天翼云 • 安全专区•云日志审计

用户使用指南

天翼云科技有限公司

目　录

1 业务控制台说明

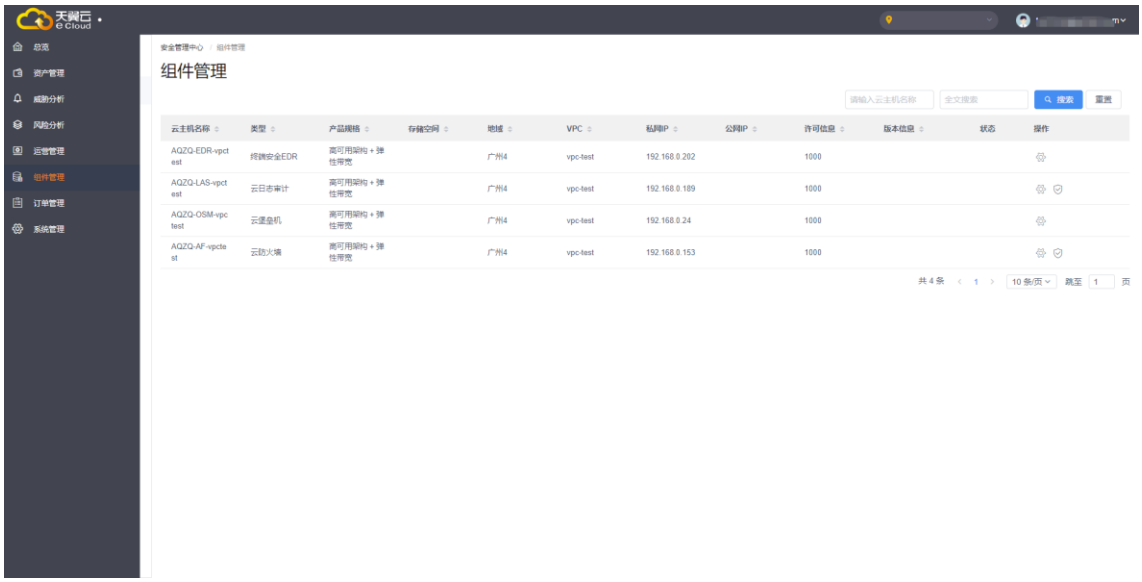
用户对 LAS 系统的绝大部分操作主要通过业务控制台完成。通过业务控制台可以对 LAS 系统的具体业务模块进行设置、安全内容进行查看，主要包含授权更新、日志标准化设置、资产管理、告警策略配置、安全事件查看等等。

使用 WEB 方式登录方式

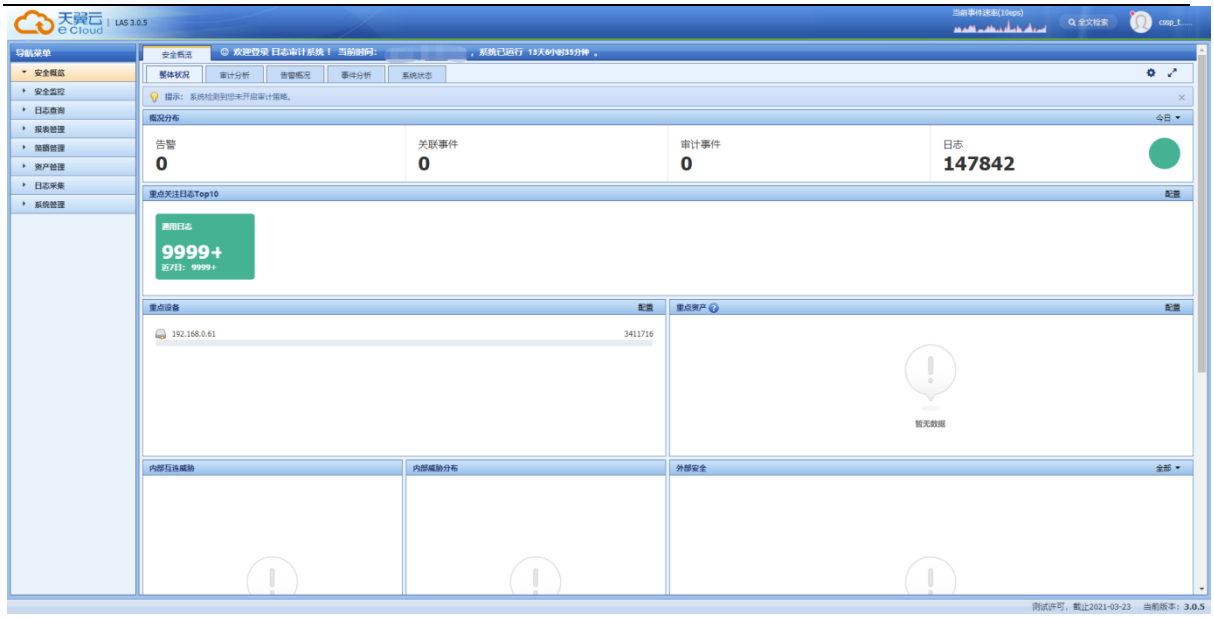
操作步骤:

单点登录日志审计

1、 通过天翼云安全账号登录天翼云控制中心，进入天翼云等保安全专区安全管理平台，在平台中找到安全专区，点击【云日志审计】->【操作】登录。



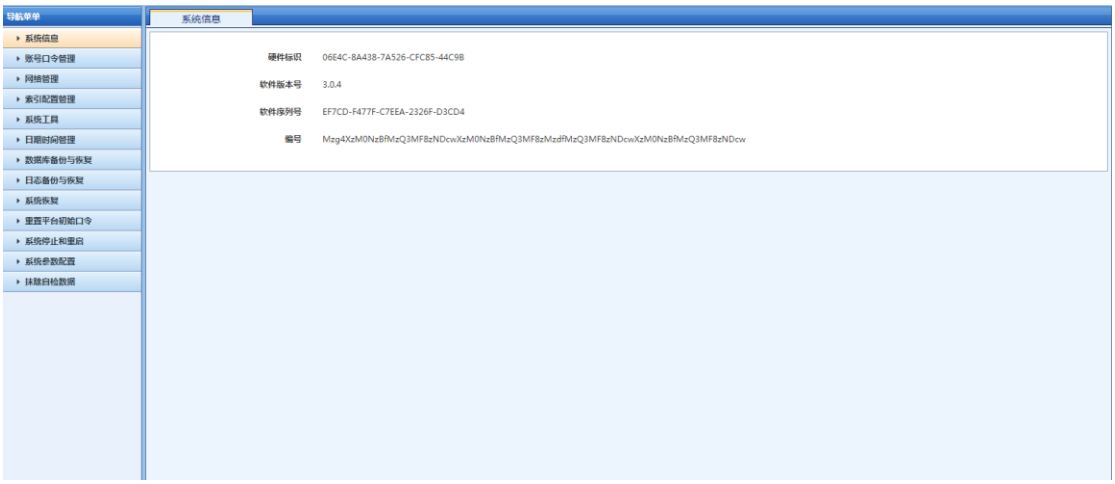
2、从安全管理平台进行单点登录，无需密码，点击进入，即跳转进入。



1.1. 管理控制台说明

1.1.1. 系统信息

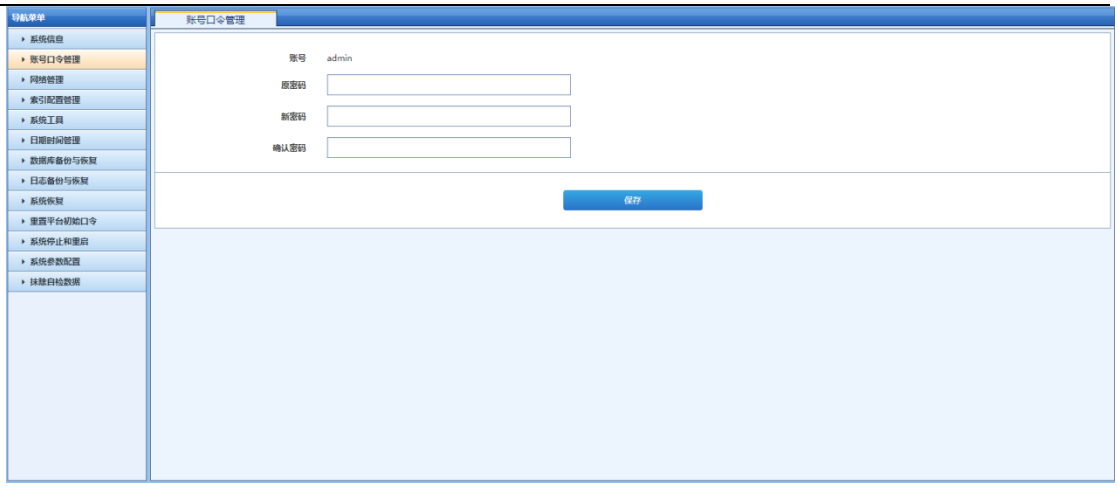
展示产品硬件、版本等信息，如下：



展示产品硬件、版本等信息。

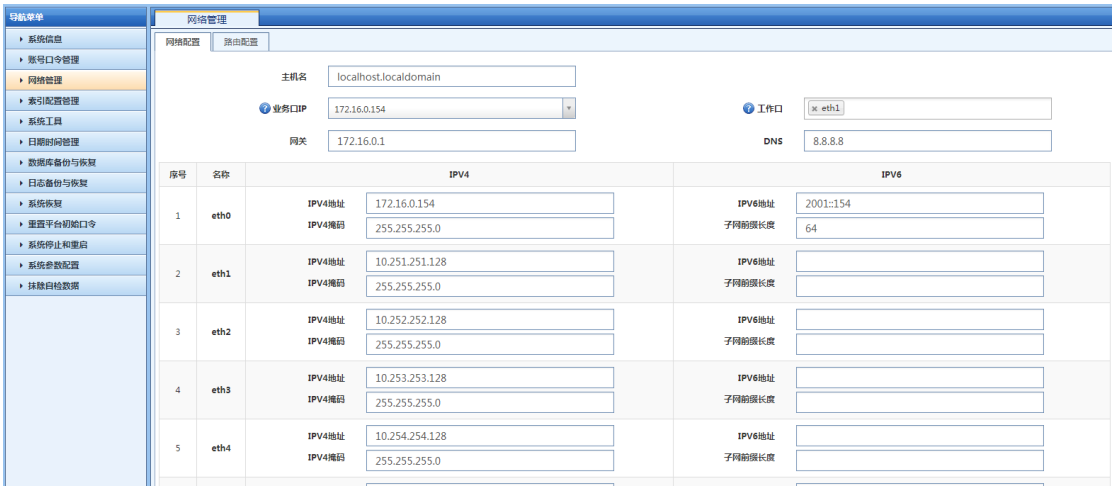
1.1.2. 账号口令管理

用户可以修改管理的口令，如下：

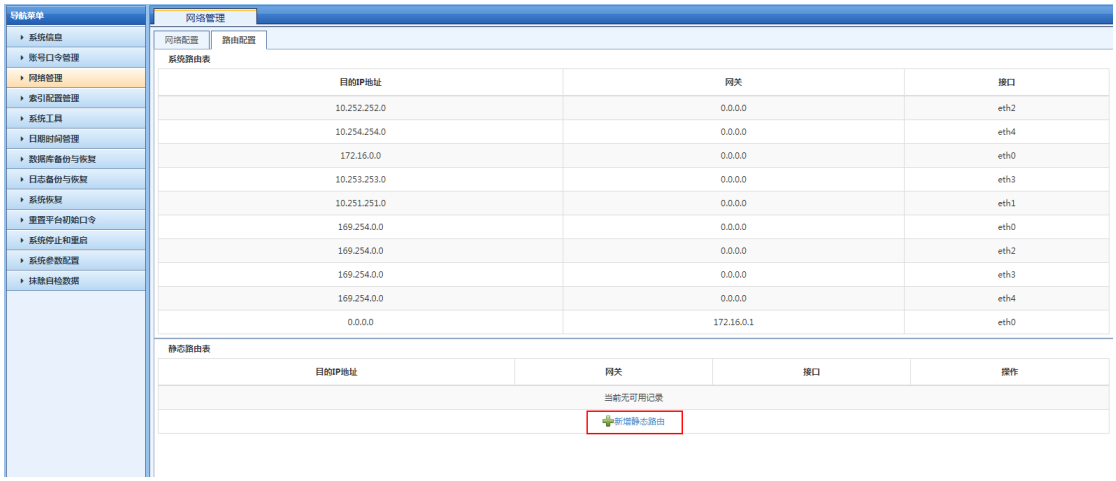


1.1.3. 网络管理

1. 用户可以设置网络的地址、掩码、DNS、网关等（工作口配置任何网口都可用于流量接入口使用），如下：

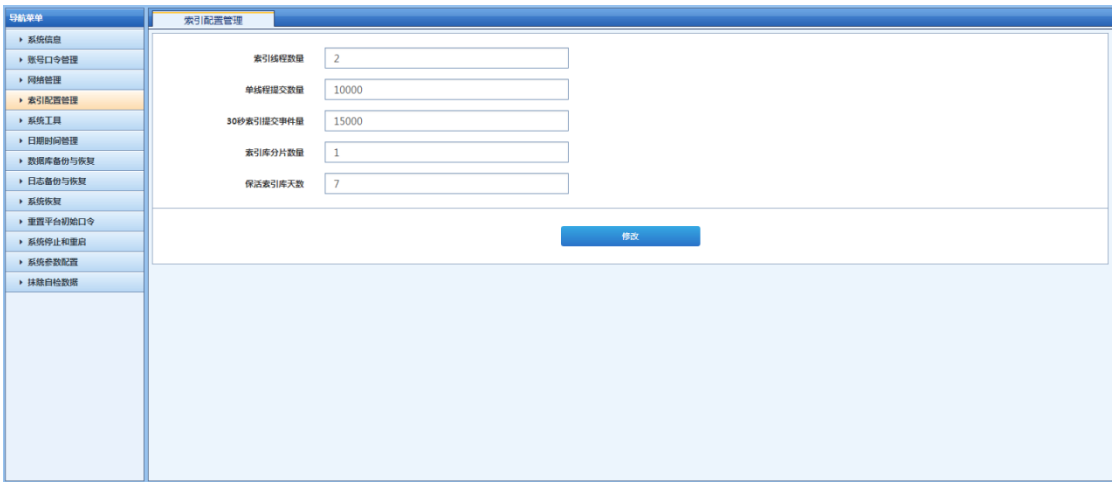


2.路由配置工具：设置系统路由信息



1.1.4. 日志配置管理

配置日志库提交线程与性能，如下：

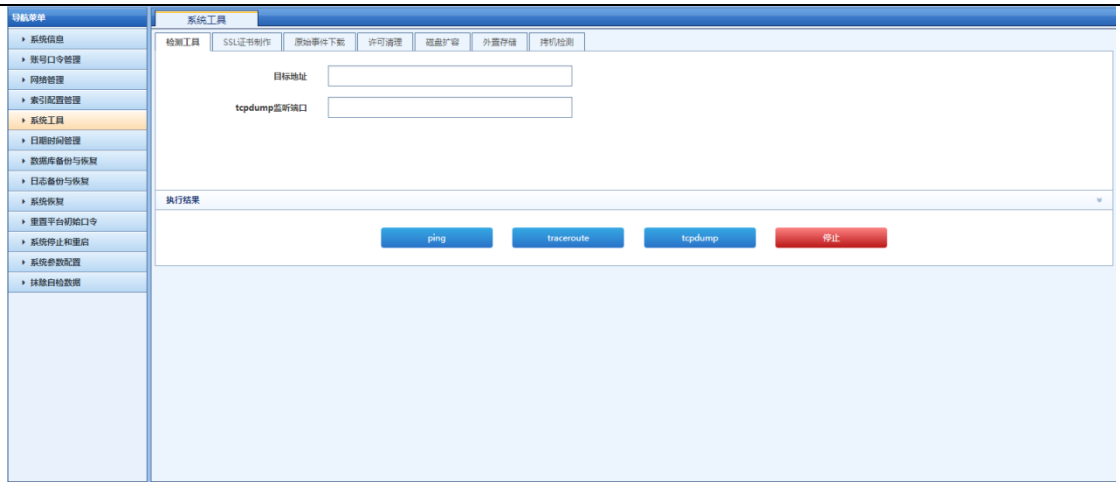


详细说明：

参数项	优化说明
日志线程数量	1、 提交日志的线程数与 CPU 的线程数有关系，可以配置最大线程数的一半 2、 可以提升事件的写入性能
单线程提交数量	1、 单线程的日志写入能力，依赖 CPU 的性能，默认配置 10000，一般不建议修改
30 秒日志提交事件量	1、 触发日志序列化的数据量大小，一般不建议修改
日志库分片数量	1、 非集群项目不做修改
保活日志天数	1、 ES 保持开启的最大日志库数量，默认 31 天，如果业务上对 31 天以前的数据 2、 不频繁查询，不建议修改

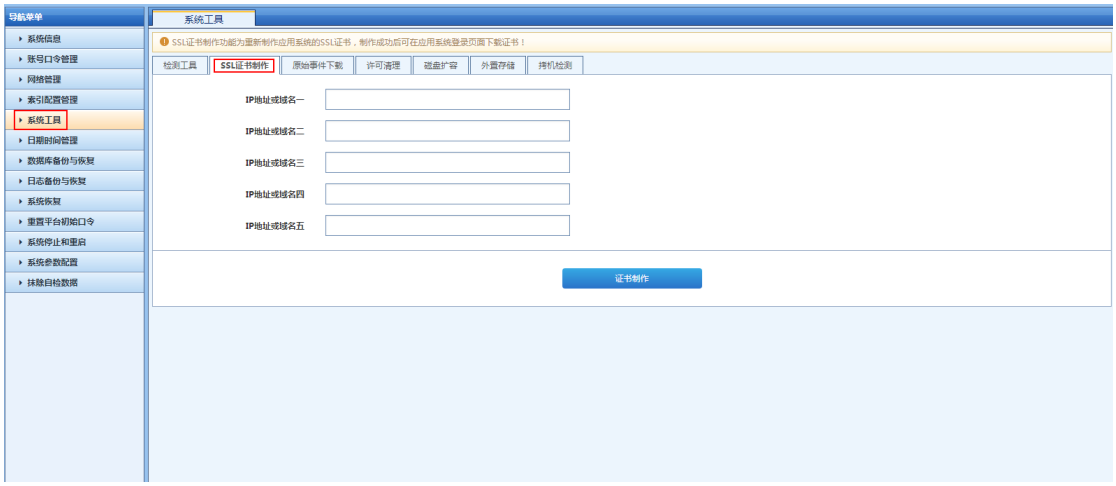
1.1.5. 系统工具

1. 检测工具：对目标地址进行 traceroute、ping、tcpdump 操作



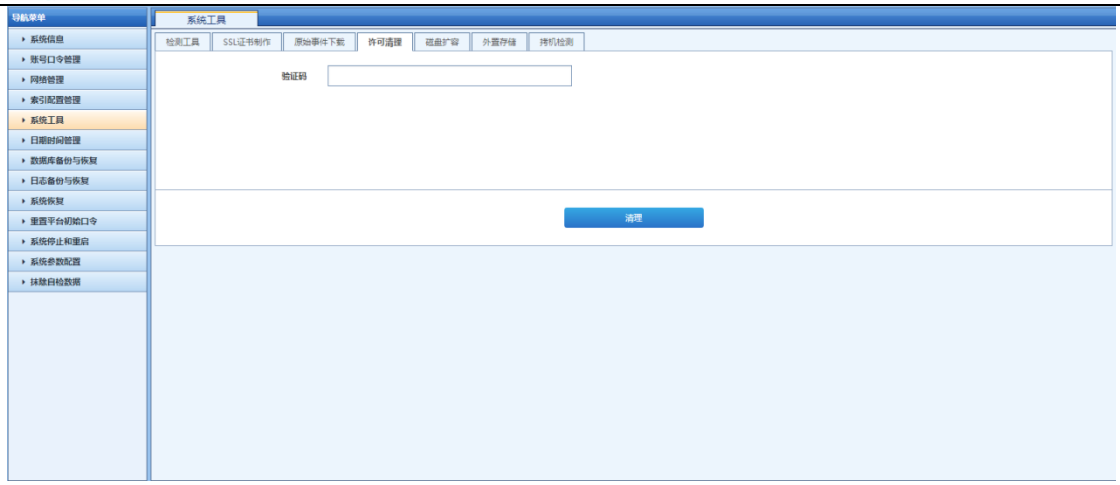
2.SSL 证书制作：由于浏览器对 HTTPS 服务的非授权机构授权证书不信任，浏览器会弹出信任警告并支持添加例外，用户也可以通过制作 SSL 证书并导入客

户端浏览器，使其信任该网站



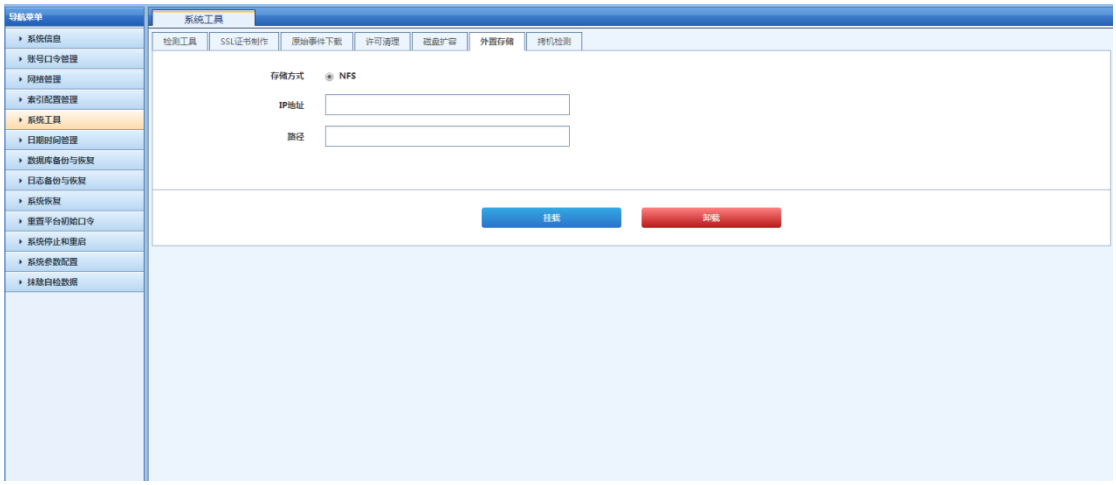
3. 原始日志下载：下载原始日志或者通用日志

4. 许可清理：清理产品当前许可信息已便重新授权

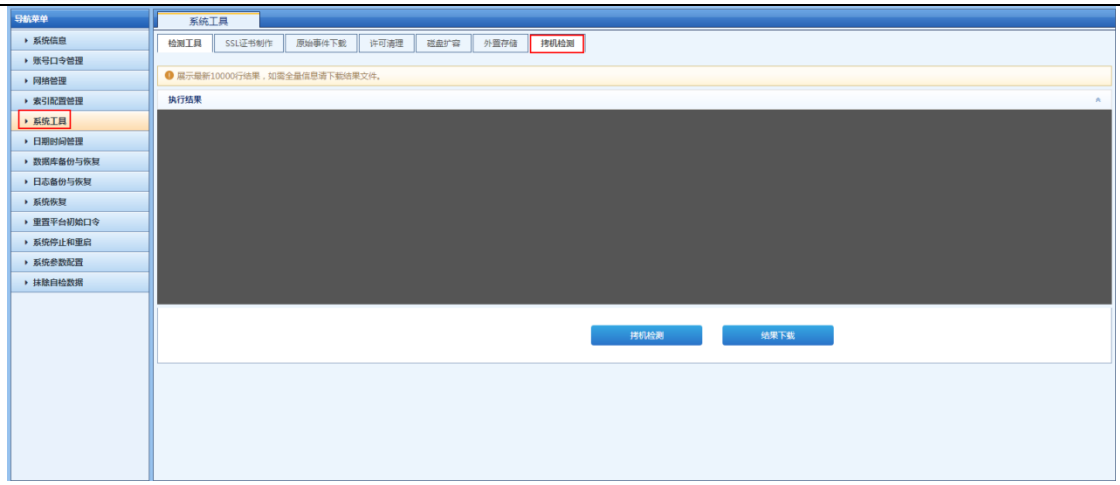


5. 磁盘扩容：当系统内置存储不足以支撑用户的存储需求时，可以通过该功能进行本地磁盘扩容

6. 外置存储：当系统内置存储不足以支撑用户的存储需求时，可以通过该功能进行外置存储扩容（IP 地址：172.16.0.171；路径：/opt/nfstest）

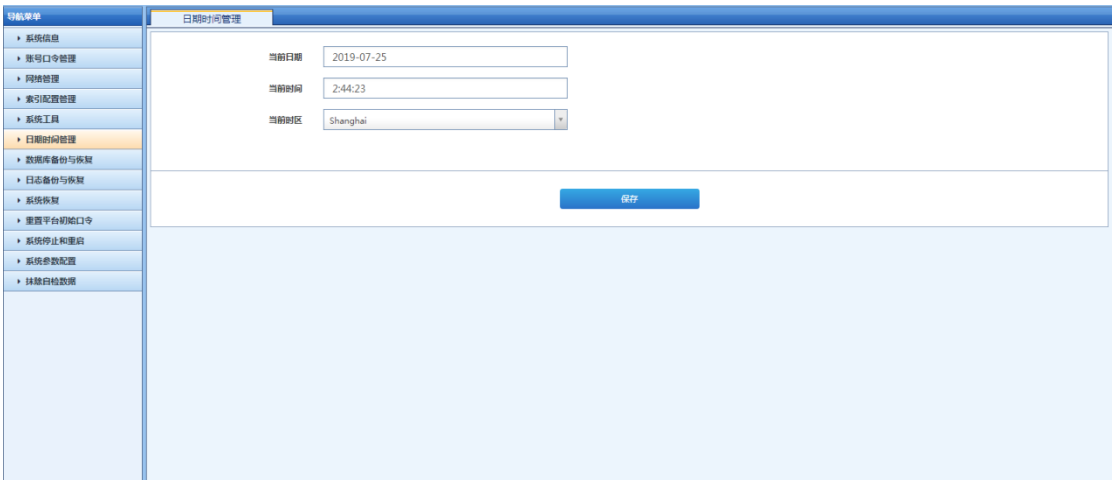


7. 拷机检测：硬件出厂前设备稳定性测试，一般不建议用户使用



1.1.6. 日期时间管理

用户可以修改时间、日期及时区信息（仅限平台服务器），如下：



1.1.7. 数据库备份与恢复

用户可以设置数据的备份方式（仅限平台服务器），如下：

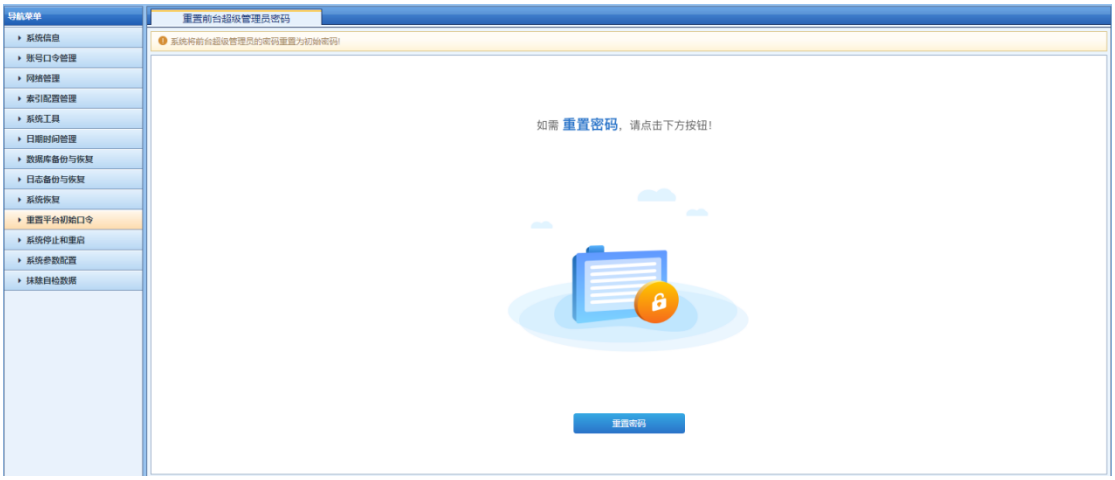
1.1.8. 日志备份与恢复

1.1.9. 系统恢复

用户可以将系统恢复至初始状态，即清除所有过往数据，故需慎用，如下：

1.1.10. 重置平台初始化口令

重置 8443 页面 admin 用户密码，如下：

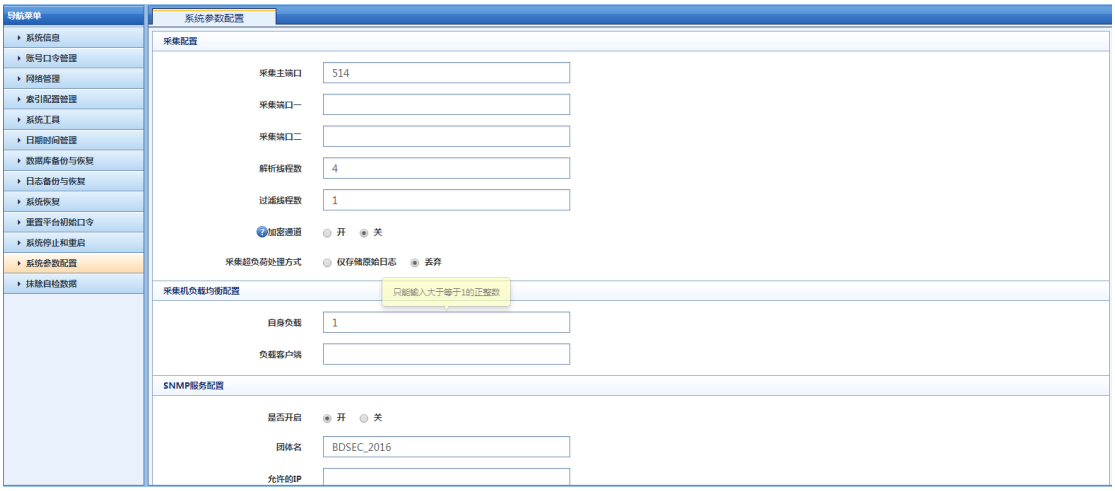


1.1.11. 系统停止和重启

重启或关闭机器，如下：

1.1.12. 系统参数配置

配置系统参数信息，如下：



采集配置：配置日志接受的端口；

采集机负载均衡配置：集群信息配置，（需要搭建集群环境）；

SNMP 服务配置：配置团体名信息（团体名：test；允许的 IP：172.16.0.171）；

SYSLOG 服务配置：配置转发第三方服务（服务 IP：172.16.0.171）；

SSH 服务配置：配置是否可以使用 ssh 直接连接；

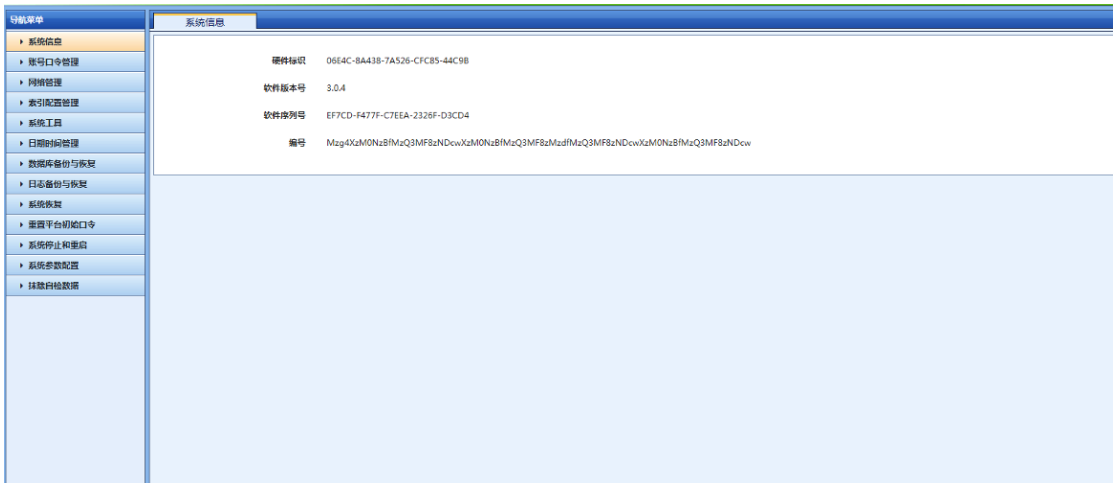
U-key 配置：指定 Ukey 服务器配置。

1.1.13. 配置管理

配置管理功能适用于新旧产品配置迁移场景，迁移的新旧产品必须为同一版本。

1.1.14. 下载运维日志

下载系统组件运行日志，下载文件为加密文件，一般用于提供给技术人员定位问题。



2 业务系统配置

业务系统配置步骤简介

1、日志标准化（必配）：

在 LAS 系统上首先设置需要接收、标准化具体设备/系统的安全事件/日志；它是安全事件管理的核心内容，也是系统安全事件/日志的唯一来源。LAS 上完成日志标转化后，能够识别各种设备日志，并进行标准化、模版化呈现、日志归并、日志过滤、关联告警等核心内容呈现，该项配置主要包含以下两项步骤：

（1）网络设备、服务器等日志指向 LAS 存储；

（2）LAS 系统采集器配置，将接收的日志执行标准化。

2、安全策略关联配置（必配）：

关联分析功能是系统中的重要功能之一，将标准化后的日志与系统内置安全策略相匹配比对，如果符合关联策略,将以告警的形式在实时监控模块呈现给用户，用户可以对告警进行相关的处理。该项配置主要包含以下内容:

（1）启用系统内置关联策略库;

（2）根据实际用户需求，手工增加策略（按需配置）；

（3）对安全策略产生的告警进行处理。

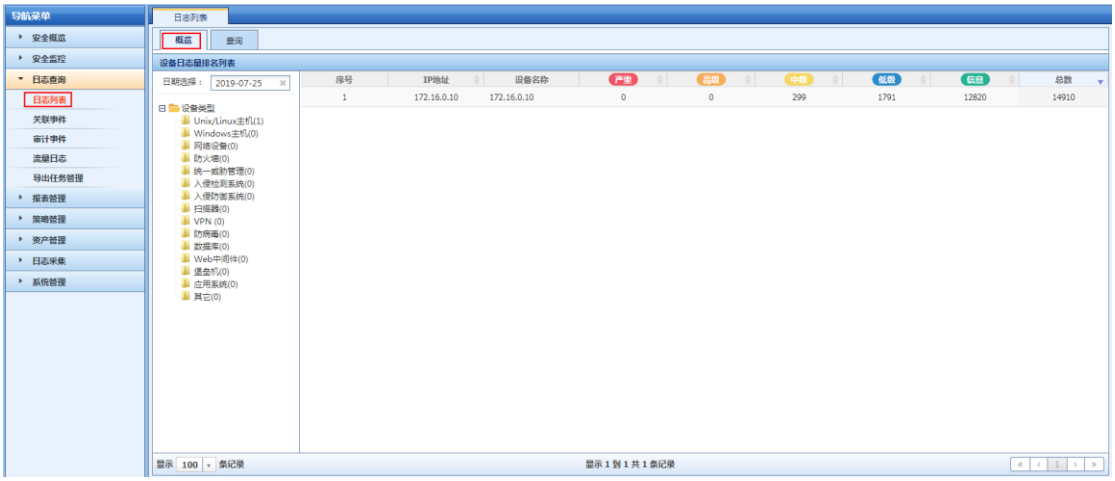
2.1. 资产管理配置

2.1.1. 简介

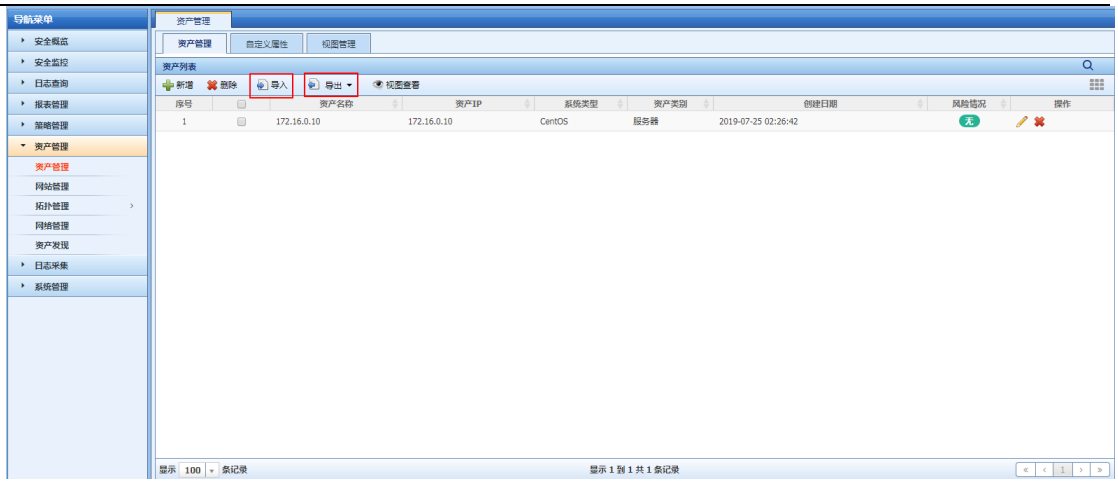
1、资产管理便于 LAS 设备对当前设备进行识别及管理:

（1）通过资产管理在 LAS 系统上登记了资产后，在 日志查询->日志列表中的相关日志信息，将显示登记 ip 的资产名称;

（2）如未进行登记，获取到的安全日志信息将只显示 ip 地址，不显示设备名称。



2、资产管理支持批量资产导入导出，同时支持按视图对资产进行分类（资产分组）：



2.1.2. 常规设置

一、单台资产添加

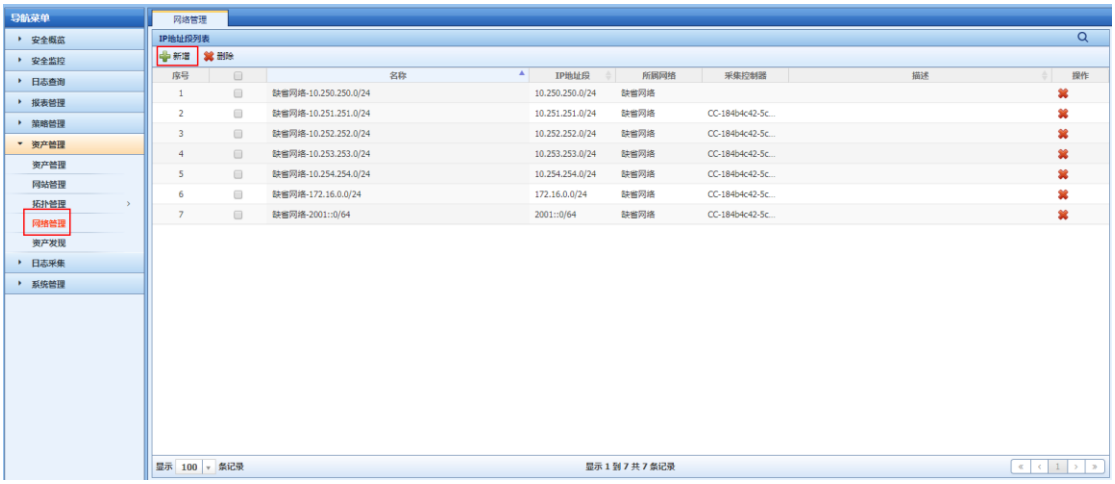
场景：添加 1 台 windows server2008 服务器，ip 地址为 5.5.5.5。

二、具体配置

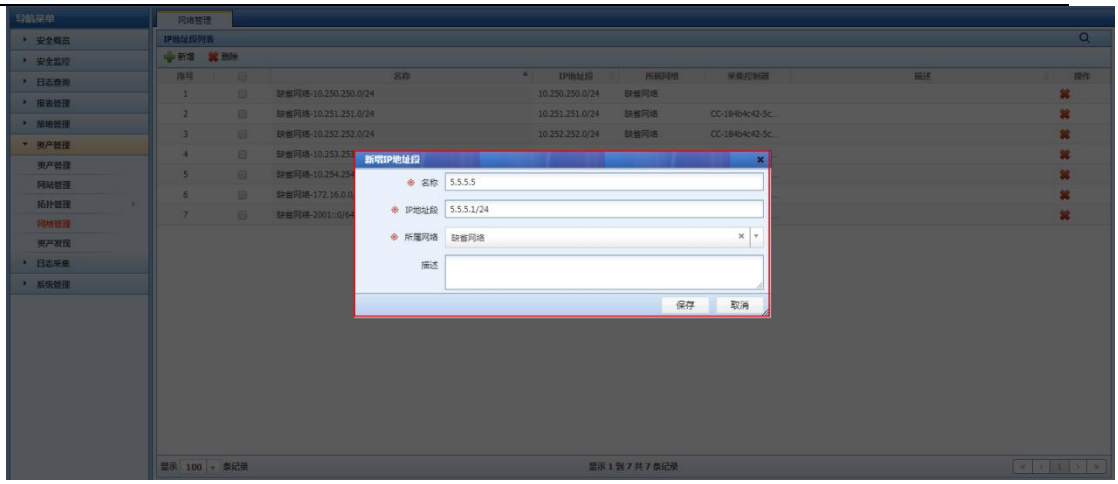
WEB 登录 LAS 业务控制台：https://10.250.250.128（软件版根据实际设定的 ip 地址进行登录）默认用户名：admin，密码 admin。

（1）增加 ip 地址段：

选择 资产管理->网络管理->IP 地址段列表，点击新增。



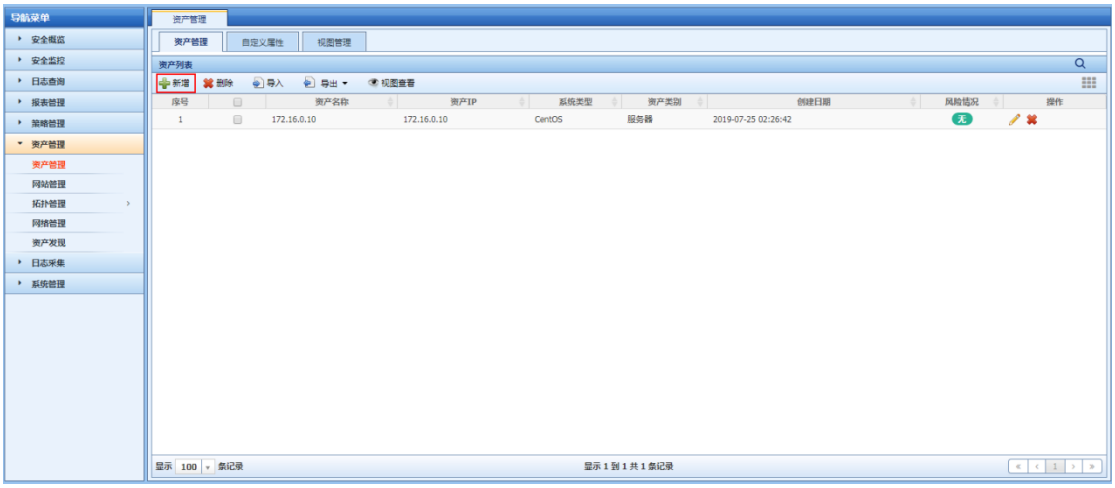
增加 5.5.5.0/24 网段，如下图配置。



注意：绝大多数情况下【所属网络】请务必选择缺省网络，否则将造成其他功能模块解析异常。

（2）增加具体资产：

点击资产管理->资产管理->新增



如下图进行配置：

注意：红*为必填项

资产名称：根据实际网络、设备自定义取名

系统类型：选择 windows 2008

ip 地址段：选择已有的 5.5.5.0;如果是新增的 ip 地址段，可以直接点击后面的+号

资产类别：此处选择服务器

资产 ip：此处填写需要增加资产的实际 ip

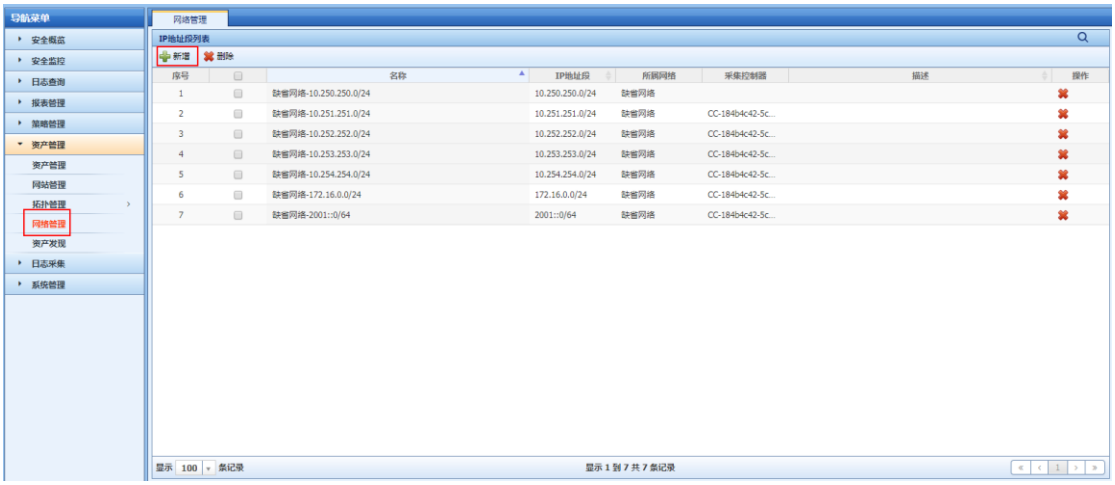
通过"查询"，按钮可以快速的查询当前已添加的资产

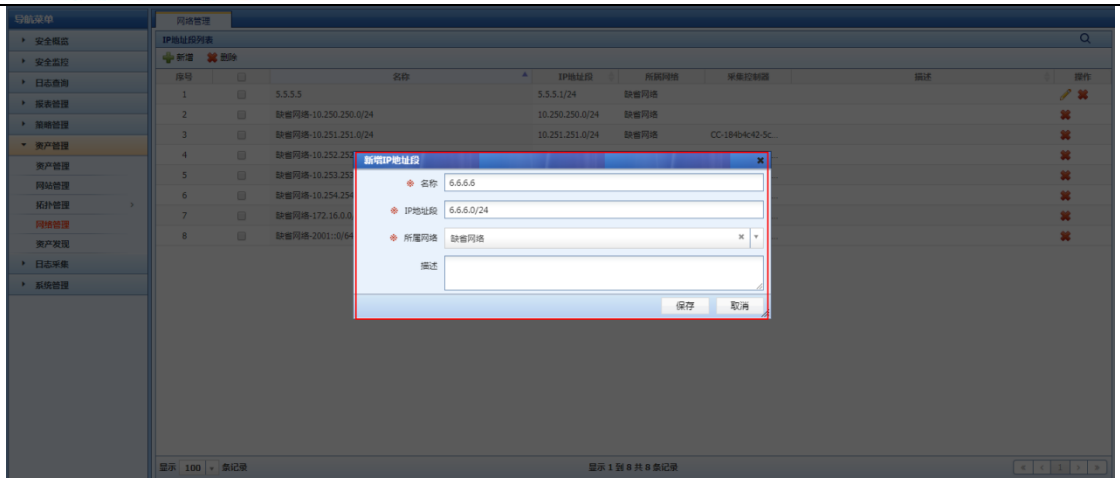
三、资产批量导入

场景：批量导入 6.6.6.1->6.6.6.10 这十台设备。

注意：LAS 系统仅支持 CSV 格式的文件导入，文件大小不能超过 5M。

（1）增加 6.6.6.0/24ip 地址段：

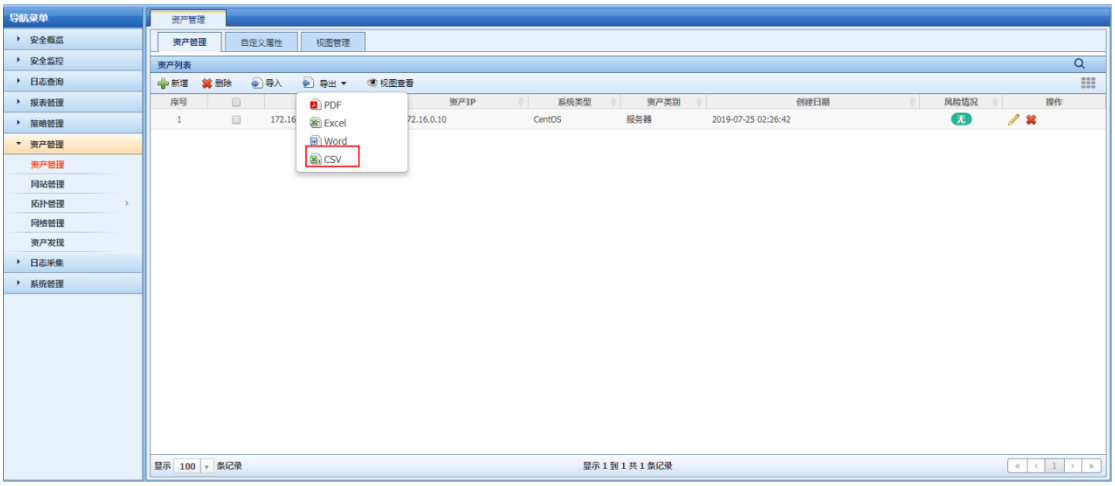




注意：通常情况下【所属网络】请务必选择缺省网络，否则将造成其他功能模块解析异常。

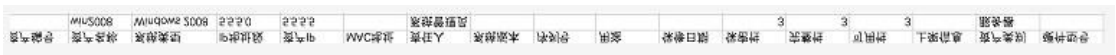
（2）建议操作：从 LAS 导出某一台设备的 csv 文件，作为模版；此处以设备 5.5.5.5 为例：

选中主机 5.5.5.5,并选择导出为 csv 文件。



（3）打开本地保存的 csv 文件（导出文件名为"资产列表.csv"），参照 5.5.5.5 资产格式，根据实际情况录入 6.6.6.1->6.6.6.10 这十台设备：

5.5.5.5 资产导出 csv 格式，如下图：



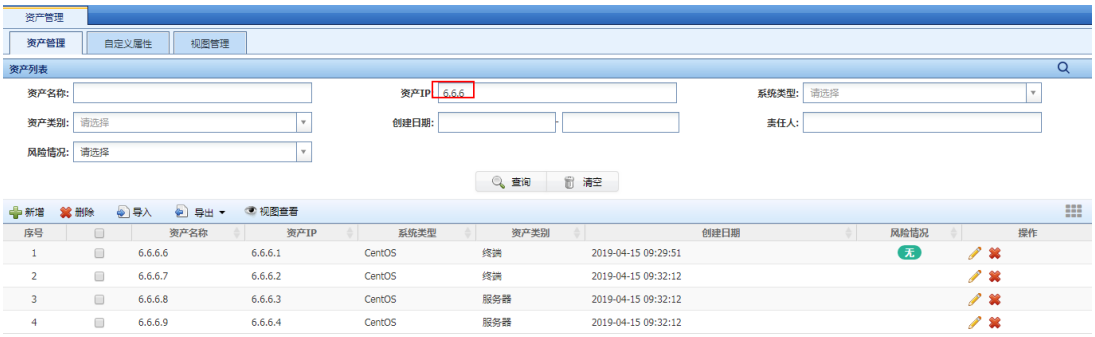
参照格式进行录入，如下图（登记完成后注意删除原有的 5.5.5.5 资产，否则 LAS 系统会因为资产重复报错，无法执行导入）。

资产编号	资产名称	系统类型	IP地址段	资产IP	MAC地址	责任人	系统版本	序列号	用途	保修日期	保密性	完整性	可用性	上架信息	资产类别	硬件型号
	6.6.6.1	Windows 2008	6.6.6.0	6.6.6.1		系统管理员					3	3	3		服务器	
	6.6.6.2	Windows 2008	6.6.6.0	6.6.6.2		系统管理员					3	3	3		服务器	
	6.6.6.3	Windows 2008	6.6.6.0	6.6.6.3		系统管理员					3	3	3		服务器	
	6.6.6.4	Windows 2008	6.6.6.0	6.6.6.4		系统管理员					3	3	3		服务器	
	6.6.6.5	Windows 2008	6.6.6.0	6.6.6.5		系统管理员					3	3	3		服务器	
	6.6.6.6	Windows 2008	6.6.6.0	6.6.6.6		系统管理员					3	3	3		服务器	
	6.6.6.7	Windows 2008	6.6.6.0	6.6.6.7		系统管理员					3	3	3		服务器	
	6.6.6.8	Windows 2008	6.6.6.0	6.6.6.8		系统管理员					3	3	3		服务器	
	6.6.6.9	Windows 2008	6.6.6.0	6.6.6.9		系统管理员					3	3	3		服务器	
	6.6.6.10	Windows 2008	6.6.6.0	6.6.6.10		系统管理员					3	3	3		服务器	

（4）查看导入后的资产：

导入成功，将会在页面右下角提示导入成功

查看新导入的 10 台资产



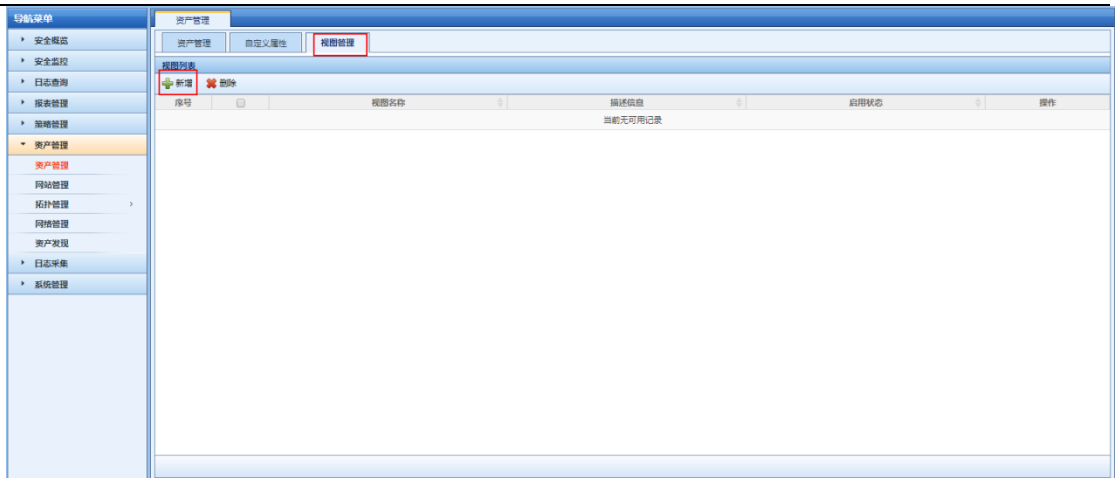
四、视图（分组）配置

场景：将增加的 10 台 6.6.6.1->6.6.6.10，以及 5.5.5.5 增加组别信息。

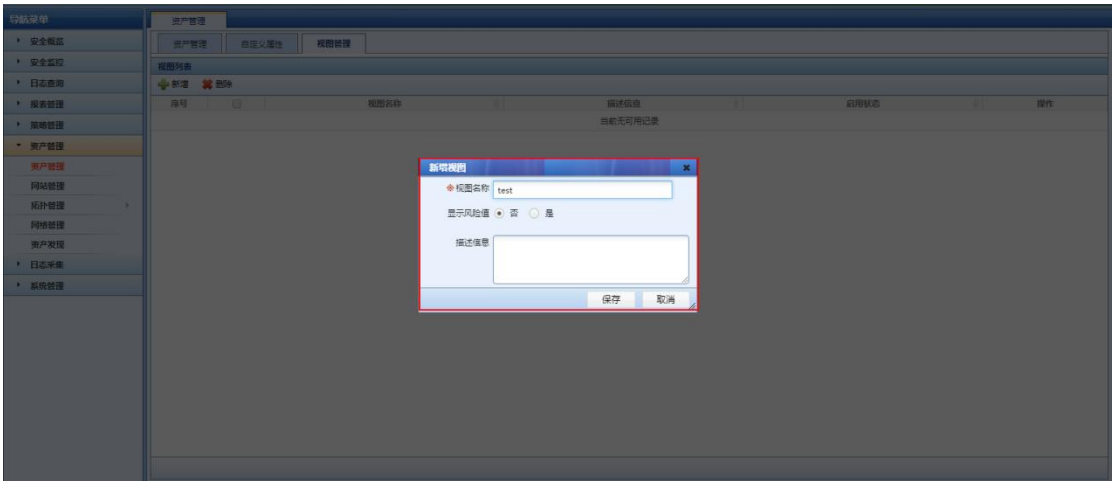
- 6.6.6.1->6.6.6.10：父组【test】、子组【6 网段】；
- 5.5.5.5：父组【test】、子组【5 网段】。

（1）添加父组：test：

选择资产管理->资产管理->视图管理,点击 新增，如下图：



新增 test 父组，如下图

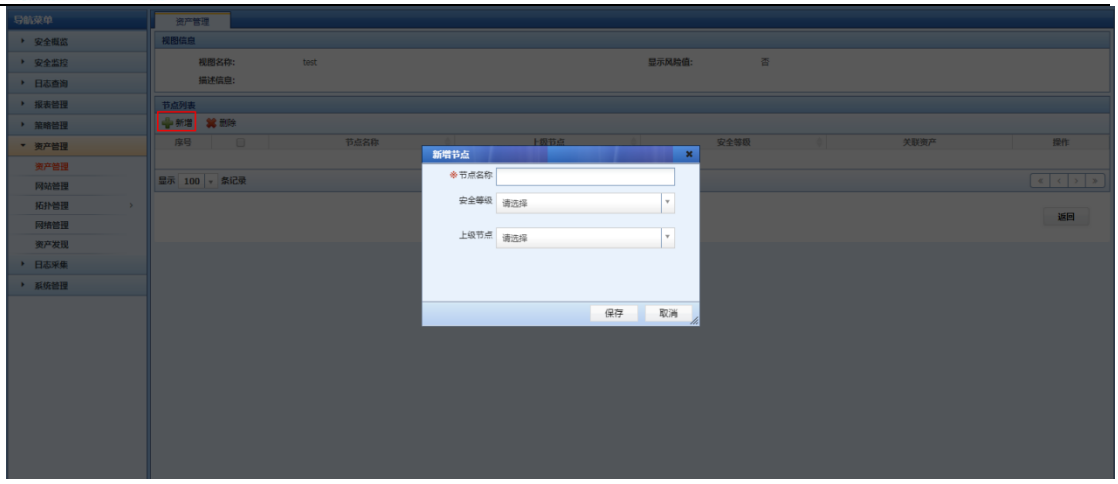


（2）添加子组 6 网段和 5 网段：

点击 节点管理

点击 新增

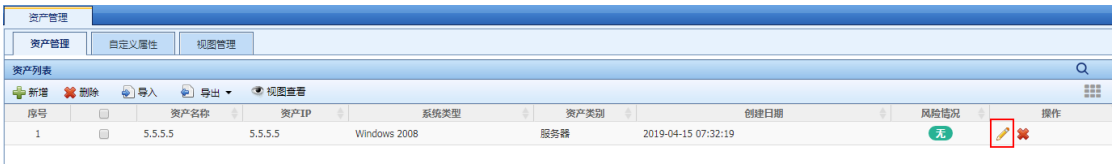
增加 6 网段和 5 网段



（3）将资产划入相应分组：

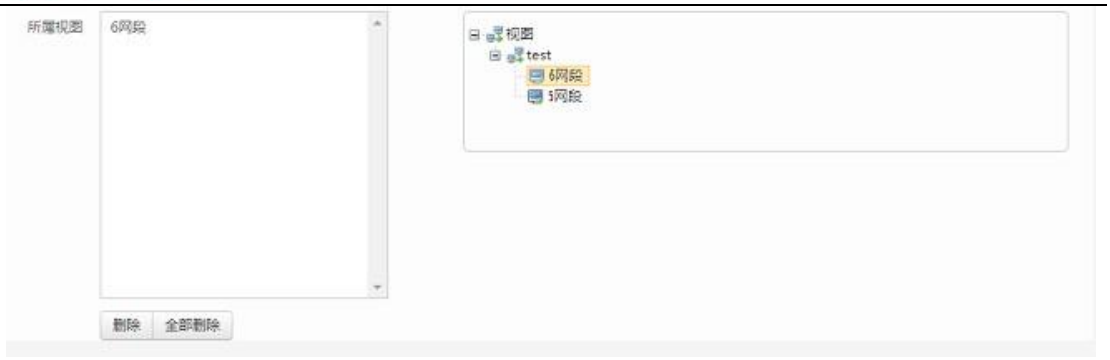
将 5.5.5.5 划入 5 网段；

在 资产管理-> 资产管理-> 资产管理,选中 5.5.5.5 资产，进行修改，如下：

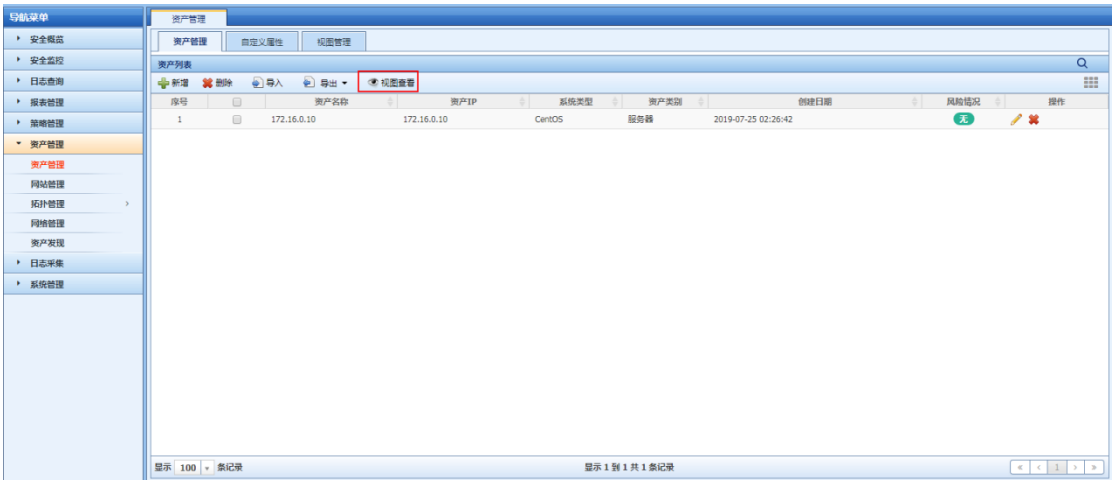


在所属视图中选中 5 网段，并保存

同理将 10 台 6 网络设备加入【6 网段】；



（4）点击 资产管理->资产管理->视图查看，可以查看当前已经建立的分组：



按分组查看

2.1.3. 自定义资产添加

一、自定义厂商、产品、系统类型（非 LAS 默认自带）资产添加

场景：

添加一台防火墙：

ip 地址：10.250.250.12

厂商：A 厂商

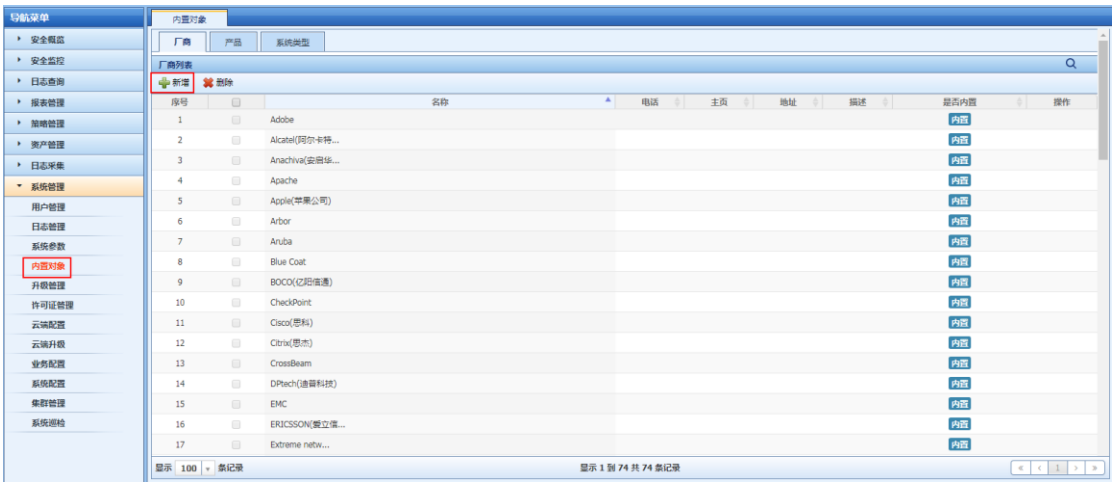
产品：A 产品

系统型号：A 系统

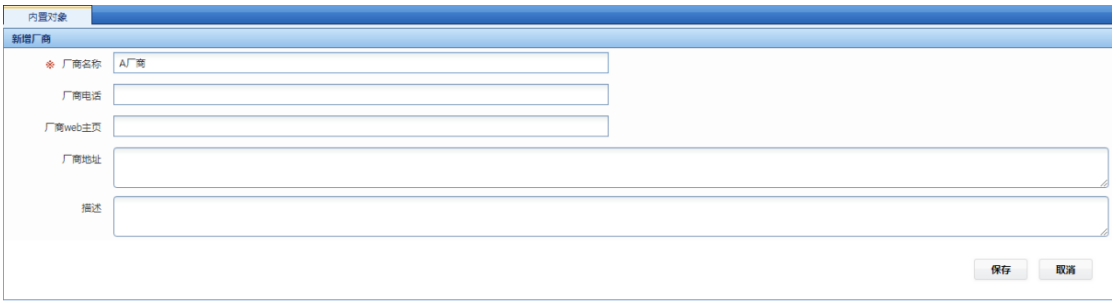
二、具体配置

（1）添加厂商：

点击系统管理->内置对象->厂商->新增

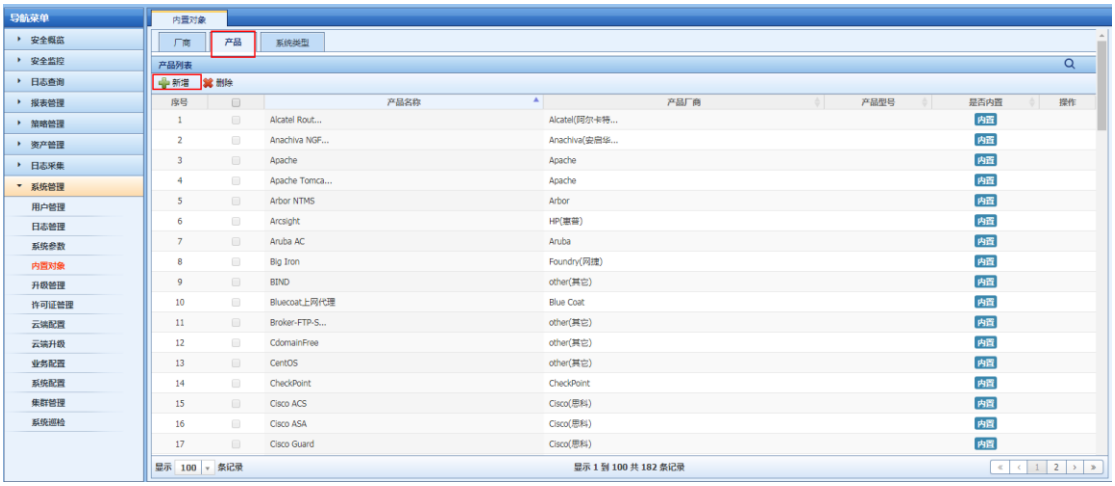


如下图进行配置：



（2）增加产品：

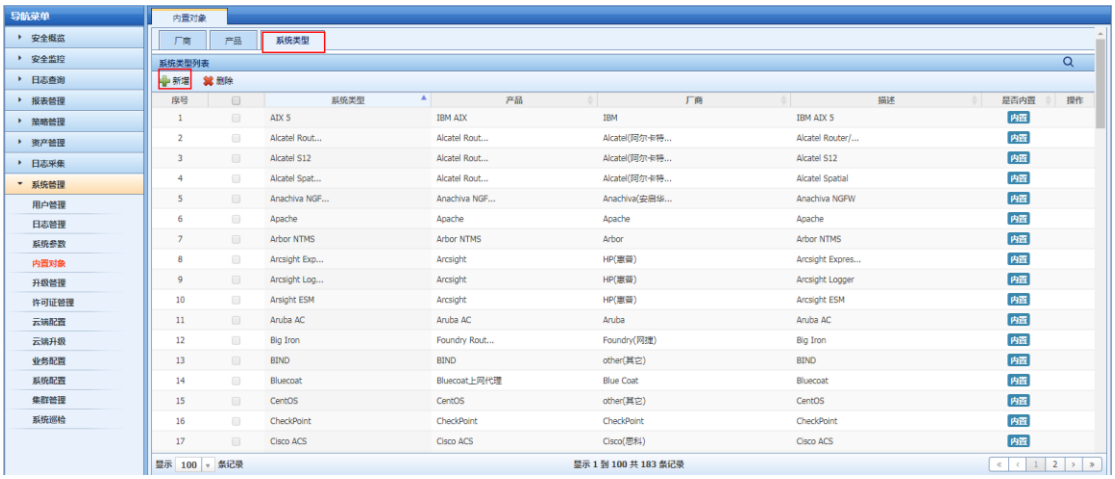
点击系统管理->内置对象->产品->新增



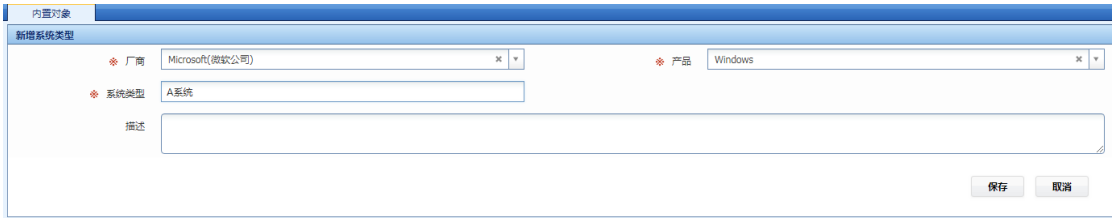
如下图进行配置，产品厂商选择刚建立的【A 厂商】：

（3）增加系统类型:

点击 系统管理->内置对象->系统类型->新增

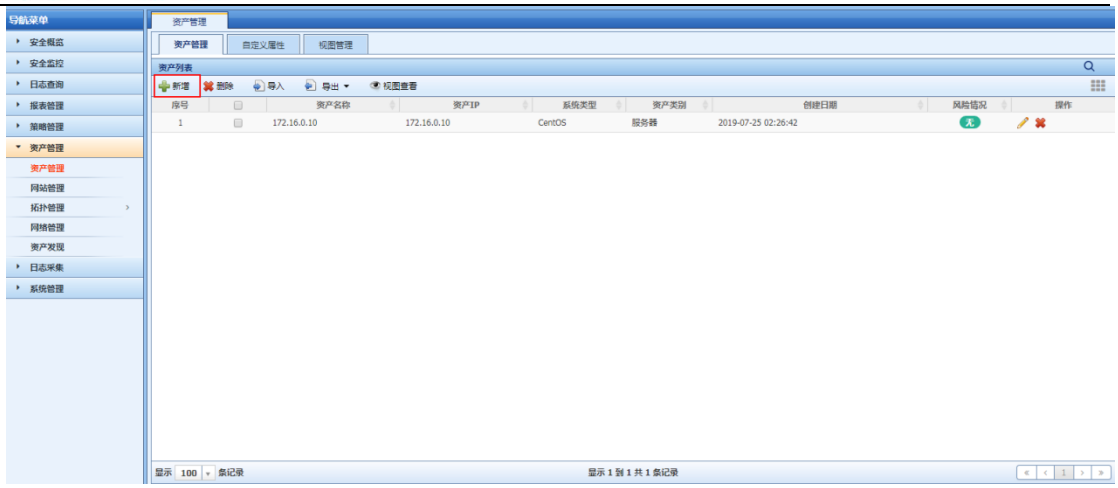


如下图 进行配置，产品厂商选择刚建立的【A 厂商】，产品选择刚建立的【A 产品】：



（4）添加资产，调用新建的【A 系统】：

点击资产管理->资产管理->资产管理->新增



参照下图配置，系统类型选择刚建立的【A 系统】，即可完成自定义资产的调用：

2.2. 日志标准化配置（必配）

2.2.1. 日志接入说明

1、日志标准化

在 LAS 系统上首先设置需要接收、标准化具体设备/系统的安全事件/日志；它是安全事件管理的核心内容，也是系统安全事件/日志的唯一来源。LAS 上完成日志标准化后，能够识别各种设备日志，并进行标准化、模版化呈现、日志归并、日志过滤、关联告警等核心内容呈现；该项配置主要包含以下两项步骤：

（1）网络设备、服务器等日志指向 LAS 存储；

（2）LAS 系统采集器配置，将接收的日志执行标准化。

2、各种采集方式适用的场景不尽相同，在实际设置时应根据具体的被接入设备进行设置：

（1）Syslog 方式：适用于大多数 Linux/Unix 类系统及多数网络和防火墙类设备；

（2）SNMP Trap 方式：适用于一般的网络设备；

（3）WMI 方式：适用于 Windows 系统的事件接入；

（4）数据库方式：适用于部分数据库自身的审计日志接入以及一些仅能将日志保存在数据库中的软件系统，如 Symantec 网络防毒系统、趋势网络防毒系统等；

（5）文件方式：适用于无法通过上述方式实时接入系统的或需集中审计（特别是事后审计）的软件或应用系统所留存的日志信息；

（6）Socket 方式：适用于对日志信息丢失零容忍的场景，但相关被采系统需进行一定程度的改造以发出符合 LAS 要求的日志格式；（由于实施难度大，需要定制开发，不建议使用）；

(7)SMB 方式：用于 web 连接和客户端与服务器之间的信息沟通；

(8)CONSOLE 方式：**主动采集目标设备的原始日志具体采集方式由插件类型决定对应参数请根据系统要求填写；**

(9) **日志导入：适用于对日志进行手动导入；**

(10)流量镜像接入方式：采用旁路模式接受镜像流量，只需将网线插入对应的网卡接口，通过网线接受镜像流量。

2.2.2. syslog 方式（常见）：linux 系统及网络设备接入

一、 场景：

LAS 系统上需要识别 2 台负载均衡、1 台防火墙、1 台天泰防火墙以及若干 linux 主机日志，进行标准化呈现：

2 台负载均衡地址： 172.16.32.11、 172.16.32.12；

防火墙地址：210.x.x.x；

1 台天泰 waf 防火墙： 210.x.x.x；

若干台 linux 主机：主机数量较多，具体 ip 未统计，需要一段周期的添加时间。

二、注意事项

网络通信正常：被采集设备与日志服务器之间网络可达，与日志采集器的 UDP：514 端口畅通。

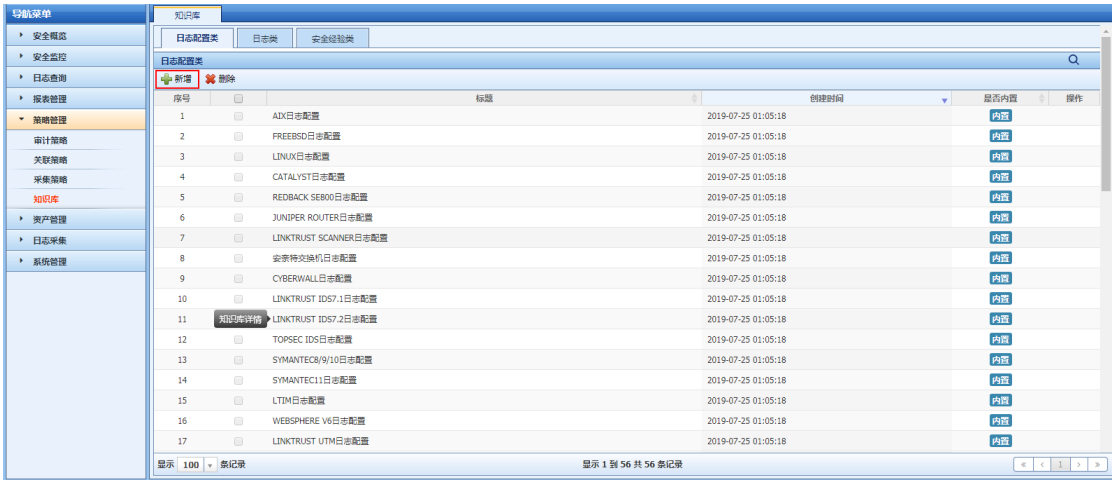
日志编码格式正确：Syslog 编码需要文本格式，UTF->8 或者 GBK。

三、各类设备配置：将 syslog 日志指向 LAS 系统。

1、常规网络、安全设备

在 web 界面或者命令行，将 syslog 服务器设置为 LAS 系统（采集器）ip 地址。

各类设备的 Syslog 或者 SNMP Trap 日志外发的配置方式，可以参见 LAS 系统里的" 策略管理->知识库->日志配置类"，针对不同设备有不同的配置方法，如下图:



注意：被采集设备的日志配置需要这些设备的系统管理员协助

2、Redhat Linux 系统

(1)登录到 Redhat 系统中，执行命令："vi /etc/syslog.conf"（或者为 rsyslog.conf）；

(2)在文件末添加如下内容：*.debug　@SyslogserverIP 其中 debug 和@符号之间是一个 Tab 键而不是空格，IP 地址填写收集 Syslog 接收服务器的地址（LAS 地址）；

(3)保存配置文件：执行命令":wq" ；

(4)重新启动 syslog 服务：执行命令“service rsyslog restart”。

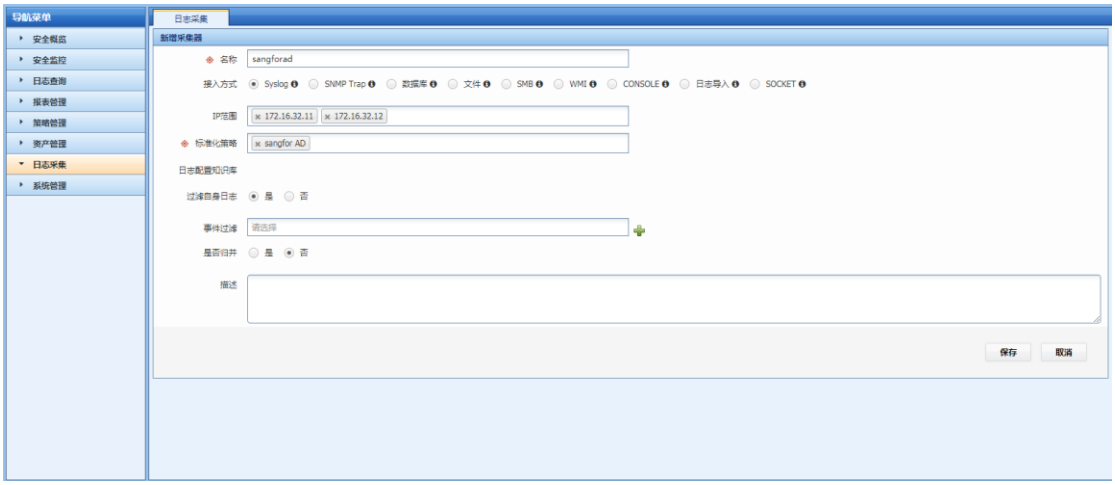
四、LAS 系统配置：日志标准化配置

2 台负载均衡、1 台防火墙、1 台天泰 waf、若干台 linux 主机已经将日志指向 LAS 系统，需要在 LAS 系统上配置相应的标准化策略。

1、登录系统进入日志采集页面，点击"新增"按钮

2、配置相关参数

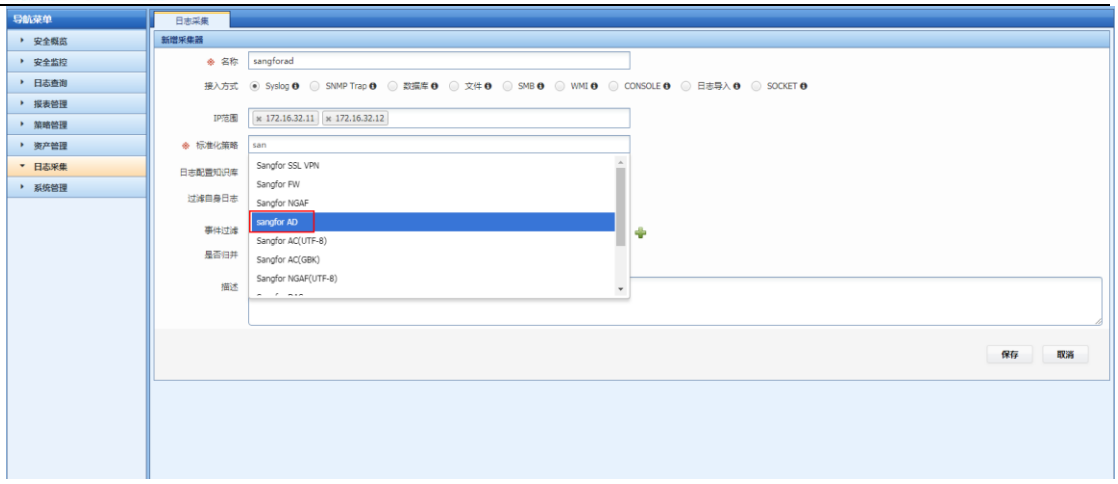
（1）增加 2 台负载均衡：172.16.32.11、172.16.32.12：



名称：自定义；例如本例自定义取名为 Test_AD；

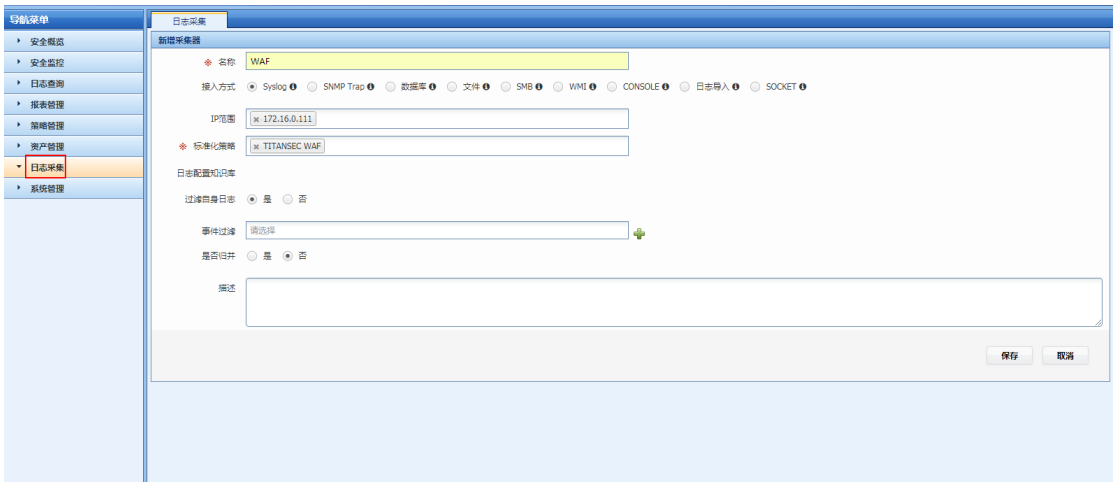
类型：选择"事件采集器"；

标准化策略：选择系统内置对应的模版，在对话框中输入厂商名称首几位，系统将自动关联。

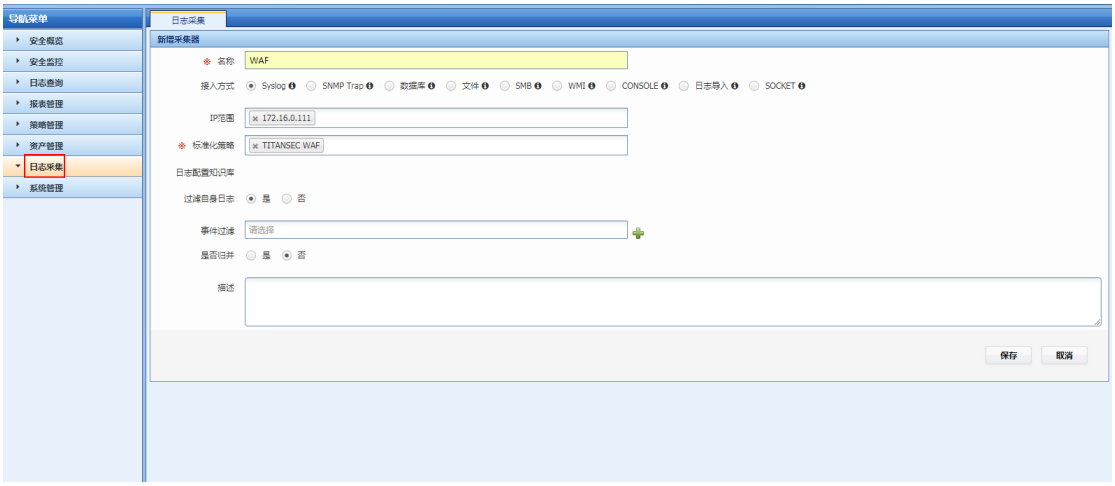


ip 范围：输入两台负载均衡的具体地址；此项可以为空系统将自动识别；建议填写准确 ip 以便系统能够识别。

（2）添加防火墙标准化策略（参考负载均衡）210.x.x.x:

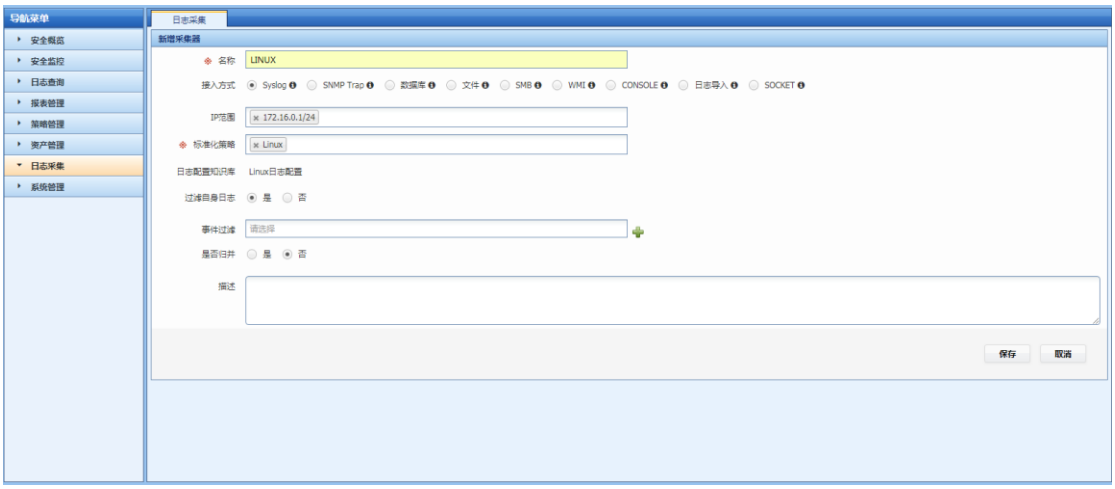


（3）添加天泰 WAF 防火墙:

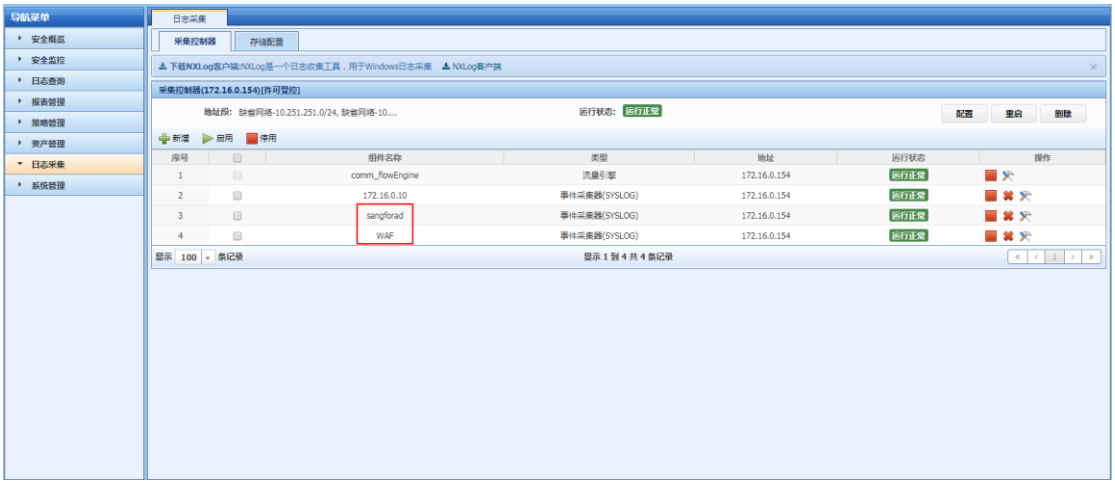


（4）添加若干台 linux 主机:

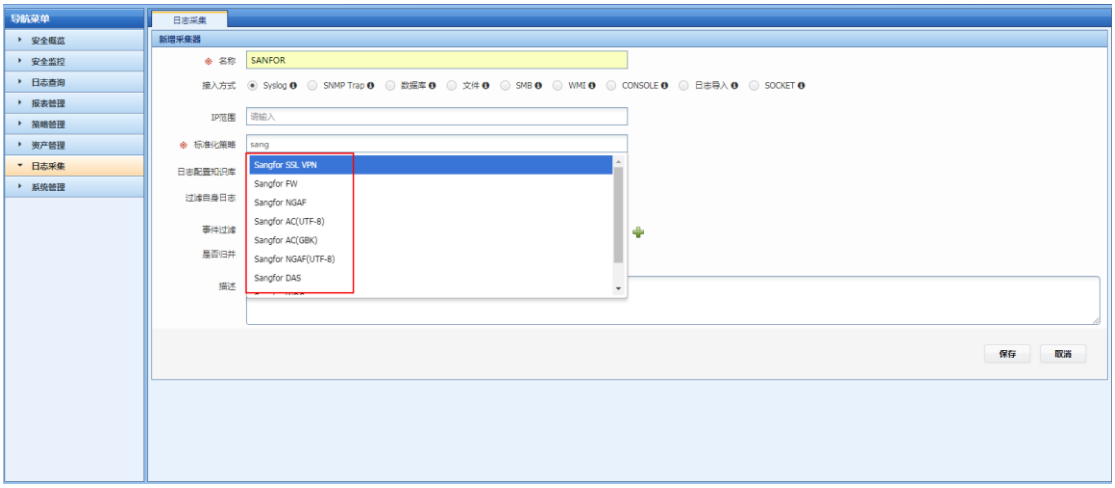
注意点：由于主机数量较多，需要一段的添加周期，故此处可以将 ip 范围留空（或者添加地址段），系统支持智能识别；其他配置与上述步骤相同。



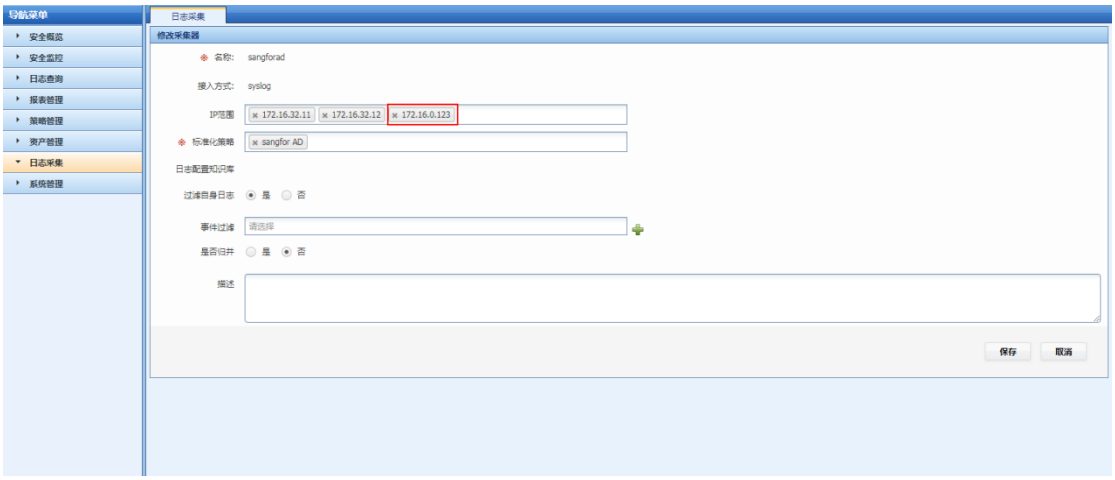
（5）查看已配置标准化策略：



注意：每种标准化策略只能添加一次，例如上例添加了 Test_AD 后，再新增事件采集器时，就无法继续选择 Test_AD,如下图显示。



如果有新的负载均衡加入，例如 172.16.32.13 加入，需要编辑原有的 sanfor->ad 标准化策略，在 ip 地址范围添加上，如下图：



五、标准化日志查看

点击"日志查询"->"日志列表"界面，可以显示已添加设备的日志收集情况（按严重、高级、中级、低级、信息）显示：

注意：

日志按照原始设备日志等级，以严重、高级、中级、低级、信息级别显示；如果原始设备部携带日志等级信息，系统将按照默认的显示等级显示；

设备名称：设备在"资产管理"->"资产管理"中完成相应资产设置的，在此处将显示具体信息，如上图中的 172.16.0.10；如果没有则留白不显示；

左键点击具体设备，可以显示设备当日具体日志信息，点击某一条日志，将显示具体的日志信息。

2.2.3. WMI 方式（常见）：windows 系统接入

一、场景：

LAS 系统上需要识别 1 台 windows 10 主机的日志，进行标准化呈现：

- win10 主机的 ip 地址：192.168.1.174

二、注意事项

- 网络通信正常：被采集设备与日志服务器之间网络可达，用于 WMI 访问的 135 端口畅通（例如没有被硬件防火墙阻断 135 端口）；
- 被采集服务器自带防火墙允许 WMI 应用通过 windows 防火墙进行通信,如下图。

使用 WMI 方式进行日志收集。WMI 为针对 Windows 系列设备的专用接入方式，适用于 Windows2003、2008、2012 系统。注意事项如下:

1、确认设备的 WMI 服务处于运行状态;

2、LAS 上需要录入具有 WMI 权限的账号进行日志采集:

（1）可以使用 administrator 账号进行采集,administrator 带有 WMI 权限，仅需要开启 WMI 服务即可（参考下文【 三、windows 配置 WMI，允许 LAS 采集日志】第 1 步）；

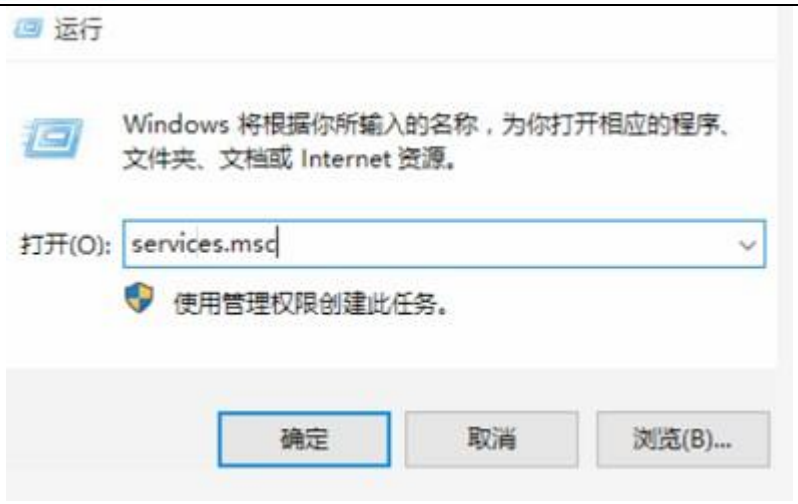
（2）如果用户由于涉密无法提供 administrator 账号，可以通过创建具有 WMI 权限的账号进行日志采集。

3、本文以创建具有 WMI 权限的 wmitest 账号为例，采集 windows 主机审核日志。

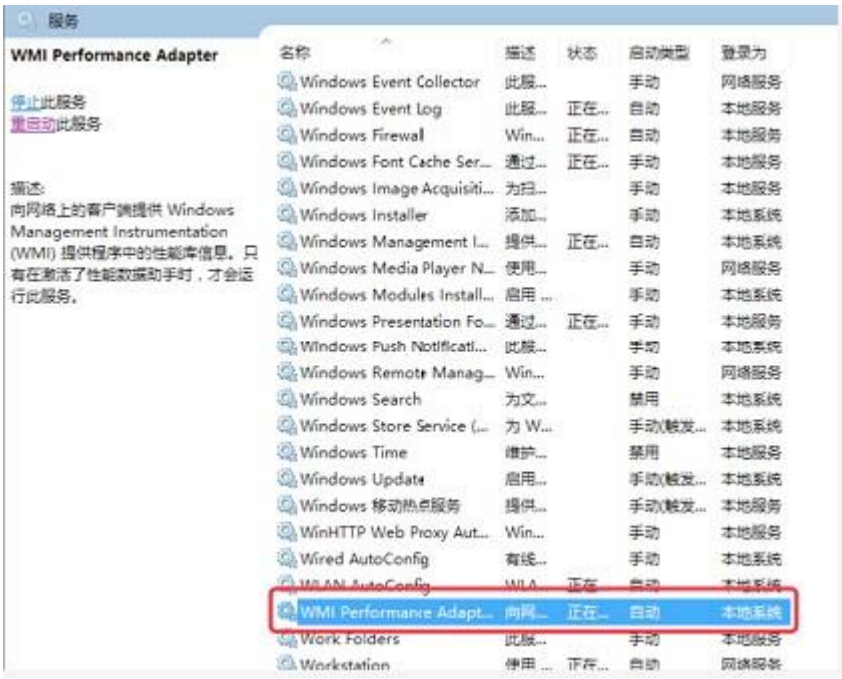
三、windows 配置 WMI，允许 LAS 采集日志

1、确保设备的 WMI 服务处于运行状态

(1)在运行对话框输入 services.msc:



(2).确保 WMI 服务处于"正在运行"的状态，如未处于"正常运行"，右键点击该服务，选择"启动":

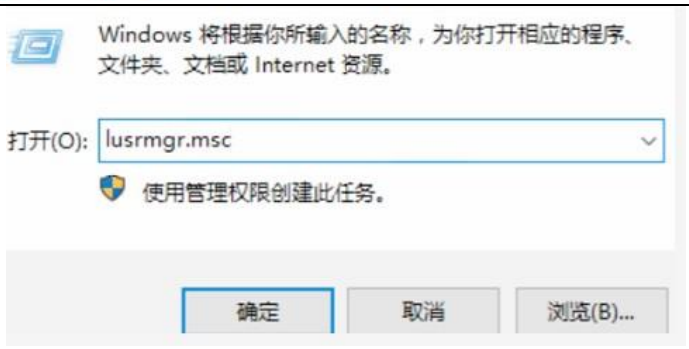


(3).如果用户可以提供 adminstrator 账号，则直接就可以在 LAS 系统上进行日志标准化配置操作;

(4).如果用户由于涉密无法提供 administrator 账号，下文以创建具有 WMI 权限的 wmitest 账号为例。

2、创建账号 wmitest 账号，并赋予 wmi 权限

（1）在运行对话框中输入 lusrmgr.msc,创建账号 wmitest;

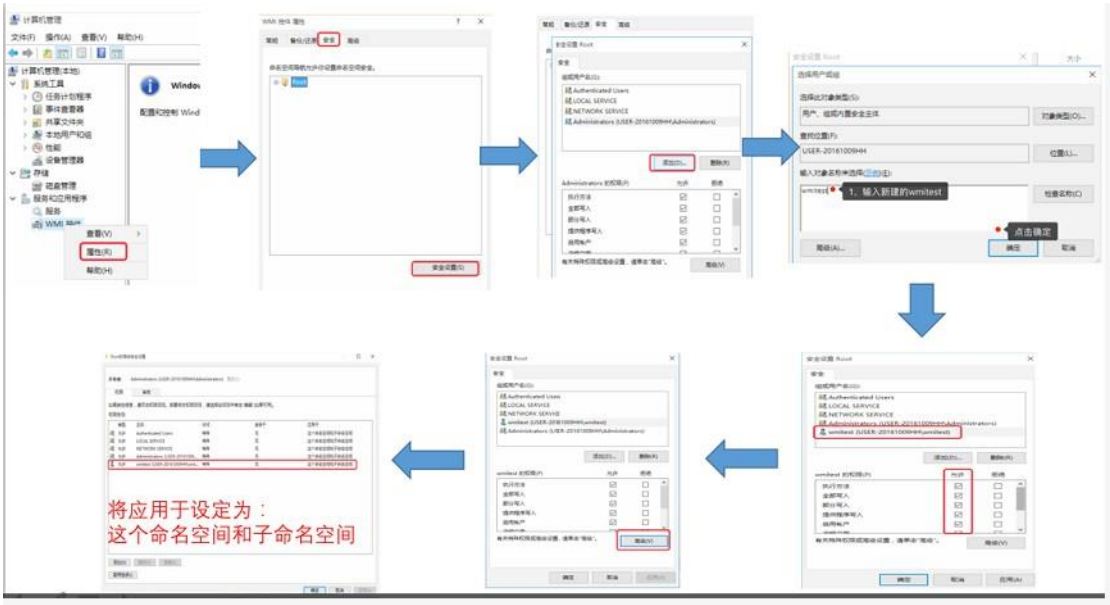


(2).在弹出的窗口中，右键点击"用户"，选择新用户；

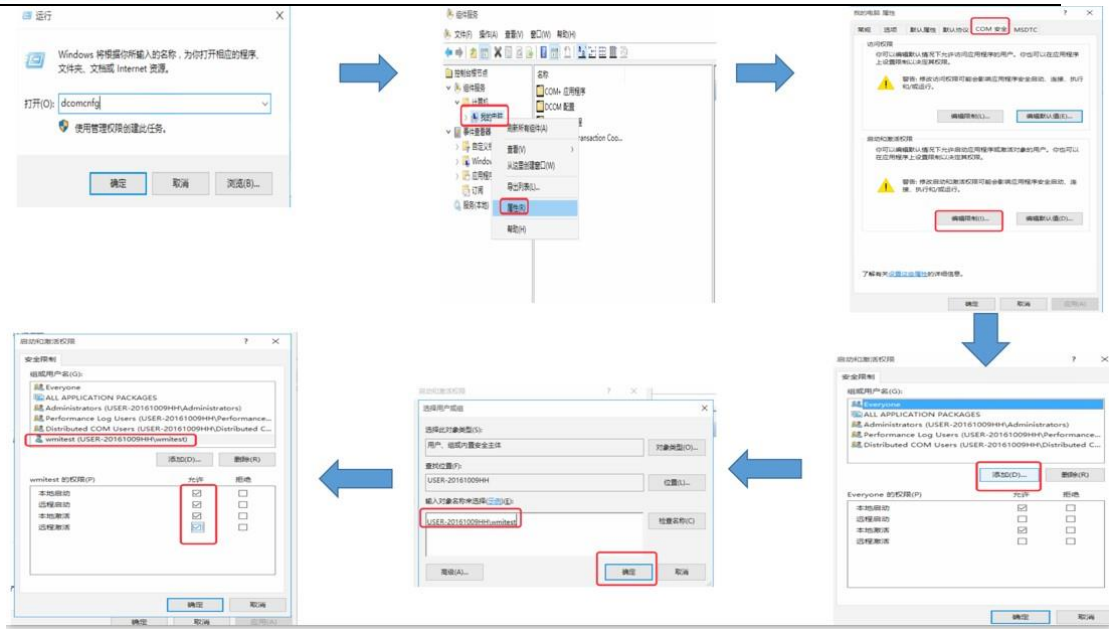
(3).设置账号 wmitest，设定密码，同时勾选用户不能修改密码、密码永不过期两个选项；

(4).给 wmitest 用户 WMI 授权；

(5).控制面板->管理工具->计算机管理->服务和应用:右键 WMI 控件属性->安全标签安全设置->为用户添加所有权限;

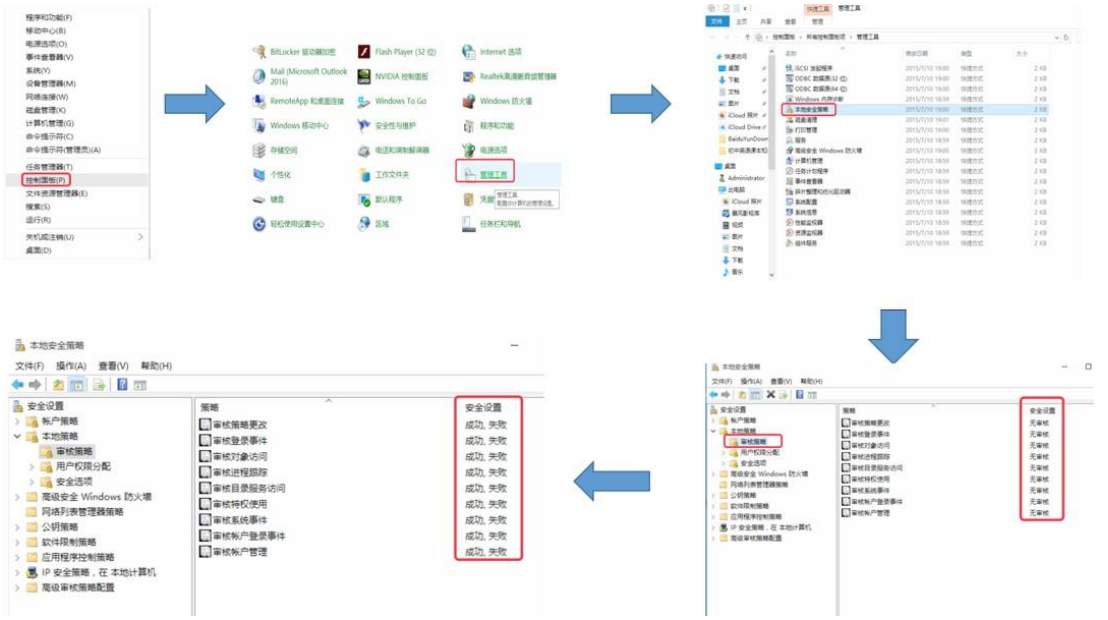


(6).组件服务->计算机属性->com 安全->启动激活权限;



(7).打开本地安全策略；

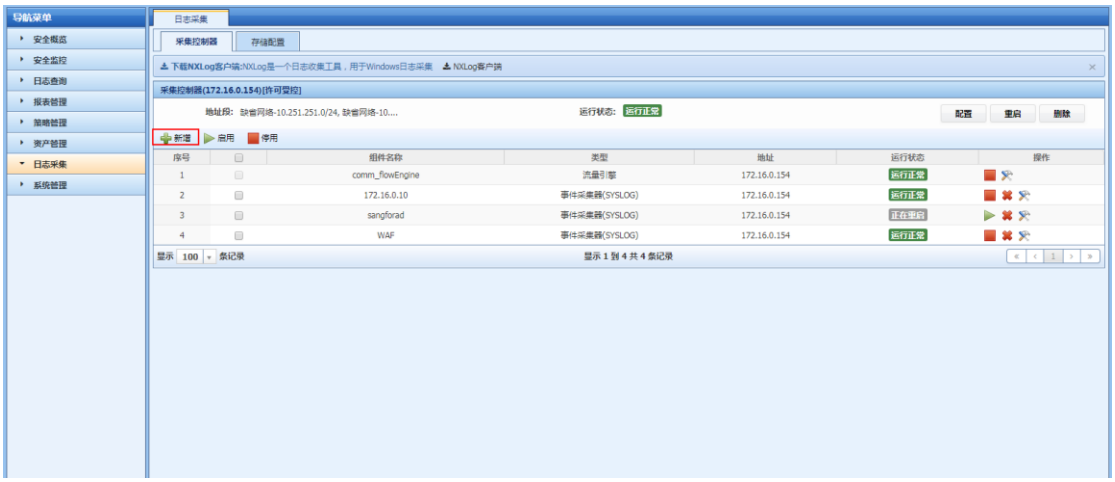
控制面板->管理工具->本地安全策略->本地策略->审核策略，根据实际需要开启相关策略。



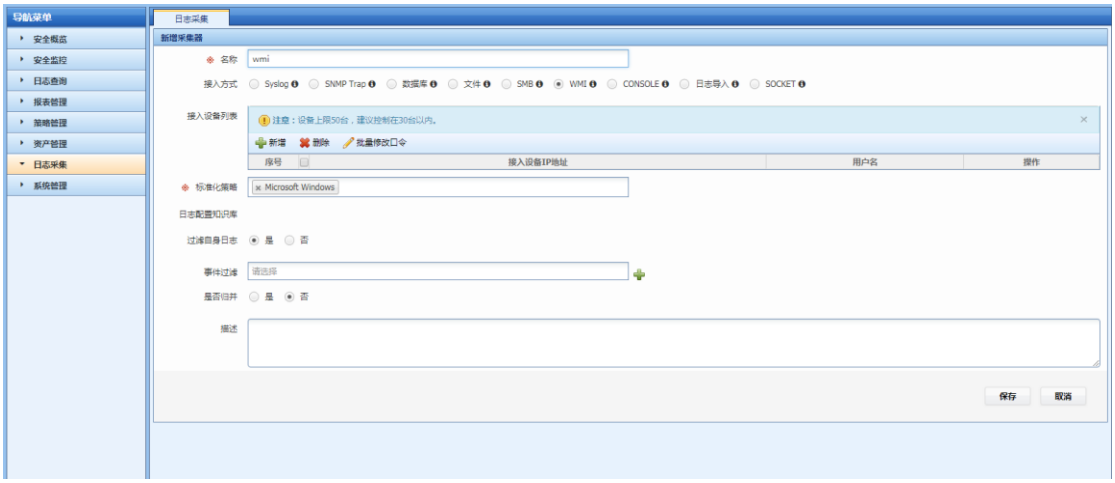
(8).最后赋予 wmi 账号"管理审核和安全日志"权限；

四、LAS 系统配置：日志标准化配置

1. 点击日志采集->新增，新增采集器，如下图所示:



2. 按照下图进行设置，设置完毕后点击接入设备列表处的"新增"按钮:



名称：自定义

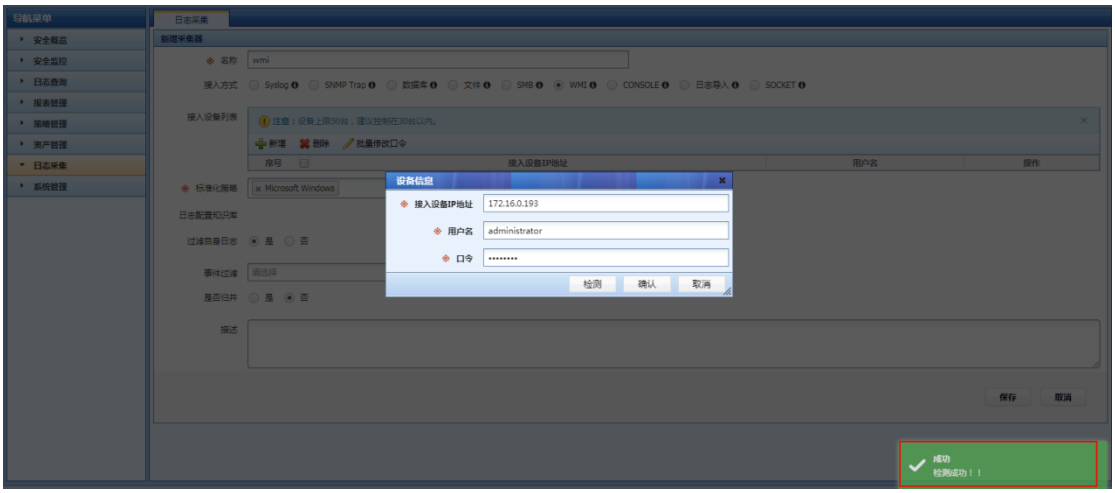
类型：选择事件采集器

接入方式：WMI

标准化策略：选择 Microsoft Windows(输入首几位字母，系统将自动检索);

输入目标主机的信息，包括 ip 地址、账号（具有 wmi 权限）、密码等，点击"检测";

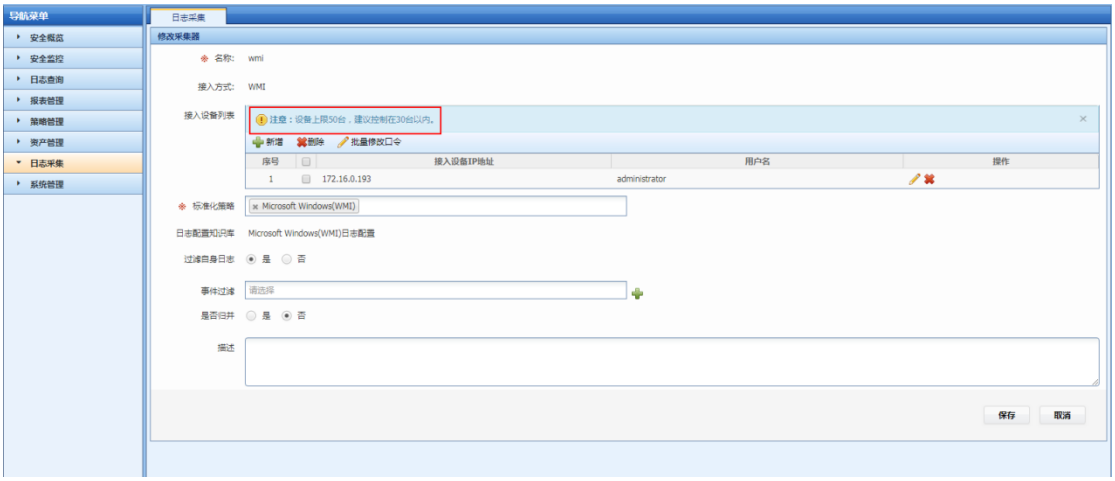
如通信正常，主机将提示检测成功，如下图:



检测通过后点击确认，完成 windows 主机添加:

注意：添加多台 windows 有两种方式

方式 1：编辑原有的采集器策略进行添加



方式 2：新增采集器进行添加

两种方式的区别在于：方式 1 添加较为便利，方式 2 多采集器处理性能更高；建议使用方式 2 进行添加；当每台 windows 主机日志量较小时可以使用方式 1。

五、标准化日志查看

点击"日志查询"->"日志列表"界面，可以显示已添加设备的日志收集情况（按严重、高级、中级、低级、信息）显示：

注意：

日志按照原始设备日志等级，以严重、高级、中级、低级、信息级别显示；如果原始设备部携带日志等级信息，系统将按照默认的显示等级显示。

设备名称：设备在"资产管理"->"资产管理"中完成相应资产设置的，在此处将显示具体信息。如果没有则留白不显示；

点击具体设备，可以显示设备当日具体日志信息，点击某一条日志，将显示具体的日志信息：

2.2.4. 文件方式

一、场景说明

适用于无法通过 Syslog 等方式实时接入系统的或需集中审计（特别是事后审计）的软件或应用系统所留存的日志信息。

二、注意事项

LAS 提供目标主机使用 sftp 登录的方式，实现文件传输。

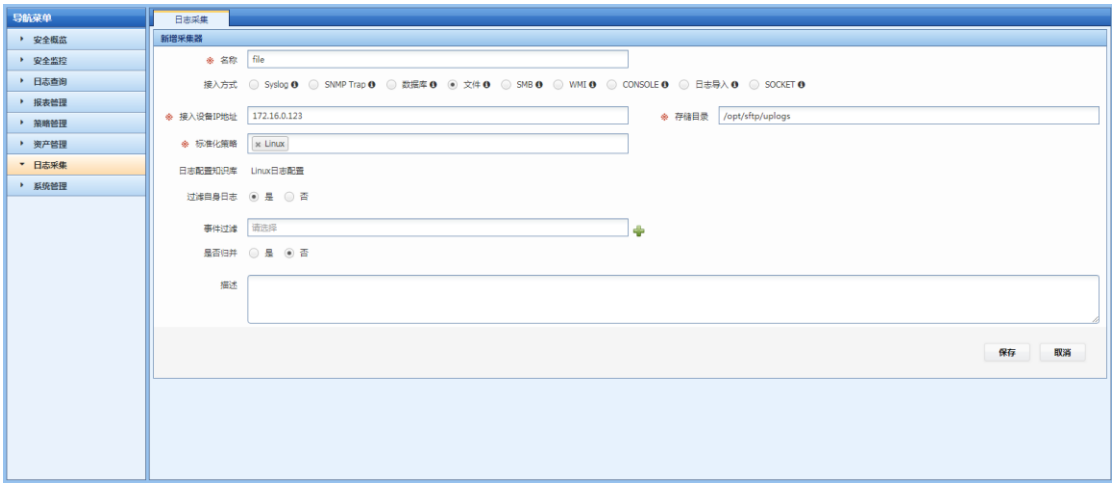
LAS 系统 SFTP 具体登录方式：（1）ip：LAS 系统地址；（2）用户名：uplogs；密码：upload-logs-by-this-user。

目标主机上需要有相应的 SFTP 客户端，可以实现日志上传 LAS 系统的功能。

三、配置步骤

1、登录系统进入日志采集页面，点击"新增"按钮

2、配置相关参数



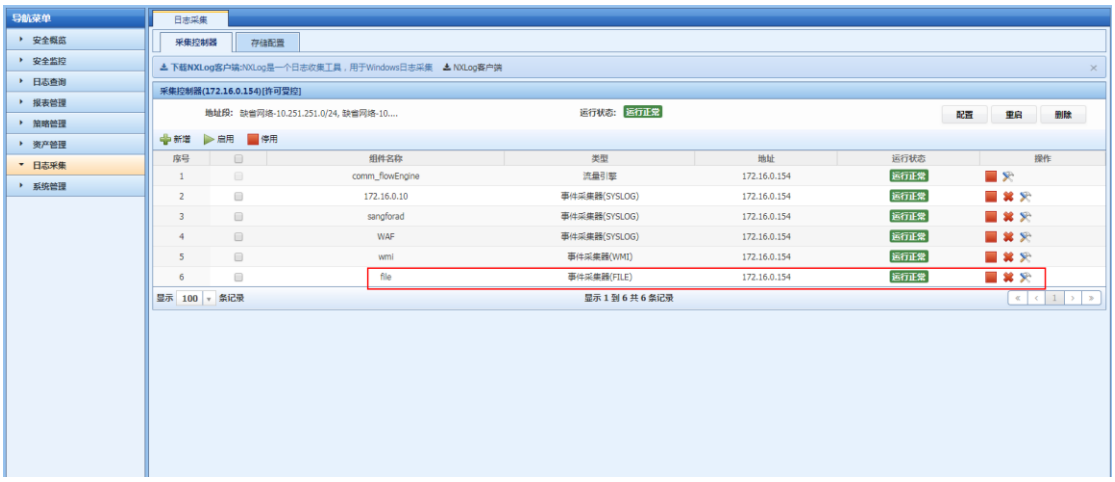
3、保存配置

点击"保存"按钮。

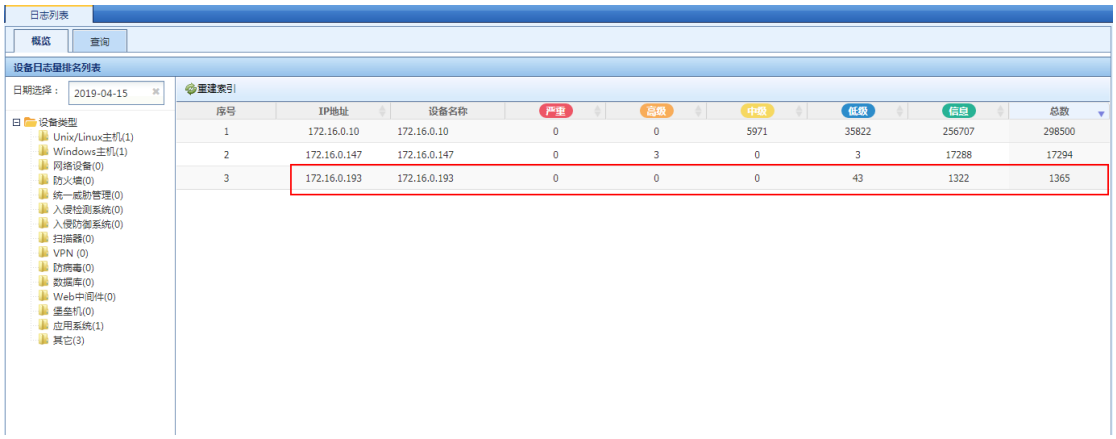
4、使用 uplogs 用户 sftp 登录到采集服务器的/opt/sftp/uplogs 目录下的 172.16.0.193 目录，将日志传入此目录。

四、功能验证

1、检查采集器状态是否正常：



2、检查是否收集到设备日志（日志查询->日志列表）：



2.2.5. 数据库方式

一、组网要求

1、被采集设备与日志服务器之间网络可达，用于数据库访问的相关端口畅通，比如 MySQL 的 3306，Oracle 的 1521；

2、需要提供被采日志数据库的表(视图)名、数据库登录参数。

二、组网拓扑

无

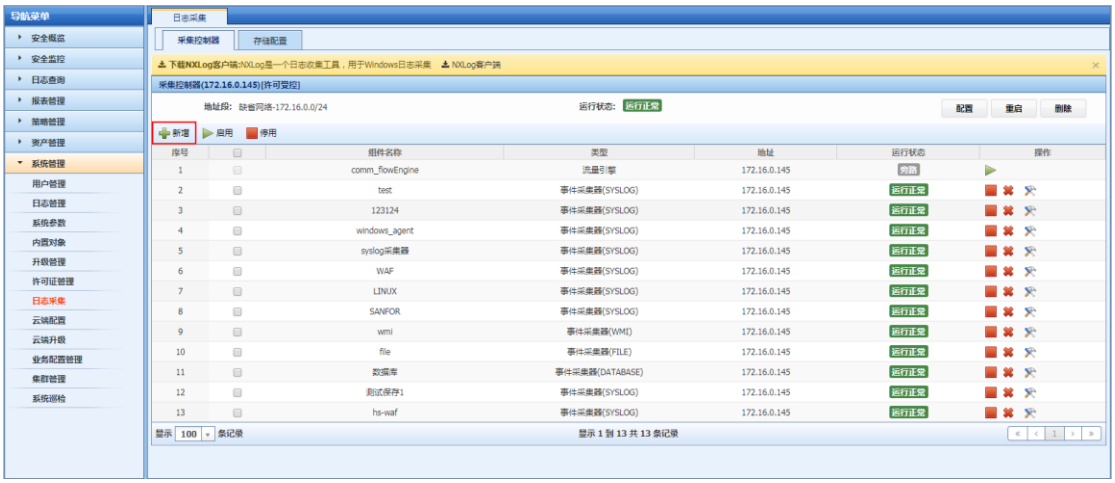
三、配置要点

适用于部分数据库自身的审计日志接入以及一些仅能将日志保存在数据库中的软件系统，如 Symantec 网络防毒系统、趋势网络防毒系统等。

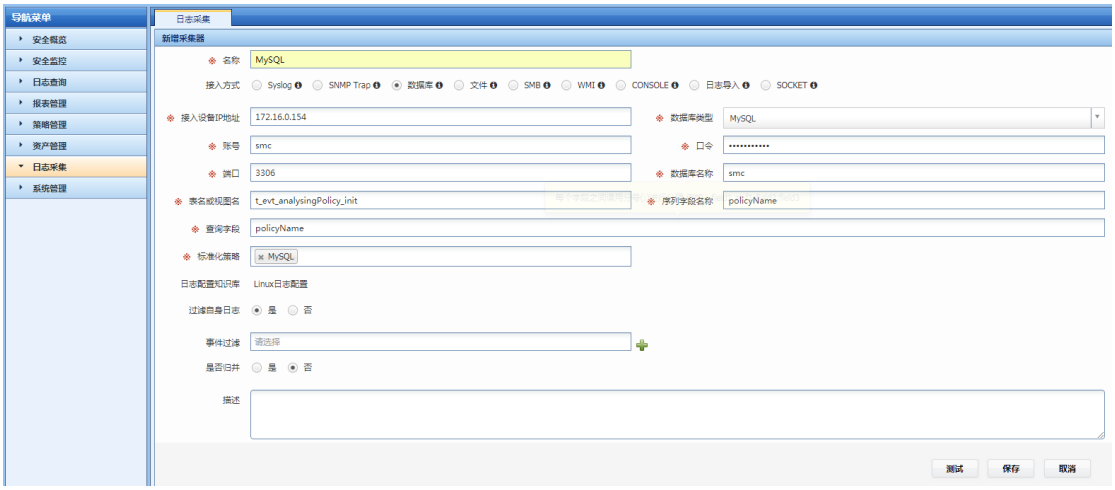
支持 SQLServer、DB2、Oracle、MySQL、Sybase。

四、配置步骤

1、登录系统进入日志采集页面，点击"新增"按钮 ：



2、配置相关参数：

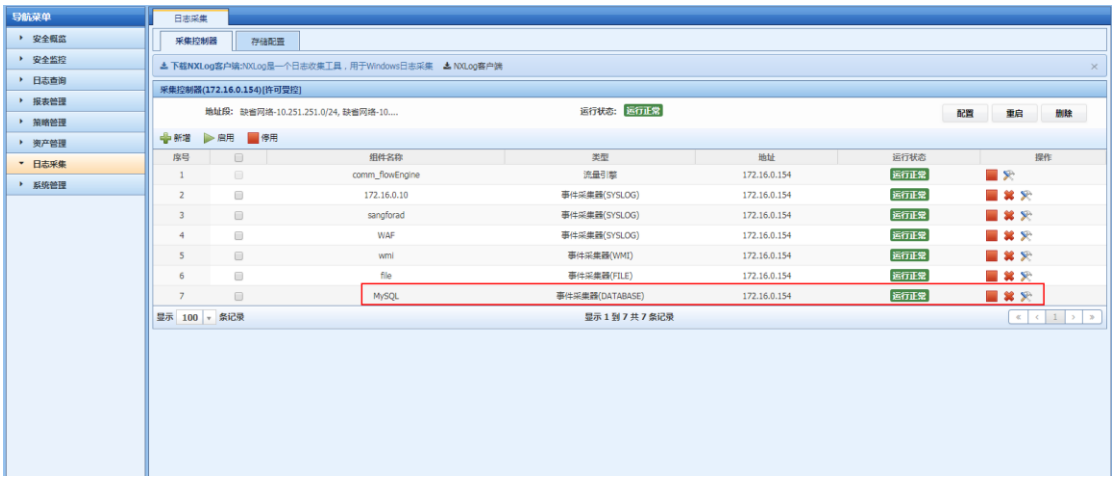


3、保存配置

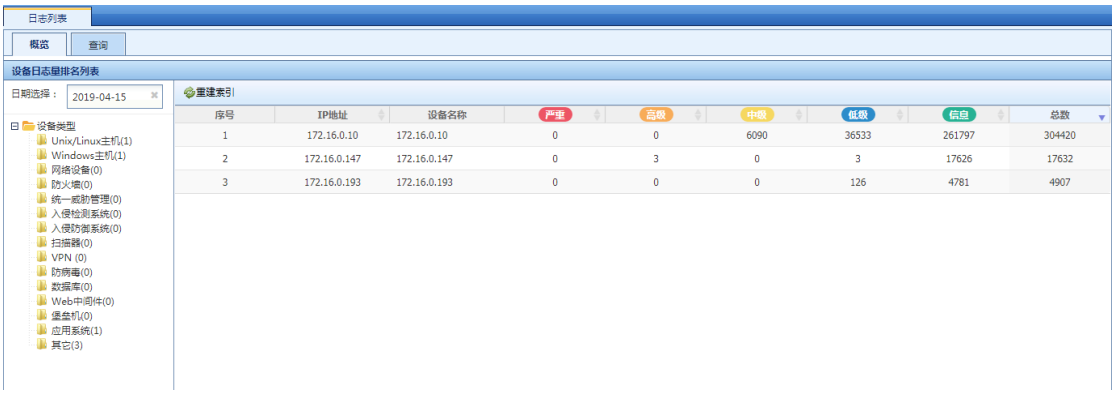
点击"保存"按钮。

五、功能验证

1、检查采集器状态是否正常：



2、检查是否收集到设备日志（日志查询->日志列表）：



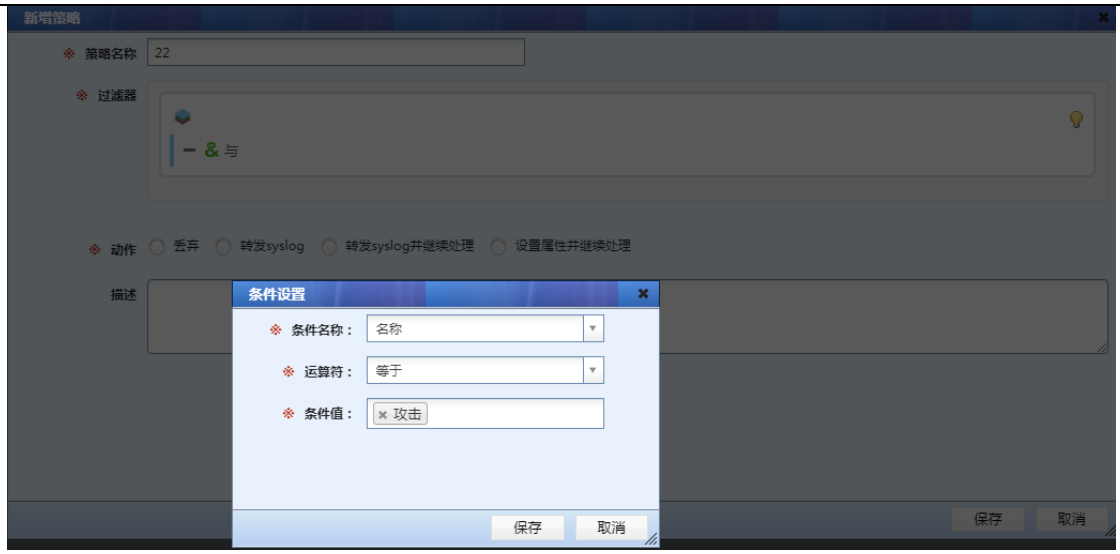
2. 2. 6. 日志归并

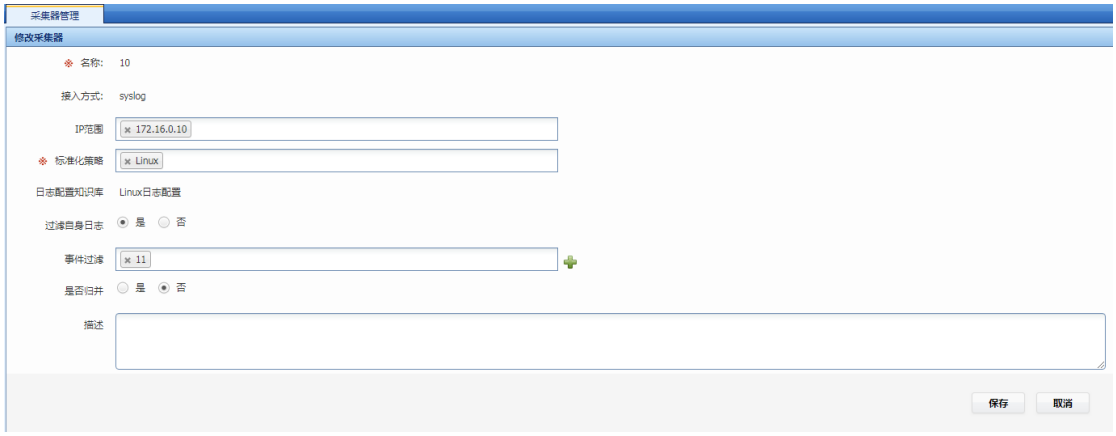
一、配置要点

归并策略是应用在采集器上的，而且一个采集器只能有一个归并策略。

二、配置步骤

1、登录系统进入日志采集，选择一个采集器，点击"修改"按钮。





2、保存配置

点击“保存”按钮 。

三、功能验证

1、检查采集器状态是否正常。

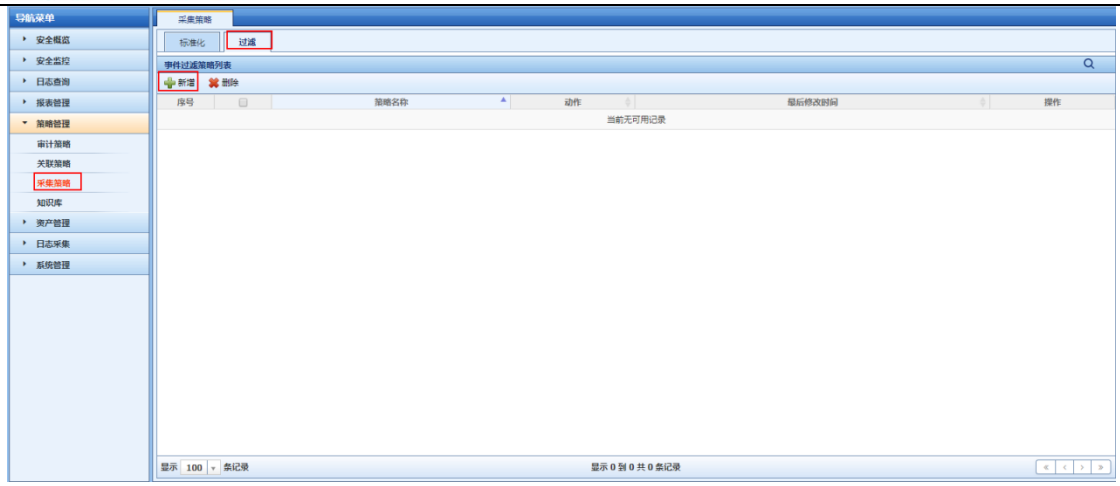
2、检查收集到设备日志是否已归并了相关日志。

2. 2. 7. 日志过滤

一、配置要点

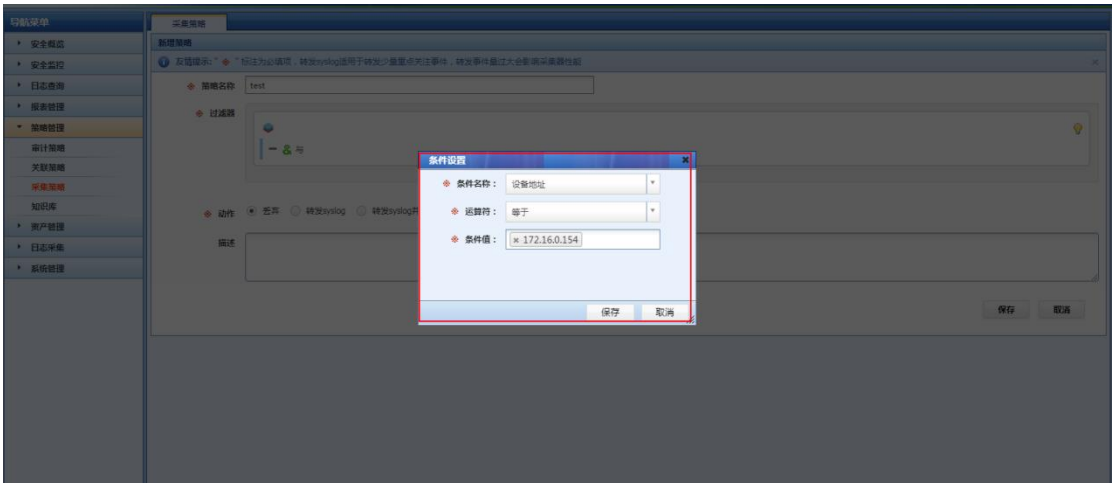
1、过滤策略是应用在采集器上的，而且一个采集器可以包含多个过滤策略。 **二、配置步骤**

1、登录系统进入策略管理->采集策略->过滤管理页面，点击"新增"按钮:



2、配置相关过滤参数:

(1).点击"过滤器"右侧条件按钮:

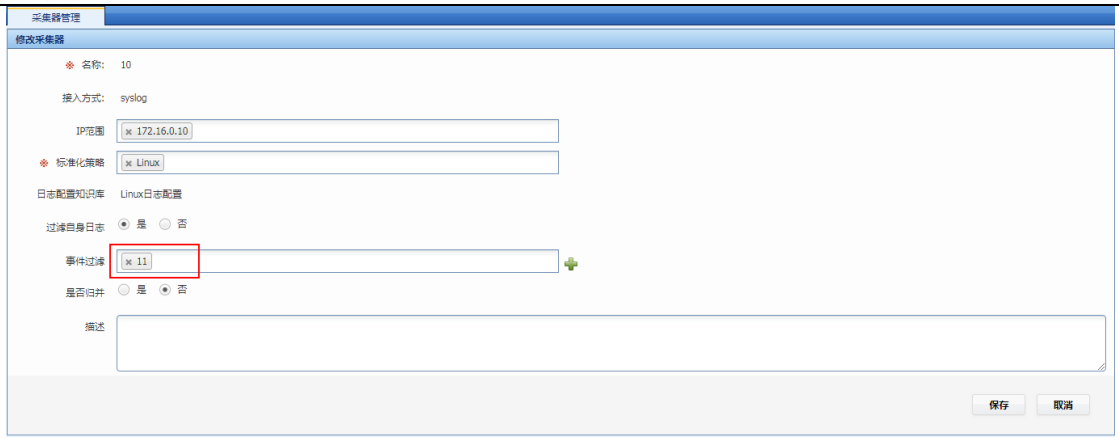


(2).保存配置 ：

点击"保存"按钮。

(3).应用策略到采集器 ：

点击"日志采集"，选择一个采集器，修改。



三、功能验证

1、检查采集器状态是否正常。

2、检查收集到设备日志是否已过滤了相关日志。

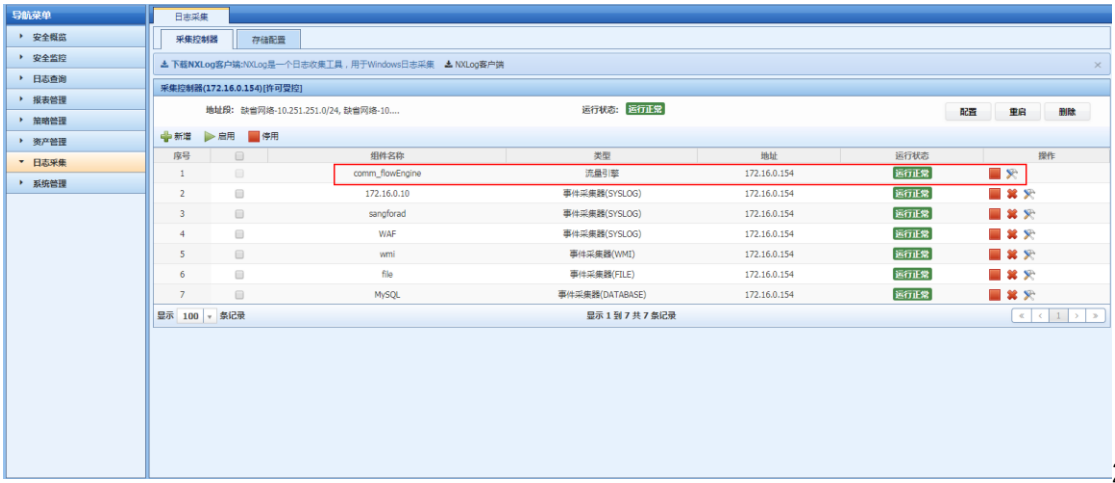
2.2.8. 流量引擎

一、流量引擎介绍

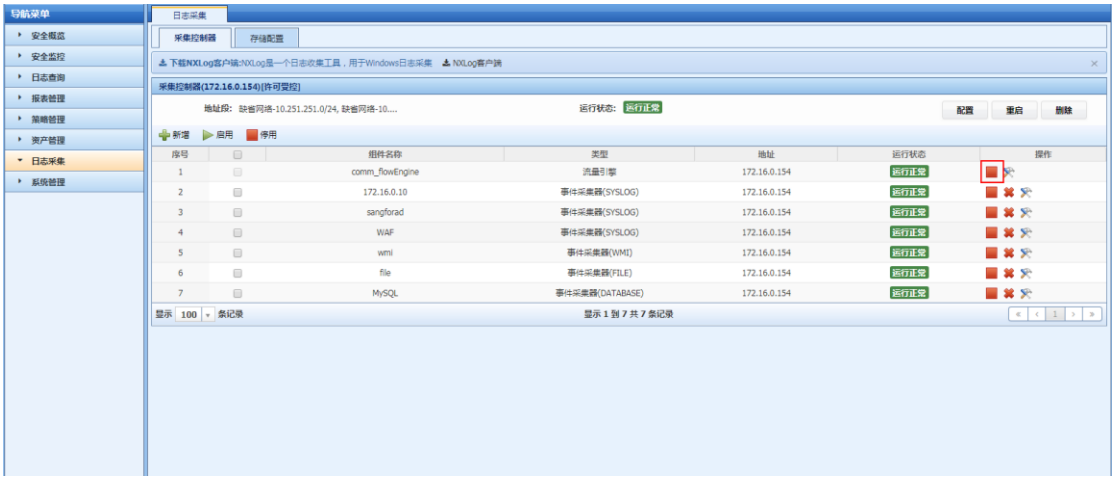
产品安装完成，流量引擎打开，系统可接收流量的镜像。当流量引擎旁路时，系统不再接收流量镜像。

二、流量引擎的启停

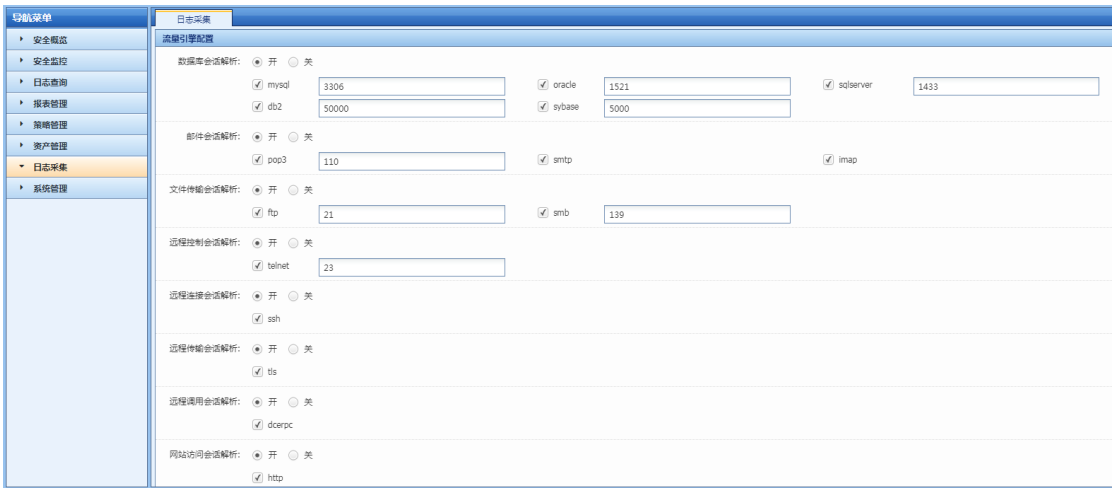
1.打开系统日志采集->流量引擎，查看流量引擎状:



2.流量引擎的启停：流量引擎默认为开启状态，用户安装产品完成时，流量引擎处于开启状态。用户可根据自身需求是否开启流量引擎，关闭方式如下 ：



3、 流量引擎配置：流量引擎默认为开启；用户可以配置自己想要的协议类型流量。



2.3. 关联策略配置（选配）

2.3.1. 关联策略说明

一、功能简介：

关联分析告警功能是系统中的重要功能之一，对于分析所产生的结果将在关联事件中呈现，如果符合关联策略,将以告警的形式在实时监控模块呈现给用户，用户可以对告警进行相关的处理。完成日志标准化策略后，建议直接启用 LAS 内置的关联告警策略。

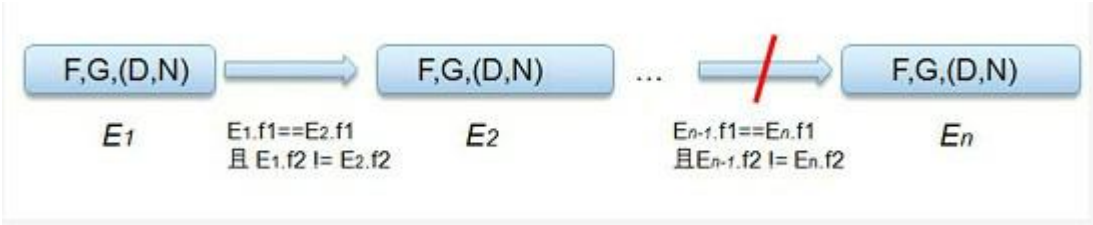
LAS 系统主要根据基于规则和基于统计的方式，关联安全事件并产生告警。

1、基于规则 ：

（1）基于规则的关联条件是这样一种状态机制，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；

- 时序：后续发生或后续不发生；
- 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）。

（2）规则关联告警举例：waf（web 防火墙）攻击日志关联防火墙访问日志，产生告警:

条件 1:【状态 1：waf（web 应用防火墙）60 秒内产生过源主机 a 到目标服务器 b 的一次网络攻击告警日志】;

条件 2:【状态 2：防火墙 60 秒内产生 10 条源主机 a 到目标服务器 b 的访问日志】;

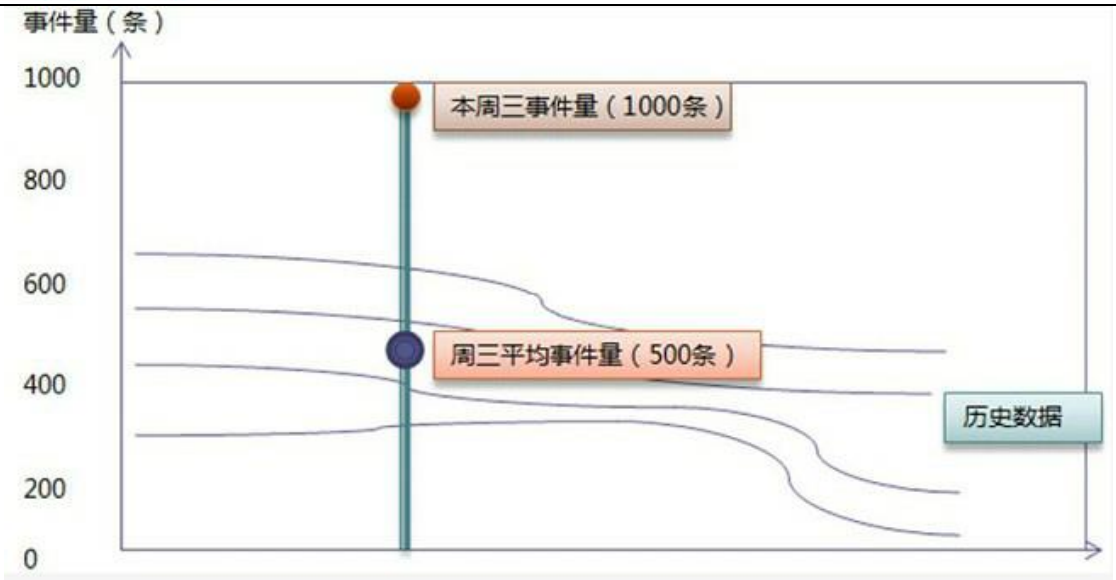
条件 3:【状态 1 发生之后接着发生了状态 2】 。

如果同时满足以上三条条件，则产生异常访问告警（一个攻击行为的源对目标进行持续访问，可能是一种探测行为）

2、基于统计 ：

（1）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）:



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、邮件、Syslog 等。

（2）基于统计的告警举例 ：

满足条件【1 分钟内产生 100 条 a 主机访问 b 服务器连接拒绝的防火墙日志】，则产生异常访问告警 ：

3、基于流量:

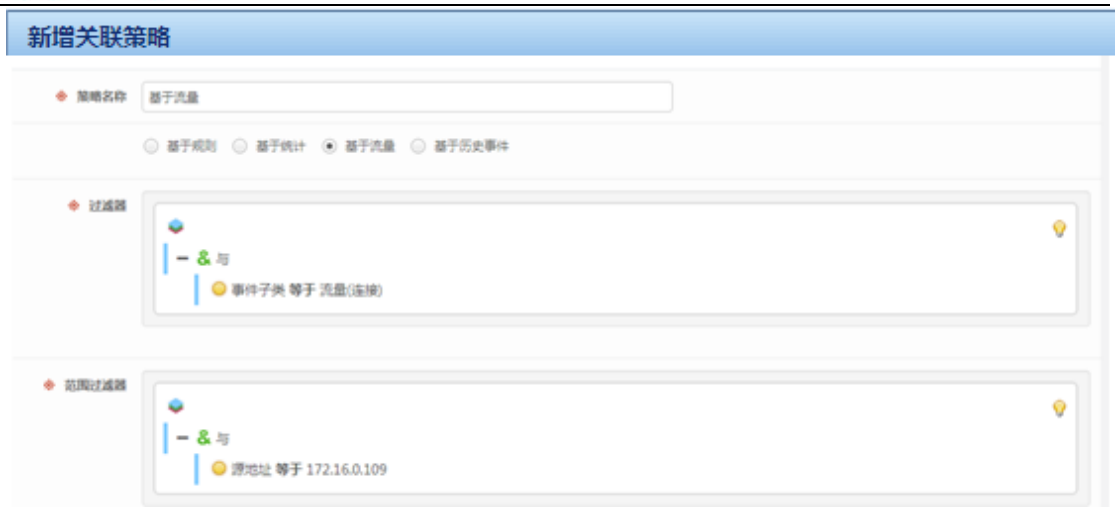
基于流量的关联策略只针对事件子类为流量（连接）的，它包括如下属性:

（1）归并字段：根据不同数据来源，对原始数据进行分组统计;

（2）触发条件：1->100 之间的整数值，超过该值时触发告警 ；

（3）统计时间：5->300 之间的整数值，单位秒，统计该时间段内的流量情况;

（4）统计字段：按照不同的维度进行统计，可选项为发送流量、接收流量、总流量。



4、基于历史事件:

基于历史事件的关联策略统计在一定时间片段内（比如 5 秒），没发生某种事件却发生了此日志，产生告警。它包括如下属性:

（1）事件 1：必选项，从某台设备收集到的事件;

（2）事件 1 之前 X 秒内不发生：5->300 之间的整数值，单位秒;

（3）事件 2：必选项，事件 1 之前发生的事件，如果在设置的时间范围内，没有收集到该事件，则产生告警。

5、总结 ：

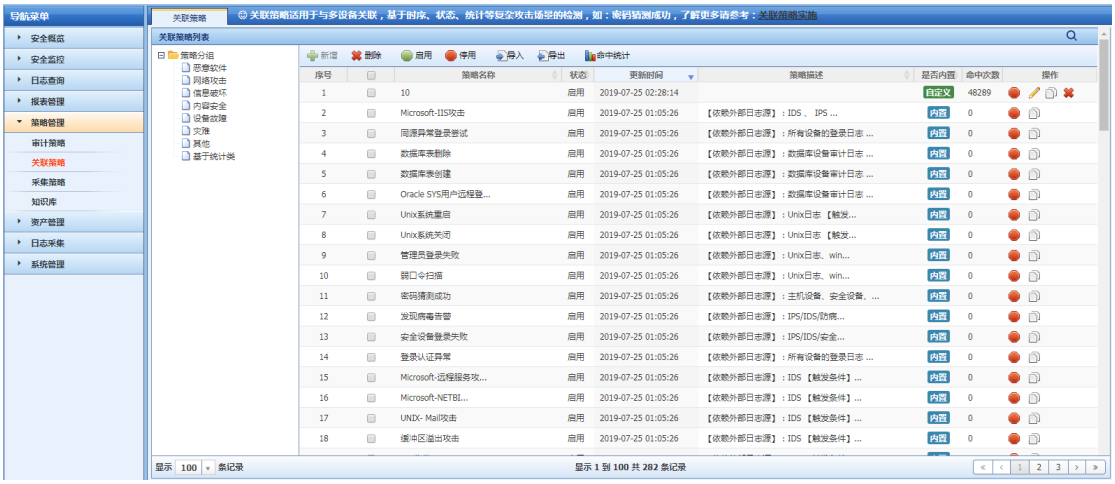
用户可以定义各类告警产生的策略（系统内置了部分策略）；在策略中可以设定对于安全数据的筛选条件、归并字段、时长和次数以及命中后产生何种响应；响应包括包含发送邮件、发送 Syslog 或 SNMP Trap、执行外部程序或脚本、暂存数据（用户可以将数据保存在临时表中作为其它策略的输入）等。

系统的关联策略不仅支持以预定义规则的方式进行关联，还支持基于模式发现方式的关联；系统不仅支持短时间内的序列关联，还支持长时间的关联（最长可达 30 天）。

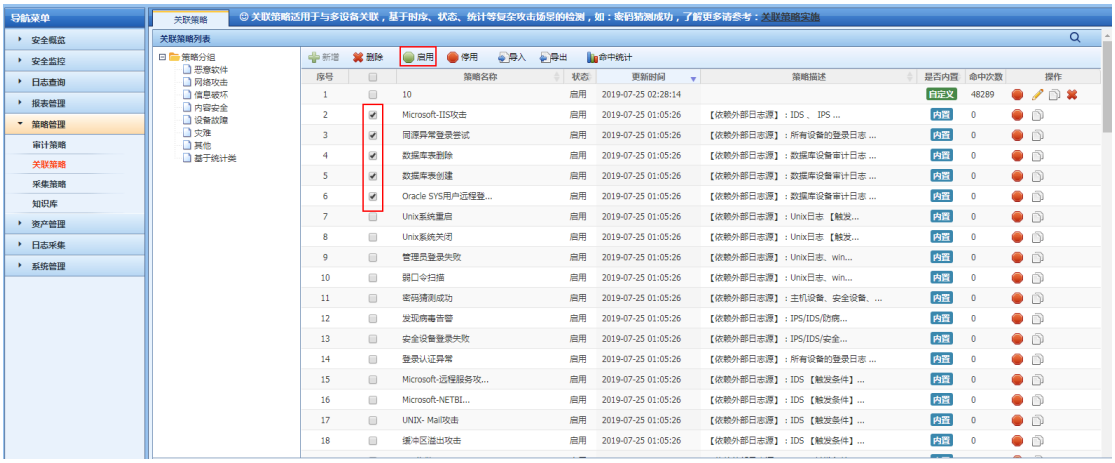
2.3.2. 具体配置

一、启用默认告警策略

点击"策略管理"->"关联策略"



勾选绿色状态灯的规则，点击启用。



查看策略状态：已启用

二、配置手工策略（按需配置）

手工关联告警举例：waf（web 防火墙）攻击日志关联防火墙访问日志，产生告警。

条件 1:【状态 1：waf（web 应用防火墙）60 秒内产生过源主机 a 到目标服务器 b 的一次网络攻击告警日志】 2.2.2.2;

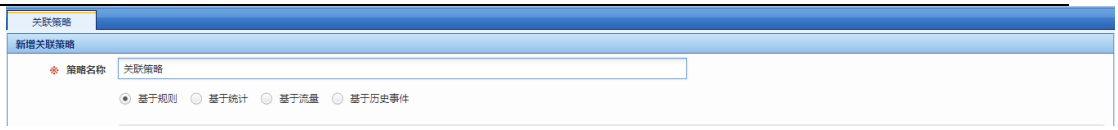
条件 2:【状态 2：防火墙 60 秒内产生 10 条源主机 a 到目标服务器 b 的访问日志】，防火墙 ip 地址：3.3.3.3;

条件 3:【状态 1 发生之后接着发生了状态 2】。

如果同时满足以上三条条件，则产生异常访问告警（一个攻击行为的源对目标进行持续访问，可能是一种探测行为）。

1、选择"策略管理->关联策略->网络攻击"，点击"新增"：

2、设定关联策略类型：



策略名称：取名任意，此例为 waf 设备日志关联防火墙日志产生告警，取名"WAF 关联防火墙"；

数据来源：本例要对 WAF 产生的攻击日志与防火墙产生的连接日志进行关联，这里选择"事件"；

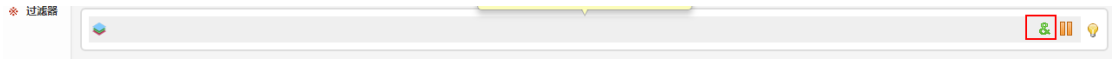
- 事件：根据来源于目标设备产生的安全日志进行告警策略设置；
- 基于规则：可以基于不同设备间的安全日志进行关联，本需对设备设备关联，此处选择"基于规则" ；
- 基于统计：基于事件频率进行关联报警 。

3、设置过滤器 ：

过滤器可以对日志等级、设备名称、时间、源目 ip、端口进行筛选，选取合适的日志信息进行关联。

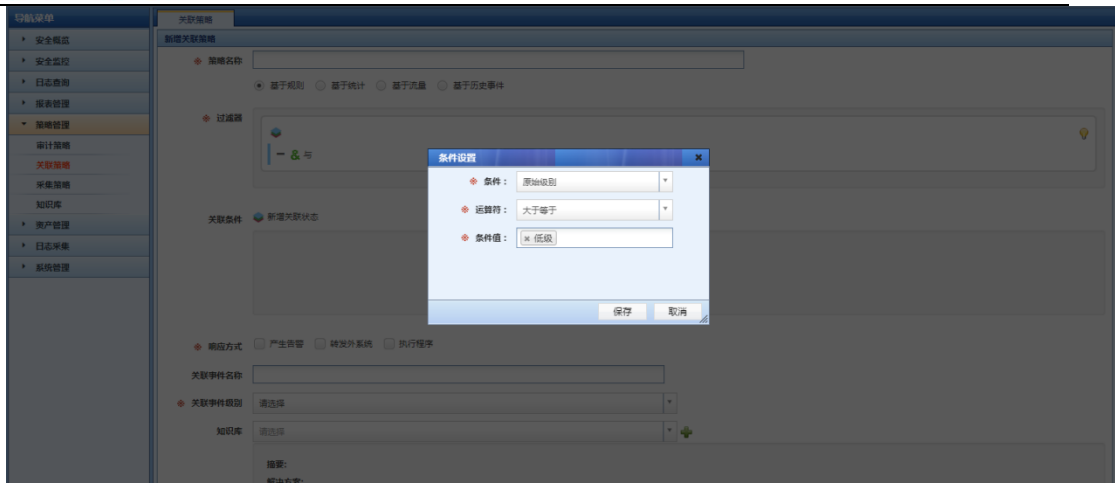
本例中对日志信息等级进行筛选，防火墙的连接日志可能属于正常连接，故这里日志级别选择较低级别的"信息"，对于日志信息大于或者等于级别为"信息"的日志，我们就进行关联分析。

点击运算符&符号，如下图 ：



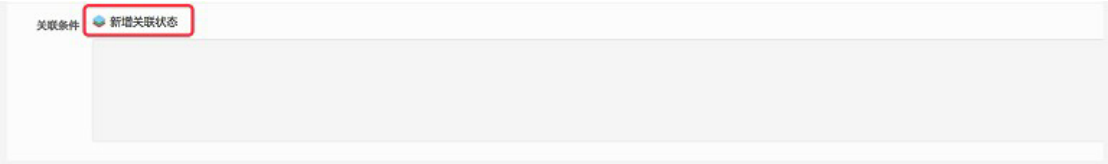
点击增加，如下图

条件设置如下图：对于安全日志信息级别属于"信息"及以上级别的，就进行关联分析。

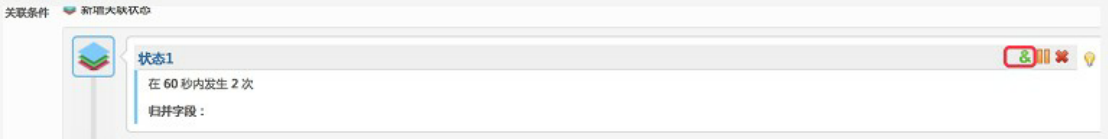


4、关联条件设置

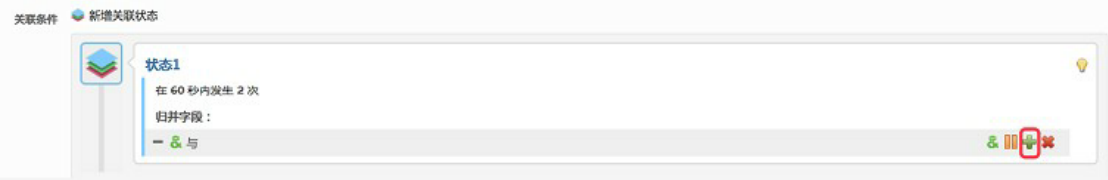
点击"新增关联状态"，如下图 ：



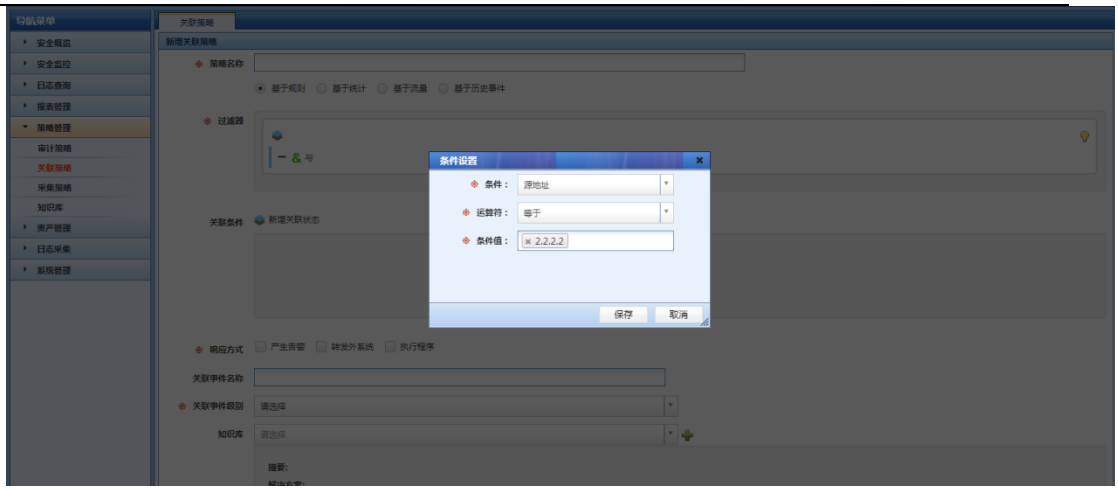
点击&运算符，如下图:



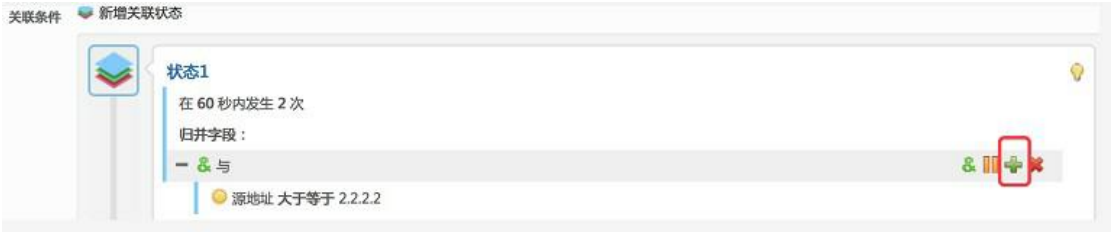
点击+号按钮，增加条件:



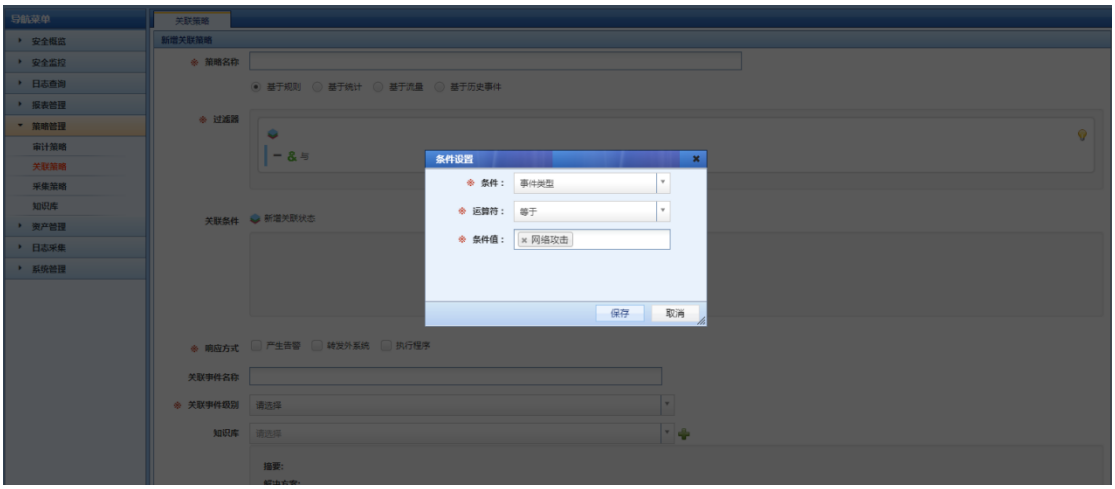
关联 WAF 防护系统的主机 ip 地址：2.2.2.2:



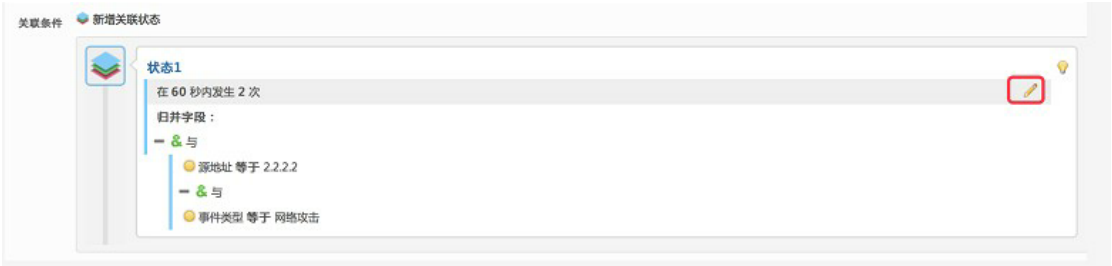
在状态 1 继续点击新增



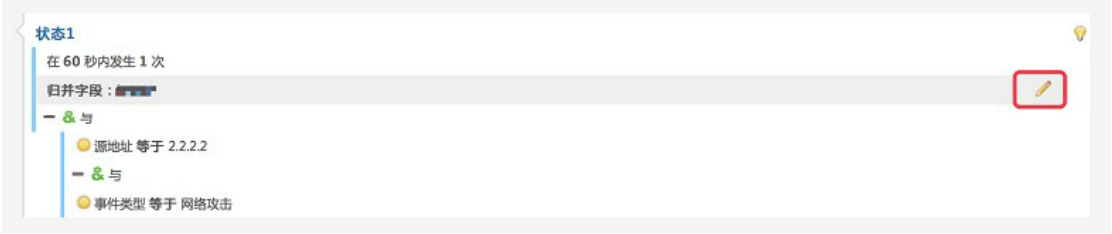
关联 WAF 防护系统的"网络攻击"事件类型



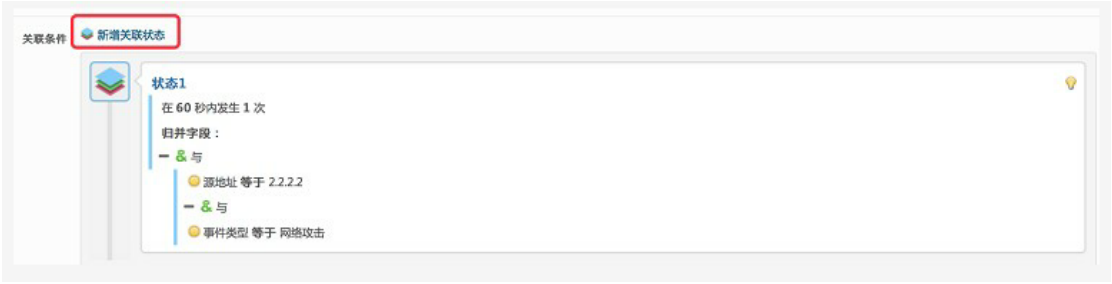
设置发生频率为 60s 发生 1 次



设置状态 1 的归并字段为源地址、目标地址（归并字段用于两个字段间进行匹配）



同理，新增状态 2，设置防火墙日志属性，如下图

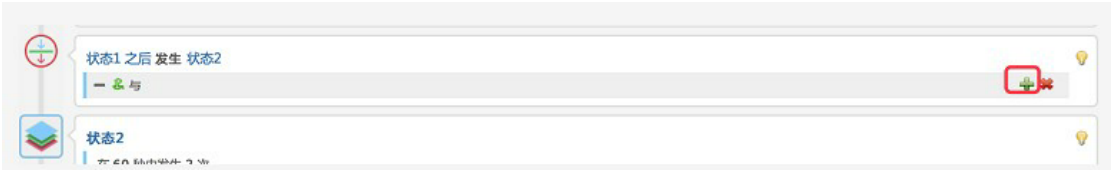


完成的设置结果如下图

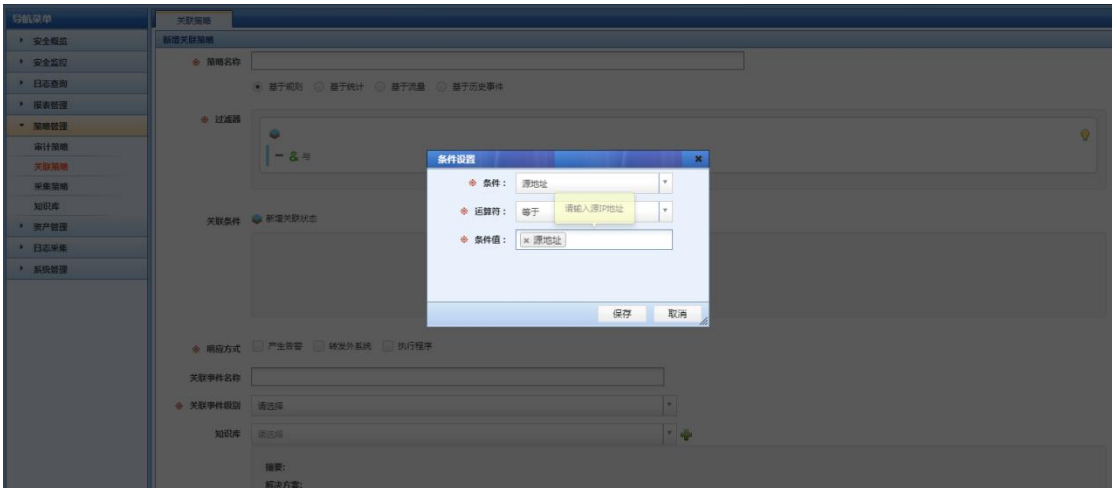
设置状态 1 和状态 2 之间的关联关系：状态 1 中的源地址、目的地址等于状态 2 中的源地址、目的地址：

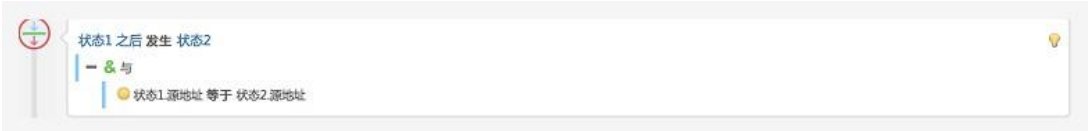
点击&符号

点击+号（如果状态 1、2 中没有设置归并字段，此处将报错提示无法添加）

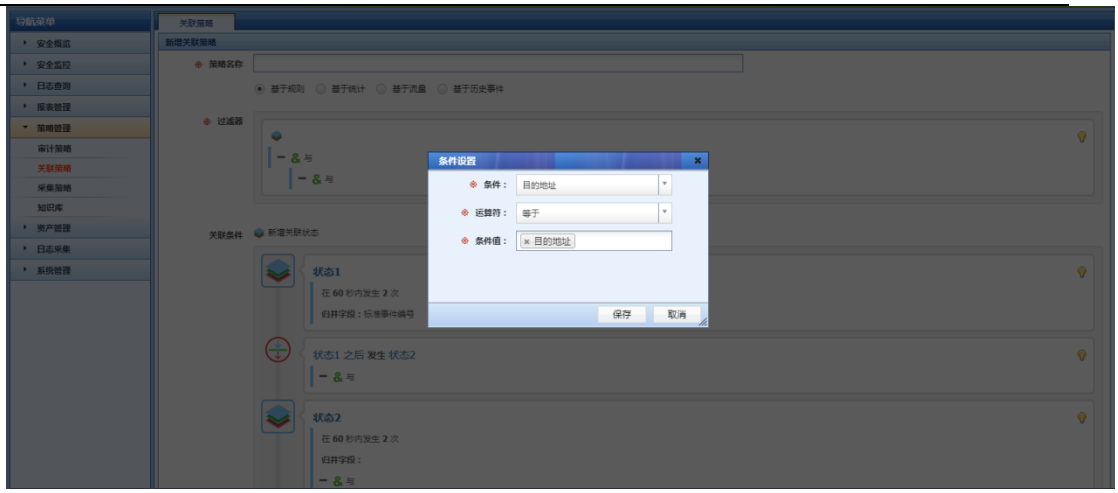


设置状态 1、2 的关联条件：源、目的 ip 相同

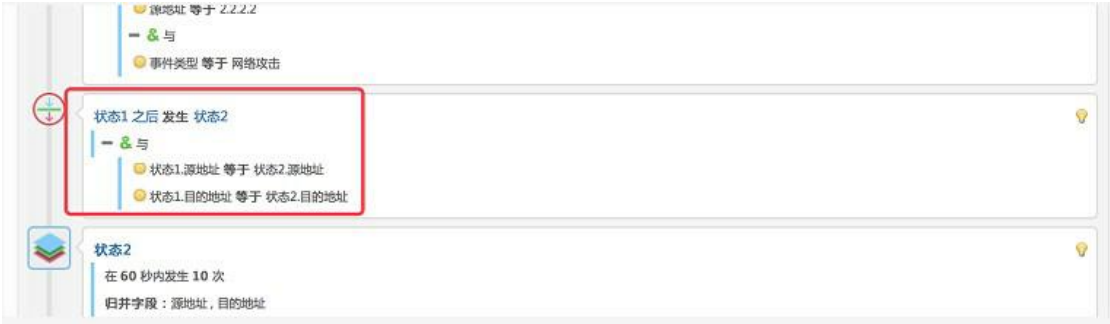




再增加目的 ip 相同



设置完成的界面如下图



最后设置响应方式：告警

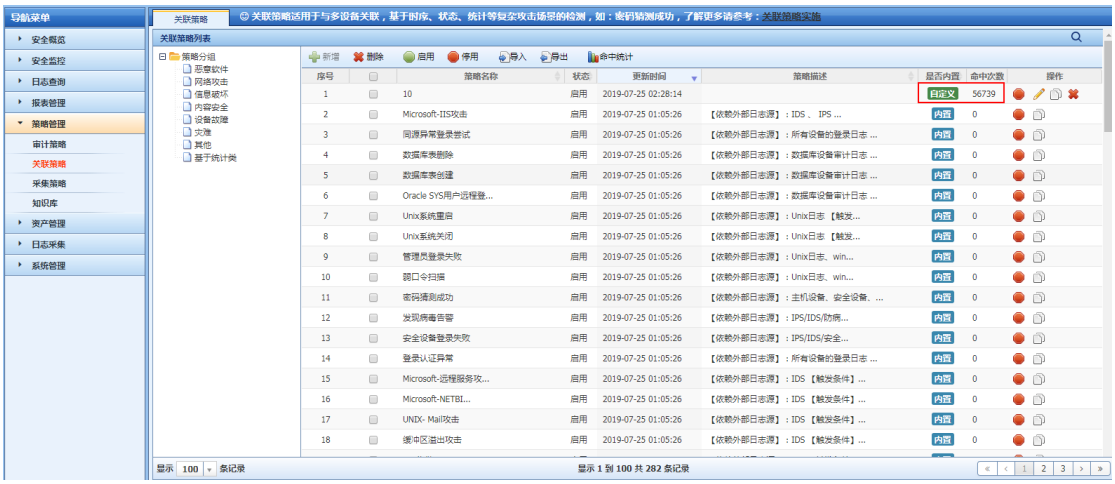
响应方式：选择告警

级别:选择严重（实际实施中结合用户实际情况）

告警子类等非必选项根据实际项目勾选

设置关联事件名称

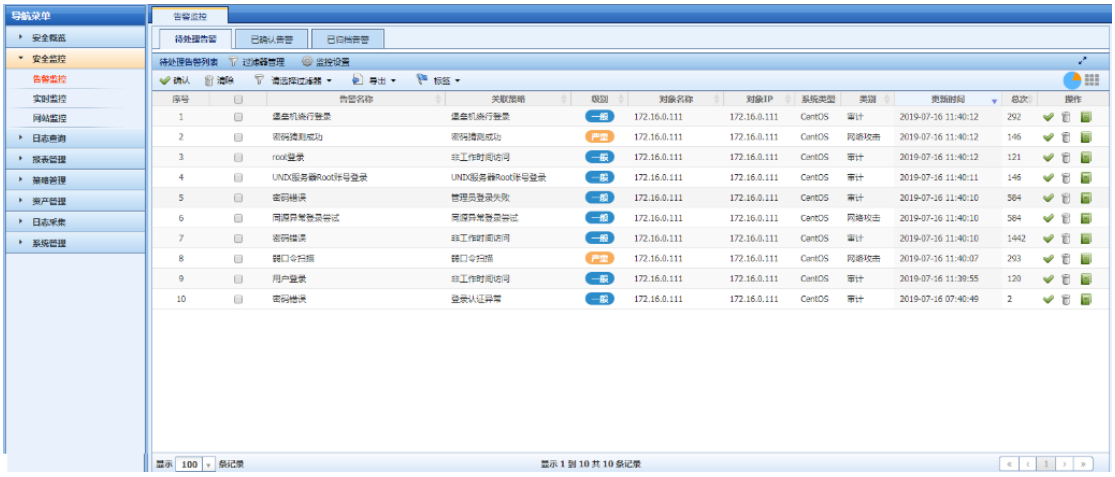
点击保存，即生成自定义的关联策略（添加的自定义策略，默认为启用状态）



三、告警信息查看

1、告警通知 ：

如果有新的告警产生，将会在 web 上方的消息处弹出气泡提示:

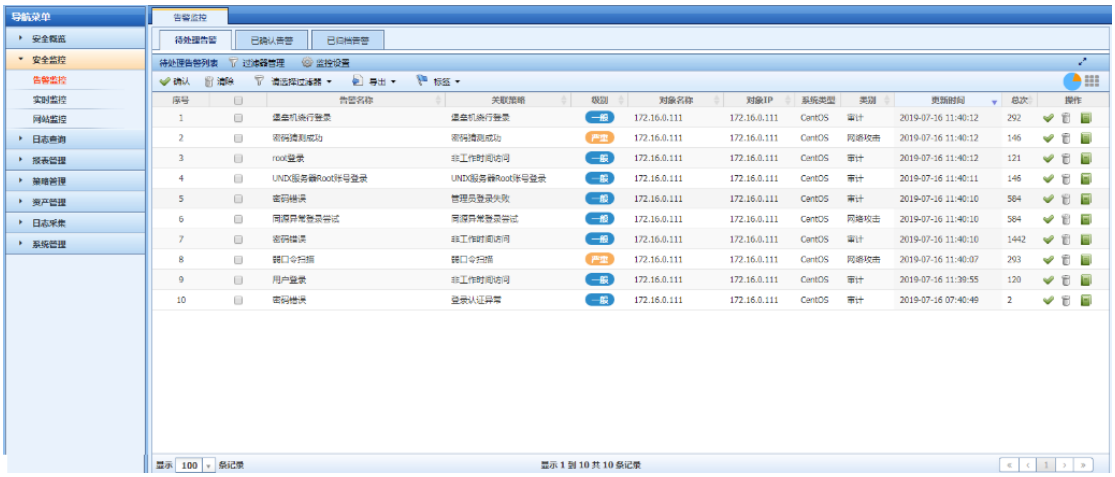


点击"消息"将会显示告警信息摘要

点击摘要，将会跳转显示具体的告警信息内容

2、告警信息查看及处理 ：

所有的告警信息均可以在"安全监控->告警监控"中进行查询



点击具体条目，可以查看具体告警信息

对于告警信息有：确认、清除两种动作:

"确认"操作：不在 LAS 上继续对告警信息进行处理，确认后的告警信息将会被移动到"已确认告警"；

"清除"操作：不在 LAS 上继续对告警信息进行处理，清除后的告警信息将会被移动到"已归档告警"；

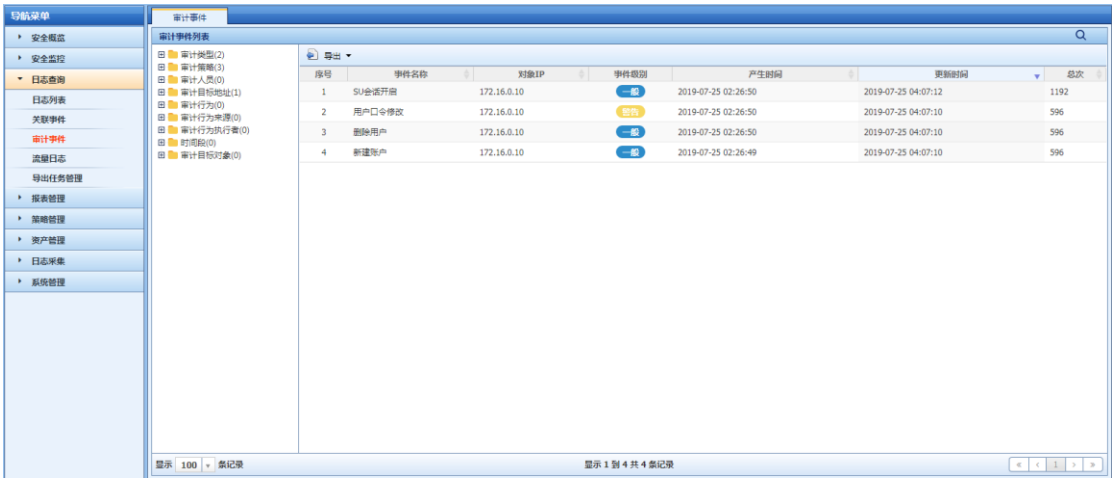
"查看知识库"：可以对告警条目进行解释，并提供建议操作。

2.4. 审计策略配置（选配）

2.4.1. 审计策略说明

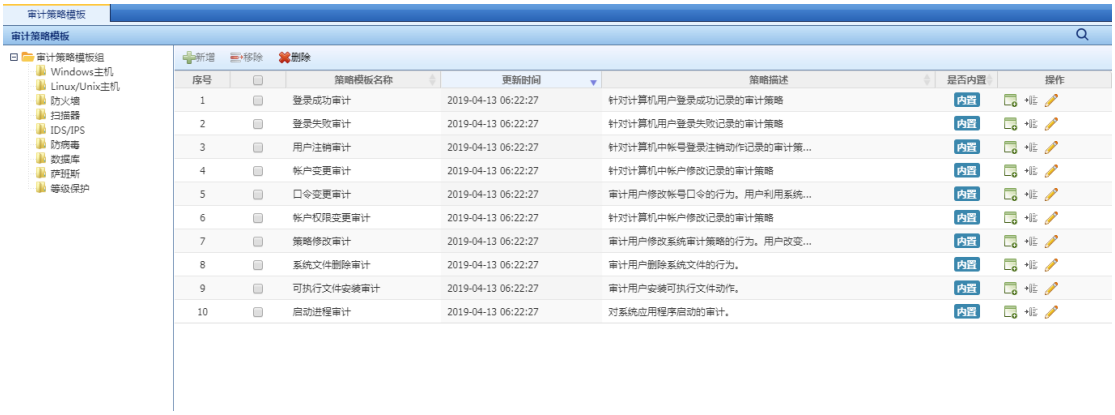
一、功能简介：

审计管理能是系统中的重要功能之一，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、IP 地址、人员、方式等，对于相符合的结果，系统将在审计事件中呈现给用户，如果符合定制的审计策略,也会在实时监控模块以告警形式展现给用户。



审计管理为审计人员、系统管理人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。

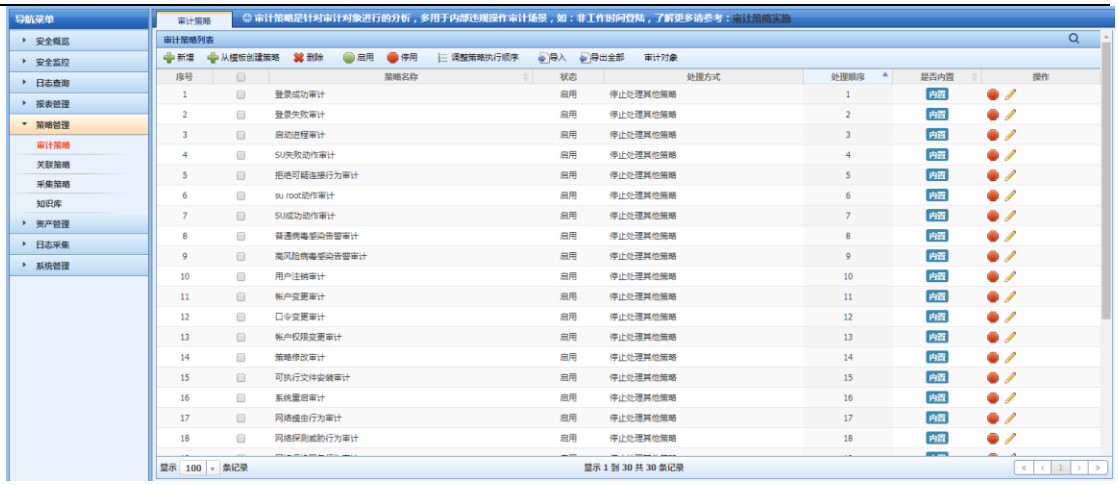
审计管理能够方便的自定义审计人员、行为对象、审计类型、审计策略等基本配置；并能够自定义审计策略模板，审计管理内置了大量审计策略模板，涵盖了常见的、对企业非常实用的审计策略模板，如主机、防火墙、数据库、萨班斯审计策略模板等。



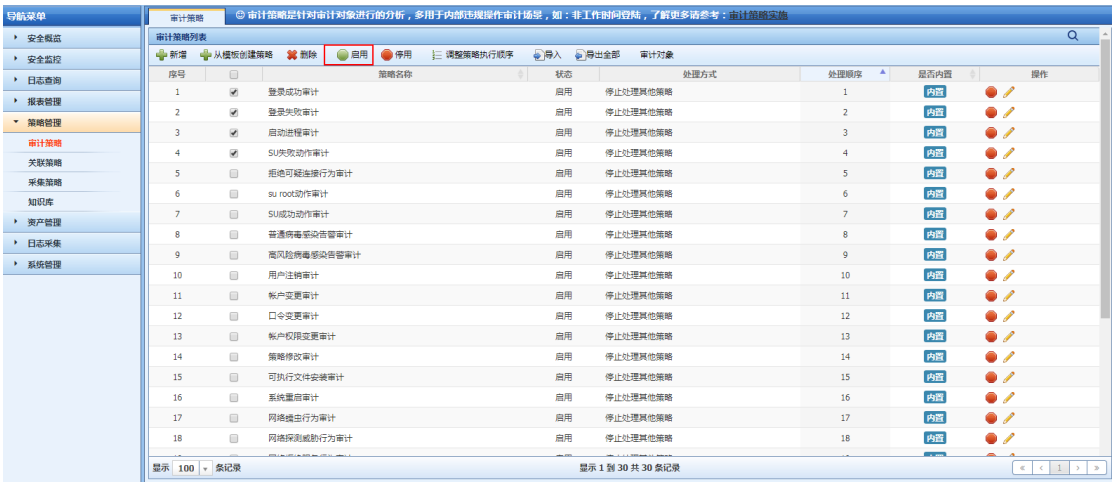
2.4.2. 具体配置

一、启用默认告警策略

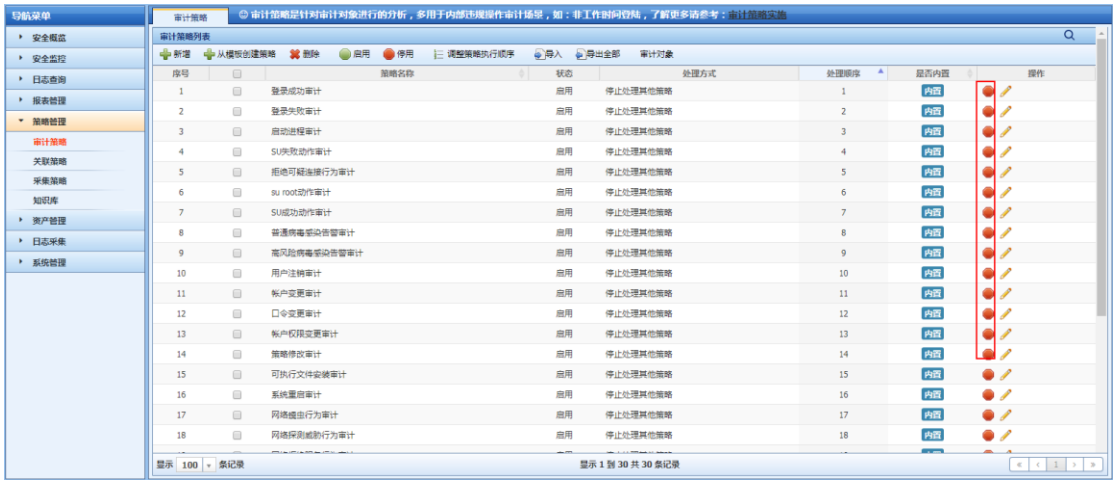
点击"策略管理"->"审计策略"



勾选绿色状态灯的规则，点击启用。



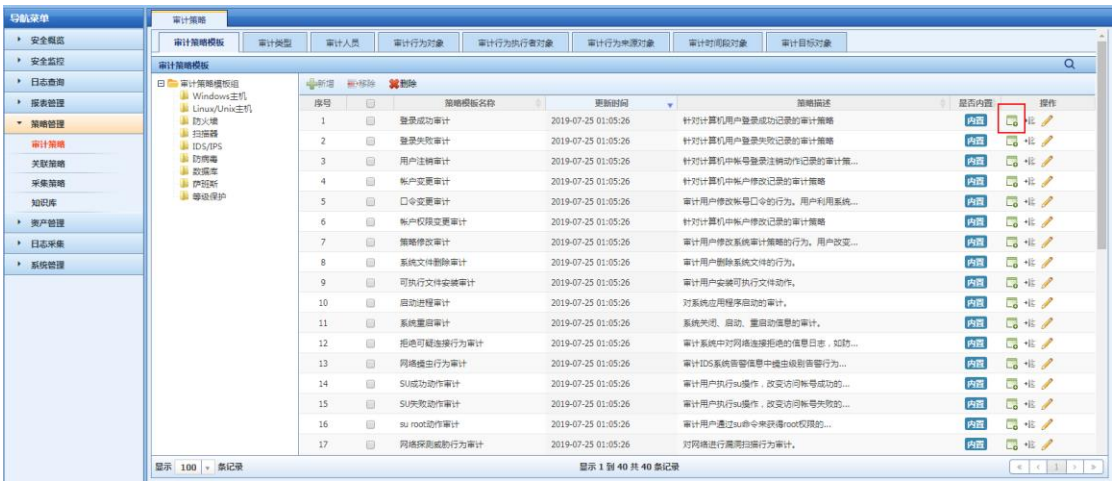
查看策略状态：已启用



二、配置手工策略（按需配置）

方法一：从审计策略模板创建

进入审计策略->审计对象->审计策略模板页面



1、策略模板组：可以选择后进行模板的增删改查。也可以点击，对模板组内的模板进行分组调整。

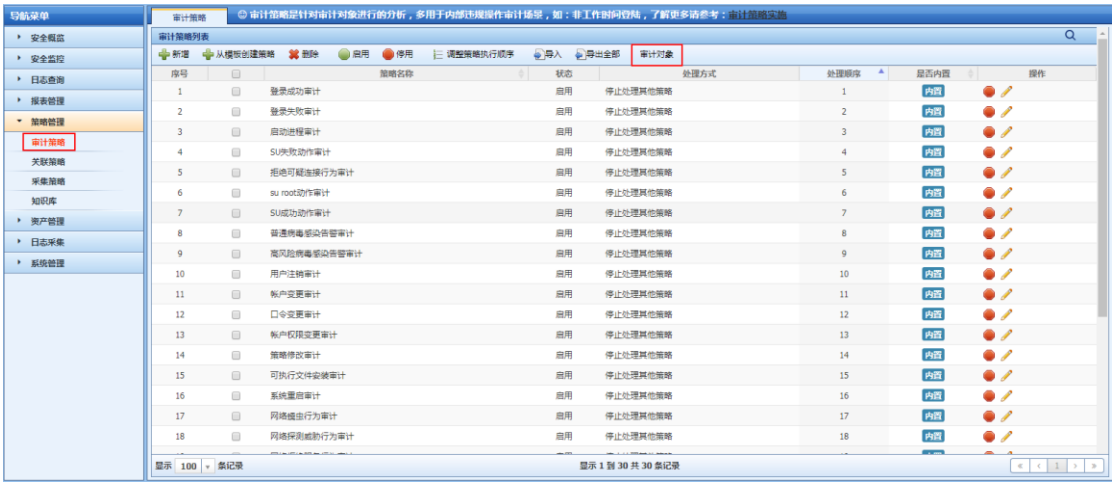
2、对模板组内的模板进行新增、移除和删除操作。

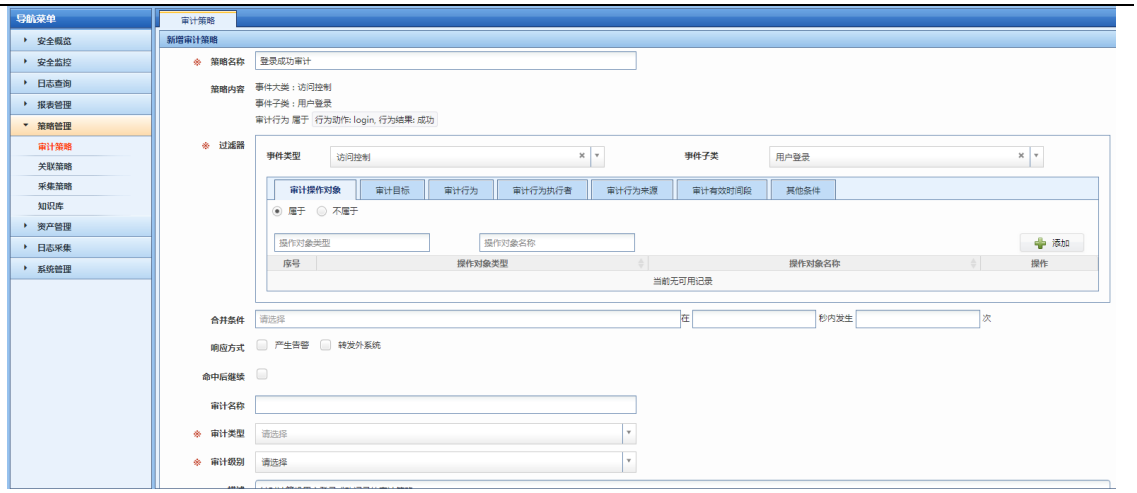
3、从模板创建策略：利用模板内的配置，创建新的策略。

4、将策略模板进行策略组调整。

5、修改策略模板。

点击从模板创建，根据实际情况对策略内容进行调整后保存即可



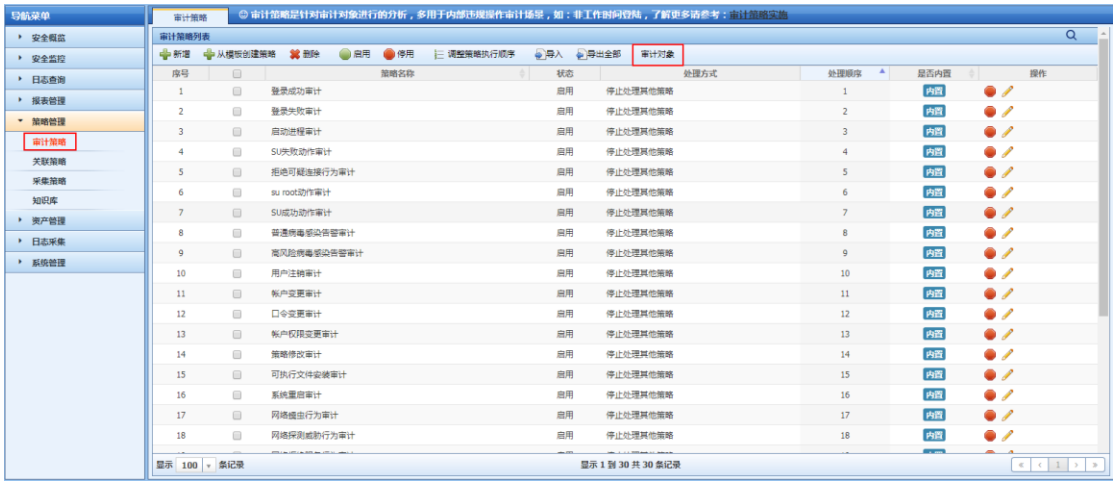


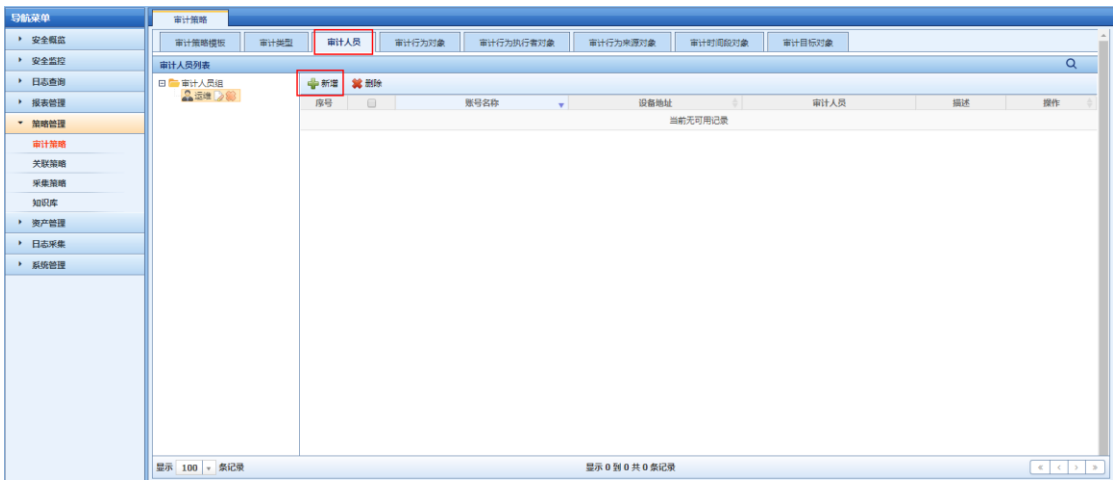
方法二、新建自定义审计策略

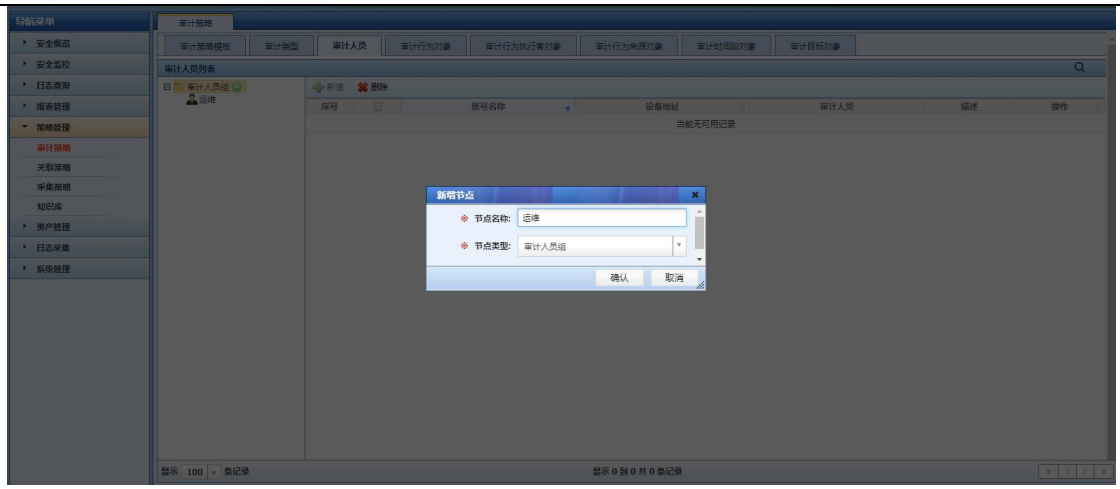
举例：访问控制日志审计

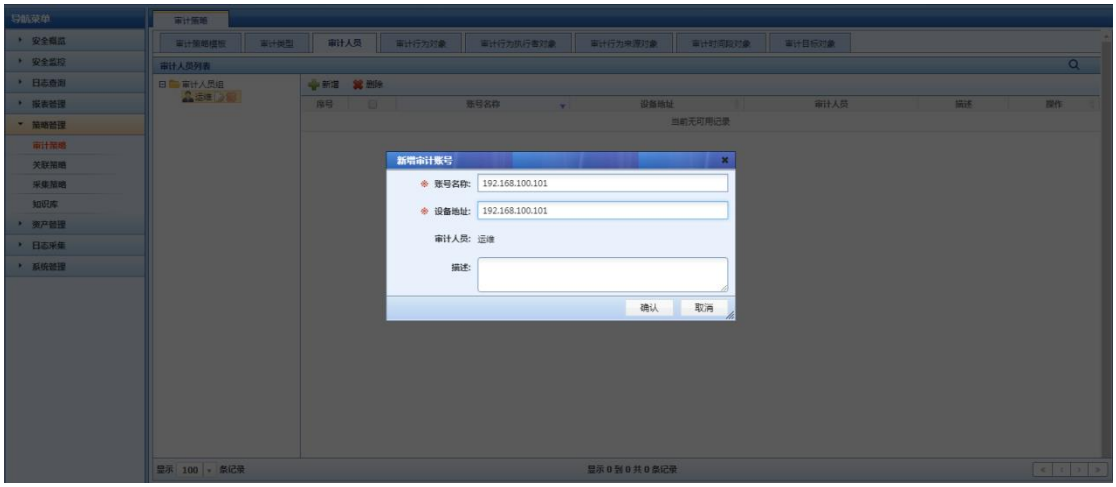
192.168.100.101 的 root 帐号属于运维人员张鹏，当 192.168.100.101 的 root 登录系统时，审计事件将显示审计人员为张鹏。

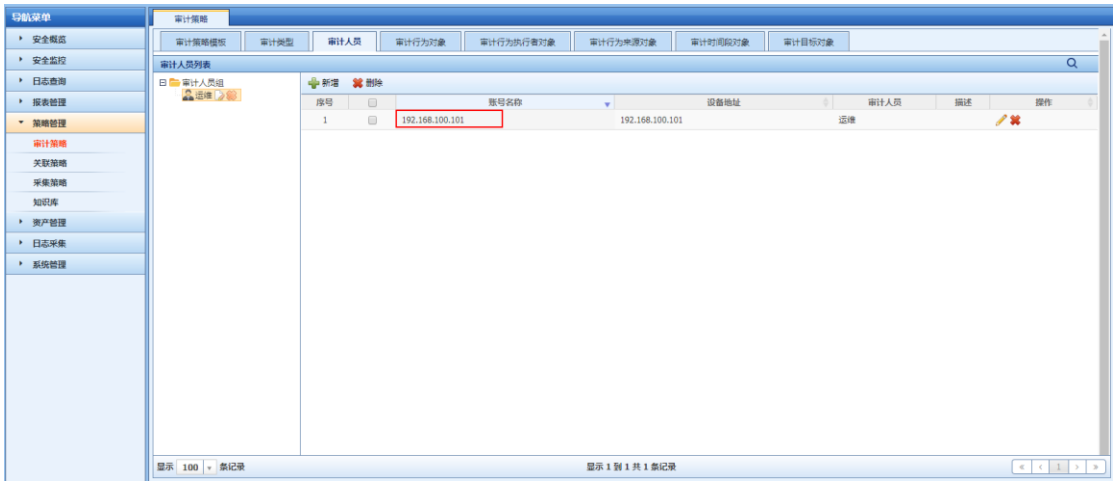
1、选择"审计策略->审计对象->审计人员"，新增审计人员 ：



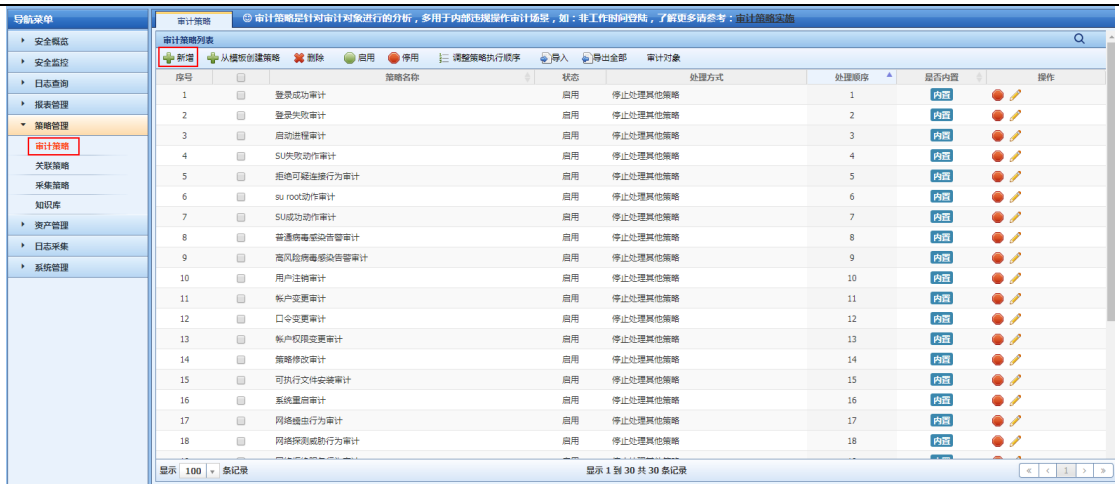


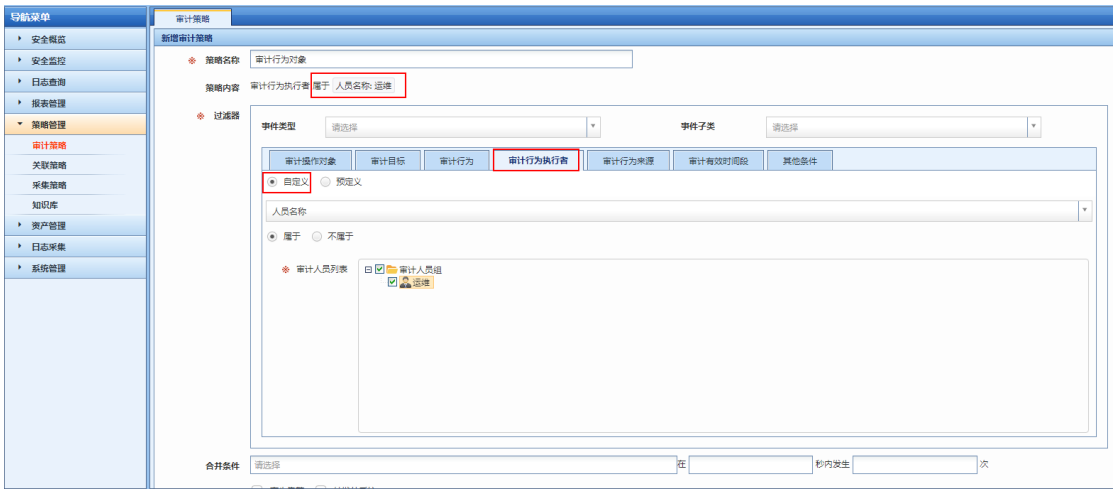


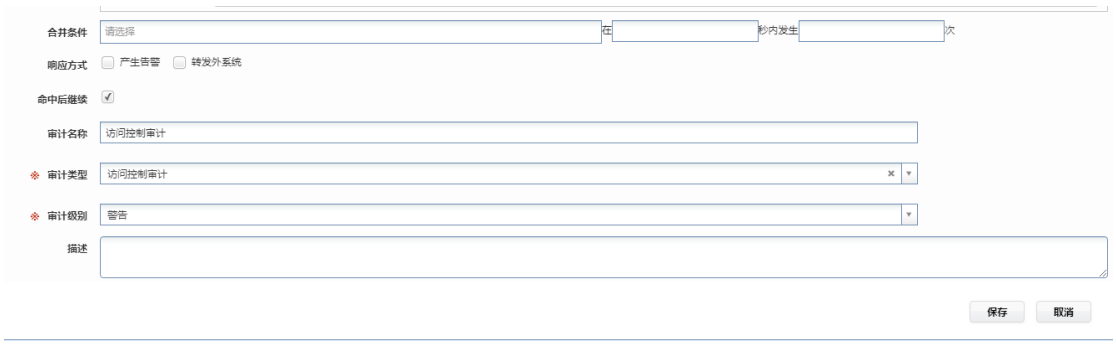




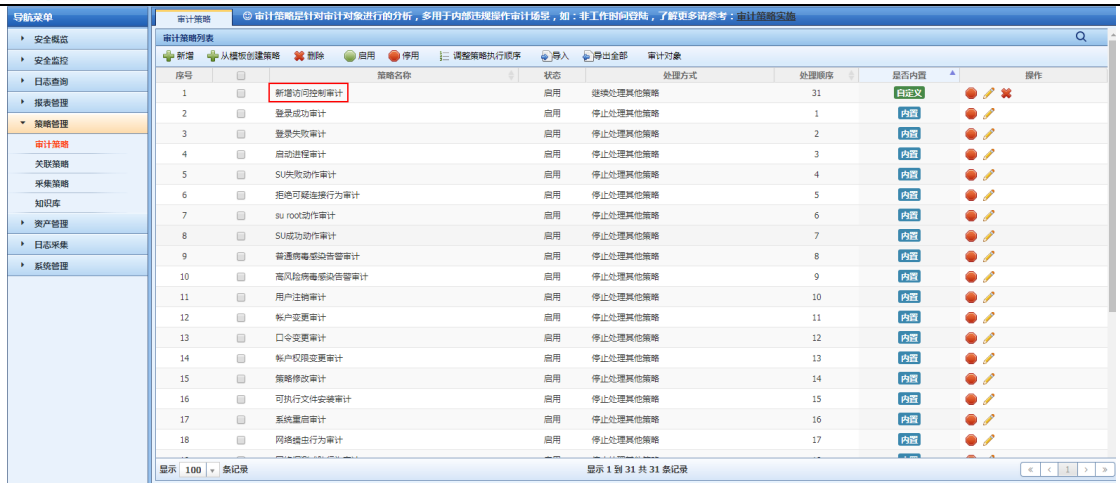
2、选择"策略管理->审计策略"，新增访问控制日志审计:







点击保存即可生成审计策略。



2.4.3. 审计对象管理

一、审计对象说明

审计对象用于创建审计策略时调用的审计对象，可在多条审计策略中重复调用。

包括审计人员、审计行为、审计行为执行者、审计行为来源、审计时间段、审计目标。

1、审计人员：将系统帐号和自然人进行关联 ；

2、审计行为：如登录动作 login、攻击动作 attack 等 ；

3、审计行为执行者：行为动作的帐号，如源用户，可选择已定义的审计人员，或者直接定义设备地址和帐号 ；

4、审计行为来源：行为的源地址 ；

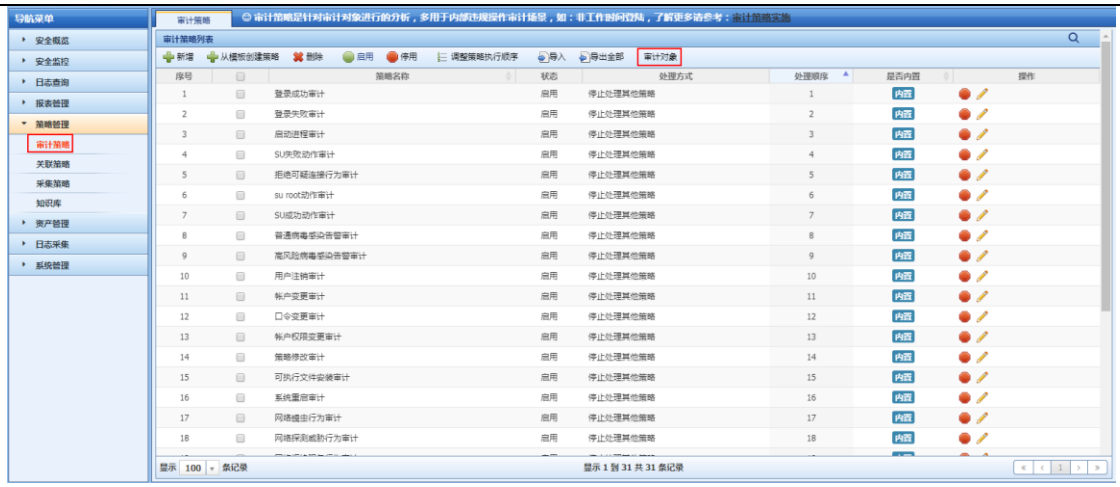
5、审计时间段：审计行为发生的时间段 ；

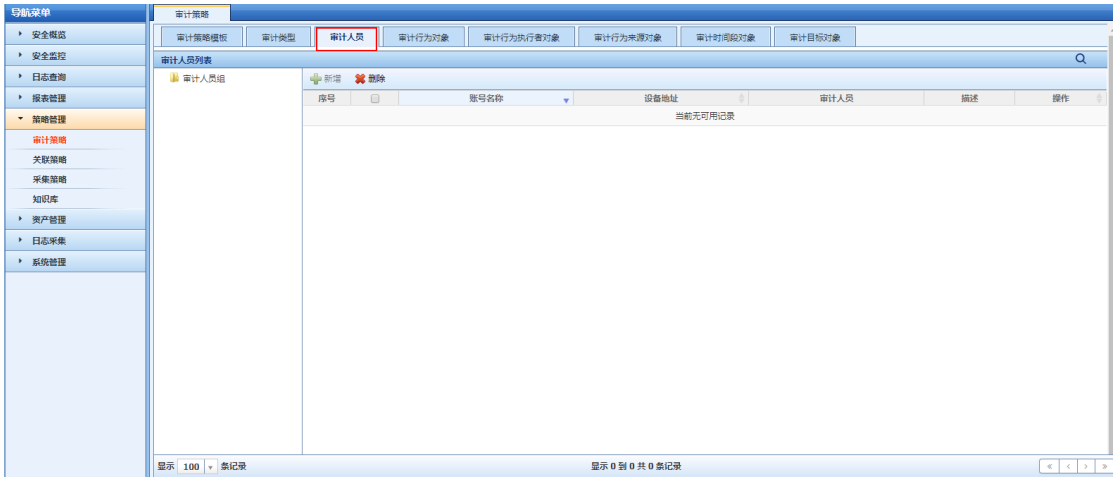
6、审计目标：行为的目标地址、主机设备等 。

2.4.3.1. 审计人员

一、审计人员配置说明

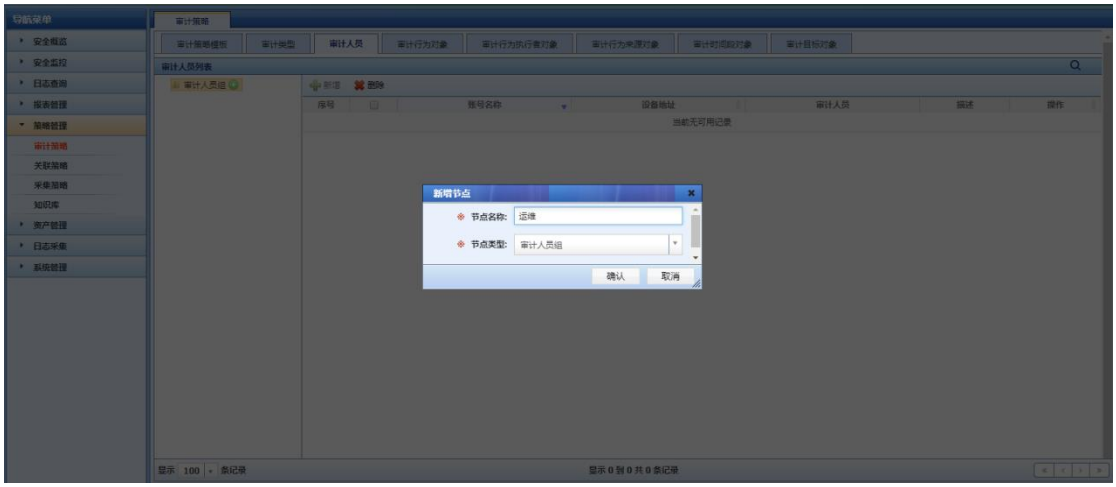
步骤一、进入审计策略->审计对象->审计人员页面：



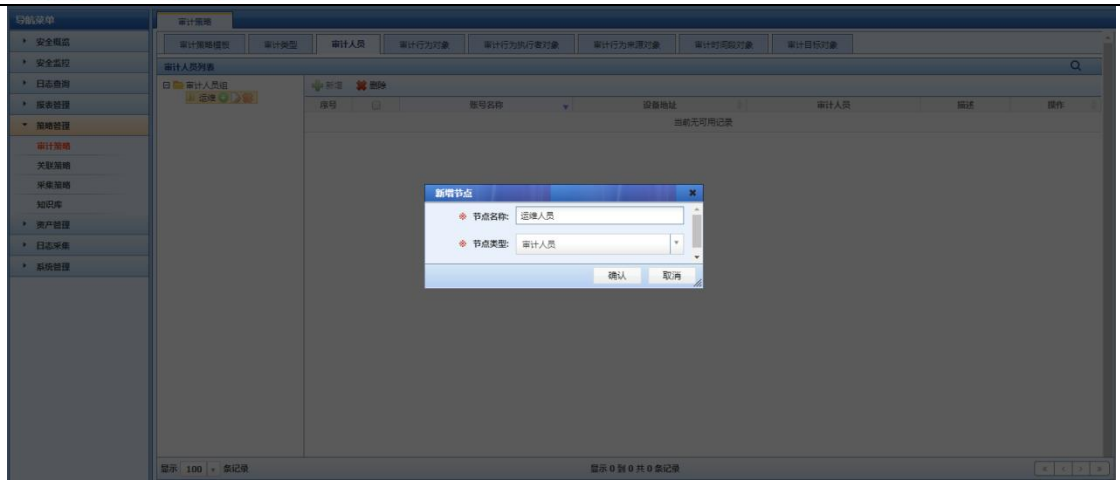


1、增加审计人员组：

(1)点击右侧+号

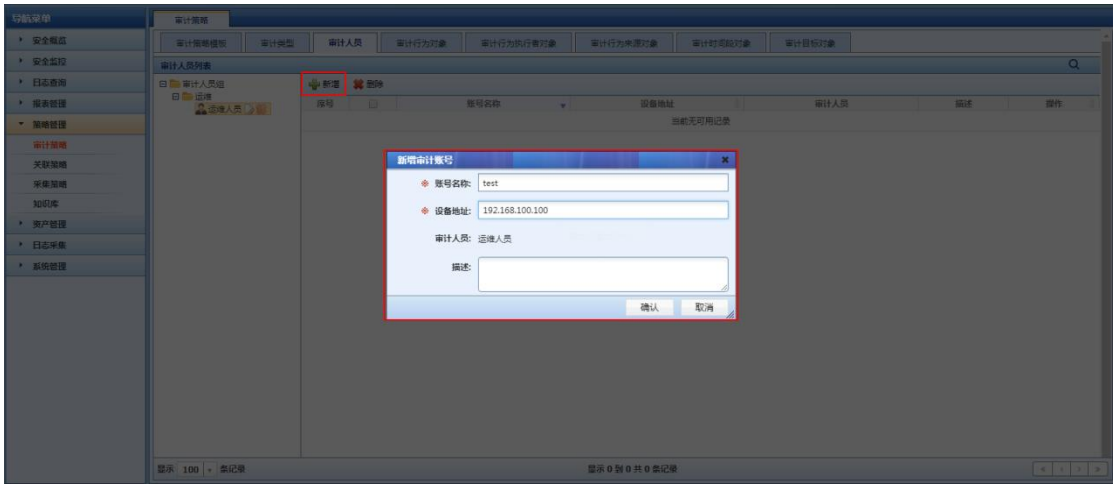


(2)点击新增节点右侧+号，创建审计人员节点



2、修改或者删除审计人员：

步骤一、选中审计人员节点，点击新增按钮，输入绑定的系统账号和 IP 地址



步骤二、点击"确认"按钮，保存审计类型。

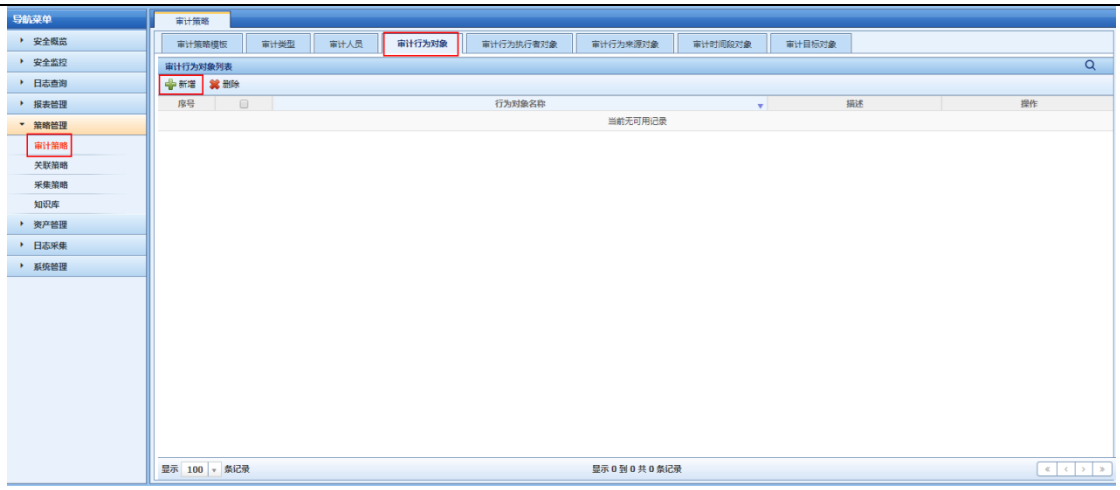
二、功能验证

1、审计人员创建成功，新增和修改审计策略时，选择审计行为执行者，在审计人员列表中能够选择人员。

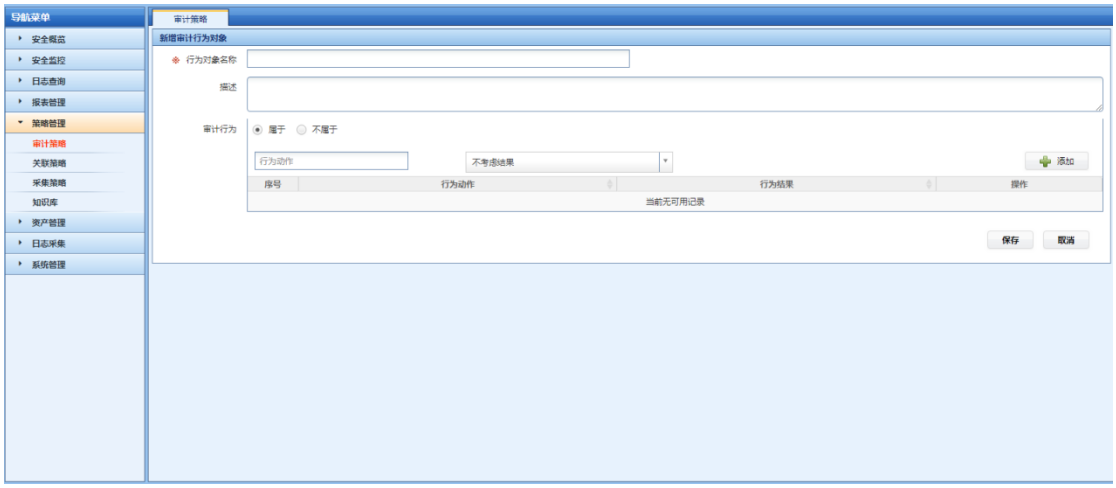
2.4.3.2. 审计行为

一、审计行为配置说明

1、进入审计策略->审计对象->审计行为对象页面：



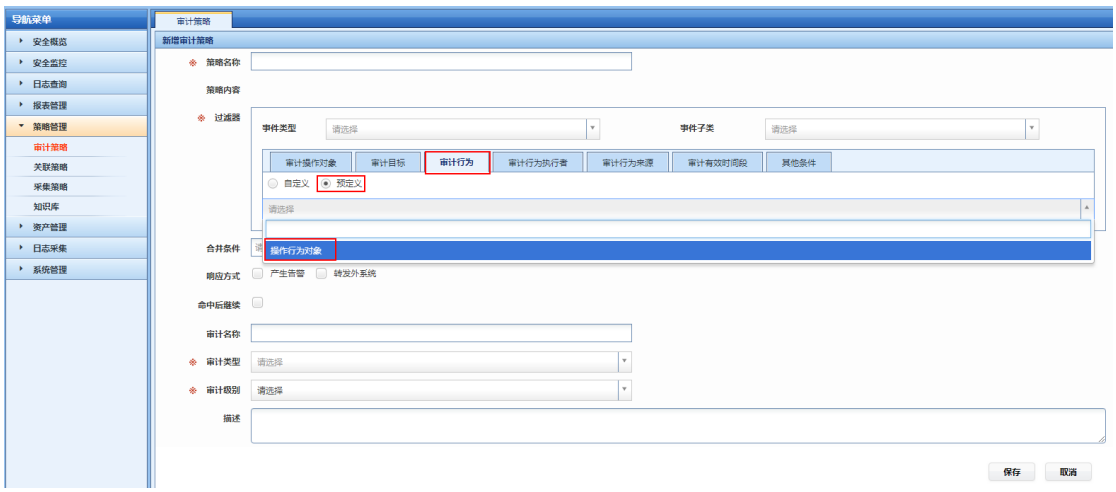
2、点击新增按钮：



3、点击"保存"按钮，保存审计行为对象。

二、功能验证

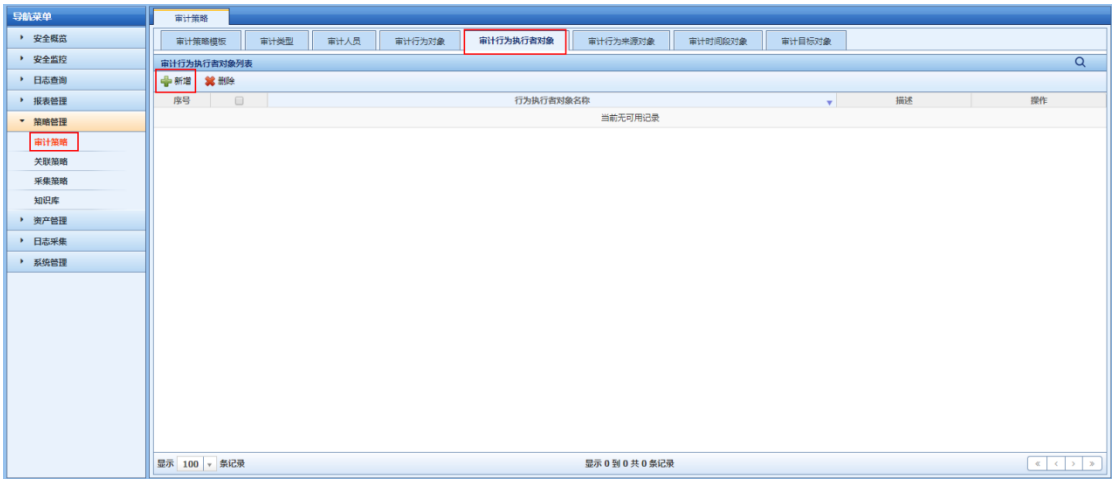
1、审计行为对象创建成功，新增和修改审计策略时，选择审计行为，在审计行为预定义里能够选择此对象：



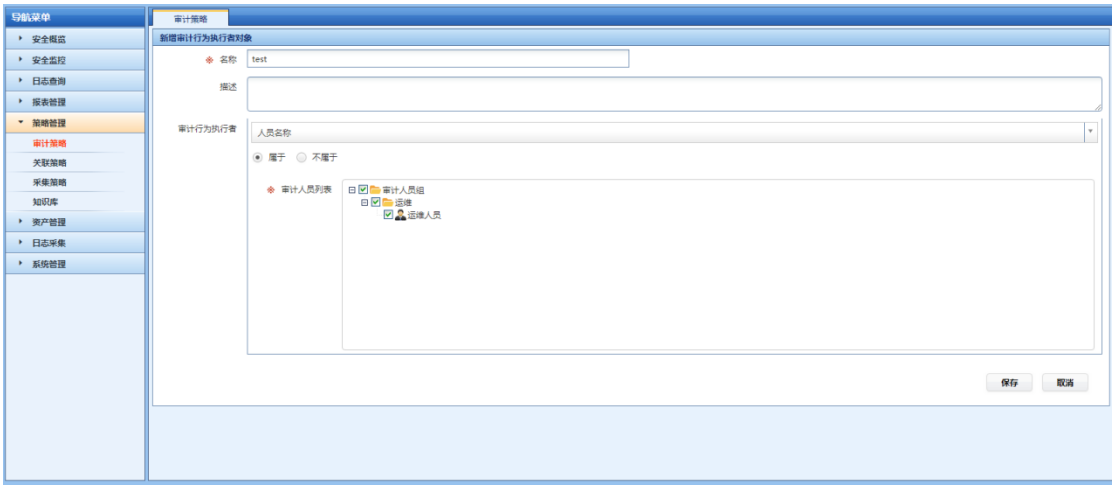
2.4.3.3. 审计行为执行者

一、审计行为执行者配置说明

1、进入审计策略->审计对象->审计行为执行者对象页面 ：



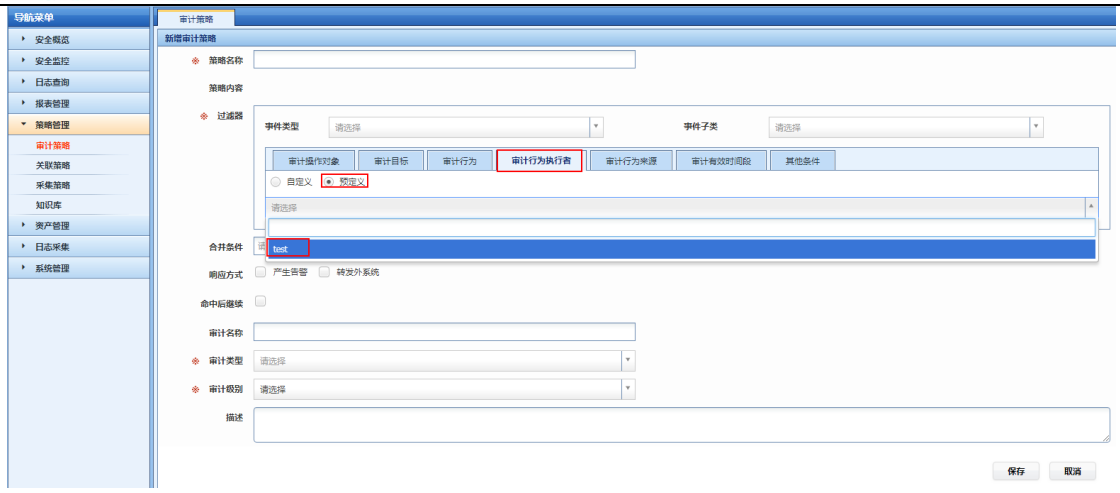
2、点击新增按钮:



3、点击"保存"按钮，保存审计行为执行者对象。

二、功能验证

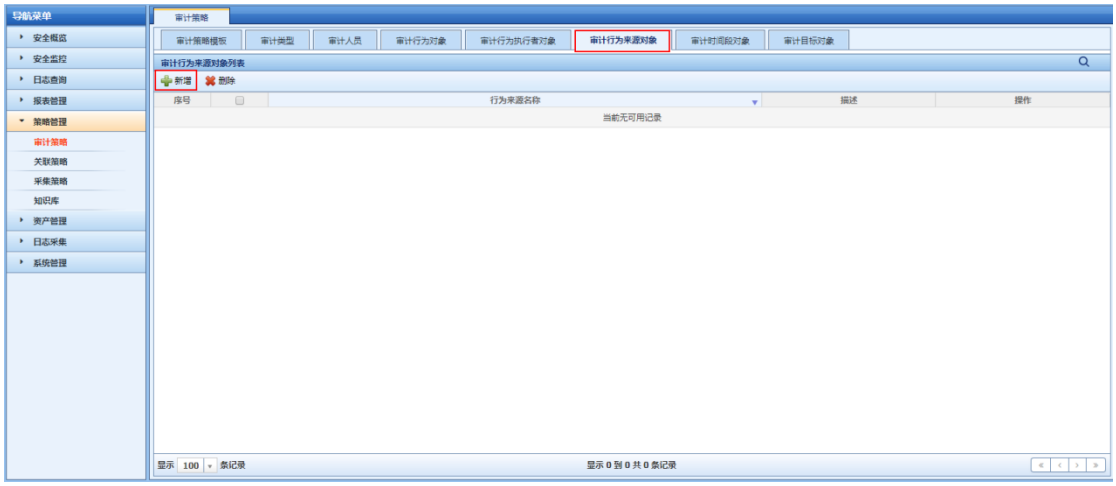
1、审计行为执行者对象创建成功，新增和修改审计策略时，选择审计行为执行者，在审计行为执行者预定义里能够选择此对象。



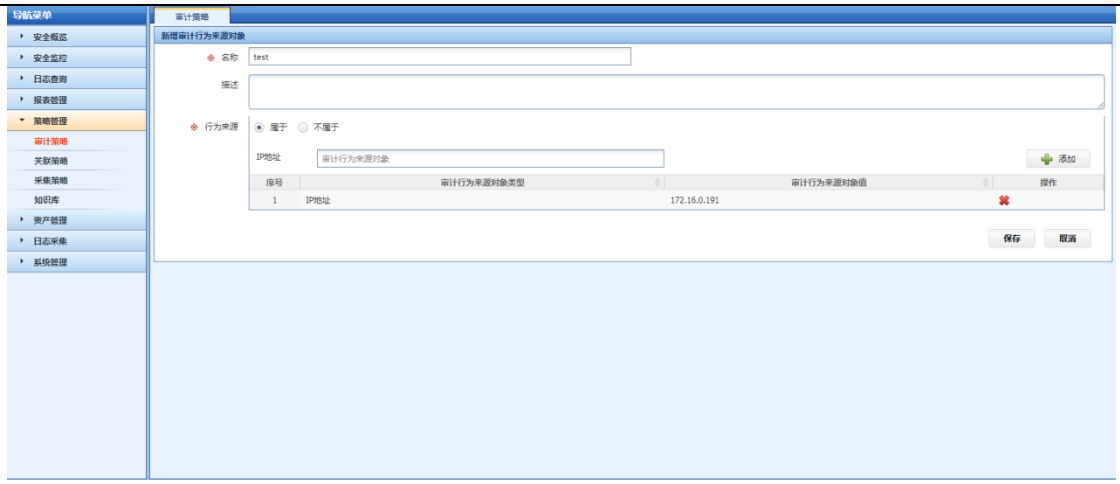
2.4.3.4. 审计行为来源

一、审计行为来源配置说明

1、进入审计策略->审计对象->审计行为来源对象页面:



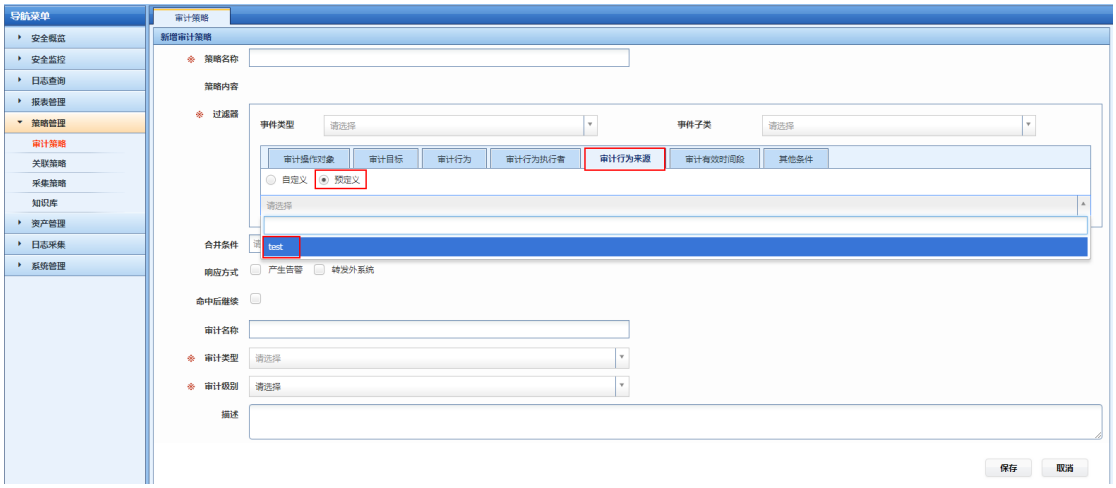
2、点击新增按钮:



3、点击"保存"按钮，保存审计行为来源对象。

二、功能验证

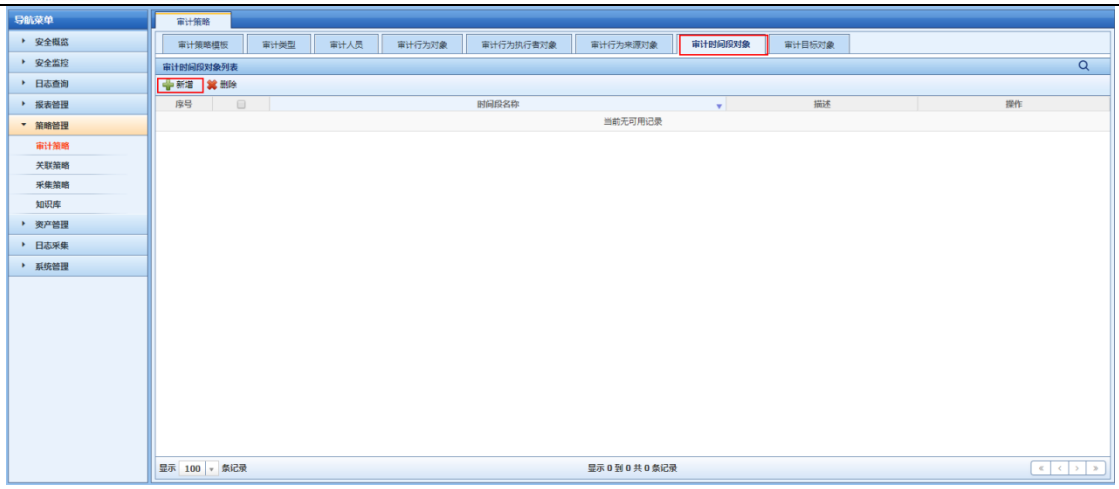
1、审计行为来源对象创建成功，新增和修改审计策略时，选择审计行为来源，在审计行为来源预定义里能够选择此对象：



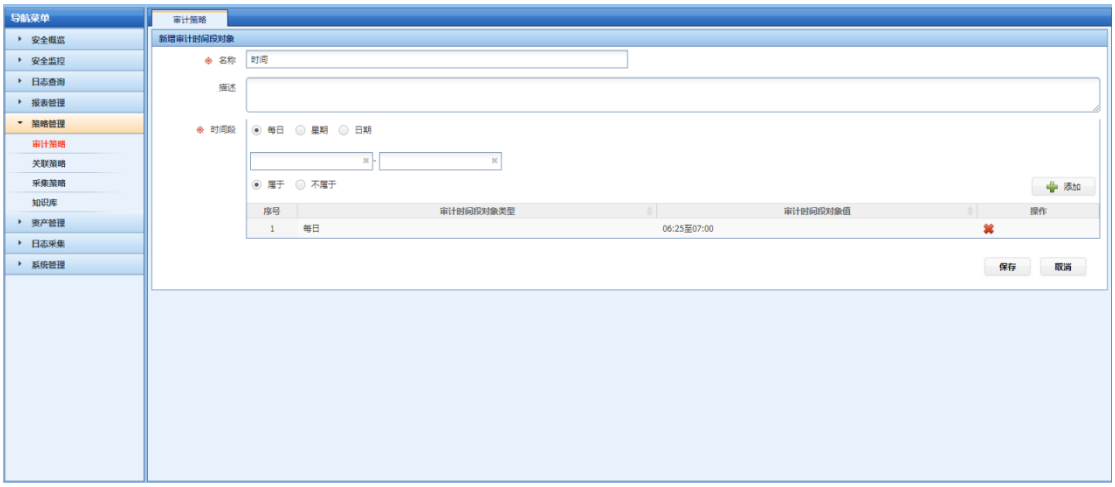
2.4.3.5. 审计时间段

一、审计时间段配置说明

1、进入审计策略->审计对象->审计时间段对象页面：



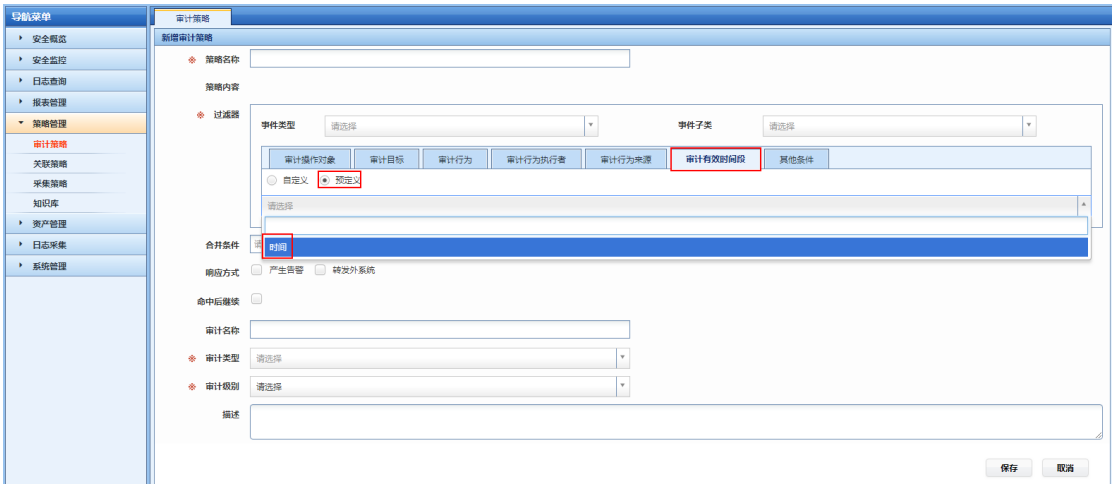
2、点击新增按钮：



3、点击"保存"按钮，保存审计行为来源对象。

二、功能验证

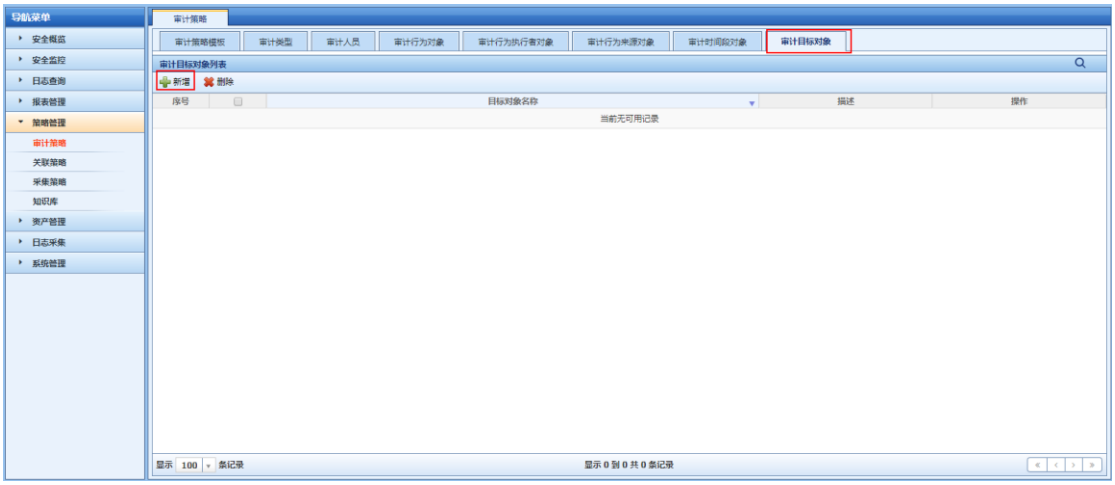
1、审计时间段创建成功，新增和修改审计策略时，选择审计时间段，在审计时间段预定义里能够选择此对象：



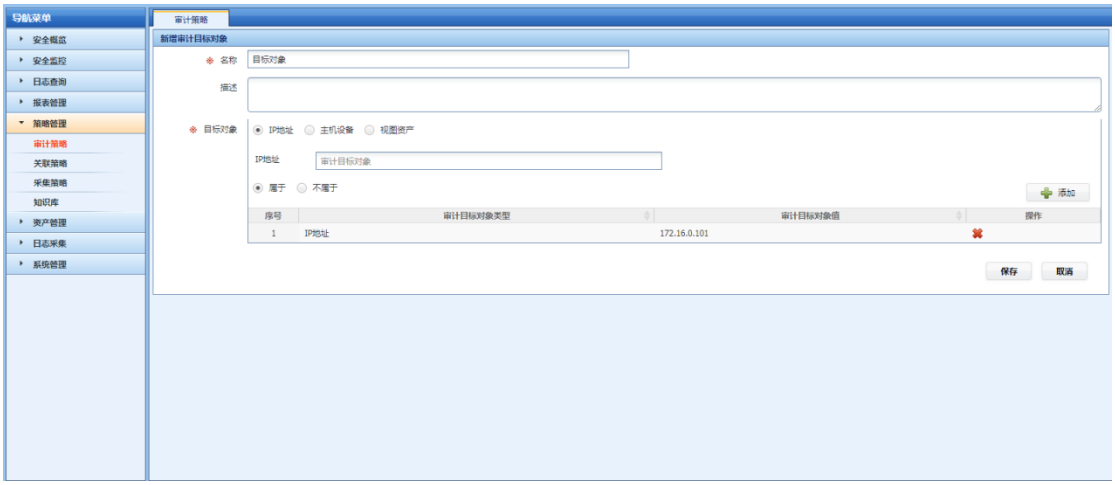
2.4.3.6. 审计目标

一、审计目标配置说明

1、进入审计策略->审计对象->审计目标对象页面:

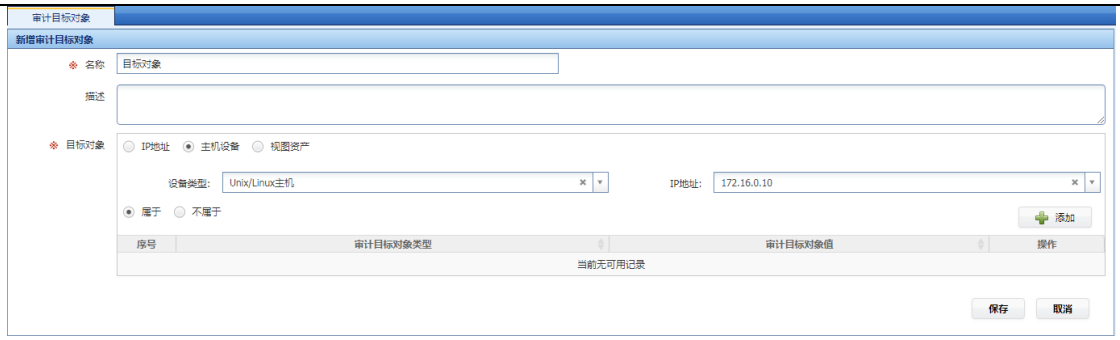


2、点击新增按钮:

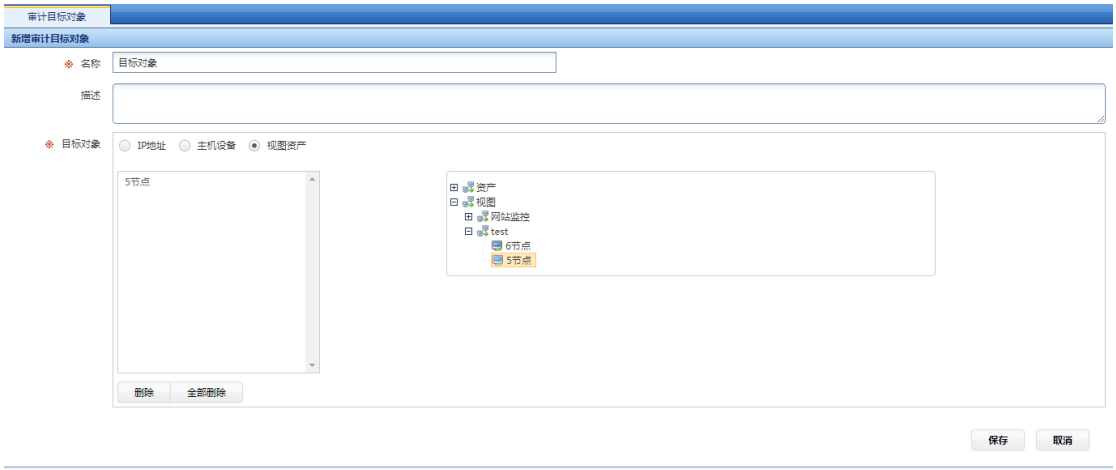


IP 地址：直接输入 IP 地址;

主机设备：选择系统内资产。



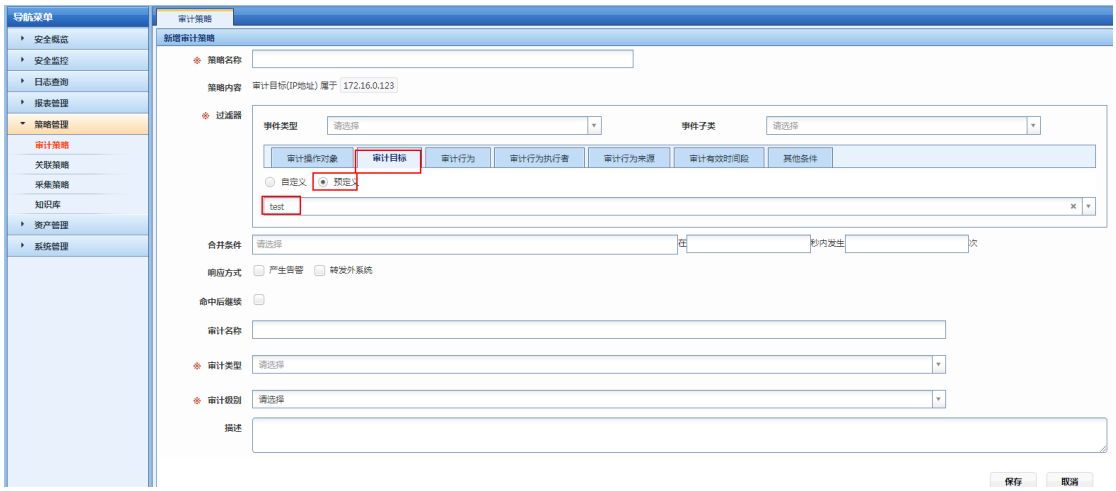
视图资产：选择系统内视图。



3、点击"保存"按钮，保存审计目标对象。

二、功能验证

1、审计目标对象创建成功，新增和修改审计策略时，选择审计目标，在审计目标段预定义里能够选择此对象：



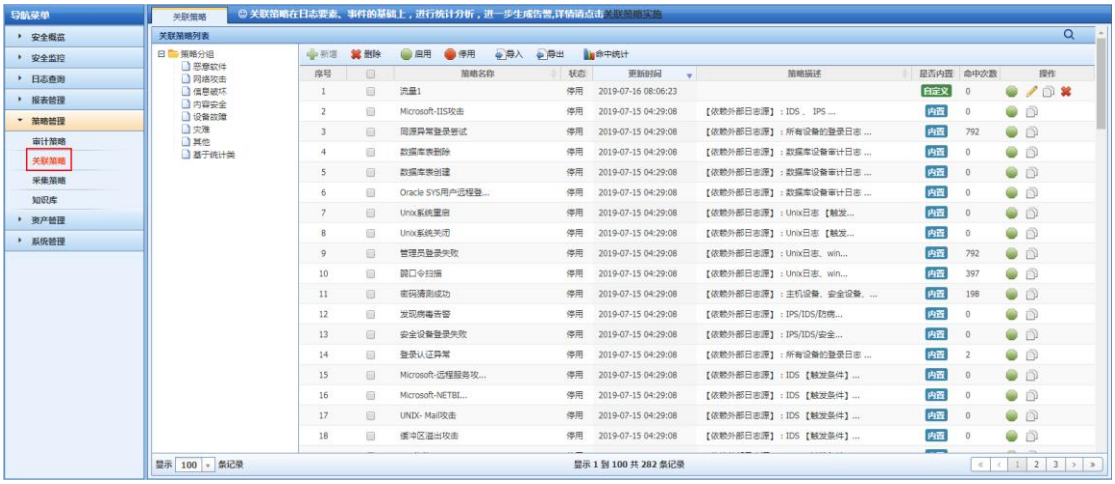
2.5. 告警监控

功能介绍

对于您关心的事件，可以在配置审计策略或关联策略时选中产生告警，使其在产生事件的同时生成告警，进入策略配置页面，设置相关的条件：

具体配置

（1）进入 LAS 系统->策略管理->关联策略:



（2）点击新增

（3）进入“安全监控->〉告警监控”，可以查看产生的告警：

（4）点击告警名称，可以查看告警基本信息及历次发生情况：

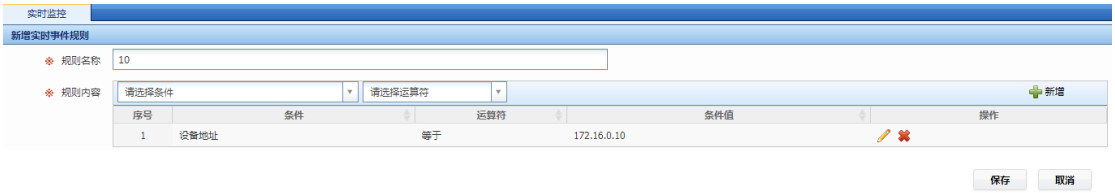
2.6. 实时监控

功能介绍

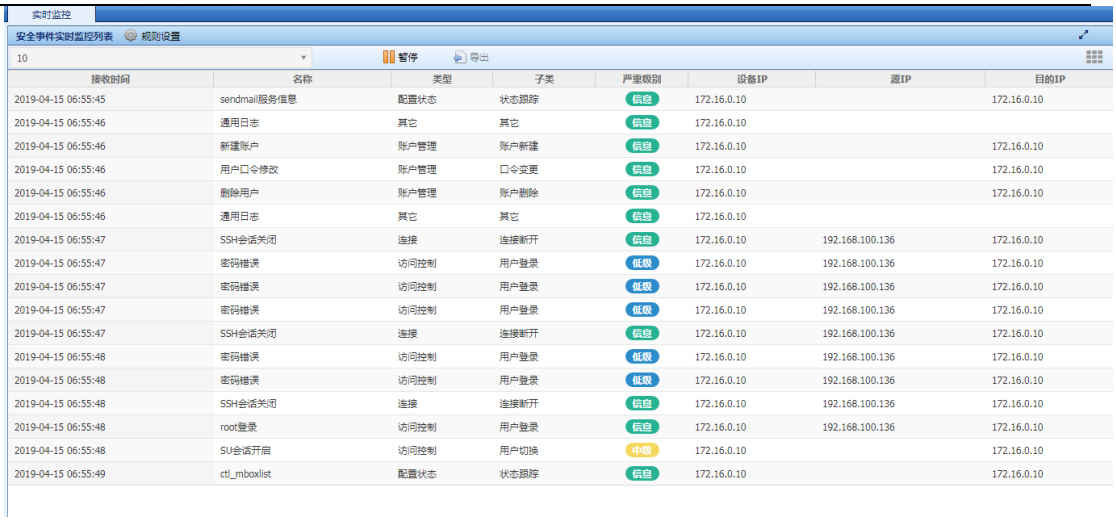
如果您想进行实时监控，可以使用监控规则将原始事件筛选出来，使其生成实时事件，进入“安全监控->实时监控->规则设置”，设置相关的条件：

具体配置

（1）如果您想进行实时监控，可以使用监控规则将原始事件筛选出来，使其生成实时事件，进入“安全监控->实时监控->规则设置”，设置相关的条件：



（2）进入“安全监控->实时监控”，选择监控规则，点击开始按钮，可以查看产生的实时事件：



2.7. 报表管理

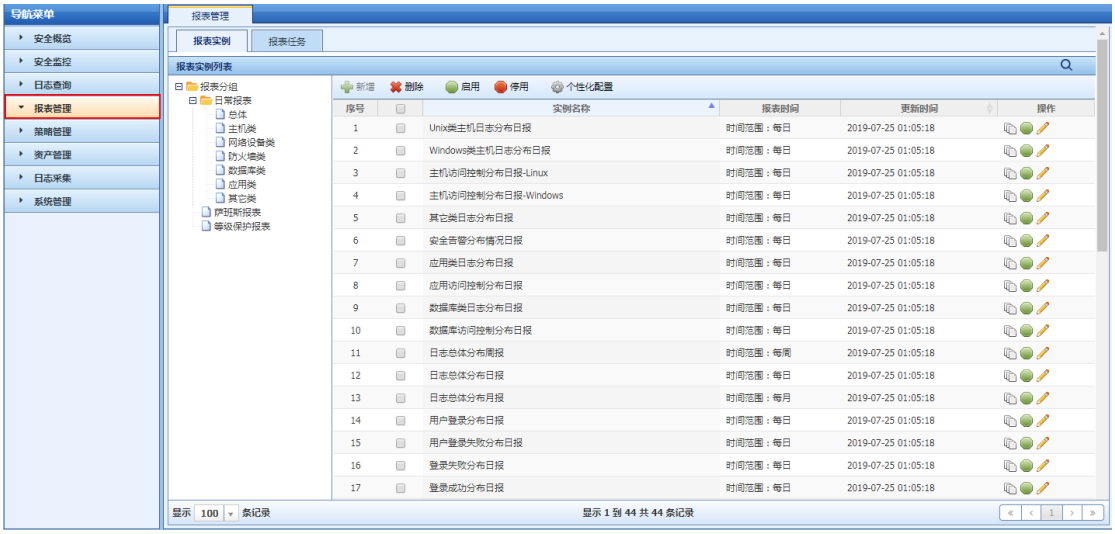
功能介绍

您可以从模板中选取需要生成报表，并且可以实时查看或定义任务生成报表。开启报表实例后，可根据报表时间统计报表，于每日凌晨 2 点统计前一天的报表数据，报表实例可根据用户需要自行新增。

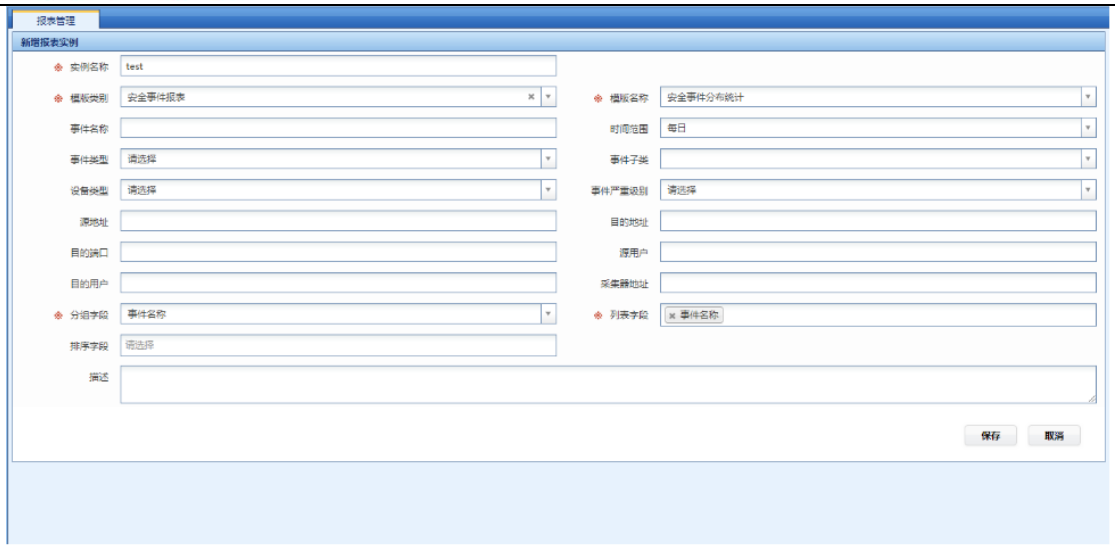
2.7.1. 报表实例

具体配置

（1） 点击报表管理->报表实例



（2） 点击新增



（3） 查看报表实例详情

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	计划任务执行	其它	信息	172.16.0.173	242
2	计划任务执行	其它	信息	172.16.0.221	242
3	postfix服务信息	配置状态	信息	172.16.0.173	120
4	postfix服务信息	配置状态	信息	172.16.0.221	120
5	系统计划任务执行	其它	信息	172.16.0.173	60
6	系统计划任务执行	其它	信息	172.16.0.221	60

2.7.2. 报表任务

功能介绍

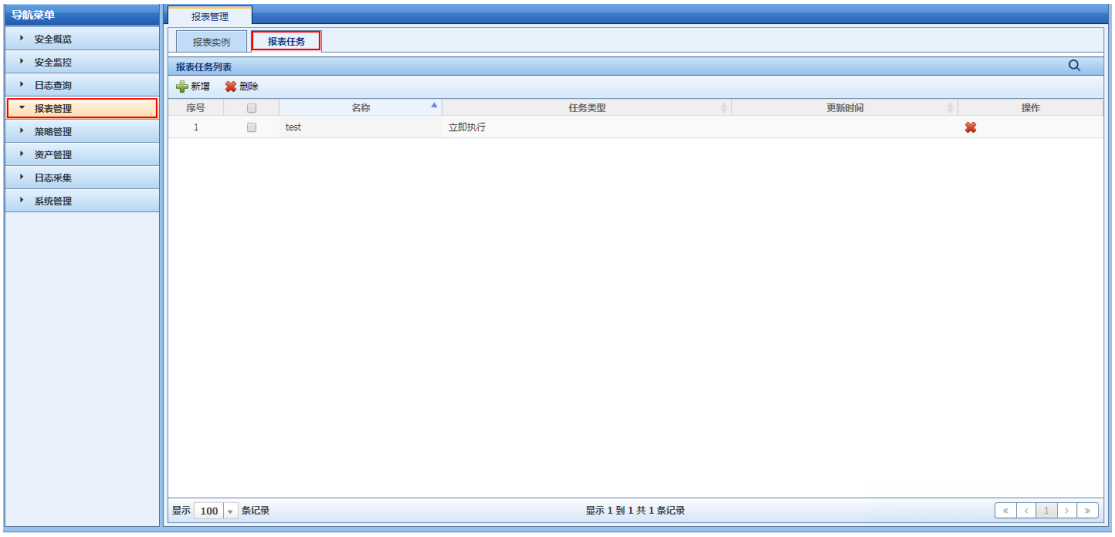
报表实例可根据用户需要自行新增。

报表任务可以设置定时执行报表实例，并将执行结果发送给配置的收件人（需在系统参

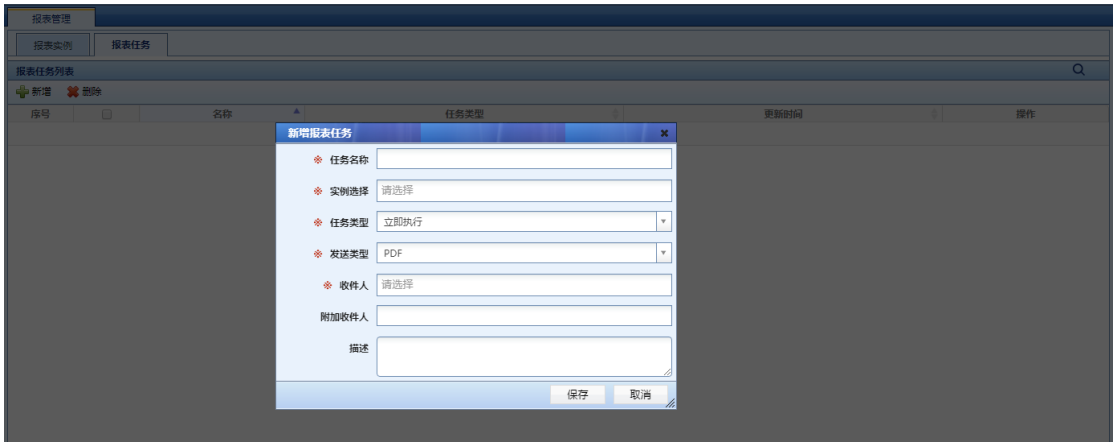
数中配置邮箱信息）。

具体配置

（1） 点击报表管理->报表任务



（2） 点击新增



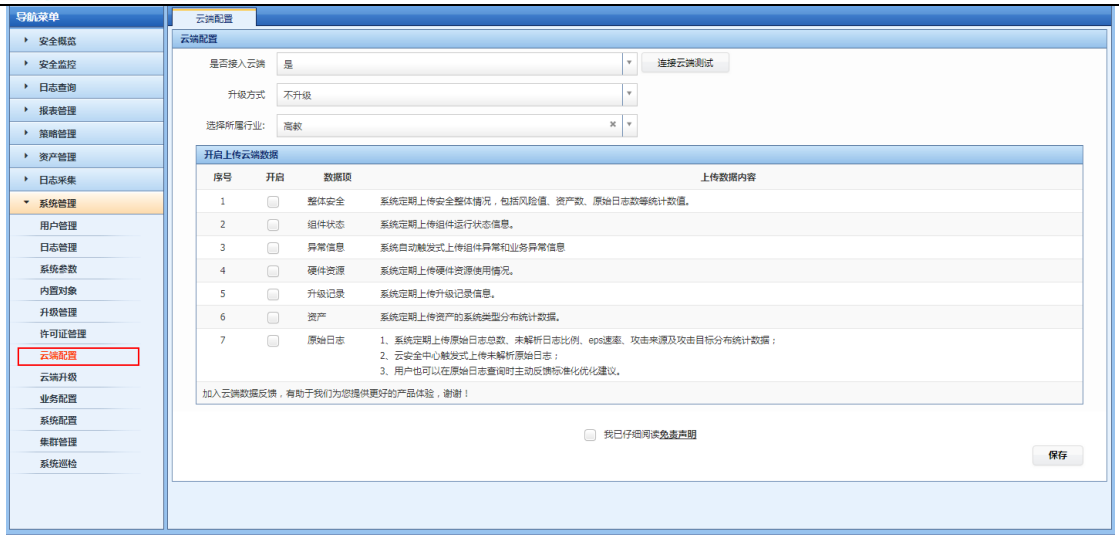
2.8. 云端配置

功能介绍

客户端在连接到云端后，会接收来自云端发布的威胁情报，安全资讯和云端升级等信息。

具体配置

1.用户在“是否接入云端”下拉选项选择“是”，并连接云端测试成功后，再去选择升级方式，是否自动执行重大事件任务，所属行业，云端上传数据等选项勾选“我已仔细阅读免责声明”后点击保存按钮完成云端配置，如下图所示：



2.9. 拓扑图配置（选配）

LAS 拓扑图配置步骤简介

1、资产管理:

在 LAS 系统上首先需要将设备加入资产列表，资产是创建拓扑图的数据来源，配置步骤参见 2.1.资产管理配置。

2、拓扑配置:

创建资产间的网络关系，网元从资产清单里选择，通过连线的方式，将系统内各个资产串联起来。

包括拓扑图的新增、修改、删除、隐藏等。

3、拓扑查看 ：

选择需要展示的拓扑图进行展示。

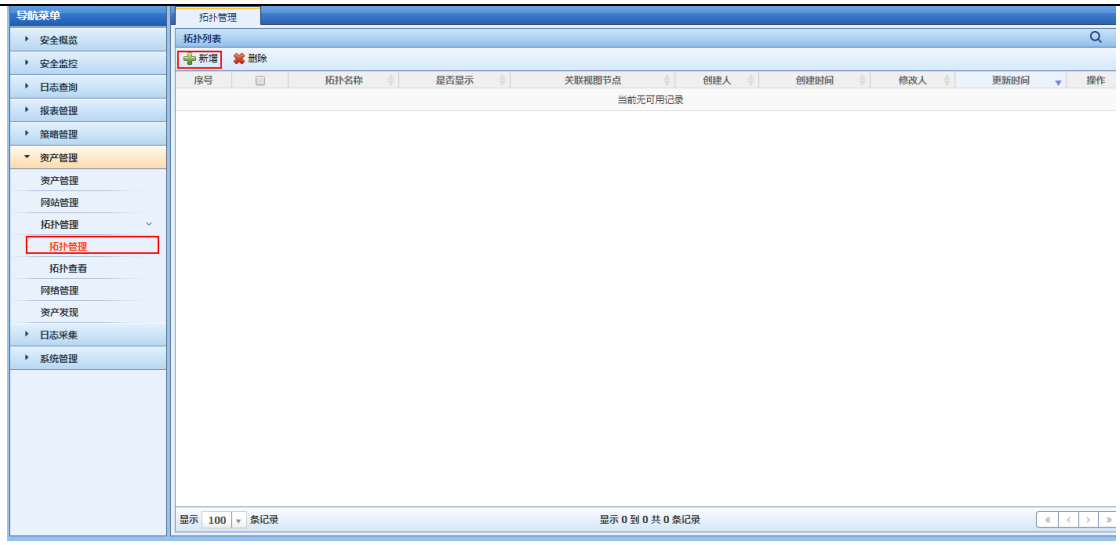
2.9.1. 具体配置

一、创建拓扑

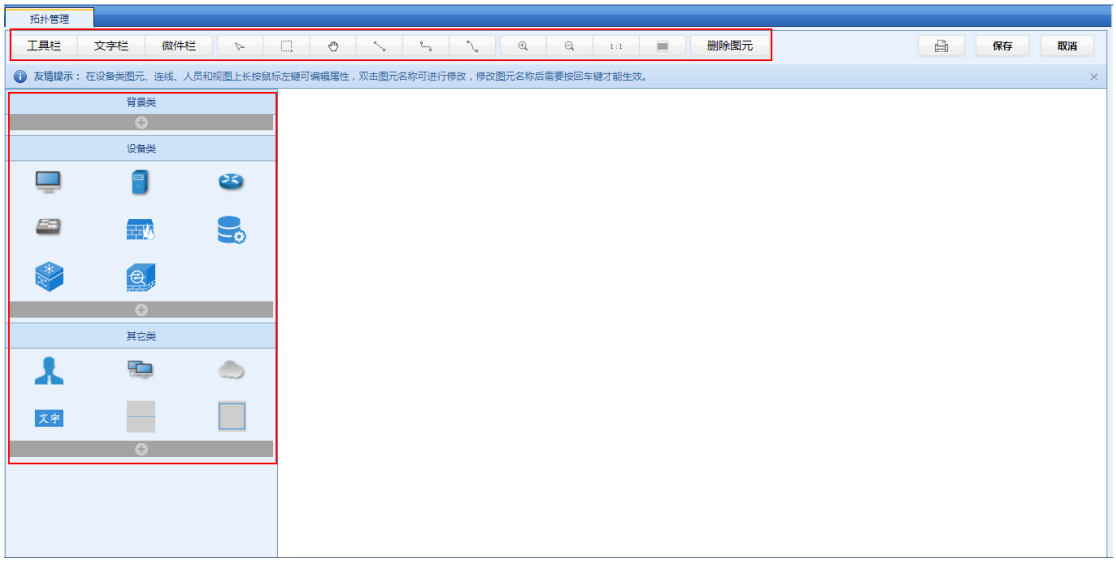
场景：将资产管理里的 1 台防火墙、1 台路由器、1 台 Linux、1 台 Tomcat 用拓扑图展示出来。

二、具体配置

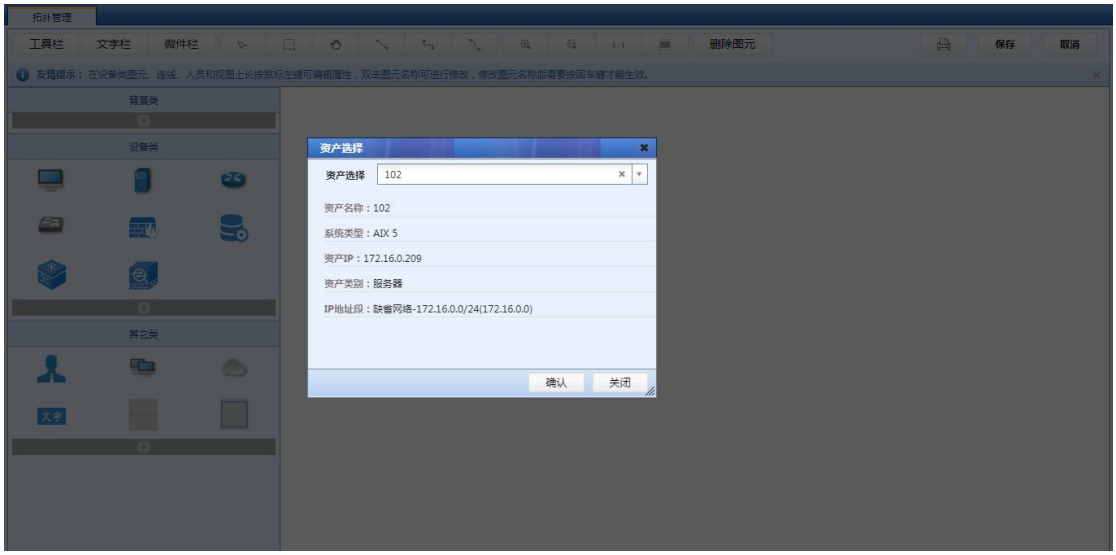
（1）进入 LAS 系统->资产管理->拓扑管理->拓扑管理:

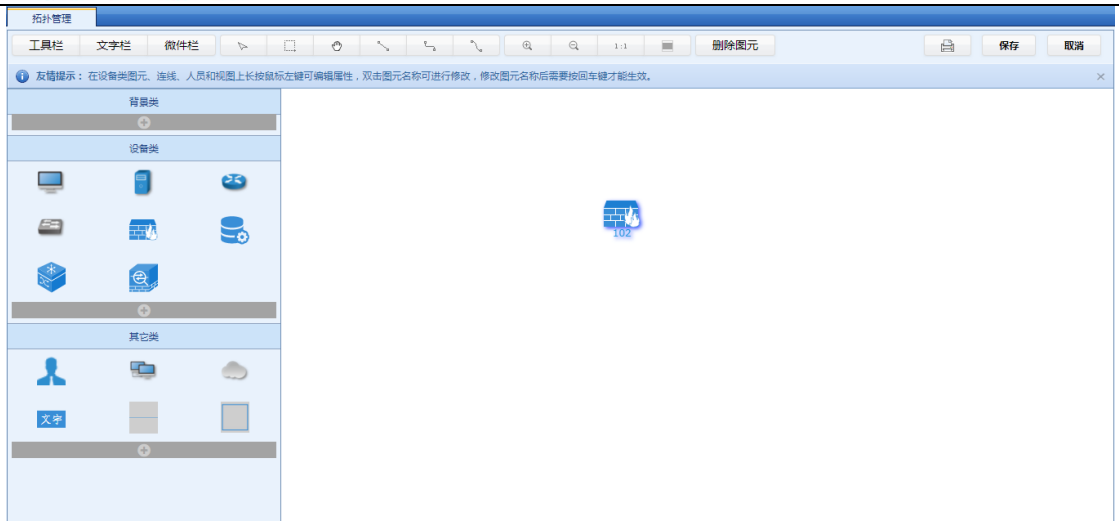


（2）点击“新增”按钮，进入拓扑图编辑页面：

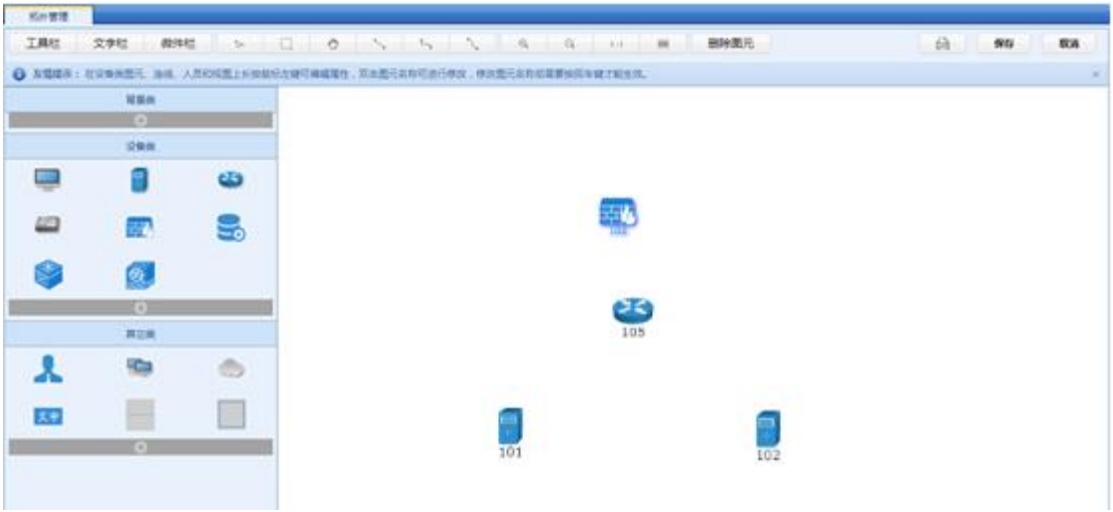


（3）从左边图元里拖拽一个防火墙进入右边空白区域：

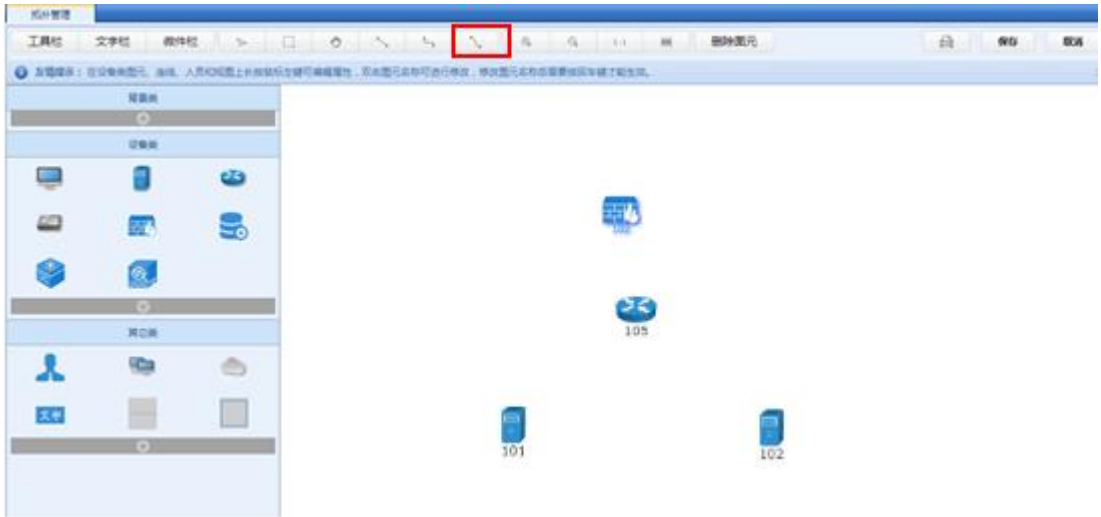


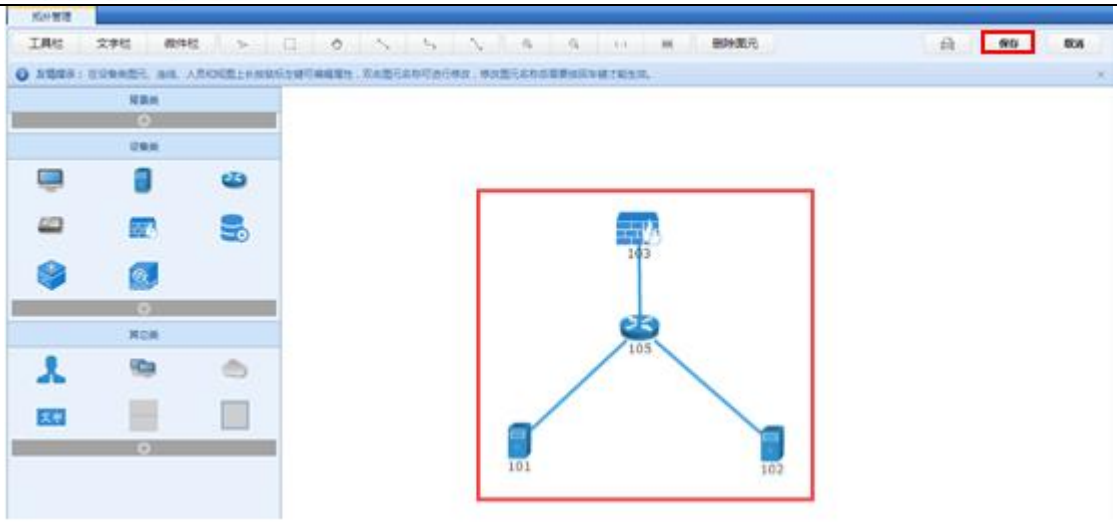


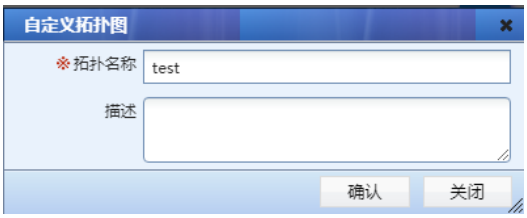
（4）重复以上的方法，将 Linux 服务器、Tomcat、路由器创建出来：

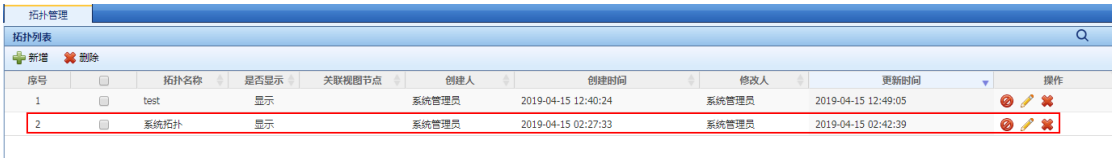


（5）创建个设备间的关系：



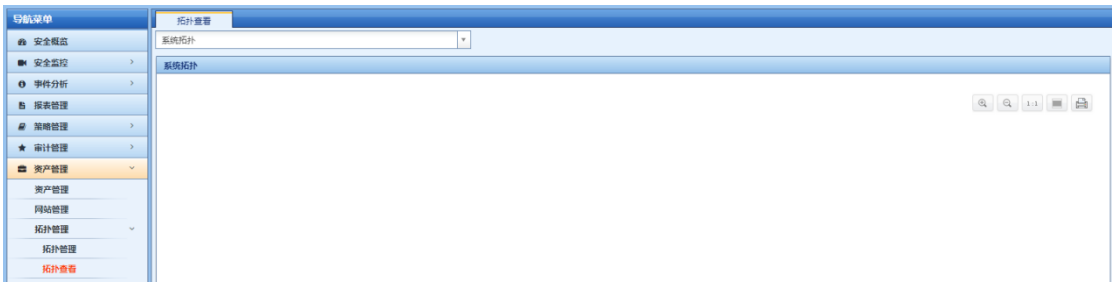


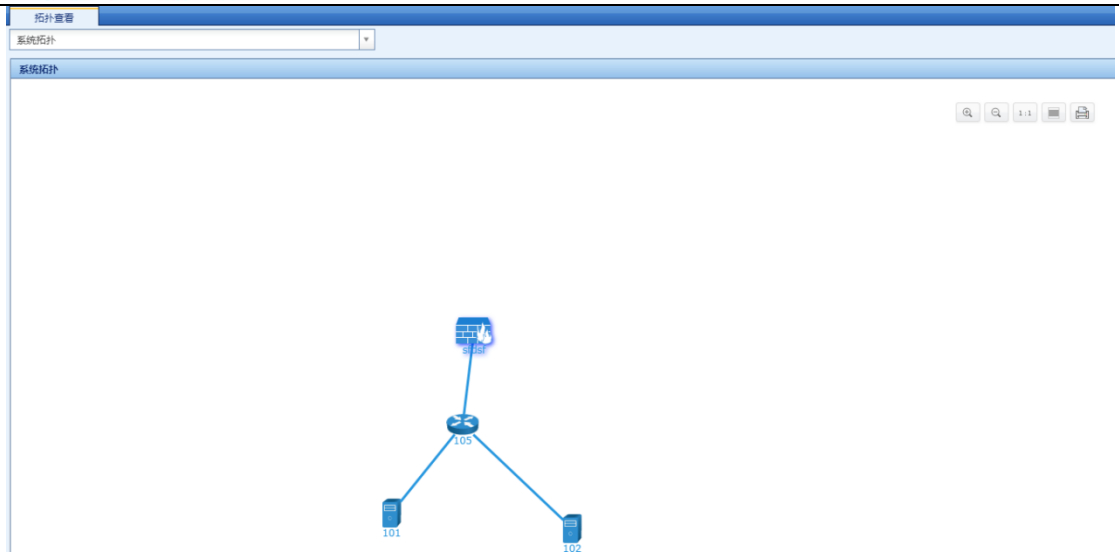




（6）拓扑查看：

点击资产管理->拓扑查看->拓扑管理，选择创建的“系统拓扑”：



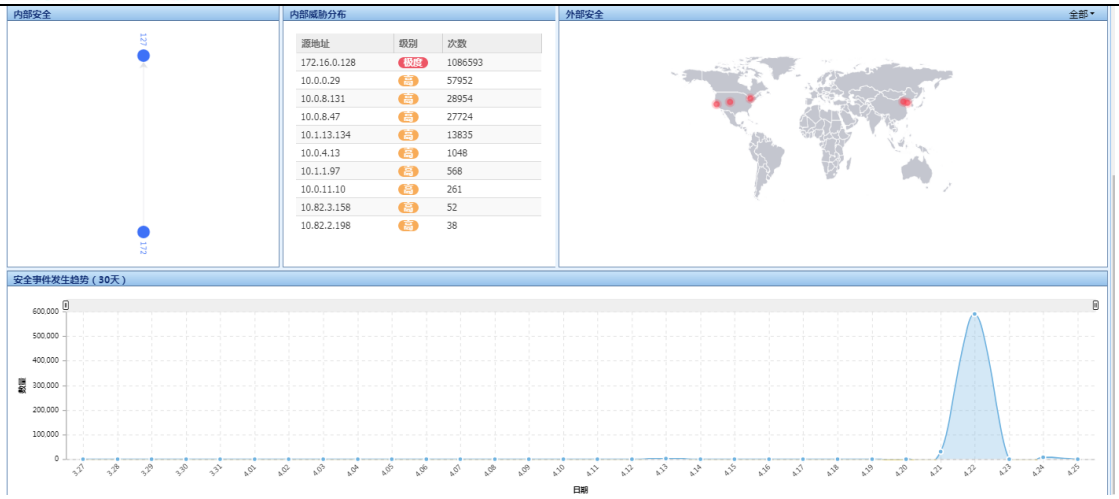


3 事件查看

3.1. 安全仪表盘查看

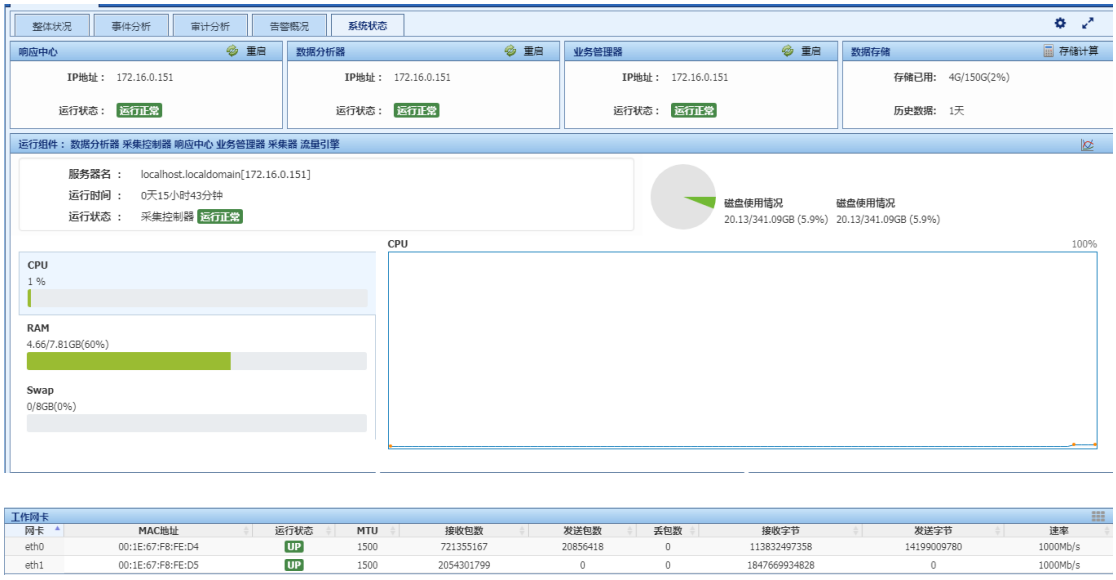
一、安全事件仪表板查看

仪表板默认包含：整体状况、事件分析、审计分析、告警概况、系统状态 5 个部分内容，也可自定义添加需要关注内容。

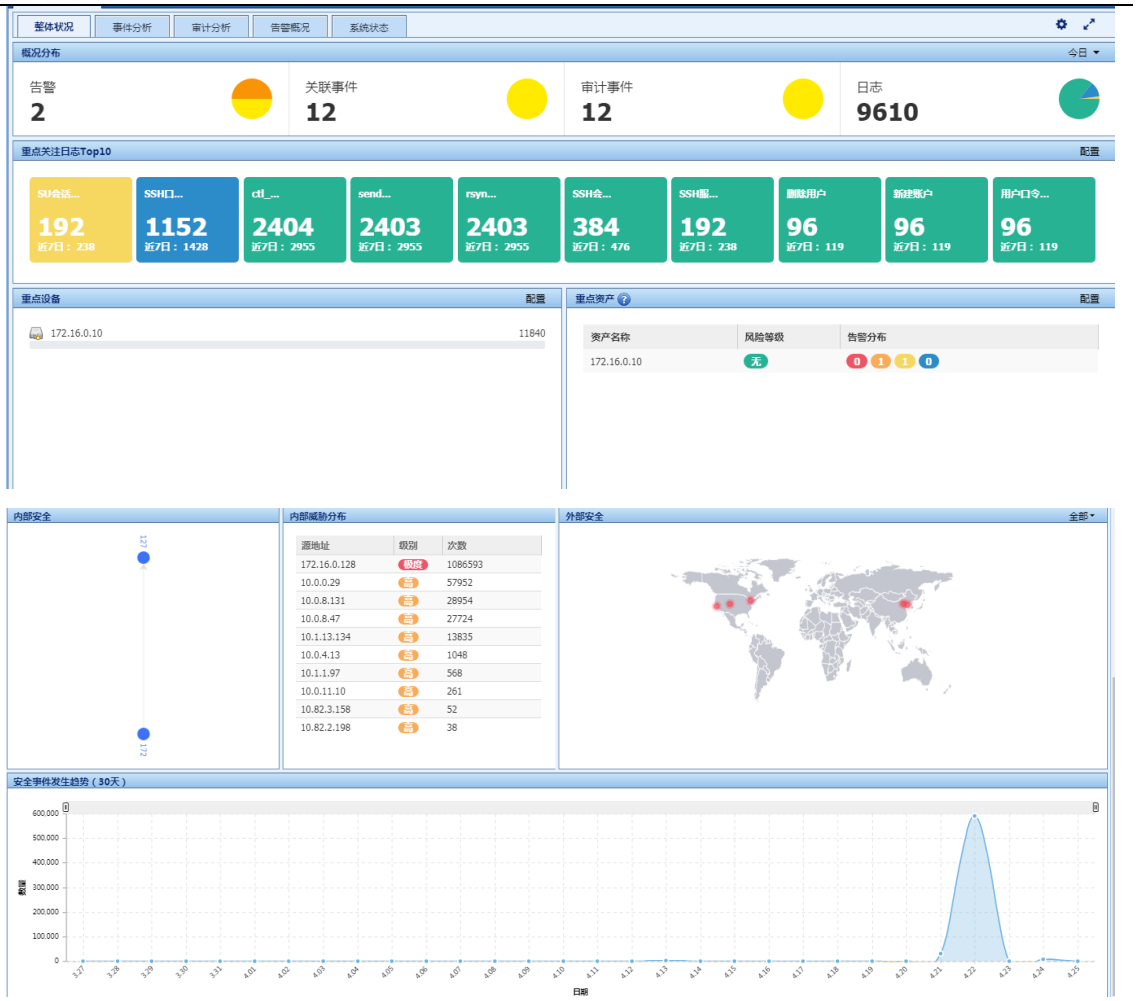


1、系统状态 ：

- 仪表板默认显示系统状态，该模块可以查看；
- 设备基本信息：设备型号、版本号、软件序列号；
- 当前关键组建的运行状态：业务管理器、响应中心、数据分析器使用情况；
- 系统资源占用情况：CPU、内存以及硬盘使用情况：系统运行时间。



2、整体安全概况 ：



点击各个模块，可以显示更详细的日志信息 。

3、日志查询 ：

- 事件类型 TOP5：柱状图显示今日整网安全日志类型数量，例如接收到的连接、配置状态、网络攻击类日志数量；

- 事件种类 TOP5：柱状图显示今日整网安全日志种类（类型里的细分项）数量，例如接收到的连接接受、连接拒绝、系统内核信息日志数量；

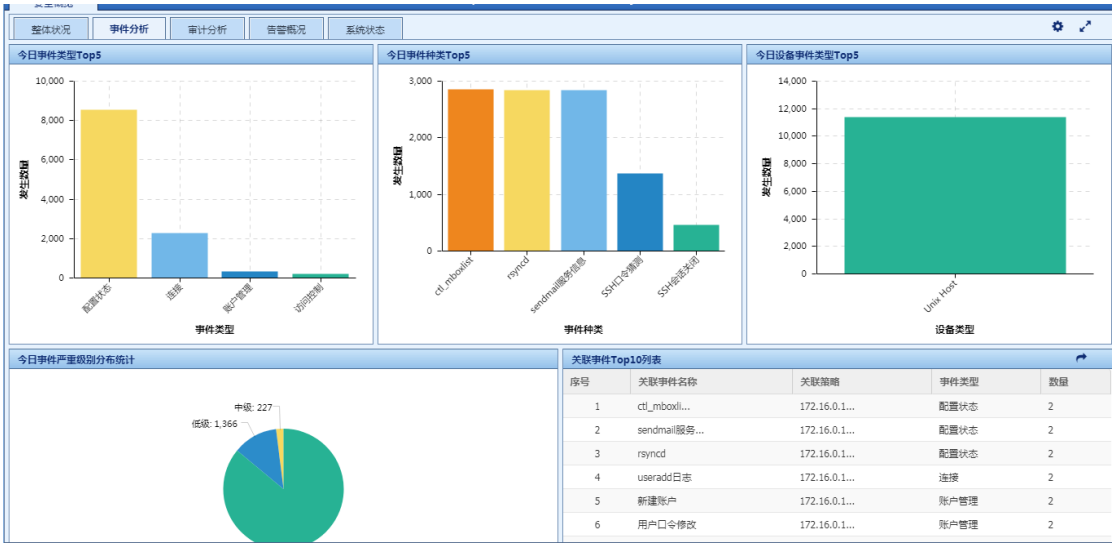
- 今日设备事件类型 TOP5：柱状图显示今日各设备类型产生的安全日志数量，例如防火墙设备、网络设备、主机设备产生的日志数量；

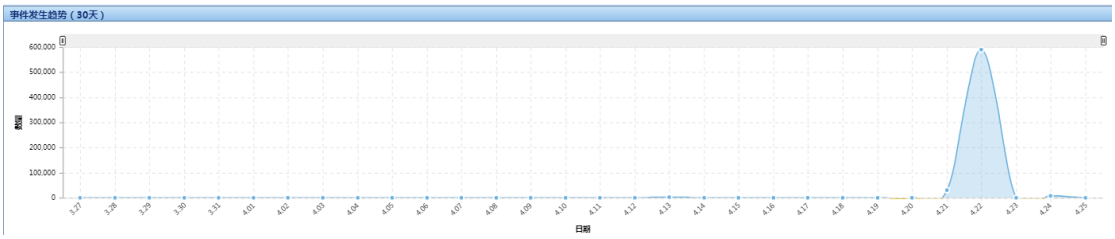
- 今日事件严重级别分布统计：饼图显示今日安全日志的等级分布，如信息、低级、中级等；

- 关联事件 Top10 列表：按关联事件名称显示关联事件列表，包含关联策略和事件数量；

- 事件发生趋势（30 天）：以日期和数量作为横纵轴，显示近 30 天每天接收到的安全日志趋势；

- 点击各个模块，可以显示更详细信息。





4、审计分析 ：

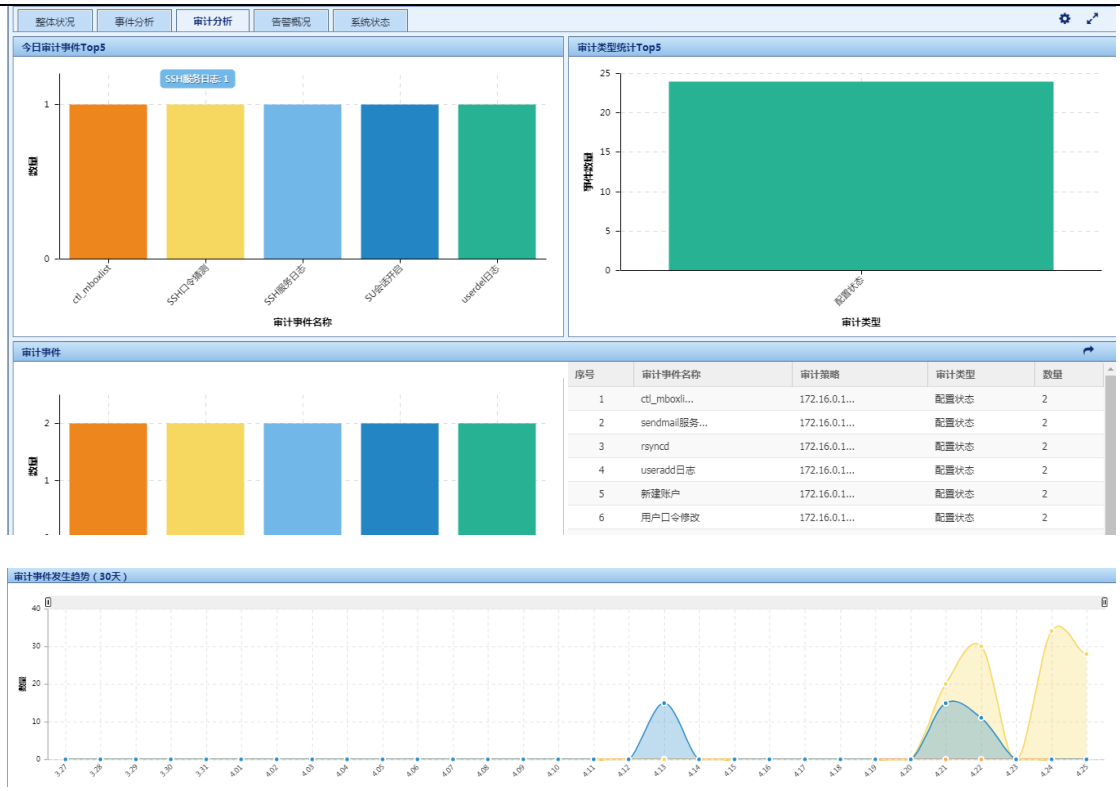
- 今日审计事件 TOP5：柱状图显示今日整网审计事件数量，例如登录日志、行为审计等日志数量；

- 审计类型统计 Top5：柱状图显示今日整网审计事件类型数量，例如接访问控制审计、网络攻击审计、账户管理审计的数量；

- 审计事件：按审计事件名称分类显示审计事件列表，包含审计策略、审计类型和事件数量；

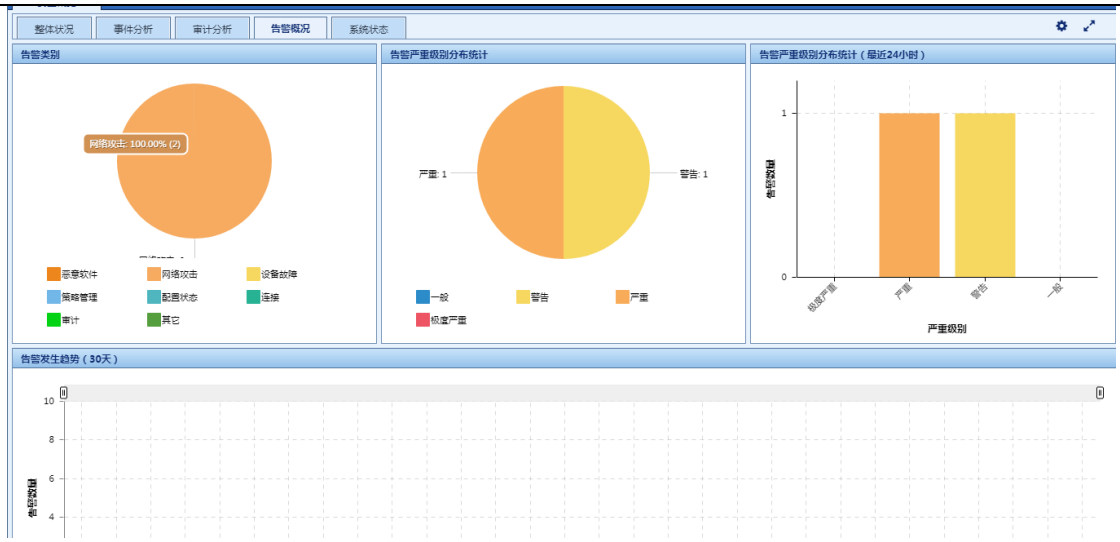
- 审计事件发生趋势（30 天）：以日期和数量作为横纵轴，显示 30 天内审计事件数量趋势；

- 点击各个模块，可以显示更详细信息。



5、告警概况 ：

- 告警类别：按照告警内容，饼状图显示当前所有告警信息类型分布情况，例如网络攻击、安全漏洞类型的数量分布；
- 告警严重级别分布统计：按告警严重级别，饼状图显示所有已产生的告警分布,例如严重、警告的告警数量及分布；
- 告警严重级别分布统计（最近 24 小时）：按告警严重级别，柱状图显示近 24 小时产生的告警分布，例如严重、警告的告警数量及分布；
- 最近 30 天安全事件发生趋势：以日期和数量作为横纵轴，显示 30 天内告警数量趋势。

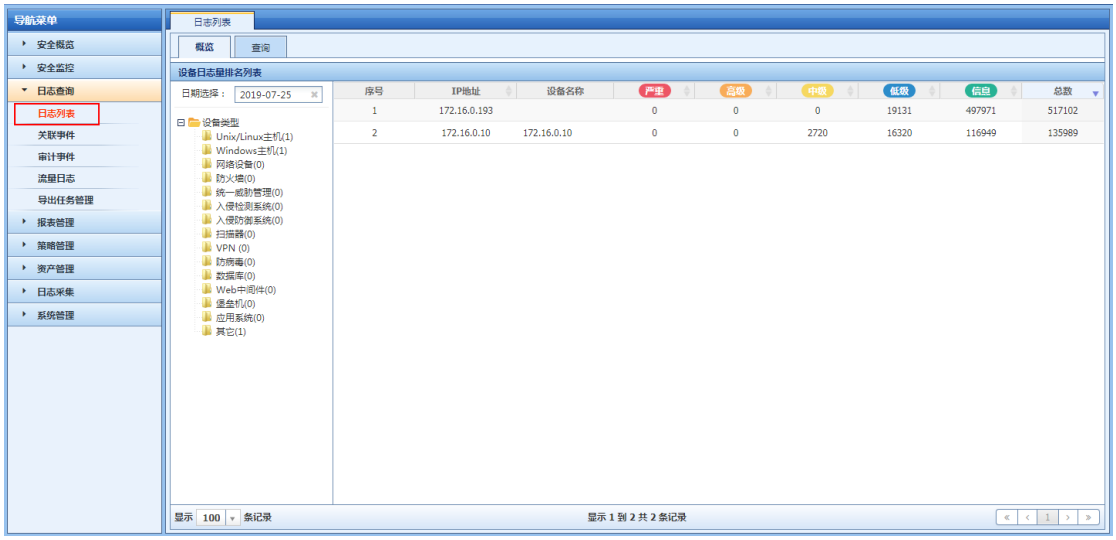


3.2. 日志列表

日志查看

日志查询 -> 日志列表:

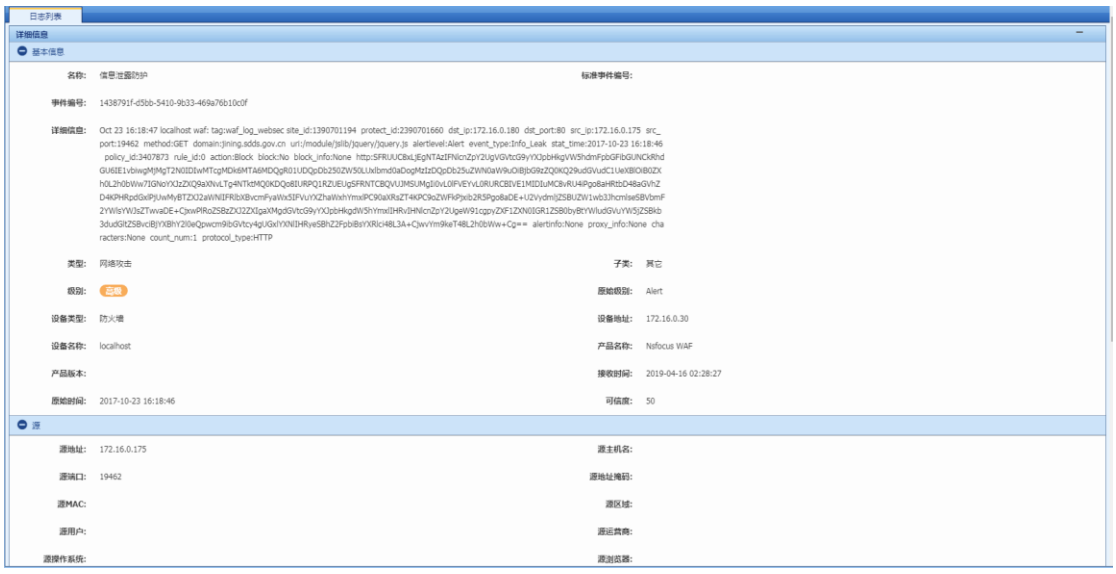
查看所有接收到的日志，可根据设备类型筛选。



点击 IP 地址，即可查看该 IP 地址当天的所有日志，如下:

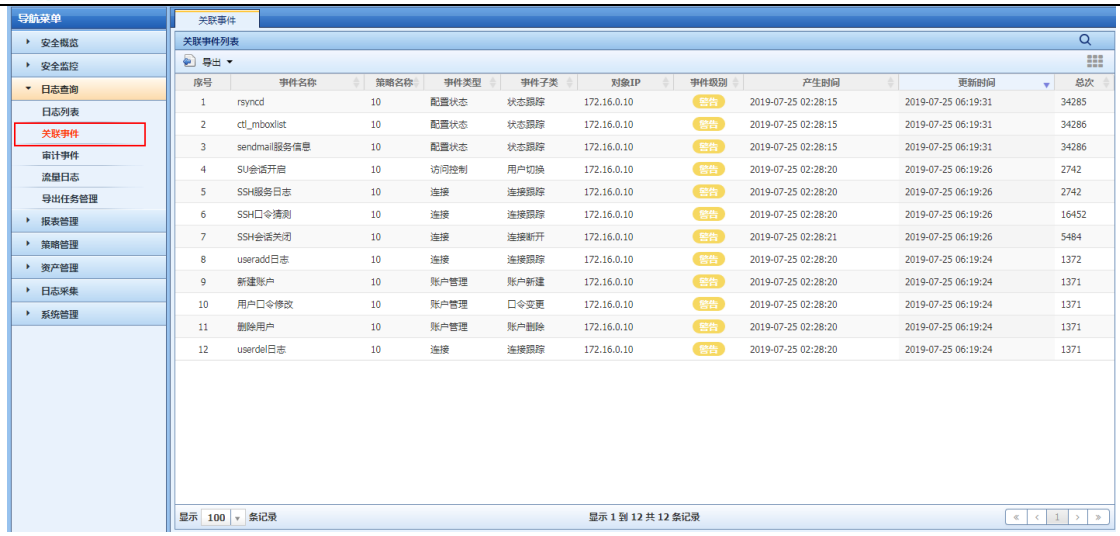
日志列表页面包含两部分，上方为查询部分，可根据日志的字段信息搜索想要关注的日志信息，下方展示搜索结果。

点击事件名称即可进入事件详细信息页面，展示该条日志的详细信息，如下：



3.3. 关联事件（选配）

查看关联策略（2.3 管理策略配置）所触发的事件列表，通过关联策略所触发的事件都会在此列表展示，如下：

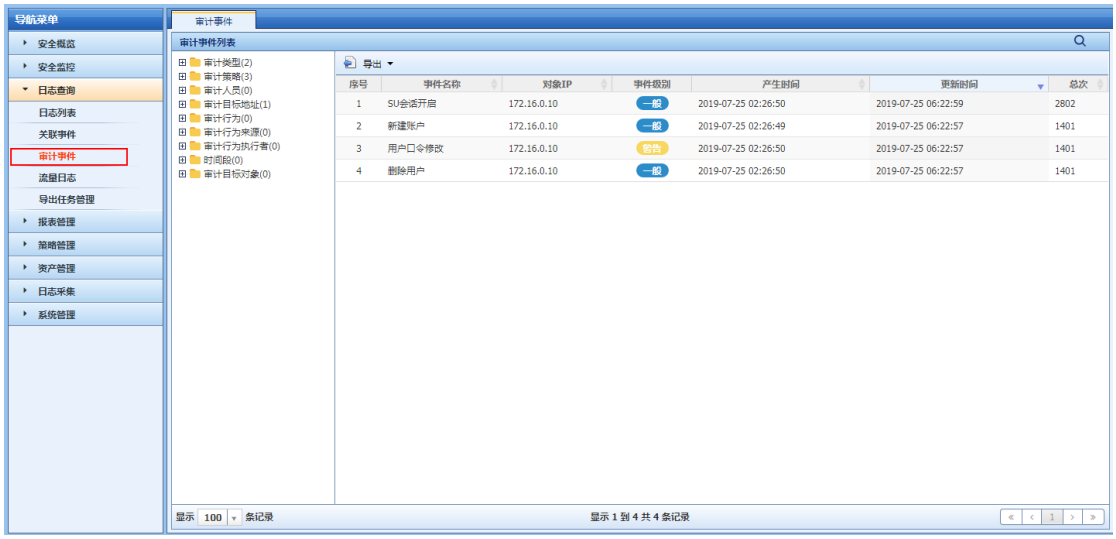


点击事件名称即可进入、该条事件类型的详细页面，如下:

该页面展示触发该事件的策略信息，以及该类型事件的列表，点击名称即可进入详细信息页面，如下：

3.4. 审计事件（选配）

查看审计策略（2. 4 审计策略）所触发的事件列表，通过审计策略所触发的事件都会在此列表展示，如下：



点击事件名称即可进入、该条事件类型的详细页面，如下：

该页面展示触发该事件的策略信息，以及该类型事件的列表，点击名称即可进入详细信息页面，如下：

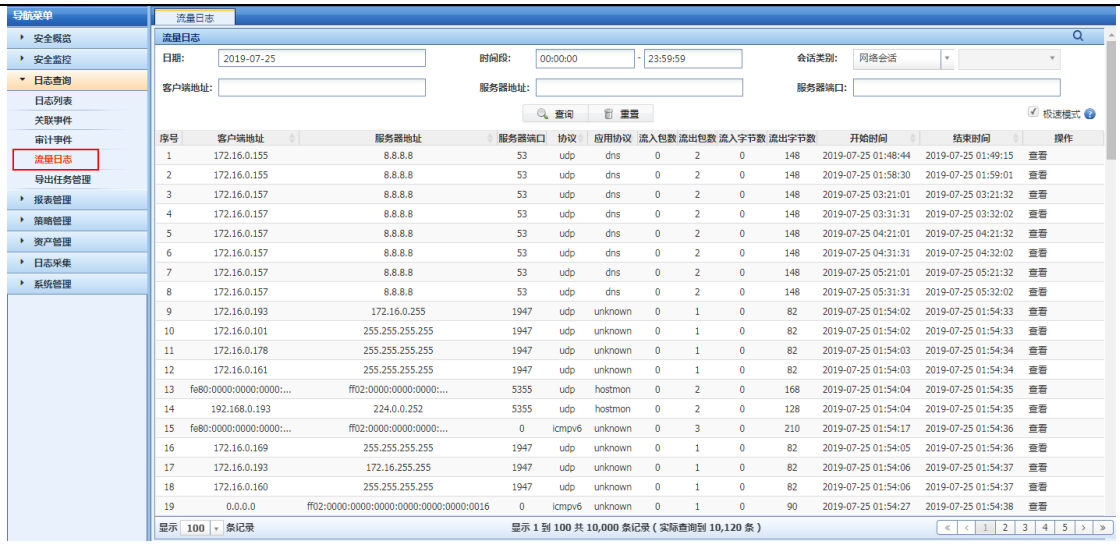
3.5. 流量日志（选配）

一、场景说明

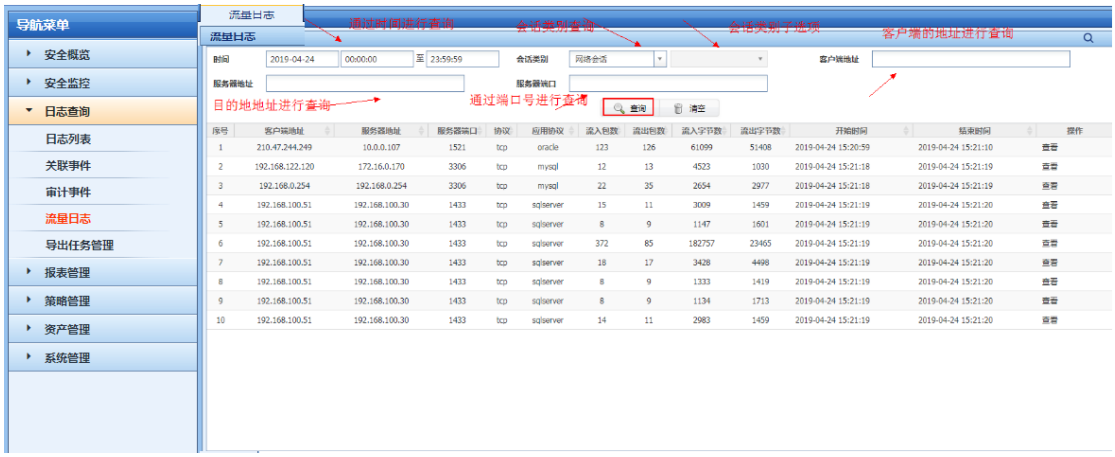
适用于流量接入后，产生会话；通过查询条件可以查看各种类型的会话以及客户端地址、服务器地址、服务端口等详细信息。可支持的类别有数据库会话、流量日志、http 会话、DNS 会话、TLS 会话等。

二、流量日志的查看

1.进入日志查询->流量日志 ：



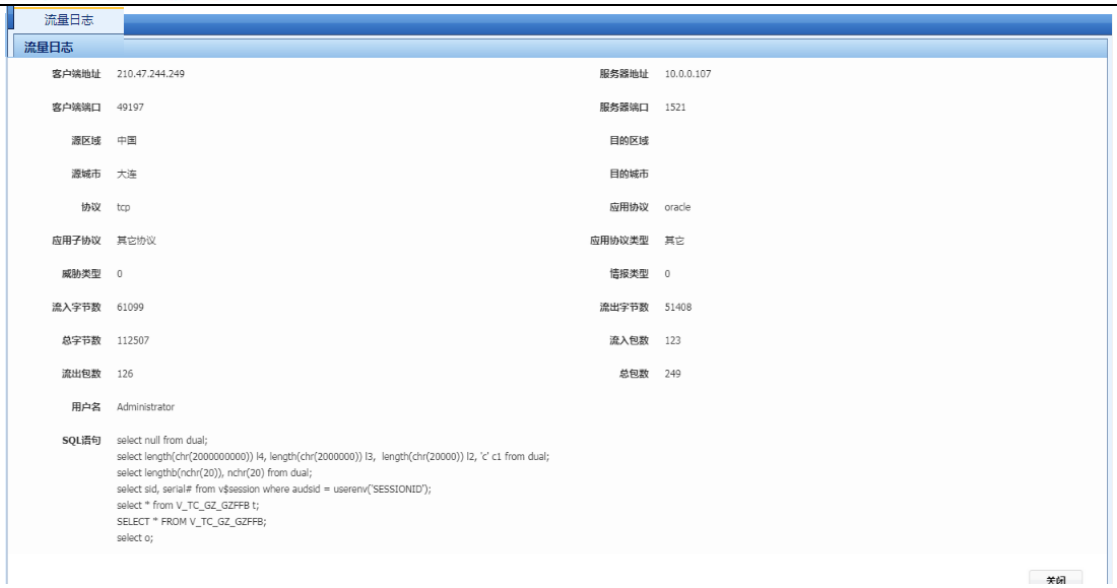
2. 通过条件对已有的流量日志进行列表查询：



3. 点击列表中会话查看会话详情：

序号	客户端地址	服务器地址	服务器端口	协议	应用协议	流入包数	流出包数	流入字节数	流出字节数	开始时间	结束时间	操作
1	210.47.244.249	10.0.0.107	1521	tcp	oracle	123	126	61099	51408	2019-04-24 15:20:59	2019-04-24 15:21:10	查看
2	192.168.122.120	172.16.0.170	3306	tcp	mysql	12	13	4523	1030	2019-04-24 15:21:18	2019-04-24 15:21:19	查看
3	192.168.0.254	192.168.0.254	3306	tcp	mysql	22	35	2654	2977	2019-04-24 15:21:18	2019-04-24 15:21:19	查看
4	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	15	11	3009	1459	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
5	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1147	1601	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
6	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	372	85	182757	23465	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
7	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	18	17	3428	4498	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
8	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1333	1419	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
9	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1134	1713	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
10	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	14	11	2983	1459	2019-04-24 15:21:19	2019-04-24 15:21:20	查看

4.会话详情查看（应用协议、协议、应用子协议、源区域、应用协议类型、流入流出、总字节数等）:

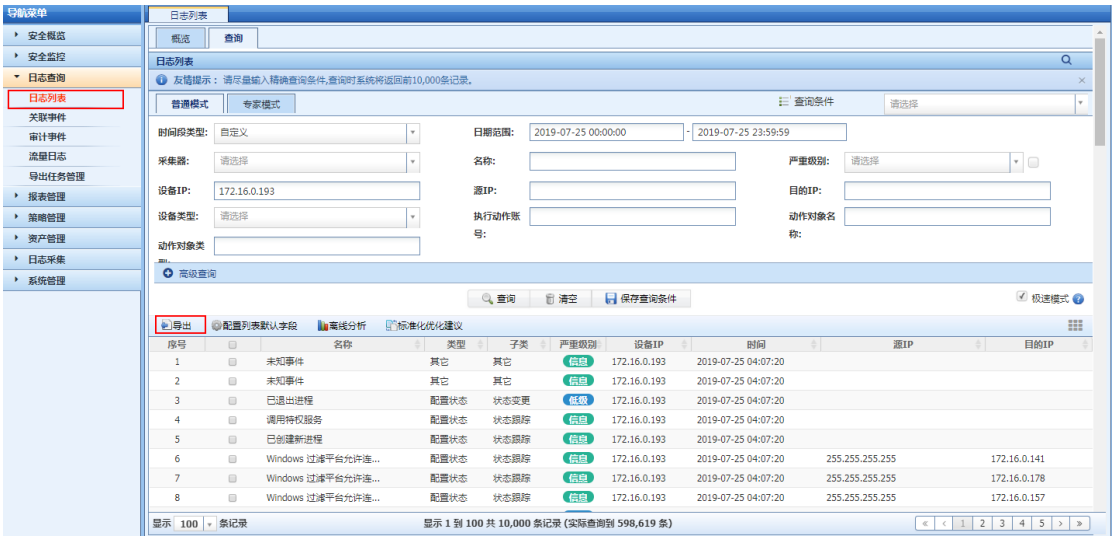


3.6. 导出任务管理

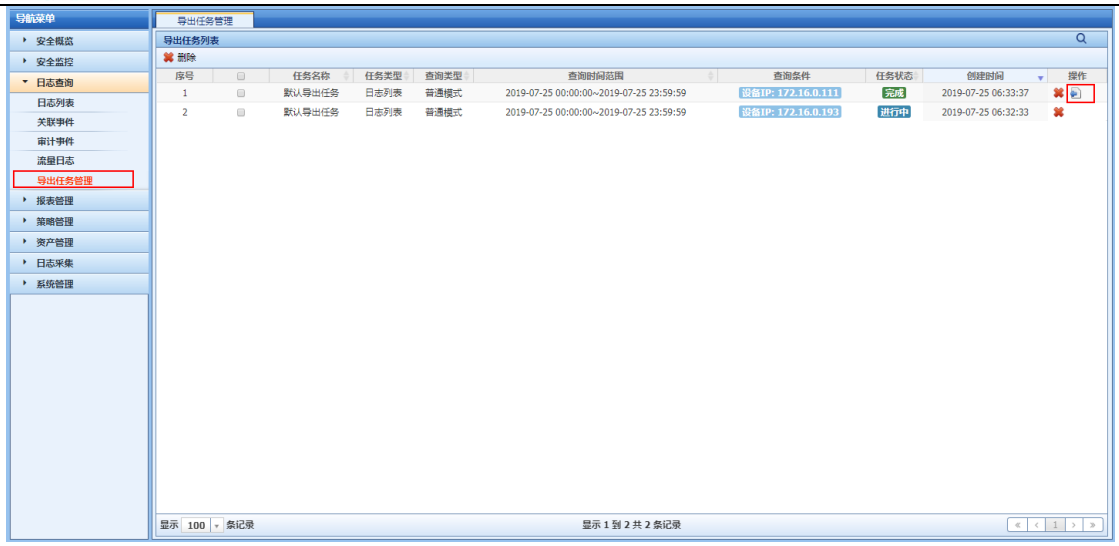
一、场景说明

对于你关心的日志事件，可以在日志查询中导出任务；导出完成可以在导出任务管理中查看导出结果；进而你可以继续导入本地查看详细信息。

1. 进入“日志查询->日志列表”菜单。



2. 进入“日志查询->导出任务管理”菜单。



4 日常维护

4.1. 软件版本升级

一、设备升级的目的（主程序及补丁包）

1、获取新功能。

2、解决软件缺陷。

二、升级注意事项

1、升级不会导致配置、日志文件、库文件、license 丢失。

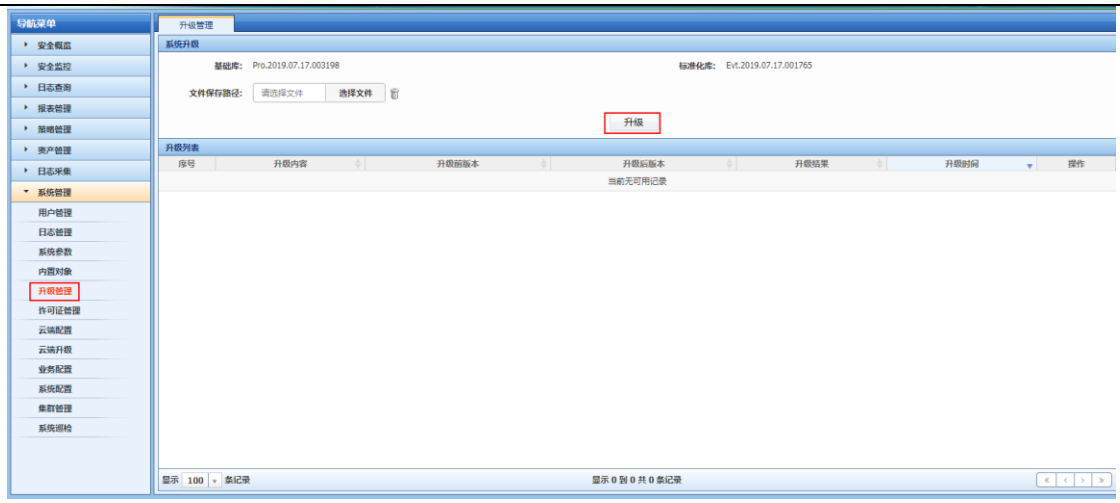
2、主程序升级需要重启设备，会造成断网，请避开业务高峰期升级。

3、主程序升级有一定风险，请务必保证升级过程中，设备供电稳定。

4、主程序升级前，请认真阅读版本发行说明及升级指导，同时注意比对下载的升级文件 MD5 值是否与发行说明提供的一致，避免因升级文件损坏造成升级失败。

三、具体步骤

1、登录 Web，进入系统管理->升级管理，界面如下图所示：



（1）在“系统升级处”处，单击“选择”按钮，选择本地 PC 机上的升级文件包(升级包后缀为.zip，前缀命名可任意，如 Las_305.xxx.xx.zip，一般用下载时的升级文件名字即可，不需修改）。

（2）点击“升级”按扭提交设置后，升级文件开始上传到设备上，上传成功后，设备会自动完成升级。

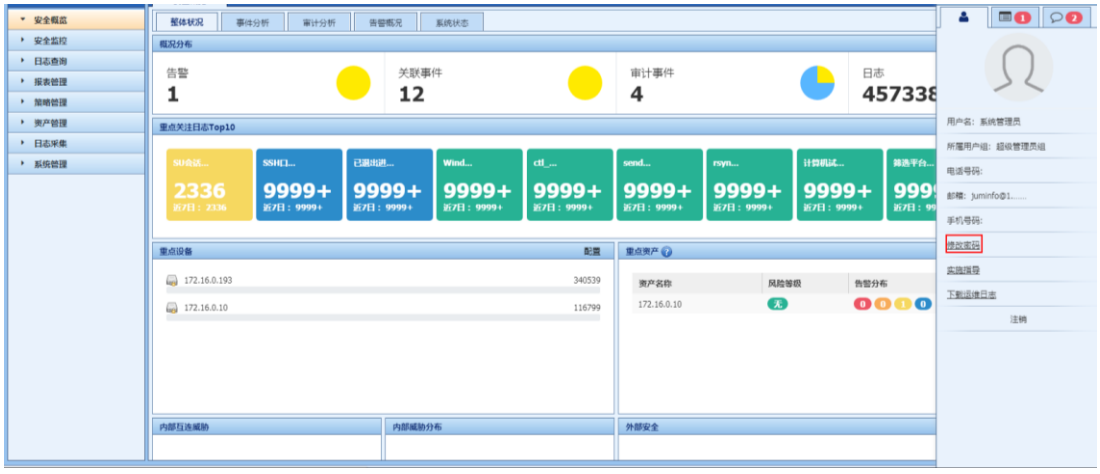
4.2. 修改密码

一、业务控制台密码修改：

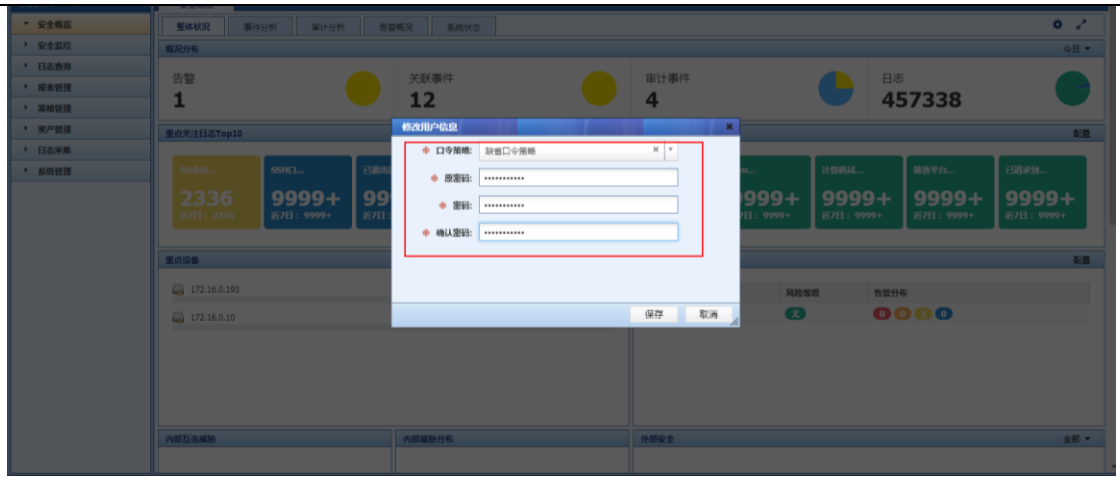
1、登录业务控制台 WEB 页面，输入 http://10.250.250.128 ：

默认用户：admin

默认密码：admin



2、点击右上角"系统管理员"->"个人信息":



3、点击"保存"，密码修改成功：

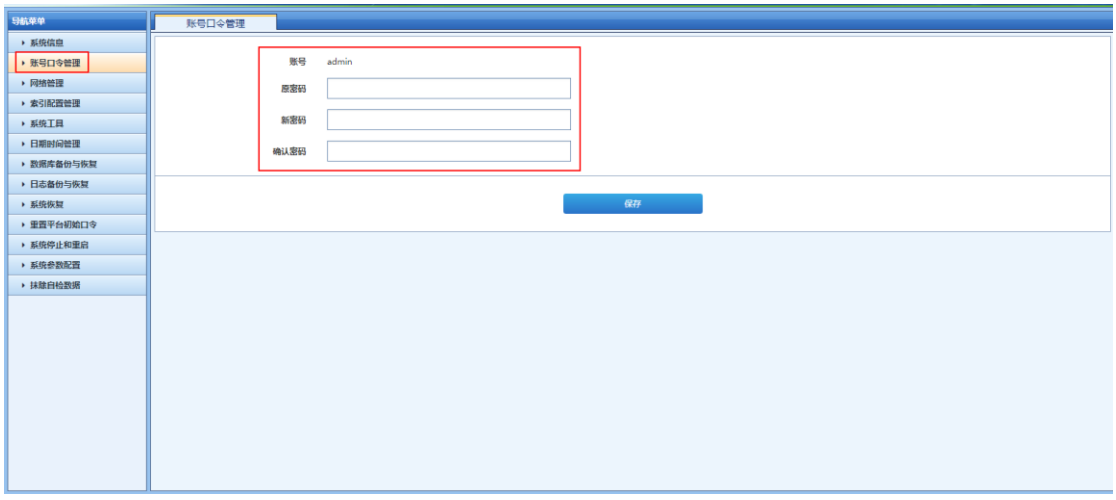
4、重新登录，验证密码。

二、管理控制台密码修改：

1、登录业务控制台 WEB 页面，输入 http://10.250.250.128:8082 ：

默认用户：admin

默认密码：admin



2、点击"保存"，密码修改成功。

3、重新登录，验证密码。

4.3. 恢复出厂设置

一、恢复出厂配置：

1、登录管理控制台 WEB 页面，输入 http://10.250.250.128:8082 ：

默认用户：admin

默认密码：admin

2、点击"系统恢复"->"系统恢复"按钮。

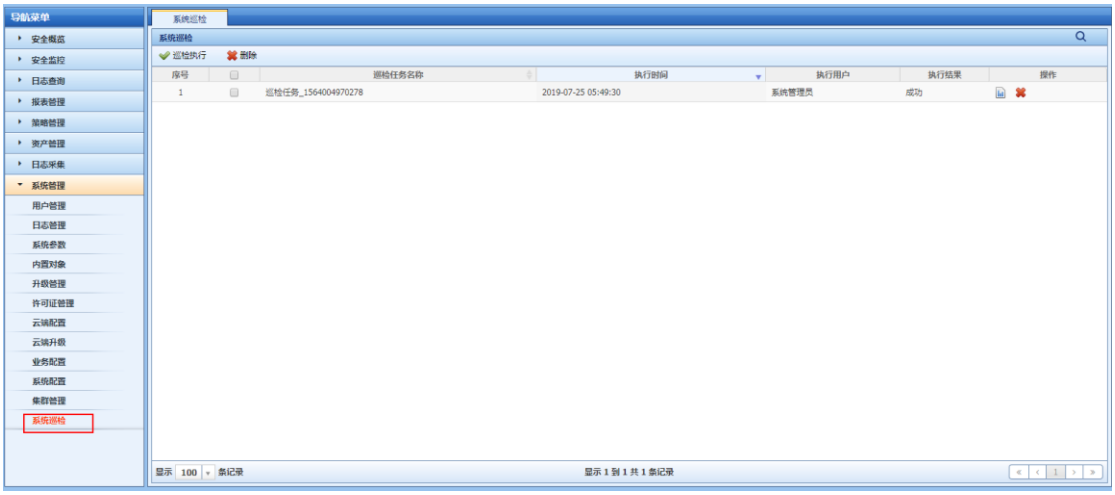
等待系统恢复完成。

3、重新登录，验证恢复结果。

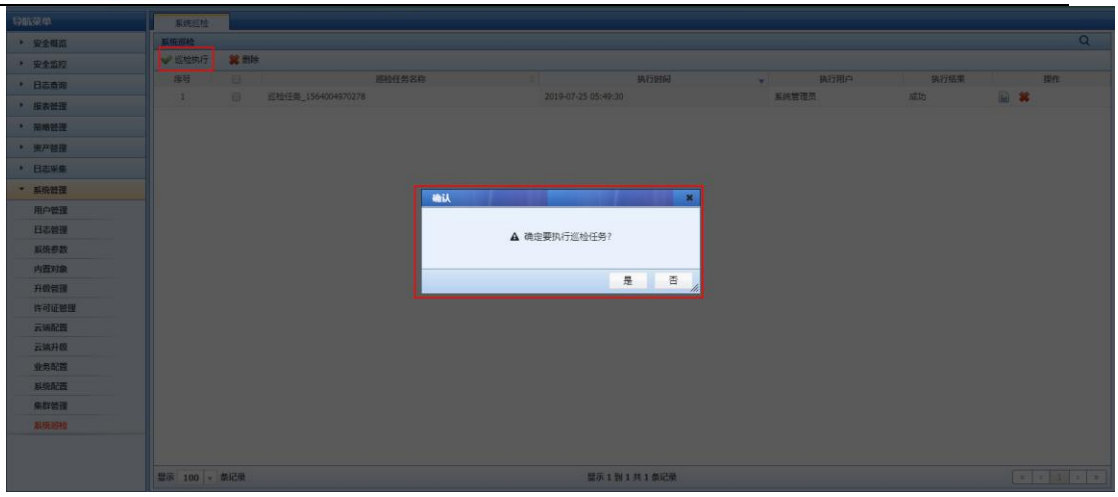
4.4. 系统巡检

巡检功能获取服务器状态，生成巡检报告。

系统管理->系统巡检。

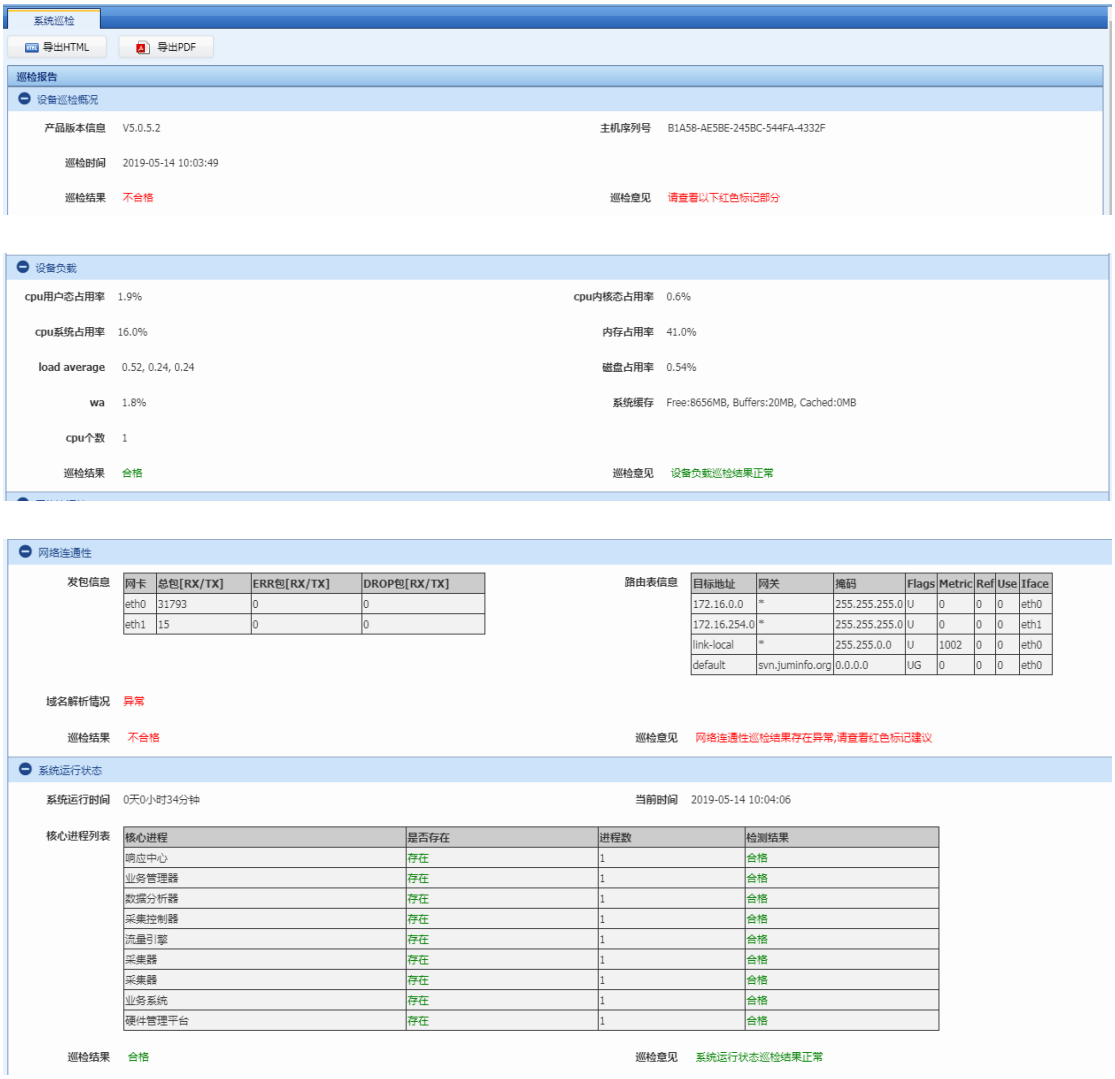


点击执行



巡检任务大致运行一分钟。

巡检结束后点击任务后方查看报告按钮，查看报告。



系统巡检

导出HTML　导出PDF

巡检报告

设备巡检概况

产品版本信息 V5.0.5.2　　主机序列号 B1A58-AE5BE-245BC-544FA-4332F

巡检时间 2019-05-14 10:03:49

巡检结果 不合格　　巡检意见 请查看以下红色标记部分

设备负载

cpu用户态占用率 1.9%　　cpu内核态占用率 0.6%

cpu系统占用率 16.0%　　内存占用率 41.0%

load average 0.52, 0.24, 0.24　　磁盘占用率 0.54%

wa 1.8%　　系统缓存 Free:8656MB, Buffers:20MB, Cached:0MB

cpu个数 1

巡检结果 合格　　巡检意见 设备负载巡检结果正常

网络连通性

发包信息

网卡	总包[RX/TX]	ERR包[RX/TX]	DROP包[RX/TX]
eth0	31793	0	0
eth1	15	0	0

路由表信息

目标地址	网关	掩码	Flags	Metric	Ref	Use	Iface
172.16.0.0	*	255.255.255.0	U	0	0	0	eth0
172.16.254.0	*	255.255.255.0	U	0	0	0	eth1
link-local	*	255.255.0.0	U	1002	0	0	eth0
default	svn.juminfo.org	0.0.0.0	UG	0	0	0	eth0

域名解析情况 异常

巡检结果 不合格　　巡检意见 网络连通性巡检结果存在异常,请查看红色标记建议

系统运行状态

系统运行时间 0天0小时34分钟　　当前时间 2019-05-14 10:04:06

核心进程列表

核心进程	是否存在	进程数	检测结果
响应中心	存在	1	合格
业务管理器	存在	1	合格
数据分析器	存在	1	合格
采集控制器	存在	1	合格
流量引擎	存在	1	合格
采集器	存在	1	合格
采集器	存在	1	合格
业务系统	存在	1	合格
硬件管理平台	存在	1	合格

巡检结果 合格　　巡检意见 系统运行状态巡检结果正常

4.5. 修改 IP 地址

一、修改 IP 地址：

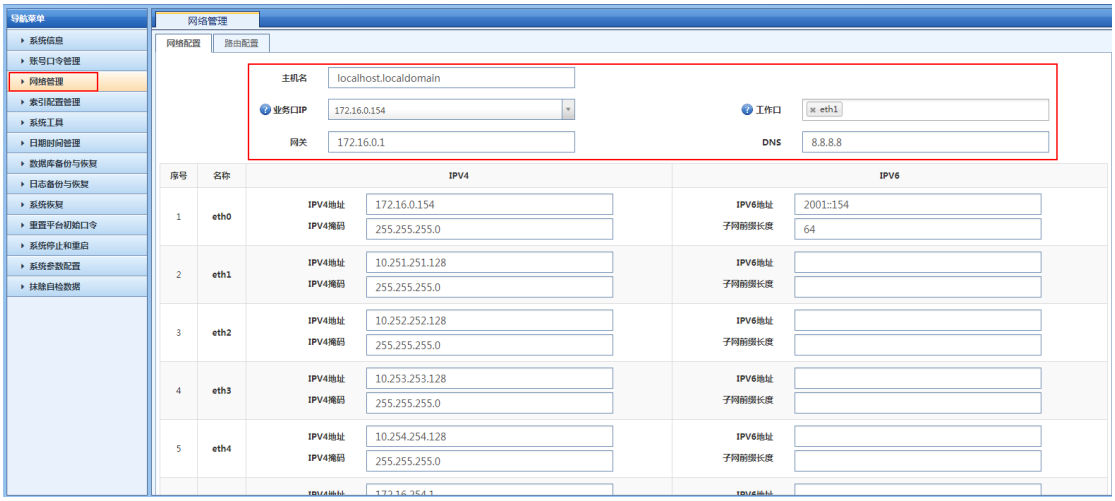
注意：设置 IP 地址将导致系统重启，请勿在业务高峰期操作（工作口配置任何网口都可用于流量接入口使用）。

1、登录管理控制台 WEB 页面，输入 http://10.250.250.128:8082 ：

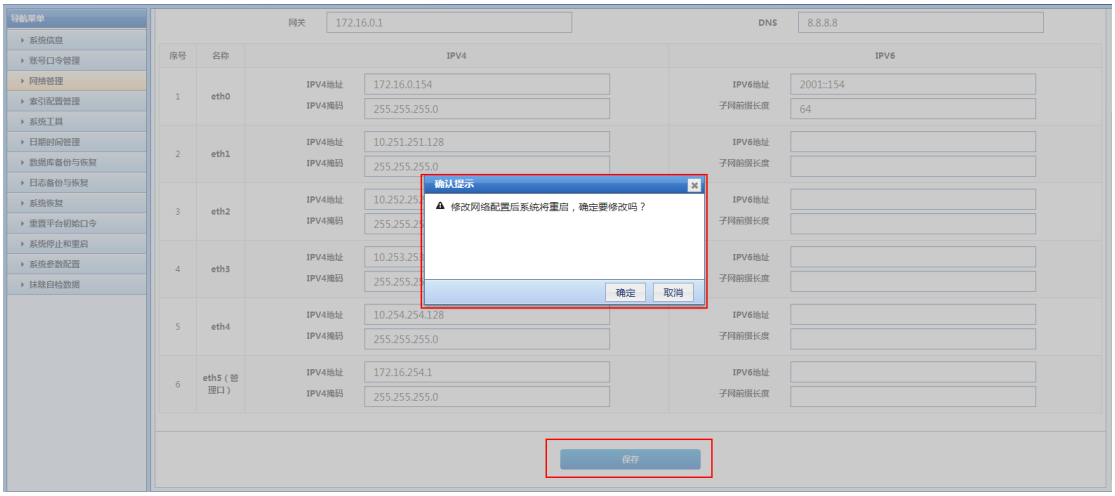
默认用户：admin

默认密码：admin

点击"网络管理"修改 IP 信息



2、点击"保存"按钮：



等待系统重启完成 IP 地址的修改。

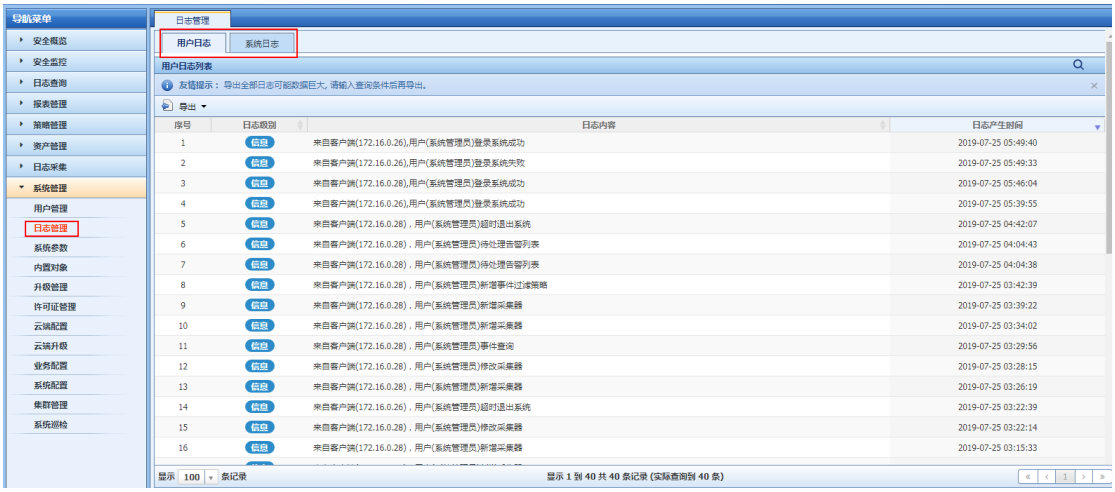
3、登录新的 IP 地址。

4.6. 日志查看

一、查看系统日志：

1、登录管理控制台 WEB 页面。

2、点击"系统管理"->"日志管理" ：



这里记录了系统各组件的运行日志，包括异常故障日志。

4.7. 日志备份与恢复

一、日志备份与恢复

1、登录业务控制台 WEB 页面，输入 https://10.250.250.128:8082（假设当前设备 IP 为 10.250.250.128）。

默认用户：admin

默认密码：admin

进入【日志库备份与恢复】

2、备份策略：不备份（系统默认不备份日志库），不会备份日志库。

3、自定义备份日志：可以选择每周、每月备份一次当前的日志库。

i、备份方式：SFTP

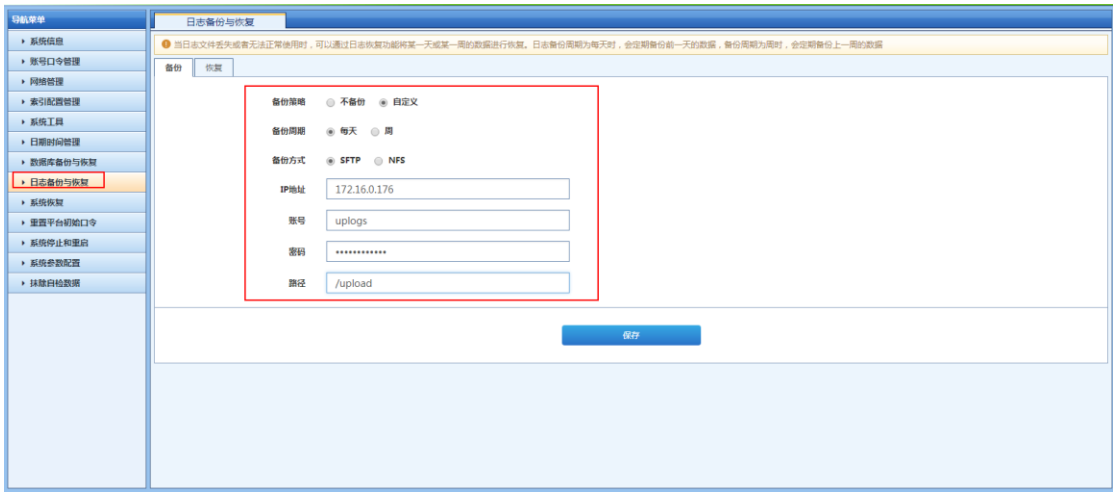
IP 地址：172.16.0.176（需要备份到的 SFTP 服务器）。

账号：uplogs（备份 SFTP 服务器的账号）。

密码：Yourpassword（备份账号的密码）。

路径：/upload（备份 SFTP 服务器的路径）。

点击保存后，系统将立即向 SFTP 服务器备份一次日志库。

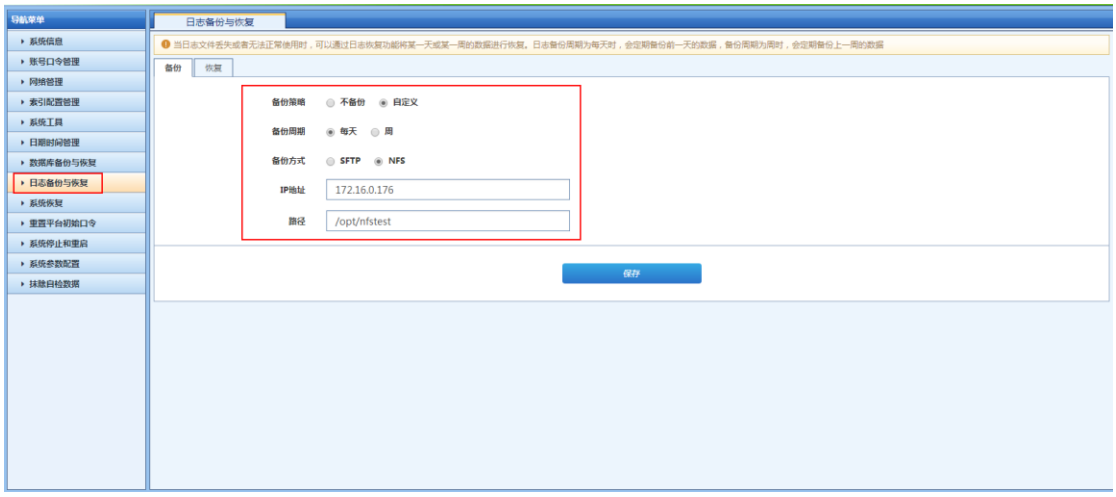


ii、备份方式：NFS

IP 地址：172.16.0.176（需要备份到的 NFS 服务器）。

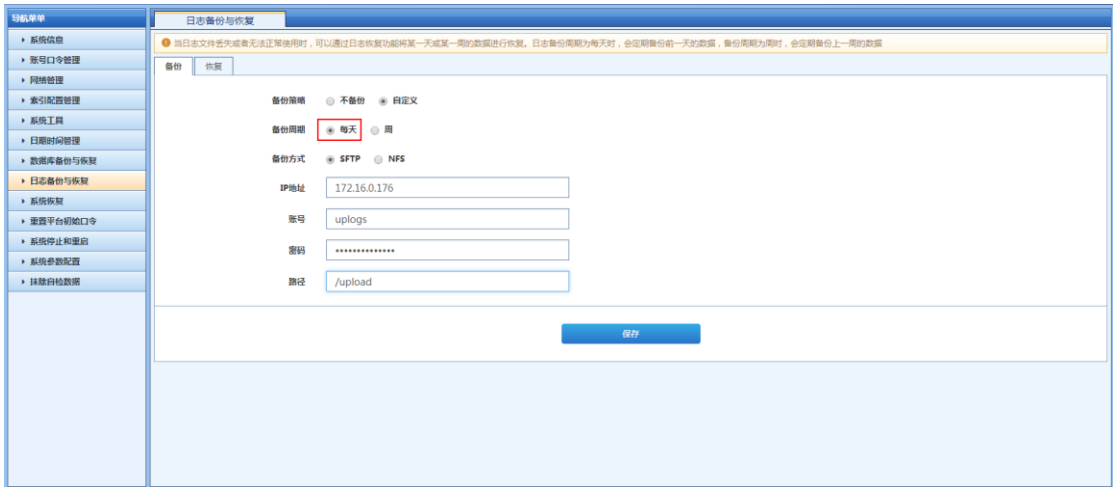
路径：/opt/nfstest（备份 NFS 服务器的路径）。

点击保存后，系统将立即向 NFS 服务器备份一次日志库。

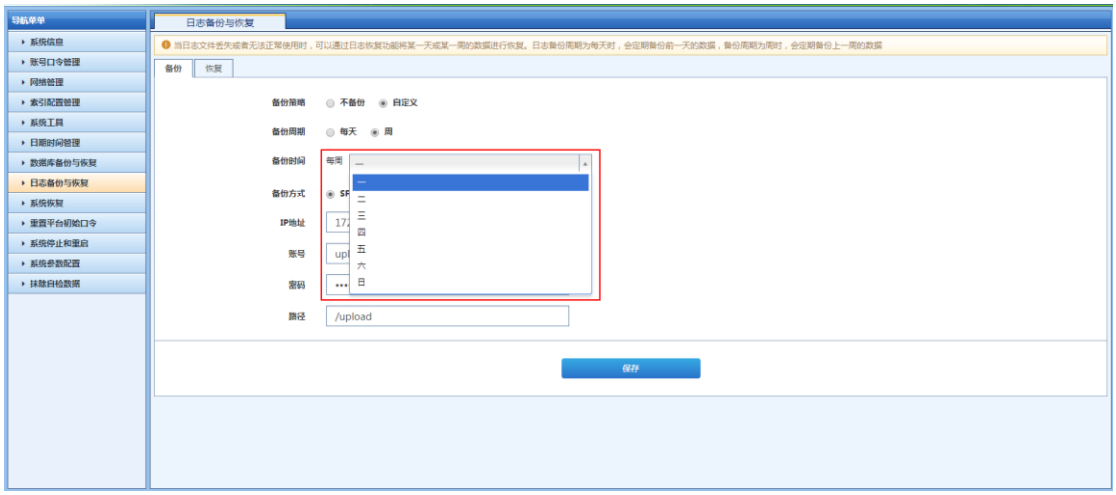


4、自定义备份日志库：用户可以根据每天、每周通过使用 SFTP 和 NFS 备份：

i、选择每天：每天凌晨 1 点左右会备份一次日志库。

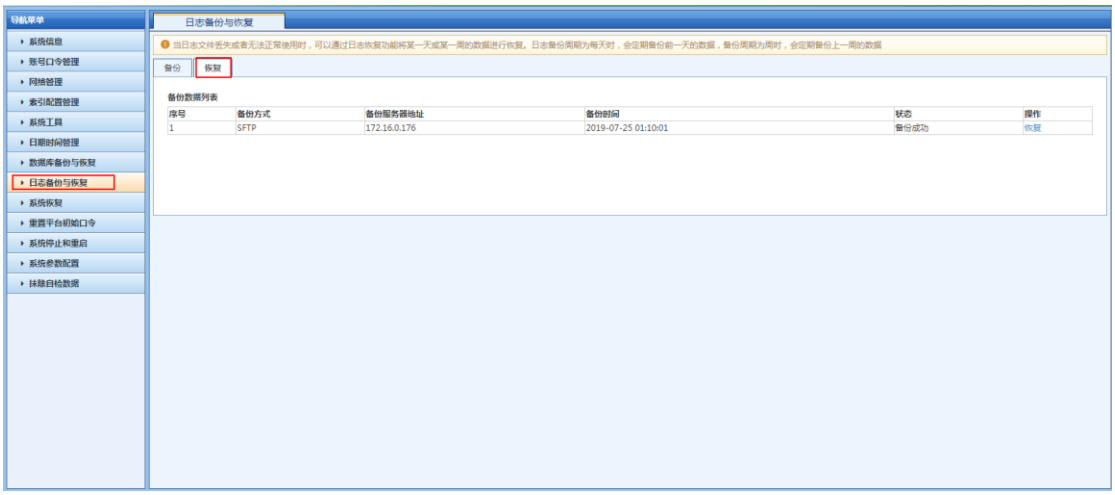


ii、选择周：可选择周一至周日的任意一天，一周备份一次。

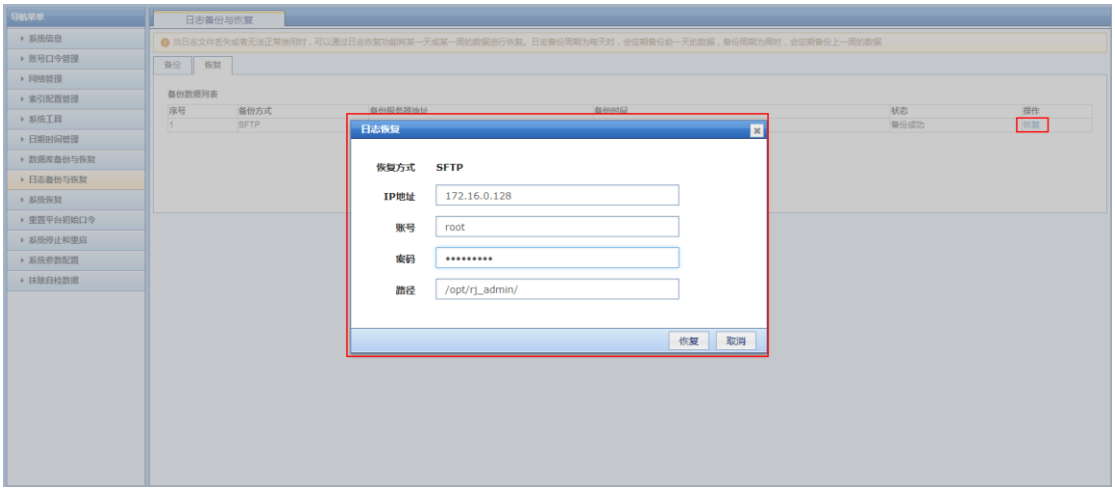


二、日志恢复

1、进入硬件管理平台->【日志备份与恢复】->【恢复】界面，可查看历史日志库备份的结果。



2、对于备份成功的结果，可以进行日志库恢复，点击【恢复】按钮，输入相关信息（与立即备份操作类似），即可进行恢复日志库，若当前系统日志库已存在会覆盖恢复。



4.8. 数据库备份与恢复

一、数据库备份

1、登录业务控制台 WEB 页面，输入 https://10.250.250.128:8082（假设当前设备 IP 为 10.250.250.128）。

默认用户：admin

默认密码：admin

进入【数据库备份与恢复】

2、备份策略：不备份（系统默认不备份数据库），不会备份数据库。

3、立即备份数据库：一次生效，立即备份一次当前的数据库。

i、备份方式：SFTP

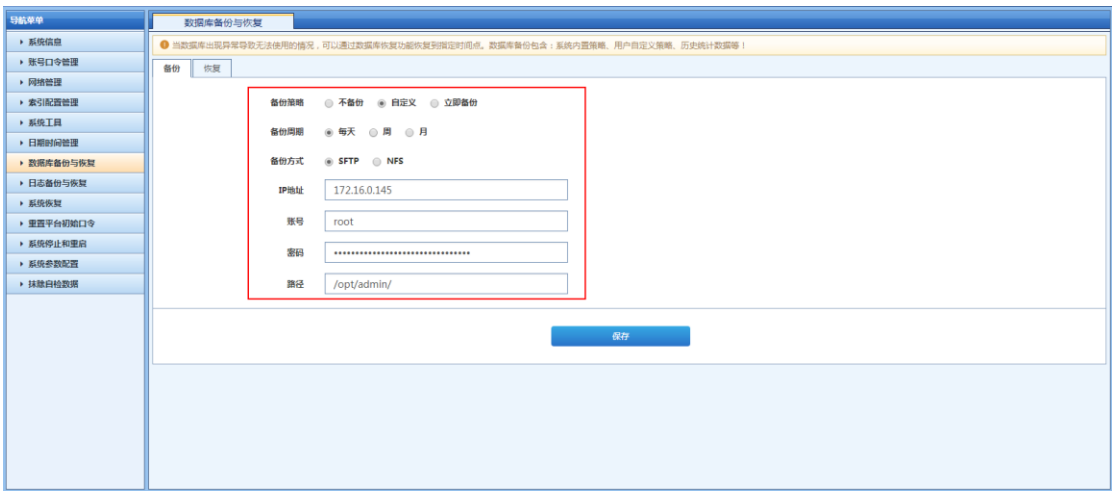
IP 地址：172.16.0.176（需要备份到的 SFTP 服务器）。

账号：uplogs（备份 SFTP 服务器的账号）。

密码：Yourpassword（备份账号的密码）。

路径：/upload（备份 SFTP 服务器的路径）。

点击保存后，系统将立即向 SFTP 服务器备份一次数据库。



ii、备份方式：NFS

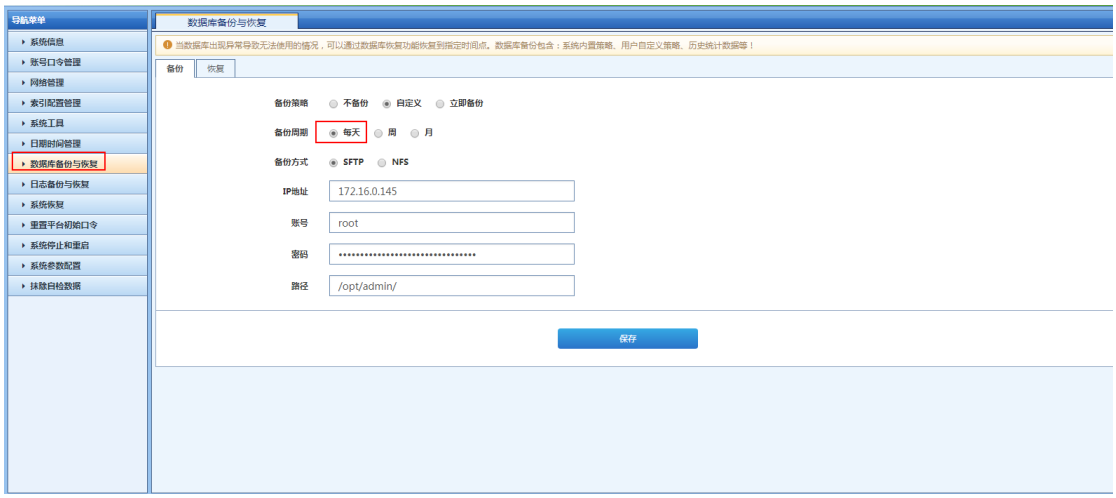
IP 地址：172.16.0.176（需要备份到的 NFS 服务器）。

路径：/opt/nfstest（备份 NFS 服务器的路径）。

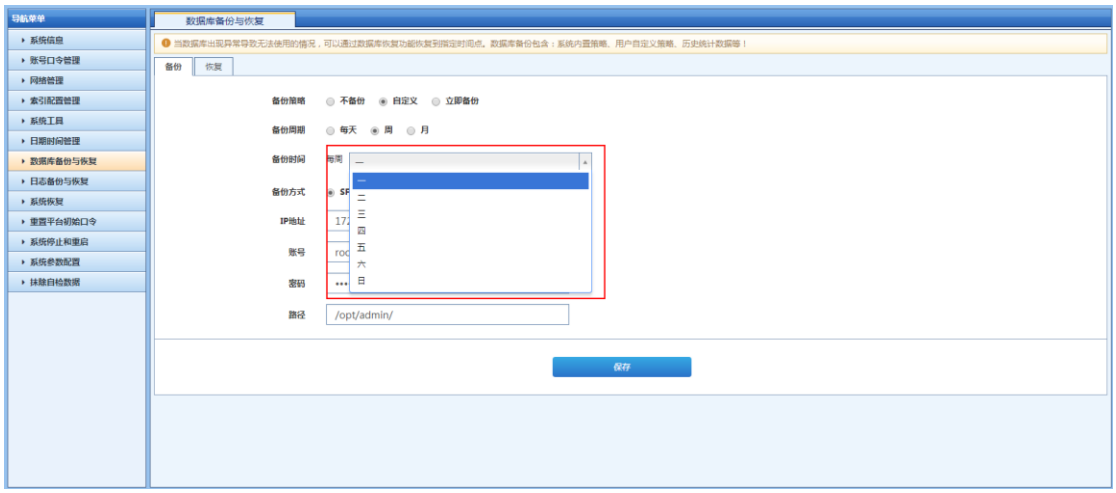
点击保存后，系统将立即向 NFS 服务器备份一次数据库。

4、自定义备份数据库：用户可以根据每天、每周、每月通过使用 SFTP 和 NFS 备份（备份方式与立即备份一致）。

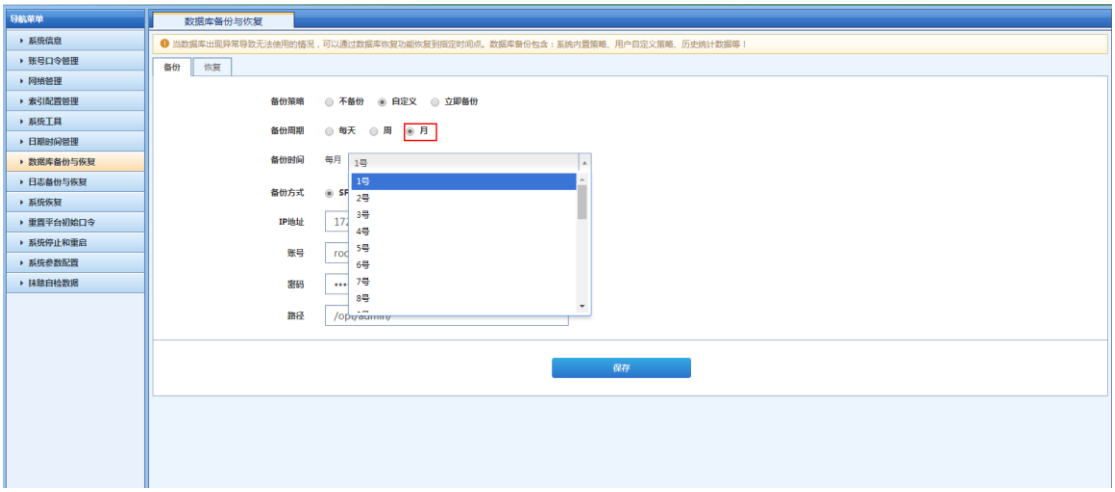
i、选择每天：每天凌晨 1 点左右会备份一次数据库。



ii、选择周：可选择周一至周日的任意一天，一周备份一次。

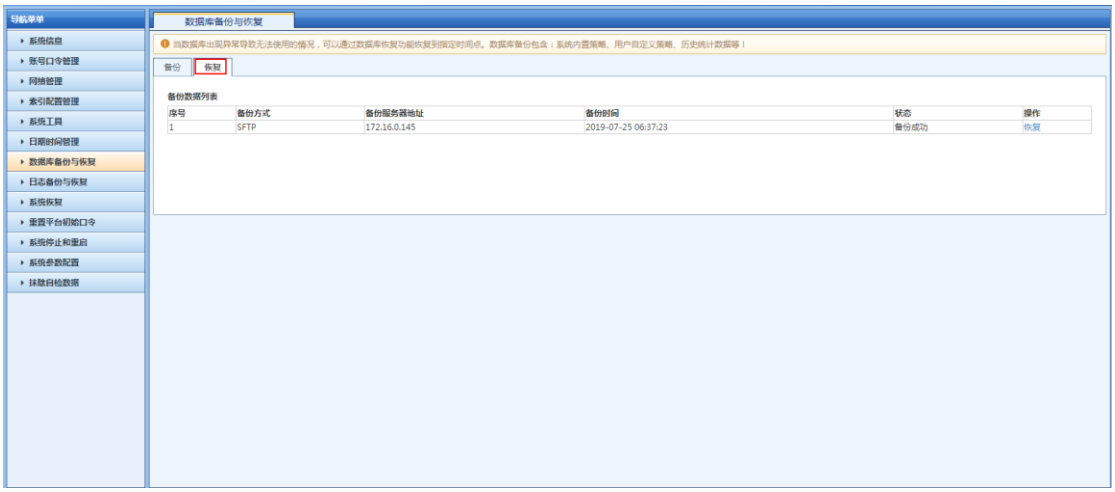


iii、选择月：可选择 1 号至 28 号的任意一天，一个月备份一次 。

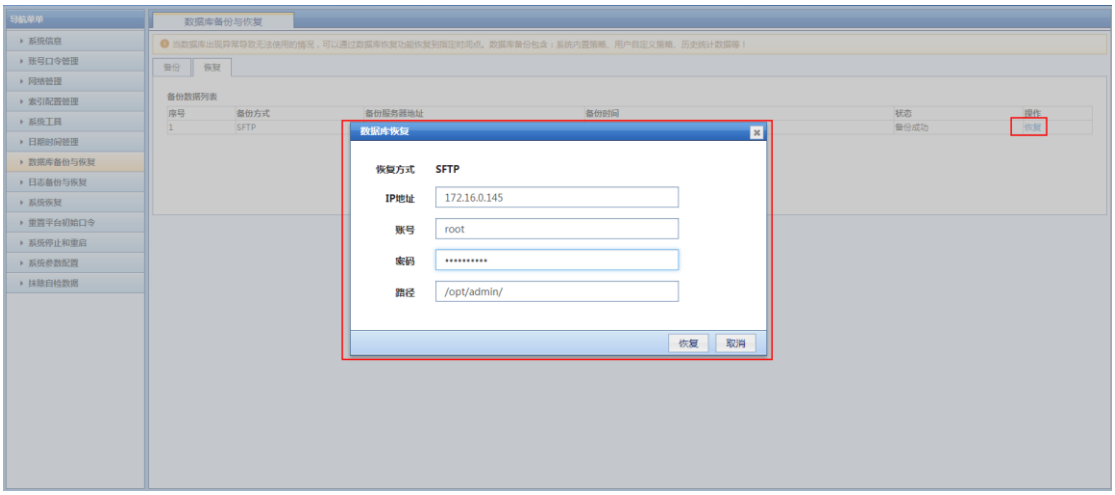


二、数据库恢复

1、进入硬件管理平台->【数据库备份与恢复】->【恢复】界面，可查看历史数据库备份的结果 。



2、对于备份成功的结果，可以进行数据库恢复，点击【恢复】按钮，输入相关信息（与立即备份操作类似），即可进行恢复数据库，若当前系统数据库已存在会覆盖恢复。



4.9. 集群维护（选配）

测试场景：

搭建集群：主节点：192.168.100.173

子节点：192.168.100.171

（备注）

登录硬件管理平台：https://192.168.100.171:8082

登录业务控制平台：https://192.168.100.173:8443

一、集群状态查看：

登录业务控制台页面进行集群维护。【系统管理】->【集群管理】查看当前集群状态。

二、集群配置操作步骤：

登录业务控制台系统管理->集群管理查看操作步骤配置集群。

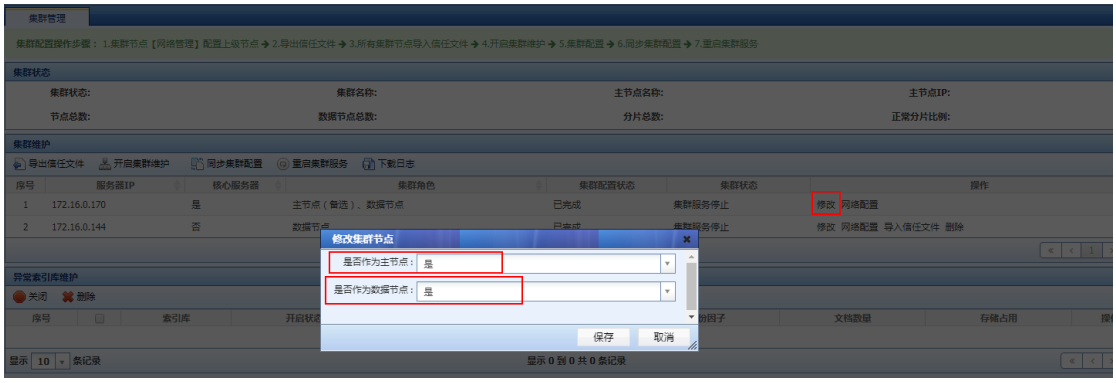
三、集群维护：

数据节点配置上级节点后可在此列表查看已注册的数据节点，通过页面顶端的配置步骤可快速配置集群，所有集群节点的集群状态更新为“已加入集群”，集群即可配置成功。若集群配置失败，可通过点击列表上的【下载日志】下载相关日志。

四、修改集群节点：

开启集群维护后可通过点击各节点的【修改】按钮来修改“是否作为主节点”“是否作为数据节点”等配置，点击【确定】后即可成功配置。

注意：至少选择一个节点作为主节点。

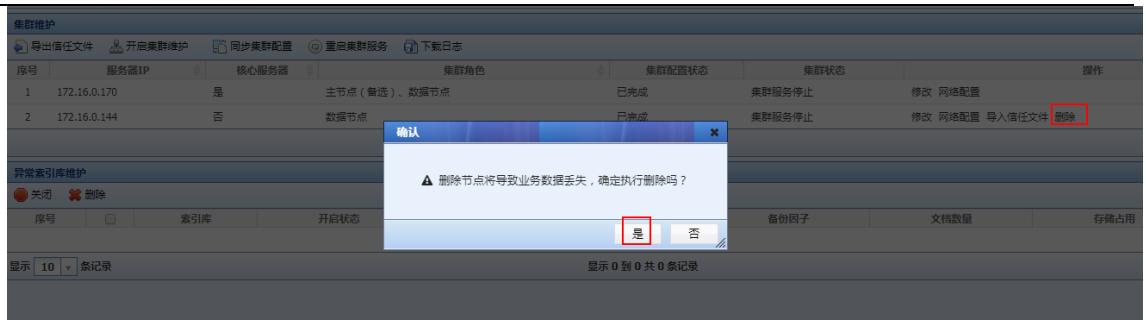


五、网络配置：

开启集群维护后可以通过点击各节点【网络配置】按钮来修改节点的网络配置信息，修改后点击【确定】即可成功应用。

六、删除节点：

开启集群维护后可以通过点击各节点【删除】按钮来删除节点，弹出框点击【确定】即可删除此节点。删除的节点可以通过重启此节点业务系统后重新加入。



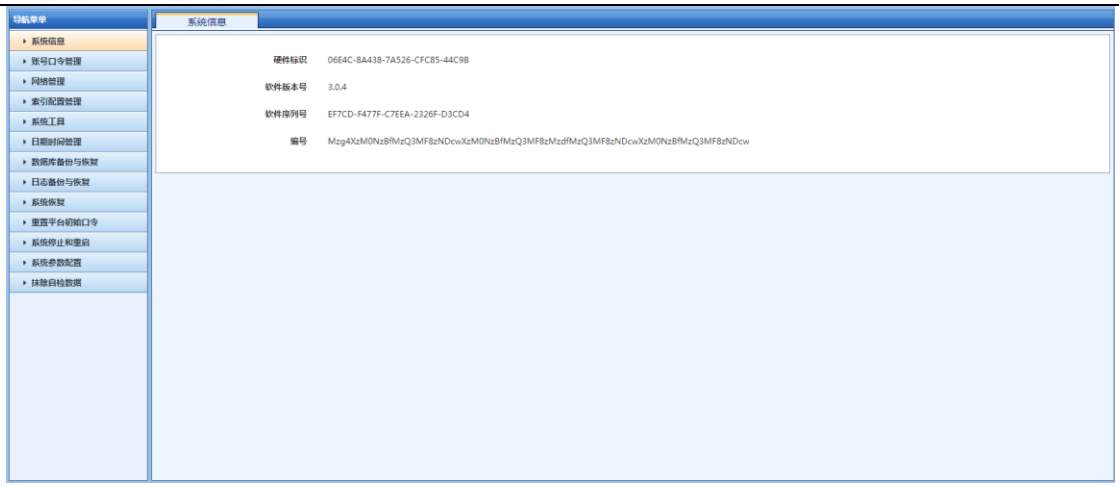
七、异常日志库维护：

通过关闭、删除对异常日志库进行维护操作。关闭或删除异常日志库后“集群状态”会更新为“正常”

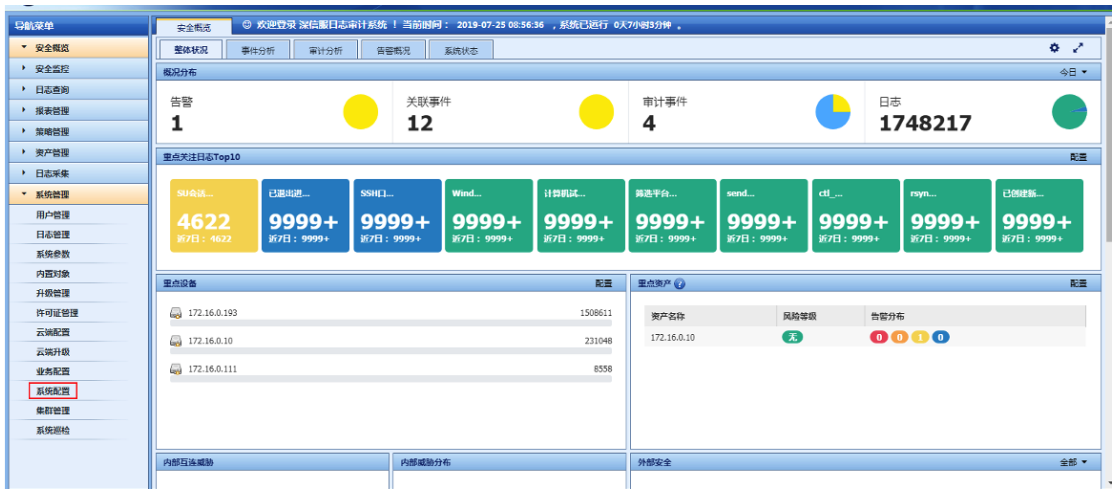
4.10. 系统配置

硬件管理功能既是当用户登录业务管理控制台；可直接跳转到硬件管理平台。

系统管理->系统配置：当用户已经登录过硬件管理平台即可直接跳转到硬件管理平台页面



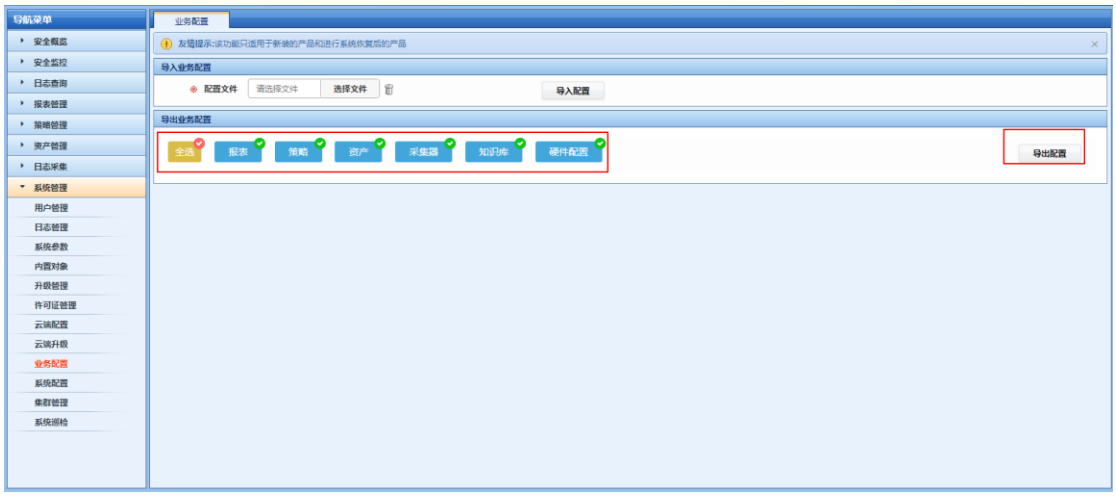
当用户未登录过硬件管理平台时，点击硬件管理会直接跳转到修改密码的页面。



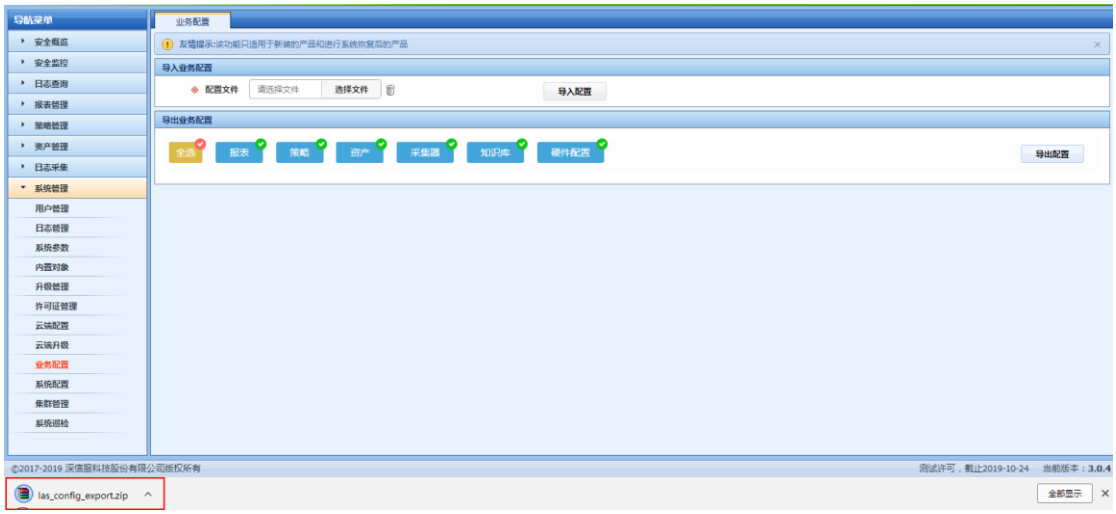
4.11. 业务配置管理

配置管理功能即是可将当前系统环境信息中，自定义信息完整导出，可在新环境导入，以做环境迁移。

配置导出：

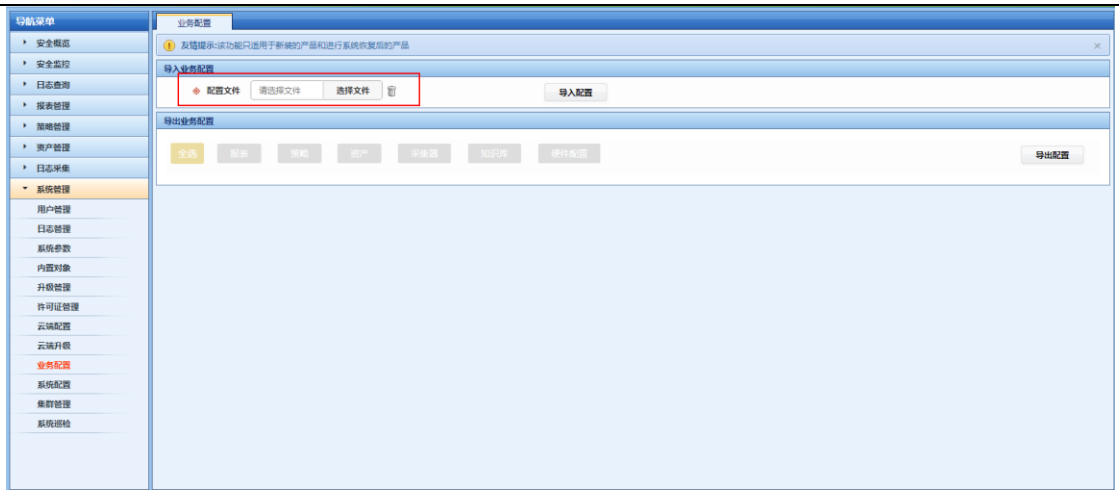


点击导出配置按钮，下载获得



配置导入：

在新的环境中打开此界面即可导入下载的配置数据。导入成功后，系统将会自动重启。



4.12. 运维日志下载

如设备出现故障，可在个人工作台中下载运维日志，下载方式如下图标识：

4.13. 常用配置命令

常用命令：

用户可以使用命令行对系统进行简单管理（使用 ssh 登录），初始用户名和口令分别为 syscli、Test@123，界面如下：

```
Welcome to CLI Management.

   2019/07/18 02:57:59

1. Reset CLI User password
2. Component Status Query
3. Component Restart
4. System Shutdown
5. System Restart
6. Enter Console
7. Reset WEB_User:admin password
8. Reset WEB_Manager:admin password
9. Version
10.Running Time
11.Show the beginning
12.Show network
13.Setup IP address
14.Setup IPV6 address
15.Change Console access port
16.Change WEB access port
0. Exit
```

输入相应序号，则可进入相应选项

1、 User Account Setting：用户账号设置，用于修改 CLI 用户密码，根据提示修改密码:

```
old password:
new password:
repeat the new password:
```

2、 Component Status Query：查看系统组件状态 ：

```
data_analyser Ok! PID:[2599]
business_manager Ok! PID:[2704]
response_center Ok! PID:[2883]
file_store Ok! PID:[3491]
database Ok! PID:[2102]
web_server Ok! PID:[28985]
collector Ok! PID:[26844]
Done.
```

3、 Component Restart：组件重启:

4、 System Shutdown：关机 ：

5、 System Restart：设备重启 ：

6、 Enter Console：输入管理员密码，进入系统后台 ：

7、 Reset WEB_User:admin password：重置 WEB 管理员密码 ：

```
Rest AdminUser password
new password:
repeat the new password:
```

8、 Reset WEB_Manager:admin password：重置管理控制台密码:

```
Rest AdminUser password
new password:
repeat the new password:
```

9、 Version：查看版本号 ：

10、 Running Time：查看系统运行时间 ：

```
Show running time
+---------------------+--------------+
| startTime           | RunningHours |
+---------------------+--------------+
| 2018-10-15 05:54:50 |      2790.76 |
+---------------------+--------------+
Done.
```

11 Show the beginning：查看开机时间 ：

12 Show network ：

```
eth0      Link encap:Ethernet  HWaddr 52:54:00:D7:F9:F7
          inet addr:172.16.0.159  Bcast:172.16.0.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fed7:f9f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49988908 errors:0 dropped:2089 overruns:0 frame:0
          TX packets:44601901 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51963282657 (48.3 GiB)  TX bytes:7409815003 (6.9 GiB)
          Interrupt:11 Base address:0xa000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:383821504 errors:0 dropped:0 overruns:0 frame:0
          TX packets:383821504 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:319315013107 (297.3 GiB)  TX bytes:319315013107 (297.3 GiB)

Done.
```

13 Setup IP address （工作口配置任何网口都可用于流量接入口使用）:

```
Input if-name[eth0|eth1|eth2]: eth0
-----------------------------------
        IP address:
           netmask:
           gateway:
               DNS:
```

14 Setup IPV6 address：修改 IPV6 地址：

```
Input if-name[eth0]:
-----------------------------------
        IP address:
            prefix:
           gateway:
               DNS:
```

15 Change Console access port：修改硬件管理平台访问端口：

```
Change Console access port
New access port:
```

16 Change WEB access port：修改 web 访问端口：

```
Change Console access port
New access port:
```

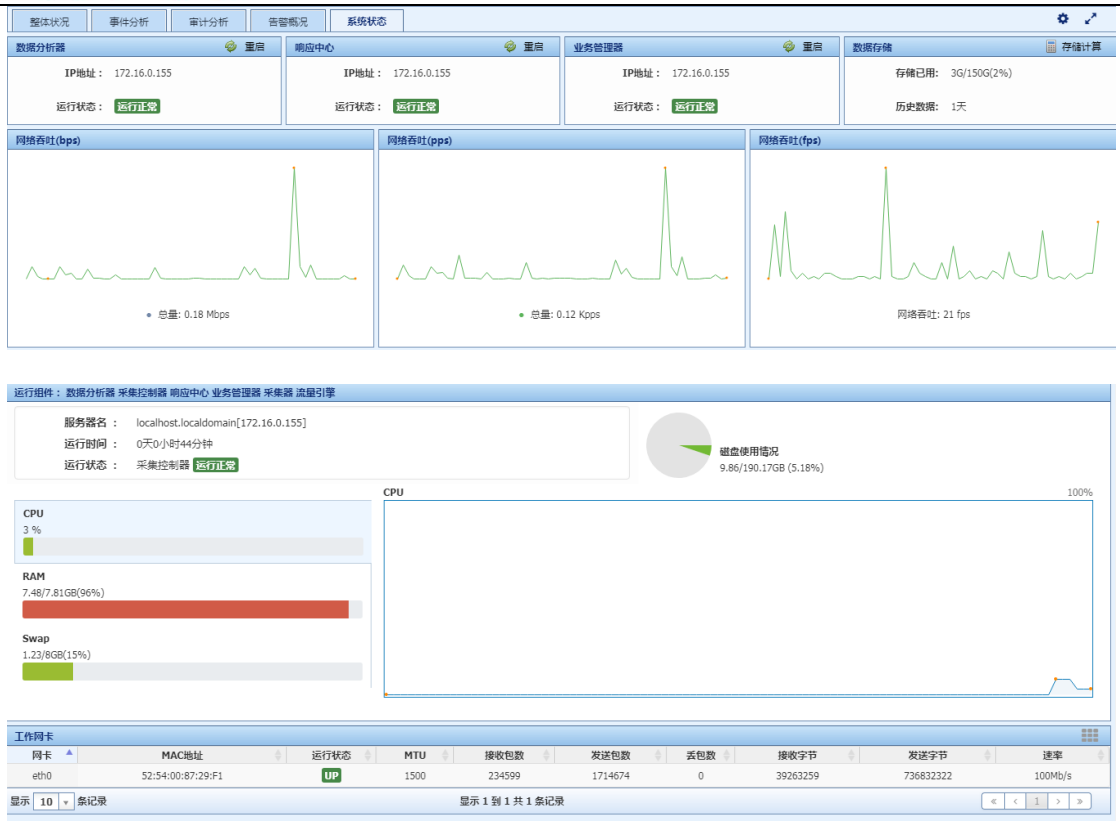
5 实施后设备运行检查

5.1 整体运行状态检查

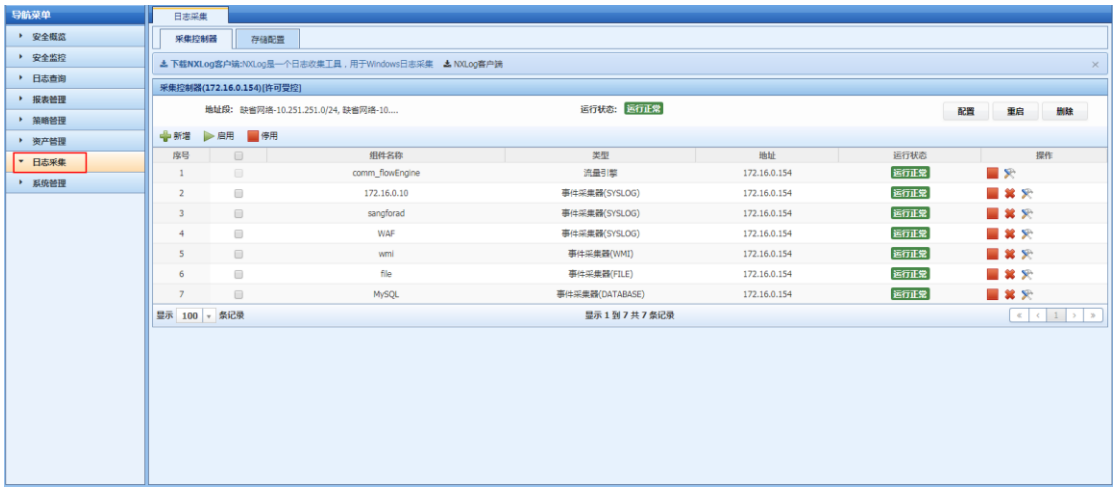
一、基础检查

操作方法：

1、 在“安全概览”->“系统状态”查看设备运行时间、CPU、内存、硬盘利用率 ：



2、在菜单日志采集查看采集器运行状态：



二、检查标准：

1、检查个组件运行是否正常；

2、硬盘利用率低于 80%是正常的，高于 80%则会自动清理硬盘；

3、CPU 和内存稳定运行时不高于 80%是正常的，CPU 或内存达到 80%以上，需要关注：

①设备是否正在高 EPS 的情况下接收日志：EPS 越高，CPU 利用率会越高。

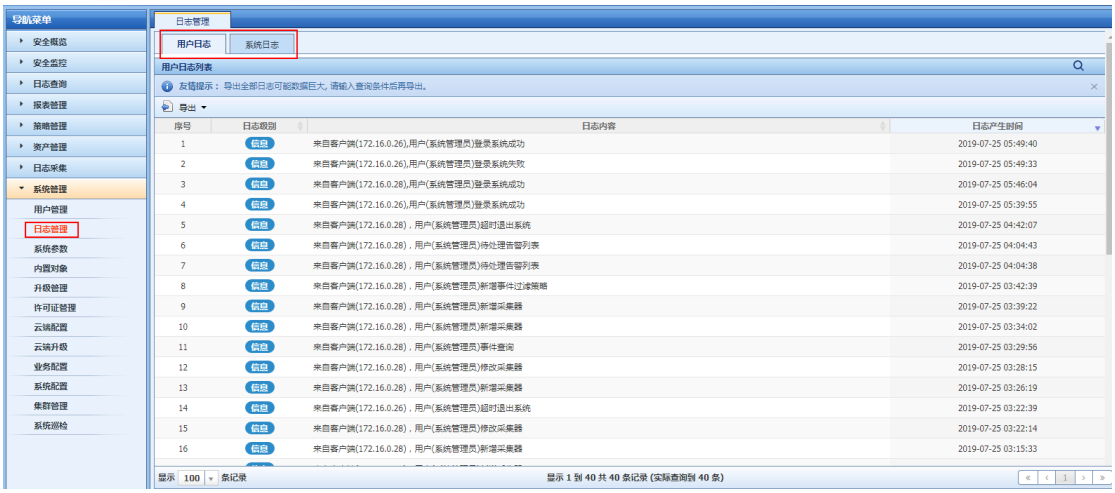
5.2 设备日志检查

一、基础检查

操作方法：

1、登录管理控制台 WEB 页面。

2、点击"系统管理"->"日志管理"。



这里记录了系统各组件的运行日志，包括异常故障日志。

二、检查标准：

1、检查系统日志里是否有异常日志，系统运行的日志都会在这里显示。

5.3 主要功能使用情况检查

一、基础检查

操作方法：

1、登录管理控制台 WEB 页面。

2、查看"日志查询"->"日志列表"是否有设备日志。

3、查看"日志查询"->"关联事件"是否有匹配关联策略的关联事件产生。

4、查看"日志查询"->"审计事件"是否有匹配审计策略的关联事件产生。

5、查看"安全概览" 下各个仪表盘是否有相应的统计报告产生。

二、检查标准：

操作方法：

1、事件列表展示系统接收到的设备日志。

2、关联事件列表展示符合关联策略的关联事件。

3、审计事件列表展示符合审计策略的审计事件。

4、安全概览下个仪表盘显示正常，统计数据正确。