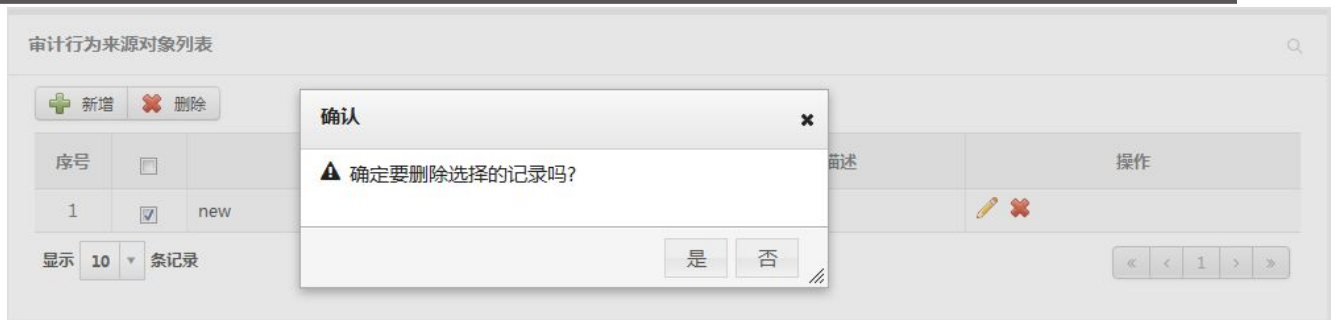
名称									
描述									
行为来源	☒ 属于 ☐ 不属于 IP地址 审计行为来源对象 + 添加 <table border="1"> <thead> <tr> <th>序号</th> <th>审计行为来源对象类型</th> <th>审计行为来源对象值</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td colspan="4">当前无可用记录</td> </tr> </tbody> </table>	序号	审计行为来源对象类型	审计行为来源对象值	操作	当前无可用记录			
序号	审计行为来源对象类型	审计行为来源对象值	操作						
当前无可用记录									

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：

修改审计行为来源对象

名称	new								
描述									
行为来源	☒ 属于 ☐ 不属于 IP地址 审计行为来源对象 + 添加 <table border="1"> <thead> <tr> <th>序号</th> <th>审计行为来源对象类型</th> <th>审计行为来源对象值</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>IP地址</td> <td>192.168.100.1</td> <td>✖</td> </tr> </tbody> </table>	序号	审计行为来源对象类型	审计行为来源对象值	操作	1	IP地址	192.168.100.1	✖
序号	审计行为来源对象类型	审计行为来源对象值	操作						
1	IP地址	192.168.100.1	✖						

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：

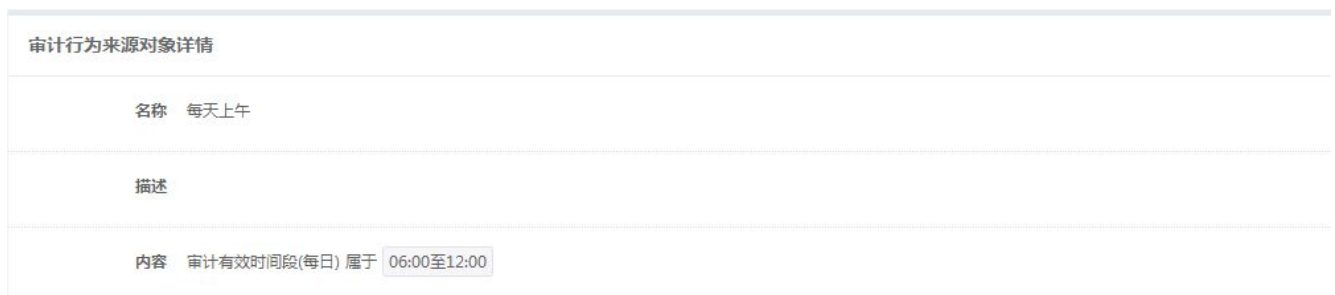


4.7.2.9. 审计时间段对象

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：

新增审计时间段对象

名称

描述

时间段 ☒ 每日 ☐ 星期 ☐ 日期

-

☒ 属于 ☐ 不属于 + 添加

序号	审计时间段对象类型	审计时间段对象值	操作
1	每日	06:00至12:00	

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：

修改审计时间段对象

名称

描述

时间段 ☒ 每日 ☐ 星期 ☐ 日期

-

☒ 属于 ☐ 不属于 + 添加

序号	审计时间段对象类型	审计时间段对象值	操作
1	每日	06:00至12:00	

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：

审计时间段对象列表

+ 新增 - 删除

序号	☐	名称	操作
1	☒	每天上午	

显示 10 条记录

确认

⚠ 确定要删除选择的记录吗?

是 否

4.7.2.10. 审计目标对象

1. 审计目标对象列表：如下图所示：

审计目标对象列表

+ 新增 - 删除

序号	目标对象名称	描述	操作
1	研发		

显示 10 条记录 显示 1 到 1 共 1 条记录

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：

审计目标对象详情

名称 研发

描述

内容 审计目标(主机设备) 属于 设备类型: Unix Host, IP地址: 172.16.0.173

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：

新增审计目标对象

* 名称

描述

* 目标对象

☒ IP地址 ☐ 主机设备 ☐ 视图资产

IP地址 审计目标对象

☒ 属于 ☐ 不属于

+ 添加

序号	审计目标对象类型	审计目标对象值	操作
当前无可用记录			

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：

修改审计目标对象

✖ 名称

研发

描述

目标对象 ✖

☐ IP地址
 ☒ 主机设备
 ☐ 视图资产

设备类型: 请选择

IP地址: 请选择

☒ 属于
 ☐ 不属于

+ 添加

序号	审计目标对象类型	审计目标对象值	操作
1	主机设备	设备类型: Unix Host, IP地址:...	✖

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：

审计目标对象列表

+ 新增

✖ 删除

序号		描述	操作
1	☒	研发	✏ ✖

显示 10 条记录

显示 1 到 1 共 1 条记录

<<

<

1

>

>>

确认

⚠ 确定要删除选择的记录吗?

是

否

4.8. 安全监控

4.8.1. 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。

4.8.2. 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

4.8.3. 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）。

4.8.4. 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。

4.8.5. 相关操作

4.8.5.1. 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：

告警监控

[首页](#) / [安全监控](#) / [告警监控](#)

待处理告警

已确认告警

已归档告警

待处理告警列表

过滤器管理

监控设置

确认

清除

请选择过滤器

导出

标签

序号		告警名称	策略名称	级别	对象IP	系统类型	类别	更新时间	总次	操作
1	☐	SSH会话关闭	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:59:03	10	☒ ☐ ☐
2	☐	root登录	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:54:00	2	☒ ☐ ☐
3	☐	SU会话开启	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:45	2	☒ ☐ ☐
4	☐	会话关闭	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:45	1	☒ ☐ ☐
5	☐	身份识别错误	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:10	1	☒ ☐ ☐

显示 10 条记录

显示 1 到 5 共 5 条记录

<<

<

1

>

>>

- 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，可以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：

基本信息

确认

清除

查看知识库

告警编号: 1

告警名称: root登录

级别: 一般

对象名称: 173

对象IP: 172.16.0.173

类别: 连接

系统类型: CentOS

策略名称: 登录

总次: 2

产生时间: 2015-06-01 10:19:46

更新时间: 2015-06-01 10:54:00

描述:

告警名称:

相关资产: 173

告警类别: 连接

严重级别: 一般

相关策略: 登录

产生时间: 2015-06-01 10:19:46

归并次数: 1

- 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：

过滤器列表

新增

删除

序号		过滤器名称	过滤器描述	操作
1		tass		
2		new		

显示 10 条记录

显示 1 到 2 共 2 条记录

<<

<

1

>

>>

- 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：

告警监控

首页 / 安全监控 / 告警监控

待处理告警

已确认告警

已归档告警

待处理告警列表

过滤器管理 监控设置

确认 清除

序号	告警名称	类别	更新时间	总次	操作
1	SSH会话	连接	2015-06-01 10:59:03	10	✓ 清除 导出
2	root登录	连接	2015-06-01 10:54:00	2	✓ 清除 导出
3	SU会话开	连接	2015-06-01 10:48:45	2	✓ 清除 导出
4	会话关闭	连接	2015-06-01 10:48:45	1	✓ 清除 导出
5	身份识别	连接	2015-06-01 10:48:10	1	✓ 清除 导出

显示 10 条记录

监控设置

※ 极重声音文件 请选择文件 选择文件

※ 严重声音文件 请选择文件 选择文件

※ 警告声音文件 请选择文件 选择文件

※ 一般声音文件 请选择文件 选择文件

保存 取消

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：

待处理告警列表

过滤器管理 监控设置

确认 清除 请选择过滤器 导出 标签

序号	告警名称	类别	更新时间	总次	操作
1	SSH会话关闭	连接	2015-06-01 10:59:03	10	✓ 清除 导出
2	root登录	连接	2015-06-01 10:54:00	2	✓ 清除 导出
3	SU会话开启	连接	2015-06-01 10:48:45	2	✓ 清除 导出
4	会话关闭	连接	2015-06-01 10:48:45	1	✓ 清除 导出
5	身份识别错误	连接	2015-06-01 10:48:10	1	✓ 清除 导出

显示 10 条记录

显示 1 到 5 共 5 条记录

告警确认

※ 确认原因

确认 取消

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：

待处理告警列表

过滤器管理 监控设置

确认 清除 请选择过滤器 导出 标签

序号	告警名称	类别	更新时间	总次	操作
1	SSH会话	连接	2015-06-01 10:59:03	10	✓ 清除 导出
2	root登录	连接	2015-06-01 10:54:00	2	✓ 清除 导出
3	SU会话开	连接	2015-06-01 10:48:45	2	✓ 清除 导出
4	会话关闭	连接	2015-06-01 10:48:45	1	✓ 清除 导出
5	身份识别错误	连接	2015-06-01 10:48:10	1	✓ 清除 导出

显示 10 条记录

显示 1 到 5 共 5 条记录

告警清除

※ 清除原因

清除 取消

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：

待处理告警列表 过滤器管理 监控设置

确认 清除 new 导出 标签

序号		请选择过滤器	级别	对象IP	系统类型	类别	更新时间	总次	操作
1	SSH	new	一般	172.16.0.173	CentOS	连接	2015-06-01 10:59:03	10	✓ 删除 打印
2	root	tass	一般	172.16.0.173	CentOS	连接	2015-06-01 10:54:00	2	✓ 删除 打印
3	SU会话开启	严重	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:45	2	✓ 删除 打印
4	会话关闭		一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:45	1	✓ 删除 打印
5	身份识别错误		一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:10	1	✓ 删除 打印

显示 10 条记录 显示 1 到 5 共 5 条记录

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：

待处理告警列表 过滤器管理 监控设置

确认 清除 请选择过滤器 导出 标签

序号		告警名称	策略名称	级别	对象IP	系统类型	类别	更新时间	总次	操作
1	SSH	会话关闭	登录			CentOS	连接	2015-06-01 10:59:03	10	✓ 删除 打印
2	root	登录	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:54:00	2	✓ 删除 打印
3	SU	会话开启	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:45	2	✓ 删除 打印
4	会话	关闭	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:45	1	✓ 删除 打印
5	身份	识别错误	登录	一般	172.16.0.173	CentOS	连接	2015-06-01 10:48:10	1	✓ 删除 打印

显示 10 条记录 显示 1 到 5 共 5 条记录

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：

待处理告警列表 过滤器管理 监控设置

确认 清除 请选择过滤器 导出 标签

序号		告警名称	策略名称	级别		类别	更新时间	总次	操作
1	☐	new 审计测试	登录	一般	17	连接	2015-06-01 14:23:46	1	☒ ☐ ☐
2	☒	SSH会话关闭	登录	一般	17	连接	2015-06-01 10:59:03	10	☒ ☐ ☐
3	☐	root登录	登录	一般	172.16.0.173	CentOS	2015-06-01 10:54:00	2	☒ ☐ ☐
4	☐	SU会话开启	登录	一般	172.16.0.173	CentOS	2015-06-01 10:48:45	2	☒ ☐ ☐
5	☐	会话关闭	登录	一般	172.16.0.173	CentOS	2015-06-01 10:48:45	1	☒ ☐ ☐
6	☐	身份识别错误	登录	一般	172.16.0.173	CentOS	2015-06-01 10:48:10	1	☒ ☐ ☐

显示 10 条记录 显示 1 到 6 共 6 条记录

4.8.5.2. 实时监控

- 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：

事件监控规则列表

+ 新增 - 删除

序号		规则名称	规则内容	操作
1	☐	登录过滤	事件类型 等于 访问控制	☐ ☒

显示 10 条记录 显示 1 到 1 共 1 条记录

- 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：

安全事件实时监控列表 规则设置

登录过滤 x 开始 导出

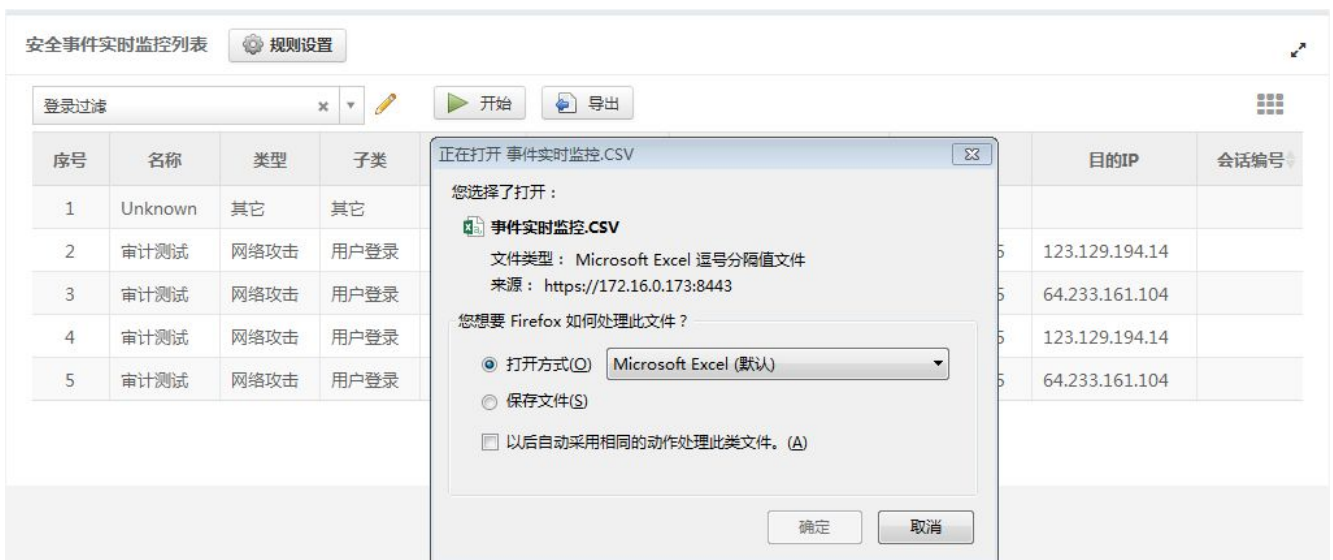
	类	严重级别	设备IP	接收时间	源IP	目的IP	会话编号
1	Unknown 其它 其它	信息	172.16.0.221	2015-06-01 14:51:12			
2	审计测试 网络攻击 用户登录		172.16.0.113	2015-06-01 14:51:17	202.108.22.5	123.129.194.14	
3	审计测试 网络攻击 用户登录		172.16.0.113	2015-06-01 14:51:17	202.108.22.5	64.233.161.104	
4	审计测试 网络攻击 用户登录		172.16.0.113	2015-06-01 14:51:18	202.108.22.5	123.129.194.14	
5	审计测试 网络攻击 用户登录		172.16.0.113	2015-06-01 14:51:18	202.108.22.5	64.233.161.104	

显示 1 到 5 共 5 条记录

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 CSV。如下图所示：



4.9. 报表管理

4.9.1. 相关操作

4.9.1.1. 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：

报表实例列表					
报表分组 日常报表 总体 主机类 网络设备类 防火墙类 数据库类 应用类 其它类 萨班斯报表 等级保护报表 新增 删除					
序号		实例名称	报表时间	更新时间	操作
1		Unix类主机日志分布日报	时间范围：每日	2015-05-30 10:54:11	
2		Windows类主机日志分布日报	时间范围：每日	2015-05-30 10:54:11	
3		主机访问控制分布日报-Linux	时间范围：每日	2015-05-30 10:54:11	
4		主机访问控制分布日报-Windows	时间范围：每日	2015-05-30 10:54:11	
5		其它类日志分布日报	时间范围：每日	2015-05-30 10:54:11	
6		安全告警分布情况日报	时间范围：每日	2015-05-30 10:54:11	
7		应用类日志分布日报	时间范围：每日	2015-05-30 10:54:11	
8		应用访问控制分布日报	时间范围：每日	2015-05-30 10:54:11	
9		数据库类日志分布日报	时间范围：每日	2015-05-30 10:54:11	
10		数据库访问控制分布日报	时间范围：每日	2015-05-30 10:54:11	
显示 10 条记录 显示 1 到 10 共 43 条记录 << < 1 2 3 4 5 > >>					

2. 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：

报表实例列表					
报表分组 日常报表 总体 主机类 网络设备类 防火墙类 数据库类 应用类 其它类 萨班斯报表 等级保护报表 自定义 新增 删除					
序号		实例名称	报表时间	更新时间	操作
1		Unix类主机日志分布日报	时间范围：每日	2015-05-30 10:54:11	
2		Windows类主机日志分布日报	时间范围：每日	2015-05-30 10:54:11	
3		主机访问控制分布日报-Linux	时间范围：每日	2015-05-30 10:54:11	
4		主机访问控制分布日报-Windows	时间范围：每日	2015-05-30 10:54:11	
5		其它类日志分布日报	时间范围：每日	2015-05-30 10:54:11	
6		安全告警分布情况日报	时间范围：每日	2015-05-30 10:54:11	

3. 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：

报表管理

首页 / 报表管理

导出HTML 导出PDF 导出EXCEL 导出WORD

报表实例详细信息

报表实例名称: Unix类主机日志分布日报

创建时间: 2015-06-09 10:07:19

创建人: 系统管理员

查询条件: 时间范围: 2015-06-10 00:00:00 ~ 2015-06-10 23:59:59

设备类型: Unix/Linux主机

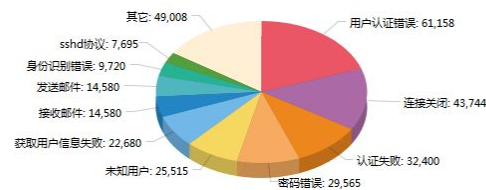
分组字段: 事件名称

列表字段: 事件名称,事件类型,事件严重级别,设备地址

描述:

安全事件分布统计

用户认证错误 连接关闭 认证失败 密码错误 未知用户 获取用户信息失败 接收邮件
发送邮件 身份识别错误 sshd协议 其它



详细列表

序号	事件名称	事件类型	事件严重级别	设备地址	数量
1	用户认证错误	访问控制	低级	172.16.0.2	61158
2	连接关闭	访问控制	信息	172.16.0.2	43744
3	认证失败	访问控制	低级	172.16.0.2	32400
4	密码错误	访问控制	低级	172.16.0.2	29565
5	未知用户	访问控制	信息	172.16.0.2	25515
6	获取用户信息失败	访问控制	低级	172.16.0.2	22680
7	接收邮件	配置状态	信息	172.16.0.2	14580
8	发送邮件	配置状态	信息	172.16.0.2	14580
9	身份识别错误	访问控制	低级	172.16.0.2	9720
10	sshd协议	连接	低级	172.16.0.2	7695

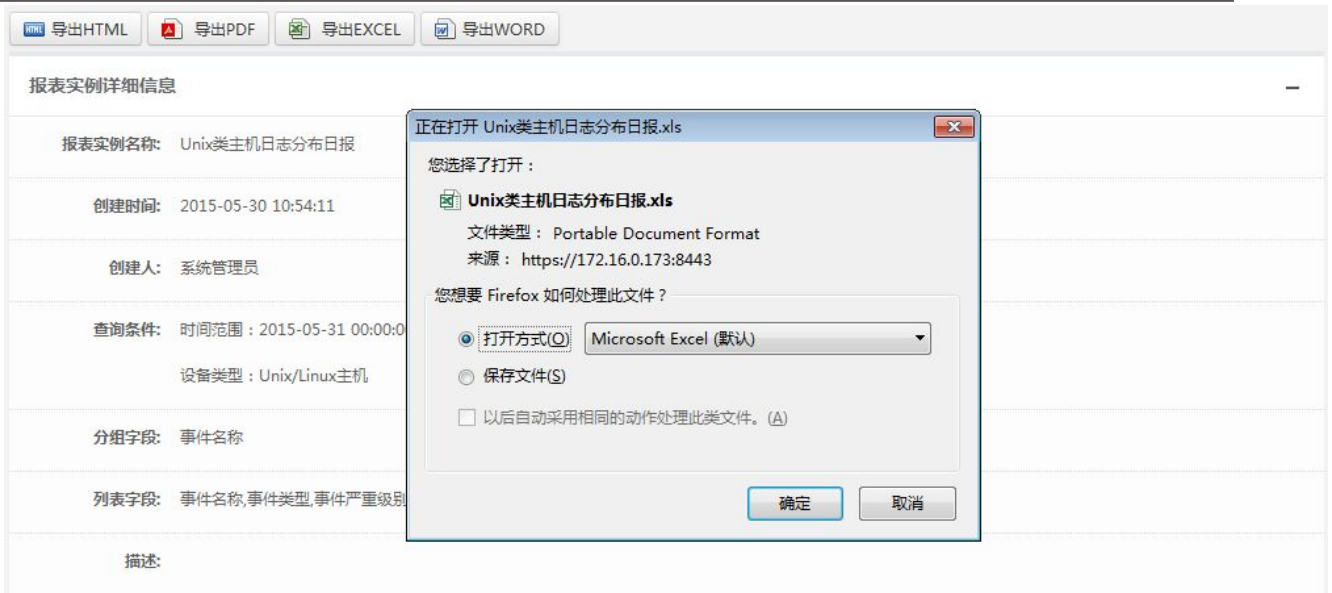
显示 10 条记录

显示 1 到 10 共 25 条记录

<< < 1 2 3 > >>

返回

4. 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:



5. 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：

新增报表实例

✱ 实例名称

✱ 模板类别 ✱ 模板名称

描述

6. 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：

修改报表

※ 实例名称	Unix类主机日志分布日报		
※ 模版类别	安全事件报表	※ 模版名称	安全事件分布统计
事件名称		时间范围	每日
事件类型	请选择	事件子类	请选择
设备类型	Unix/Linux主机	事件严重级别	请选择
源地址		目的地址	
目的端口		源用户	
目的用户		采集器地址	

4.9.1.2. 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：

报表任务列表

+ 新增 - 删除

序号		
1		new

显示 10 条记录

任务详情

任务名称: new

实例名称: 日志总体分布日报

任务类型: 立即执行

执行时间: 2015-06-01 15:19

发送类型: pdf

收件人: 系统管理员

任务类型	更新时间	操作

显示 1 到 1 共 1 条记录

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：

新增报表任务

✕

✱ 任务名称

✱ 实例选择

请选择

✱ 任务类型

立即执行

▼

✱ 发送类型

PDF

▼

✱ 收件人

请选择

附加收件人

描述

保存

取消

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：

报表任务列表

+

 新增

✕

 删除

序号	☒	
1	☒	new

显示 10 条记录

更新时间

操作

是

否

确认

✕

⚠ 确定要删除选择的记录吗?

是

否

4.10. 知识库管理

4.10.1. 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）

- 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）

4.10.2. 相关操作

- 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：

日志配置类						
+ 新增 ✖ 删除						
序号	☐	标题	摘要	创建时间	是否内置	操作
1	☐	AIX日志配置	1. 登陆到Aix系统中，执行命令：vi /etc...	2015-05-22 07:57:14	内置	
2	☐	APACHE日志配置	需要在Windows服务器上安装提供的采集程序SE...	2015-05-22 07:57:14	内置	
3	☐	CATALYST日志配置	1. set logging server ena...	2015-05-22 07:57:14	内置	
4	☐	CHECKPOINT日志配置	收集事件需要使用提供的lea_client软件。 ...	2015-05-22 07:57:14	内置	
5	☐	CISCO-ASA日志配置	以管理者身份登录ASA防火墙，然后输入以下命令配置...	2015-05-22 07:57:14	内置	
6	☐	CISCO-PIX日志配置	以管理者身份登录Pix防火墙，然后输入以下命令配置...	2015-05-22 07:57:14	内置	
7	☐	CISCO日志配置	通过telnet远程登录cisco系统，执行如下操...	2015-05-22 07:57:14	内置	
8	☐	CYBERWALL日志配置	1. 在IE地址栏中输入https:// xxx.x...	2015-05-22 07:57:14	内置	
9	☐	ERICSSON爱立信日志配置	通过ODBC方式从sybase数据库获取爱立信程控...	2015-05-22 07:57:14	内置	
10	☐	EXCHANGE日志配置	Exchange和windows系统需要配置日志发...	2015-05-22 07:57:14	内置	
显示 10 条记录 显示 1 到 10 共 51 条记录 << < 1 2 3 4 5 > >>						

- 查看知识库详情：查看知识库的详细内容。如下图所示：

知识库详情

标题:	Address-sweep扫描探测	告警规则:	
适用产品:	Windows	告警大类:	
告警级别:		告警子类:	
日期:	2015-05-22	是否内置:	内置
告警描述:	当防火墙检测到某IP进行顺序的IP地址扫描导致的，例如Ping 192.168.0.1~254的连续行为。通过sweep扫描，可以获得目标主机存活情况。		
告警触发建议:	根据发生的频率进行告警，10次/分钟以上，产生一次告警。		
解决方案:	SRC管理员（源地址业务系统管理员）根据源IP地址发生频率、时间等因素，结合源IP的业务应用情况，分析该行为是否是属于正常业务需求还是其他恶意行为，例如是正常的漏洞扫描还是其他恶意攻击行为等。 Address sweep对系统危害低，在公网中经常发生此类事件，假如在内部网络中发生大量的Address sweep行为，则可认为是可疑行为，需要由源地址所在系统管理员检查Address sweep的来源机器是否存在扫描软件。 Address sweep需要结合后续的攻击行为，确定是否存在恶意攻击。		
参考链接:			

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：

新增日志配置类

✳ 标题

适用产品

前提条件

✳ 配置方法

配置要点

保存

取消

修改日志配置类

✖ 标题
Syslog日志配置

适用产品
请输入

前提条件

✖ 配置方法
登录指定IP的服务器
进入到配置的对应目录
执行命令XX

配置要点

保存 取消

日志配置类

+ 新增 ✖ 删除

序号		标题	摘要	创建时间	是否内置	操作
1	☐	Syslog日志配置		2015-06-11 13:17:19	自定义	✖
2	☐	AIX日志配置		2015-06-09 10:07:18	内置	
3	☐	FREEBSD日志配置		2015-06-09 10:07:18	内置	
4	☐	LINUX日志配置		2015-06-09 10:07:18	内置	
5	☐	CATALYST日志配置		2015-06-09 10:07:18	内置	
6	☐	REDBACK SE800日...	1. 在console口上可以显示log信息。 [...	2015-06-09 10:07:18	内置	
7	☐	JUNIPER ROUTER日...	通过telnet远程登录系统，执行如下操作： h...	2015-06-09 10:07:18	内置	
8	☐	LINKTRUST SCANN...	1.通过浏览器登录扫描器web页面, 2.在 "系...	2015-06-09 10:07:18	内置	
9	☐	安泰特交换机日志配置	在启用 syslog 之前，需要先启用交换机的三层...	2015-06-09 10:07:18	内置	
10	☐	CYBERWALL日志配置	1. 在IE地址栏中输入https:// xxx.x...	2015-06-09 10:07:18	内置	

显示 10 条记录

显示 1 到 10 共 52 条记录

<< < 1 2 3 4 5 > >>

确认

⚠ 确定要删除选择的记录吗?

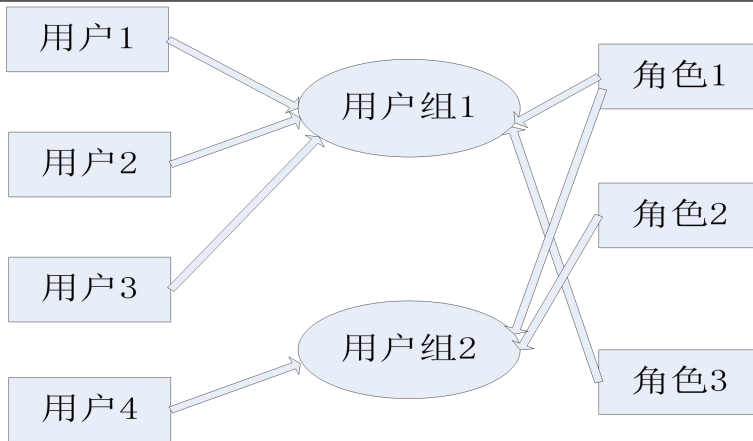
是 否

4.11. 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。

4.11.1. 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：



4.11.1.1. 角色管理

- 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：

用户管理					
首页 / 系统管理 / 用户管理					
			用户	用户组	角色
角色列表					
新增 删除					
序号		角色名	授权用户组	描述	操作
1	☐	安全审计员	超级管理员组,安全审计员组	安全审计员只对日志管理菜单予以...	
2	☐	安全管理员	超级管理员组,安全管理员组	安全管理员对除系统管理以外的所...	
3	☐	系统管理员	超级管理员组,系统管理员组	系统管理员仅对系统管理菜单下除...	
显示 10 条记录		显示 1 到 3 共 3 条记录		<< < 1 > >>	

- 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：

新增角色

友情提示： " * " 标注为必填项

* 角色名

描述

* 菜单授权 ☐ 全选/取消全选

☐ 安全概览	☐ 事件分析
☐ 知识库	☐ 事件分析->关联策略
☐ 安全监控	☐ 事件分析->事件列表
☐ 安全监控->告警监控	☐ 事件分析->关联事件
☐ 安全监控->实时监控	☐ 资产管理
☐ 报表管理	☐ 资产管理->资产管理
	☐ 资产管理->网络管理
	☐ 资产管理->资产发现

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：

修改角色

友情提示： " * " 标注为必填项

* 角色名

描述

* 菜单授权 ☐ 全选/取消全选

☒ 安全概览	☒ 事件分析
☒ 知识库	☒ 事件分析->关联策略
☒ 安全监控	☒ 事件分析->事件列表
☒ 安全监控->告警监控	☒ 事件分析->关联事件
☒ 安全监控->实时监控	☒ 资产管理
☒ 报表管理	☒ 资产管理->资产管理
	☒ 资产管理->网络管理
	☒ 资产管理->资产发现

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：

用户管理

首页 / 系统管理 / 用户管理

用户 用户组 角色

角色列表

+ 新增 - 删除

序号	☒	角色名	描述	操作
1	☒	new		 
2	☐	安全审计员	对日志管理菜单予以...	
3	☐	安全管理员	除系统管理以外的所...	
4	☐	系统管理员	超级管理员组,系统管理员组 系统管理员仅对系统管理菜单下除...	

显示 10 条记录

显示 1 到 4 共 4 条记录

« < 1 > »

确认

⚠ 确定要删除选择的记录吗?

是

否

4.11.1.2. 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：

用户管理

首页 / 系统管理 / 用户管理

用户 用户组 角色

用户组列表

+ 新增 - 删除

序号	☐	用户组名	成员	描述	操作
1	☐	安全审计员组		安全审计员组中的成员只具有日志管理菜单操作权限，且...	
2	☐	安全管理员组		安全管理员组中的成员对除系统管理以外的所有菜单进行...	
3	☐	系统管理员组		系统管理员组中的成员只具有系统管理菜单操作权限，且...	
4	☐	超级管理员组	系统管理员	超级管理员组中的成员可以对系统中所有菜单及安全对象...	

显示 10 条记录

显示 1 到 4 共 4 条记录

« < 1 > »

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：

新增用户组

友情提示：* 标注为必填项

* 用户组名

描述

* 角色授权 ☐ 系统管理员 ☐ 安全审计员 ☐ 安全管理员 ☐ new

安全对象 ☒ 全部 ☐ 选择

3. 修改用户组：修改用户组相关属性。如下图所示：

修改用户组

友情提示：* 标注为必填项

* 用户组名

描述

* 角色授权 ☐ 系统管理员 ☐ 安全审计员 ☐ 安全管理员 ☒ new

安全对象 ☒ 全部 ☐ 选择

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：

安全对象 ☐ 全部 ☒ 选择

请选择目标资产

☐ 资产
☐ 网络
☐ 视图

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：

用户管理

首页 / 系统管理 / 用户管理

用户 用户组 角色

用户组列表

+ 新增 - 删除

序号	☐	用户组名称	描述	操作
1	☒	new		 
2	☐	安全审计	管理菜单操作权限，且...	
3	☐	安全管理	理以外的所有菜单进行...	
4	☐	系统管理员组	系统管理员组中的成员只具有系统管理菜单操作权限，且...	
5	☐	超级管理员组	超级管理员组中的成员可以对系统中所有菜单及安全对象...	

显示 10 条记录

显示 1 到 5 共 5 条记录

<< < 1 > >>

确认

⚠ 确定要删除选择的记录吗?

是

否

4.11.1.3. 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：

用户管理

首页 / 系统管理 / 用户管理

用户 用户组 角色

用户列表

+ 新增 - 删除 解锁

序号	☐	登录名	用户名	所属用户组	状态	密码是否过期	创建时间	最近一次登录时间	操作
1	☐	admin	系统管理员	超级管理员组	活动	否	2015-05-28 11:12:13	2015-05-28 14:30:50	

显示 10 条记录

显示 1 到 1 共 1 条记录

<< < 1 > >>

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：

登录管理策略	用户最大登录失败次数 (次)	5	用户登录失败锁定方式	不锁定
	用户锁定时间长度 (分钟)	15	同名用户在线	☒ 允许 ☐ 不允许
	界面用户显示方式	用户名		
Syslog设置	Syslog服务器一地址		Syslog服务器一端口	514
	Syslog服务器二地址		Syslog服务器二端口	514
	Syslog服务器三地址		Syslog服务器三端口	514
	Syslog服务器四地址		Syslog服务器四端口	514
NTP服务器	NTP地址	cn.pool.ntp.org	NTP端口	123
	更新间隔时间 (小时)	24		
用户密码获取方式	用户密码发送方式 ☒ 通过界面输入密码 ☐ 通过电子邮件发送密码			
保存				

新增用户

友情提示：* * 标注为必填项

✖ 登录名

✖ 用户名

工号

电话号码

✖ 邮箱

✖ 手机号码

✖ 口令策略

请选择

👁️ +

✖ 密码

✖ 确认密码

✖ 所属用户组

请选择

▼ +

IP认证

☐

描述

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：

修改用户

友情提示：* 标注为必填项

* 登录名	admin	* 用户名	系统管理员
工号		电话号码	
* 邮箱	xxx@x.com	* 手机号码	
* 口令策略	缺省口令策略	* 密码	
* 确认密码		* 所属用户组	超级管理员组
IP认证	☐		
描述	系统管理员		

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：

用户管理

首页 / 系统管理 / 用户管理

用户 用户组 角色

用户列表

+ 新增 - 删除 解锁

序号	☒	登录名	创建时间	最近一次登录时间	操作
1	☒	adminot	2015-05-28 14:45:32		
2	☐	admin	2015-05-28 11:12:13	2015-05-28 14:30:50	

显示 10 条记录

确认

确定要删除选择的记录吗?

是 否

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：

用户管理

首页 / 系统管理 / 用户管理

用户

用户组

角色

用户列表

新增 删除 解锁

序号		登录名	最近一次登录时间	操作
1	☒	adminother	2015-05-28 14:45:32	编辑 删除 解锁
2	☐	admin	2015-05-28 11:12:13	编辑

确认

确定要解锁?

是

否

4.11.2. 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。

4.11.2.1. 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：

日志管理

首页 / 系统管理 / 日志管理

用户日志

系统日志

用户日志列表

友情提示：导出全部日志可能数据巨大，请输入查询条件后再导出。

导出

序号	日志级别	日志内容	日志产生时间
1	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:49:28
2	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:48:26
3	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:47:56
4	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:46:39
5	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:45:45
6	信息	来自客户端(172.16.0.2),用户(系统管理员)新增用户	2015-05-28 14:45:32
7	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:45:01
8	信息	来自客户端(127.0.0.1),用户(系统管理员)待处理告警列表	2015-05-28 14:44:56

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：

用户日志列表

友情提示：导出全部日志可能数据巨大, 请输入查询条件后再导出。

导出

PDF
Excel
Word

		日志内容	日志产生时间
		来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:49:28
2	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:48:26
3	信息	来自客户端(127.0.0.1),用户(系统管理员)已确认告警列表	2015-05-28 14:47:56

4.11.2.2. 系统日志管理

- 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：

首页 / 系统管理 / 日志管理

用户日志 系统日志

系统日志列表

友情提示：导出全部日志可能数据巨大, 请输入查询条件后再导出。

导出

序号	组件名称	日志级别	日志内容	日志产生时间
1	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
2	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
3	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
4	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
5	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
6	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
7	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
8	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
9	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
10	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15

显示 10 条记录

显示 1 到 10 共 10,000 条记录 (实际查询到 1,169,328)

« < 1 2 3 4 5 > »

- 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：

系统日志列表

友情提示：导出全部日志可能数据巨大, 请输入查询条件后再导出。

导出

PDF
Excel
Word

		日志级别	日志内容	日志产生时间
		信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
2	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
3	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
4	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
5	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
6	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15
7	采集器	信息	ip 地址解析失败Invalid IP content!	2015-06-05 09:15:15

4.11.2.3. 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：

日志管理策略	日志保留期限(天)	31
--------	-----------	----

4.11.3. 系统参数管理

4.11.3.1. 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：

系统参数

首页 / 系统管理 / 系统参数

系统参数

口令策略

系统参数

SMTP服务器设置	Email发件人地址		SMTP服务器地址	
	邮件发送帐号		邮件发送帐号密码	
	邮件发送端口	25	发送邮件是否需要认证	☒ 不需要 ☐ 需要
	测试邮箱地址	请输入测试邮箱地址	<button>保存设置并发送测试邮件</button>	
SNMP Traps设置	Community	tass	SNMP服务器地址	
	SNMP服务器端口	162	企业节点号	1.3.6.1.4.1.8885.2.3.1
	oid节点号	1.3.6.1.4.1.8885.2.3.1.1.2.1		
日志管理策略	日志保留期限 (天)	31		

登录管理策略	用户最大登录失败次数 (次)	5	用户登录失败锁定方式	不锁定
	用户锁定时间长度 (分钟)	15	同名用户在线	☒ 允许 ☐ 不允许
	界面用户显示方式	用户名		
Syslog设置	Syslog服务器一地址		Syslog服务器一端口	514
	Syslog服务器二地址		Syslog服务器二端口	514
	Syslog服务器三地址		Syslog服务器三端口	514
	Syslog服务器四地址		Syslog服务器四端口	514
NTP服务器	NTP地址	cn.pool.ntp.org	NTP端口	123
	更新间隔时间 (小时)	24		
用户密码获取方式	用户密码发送方式	☒ 通过界面输入密码 ☐ 通过电子邮件发送密码		

保存

4.11.3.2. 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：

系统参数

首页 / 系统管理 / 系统参数

系统参数

口令策略

口令策略管理列表

[+ 新增](#) [✖ 删除](#)

序号		策略名称	创建人	更新时间	是否内置	是否被使用	操作
1	☐	缺省口令策略	系统管理员	2015-05-28 11:12:13	内置	正在被使用	

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：

新增口令策略

✖ 口令策略名称

✖ 口令长度范围

-

位

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

是否检查历史代码

☐ 是
 ☒ 否

不允许使用与用户名相同口令

☐ 是
 ☒ 否

口令是否过期

☐ 是
 ☒ 否

描述

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：

修改口令策略

* 口令策略名称

* 口令长度范围 - 位

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

是否检查历史代码 ☐ 是 ☒ 否

不允许使用与用户名相同口令 ☐ 是 ☒ 否

口令是否过期 ☐ 是 ☒ 否

描述

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：

口令策略管理列表

新增 删除

序号		策略名称	是否内置	是否被使用	操作
1	☐	缺省口令策略	内置	正在被使用	
2	☐	new	自定义		

确认

⚠ 确定要删除选择的记录吗?

4.11.4. 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：

内置对象

首页 / 系统管理 / 内置对象

厂商

产品

系统类型

厂商列表

+ 新增 - 删除

序号	☐	名称	电话	主页	地址	描述	是否内置	操作
1	☐	Adobe					内置	
2	☐	Apache					内置	
3	☐	Apple					内置	
4	☐	Bluecoat					内置	
5	☐	CrossBeam					内置	
6	☐	ERICSSON					内置	

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：

内置对象

首页 / 系统管理 / 内置对象

厂商

产品

系统类型

产品列表

+ 新增 - 删除

序号	☐	产品名称	产品厂商	产品型号	描述	是否内置	操作
1	☐	Alcatel Rout...	阿尔卡特(Alcatel...	3	Alcatel Router/...	内置	
2	☐	Apache	Apache	15	Apache	内置	
3	☐	Apache Tomca...	Apache	15	Apache Tomcat	内置	
4	☐	Arcsight	惠普(HP)	51	Arcsight	内置	
5	☐	Big Iron	Foundry	3	Big Iron	内置	

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：

内置对象

首页 / 系统管理 / 内置对象

厂商

产品

系统类型

系统类型列表

+ 新增 - 删除

序号	☐	系统类型	产品	厂商	描述	是否内置	操作
1	☐	AIX 5	IBM AIX	IBM	IBM AIX 5	内置	
2	☐	Alcatel Rout...	Alcatel Rout...	阿尔卡特(Alcatel...	Alcatel Router/...	内置	
3	☐	Apache	Apache	Apache	Apache	内置	
4	☐	Arcsight Exp...	Arcsight	惠普(HP)	Arcsight Expres...	内置	
5	☐	Arcsight Log...	Arcsight	惠普(HP)	Arcsight Logger	内置	

4.11.5. 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：

升级管理

首页 / 系统管理 / 升级管理

系统升级

文件保存路径:

请选择文件

选择文件

升级

升级列表

序号	升级内容	升级前版本	升级后版本	升级结果	升级时间
当前无可用记录					

显示

10

条记录

显示 0 到 0 共 0 条记录

<<

<

>

>>

4.11.6. 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：

许可证管理

首页 / 系统管理 / 许可证管理

许可证

客户名: TASS

有效期: 2015-08-04

服务有效期: 2015-08-04

采集控制器数量: 2个

设备数: 200个

序列号: ae1b50b1-beca-4f21-8a1c-cb858b11a623

主机标识码: DF7B10C4-4FA5-5AB7-9360-F76DE4D6F9B6

许可证更新

许可证升级列表

序号	许可证升级时间	描述
1	2015-06-09 10:11:17	此许可证有效期至2015-08-04，服务有效期至2015-08-04，含有200个设备数，拥有全部...

显示

10

条记录

显示 1 到 1 共 1 条记录

<<

<

1

>

>>

性能参数列表

型号	JNTA-SAS-STD	JNTA-SAS-PRO	JNTA-SAS-ENT
并发用户数	小于等于10个	小于等于30个	大于50个
最大吞吐量	2000EPS	5000EPS	8000EPS
部署方式	一体式	一体式、分布式	一体式、分布式
采集控制器	1个（不可扩展）	1个（最多可扩展到5个）	不限
可管理设备数量	100个（不可扩展）	100个（可扩展到300个）	100个（可扩展1000个）
支持的采集方式	Syslog、Snmp Trap、WMI、socket、文件、数据库	Syslog、Snmp Trap、WMI、socket、文件、数据库	Syslog、Snmp Trap、WMI、socket、文件、数据库

4.12. 其它

4.12.1. 安全概览

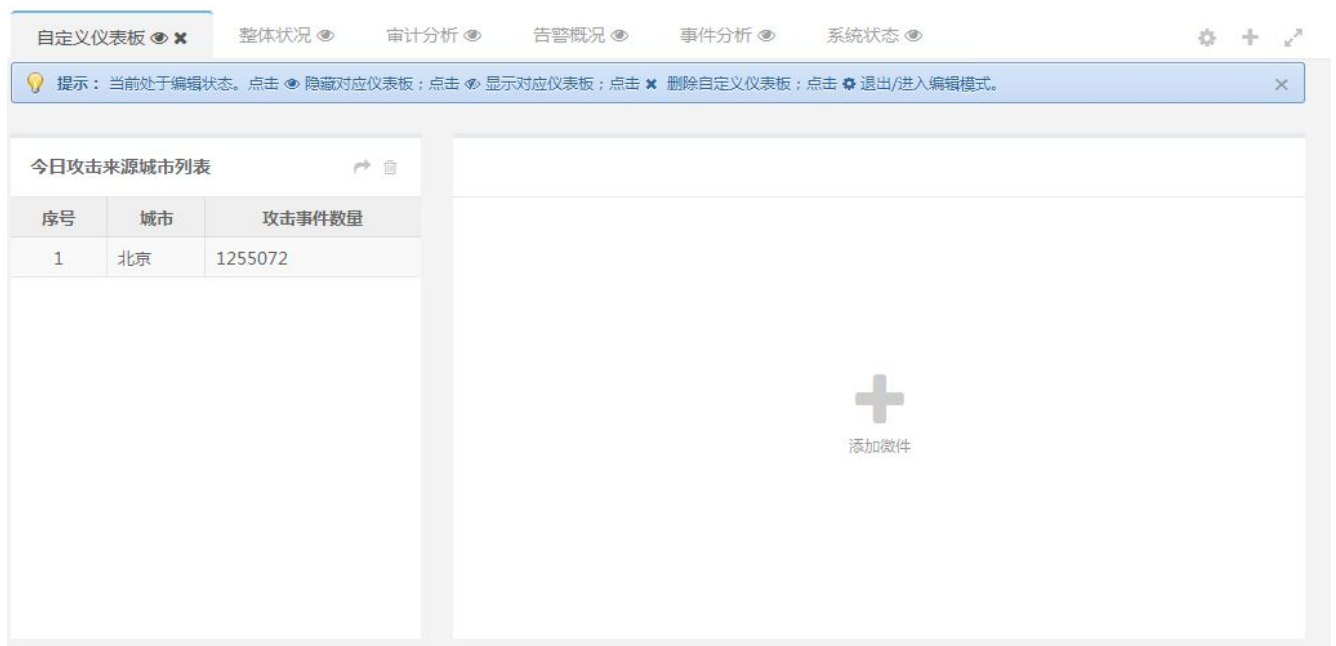
安全概览是日志审计系统风险的集中展示区域，也是日志审计系统展现给用户的第一个视觉界面；它支持以 TAB 页及微件（Widget）形式展现，用户也可对仪表的布局和内容进行调整。

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：

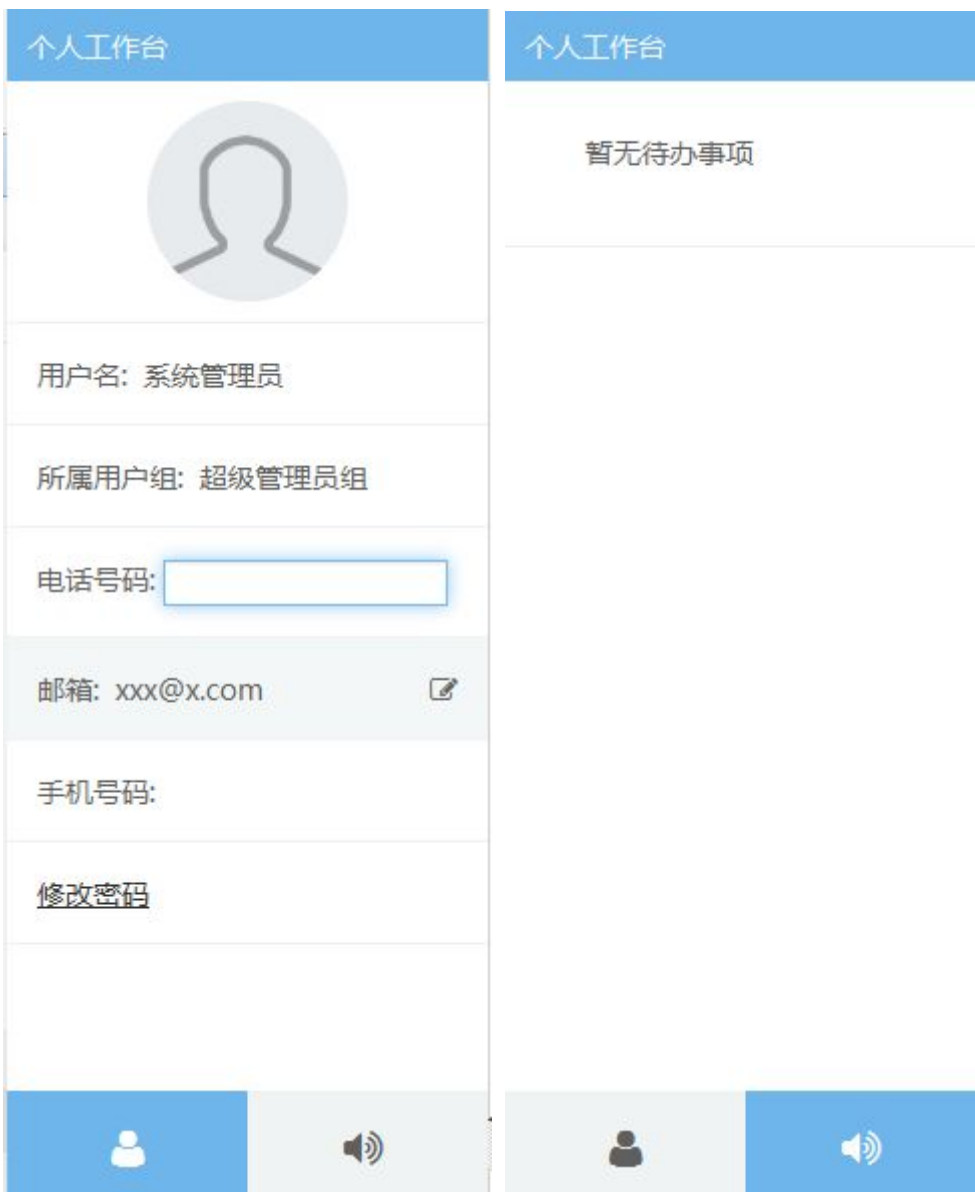


4.12.2. 个人工作台

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：



4.12.3. 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：



铨迅信息**Yxlink**

未获得南京铨迅信息技术股份有限公司的书面许可，不可擅自以任何形式复制此说明书的全部或部分内容（评价或介绍文章的简单引用除外）。

南京铨迅信息技术股份有限公司

江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

Nanjing Yxlink Information**Technology Co., Ltd.**

4th floor, Building D of Qinsheng Science Park, No. 18

Ningshuang Rd., Yuhua District, Nanjing, Jiangsu, P.R.China

NJYXHWAFAM010-11(02)