# UNIS D2000-G 系列数据库审计系统

## Web 配置指导

紫光恒越技术有限公司
www.unisyue.com

资料版本：5W102-20220614

# 前 言

本配置指导介绍了 UNIS D2000-G 系列应用层网关各软件特性的原理及其通过 Web 配置的方法，包含原理简介、配置任务描述和配置举例。

前言部分包含如下内容：



## 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

## 本书约定

### 1. 命令行格式约定

| 格　式 | 意　义 |
| --- | --- |
| **粗体** | 命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。 |
| *斜体* | 命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。 |
| [ ] | 表示用“[ ]”括起来的部分在命令配置时是可选的。 |
| { x \| y \| ... } | 表示从多个选项中仅选取一个。 |
| [ x \| y \| ... ] | 表示从多个选项中选取一个或者不选。 |
| { x \| y \| ... }* | 表示从多个选项中至少选取一个。 |
| [ x \| y \| ... ]* | 表示从多个选项中选取一个、多个或者不选。 |
| &<1-n> | 表示符号&前面的参数可以重复输入1～n次。 |
| # | 由“#”号开始的行表示为注释行。 |

### 2. 图形界面格式约定

| 格　式 | 意　义 |
| --- | --- |
| < > | 带尖括号“< >”表示按钮名，如“单击<确定>按钮”。 |
| [ ] | 带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。 |
| / | 多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下 |

| 格　式 | 意　义 |
| --- | --- |
| | 的[文件夹]菜单项。 |

### 3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

| | |
| --- | --- |
|  警告 | 该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。 |
|  注意 | 提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。 |
|  提示 | 为确保设备配置成功或者正常工作而需要特别关注的操作或信息。 |
|  说明 | 对操作内容的描述进行必要的补充和说明。 |
|  窍门 | 配置、操作、或使用设备的技巧、小窍门。 |

### 4. 图标约定

本书使用的图标及其含义如下：

| | |
| --- | --- |
|  | 该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。 |
|  | 该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。 |
|  | 该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。 |
|  | 该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。 |
|  | 该图标及其相关描述文字代表无线接入点设备。 |
|  | 该图标及其相关描述文字代表无线终结单元。 |
|  | 该图标及其相关描述文字代表无线终结者。 |
|  | 该图标及其相关描述文字代表无线Mesh设备。 |
|  | 该图标代表发散的无线射频信号。 |
|  | 该图标代表点到点的无线射频信号。 |
|  | 该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。 |

| | |
|---|---|
|  | 该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。 |

### 5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

## 产品配套资料

UNIS D2000-G 系列应用层网关的配套资料包括如下部分：

| 大类 | 资料名称 | 内容介绍 |
|---|---|---|
| 产品知识介绍 | 产品彩页 | 帮助您了解产品的主要规格参数及亮点 |
| 硬件描述与安装 | 安全兼容性手册 | 列出产品的兼容性声明，并对兼容性和安全的细节进行说明 |
| | 快速入门 | 指导您对设备进行初始安装、配置，通常针对最常用的情况，减少您的检索时间 |
| | 安装指导 | 帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装 |
| 业务配置 | 配置指导 | 帮助您掌握设备软件功能的配置方法及配置步骤 |
| | 典型配置举例 | 帮助您了解产品的典型应用和推荐配置，从组网需求、组网图、配置步骤几方面进行介绍 |
| 运行维护 | 版本说明书 | 帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法 |

## 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：mailto:info@unisyue.com

感谢您的反馈，让我们做得更好！

# 目 录

# 1 概述

## 1.1 系统背景

企业机构的信息化程度越高，企业对信息系统的依赖就越强烈，而后台的数据库是信息化系统的心脏，数据库中存放着大量企业的重要信息，例如：财务信息、客户信息、合同等。数据库是企业的核心资产，是最有价值的部分，因此也引起了不少黑客的觊觎。

对信息资产的威胁主要分为两类：一类是破坏，将数据篡改、删除、损坏；另一类是数据泄漏，对机密信息的窃取。

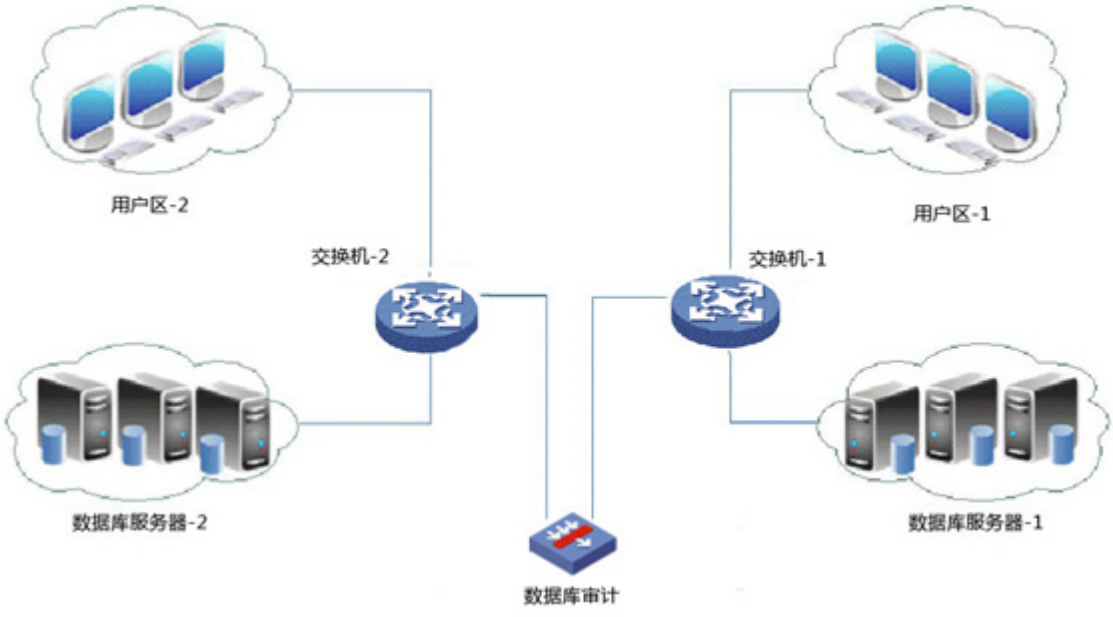
## 1.2 产品特点

UNIS 数据库审计系统利用更合理的网络和信息安全技术手段，实现对数据库操作行为审计、深入分析，监测并识别风险事件，及时告警并对其取证保留现场，是多功能为一体的全方位的数据库安全审计系统。

系统支持同时审计多种不同的数据库，具有灵活性和广泛的适用性。

该系统采用网络旁路实时侦听方式，全线速采集网络上所有会话流，对网络中业务系统数据库进行全面的风险分析与安全监控审计、告警。关注核心数据和业务的完全审计，不参与被监控网络的数据传输活动，因此不对网络结构和性能产生任何影响，具有很好的透明性和安全性。

图1-1 典型部署图



## 1.3 系统功能

系统分为五大模块分别是：监控中心、审计中心、策略中心、报表中心及系统管理。五大模块功能各有侧重点，相互作用，使系统具备了以下功能，帮助系统管理员解决实际问题。

(1) 系统实时监控

不仅对自身性能（CPU 使用率、内存使用率和硬盘使用率）进行状态监控，还对信息系统数据库产生的安全事件进行 24 小时监控，并以统计图表的形式展示，让管理员一目了然。

(2) 事前预防

准确的定位各种风险事件行为，检测到威胁时可根据用户需求进行告警，将业务系统的风险事件防范工作，由被动式的事后分析，提升到主动式全面预防的水平。

(3) 有效、准确的识别规则

任何违反审计规则的操作都会被检测，做到准确、有效地识别具有风险的行为。

(4) 事中现场取证

通过实时监测并智能地分析、还原各种数据库操作，解析数据库操作，还原 SQL 操作语句；跟踪数据库访问过程中的所有细节。提供数据库操作行为、应用服务器行为、终端录像实现事后审计，为追踪、惩罚犯罪份子提供强有力的证据。

(5) 报表管理

除了根据安全经验和行业需求提供了预定义的报表模板外，管理员还可利用自定义报表功能根据需要定制报表。此外还可将生成的报表发送到指定邮箱，方便查阅。此外报表支持导出成 PDF 格式文件。

(6) 审计日志管理

保存大量数据库审计日志的同时，还支持对早期的数据进行归档。当需要时可以通过数据回档的形式调阅早期的数据。解决了海量数据的有效存取的问题，为用户提供更全、更有效的数据。

## 1.4 系统登录

系统将系统角色划分为四类：系统管理员、系统审计员、系统安全员、系统监察员。每类角色对系统拥有不同的访问、控制权限。具体如下：

(1) 系统管理员（sys）

系统默认用户名及密码为：sys/sys。对系统的主要操作包括：

- 个人信息管理。
- 查看系统运行状态。
- 系统运行参数配置。
- 此外无权操作其他角色功能。

(2) 系统审计员（audit）

系统默认用户名及密码为：audit/audit。对系统的主要操作包括：

- 个人信息管理。
- 查看系统运行状态。
- 系统自身运行日志信息。
- 无权操作其他角色功能。

(3) 系统安全员（sec）

系统默认用户名及密码为：sec/sec。对系统的主要操作包括：

- 个人信息管理。
- 查看系统运行状态。
- 与业务有关的操作及信息查看。
- 无权操作其他角色功能。

(4) 系统监察员（mon）

系统默认用户名及密码为：mon/mon。对系统的主要操作包括：

- 个人信息管理。
- 与业务有关的操作及信息查看。
- 无权操作其他角色功能。

四类角色对系统的操作权限不同，分别被赋予了不同的权限，参见表 1-1。

**表1-1 各类角色权限分配**

| 一级菜单 | 二级菜单 | sys | audit | sec | mon |
|---|---|---|---|---|---|
| 监控中心 | 运行状态 | √ | √ | √ | - |
| | 安全态势 | - | - | √ | - |
| | 流量钻取 | - | - | √ | - |
| | 统方事件 | - | - | √ | √ |
| | 事件查看 | - | - | √ | - |
| | 入侵事件 | - | - | √ | - |
| | 监察视图 | - | - | - | √ |
| 审计中心 | 语句查询 | - | - | √ | - |
| | URL审计 | - | - | √ | - |
| | 行为审计 | - | - | √ | - |
| | SQL模板 | - | - | √ | - |
| | 因子监测 | - | - | √ | - |
| | 网络审计 | - | - | √ | - |
| | 对比分析 | - | - | √ | - |
| 报表中心 | 报表任务 | - | - | √ | √ |
| | 事件报表 | - | - | √ | - |
| | 统方报告 | - | - | √ | √ |
| | 报表查看 | - | - | √ | √ |
| 策略中心 | 监听配置 | √ | - | √ | - |
| | 事件定义 | √ | - | √ | - |
| | 对象管理 | √ | - | √ | - |

| 一级菜单 | 二级菜单 | sys | audit | sec | mon |
| --- | --- | --- | --- | --- | --- |
| | 客户端信息 | √ | - | √ | - |
| | 敏感信息 | √ | - | √ | - |
| | 事件响应 | √ | - | √ | - |
| | 三层关联 | √ | - | √ | - |
| | 入侵检测规则 | √ | - | √ | - |
| | 交换机信息 | √ | - | √ | - |
| 系统管理 | 网络配置 | √ | - | - | - |
| | 用户管理 | √ | √ | √ | √ |
| | 进程管理 | √ | - | - | - |
| | 日志响应 | √ | - | - | - |
| | 数据归档 | - | - | √ | - |
| | 调试工具 | √ | - | - | - |
| | 配置管理 | √ | - | - | - |
| | 系统信息 | √ | - | - | - |
| | 管理主机 | √ | - | - | - |
| | 运行日志 | √ | - | - | - |
| | 操作日志 | - | √ | √ | - |

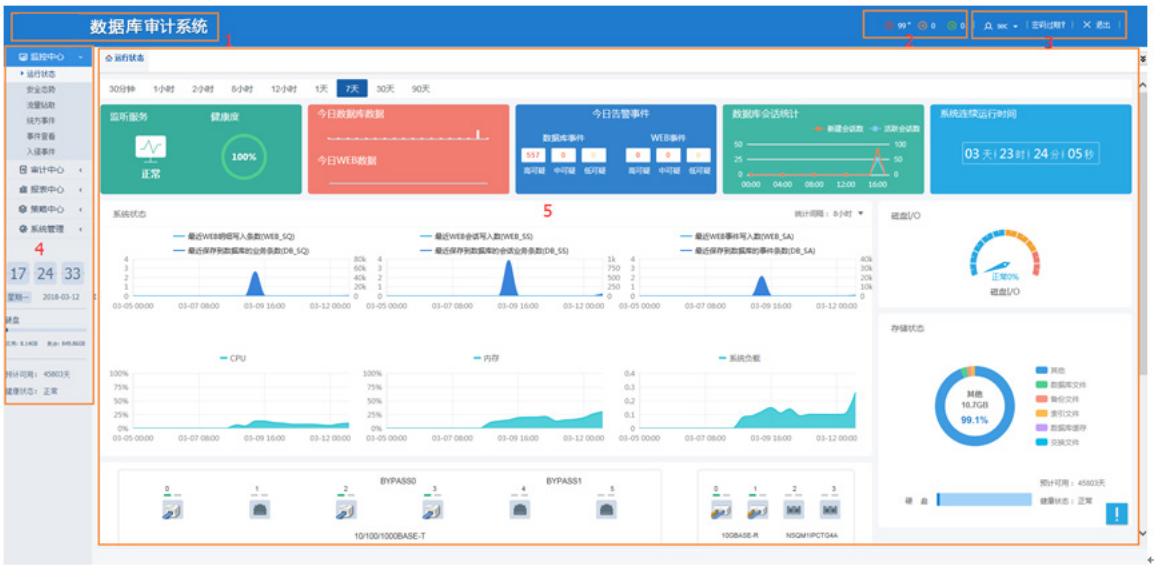
说明

sys、audit、sec、mon 是系统超级用户，四个超级户默认是不可以被删除，但可以被锁定（但要求创建一个与根用户一样的权限）。

各角色除了上表描述的权限外，还拥有对本组用户增删改查的权限。且 sys 就类似信息科人员，协助纪检科定义准确的统方规则。所以分配他们对象定义及事件定义的权限。

## 1.5 主界面说明

图1-2 主界面




上图是系统界面的分布图，每个区分别是：

1、产品版本信息；2、系统提示栏；3、账户信息；4、左栏菜单；5、功能操作区。

下面逐个介绍各个区的主要功能。

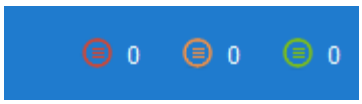
### 2. 产品版本信息

此处放置的是产品名称、Logo 及版本信息。本版是标准版。

### 2. 系统提示栏

本系统中放置了三个图标，分别显示了自系统运行时管理员未查看的高可疑、中可疑、低可疑事件的统计。单击对应的图标会跳转到“事件查看”界面，相关的内容可以参考“事件查看”部分的介绍。如下图所示从左到右依次是高、中、低可疑事件的状态提示。

图1-3 系统提示栏




当统计数量超过 99 条时，系统将显示“99+”，鼠标移动到在数值上可以看到事件的等级和发生统计结果。如下图所示

图1-4 悬浮提示

### 3. 账户信息

点击当前登录用户旁的下拉按钮可以更改当前用户密码和个人设置及锁定，如下图所示：

图1-5 账户信息


(2) 更改密码

点击<更改密码>后在弹出的[修改密码]对话框中输入旧密码重设密码，如下图所示：

图1-6 修改密码


(3) 个人设置

点击<个人设置>修改个人基本信息，具体内容如下图所示：

图1-7 修改个人信息


(4) 锁定

点击<锁定>后，系统将锁定在当前界面，无法操作，用户需要重新输入登录密码后才能正常操作，如下图所示：

图1-8 锁定状态

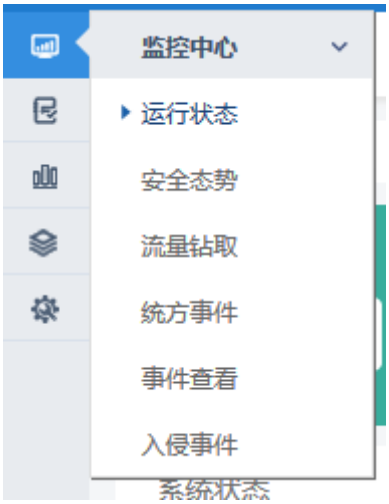

## 4. 左栏菜单

左栏是系统的菜单栏，点击后可以逐级查看菜单，点击二级菜单后在右栏功能操作区进行相关操作。默认为收缩，可点击展开。

左侧导航栏新增时间提示，将磁盘存储的使用情况、预计可用时间、系统健康状态等常用信息移至左侧栏展示。

图1-9 左栏菜单


监控中心
运行状态
安全态势
流量钻取
统方事件
事件查看
入侵事件
审计中心
报表中心
策略中心
系统管理
11
02
37
星期一
2017-12-11
硬盘
已用: 350 MB
剩余: 560.24GB
预计可用： 71711天
健康状态： 正常




### 5. 功能操作区

是系统主要工作区域，展示系统各种信息，及各项参数配置配置。

---

说明

建议使用火狐浏览器，以达最佳用户体验。

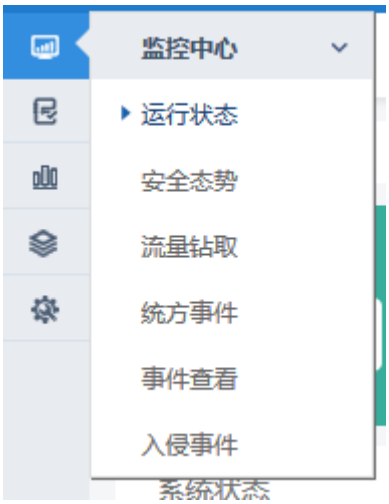
---

# 2 监控中心

## 2.1 概述

监控中心主要是监控系统状态。包括系统运行状态，最近发生的高可疑的事件进行监控。帮助管理员及时掌握系统的状态。如下图所示：

图2-1 监控中心




## 2.2 运行状态

在左栏菜单中[监控中心/运行状态]，功能操作区界面包含的内容：业务系统监听正常情况、今日审计数据量、今日告警事件数、设备运行健康度、无故障运行时间等设备状态，系统状态，系统资源使用情况，网络设备连接状态、监听网卡流量、登录日志等信息。通过查看可以观测系统的运行状态及健康状态。如下图所示：

图2-2 运行状态

下面逐个介绍各个部分：

## 2. 重要消息弹窗

点击右下角  按钮，即可展开重要系统通知。当侦测到磁盘错误、试用 license 过期、无配置备份、系统掉电、监听网卡断开重连等 17 类系统异常时，弹窗提示用户阅览，并为部分消息类型提供及时处理操作的跳转功能。如下图所示：

图2-3 重要消息弹窗


---

 注意

根据权限的不同，将提示不同的消息提示类型。此功能出现于所有界面。

---

### 3. 时间条

为运行状态页的展示提供 30 分钟、1 小时、2 小时、8 小时、12 小时、1 天、7 天、30 天、90 天等丰富的时间范围选项，如下图所示：

图2-4 时间条


当选择不同长度的时间范围项时，运行状态页、安全态势页中有关分析项的统计时间间隔也不同，如下图所示：

图2-5 时间选项


- 30 分钟、1 小时：统计时间间隔有 1 分钟、10 分钟。
- 2 小时、8 小时：统计时间间隔有 1 分钟、10 分钟、1 小时。
- 12 小时：统计时间间隔有 10 分钟、1 小时。
- 1 天：统计时间间隔有 10 分钟、1 小时、8 小时。
- 7 天：统计时间间隔有 8 小时、1 天。
- 30 天、90 天：统计时间间隔有 1 天、1 周。

### 4. 设备状态

监测业务系统监听正常情况、设备运行健康度、今日数据库审计数据、今日 WEB 审计数据、今日告警数据库事件数、今日告警 WEB 事件数、数据库会话统计、系统连续运行时间等设备状态，如下图所示：

图2-6 设备状态

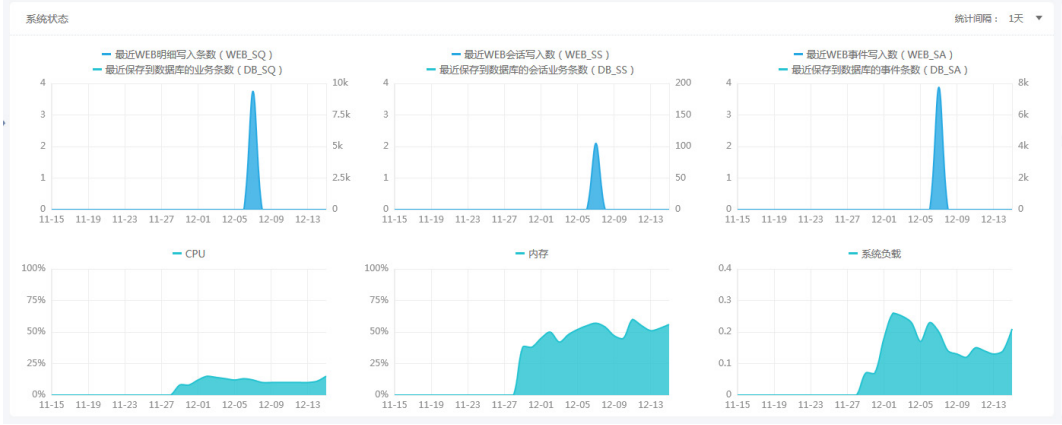

- 监听服务：显示业务系统监听服务是否正常。
- 健康度：显示系统运行情况、健康程度。

- 今日数据库审计数据：按小时统计每日零点开始的数据库审计数，鼠标停留可显示当小时的数据库审计数和昨日同时段的数据库审计数。
- 今日 WEB 审计数据：按小时统计每日零点开始的 WEB 审计数，鼠标停留可显示当小时的 WEB 审计数和昨日同时段的 WEB 审计数。
- 今日告警数据库事件：显示系统每日产生的高可疑、中可疑、低可疑数据库事件的统计，鼠标停留可显示具体明细数。
- 今日告警 WEB 事件：显示系统每日产生的高可疑、中可疑、低可疑 WEB 事件的统计，鼠标停留可显示具体明细数。
- 数据库会话统计：按小时统计每日零点开始的数据库会话数，鼠标停留可显示当小时的数据库新建会话数和当小时的数据库活跃会话数。
- 系统连续运行时间：自系统开机伊始，计算系统持续运行时间，系统重启后将重新开始计时。

### 5. 系统状态

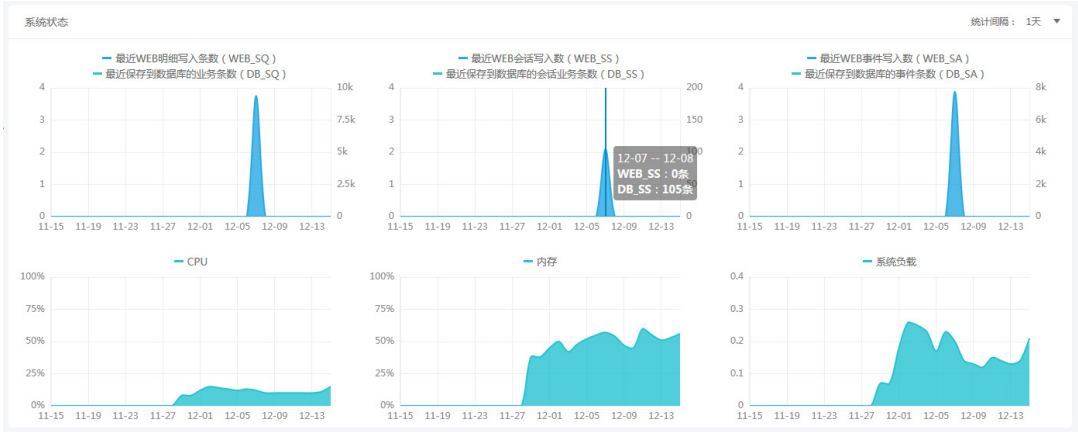
以曲线图的方式形象地展示处理及保存到 WEB 明细/数据库的业务、会话、预警、CPU、内存、系统负载等状态，当系统负载过高时需要引起管理员的注意，并采取相应的控制措施。统计时间间隔有 1 小时、8 小时、1 天，如下图所示：

图2-7 系统状态




将鼠标放在统计图上可以查看具体的数量，如下图所示：

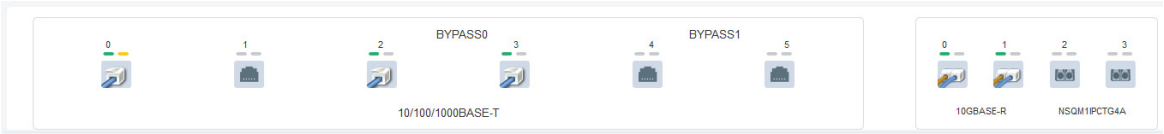
图2-8 具体数值




## 6. 网卡信息

展示与物理设备面板一一对应的网卡模拟展示图，根据实际连线情况实时展示网卡当前接线状态，并以水量方式展示网卡当前负载。如图如下图所示：

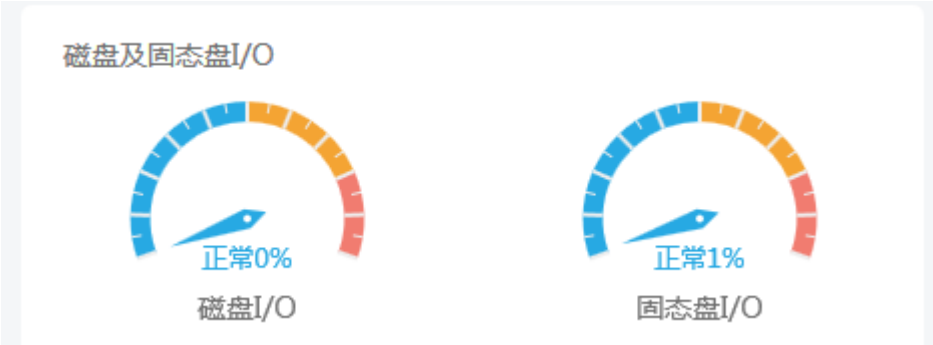
图2-9 网卡信息




## 7. 硬盘及固态盘 I/O

展示磁盘及固态盘的 I/O 利用率。如下图所示：

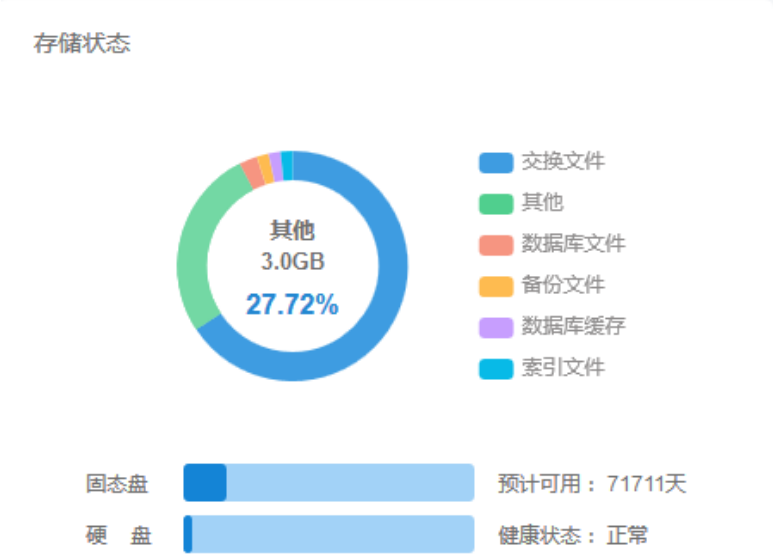
图2-10 硬盘及固态盘 I/O




## 8. 存储状态

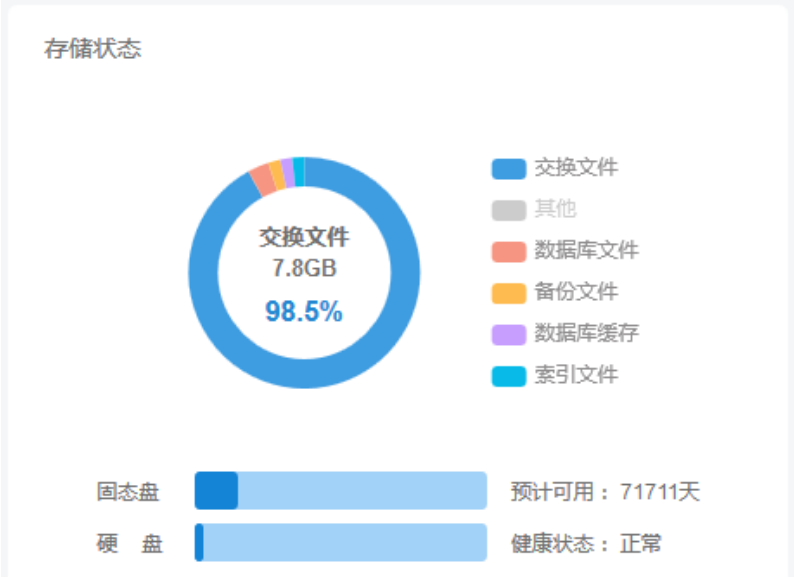
为磁盘提供数据库文件、交换文件、备份文件、数据库缓存等丰富的文件存储状态展示，显示空间使用情况、健康状态，并智能的预计剩余磁盘空间可用的天数供管理员参考。如下图所示：

图2-11 存储状态



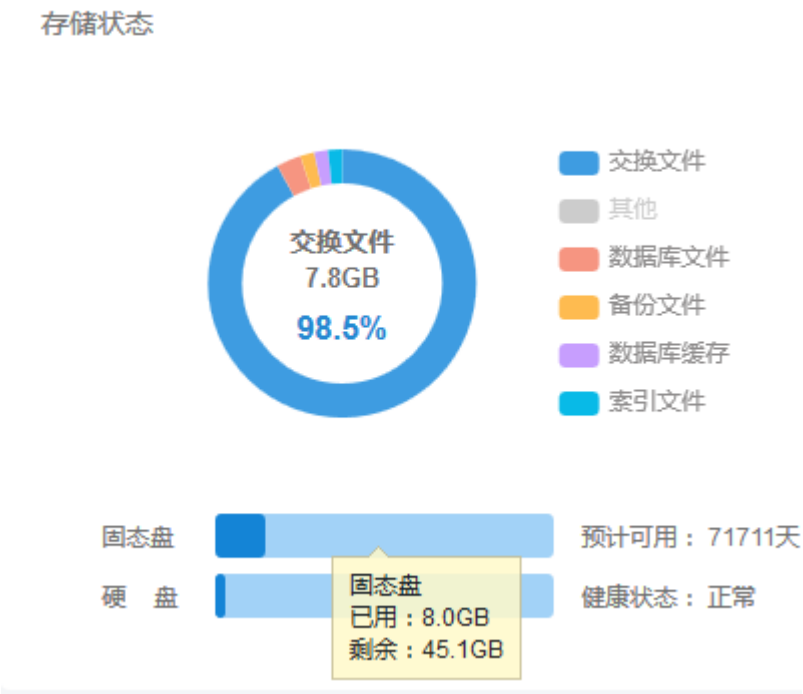

点击右侧图例按钮可设置该类文件存储状态进行隐藏或显示，如下图所示：

图2-12 隐藏选项




将鼠标放置在条形图上可以查看已用和剩余空间量，如下图所示：

图2-13 查看容量情况

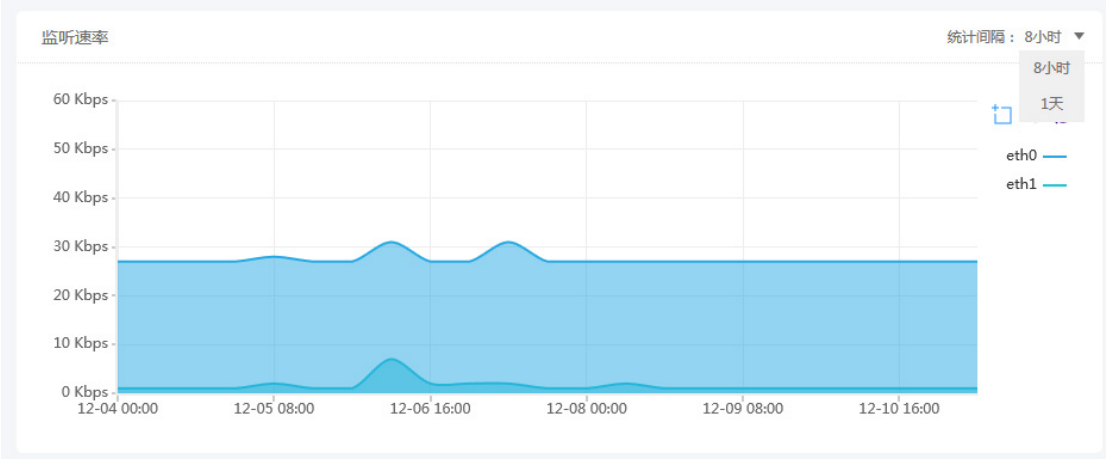



- 预计可用天数：根据系统运行情况，分析平均每天审计数据占用磁盘空间的百分比，通过与剩余空间比较，预算出系统磁盘空间的可用天数。
- 健康状态：当磁盘空间使用率小于 80%时，认定系统磁盘是正常状态，但使用率大于 80%是显示异常，需要管理员注意并采取措施进行控制。

## 9. 监听网卡流量

通过曲线图实时展示监听网卡的网络流量，统计时间间隔包括 8 小时、1 天，如下图所示：

图2-14 监听网卡流量




## 10. 登录日志

展示系统用户登录、动作的记录情况，具体参数如下图所示。

图2-15 登录日志

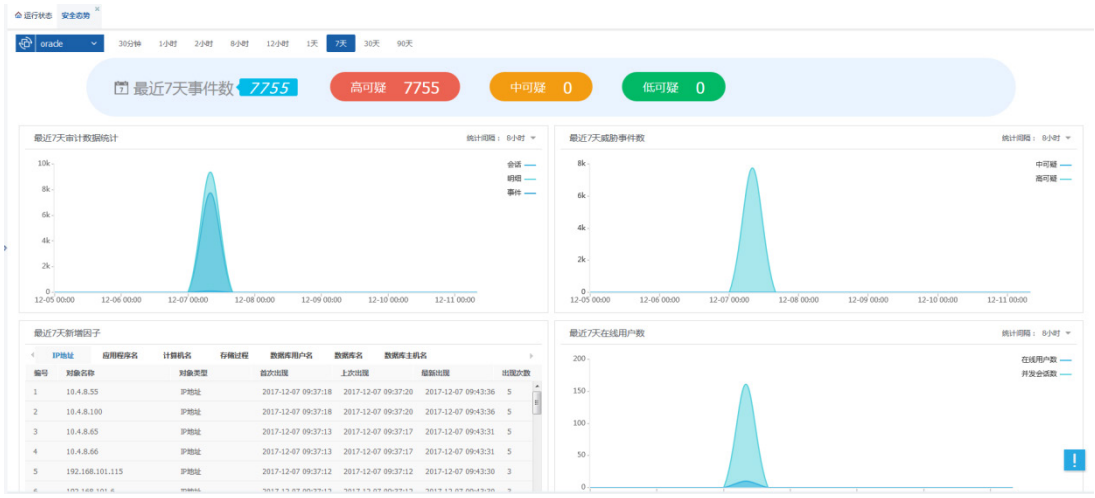
登录日志

| 时间 | 日志信息 | 行为 | 操作者 | 登录IP |
| --- | --- | --- | --- | --- |
| 2017-12-11 10:08:45 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.8.68 |
| 2017-12-11 10:01:09 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.8.220 |
| 2017-12-08 16:38:14 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.8.117 |
| 2017-12-08 15:07:16 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.8.33 |
| 2017-12-08 15:06:32 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.8.117 |
| 2017-12-07 16:47:08 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.10.101 |
| 2017-12-07 15:36:44 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.8.88 |
| 2017-12-07 14:47:27 | 登录系统成功 | 登录用户名为:sec | sec | 10.4.10.101 |

## 2.3 安全态势

在左栏点击[监控中心/安全态势]，在右栏的功能操作区中打开界面，根据业务系统及时间的不同，将最近发生的事件多元化地展现给用户。包含的内容有：告警事件列表、新增因子、威胁事件统计、审计数据统计、在线用户数统计、当前会话数、流量统计等信息。如图下图所示：

图2-16 安全态势界面




可根据业务和统计时间范围的不同，选择需要查看的业务系统某个时间范围内的分析情况，如下图所示：

图2-17 选择业务系统和时间范围


## 2.3.2 最近事件数

点击高、中、低可疑事件数，即可展开告警事件列表，从告警事件列表中可以看到事件发生的时间、地点、行为者，更多详尽的数据，协助管理员对事件进行核查、分析。如下图所示：

图2-18 最近事件数


在列表中点击某个记录后面的 事件追踪 按钮查看事件的详细信息。主要有：发生的时间、事件概述、件相关的客户端信息、服务端信息及其他关联的信息。如下图所示：

图2-19 事件追踪


## 2. 事件追踪

以表格的形式概要展示事件的相关信息，包括事件时间、概述、客户端信息、服务端信息、语句及语句翻译。各项信息描述如下：

- 事件时间：包括事件发生、结束时间，时间精确到时、分、秒。
- 事件概述：用通俗易懂的语言概括该事件的时间、地点、人物、事件，让用户快速了解该事件。
- 客户端信息：该事件相关的客户端信息，包括该终端的使用者 IP（或业务账号）、源端口、客户端 MAC 计算机名等协助管理员定位事件的主体，除此之外还有事件发生的地点，鼠标停留在事发地点旁的查看详细，可以查看事发的物理位置。如下图所示：

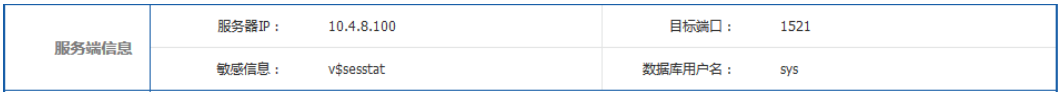
图2-20 客户端信息


说明

此处所展示信息内容，依据[策略中心/客户端信息]中配置。

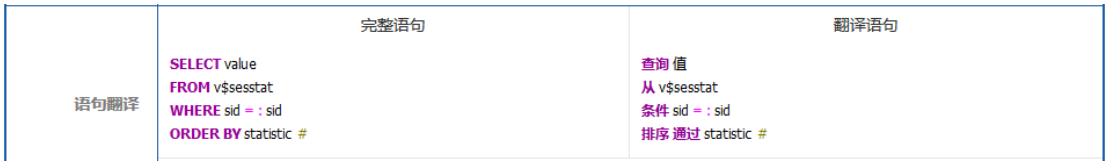
- 服务端信息：服务端信息包括：服务器 IP 地址，目标端口号，事件涉及的敏感信息，以及登录数据库的用户名。如下图所示：

图2-21 服务端信息




- 语句翻译：对触发规则的语句进行人性化的智能翻译，用户不必精通数据库也可以很容易看懂该事件的操作内容。如下图所示：

图2-22 语句翻译



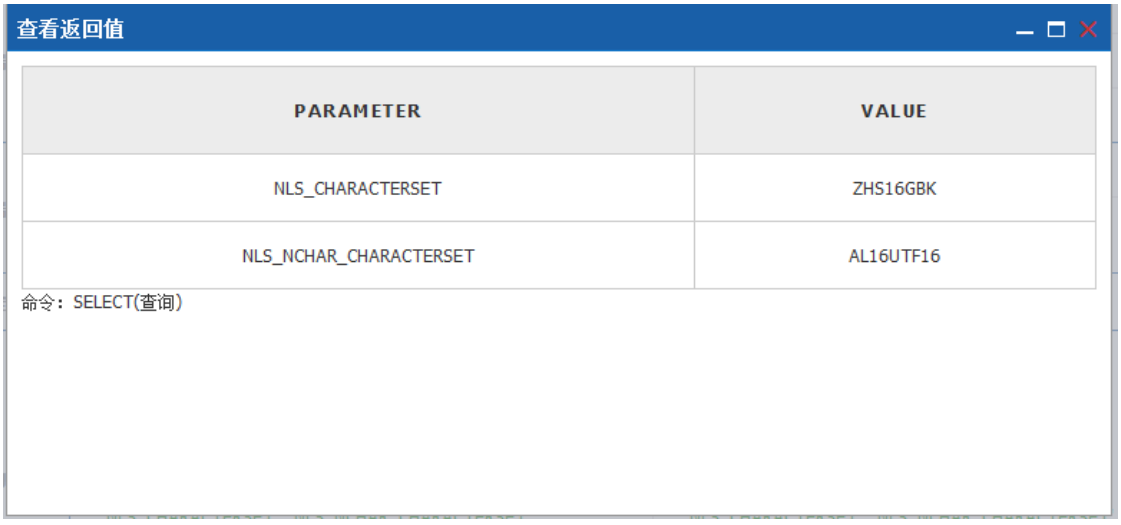

### 3. 其他操作

- 查看更多相关信息：点击<查看更多相关信息>可以查看完整的数据库访问行为，如下图所示：

图2-23 更多相关信息


- 查看返回值：点击<查看返回值>，可以查看操作后系统返回的详细信息。设备可自动将敏感信息进行掩码，用“*”替换其内容。

图2-24 查看返回值




- 设置为安全：将该事件设置为安全。该项设置只对本事件生效，未来发生同样的事件并不会被识别为安全事件。如下图所示：

图2-25 确认


- 添加到规则：将本事件设置为规则，并对未来发生的事件生效，如下图所示 2-26：

图2-26 添加到规则


- 设置某类语句为安全：在“事件追踪”页面中，点击<设置此类语句为安全>在弹出[确认]的对话框中点击<确定>，将会新增一条规则——把与该事件语句结构相同的语句设置为安全事件。

图2-27 确认


### 4. 关联信息

在此页面可以查看到与该事件关联的其他信息。如该会话中的其他数据库操作，终端录屏，Telnet 外连事件，FTP 事件，URL 关联。

说明

并不是每个事件的关联信息都有 FTP、Telnet、终端录像这些关联信息。

- 操作信息：展示与该事件关联的数据库操作信息，如下图所示 2-28：

图2-28 操作信息


- 终端录像：当发生风险事件时，系统向用户提供了事发前后 5 分钟，即共 10 分钟的终端录像。点击<下载>，可以将视频下载到本地进行播放。

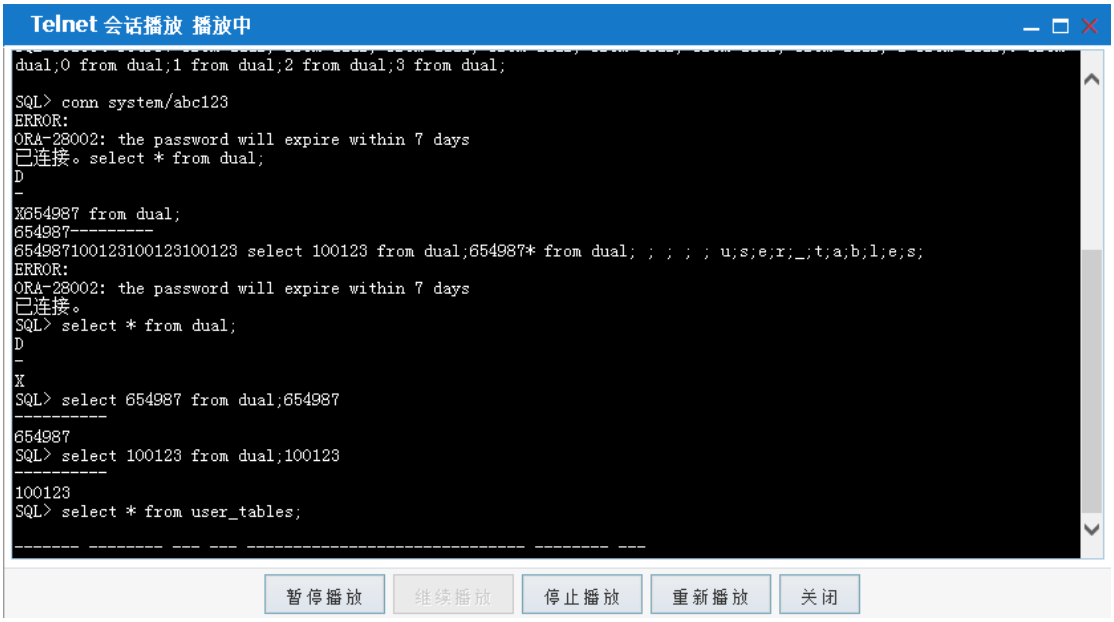
图2-29 终端录像


- Telnet 操作：系统审计到了与事件关联的 Telnet 时间，用户可以直接在界面中回放。

图2-30 Telnet 操作


单击某记录，即可查看：

图2-31 Telnet 会话播放

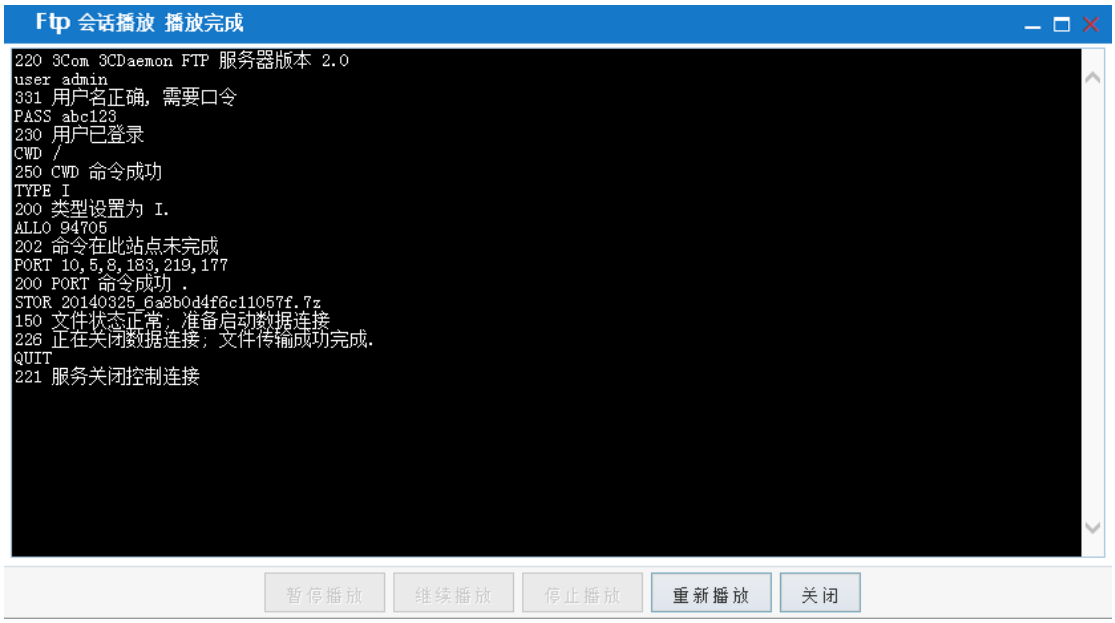



- FTP 事件

图2-32 FTP 事件


单击记录可以查看播放：

图2-33 FTP 会话播放

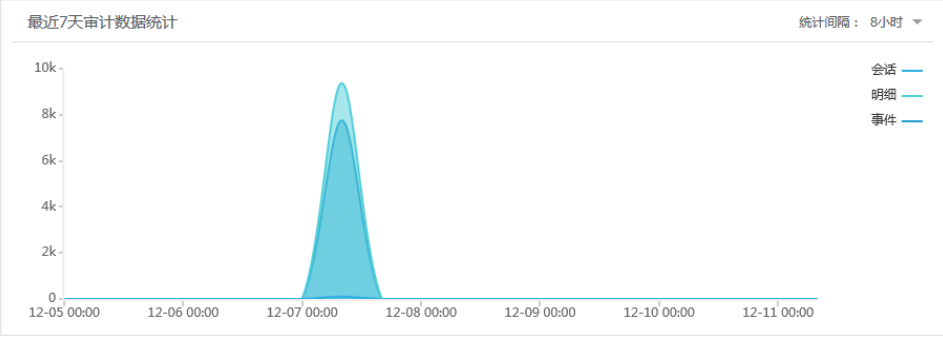



## 2.3.3 其他态势数据

### 1. 最近审计数据统计

对最近时间范围内审计到的会话数、明细条数以及触发预警的次数进行统计，如下图所示：

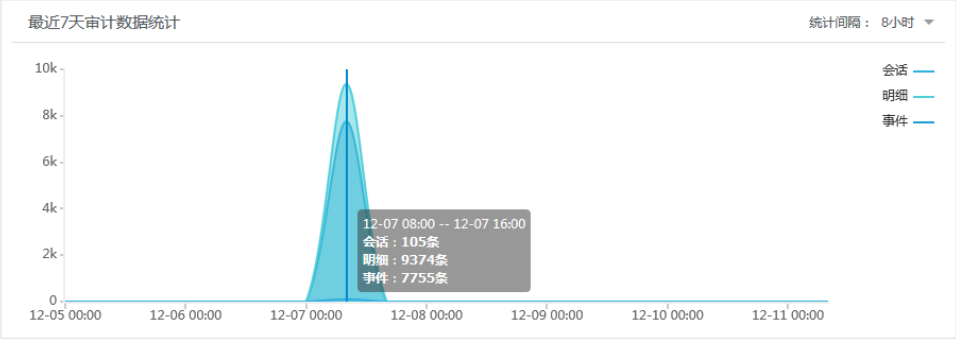
图2-34 最近审计数据统计




图中纵坐标的单位是 k（条）即千（条），M（条）即百万（条）

将鼠标放在统计图上可以查看具体的数量，如下图所示：

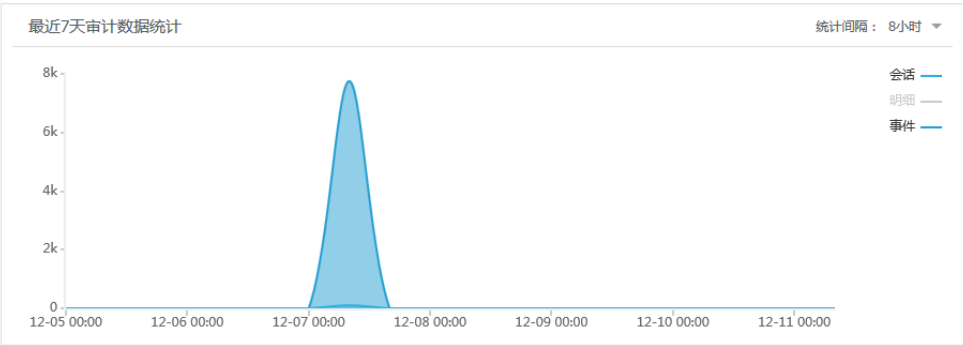
图2-35 具体数据




通过单击图表右侧的图例可以显示或隐藏该项数据的统计图；

当某项统计结果与其他两项有很大的差距导致在图上无法识别，除了将鼠标放置在图标上查看外，还可以通过将另外两项数据都隐藏掉来查看，如下图所示：

图2-36 隐藏选项



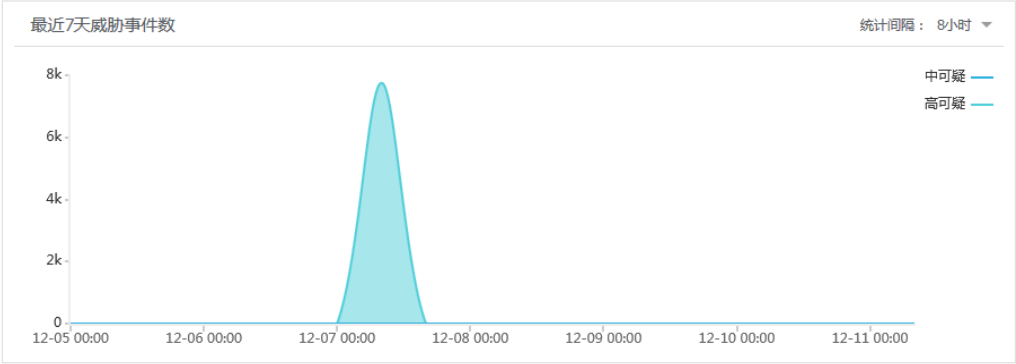

说明

由于“明细”统计结果数量与其他两项结果差距很大，隐藏了“明细”这类后可以清楚的看到其他两类的统计结果。

## 2. 最近威胁事件数

为管理员展示最近时间范围内系统发生的高、中可疑风险事件趋势统计图，可快速掌握最近时间范围内事件发生的“高峰期”，如下图所示：

图2-37 最近威胁事件数




说明

鼠标暂定可显示相关信息，点击右侧的图例可以隐藏或显示某类事件统计图。

### 3. 最近新增因子

监测最近统计时间范围内，各类因子对象的创建、更新情况，提供发现新增因子的提醒，以因子名称表现页显示红点的方式展示，方便查看。如下图所示：

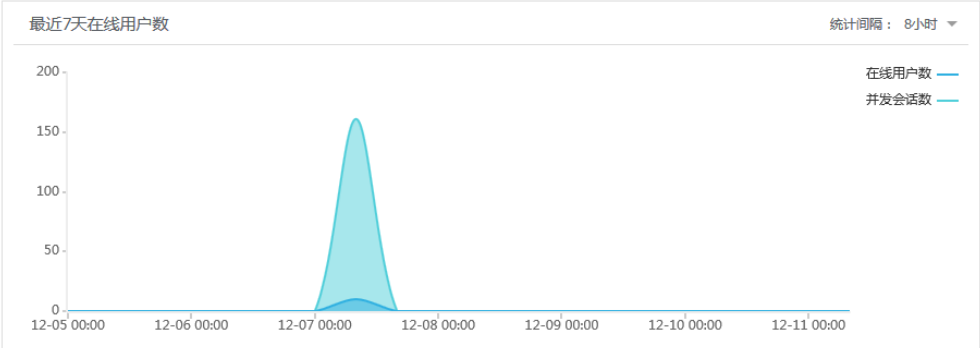
图2-38 最近新增因子


| 编号 | 对象名称 | 对象类型 | 首次出现 | 上次出现 | 最新出现 | 出现次数 |
|---|---|---|---|---|---|---|
| 1 | 10.4.8.55 | IP地址 | 2017-12-07 09:37:18 | 2017-12-07 09:37:20 | 2017-12-07 09:43:36 | 5 |
| 2 | 10.4.8.100 | IP地址 | 2017-12-07 09:37:18 | 2017-12-07 09:37:20 | 2017-12-07 09:43:36 | 5 |
| 3 | 10.4.8.65 | IP地址 | 2017-12-07 09:37:13 | 2017-12-07 09:37:17 | 2017-12-07 09:43:31 | 5 |
| 4 | 10.4.8.66 | IP地址 | 2017-12-07 09:37:13 | 2017-12-07 09:37:17 | 2017-12-07 09:43:31 | 5 |
| 5 | 192.168.101.115 | IP地址 | 2017-12-07 09:37:12 | 2017-12-07 09:37:12 | 2017-12-07 09:43:30 | 3 |
| 6 | 192.168.101.6 | IP地址 | 2017-12-07 09:37:12 | 2017-12-07 09:37:12 | 2017-12-07 09:43:30 | 3 |

### 4. 在线用户数

实时监控系统当前在线用户数量、并发会话数量，如下图所示：

图2-39 在线用户数



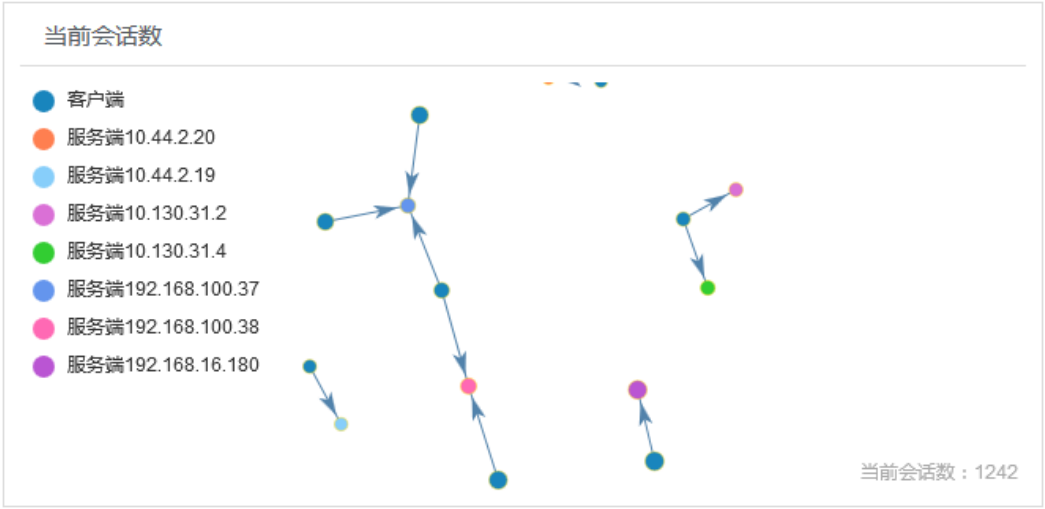

说明

鼠标暂定可显示相关信息，点击右侧的图例可以隐藏或显示某类事件统计图。

### 5. 当前会话数

以点-线的形式描述当前服务器与客户端的连接关系，由客户端指向服务端，如下图所示：

图2-40 当前会话数

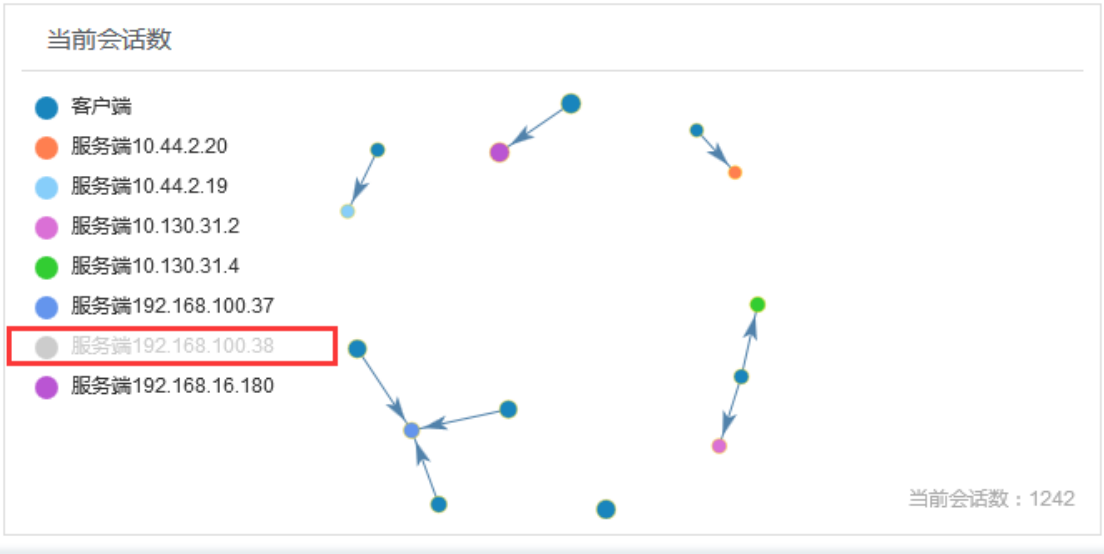



图表左侧是服务端和客户端的图例，右侧是它们之间的连接关系，图中的节点表示不同的客户端或服务器，节点之间的连线表示会话连接。

- 隐藏或显示某节点

  点击图例中的各点可以使该点在右侧连接关系图中隐藏或显示，如下图所示是隐藏了服务端192.168.100.38后，其他服务端与所有客户端的连接关系。

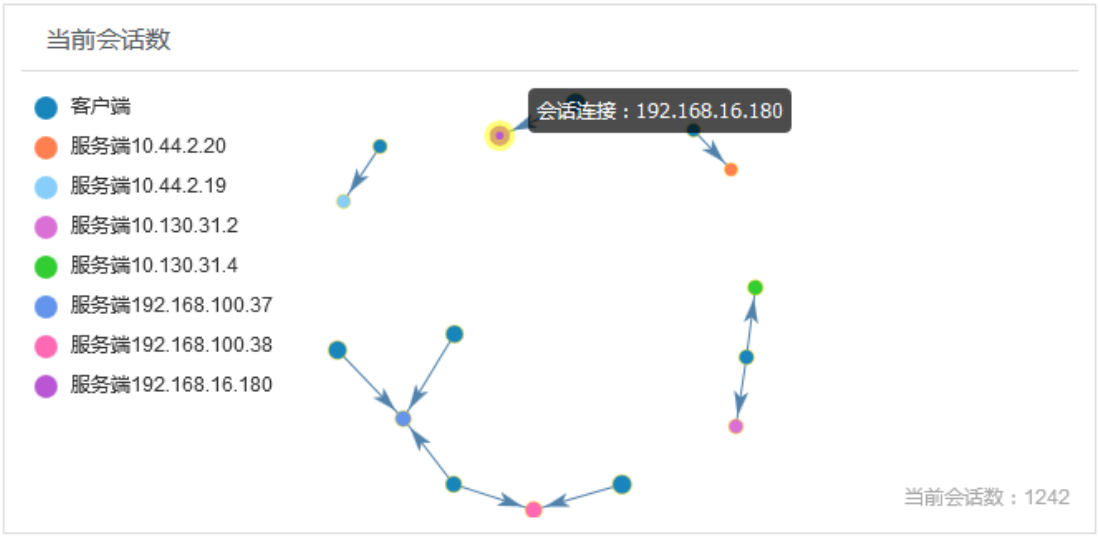
图2-41 隐藏数据




- 查看节点信息

  鼠标停留在连接关系图某节点上会显示该节点是客户端或服务器以及它的 IP 地址。

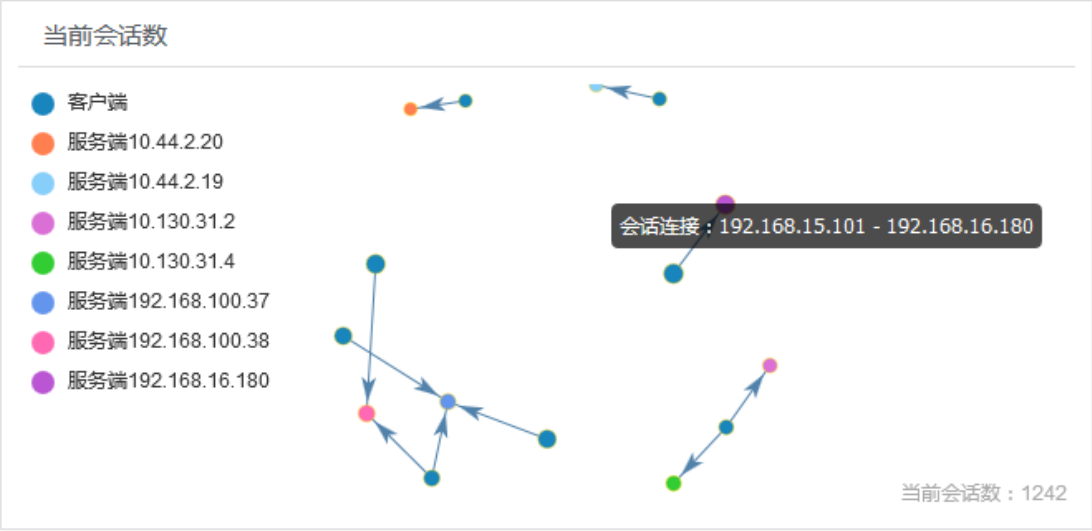
图2-42 具体数据




- 会话信息

  鼠标停留在某连线上，系统会展示该会话连接的双方。如下图所示：

图2-43 会话信息

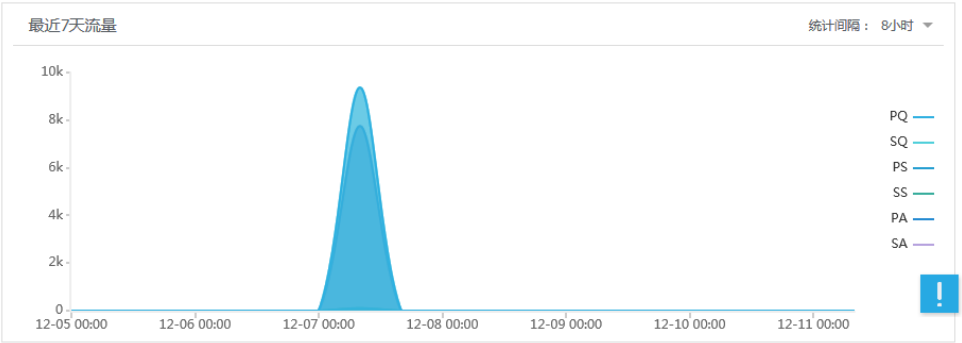



说明

拖拽连接关系图中的节点可移动该节点而不影响原有的连接关系。

## 6. 最近流量

图2-44 最近流量




右侧图例及各项的含义：

- PQ：最近已处理的业务条数。
- SQ：最近已保存到数据库的业务条数。
- PS：最近已处理的会话业务条数。
- SS：最近以保存到数据库的会话业务条数。
- PA：最近触发的预警条数。
- SA：最近已保存到数据库的预警条数。

说明

鼠标暂定可显示相关信息，点击右侧的图例可以隐藏或显示某类统计图。

## 2.4 流量钻取

默认向用户提供了系统的八个数据统计表，让用户展示系统相关数据统计，便于用户快速了解业务系统运行情况。流量钻取默认包括以下统计信息：

- 在线会话信息。
- 告警事件类型统计。
- 告警事件级别统计。
- 数据库用户名统计。
- 应用程序名统计。
- 客户端计算机名统计。
- 操作方式统计。
- 执行时长大于 20 秒语句统计。

除“在线会话信息”外，报表若不希望统计信息在此页面展示，用户可以到[报表中心/报表任务]中修改报表任务，并将发送到流量钻取项前的钩去掉。

此外用户也可以将流量周期统计报表发送到[监控中心/流量钻取]中展示，但要求报表对象列表中的统计对象只能有一个。具体操作可以到[报表任务]“新建流量周期统计报表”中查阅。

点击[监控中心/流量钻取]，进入界面：

图2-45 流量钻取

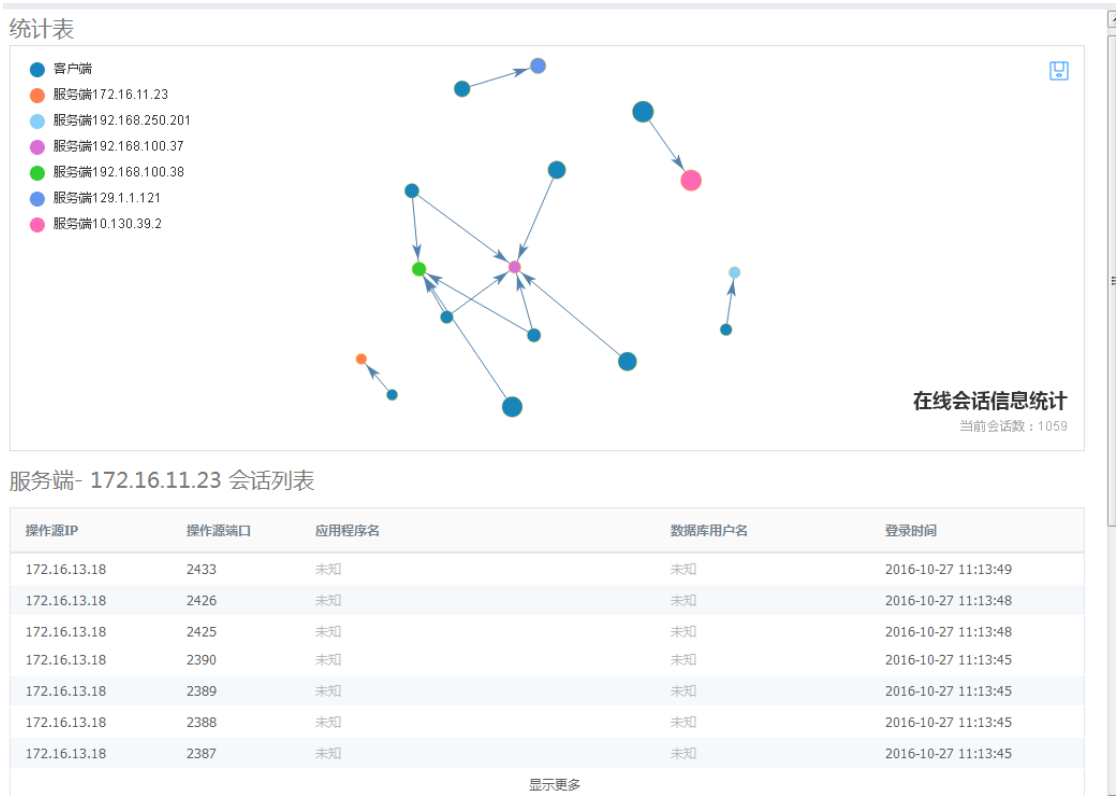

左侧是统计表类型，右侧是统计表的内容，每个统计表都分两个模块：统计图表和详细信息表。在统计表中会有以下操作：

-  ：数据视图按钮，点击后以数据的形式展示图表信息。
-  ：还原按钮，图表中的信息可以拖拽，可以按此按钮恢复到原样。
-  ：保存为图片按钮，将统计图表保存为图片形式。点击该按钮后，右击弹出的图片将图片另存到自定义的目录下。

## 2.4.2 在线会话信息

在线会话信息统计的是当天凌晨点开始的 24 小时内会话信息，以点-线的形式描述当前服务器与客户端的连接关系。并增加了详细的会话列表。如下图所示：

图2-46 在线会话信息




说明

此处功能与运行状态中的[当前会话数]有点区别，后者具有实时性，并以一定频率实时刷新。

(2) 在线会话信息统计

图表的操作方式与 2.3 安全态势中的[当前会话数]一致，这里就不在重复描述。

(3) 会话列表

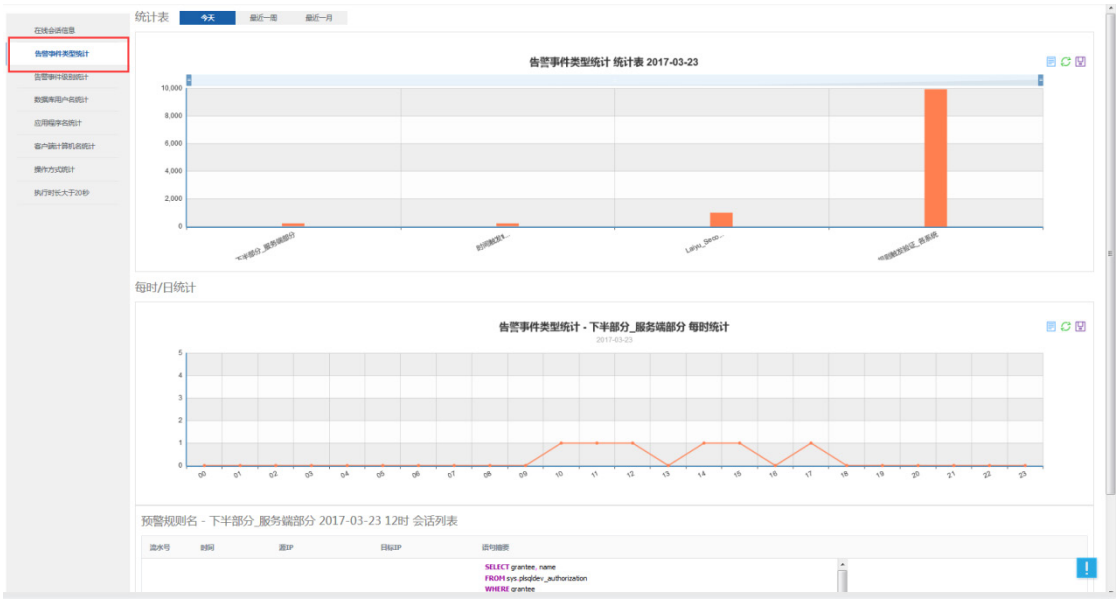
点击某个节点（客户端或服务端），将会以该节点为中心展示与它相关的会话信息。例如，上图中展示的是当天与服务端 172.16.11.23 相关的所有会话信息。

点击<显示更多>可以查看更多信息。

### 2.4.3 告警事件类型统计

对触发告警的事件类型分类统计，统计范围包括今天、最近一周、最近一月三种。如下图所示：

图2-47 告警事件类型统计




(2) 统计图表

- 今天：今天凌晨至 24 点统计情况。
- 最近一周：最近七天的统计情况。
- 最近一月：最近 30 天的统计情况。

(3) 详细信息

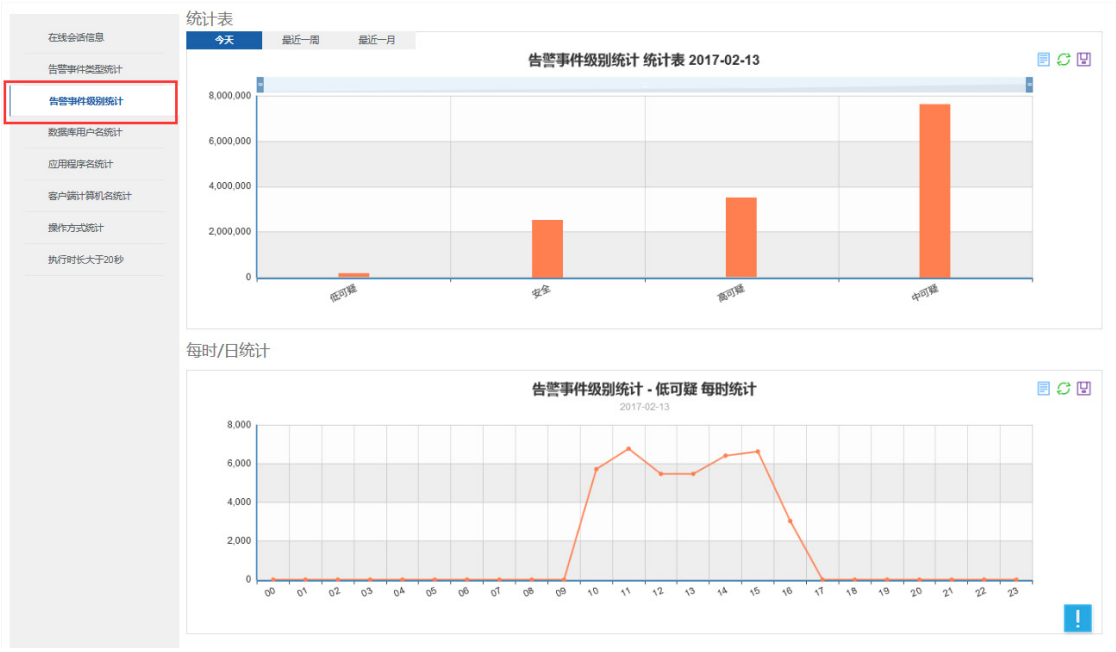
统计表中点击某个统计项，下图将会展示该项的详细信息，如上图中：展示的是“今天”告警事件的类型统计，点击直方图“下半部分_转换部分”，下方展示今天该类事件在“今天”某时发生的具体事件。

图2-48 告警事件类型详细信息

### 2.4.4 告警事件级别统计

对已发生的事件按告警级别进行统计。界面如下图所示：

图2-49 告警事件级别统计

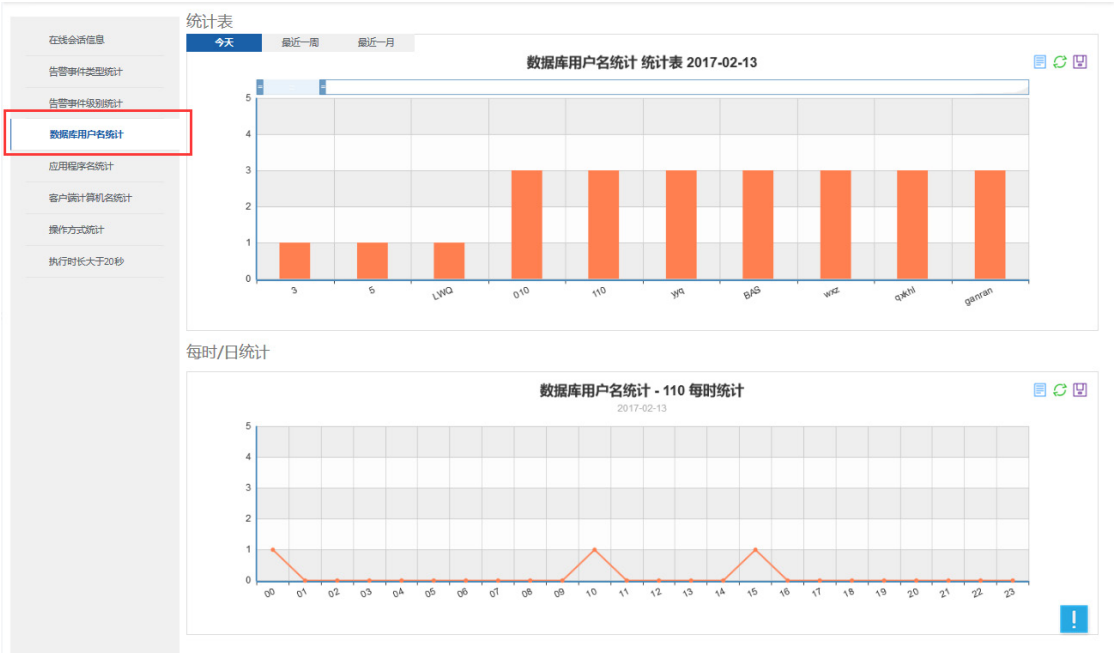



具体操作方式与告警事件类型统计相似。这里不再赘述。

### 2.4.5 数据库用户名统计；

统计各数据库用户及其访问数据库的次数。

图2-50 数据库用户名统计




说明

上图是数据库用户名访问情况统计，下表展示的是具体某个用户名访问数据库的时间趋势。

## 2.4.6 应用程序名统计

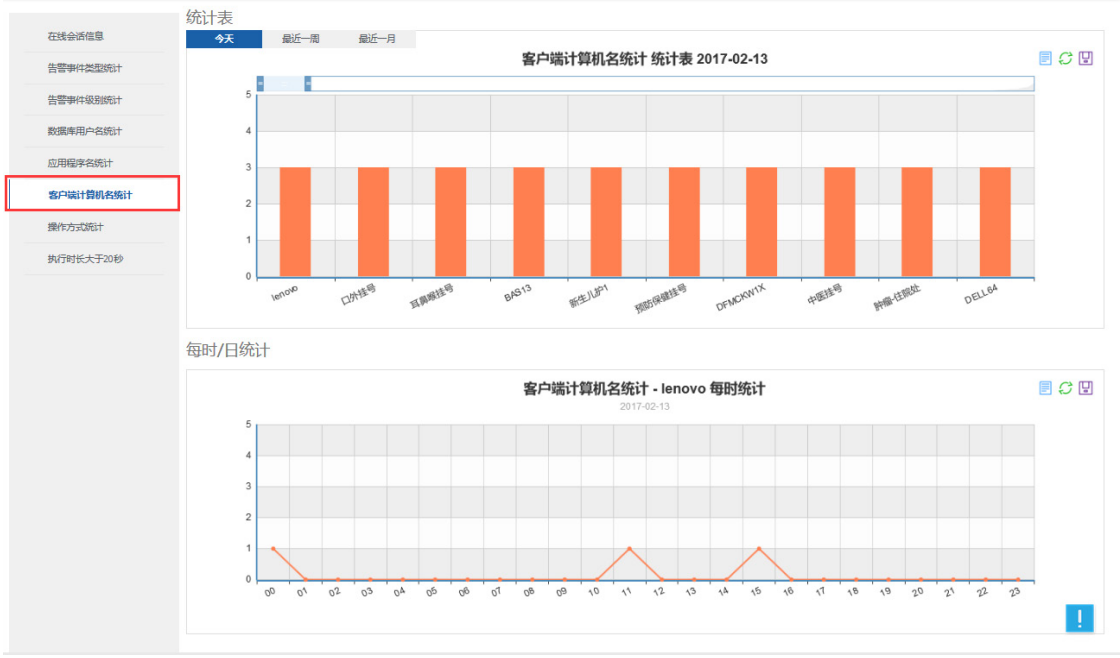
统计访问数据库的所有应用程序名。点击某个应用程序可以查阅该程序访问的时间趋势。界面如下图所示：

图2-51 应用程序名统计


## 2.4.7 客户端计算机名统计

统计连接到数据库的客户端计算机名称，点击某个计算机名可查阅它访问数据库的时间点。界面如下图所示：

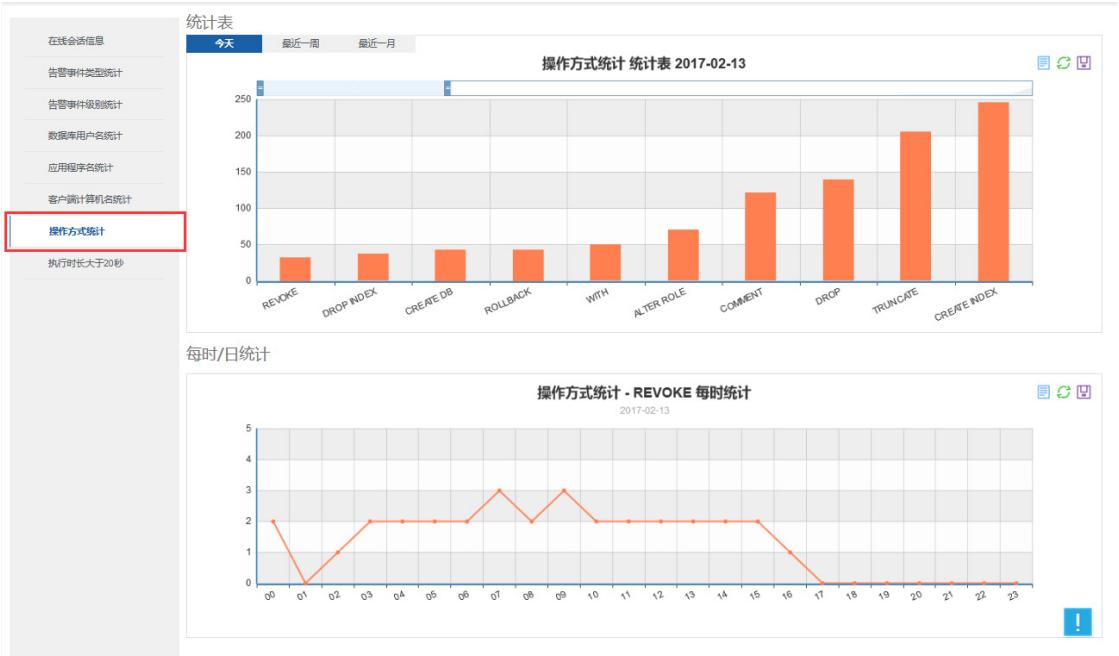
图2-52 客户端计算机名统计



## 2.4.8 操作方式统计

对数据库操作方式进行统计，用户可通过查看统计结果初步判断是否有异常操作。

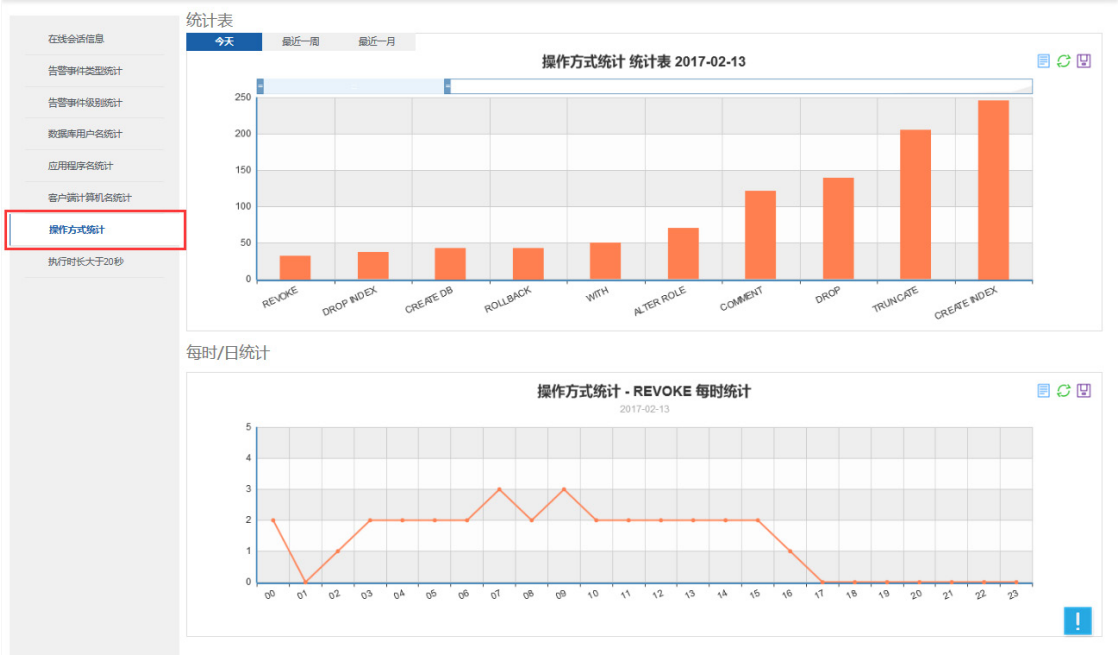
图2-53 操作方式统计




## 2.4.9 执行时长大于 20 秒

日常工作中对数据库的操作都比较简单，执行时间都比较短。对于大于 20 秒的操作是异常的，很可能是风险事件，用户借助统计结果初步判定哪些是风险事件。

图2-54 执行时长大于 20 秒




## 2.5 统方事件

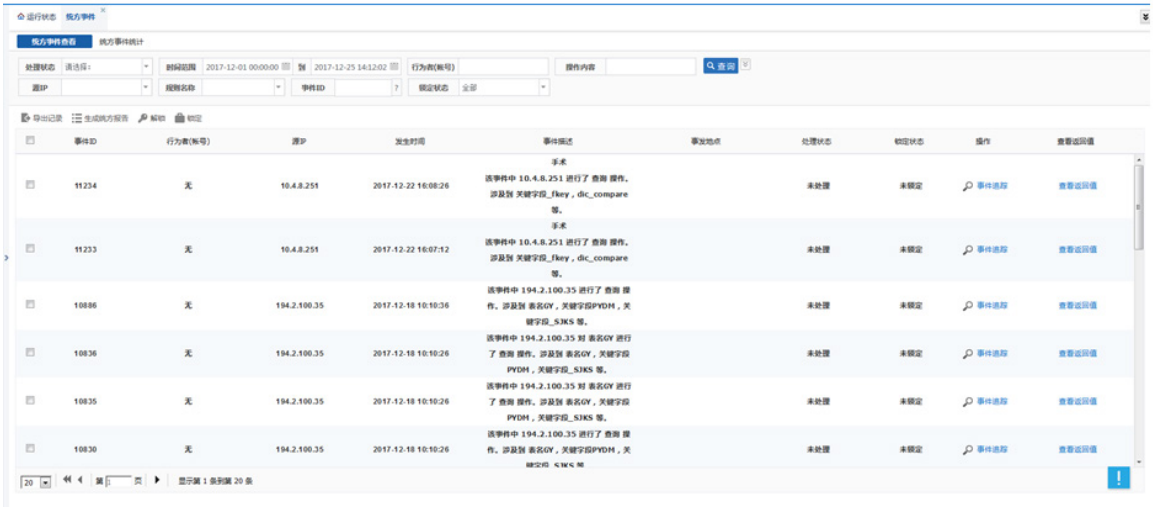
向用户展示发生可疑的统方事件，并对事件的时间、地点、人物、内容进行追踪、回溯。若该组织机构被上级机构纳入集中管理平台中，系统发生的统方事件将会被同步到集中管理平台，上级机构的监管人员可以随时了解该系统的动态。

统方事件必须是高可疑事件，基于高可疑事件的基础上要满足至少两个不同的敏感信息的配置，即可触发统方事件。

### 2.5.1 统方事件查看

左栏点击监控中心/统方事件，右栏的操作功能区打开统方事件查看界面。用户可以根据关键字进行检索，查询条件主要有：处理状态、发生的时间范围、行为者（帐号）、操作内容、规则名称、事件 ID，锁定状态等。统方事件提供查看返回值功能，可通过点击<查看返回值>按钮，查看返回值信息。界面如下图所示：

图2-55 统方事件查看



## 2. 事件追踪

点击某个记录后面的 事件追踪 按钮查看事件的详细信息。功能与本文档中“安全态势”中的事件追踪功能基本一致，唯一不同的是事件的处理的动作，如下图所示：

图2-56 事件查看/实时监视页面

图2-57 统方事件页面


如上图所示，在统方事件模块中管理员“事件追踪”页面中除了可以查看更多相关信息、查看返回值，还可以人工对事件进行分类处理。

通过在事件追踪页面对事件发生的时间、地点、人物、内容，以及如该会话中的其他数据库操作、终端录屏、Telnet 外连事件、FTP 事件、URL 关联等信息进行综合分析后，可以人工对事件进行进一步的判断、处理。人工处理即可将该事件“设置为统方”、“设置为疑似统方”、“设置为非统方”。若都没有进行分类，在统方事件模块中事件的状态被标识为未处理。

- 设置为统方：通过综合分析，认为证据充足，将该事件人工判断为统方事件。
- 设置为疑似统方：通过综合分析，认为该事件可能是统方事件。
- 设置为非统方：经分析，认为该事件不是统方事件。
- 设置为合规统方：经分析，认为该事件是合规统方事件。

### 3. 查看返回值

通过配置[监听配置]页面中业务系统的返回值配置，可在统方事件中展示语句的返回值信息

图2-58 查看返回值


(2) 导出记录

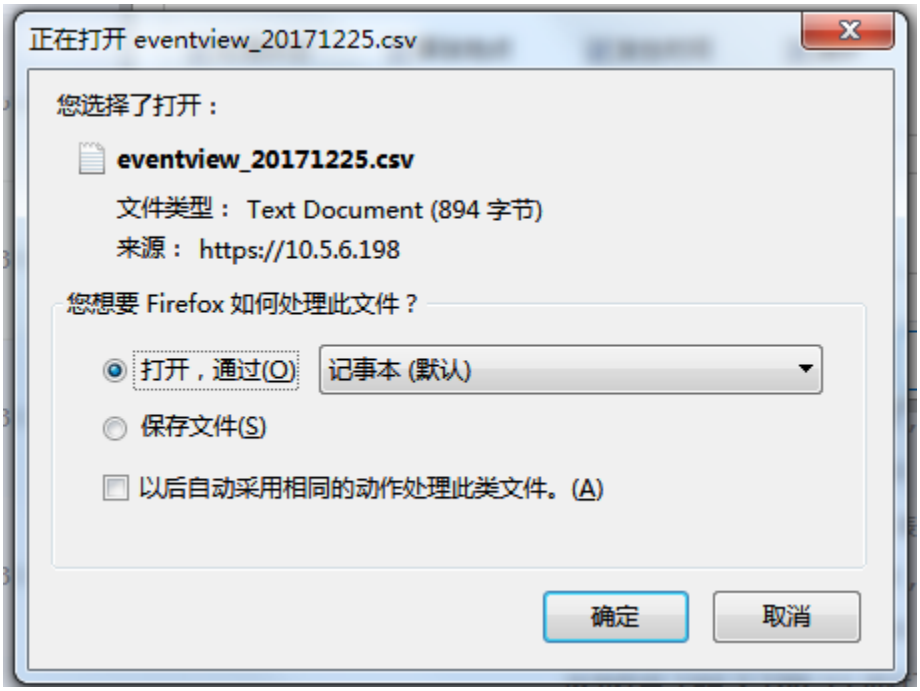
将查询的结果按照用户的要求导出。点击 导出记录 按钮弹出导出设置对话框如下图所示：

图2-59 导出记录设置


- 导出记录设置：可以设置导出选中的或所有查询结果的记录。默认是选择导出选中记录。
- 导出项设置：通过勾选展示列表中的字段来设置导出记录的各项内容，默认是导出可疑程度、物理地点、发生时间、行为者、事件描述这五个关键信息。
- 导出文件格式设置：设置导出文件格式，选则导出个时候如果没有弹出框可能是浏览器阻止了弹出框。

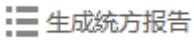
  点击确定按钮后，在弹出框中可以选择直接打开或下载，如下图所示：

图2-60 下载提示




(3) 生成统方报告

统方报告中展示了某个事件的相关信息，并对其进行分析、总结。报告包含了这些内容：报告基本信息，事件基本信息，事件描述以及系统对该事件的分析总结。

勾选统方事件后点击 

按钮，系统自动生成事件统方报告并在新的页面打开。如下图所示：

图2-61 统方报告

统方事件风险分析

（版本Ver 1.0）

保存

编制人：

编制单位：

创建日期：2017-12-25

• 基本信息：

"统方"特指在医药灰色产业链中，为商业目的的"统方"，其主要指医院中个人或部门为医药营销人员提供医院或部门在一定时期内临床用药量统计信息，供其作为发放药品回扣等不良违法行为的重要参考依据。

本报告根据先前定义的关键敏感信息，通过网络旁路的捕包分析，截获该疑似事件，关键信息如下：

| | | | |
|---|---|---|---|
| 发生时间 | 2017-12-18 10:10:26 | 事件ID | 10790 |
| HIS数据库 | 194.1.3.1 | 中间件服务器 | 无 |
| 来源用户 | 194.2.100.35 | 使用工具 | bqgl.exe |
| 触发条件 | 查询返回结果中包含以下敏感内容：gy_ksdm | | |

• 事件描述：

该事件中 194.2.100.35 对 表名GY 进行了 查询 操作。涉及到 表名GY，关键字段PYDM，关键字段_SJKS 等。

• 分析总结：

该用户利用HIS的 bqgl.exe 模块进行了相关操作，疑似程度高，请重点关注。

• 原始数据：

SELECT GY_KSDM.KSMC, GY_KSDM.PYDM, GY_KSDM.KSDM, GY_KSDM.SJKS FROM GY_KSDM WHERE GY_KSDM.KSDM > 0

- 报告基本信息：用户填写报告编制人、编制单位、创建时间后，可以点击报告标题旁的“保存”按钮保存该报告。已保存的报告可以在[统方事件/统方报告]中检索、查阅。

- 事件基本信息：事件基本信息中概述了统方事件及其危害，并提供了该统方事件的基本信息，主要包括：发生时间、涉及的 HIS 数据库地址、中间件服务器地址、发起该事件的用户（IP 地址），以及该用户所使用的工具，以及该事件的触发条件。
- 事件描述：使用通俗易懂的语言文字对事件进行概述。
- 分析总结：系统综合报告中的与事件相关的所有信息，对该事件进行总结，为管理员提供处理该事件的建议。
- 原始数据：记录该事件原始操作语句数据。

(4) 锁定

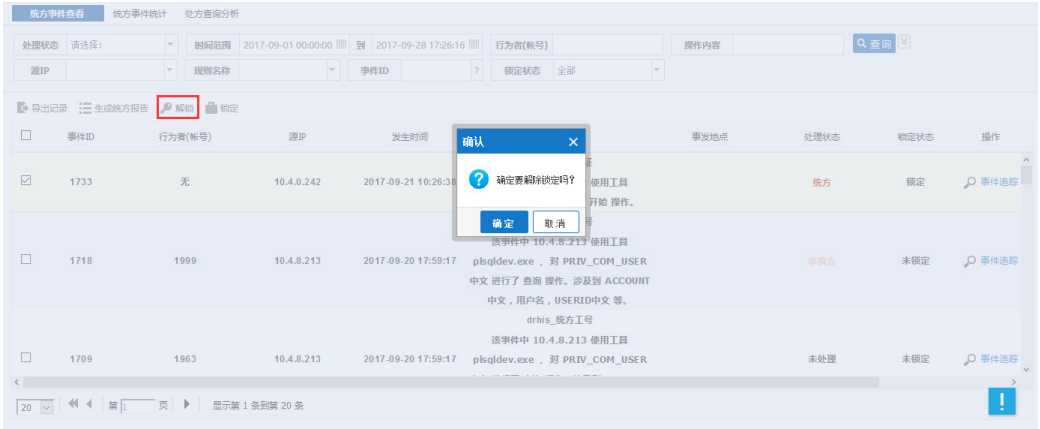
统方事件提供永久保存功能。如某事件需长期保存，勾选该事件，点击“锁定”按钮，提示是否锁定，确认后，该事件被锁定，系统不会自动删除该事件。

图2-62 锁定


(5) 解锁

如若锁定的某事件无需长期保存，勾选该事件，点击“解锁”按钮，提示是否解锁，确认后，该事件被解锁，系统到期会自动删除该事件。

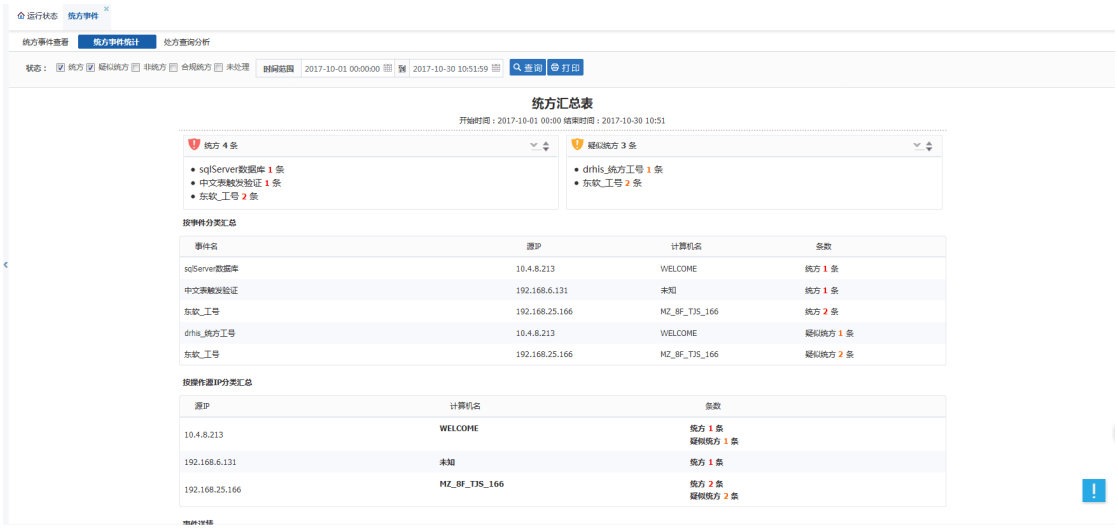
图2-63 解锁



## 2.5.2 统方事件统计

左栏点击[监控中心/统方事件]，右栏的操作功能区打开统方事件统计界面。用户可根据事件状态、时间范围进行检索，结果统计汇总到下方列表，如下图所示：

图2-64 统方事件统计




## 2.5.3 处方查询分析

提供处方查询分析功能，以便监察人员核实统方事件，快速定位相关责任人。点击左侧菜单栏，[监控中心/统方事件]，右侧的操作功能区打开处方查询分析界面。用户可根据选择月份，查询总次数最多的前 N 条，行为者（帐号），查询次数等进行查询。

在 API 页面，启用医生工号，并且配置好所要分析统计的统方 SQL 模板编码即可产生相应的处方数据

结果显示如下图所示：

图2-65 处方查询分析


(2) 处方查询统计（总次数）

统计查询月及其前 2 月每月的处方查询的总次数，协助判断。如下图所示：

图2-66 统计

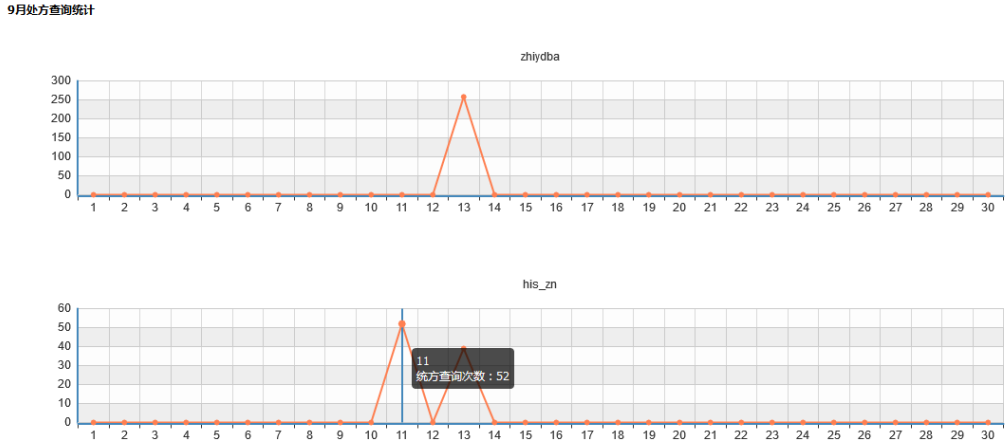
9月处方查询统计（总次数）

| 序号 | 行为者（工号） | 9月次数 | 8月次数 | 7月次数 |
|---|---|---|---|---|
| 1 | zhiydba | 258 | 0 | 0 |
| 2 | his_zn | 91 | 14 | 0 |
| 3 | sd_Hospital | 18 | 14 | 0 |
| 4 | 未知 | 15 | 0 | 0 |
| 5 | scott | 12 | 15 | 0 |
| 6 | SD_HOSPITAL | 9 | 13 | 0 |

(3) 处方查询统计

按日统计各月各行为者处方查询的次数，当鼠标停留时可显示当天的处方查询次数。如下图所示：

图2-67 图表




(4) 处方查询分析信息

用户可点击某个行为者（帐号）的趋势图中某一时间段，可弹出该行为者的处方详细分析信息。

图2-68 处方查询分析信息

**处方查询分析信息**

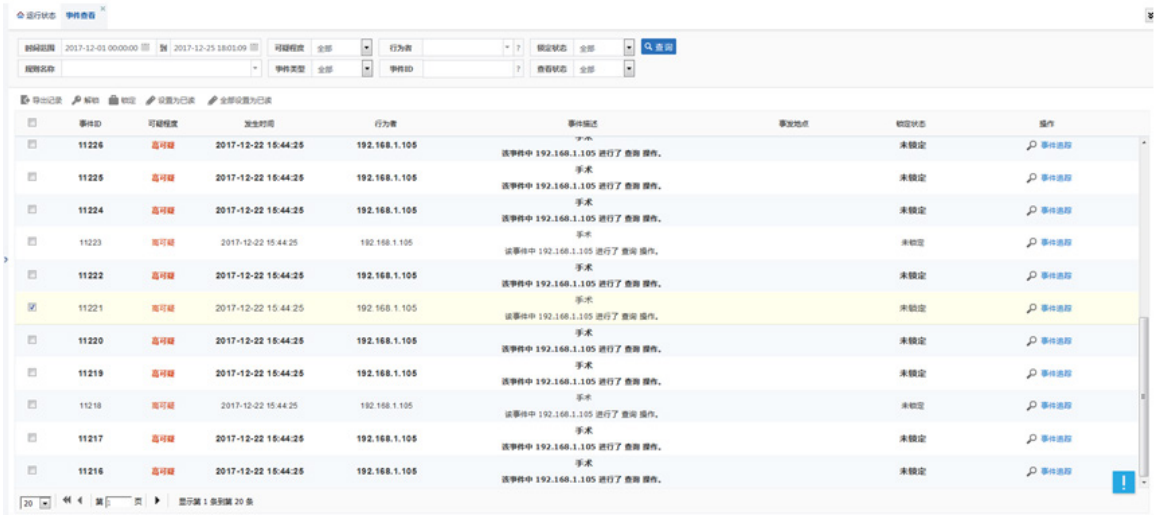
| 编号 | 时间 | 操作源IP | 计算机名 | 应用程序名 | 数据库用户名 | 语句摘要 |
|---|---|---|---|---|---|---|
| 1 | 2017-09-11 09:30:55 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Person.SelectByID' |
| 2 | 2017-09-11 09:30:55 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.DepartmentStatManager.GetMultiDeptNew' |
| 3 | 2017-09-11 09:30:55 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.UserManager.GetLastLoginInfo' |
| 4 | 2017-09-11 09:30:55 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Department.SelectDepartmentByID' |
| 5 | 2017-09-11 09:30:55 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='QueryControlerInfo.2' |
| 6 | 2017-09-11 09:30:56 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='UserManager.2' |
| 7 | 2017-09-11 09:30:56 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.UserManager.GetPersonGroupList' |
| 8 | 2017-09-11 09:30:56 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.Department.GetNurseStationFromDept' |
| 9 | 2017-09-11 09:30:56 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.Notice.GetNotice.Select' |
| 10 | 2017-09-11 09:30:56 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.Notice.GetNotice.Where.ByDept' |
| 11 | 2017-09-11 09:30:56 | 192.168.25.166 | MZ_8F_TJS_166 | his.exe | his_zn | select id,name,memo from OPSN_COM_SQL where id='Manager.UserManager.GetLoginSessionID' |

## 2.6 事件查看

用户可以在事件查看中查询包含风险事件在内的所有数据库操作风险事件。管理员可以在此查看事件发生的时间、物理地点、行为者等相关信息。此外通过事件追踪，查看更加详细的信息，对事件进行追踪核查后调整优化事件的识别规则。

点击左栏菜单中的[监控中心/事件查看]，打开的事件查看界面如下图所示：

图2-69 事件查看



可以根据可疑程度、时间范围，行为者（IP 或业务账号），规则名称、事件 ID、事件描述、事件类型等关键字进行检索。

### 2. 事件追踪

在检索列表右侧点击事件追踪，可以在新窗口中查看事件更详细的信息。如下图所示：

图2-70 事件追踪


(2) 查看详细的操作

点击<查看更多相关信息>可以查看完整的数据库访问行为，如下图所示：

图2-71 更多相关信息


(3) 调整识别规则

在查看、分析事件的具体操作，终端录像等相关信息后，用户可以调整、优化系统现有的识别规则。

说明

系统为事件提供了与该事件相关的操作信息、终端录屏、Telnet 操作和 FTP 事件等信息，但若该事件没有相应的信息则界面不会展示出来。

图2-72 展示


- 设为安全

  认为系统识别不准确，该事件是安全的，单击<设为安全>后，在弹出[确认]框中点击<确定>将该事件设置为安全事件。

图2-73 设为安全


---

说明

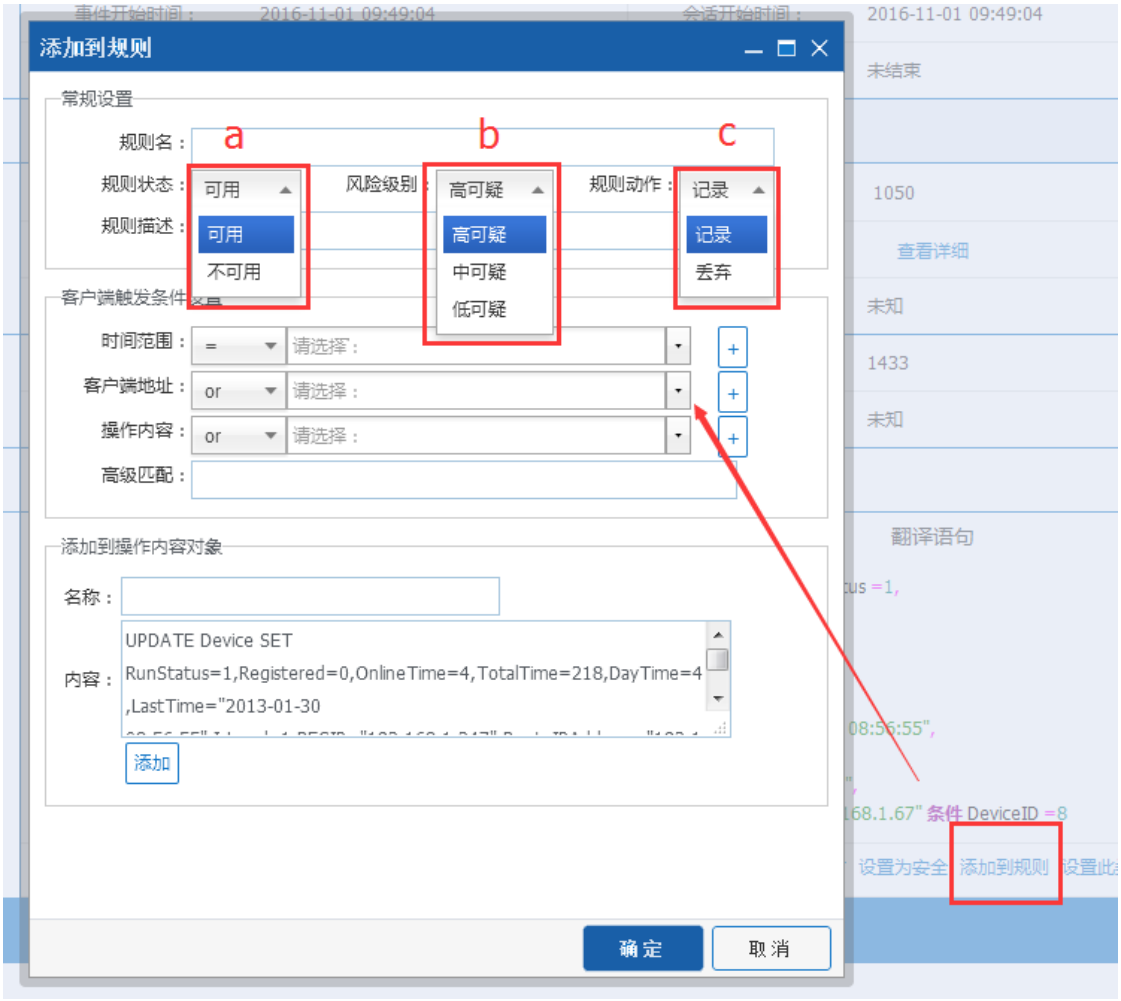
若同类语句中没有识别的语句，在此处设置为安全将无效。

---

- 添加到规则

  点击<添加到规则>后，用户在弹出[添加到规则]框中根据该事件的内容，设置规则。如下图所示：

图2-74 添加到规则




- 规则状态：设置规则的是否可用，不可用即不生效。
- 风险级别：设置事件的风险等级。
- 规则动作：设置为记录才会产生事件，若设为丢弃，则是过滤该事件，即过滤规则。

### 3. 导出记录

勾选需要导出的记录后，点击 导出记录 ，在弹出[导出记录设置]的对话框中进行导出设置后点击<确定>即可。导出项设置包含数据库事件、WEB 事件。导出文件格式包括，XML 格式、CSV 格式、EXCEL 格式，默认为 CSV 格式。如下图所示：

图2-75 导出记录设置


导出的文件里包含了事件明细的具体内容：时间、源 IP、目的 IP、事件名称、触发告警的语句（不包含完整会话信息）、数据库用户名、连接工具、计算机名。

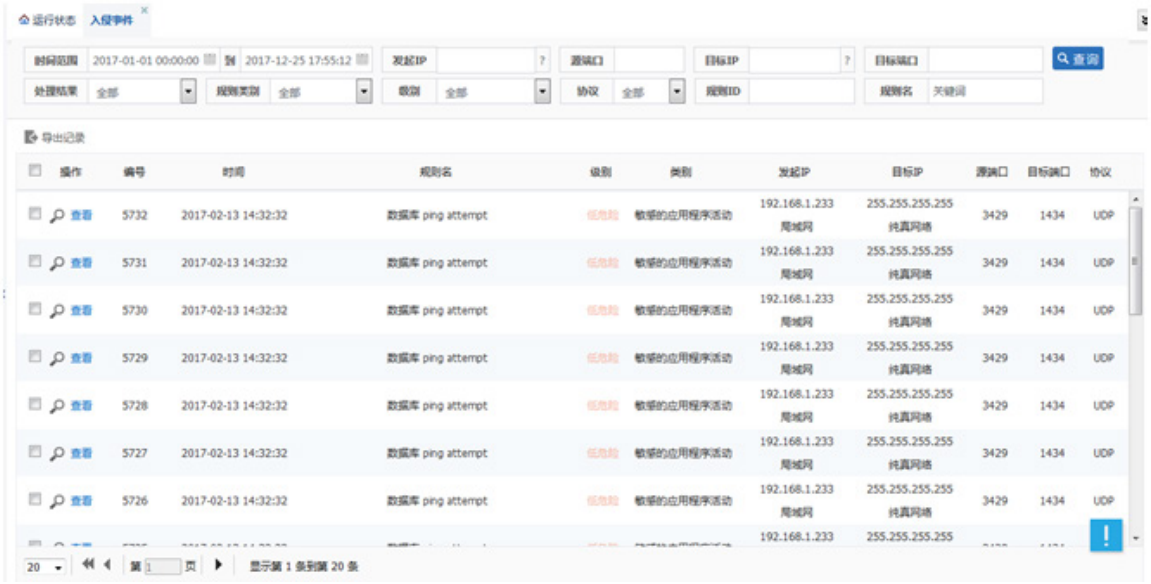
说明

用户实际操作时，可根据目前的检索条件，筛选事件内容，获得查询结果，点击导出按钮将查询结果导出成 CSV 文件。隐含要约：导出的 CSV 文件不超过 100M。

## 2.7 入侵事件

用户可以在入侵事件中查询所有触发数据库入侵检测规则的事件，管理员可以在此查看事件发生的时间、发起 IP、目标 IP、端口、协议等相关信息。此外通过查看按钮，可以查看根据详细的信息。点击左栏菜单中的[监控中心/入侵事件]，进入入侵事件界面，如下图所示：

图2-76 入侵事件




根据时间范围、行为者、端口、处理结果等关键字进行检索。在检索列表左侧点击 查看 按钮，可以在新窗口中查看事件证据更详细的信息。如下图所示：

图2-77 关联证据


## 2. 证据详情

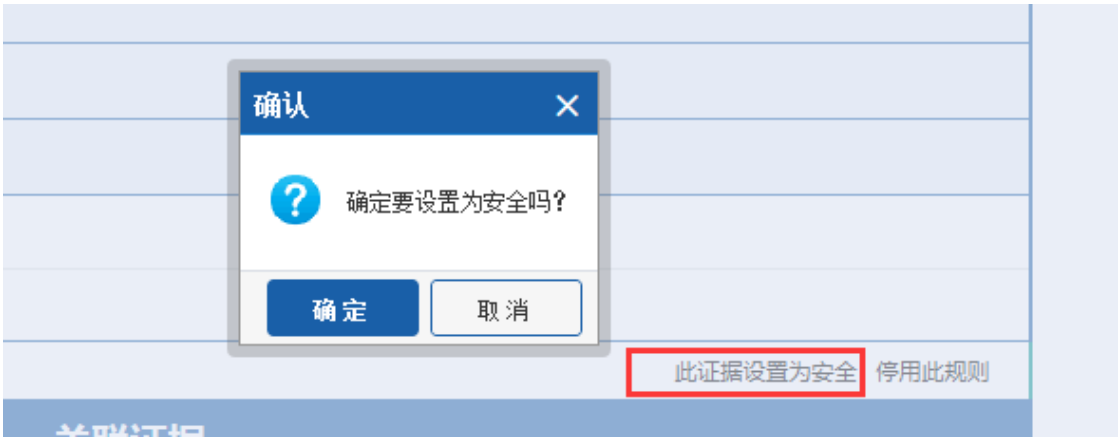
以表格形式展示证据的相关信息，包括证据信息、报文特征等：

- 证据信息：该事件相关的证据信息，包括触发规则、触发时间、规则 ID、规则等级、端口、IP 等。
- 查看规则详情：点击<查看规则详情>可以展开规则的相关信息，也可选择隐藏。如下图所示：

图2-78 规则详情

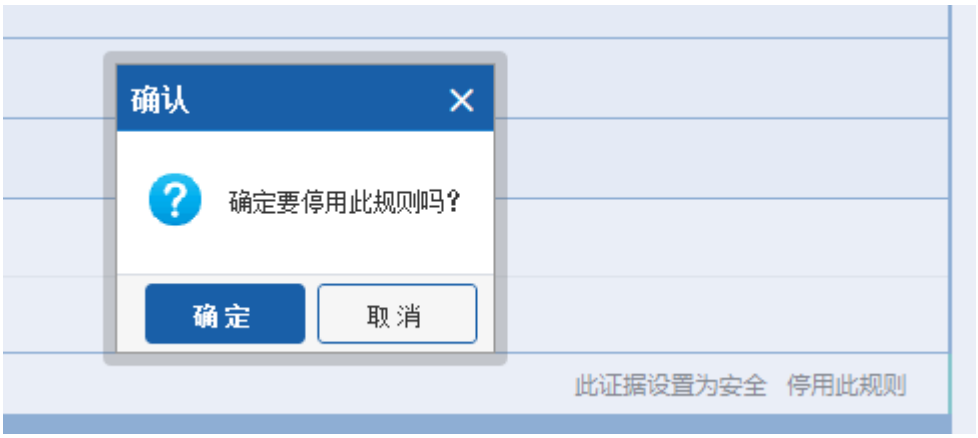

- 此证据设置为安全：在展开的规则详情页面中，点击<此证据设置为安全>在弹出[确认]的对话框中点击<确定>，将会把与该证据设置为安全事件。

图2-79 此证据设置为安全




- 停用此规则：将触发的规则设置停用，未来不会触发该规则，如下图所示：

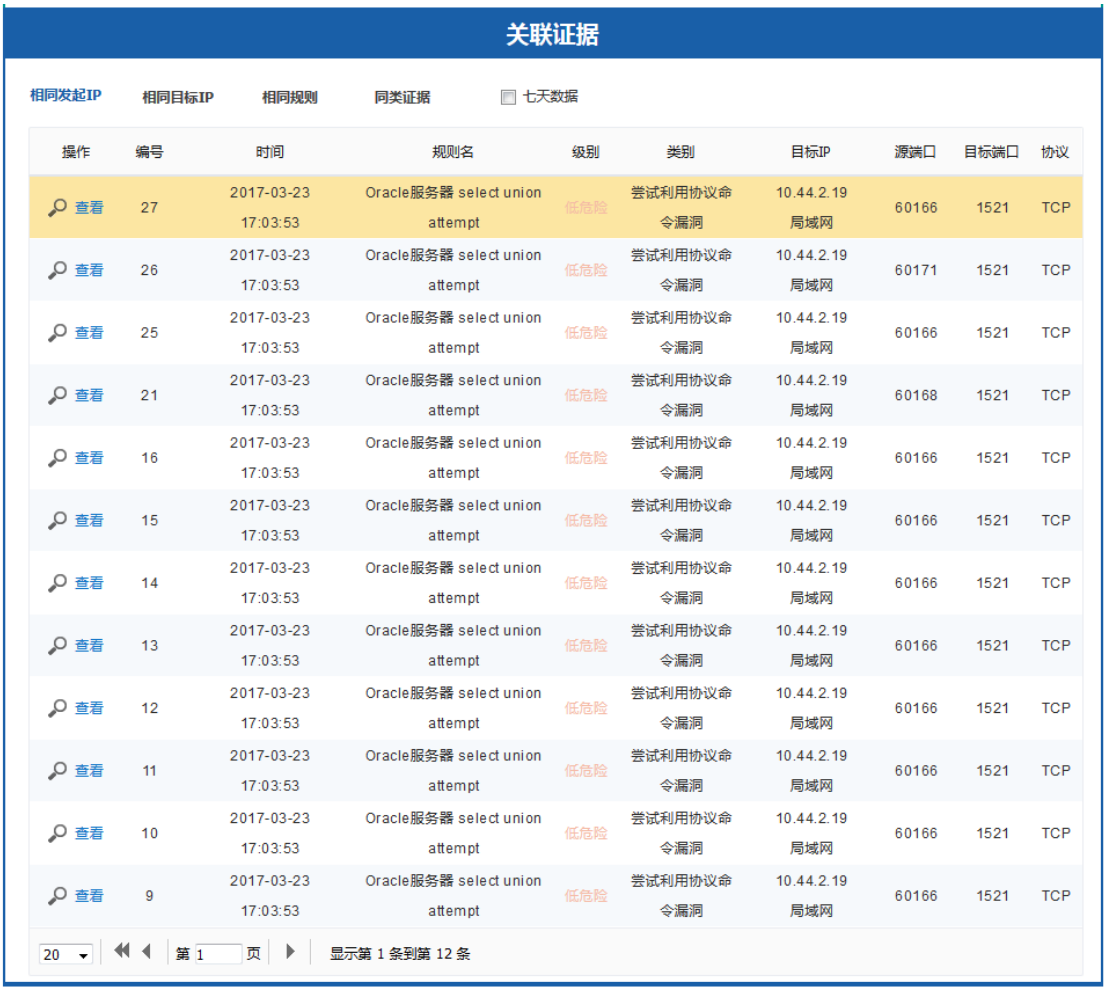
图2-80 停用此规则




### 3. 关联证据

在此页面可以查看到与该证据关联的其他信息，如相同发起 IP、相同目标 IP、相同规则、同类证据，如下图所示：

图2-81 关联证据其他信息

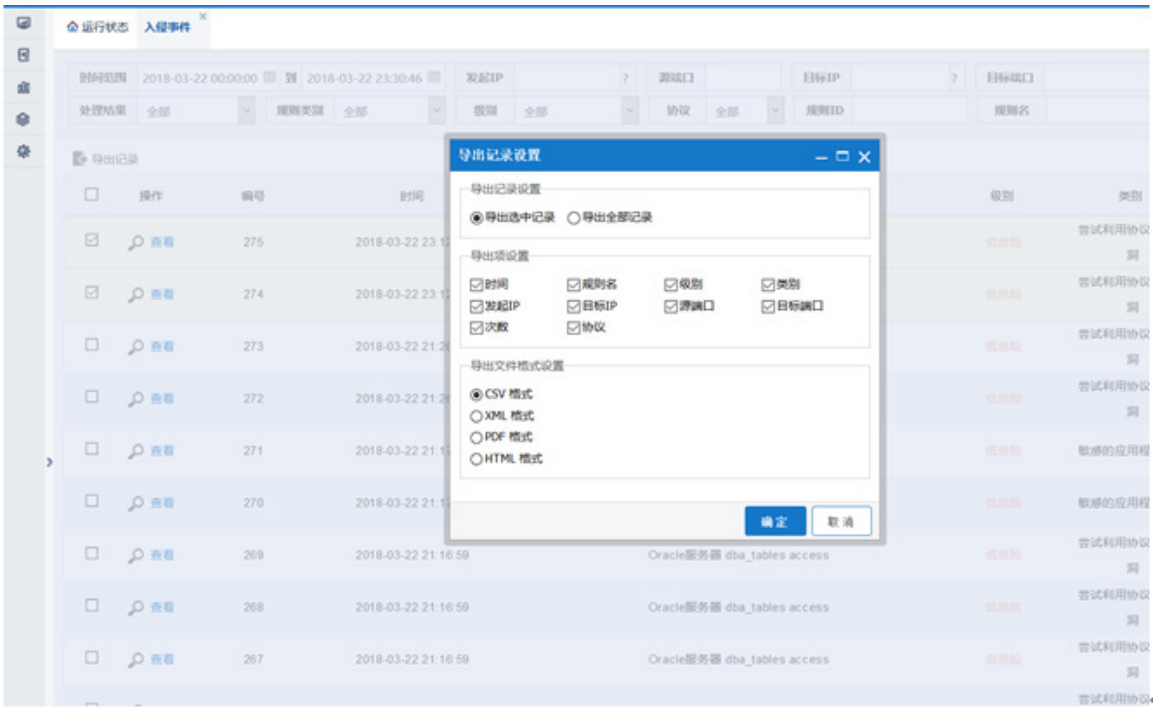



| 操作 | 编号 | 时间 | 规则名 | 级别 | 类别 | 目标IP | 源端口 | 目标端口 | 协议 |
|---|---|---|---|---|---|---|---|---|---|
| 查看 | 27 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 26 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60171 | 1521 | TCP |
| 查看 | 25 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 21 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60168 | 1521 | TCP |
| 查看 | 16 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 15 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 14 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 13 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 12 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 11 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 10 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |
| 查看 | 9 | 2017-03-23 17:03:53 | Oracle服务器 select union attempt | 低危险 | 尝试利用协议命令漏洞 | 10.44.2.19 局域网 | 60166 | 1521 | TCP |

### 4. 导出记录

勾选需要导出的记录后，点击 导出记录 ，在弹出[导出记录设置]的对话框中进行导出设置后点击<确定>即可。导出项设置包含时间、规则名、级别、类别、发起 IP、目标 IP、源端口、目标端口、次数、协议。导出文件格式包括，XML 格式、CSV 格式、PDF 格式以及 HTML 格式，默认为 CSV 格式。如下图所示：

图2-82 导出记录



# 3 审计中心

## 3.1 概述

展示系统审计到的 SQL 操作数据，URL 信息，行为审计、SQL 模板、因子监测等各类审计数据，供用户查询、深度分析的功能。主要包含以下功能模块：

图3-1 审计中心

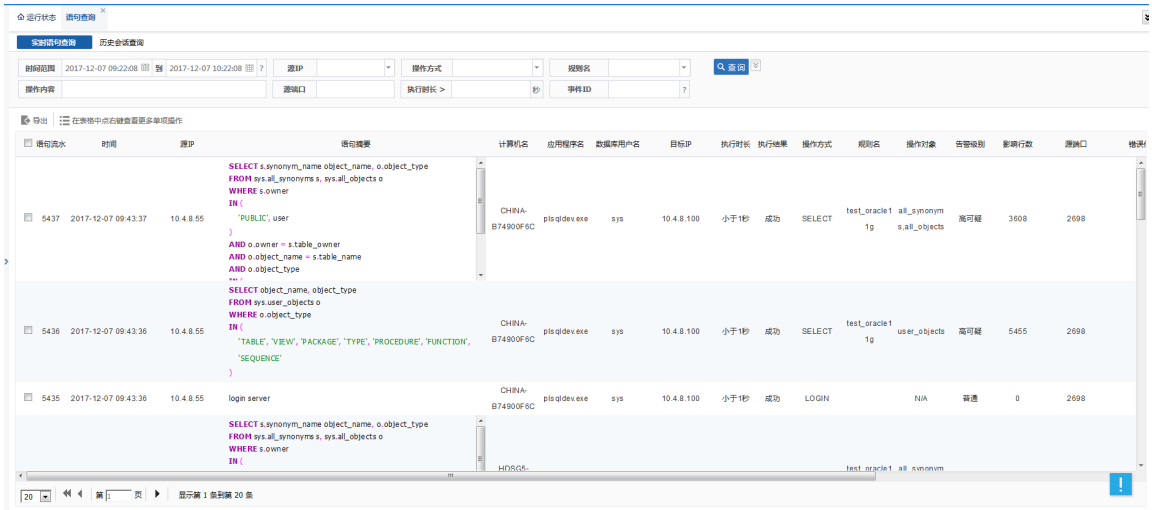

## 3.2 语句查询

单击左栏菜单中[审计中心/语句查询]，进入审计数据语句查看分析界面。

语句查询中分实时查询和历史查询。实时查询是对当天系统内审计数据进行查询分析，历史查询为对当天之前的审计数据进行查询分析。

输入查询条件即可对历史数据和实时数据进行详细的查询，可以用手动输入子网掩码的方式进行 IP 地址组查询。设备可自动将敏感信息进行掩码，用“*”替换其内容。如下图所示：

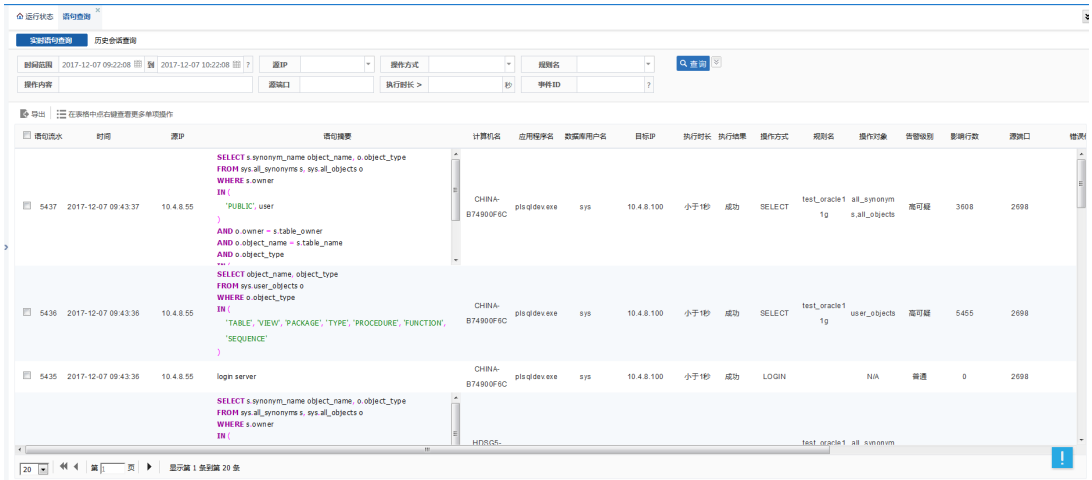
图3-2 语句查询



### 3.2.2 实时查询

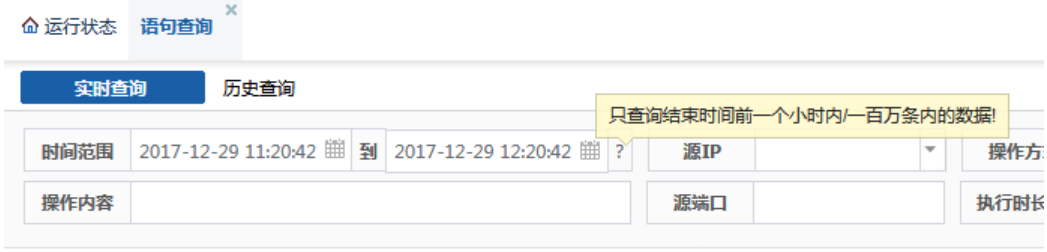
对当天系统中任意一小时内的审计数据进行查询分析。如下图所示：

图3-3 实时语句查询



当鼠标停留在结束时间右侧的“？”号时，系统将会出现如下提示：

图3-4 提示语



## 2. 高级查询

点击<查询>按钮旁的  按钮可设置更多查询条件，再点击一次可以回到简单查询界面。如下图所示红色框的内容是增加的高级查询条件：

图3-5 高级查询条件


## 3. 查询结果处理

在查询结果中右击某条记录，可以进行查看 SQL 模板、过滤类似语句、查看类似语句、设置别名、丢弃此类语句等操作，界面如下图所示：

图3-6 查询结果处理


- 明细信息

  在查询结果列表中选择某条记录，右击选择 

按钮，可以查看该记录的详细信息，如下图所示：

图3-7 详细信息


- 查看 SQL 模板

  点击<查看 SQL 模板>后，页面会跳转到 SQL 模板页面，显示对应的 SQL 模板。

- URL 关联

  在查询结果列表中选择某条记录，右击选择 URL URL关联 按钮，打开的[URL 审计]界面展示与之关联的 URL 审计信息。

- 过滤类似语句

  在查询结果中过滤掉与该语句类似的语句。此类语句将不会在本次查询结果中出现。

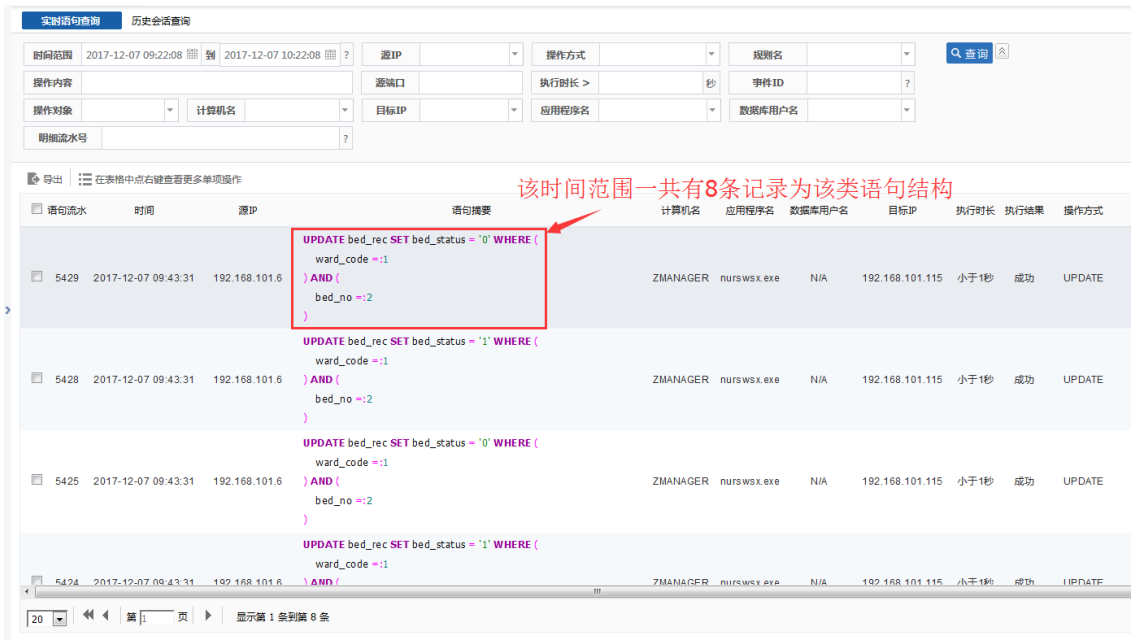
- 查看类似语句

  点击后查询结果中只会剩下与该语句类似的语句，在某条记录上右击，并选择查看类似语句，如下图所示：

图3-8 查看类似语句


系统将在查询结果中筛选，并只展示与该语句结构相似的记录，如下图所示：

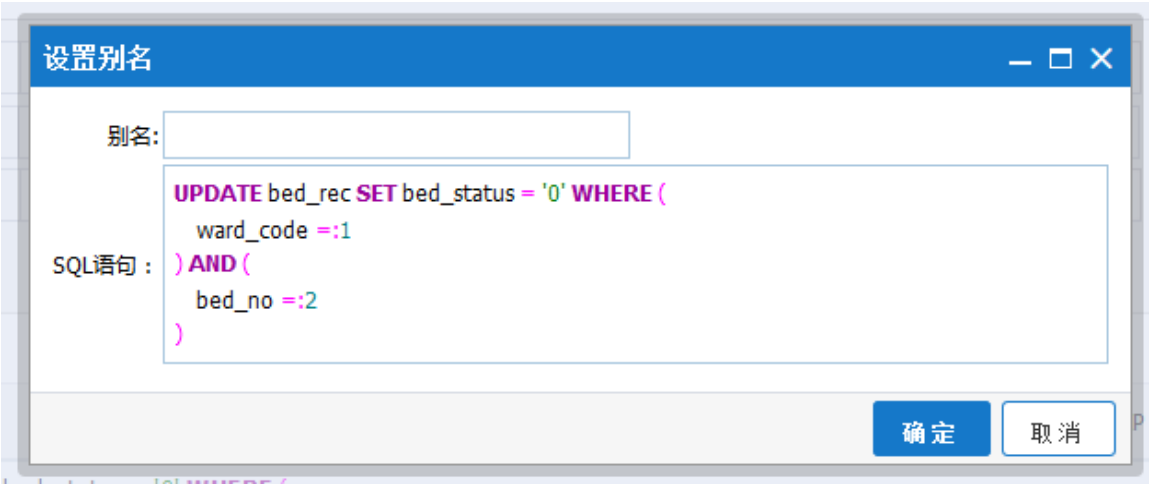
图3-9 查询结果




- 设置别名

  右击某条语句并点击<设置别名>将会为该类事件事件设置别名，未来可用于检索等其他功能的扩展。

图3-10 设置别名




- 丢弃此类语句

  点击<丢弃此类语句>将会生成规则，在之后的审计数据中发现结构相同的语句，则自动丢弃该类语句。

---

说明

四种操作中，只有“丢弃此类语句”将会形成规则，对未来的数据产生影响。其他的 3 种操作仅仅对本次查询结果生效。

---

### 4. 导出

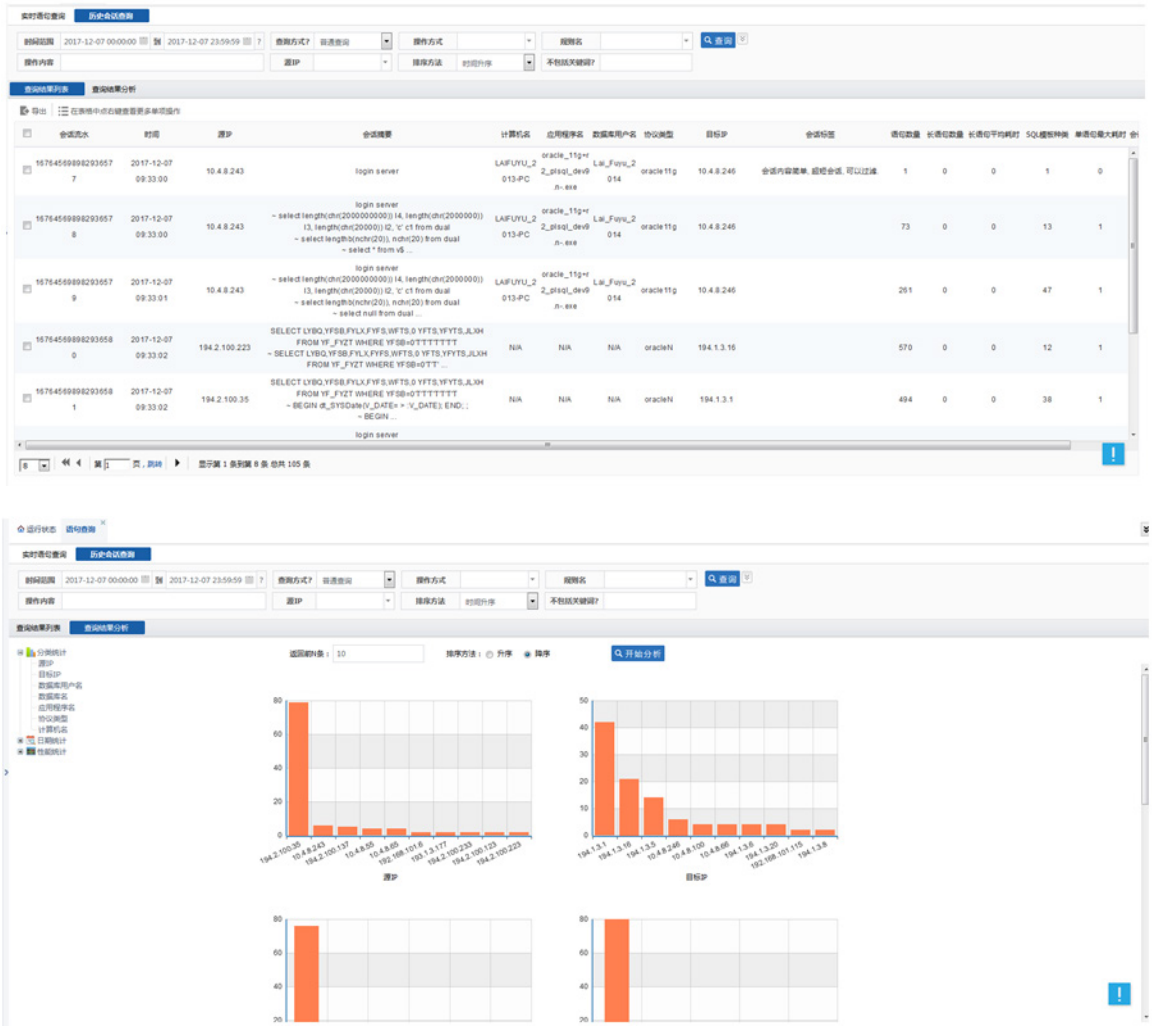
选中一条或多条记录后点击<导出>进行导出设置后可将查询结果导出，最多 600 条记录。导出文件格式包括，XML 格式、CSV 格式、EXCEL 格式，默认为 CSV 格式。如下图所示：

图3-11 实时查询记录导出设置


### 3.2.3 历史查询

默认提供最近有语句数据的、七天范围内的查询分析，若选择的查询时间范围内的数据量较大，系统会进行提示，需缩小时间范围后，再重新查询。查询的时间范围不能超过 30 天。查询结果展示可分为查询结果列表、查询结果分析两种视图，界面如下图所示：

图3-12 历史查询



- 排序方式

  可以设置查询结果是按时间升序或降序展示。

- 查询方式

  表示对操作内容的多关键词进行查询。

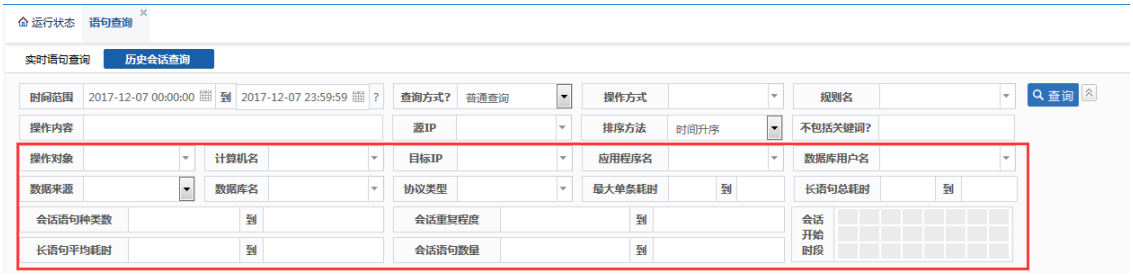
  - 普通查询，只要关键词全部出现即可被检索，无论前后顺序或中间是否夹杂字符；模糊查询，在整个 SQL 会话中匹配出所有 SQL 关键词个数的一半以上，即可被检索。
  - 明细查询，在单条 SQL 语句中匹配出所有 SQL 关键词，即可被检索，关键词的先后顺序不影响结果。
  - 词组查询，在单条 SQL 语句中匹配出整个 SQL 关键词组，严格按照关键词的先后顺序，中间不带其他关键词。

例如，输入查询关键字“select user”，普通查询：查询结果中只需包含“select”和“user”即可，无论前后顺序或中间是否有夹杂字符；模糊查询：查询结果中只需包含“select”或“user”即可，可仅出现关键词的任意一个；明细查询：查询结果中，会话的单条 SQL 语句中包含“select”和“user”即可；词组查询：查询结果中必须包含“select user”，单词中间仅能出现空格，不能有其他字符。

- 高级查询

  点击“查询”按钮旁的  按钮可设置更多查询条件，再点击一次可以回到简单查询界面。如下图所示：

图3-13 更多查询条件




- 会话语句耗时：单条会话中语句的耗时时长。
- 会话语句种类数：单条会话中 SQL 语句模板种类数量。
- 会话重复程度：单条会话中语句总数除以语句类型数得到重复程度。
- 会话语句数量：单条会话中 SQL 语句总数量。
- 时段：查询选中时段内的语句。

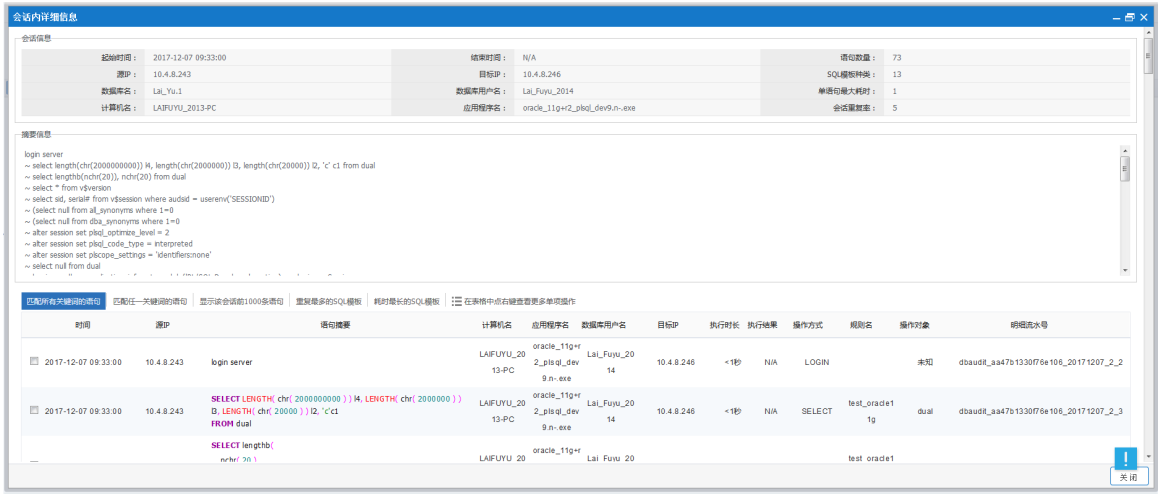
## 2. 查询结果列表

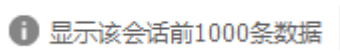
- 查看详细

  查询结果列表中选择某条记录，右击选择 

按钮，可以查看记录的详细信息，如下图所示：

图3-14 查看会话详细




在会话中可能有很多条数据，用户可以点击  按钮查看前 1000 条数据。



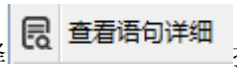
勾选某条语句，右击选择  按钮可以查看该语句的详细内容，包含对 oracle、SQL server、mySQL、pgSQL 影响行数解析与返回时长的计算。系统将记录某一数据库请求而影响的行数，和每个请求使用的时长，时长精确到 ms 级别。如下图所示：



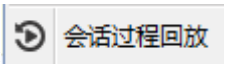
图3-15 语句详细信息

- 导出

  在历史会话查询结果中，选择一条或多条记录后点击<导出>按钮，进行导出设置后可将查询结果导出。导出文件格式包含 XML 格式、CSV 格式、PDF 格式、HTML 格式、EXCEL 格式，默认为 CSV 格式。如下图所示：

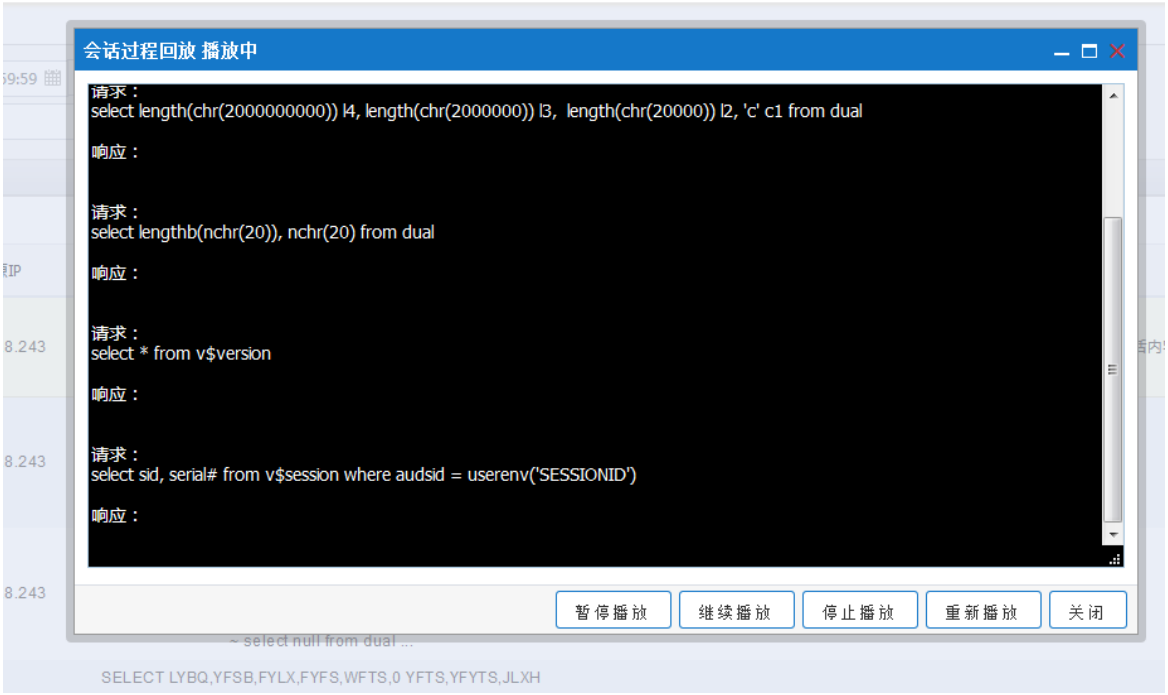
图3-16 历史查询记录导出设置


- 会话回放

  查询结果列表中选择某条记录，右击选择 

按钮，可以查看记录的会话过程，将原有的会话文本记录展示方式，增加以 shell 执行动画的展示方式如下图所示：

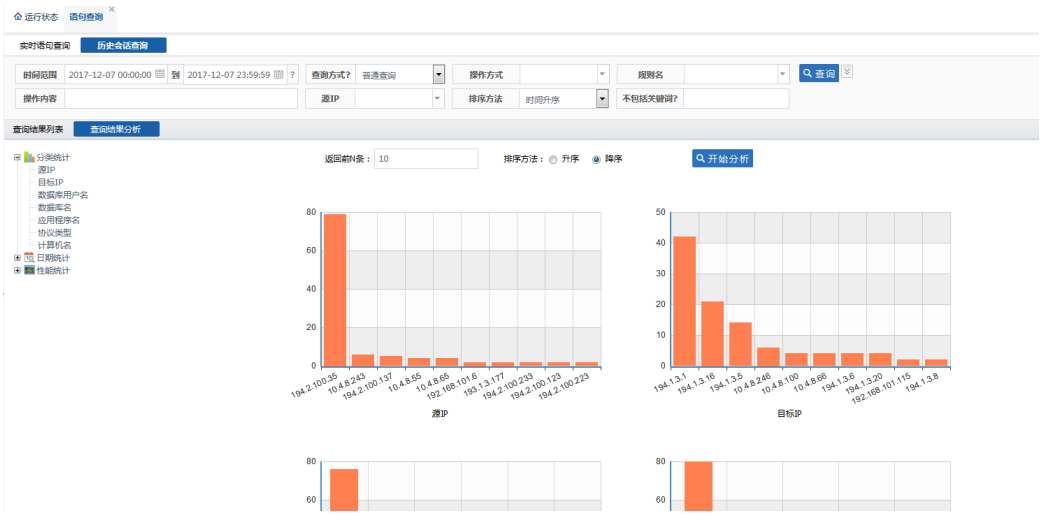
图3-17 会话回放




### 3. 查询结果分析

根据上述条件查询的结果进行二次分析，返回前 N 条信息升序或降序展示，如下图所示：

图3-18 查询结果分析




- 分类统计

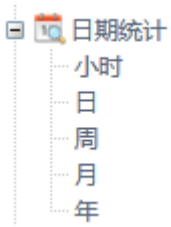
  查询结果分析中点击<分类统计>按钮，可以查看不同条件类型统计的详细信息，如下图所示：

图3-19 分类统计


- 时间统计

  查询结果分析中点击<时间统计>按钮，可以查看按时间类型统计的详细信息，如下图所示：

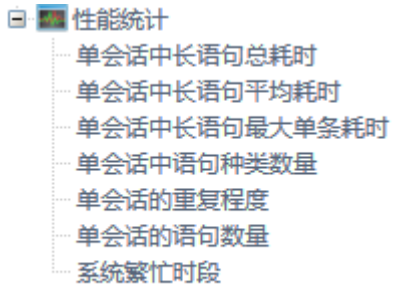
图3-20 时间统计




- 性能统计

  查询结果分析中点击<性能统计>按钮，可以查看分类统计的详细信息，如下图所示：

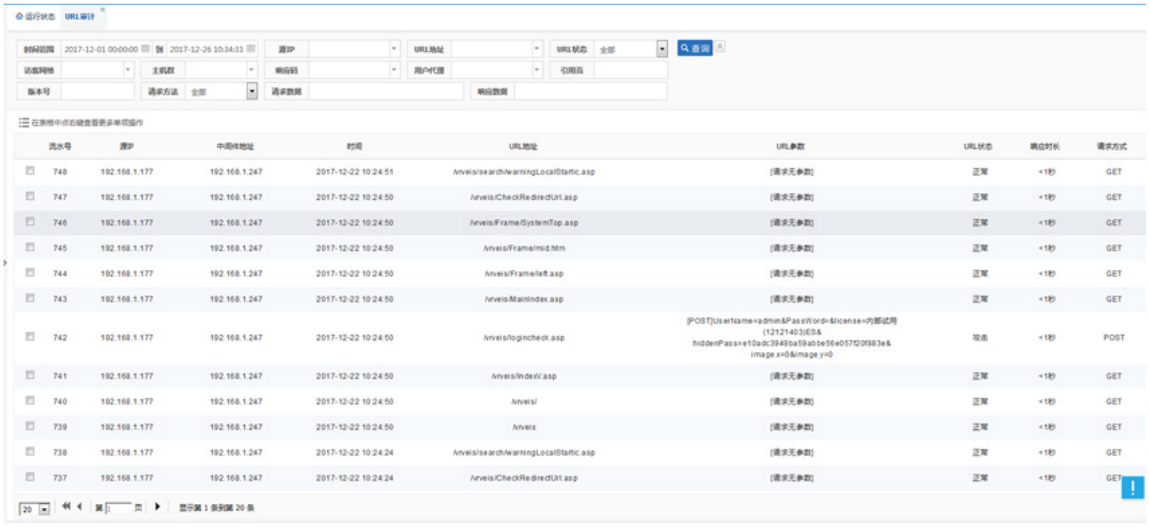
图3-21 性能统计




## 3.3 URL审计

在左栏菜单中点击[审计中心/URL 审计]，即可在右栏功能区打开 URL 审计查询界面。输入时间范围、操作源 IP 或 URL 地址、访客网络、主机群、响应码、用户代理、引用页、URL 状态等查询条件后点击<查询>按钮即可，如下图所示：

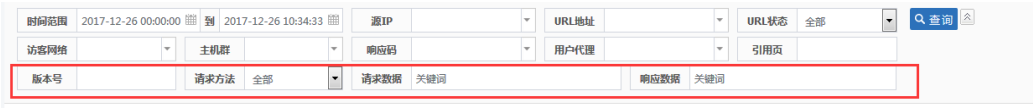
图3-22 URL 审计



## 2. 高级查询

点击“查询”按钮旁的  按钮可设置更多查询条件，再点击一次可以回到简单查询界面。如下图所示红色框的内容是增加的高级查询条件：

图3-23 高级查询条件

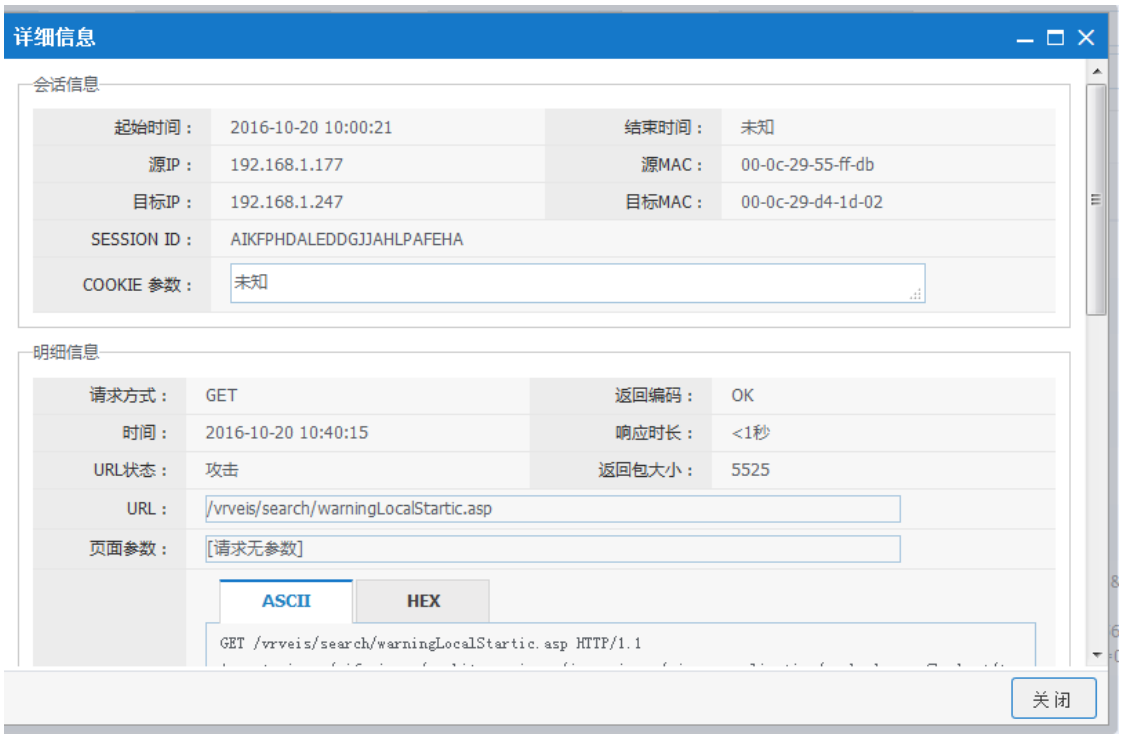


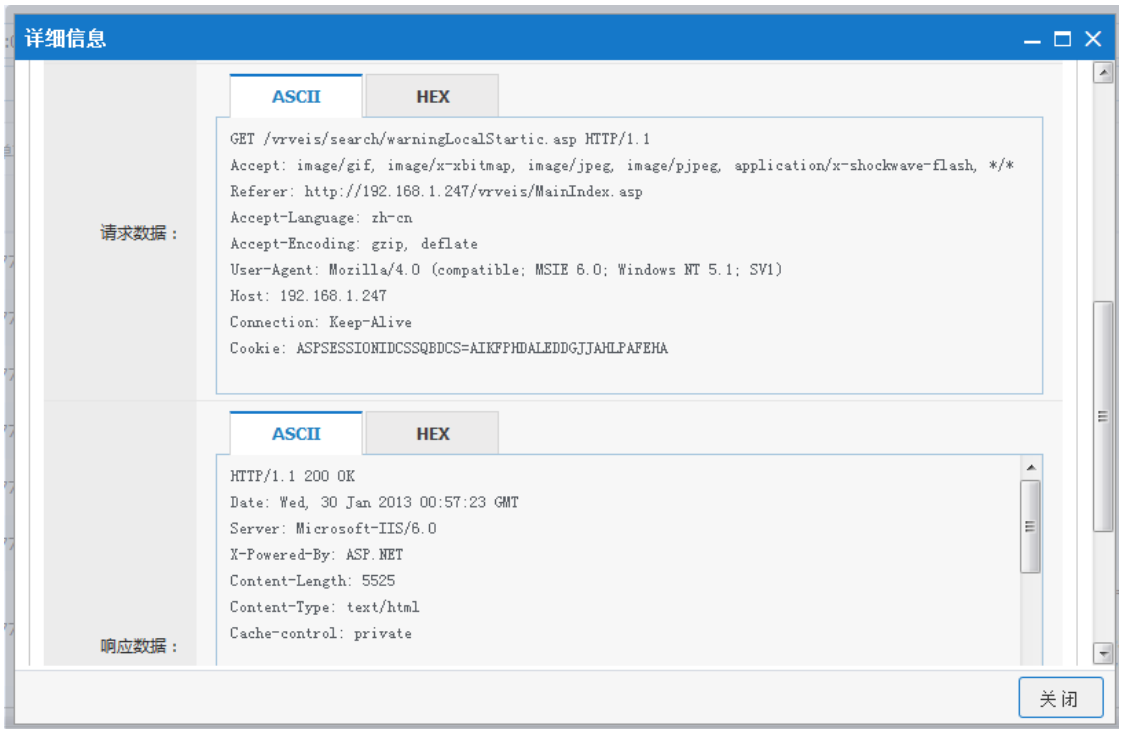

## 3. 查看详细

选择某条记录后，右击选择 

按钮，在弹出[详细信息]框中可以查看审计结果明细，对 web 审计中 reques 请求与 respon 响应数据的保存，如下图所示：

图3-24 详细信息

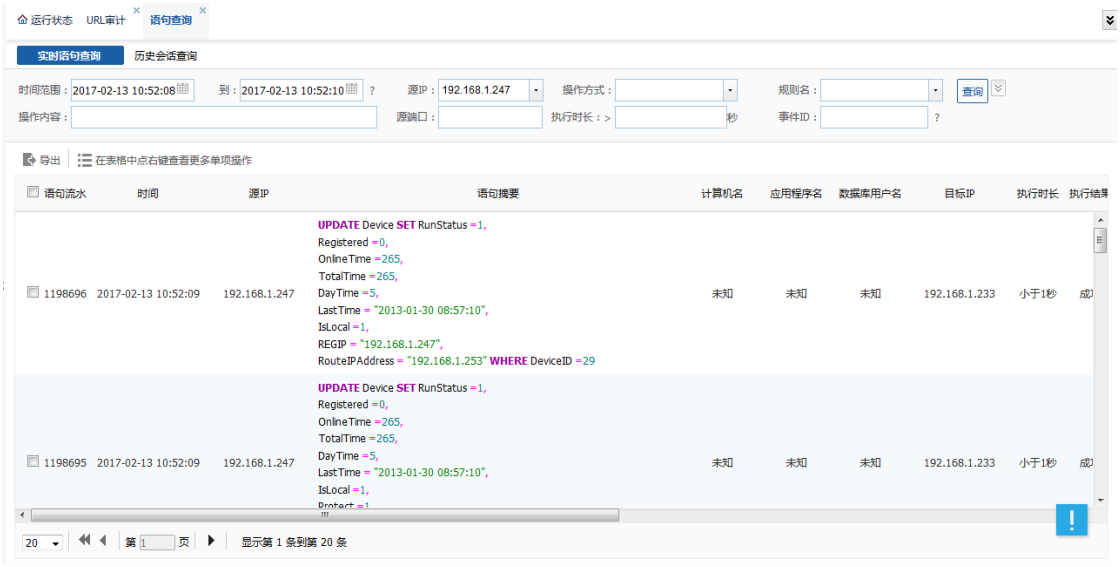



- SQL 关联

选择某记录后，右击选择 SQL关联 按钮，打开的“语句查询”界面展示与之关联的 SQL 语句。如下图所示：

图3-25 SQL 关联




说明

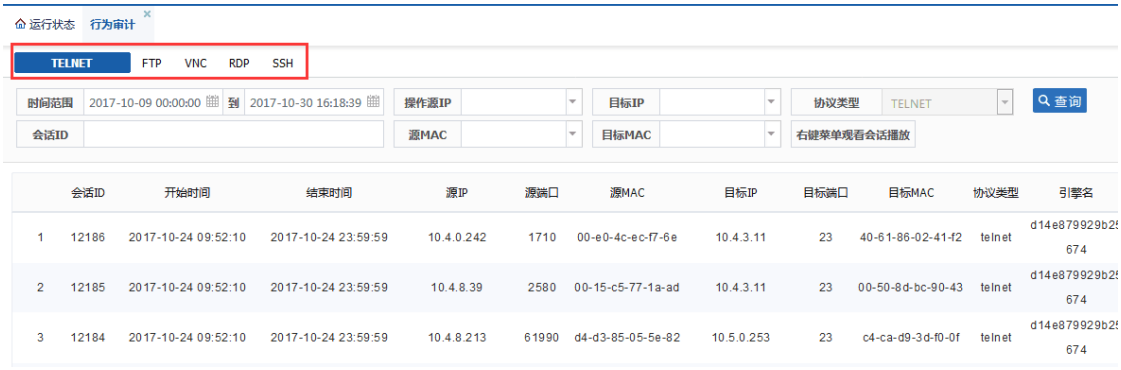
这里仅介绍 URL 审计的查询展示界面，配置请查阅[策略中心/监听配置/中间件服务器配置/WEB 协议服务器配置]中设置。如下图所示 3-26

图3-26 WEB 协议服务器配置


## 3.4 行为审计

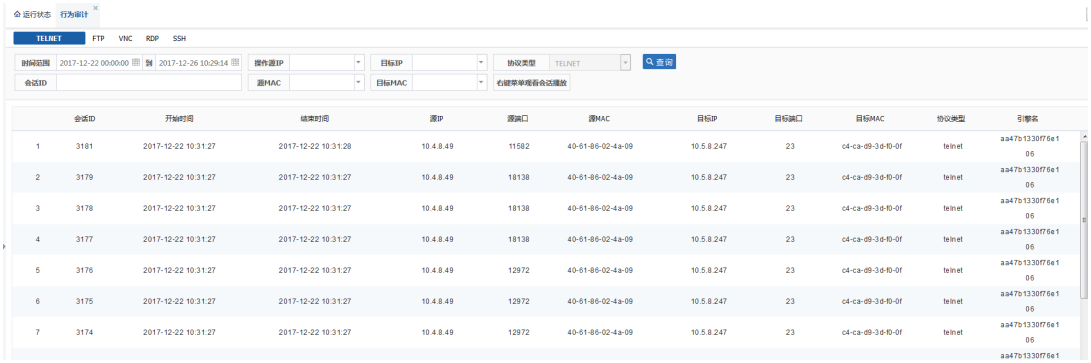
可以通过该功能，对 Telnet、FTP、VNC、RDP 等远程登录会话行为进行审计，同时可以对会话进行回放。点击左栏菜单[审计中心/行为审计]即可进入行为审计界面，如下图所示：

图3-27 行为审计



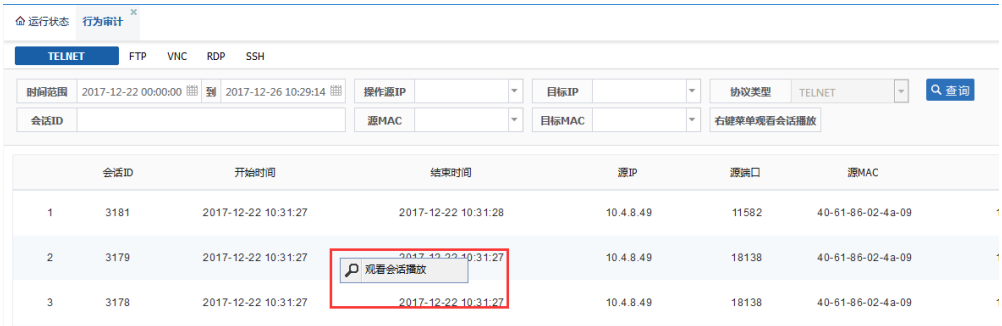

## 3.4.2 Telnet 审计

图3-28 Telnet 审计



右击某记录任意字段，系统会出现观看会话播放提示，点击可回放该会话，如下图所示：

图3-29 观看会话播放



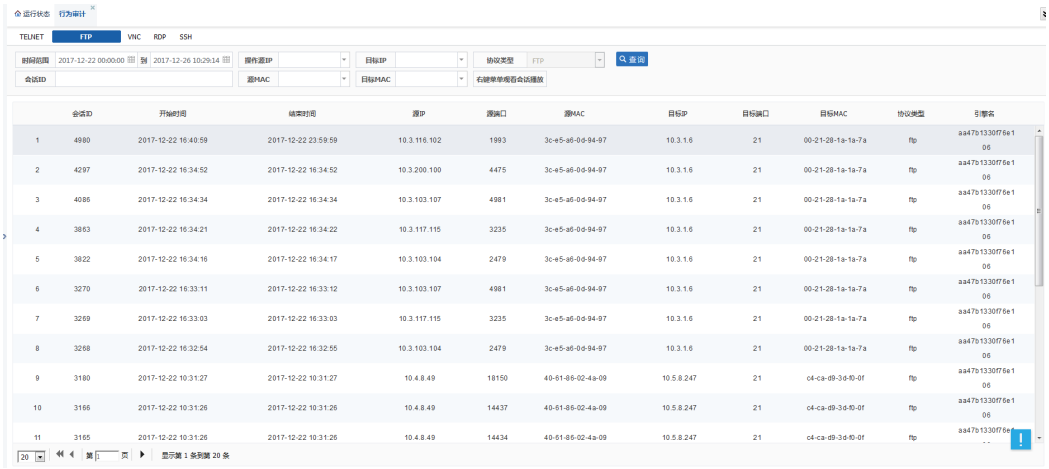

点击后自动播放会话内容，可点击窗口下方的按钮对播放进行控制，如下图所示：

图3-30 Telnet 会话播放


## 3.4.3 FTP 审计

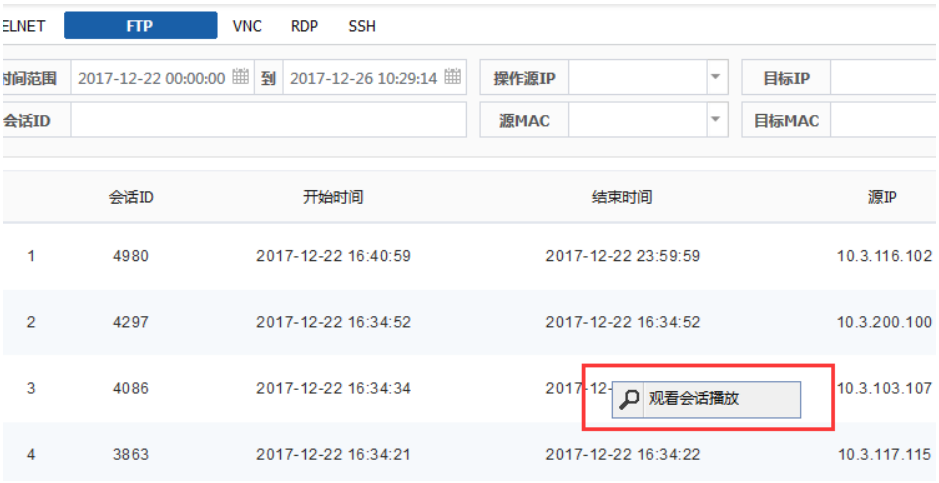
在行为审计界面中点击<FTP 审计>标签，进入 FTP 审计界面，然后设置查询条件对审计结果进行查询。

图3-31 FTP 审计



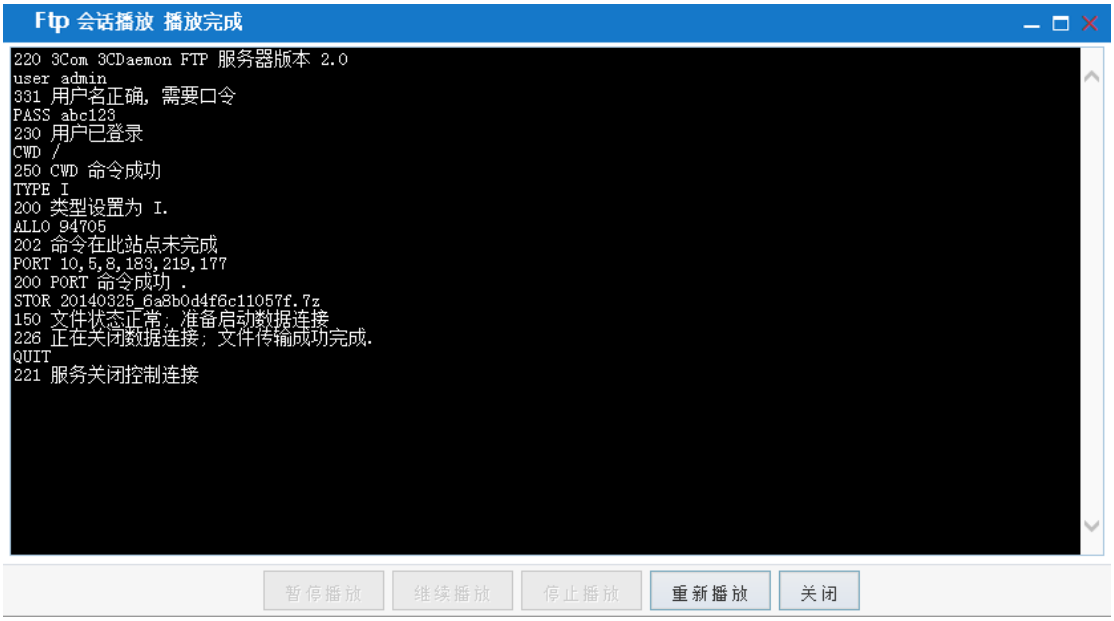
右击某记录任意字段，系统提示观看会话播放，点击可对该会话进行回放。

图3-32 观看会话播放




点击后自动播放会话内容，可点击窗口下方的按钮对播放进行控制，如下图所示：

图3-33 FTP 会话播放

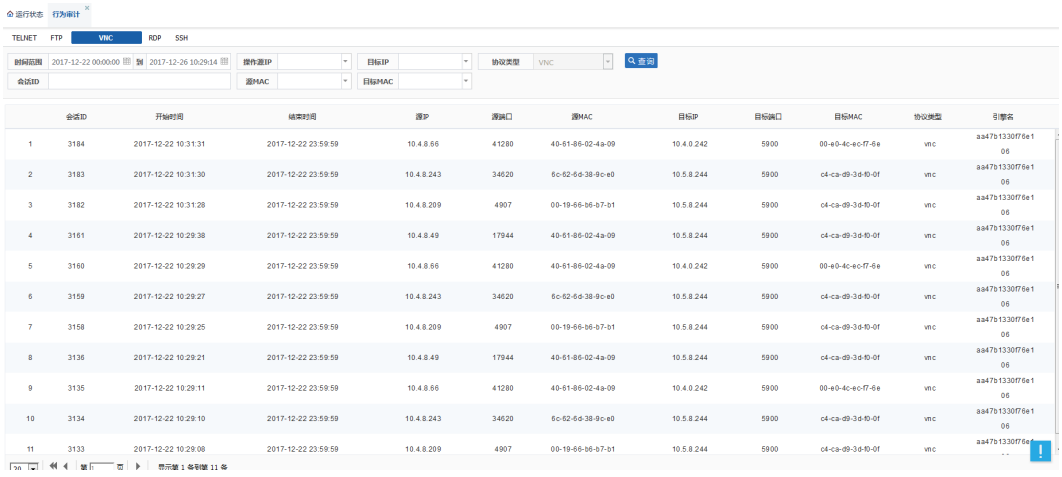



说明

若没有数据可播放，系统会在播放窗口中提示。

### 3.4.4 VNC 审计

图3-34 VNC 审计




可以根据时间范围，操作源 IP，目标 IP，协议类型等关键信息多 VCN 审计数据进行查询

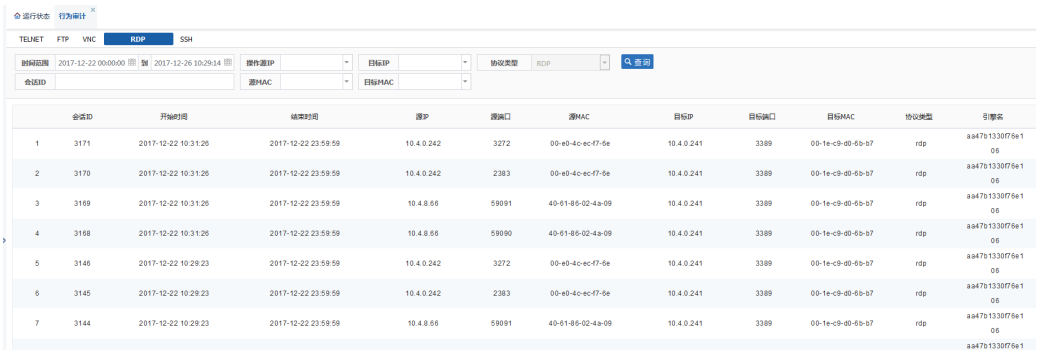
**说明**

因 VNC 为加密通讯，目前不支持对 VNC 会话的回放功能。

### 3.4.5 RDP 审计

系统对 RDP 协议（远程桌面协议）进行审计，并提供了查询界面，协助管理员进行分析工作。查询界面如下图所示：

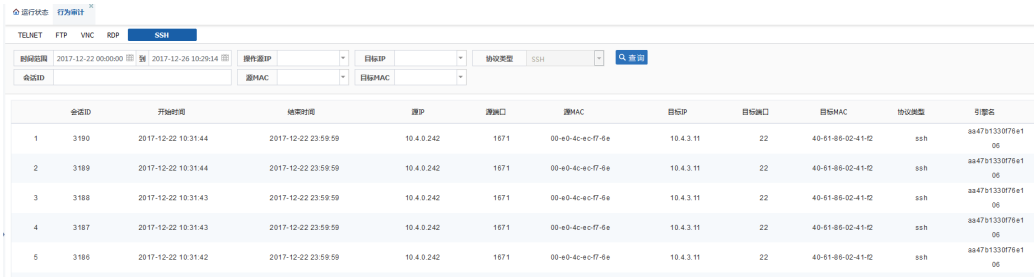
图3-35 RDP 审计




### 3.4.6 SSH 审计

可以根据时间范围，操作源 IP，目标 IP，会话 ID 等关键信息对 SSH 审计数据进行查询。查询界面如下图所示：

图3-36 SSH 审计



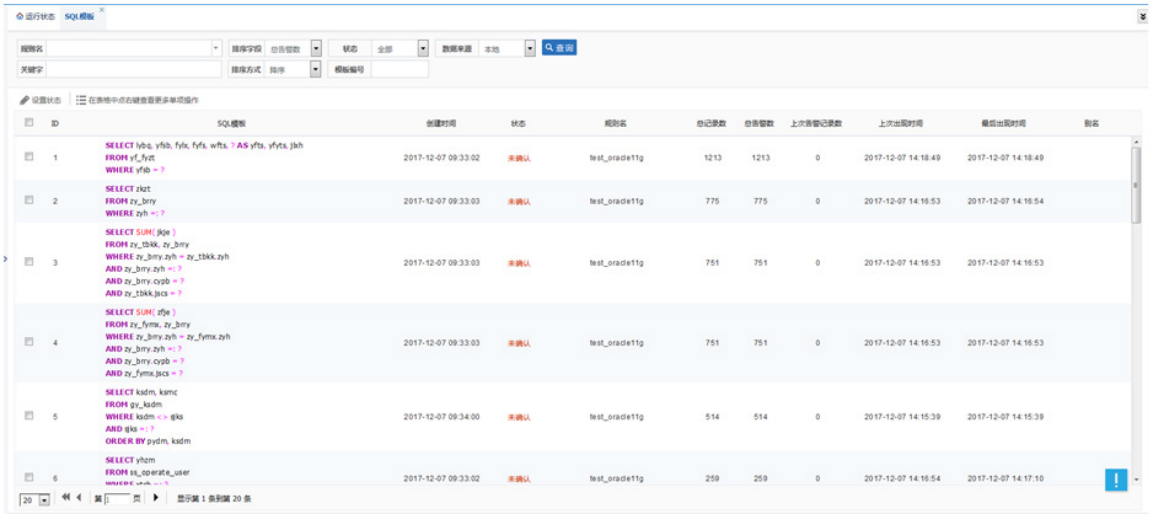
## 3.5 SQL模板

对系统审计到的 SQL 语句进行分析，将句式相同、参数不同的数据库语句视为相同的语句类型，得到 SQL 模板。SQL 模板中使用通配符“？”问号代表具体的语句参数。

SQL 模板主要用于协助管理员对审计数据进行处理，将大量的、常见的语句设置为安全规则或过滤规则，大大增加了规则的准确度，优化系统识别事件规则库。

点击[审计中心/SQL 模板]，进入如下图所示所示界面：

图3-37 SQL 模板



界面中的列表默认显示发现的所有 SQL 模板，并默认根据该模板触发的总告警数进行降序排序——最多触发的显示在最上面。在列表上方检索栏中，用户可以根据规则名、排序字段、语句状态、关键字、排序方式、模板编号等条件进行检索。

下面介绍一些关于 SQL 模板的管理：

### 2. 模板分析

系统将模板分为以下几种数据分析：

- 规则名：该模板触发的规则名，及对应的触发次数。
- 总记录数：该模板在设备上线后发生的所有记录总数。
- 总告警数：该模板在设备上线后发生的所有告警总数。

- 上次告警记录数：该模板在上个工作日发生时触发的告警记录数。
- 上次出现时间：该模板上次发生时的时间记录。
- 最后出现时间：该模板最后一次发生时的时间记录。

### 3. 模板的状态

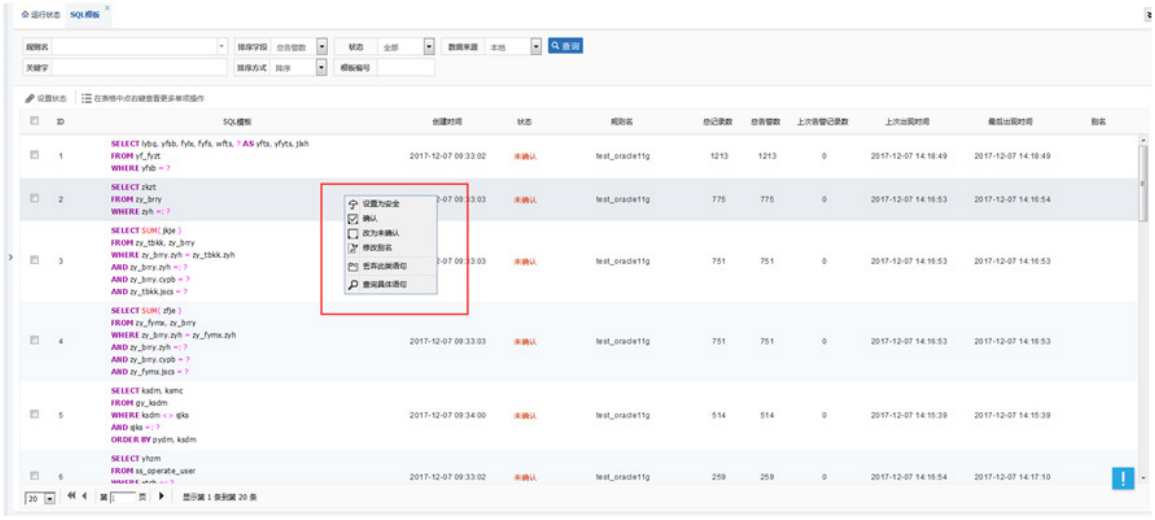
系统将模板状态主要分为以下几种：

- 设置为安全：表示此类语句以后被定义为安全的，将不会被触发规则报警。
- 已确认、未确认：是 SQL 模板的一种状态标签，表示管理员是否已经看过、知道了该类语句。
- 设置为统方：是 SQL 模板的一种状态标签。
- 修改别名：为了便于管理、沟通，管理员可以为 SQL 模板设置别名。
- 丢弃此类语句：表示此类语句以后将被直接过滤，不被保存。

### 4. 状态设置

将鼠标放在列表中某 SQL 模板上，右击鼠标可修改该类模板的状态，如下图所示所示：

图3-38 状态设置



右击并选择某个状态，在弹出[确认]的对话框中选择<确认>即可。

### 5. 查询具体语句

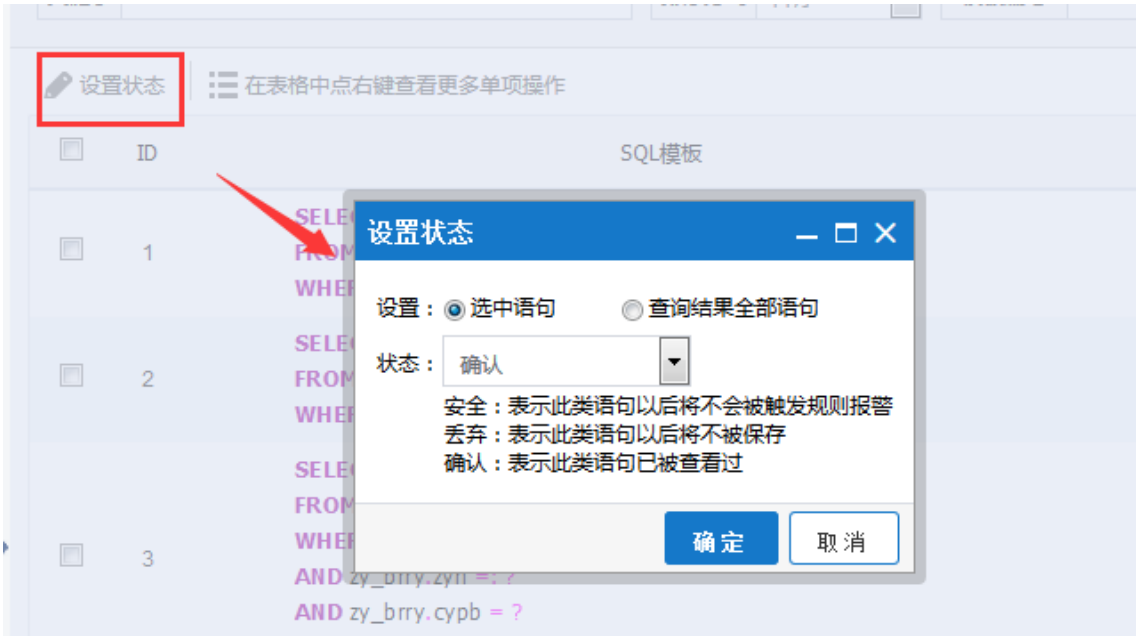
选中语句，右击选择<查询具体语句>，可跳转到具体语句查询界面。

图3-39 查询具体语句


### 6. 批量设置模板状态

点击界面上的<设置状态>按钮，可以批量设置 SQL 模板的状态。如下图所示：

图3-40 设置状态



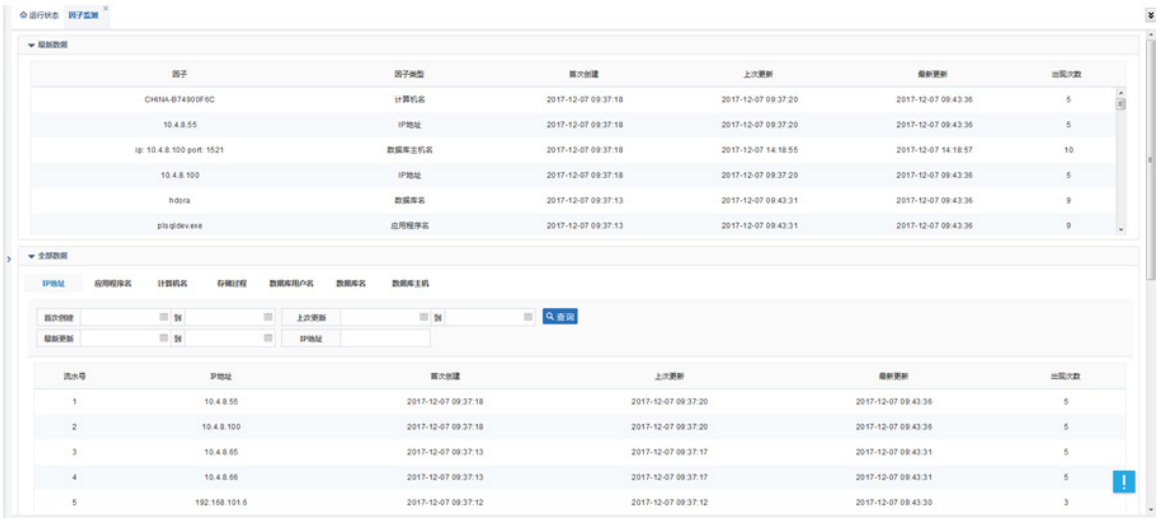

如上图所示，用户可以将列表中所有语句或选中的语句设置为安全、丢弃、统方、确认状态。

## 3.6 因子监测

对系统审计到的对象进行分析，实时展示突然出现的对象，监控内容包括：IP 地址、应用程序名、计算机名、存储过程、数据库用户名、数据库名和数据库主机。每一个被监测的因子，都会记录首次出现时间、上次更新时间和最新更新时间。

点击[审计中心/因子监测]，进入如下图所示所示界面：

图3-41 因子监测



说明

在没有配监听配置的情况下，审计引擎通过镜像流量识别的方式发现被审计的数据库对象，发现的数据库对象在因子监测中展示为数据库主机。

下面介绍一些关于因子监测的管理：

### 2. 最新数据

界面中的列表默认显示每类对象 20 条最近更新数据，根据时间降序排列。

### 3. 全部数据

可根据首次创建时间范围、上次更新时间范围、最新更新时间范围、因子名等条件进行查询。界面中的列表提供各类别对象因子的创建和更新等数据信息。

说明

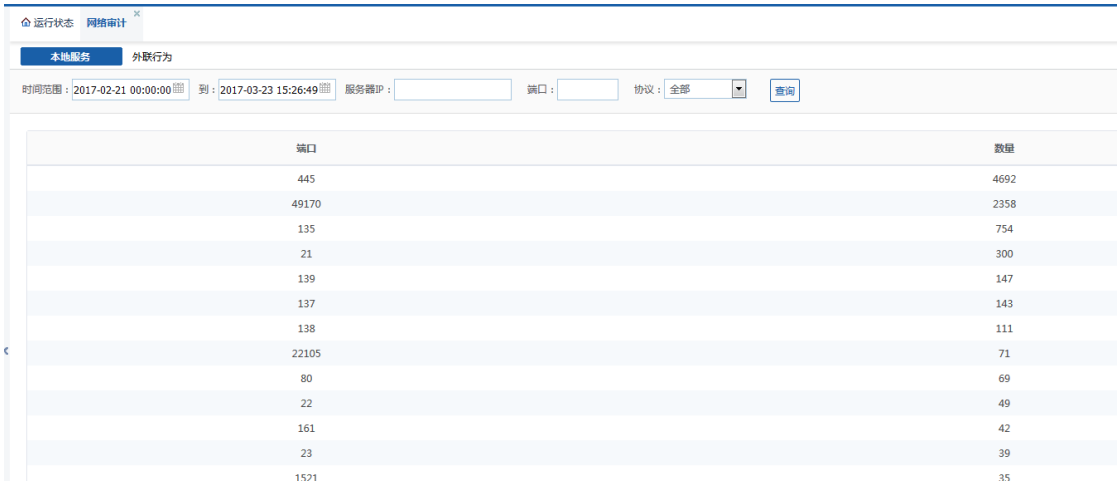
IP 地址、数据库主机页面，IP 地址可支持地址网段。

## 3.7 网络审计

可定期获知数据库服务器是否存在非数据库的访问通讯，以协助判断潜在风险。通过镜像流量可发现数据库服务器访问外部主机上开放的服务端口和数据库服务器上开放的端口；支持按时间范围、服务器 IP、端口、协议(TCP&UDP)为条件，查询非数据库通讯的结果；查询结果以表格形式展示，列出条件范围内的所有服务端口，端口以升序方式排列。支持实时查询当前通讯情况。

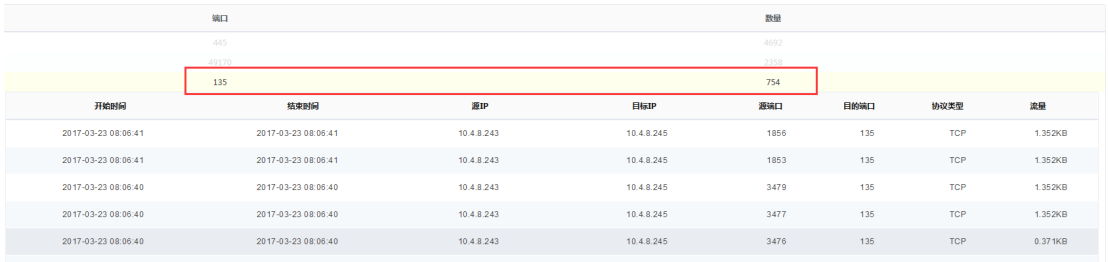
点击[审计中心/网络审计]，进入如下图所示所示界面：

图3-42 网络审计




点击端口可展开详细信息，如下图所示：

图3-43 详细信息




## 3.8 对比分析

通过对比不同时期（按月、按周、按天）的审计数据，分析审计数据量、源 IP、帐号数、客户端工具数等的差异情况，协助用户对业务系统的运维。

点击[审计中心/对比分析]，右栏的操作功能区打开对比分析界面。根据数据来源：业务系统、数据库 IP，以及时间范围，进行对比分析。可选择对比类型：单一数据库 IP 不同时段、单一业务系统不同时段、不同数据库 IP 相同时段、不同业务系统相同时段。结果显示如下图所示：

图3-44 对比分析


| 对比分析结果 | | | | | |
|---|---|---|---|---|---|
| oracle | | | | | |
| | □基础对象 □比较对象 | □基础对象 □比较对象 | □基础对象 □比较对象 | □基础对象 □比较对象 | 勾选对象进行对比 |
| 比较项 | 2017-10-17 00:00:00 -- 2017-10-17 23:59:59 | 2017-10-20 00:00:00 -- 2017-10-20 23:59:59 | 2017-10-23 00:00:00 -- 2017-10-23 23:59:59 | 2017-10-24 00:00:00 -- 2017-10-24 23:59:59 | 对比结果 |
| 源IP | 2 | 2 | 1523 | 1514 | |
| 帐号数 | 2 | 2 | 109 | 108 | |
| 客户端工具数 | 2 | 2 | 88 | 85 | |
| 客户端主机数 | 2 | 3 | 191 | 181 | |
| 表对象数 | 52 | 50 | 3335 | 3198 | |
| 操作类型数 | 8 | 5 | 36 | 34 | |
| 明细语句数 | 161 | 478 | 3285612 | 622541 | |
| 会话数 | 10 | 3395 | 39993 | 7421 | |
| 告警数 | 27 | 117 | 7121 | 6429 | |
| SQL模板数 | 67 | 60 | 8874 | 8465 | |

对比分析结果以列表和图表的形式展示。比较项包括：源 IP，账号数，客户端工具数，客户端主机数，表对象数，操作类型数，明细语句数，会话数，告警数，SQL 模板数。

## 2. 对比列表

选择基础对象和比较对象，以基础对象为标准，对比结果显示为比较对象与基础对象的差值，差值为零，则显示无变化；差值为正数，则显示蓝色字体；差值为负数，则显示红色字体。

图3-45 对比分析结果

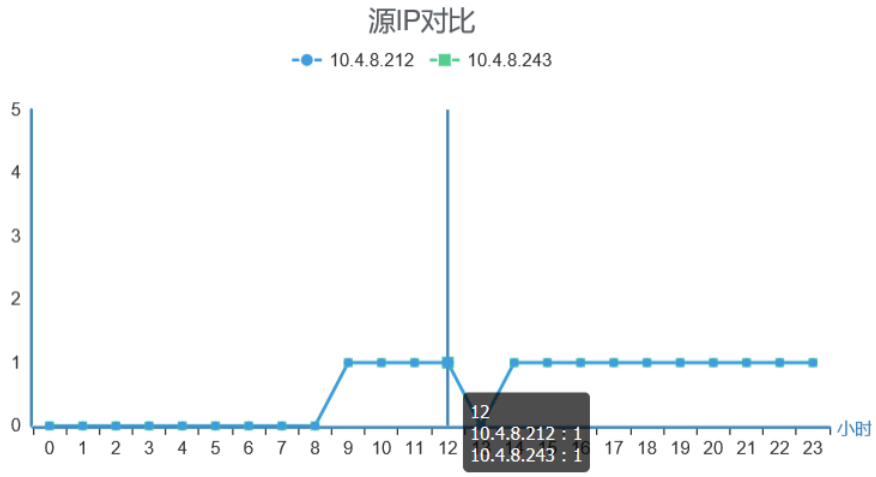
| 对比分析结果 | | | |
|---|---|---|---|
| 2017-09-21 00:00:00--2017-09-21 23:59:59 | | | |
| | ▣基础对象 □比较对象 | □基础对象 ▣比较对象 | |
| 比较项 | 10.4.8.212 | 10.4.8.243 | 对比结果 |
| 源IP | 1 | 1 | 无变化 |
| 帐号数 | 2 | 1 | -1 |
| 客户端工具数 | 2 | 1 | -1 |
| 客户端主机数 | 2 | 1 | -1 |
| 表对象数 | 24 | 18 | -6 |
| 操作类型数 | 12 | 18 | 6 |
| 明细语句数 | 401 | 3210 | 2809 |

## 3. 对比图表

(1) 源 IP 对比

按小时统计每日零点开始的源 IP 数，鼠标停留时显示当小时基础对象和比较对象的源 IP 数。

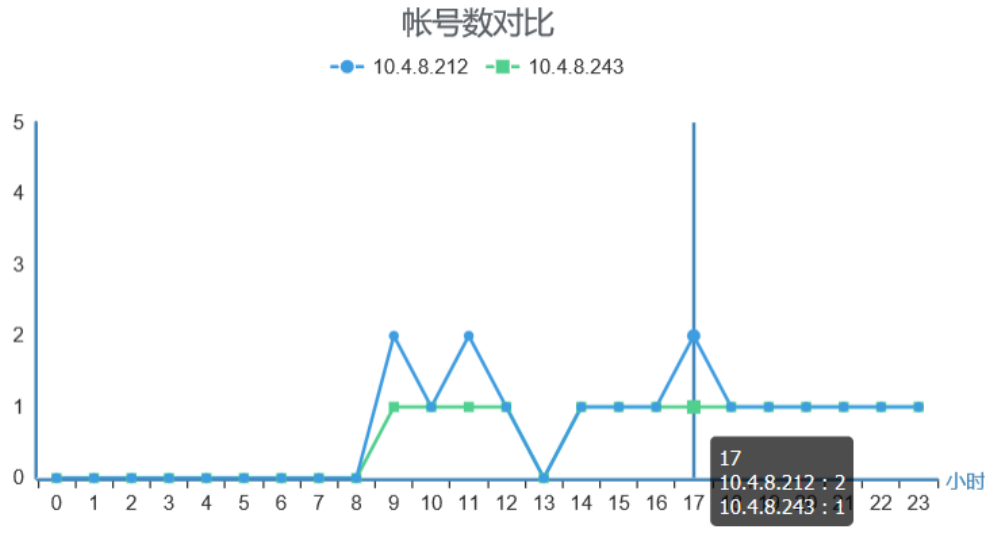
图3-46 源 IP 对比




(2) 账号数对比

按小时统计每日零点开始的账号数，鼠标停留时显示当小时基础对象和比较对象的账号数。

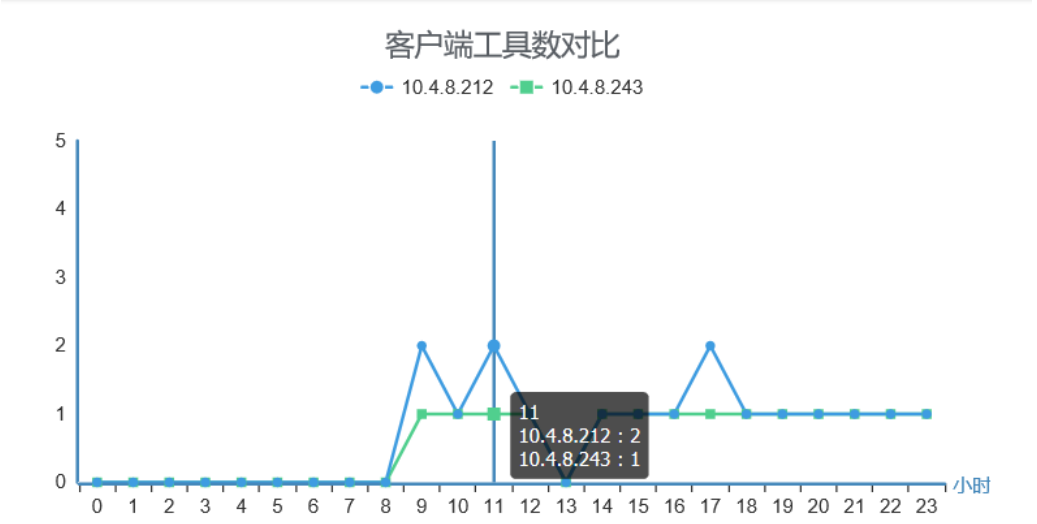
图3-47 账号数对比




(3) 客户端工具数对比

按小时统计每日零点开始的客户端工具数，鼠标停留时显示当小时基础对象和比较对象的客户端工具数。

图3-48 客户端工具数对比




(4) 客户端主机数对比

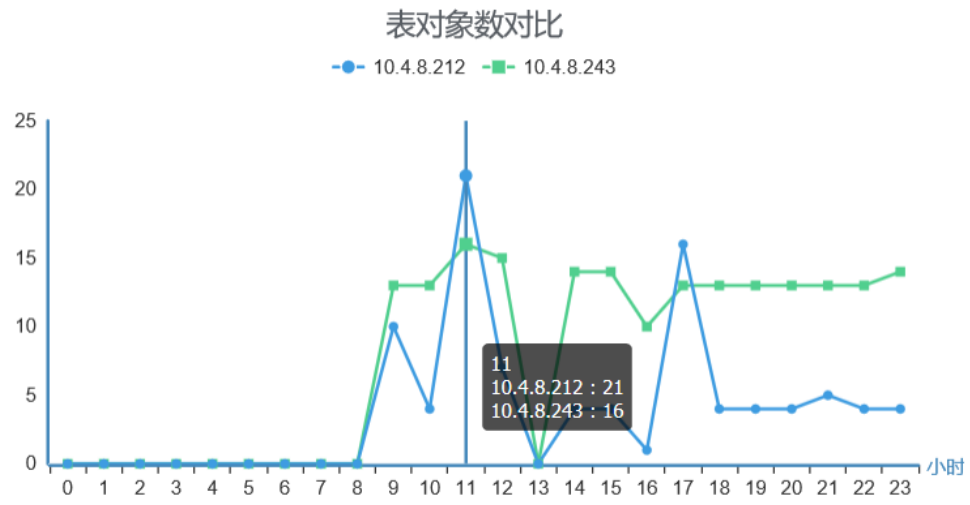
按小时统计每日零点开始的客户端主机数，鼠标停留时显示当小时基础对象和比较对象的客户端主机数。

图3-49 客户端主机数对比


(5) 表对象数对比

按小时统计每日零点开始的表对象数，鼠标停留时显示当小时基础对象和比较对象的表对象数。

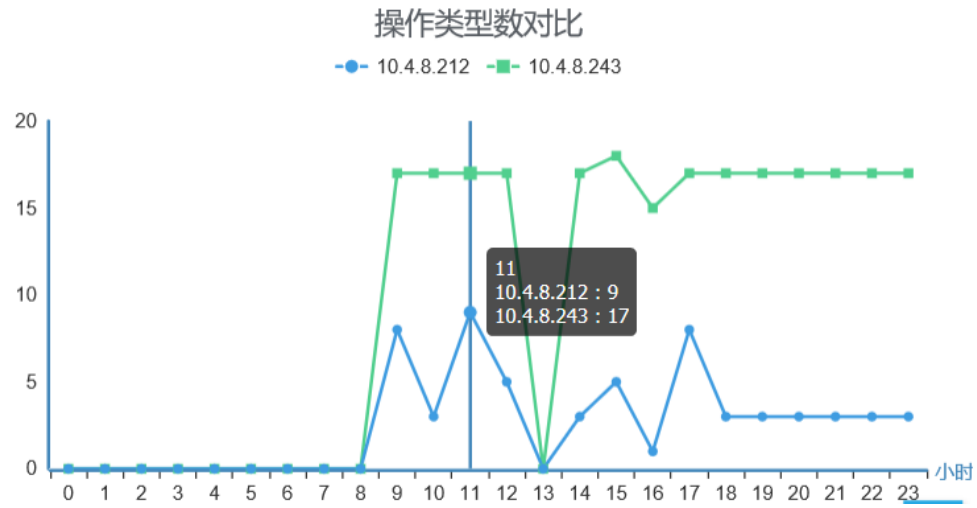
图3-50 表对象数对比




(6) 操作类型数对比

按小时统计每日零点开始的操作类型数，鼠标停留时显示当小时基础对象和比较对象的操作类型数。

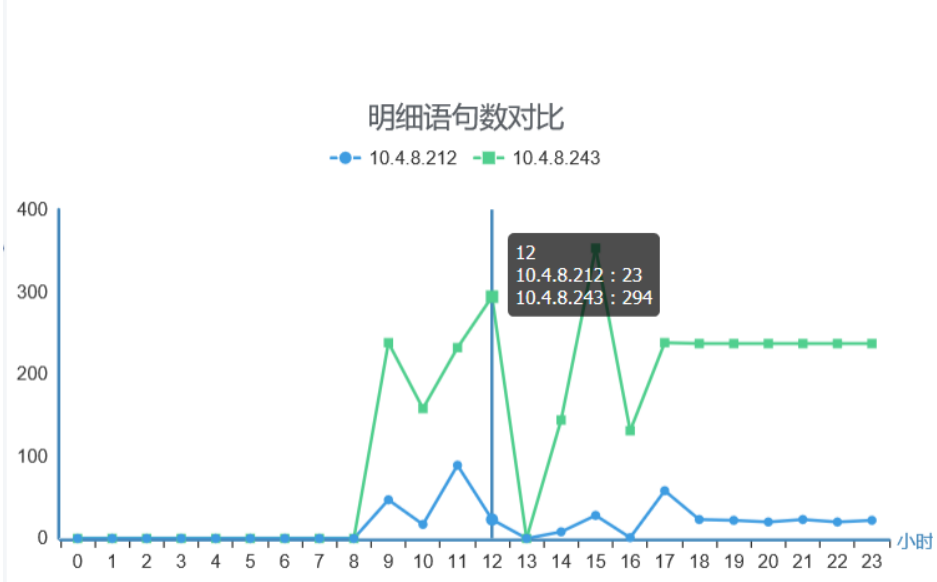
图3-51 操作类型数对比




(7) 明细语句数对比

按小时统计每日零点开始的明细语句数，鼠标停留时显示当小时基础对象和比较对象的明细语句数。

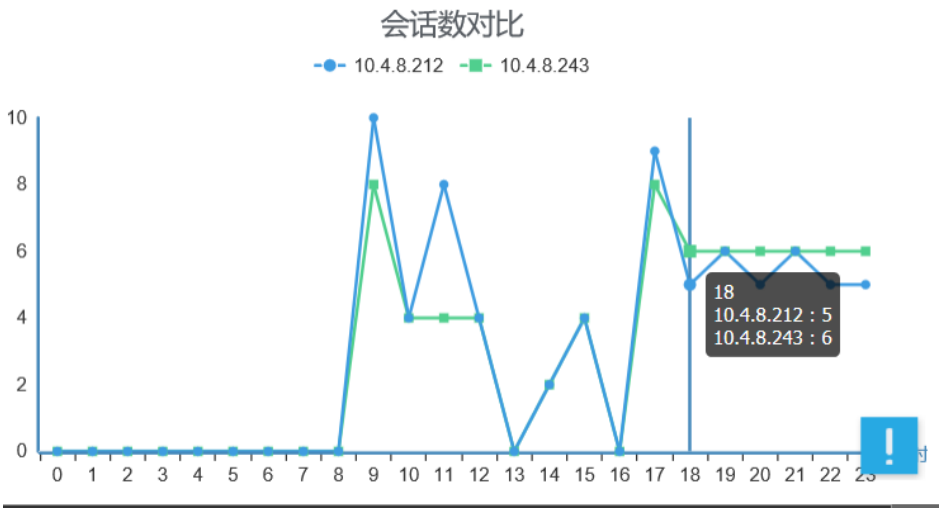
图3-52 明细语句数对比




(8) 会话数对比

按小时统计每日零点开始的会话数，鼠标停留时显示当小时基础对象和比较对象的会话数。

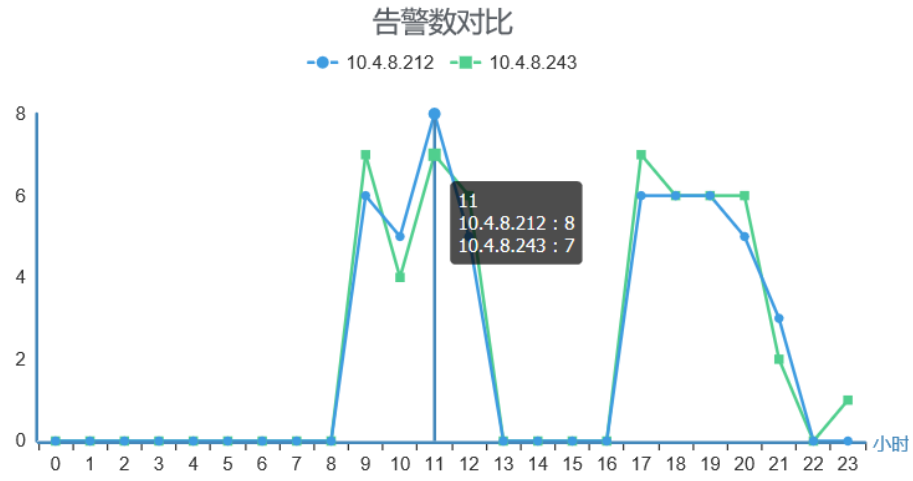
图3-53 会话数对比




(9) 告警数对比

按小时统计每日零点开始的告警数，鼠标停留时显示当小时基础对象和比较对象的告警数。

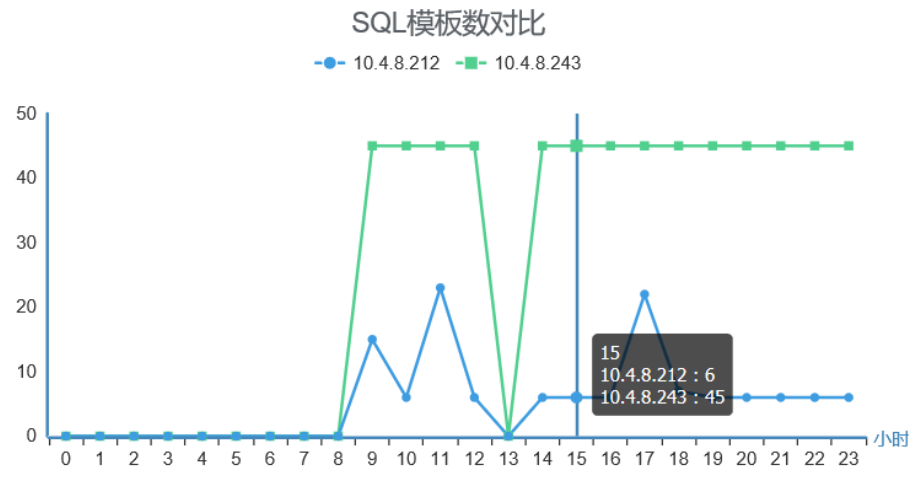
图3-54 告警数对比




(10) SQL 模板数对比

按小时统计每日零点开始的 SQL 模板数，鼠标停留时显示当小时基础对象和比较对象的 SQL 模板数。

图3-55 SQL 模板数对比



# 4 报表中心

## 4.1 概述

用户关心的与业务紧密关联的各种数据统计报表。用户可以通过报表任务管理设置各种类型的报表。另外，事件报表是对系统审计到的高风险事件，并鉴定为风险事件。

报表中心包括三个模块：报表任务、事件报表、报表查看。用户可以在报表任务中指定各种报表计划，然后在事件报表中查看已生成各种的报表。

图4-1 报表中心


## 4.2 报表任务

报表任务，是生成报表的依据，包含两种类型：自定义，系统默认。自定义报表任务，是系统根据用户制定的任务生成符合条件的报表；系统默认提供了七个报表任务，生成的报表也可以在[监控中心/流量钻取]中查看。

报表任务界面主要操作有：查看报表、新建报表、编辑报表、删除报表、导入报表配置、导出报表配置等功能。

左栏菜单中点击[报表中心/报表任务]即可在功能区中管理报表任务，如下图所示：

图4-2 报表任务


报表任创建后，目前系统默认会在 00:00——07:00 期间生成报表，生成的报表将会保存 30 天，30 天后将被删除。所以，需要保留的报表请在此期间将报表导出。

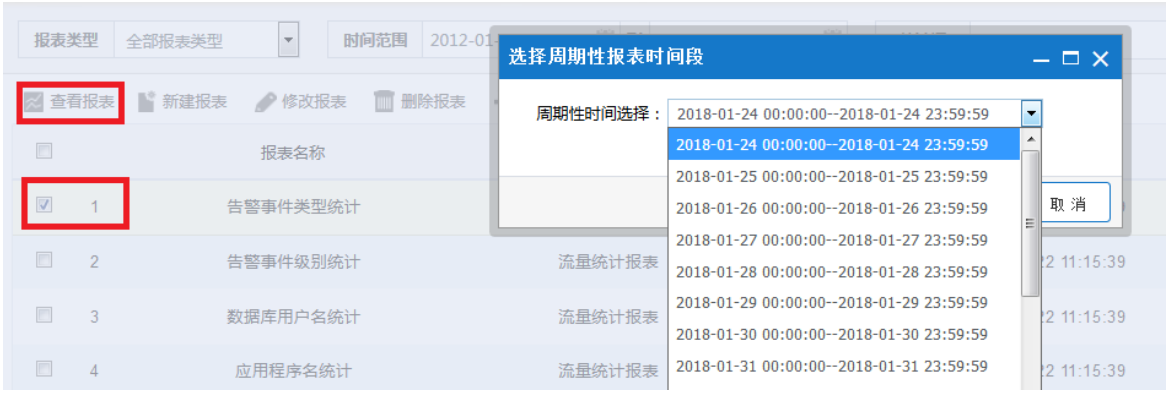
### 4.2.2 查看报表

在报表任务界面中，查询报表任务后，可以直接查看该报表任务的执行结果，即已生成的报表。在检索条件中输入报表类型、关键词、时间范围等查询条件，点击报表查询按钮，符合条件的报表将以列表形式展示，如下图所示：

图4-3 查看报表


选择某报表任务，然后点击  按钮，在弹出[选择周期性报表时间段]窗口中选择时间范围，如下图所示：

图4-4 选择任意报表查看

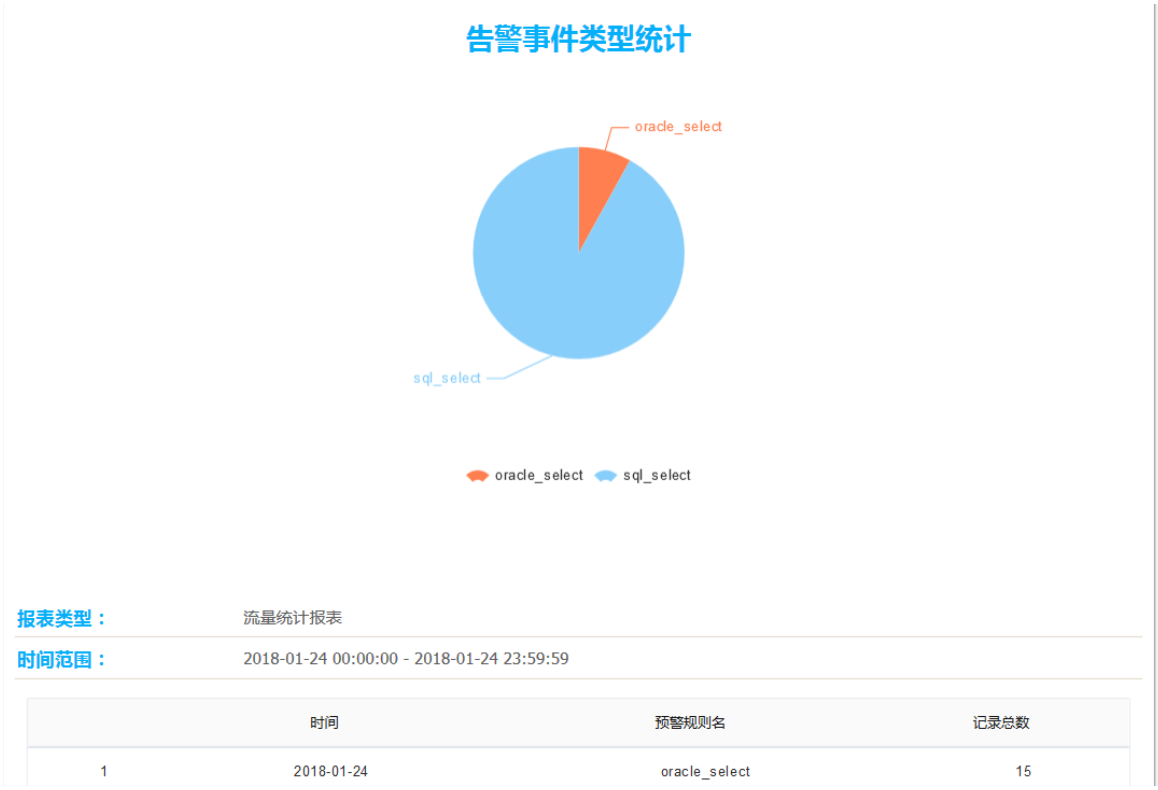



说明

在这里可以选择按照任务生成的所有未归档的报表任务，即使报表中符合条件没有数据。

点击<确定>后，报表将弹出新的页面展示报表，用户可以将报表内容打印或导出。如下图所示：

图4-5 告警事件类型统计




报表任务的状态主要有两种：已完成和预备中，表示报表任务的完成状态。如下图所示：

图4-6 报表状态


| | 报表名称 | 报表类型 | 进度状态 | 制定时间 | 展示类型 |
|---|---|---|---|---|---|
| 1 | 告警事件类型统计 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 2 | 告警事件级别统计 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 3 | 数据库用户名统计 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 4 | 应用程序名统计 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 5 | 客户端计算机名统计 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 6 | 操作方式统计 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 7 | 执行时长大于20秒 | 流量统计报表 | 已完成 | 2018-01-22 11:15:39 | 流量钻取展示 |
| 8 | 1 | 流量统计报表 | 预备中 | 2018-04-11 15:06:16 | |

### 2. 已完成

表示该任务至少已经完成了一次（一次性报表）或一个周期（周期性报表），可以查阅。

### 3. 预备中

报表任务已经建立，由于还没有到执行时间，第一次报表任务还未完成。

说明

目前系统默认会在 00:00——07:00 期间生成报表。

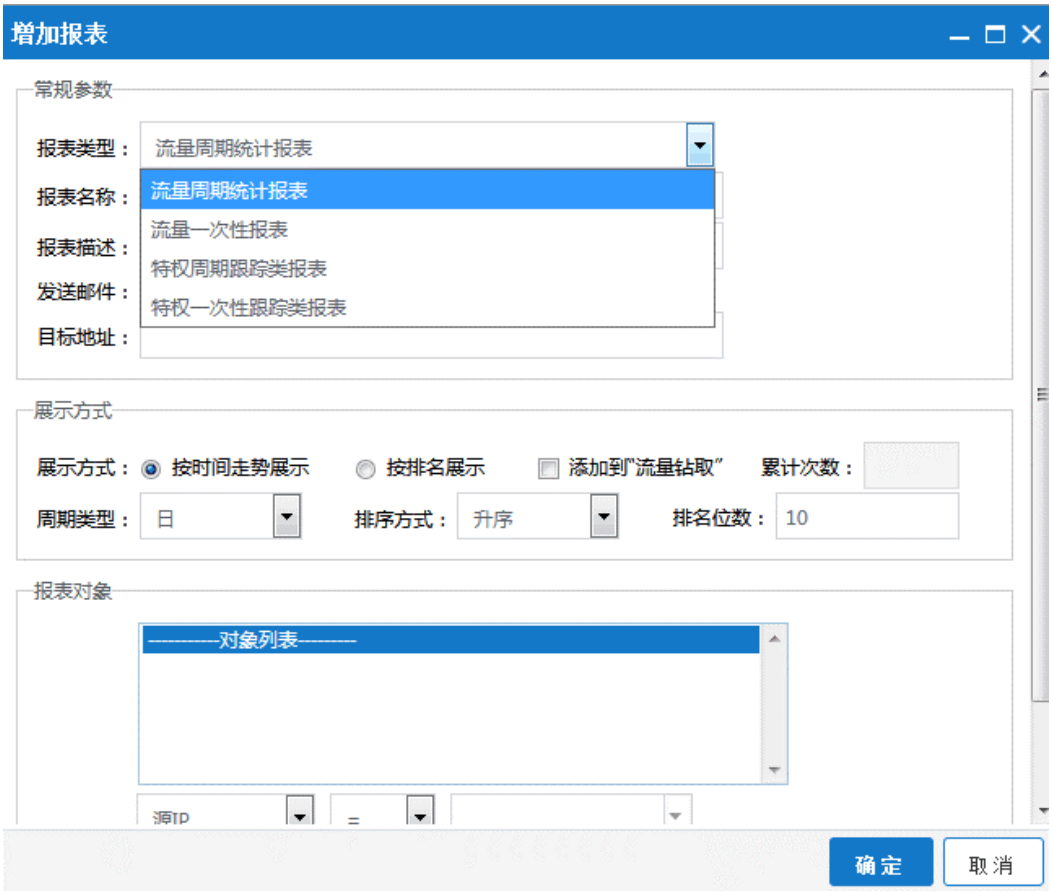
## 4.2.3 新建报表任务

新建报表任务，让系统定期生成报表。目前系统支持的常规报表模板内容主要有：流量统计、特权跟踪类。每类报表又可以分为：一次性（只生成一次，不重复）、周期性（将会重复、周期性的生成）。

可实现对告警的统计报表，根据时长、累计次数、累计条件（对象）进行周期性统计。

点击[报表任务/新建报表]，将弹出[增加报表]窗口，支持的报表任务有以下几种，如下图所示：

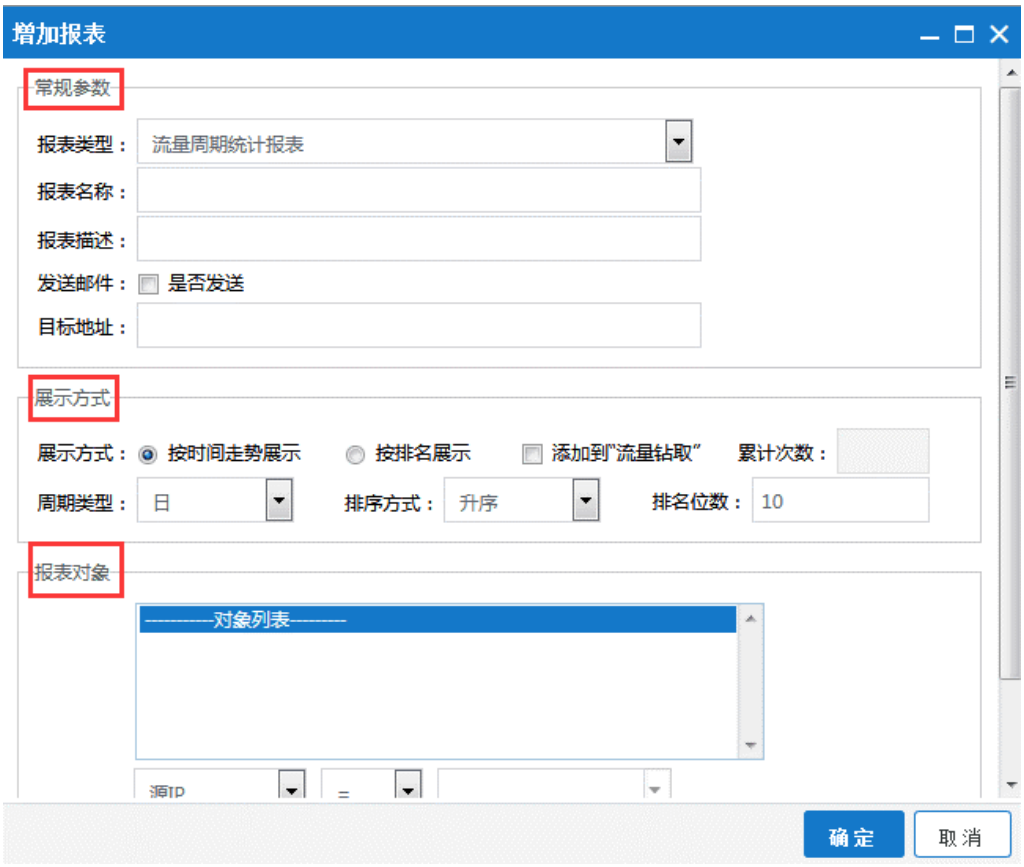
图4-7 增加报表




## 2. 新建“流量周期统计报表”

需要配置的参数主要有这几个方面：常规参数、展示方式、报表对象。下面将详细各项参数：

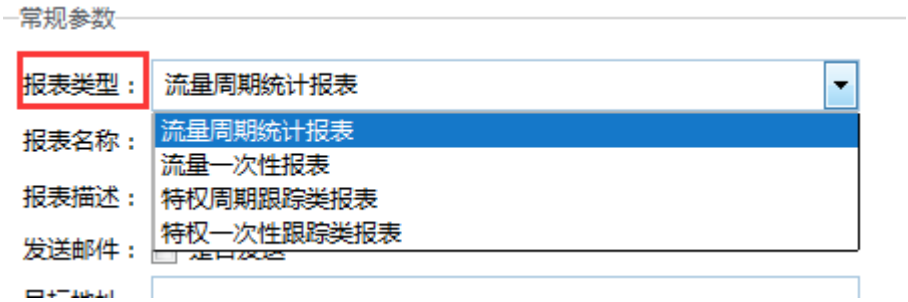
图4-8 增加报表




(2) 报表类型

需要生成的报表类型，通过下拉列表选择。如下图所示所示：

图4-9 报表类型

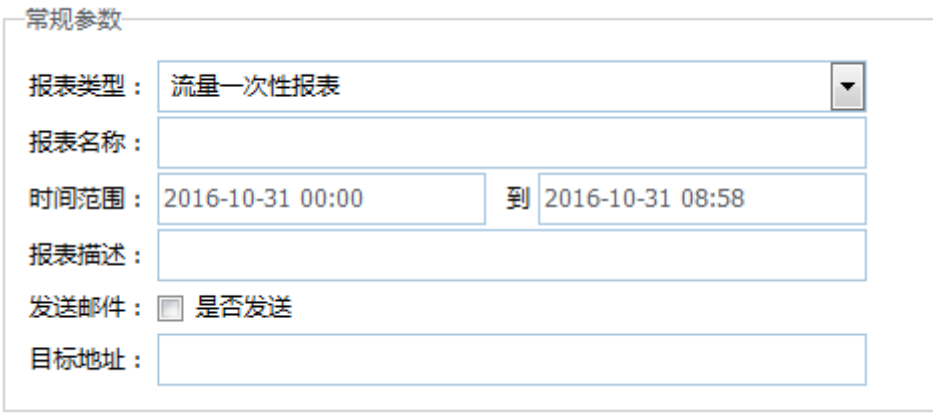



(3) 常规参数设置

设置报表任务的备注信息，以及是否发送到邮件。周期性报表任务和一次性的参数不太一样，如下图所示：

- 一次性报表任务_常规参数设置

图4-10 常规参数




- 周期性报表任务_常规参数设置

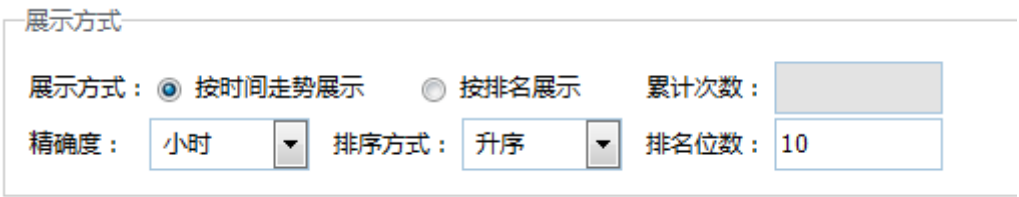
图4-11 常规参数设置


(4) 展示方式设置

报表展示方式配置，例如是按趋势或排名方式展示等信息。周期性报表任务和一次性的参数不太一样，如下图所示：

- 一次性报表任务_展示方式设置

图4-12 图 展示方式



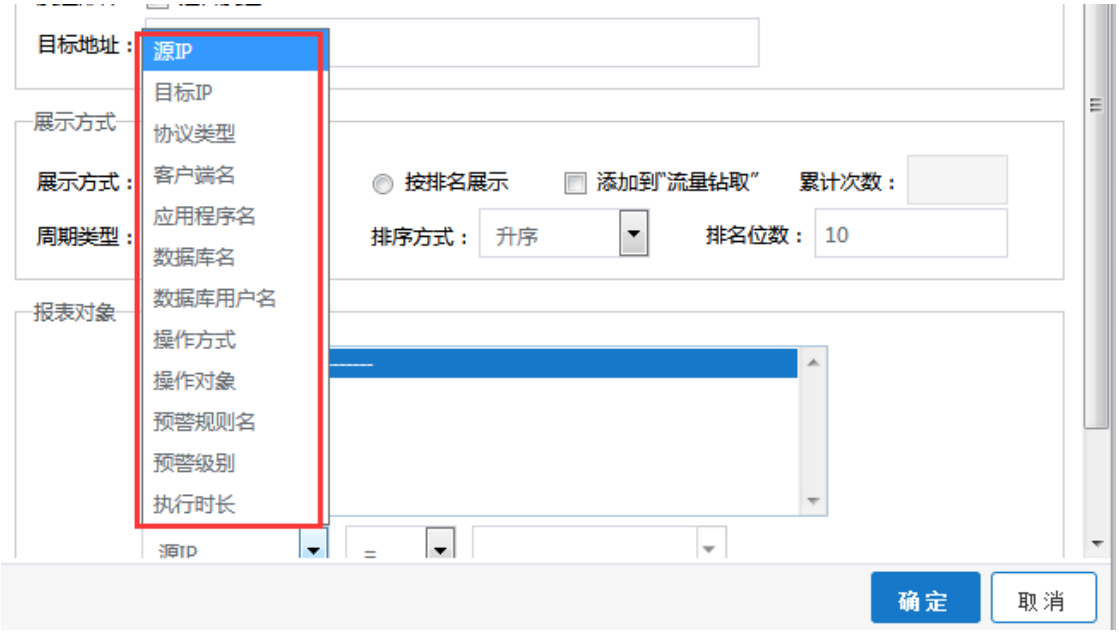

- 周期性报表任务_展示方式设置

图4-13 展示方式设置


(5) 报表对象设置

设置生成报表的数据来源，一次性报表任务和周期性报表任务的该项设置内容都一样，如下图所示：

图4-14 数据来源

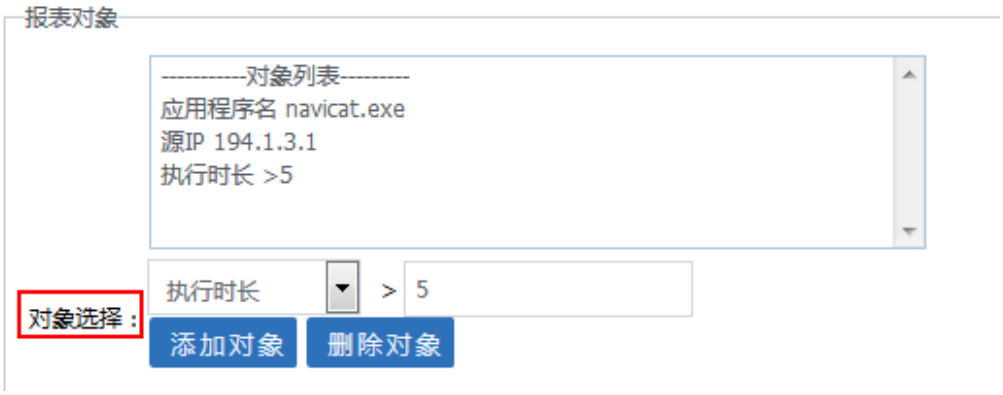



如上图中新建的报表内容是：对每周 SQL 语句中“应用程序名=charge，且源 IP=11.9.1.82，执行时长>5s”的语句进行统计，统计结果按照升序排序的方式展示前 10 个符合条件的结果。

- 添加对象

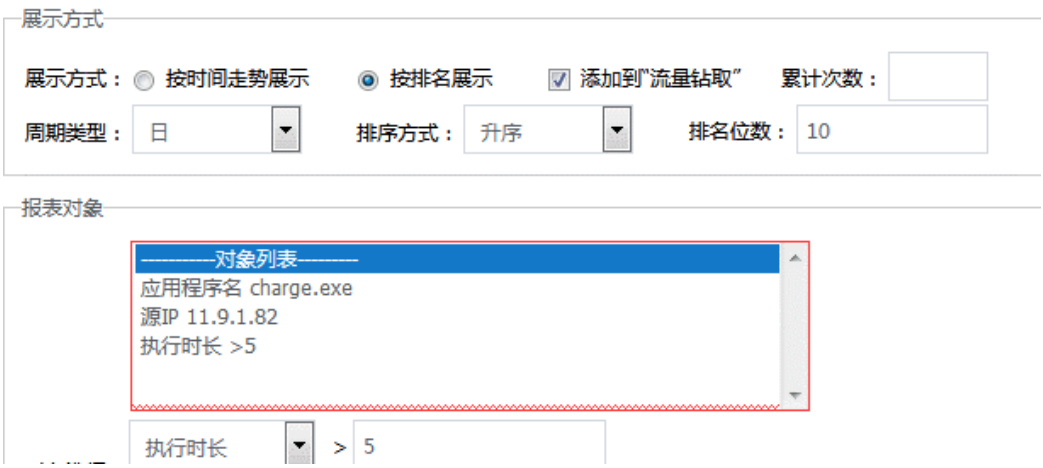
  在左边的下拉列表中选择需要展示的字段，在右侧下拉列表中选择需要统计的字段内容。选好后点击 添加对象 按钮将对象添加到上面的文本框中。也可以在文本框中选择某对象点击 删除对象 按钮删除该对象。如下图所示：

图4-15 对象选择




允许将流量周期统计报表发送到[监控中心/流量钻取]中展示，但要求“报表对象”列表中的统计对象最多只能为两种。如下图所示报表配置无法进行流量展示：

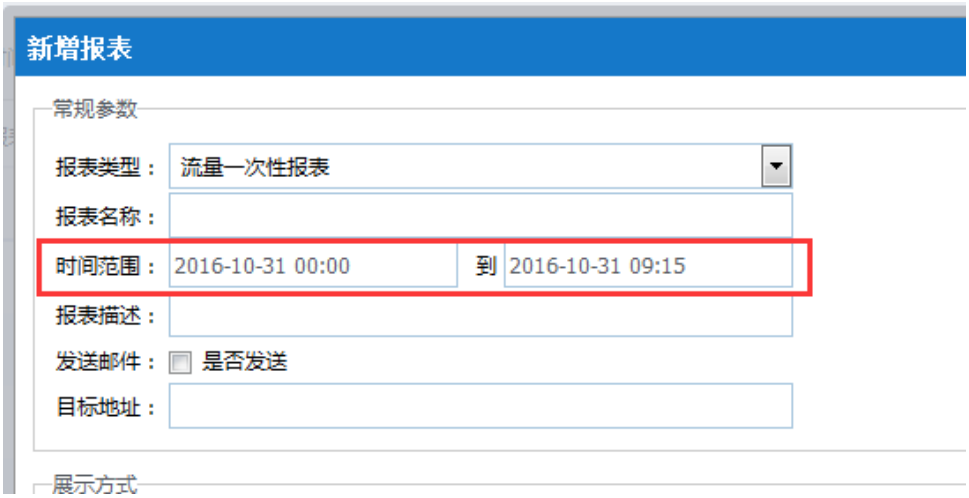
图4-16 对象列表




### 3. 新建“流量一次性报表”

设置与新建流量周期统计报表相似，最大的区别在于，要设置生成报表的时间范围。如下图所示：

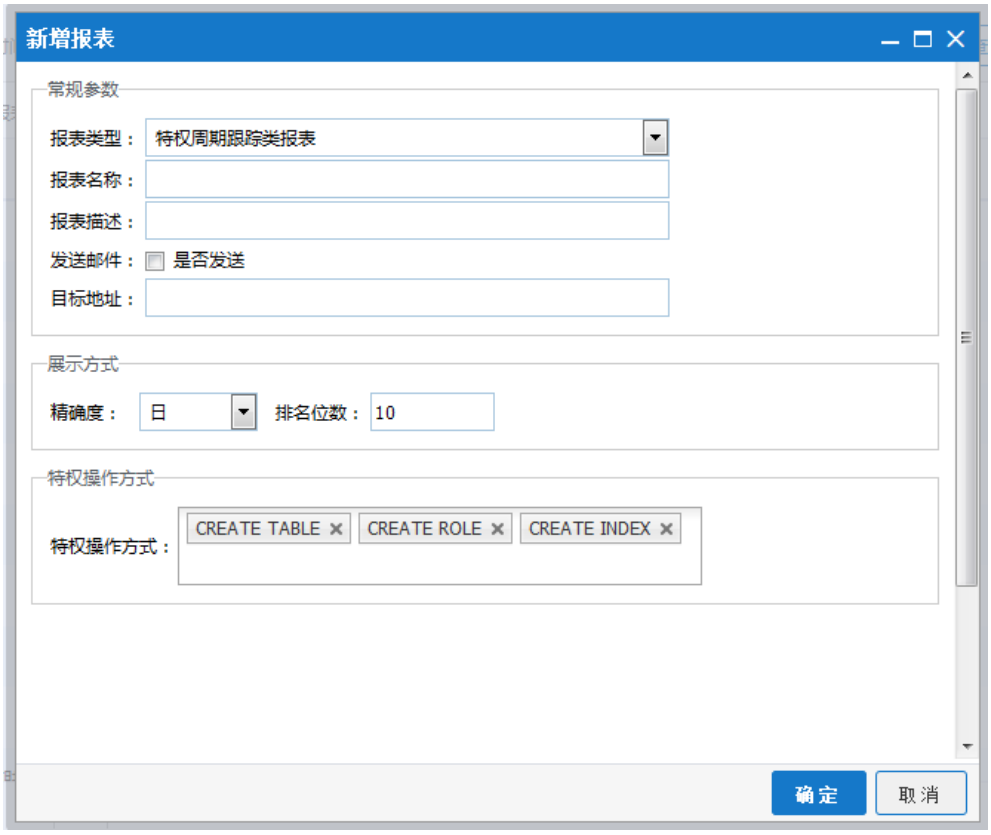
图4-17 新增报表




### 4. 新建“特权周期跟踪类报表”

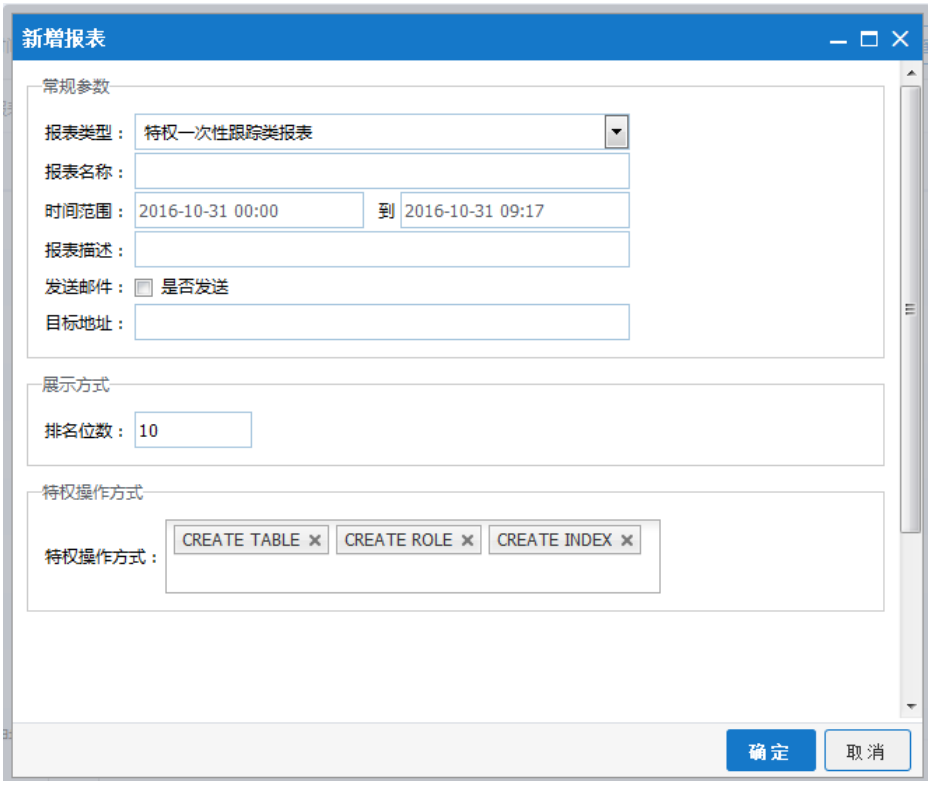
对某些特权操作进行跟踪按照设置的范围进行周期性统计。如下图所示所示：将对每天中包含 create table、create role、create index 三种操作方式的 SQL 语句分别进行统计。

图4-18 新增报表



5. 新建“特权一次性跟踪类报表”

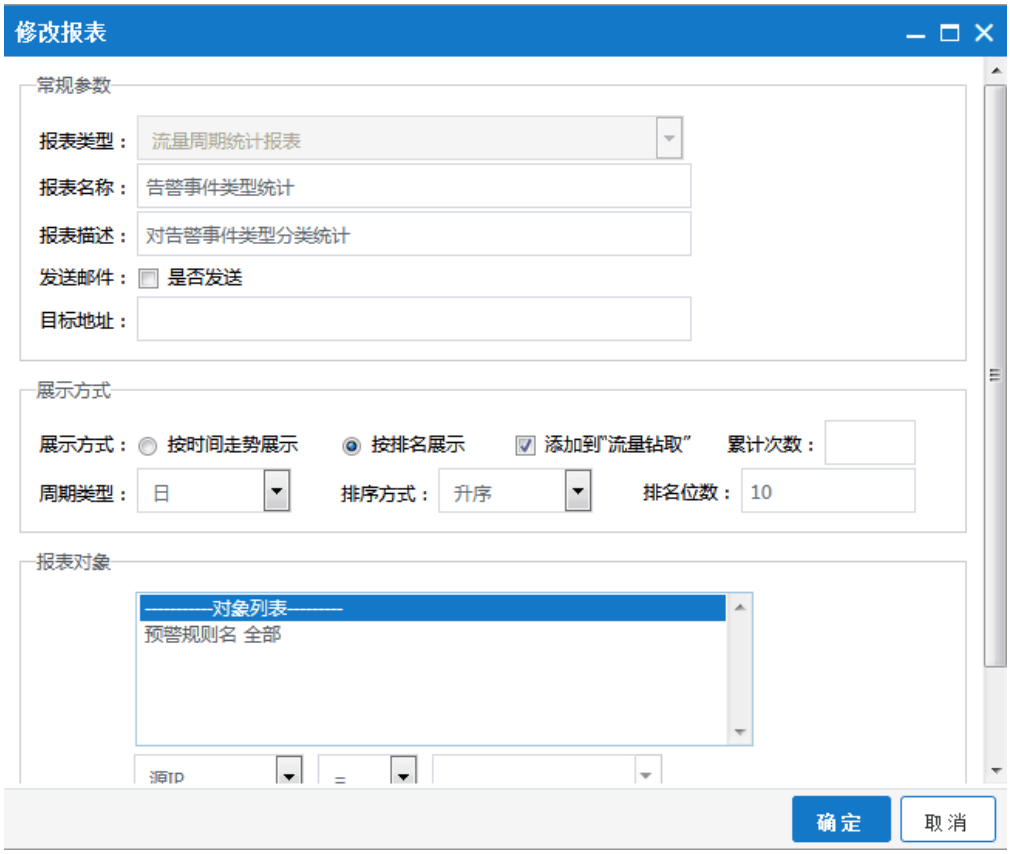
图4-19 新增报表




## 4.2.4 编辑报表任务

选择某报表任务，点击<修改报表>按钮，可以修改报表任务的内容。报表任务正在执行的时候，点击<编辑>只能查看内容。如下图所示：

图4-20 修改报表




## 4.2.5 删除报表任务

选择一个或多个某报表任务，点击<删除报表>按钮，将删除彻底该报表任务，不再执行该任务。

图4-21 删除

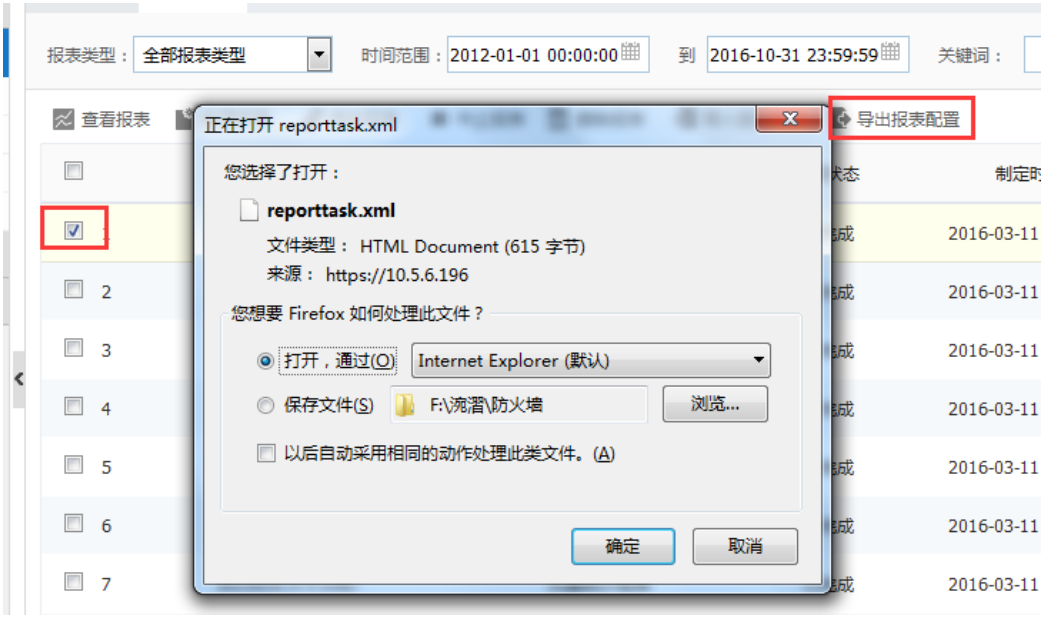
### 4.2.6 导入导出报表配置

系统提供的报表配置的导入导出，只需要将报表任务配置导出，若报表任务被删除了，管理员不需要重新新建任务，只需重新导入该任务的报表配置文件即可。简化了报表任务的管理工作。

#### 1. 导出报表配置

勾选某个报表任务，点击 导出报表配置 按钮，在弹出的提示框中将.xml 文件保存或打开。如下图所示：

图4-22 导出报表配置




说明

点击<确定>按钮上方的浏览可以将文件保存到指定目录。

#### 2. 导入报表配置

点击 导入报表配置 按钮后，在弹出[导入报表配置]窗口中点击<浏览>找到之前导出的报表配置文件，点击<确定>即可。如下图所示：

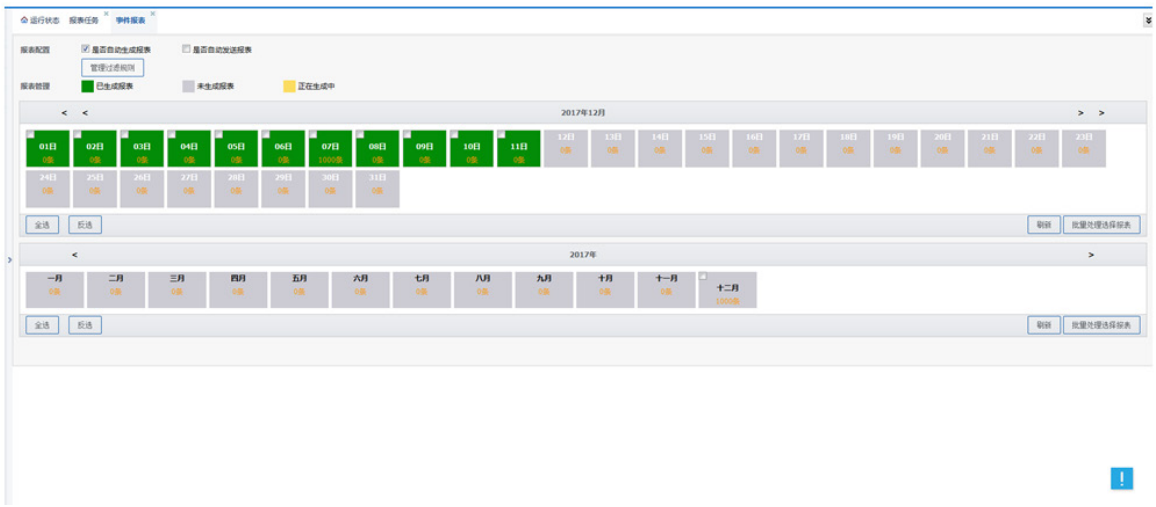
图4-23 导入报表配置


## 4.3 事件报表

事件报表主要是对“年报表”和“月报表”两个模块。通过不同的色块能对一目了然的查看当前月份和本年所有月的高危报表生成情况。同时支持对报表进行编辑。

点击左栏的菜单的[报表中心/事件报表]进入界面，如下图所示：

图4-24 事件报表



### 4.3.2 报表配置

进入事件报表后，可以看到界面上方的报表配置如下图所示：

图4-25 报表配置

### 2. 自动生成报表

勾选“是否自动生成报表”，系统就会根据现有过过滤规则、统方规则，在系统配置的报表生成时间自动生成报表。

### 3. 自动发送报表

勾选“是否自动发送报表”，系统将生成的报表自动发送到用户指定的邮箱。

### 4. 管理过滤规则

点击<管理过滤规则>按钮，弹出[管理过滤规则]页面，如下图所示：

图4-26 管理过滤规则


该界面主要提供的给已添加的过滤规则，提供删除的功能。用户如果发现这些（源 IP、目标 IP、SQL 相似度、操作方式、操作对象、规则编号、应用程序名）对象的具体内容存在不安全因素，可以勾选具体项将其删除。

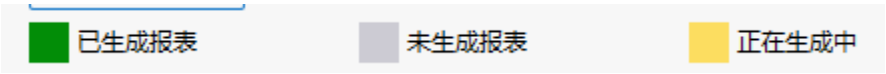
## 4.3.3 报表管理

报表管理包含“日报表的管理”和“月报表的管理”。

### 1. 报表生成状态

绿色表示已生成报表，灰色未生成报表，黄色表示正在生成中的报表。如下图所示：

图4-27 报表生成状态




说明

只有已“生成的报表”才具有查看和编辑功能。“未生成的报表”和“正在处理的报表”无此功能。

## 2. 报表查询

点击时间那一栏的对应的箭头，对应的是分别是“上一年”、“上一月”或“下一年”、“下一月”。

图4-28 查询


在展示列表中直接显示了某天，或者某月的高危记录条数，并且可以对他们进行编辑、查看详细等操作。如下图所示：

图4-29 功能


## 3. 编辑报表

点击  按钮以图表的形式展示了各个过滤字段的统计情况，在列表中可以通过勾选修改过滤规则，如下图所示：

图4-30 编辑


## 4. 查看报表详情及处理

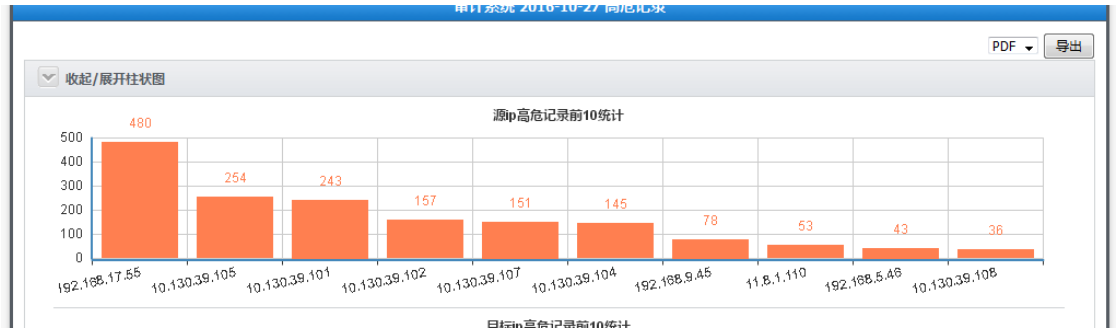
点击在已生成的报表上悬浮的  按钮，可以查看报表详情。主要包含三部分：柱状统计图，严重（高可疑）事件展示列表、报表小结。

(1) 柱状统计图

柱状统计图展示了被审计到的记录中关键信息的前十名统计情况。系统统计内容主要有：源 IP 高危记录前十统计、目标 IP 高危记录前十统计、SQL 相似度高危记录前十统计、操作方式高危记录前十统计、操作对象高危记录前十统计、规则编号高危记录前十统计、应用程序名高危记录前十统计。

如下图所示是源 IP 高危记录前十统计：

图4-31 统计




(2) 事件展示列表

图4-32 事件展示列表

| IP | 时间 | 数据库表名 | 操作明细 | 分类 |
|---|---|---|---|---|
| 172.16.11.56 | 2016-10-27 11:13:51 | 未知 | login server | 严重 |
| 172.16.11.56 | 2016-10-27 11:14:03 | 未知 | login server | 严重 |
| 172.16.11.56 | 2016-10-27 11:14:04 | 未知 | login server | 严重 |
| 11.9.1.112 | 2016-10-27 11:14:16 | return_medicine_master,return_medicine_detail,sick_diagnosis_record,sick_diagnosis_record,sick_diagnosis_record,sick_diagnosis_record,lay_physic_queue_pool,lay_physic_queue_pool,lay_physic_window_config,staff_dict,base_dictv_lay_physic_union,sick_basic_info,department_dict,t.take_medicine_ways_dict,clinic_item_dict,bill_kin | SELECT a.apply_no apply_no, b.name sick_name, a.SICK_ID sick_id, b.sex sex, b.rate_type rate_type, decode(trunc(months_between(g.write_time ,b.birthdate),0),0,trun | 严重 |
| | | | select a.sick_id as sick_id, b.name as sick_name, b.sex as sex, decod | |

(3) 报表小结

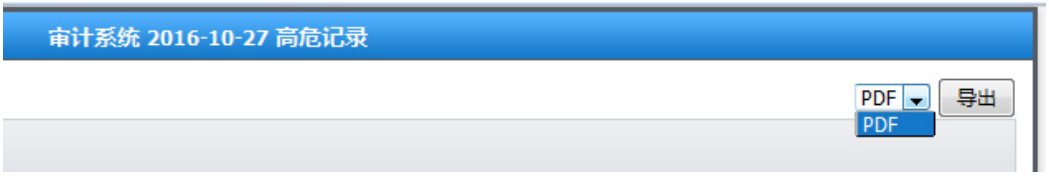
系统管理员在查阅了统方事件报表后可以对报表做概括性的总结，具体内容如下图所示：

图4-33 报表小结


(4) 报表导出

此外，系统还支持高危报表导出为 PDF 文件。如下图所示：

图4-34 导出



## 4.4 统方报告

统方报告界面可以通过编制人、编制单位检索和查看已生成的报告。点击左栏菜单中[报表中心/统方报告]进入界面。如下图所示：

图4-35 统方报告


- 报告查询

  在界面中输入编制人或编制单位信息，点击“查询”按钮进行查询。查询结果以列表的形式展示，并展示了创建日期、编制人、编制单位、报告概述等信息。

- 查看报告

  在查询结果列表中点击 查看报告 图标，将会在新页面中展示该事件报告。如下图所示：

图4-36 统方事件风险分析

统方事件风险分析

（版本Ver 1.0）

编制人：

编制单位：

创建日期：2017-02-14

◆基本信息:

"统方"特指在医药灰色产业链中，为商业目的的"统方"，其主要指医院中个人或部门为医药营销人员提供医院或部门在一定时期内临床用药量统计信息，供其作为发放药品回扣等不良违法行为的重要参考依据。
本报告根据先前定义的关键敏感信息，通过网络旁路的捕包分析，截获该疑似事件，关键信息如下：

| | | | |
|---|---|---|---|
| 发生时间 | 2017-02-13 16:49:33 | 事件ID | 4451094 |
| HIS数据库 | 10.5.8.243 | 中间件服务器 | 无 |
| 来源用户 | 10.4.8.243 | 使用工具 | plsqldev.exe(plsqldev.exe) |
| 触发条件 | 查询返回结果中包含以下敏感内容：yp_item(yp_item) | | |

◆事件描述:

该事件中 10.4.8.243 使用工具 plsqldev.exe ， 对 yp_item 进行了 查询 操作。涉及到 yp_name 等。

◆分析总结:

该用户利用HIS的 plsqldev.exe(plsqldev.exe) 模块进行了相关操作，疑似程度高，请重点关注。

◆原始数据:

select count ( yp_name ) from yp_item

关于报告的内容与介绍在统方事件中“生成报告”中已做详细说明，此处不再赘述。

- 查看统方事件

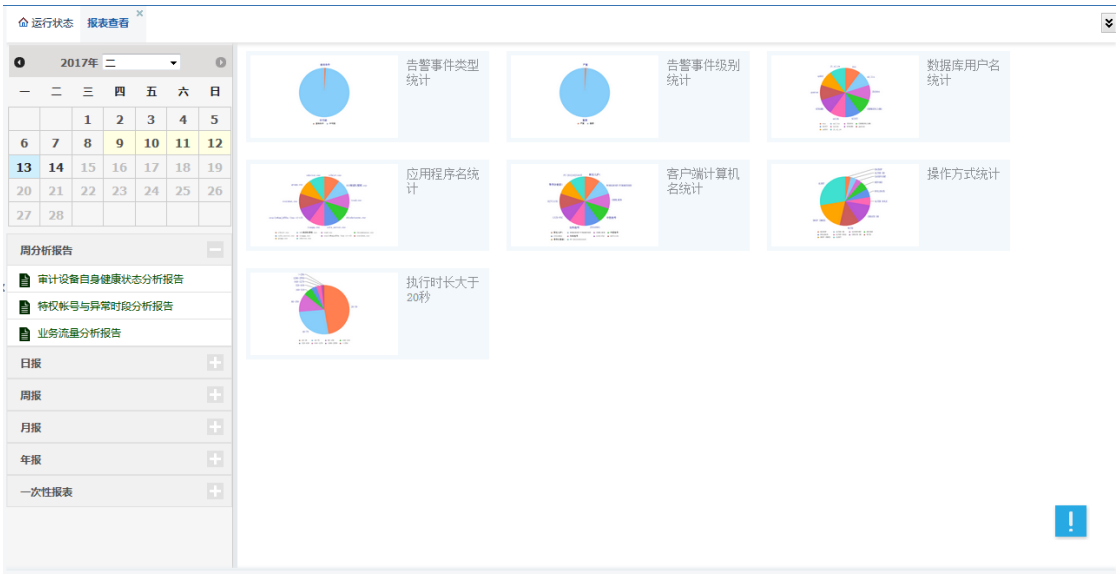
在查询界面中点击 

图标，将会跳转到统方事件查询页面。

## 4.5 报表查看

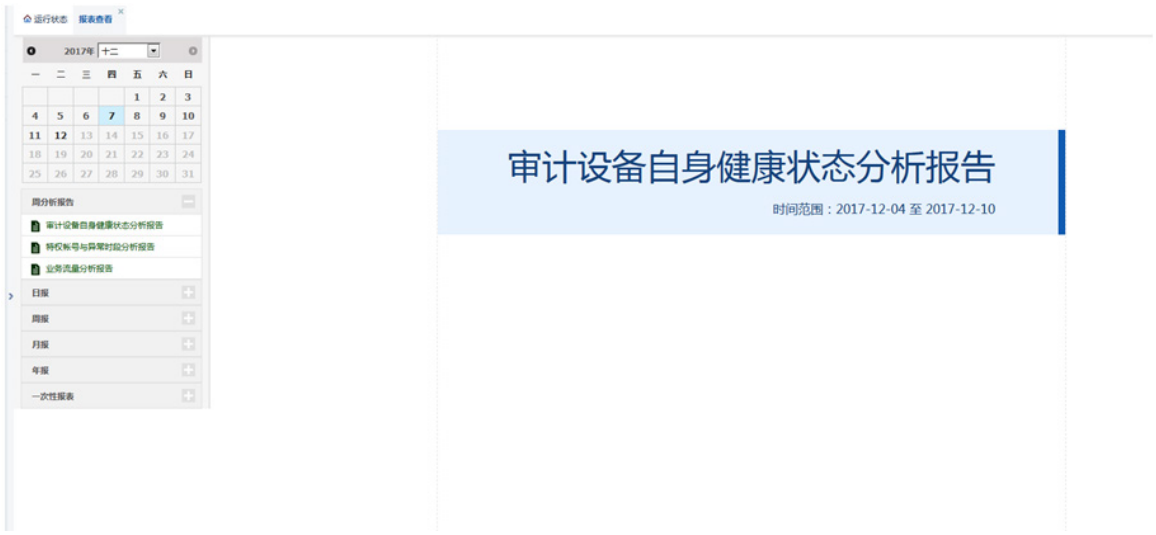
报表查看，以日历为主线向用户展示系统报表，简单、易用。有数据日期显黄色，无数据日期显灰色，方便使用查询。点击[报表中心/报表查看]进入页面，如下图所示：

图4-37 报表查看




页面是左右结构，左栏是菜单栏，右栏是报表展示区。左栏的上半部分是个日历表，下半部分是报表列表，根据生成周期分为：日报、周报、月报、年报、一次性报表。右栏报表展示区用于展示被选择的报表，并用图表和列表两种形式进行展示。所有报告和报表增加封面，提供报表缩略图功能，点击即可跳转到详细报表页面。

图4-38 详细报表



## 2. 周分析报告

每周更新提供审计设备自身健康状态分析报告、特权账号与异常时段分析报告、业务流量分析报告，有助于管理员了解设备运行情况、数据库业务安全状况。

(1) 审计设备自身健康状态分析报告

本分析报告提供对审计设备在一周范围内，设备发生异常状态的情况记录，并对异常情况进行分析形成报告，为反映审计设备自身的运行状况提供依据。如下图所示：

图4-39 审计设备自身健康状态分析报告


(2) 特权账号与异常时段分析报告

本分析报告提供对数据库在一周范围内，帐号在非业务处理时段的操作与特权帐号操作的监控记录，并对监控记录进行分析、得出结论，形成特权帐号与异常时段分析报告，以供反映数据库的业务安全状况，提供依据。如下图所示：

图4-40 特权账号与异常时段分析报告


(3) 业务流量分析报告

本分析报告提供在一周范围内，对数据库产生的语句流量、数据库账号使用情况、语句响应时长等进行分析，并形成报告，以供反映数据库业务安全状况。如下图所示：

图4-41 业务流量分析报告

### 3. 内置日报表

(1)　审计数据概况分析报表

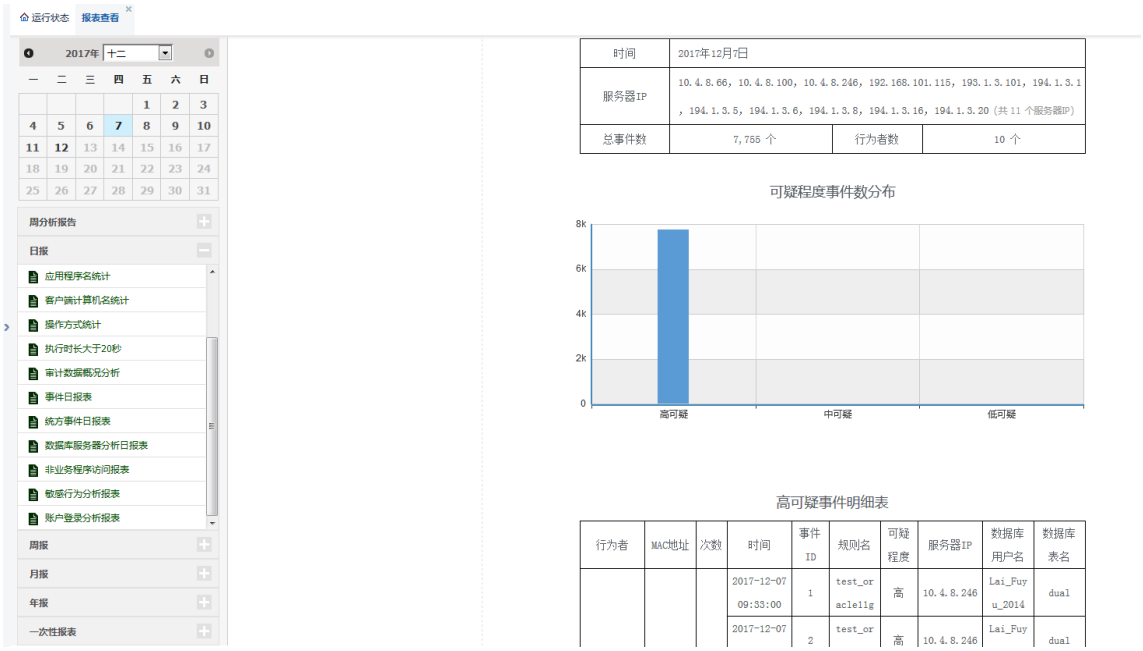
本报表每日、每周、每月针对在线用户数、并发会话数、明细记录数进行统计分析，便于管理员掌握此时段内系统的数据情况，如下图所示：

图4-42 审计数据概况分析报表


(2)　事件分析报表

本报表针对每日、每周、每月生成的告警事件统计分析，罗列出系统中发生高可疑、中可疑、低可疑风险事件的明细信息，对此时段内发生的事件一目了然，如下图所示：

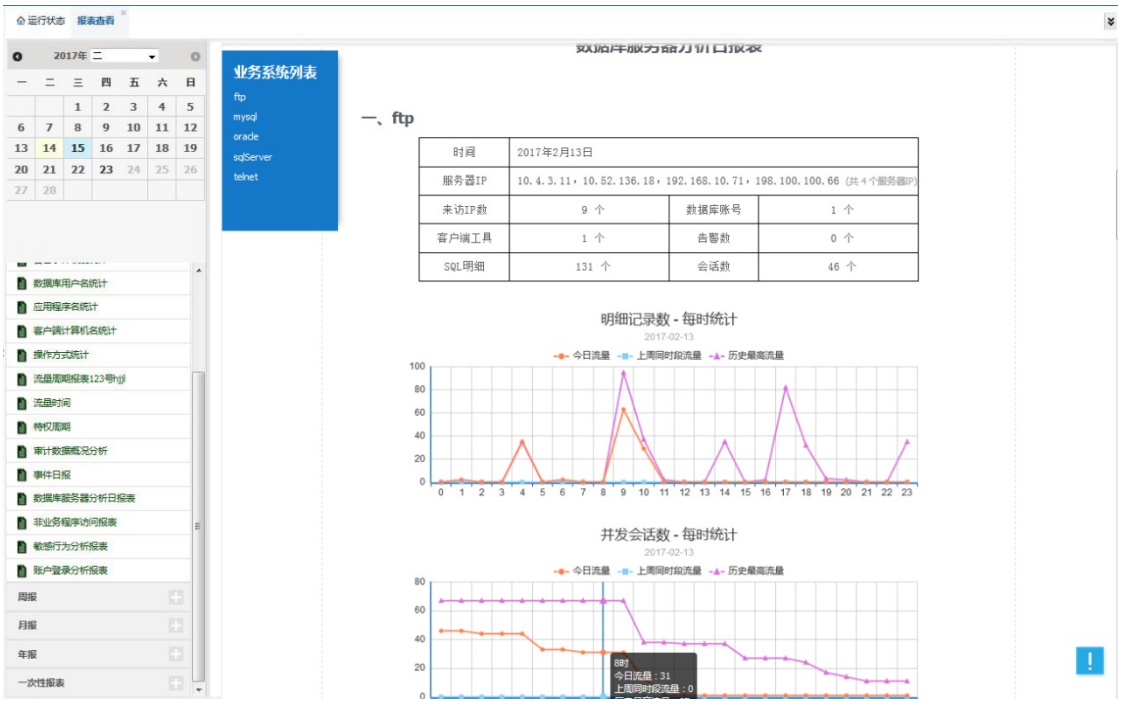
图4-43 事件分析报表




(3) 数据库服务器分析日报表

本报表以业务系统划分，针对业务系统服务器相关的一些统计分析，以供反映数据库服务器业务安全状况。如下图所示：

图4-44 数据库服务器分析日报表




(4) 非业务程序访问报表

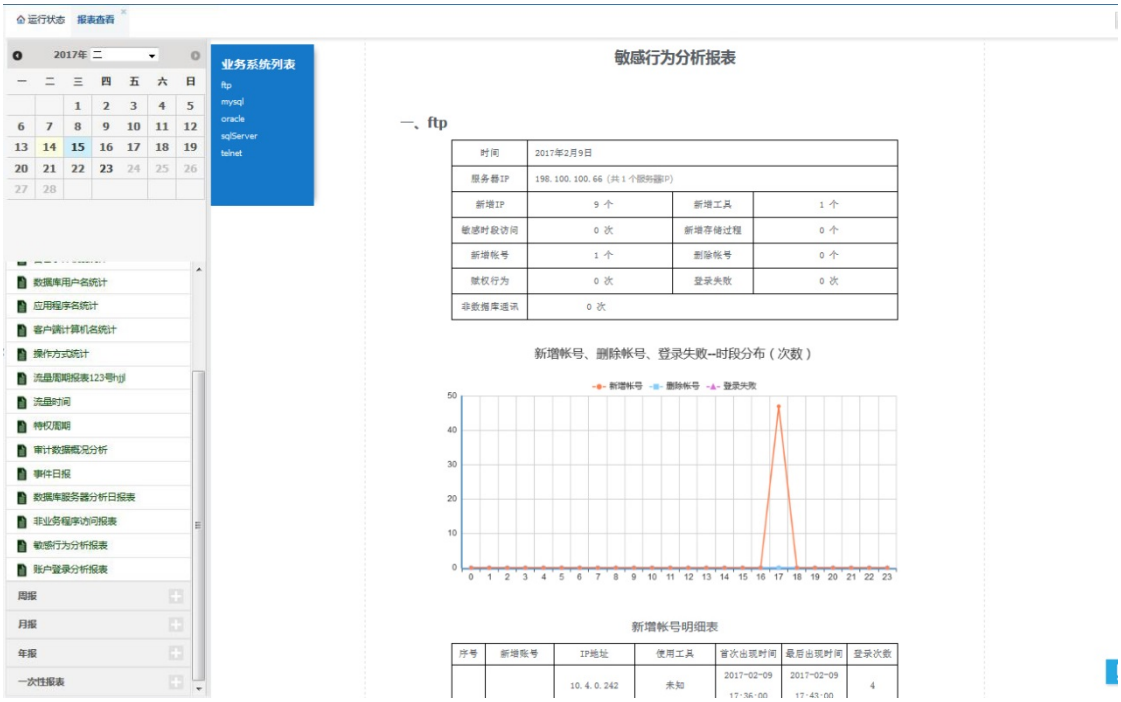
本报表以业务系统划分，统计业务系统的非业务程序访问情况，便于管理员了解业务系统安全。如下图所示：

图4-45 非业务程序访问报表


(5) 敏感行为分析报表

本报表以业务系统划分，是针对业务系统发生的各类敏感行为的统计分析，便于管理员从敏感行为角度分析业务系统的安全性。如下图所示：

图4-46 敏感行为分析报表




(6) 账户登录分析报表

本报表以业务系统划分，分析账户登录情况，快速了解是否可能存在账户破解或敏感时段登录的情况。如下图所示：

图4-47 账户登录分析报表

### 4. 查看报表

报表的查阅主要是以数据产生的日期为条件，即当选择某个日期后，左栏下半部分显示的是包含该天数据的所有报表，并根据生成周期进行分类展示。

(1)　选择要查看报表的日期

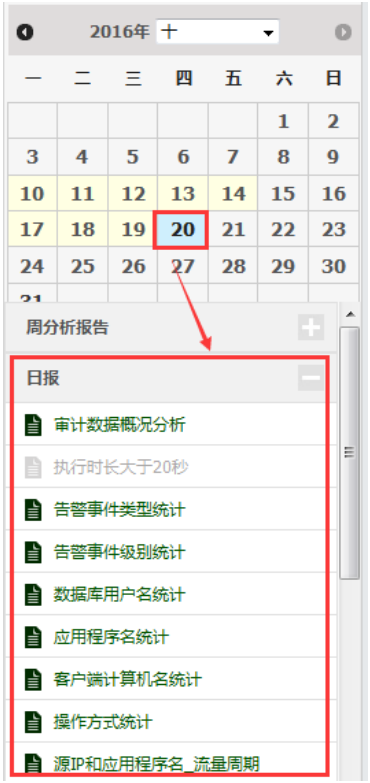
进入系统后，默认选择的是当天。日历中点击某天，便会在左栏下半部分展示与该天相关的所有报表，这些报表根据生成周期进行分类展示。

图4-48 分类


(2)　选择需要查报表的类别

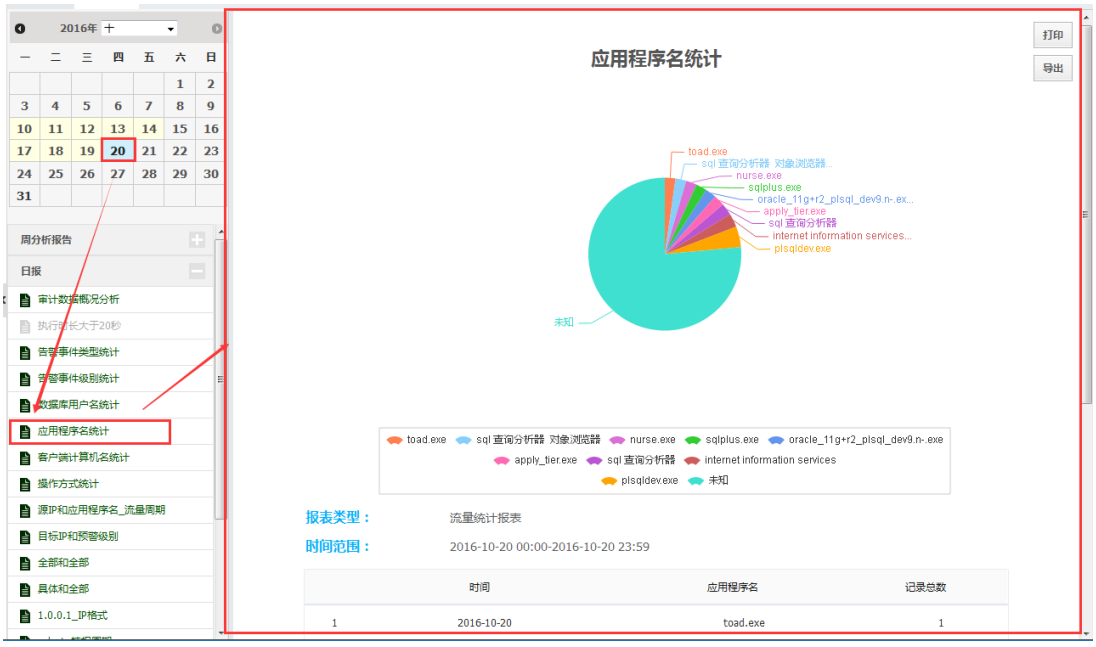
在报表类别中点击某类报表，便会出现符合条件的报表。如下图所示是查看 10 月 20 日“日报”中看到的有关报表：

图4-49 日报




在列表中点击某张报表即可在右栏中查看该报表的详细内容，如下图所示是点击上图中“应用程序名统计”报表后看到的内容：

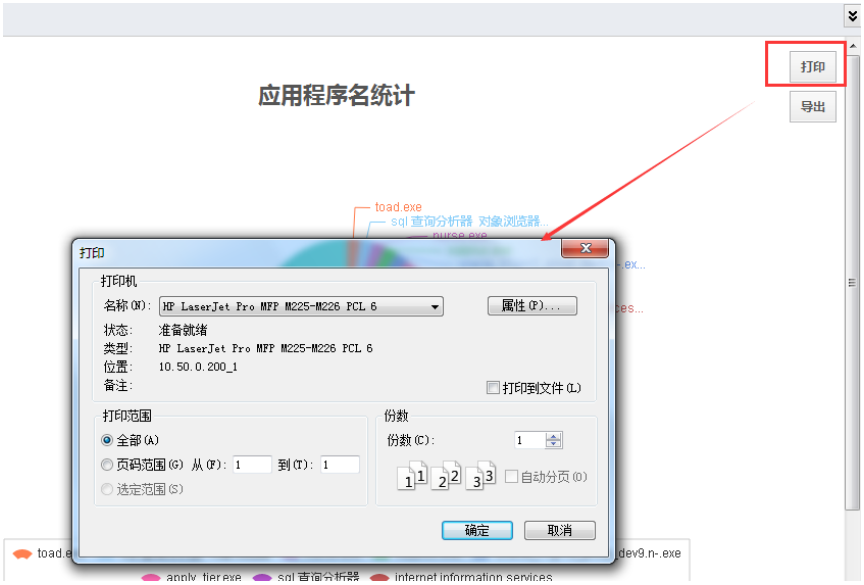
图4-50 选择报表



## 5. 打印报表

点击报表右上角的<打印>按钮在弹出对话框中选择打印机后打印即可。

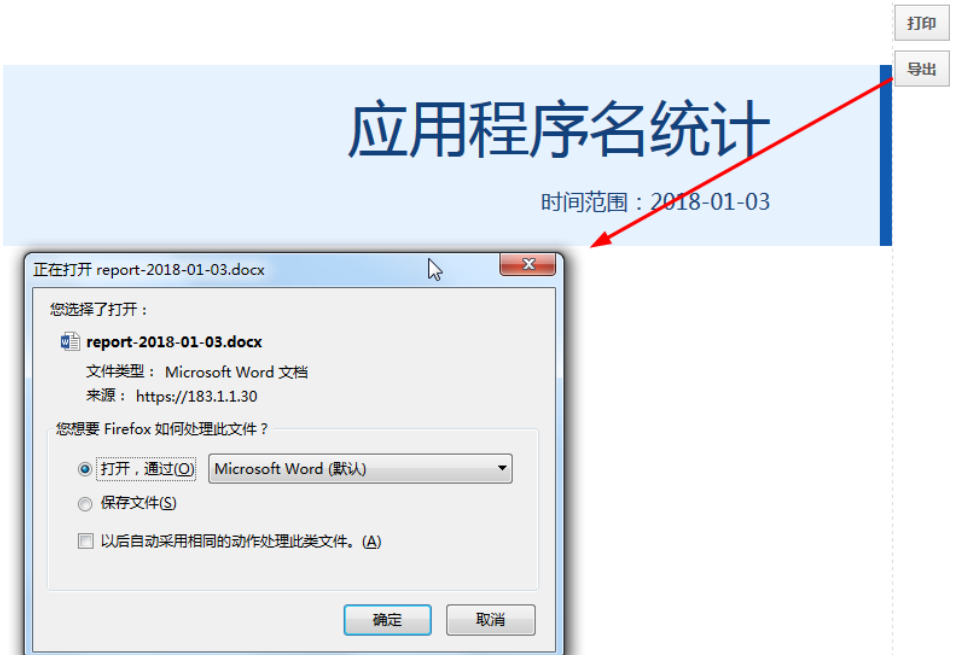
图4-51 打印




## 6. 导出报表

系统支持将报表导出成 Word 格式的文件，点击报表右上角的<导出>按钮，在弹出的提示框中选择<保存>或点击<保存>右侧的下拉列表可将文件另存到指定目录中。

图4-52 导出报表



# 5 策略中心

## 5.1 概述

策略中心，主要是配置审计内容，定义事件规则，还对系统中涉及的各种对象进行管理。是系统识别各类风险事件的第一步。

主要包含以下这些模块：监听配置、事件定义、对象管理、客户端信息、敏感信息、事件响应、三层关联、入侵检测规则、交换机信息等。左栏菜单如下图所示：

图5-1 策略中心


## 5.2 监听配置

监听配置模块主要功能是设置系统监听的范围，主要包括业务系统配置、三层应用服务配置、指定源 IP 审计。点击[策略中心/监听配置]进入界面，如下图所示：

图5-2 监听配置


## 5.2.2 业务系统配置

点击界面中的监听配置页面中的标签业务系统配置进入配置页面。系统可将多个数据库捆绑定义为一个业务系统，方便数据的统一展示，管理员在此设置需要监听的业务系统数据库和相关的行为。目前系统支持 Oracle、Sybase、DB2、Mysql、SQL server、Informix 等主流数据库，达梦、金仓等国产数据库，Postgresql、Cache 等专用数据库，以及 Telnet、Ftp、Vnc、Rdp、Ssh 等其他应用的审计。如下图所示：

图5-3 业务系统配置


界面中展示了已添加需要监听的业务系统数据库类型、字符集编码、IP 地址及端口号，此外还可以添加、删除、修改监听的业务系统。

### 2. 添加业务系统配置

点击<添加>按钮弹出[添加业务系统]对话框，如下图所示：

图5-4 添加业务系统配置


管理员只需填写业务系统的名称，勾选状态、编码策略、数据库类型，并配置服务器 IP 和监听端口号，点击<确定>即可。

说明

当编码策略设置为自动识别时，系统自动识别编码类型，后可手动修改。当 IP 设置为 0.0.0.0 时，系统自动审计所有被系统检测到的服务器。

### 3. 编辑业务系统配置

在列表中选择某业务系统后点击<修改>按钮便可以编辑、修改配置信息，如下图所示：

图5-5 编辑业务系统配置


### 4. 删除业务系统配置

点击选择某业务系统后，点击界面中的删除按钮，在弹出[确认]对话框中点击<确定>即可删除该配置信息。如下图所示：

图5-6 删除业务系统配置


## 5.2.3 中间件服务器配置

设置需要监听的协议服务器类型，主要配置内容包括 IP 地址和端口。点击监听配置页面中的中间件服务器配置标签，打开的界面如下图所示：

图5-7 中间件服务器配置


界面中展示了已添加的需要监听的 WEB 协议服务器 IP 地址及端口号，此外还可以添加、删除、修改服务器配置。

### 2. 添加监听的 WEB 协议服务器配置

点击 WEB 协议服务器配置标签的<添加>按钮弹出[添加应用服务器配置]对话框，如下图所示：

图5-8 添加应用服务器配置


首先要配置被审计的 WEB 服务器的 IP 和监听端口号，域名等基本信息。然后配置需要审计的 COOKIE、配置审计的过滤规则。

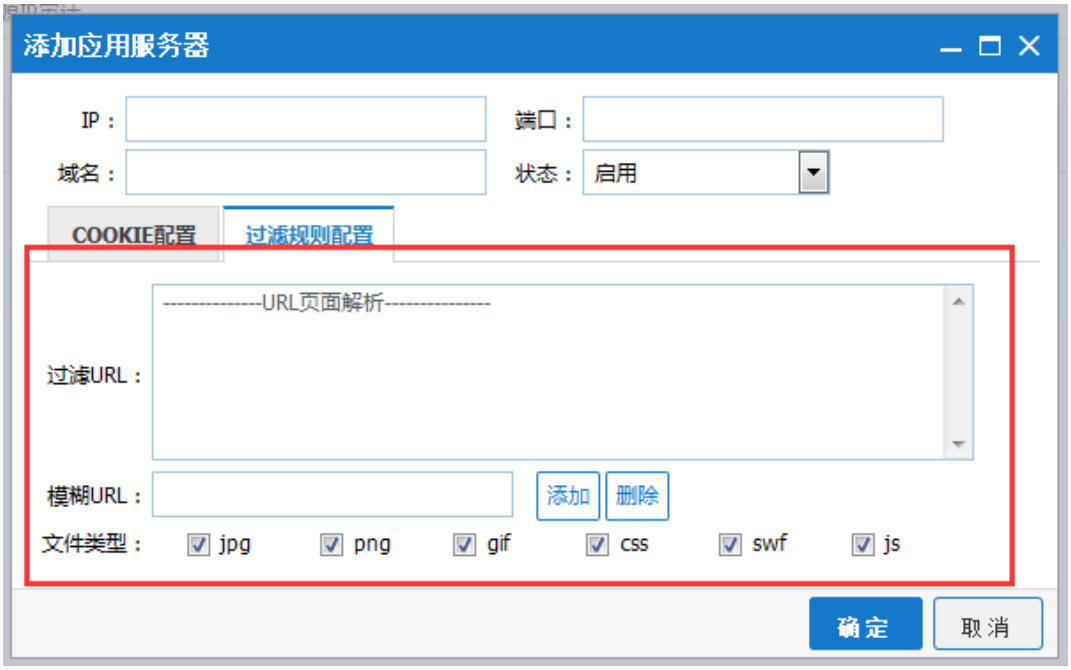
- COOKIE 配置

  配置 COOKIE 中所使用的会话 ID 的参数名（比如 WEBLOGIC 中一般使用”JSESSIONID”）及一些参数字段信息，如上图。

- 过滤规则配置

  设置 URL 解析时，需要过滤掉的信息。可以是图片，FLASH 动画等，配置界面如下图所示：

图5-9 配置界面




设置完毕，点击<确定>后配置即可生效。

### 3. 编辑 WEB 协议服务器配置

在列表中选择某应用服务器后点击<编辑>按钮便可以编辑、修改配置信息，如下图所示：

图5-10 修改应用服务器


### 4. 删除 WEB 协议服务器配置

点击选择某应用服务器后，点击界面中的删除按钮，在弹出对话框中点击<确定>即可删除该配置信息。如下图所示：

图5-11 删除


### 5. 添加监听的非 WEB 协议服务器配置

点击非 WEB 协议服务器配置标签的<添加>按钮弹出[添加中间件服务器配置]对话框，如下图所示：

图5-12 添加


管理员只需填写中间件服务的名称，选择状态、编码策略、协议类型，并配置服务器 IP 和监听端口号，点击<确定>即可。

### 6. 编辑非 WEB 协议服务器配置

在列表中选择某服务器后点击<修改>按钮便可以编辑、修改配置信息，如下图所示：

图5-13 编辑


### 7. 删除非 WEB 协议服务器配置

点击选择某应用服务器后，点击界面中的删除按钮，在弹出对话框中点击<确定>即可删除该配置信息。如下图所示：

图5-14 删除


### 5.2.4 应用审计配置

#### 1. 添加监听的 FTP 服务器配置

点击应用审计配置标签页的<添加>按钮弹出[添加应用审计配置]对话框，如下图所示：

图5-15 添加 FTP 应用审计配置


管理员只需填入应用审计名称，选择协议类型为 FTP 填写 FTP 服务器 IP 后点击<确定>即可。

#### 2. 删除 FTP 服务器审计配置

选择需要删除的服务器配置，点击<删除>按钮，在弹出对话框中点击<确定>即可删除该配置信息。如下图所示：

图5-16 删除


说明

其它类型的运维协议审计的配置方法与配置 FTP 协议一致。

### 5.2.5 指定源 IP 审计

点击监听配置页面中的指定源 IP 审计标签，打开的界面如下图所示：

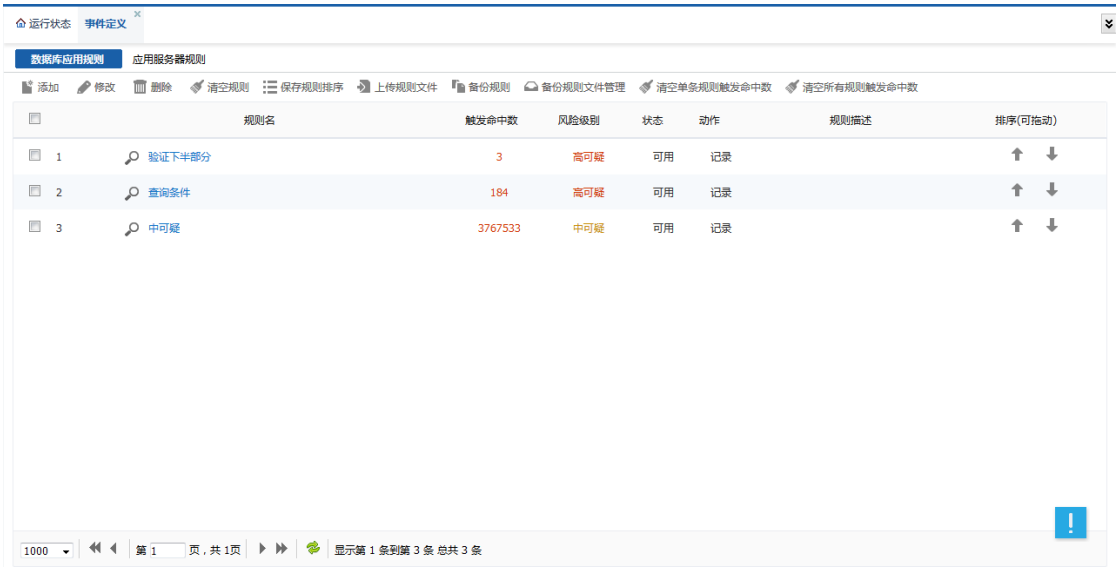
图5-17 指定源 IP 审计


根据单个 IP、网段的 IP 类型，输入 IP 地址并保存，进行源地址 bpf 过滤，减少设备执行数据过滤时的性能消耗。

## 5.3 事件定义

该功能模块主要是定义各种规则，用于识别系统中关于数据库、应用服务器的风险事件。模块包含两个部分：数据库应用规则、应用服务器规则。点击[策略中心/事件定义]，打开的界面如下图所示：

图5-18 事件定义




- 数据库应用规则：识别数据库上风险行为的规则。
- 应用服务器规则：识别发生在应用服务器上风险行为的规则。

## 5.3.2 数据库应用规则

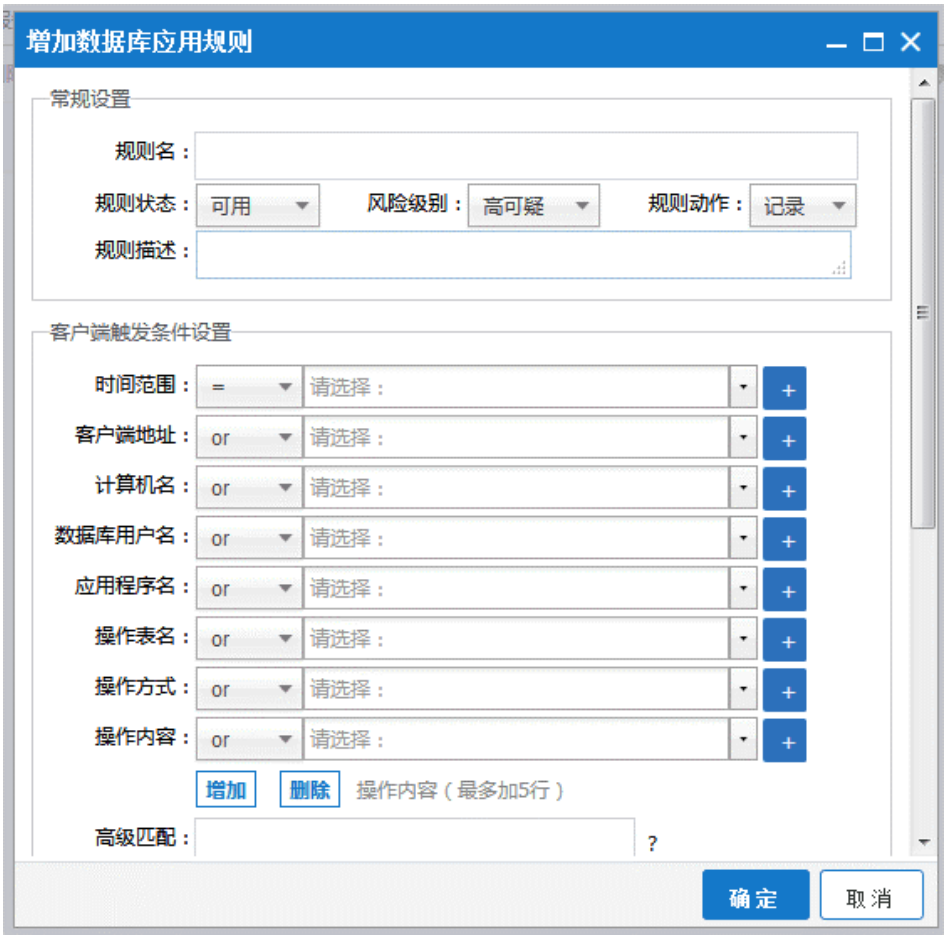
点击[策略中心/事件定义]，在功能区中点击[数据库应用规则]标签，进入数据库审计规则页面。在此对规则所触发的次数做统计，并能手工清零当前的计数值。如下图所示：

图5-19 数据库应用规则


### 2. 添加规则

点击<添加>按钮新建识别规则。主要设置项如下图所示：

图5-20 添加




(2) 常规设置

- 规则名：可以是汉字、字母或者二者的组合，是必填项。
- 规则状态：可用或不可用，及规则的启用、停用。
- 风险级别：定义触发该规则的事件的风险程度，分别是：高可疑、中可疑、低可疑。
- 规则动作：触发该规则的事件是被记录保存下来还是丢弃。

说明

系统强制设置高、中、低可疑事件都需要被记录，不允许丢弃。被设置为丢弃的事件一定不是高、中、低可疑事件。

- 规则描述：对该规则的补充说明。

(3) 客户端触发条件设置

设置与触发规则相关的参数，详细内容如下图所示：

图5-21 客户端触发条件设置


说明

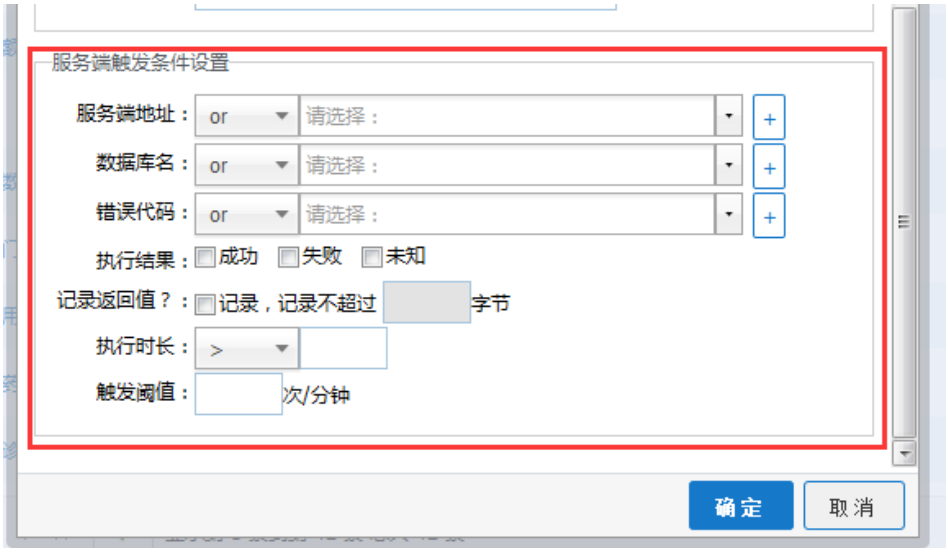
多个参数间是“与”的关系，即同时满足才能触发规则。

每个参数可以设置多个值，并支持对多个值进行 or、and、=、not 等逻辑运算。点击文本框右侧的下三角可直接选择已有的对象，点击最右侧的+号可新建对象；

(4) 服务端触发条件设置：

设置服务器端触发规则的条件，主要参数如下图所示：

图5-22 服务端触发条件设置



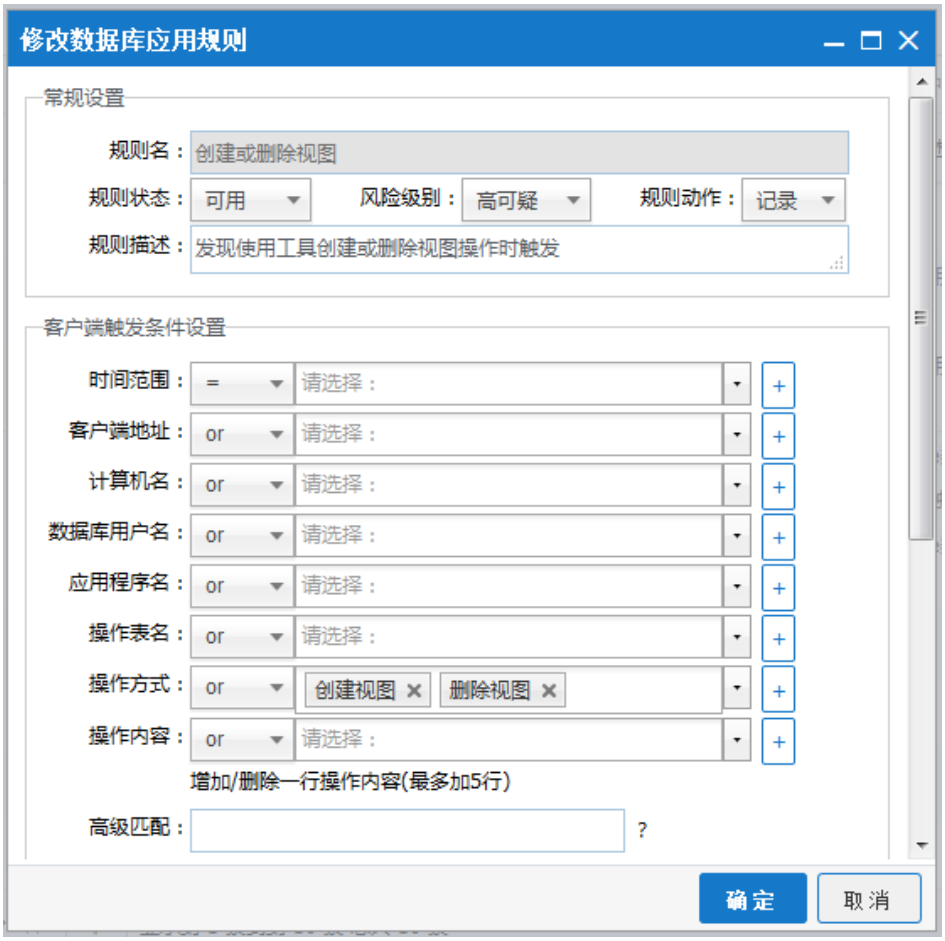

说明

当事件同时满足“客户端触发条件”和“服务端触发条件”的条件才会触发该规则。

### 3. 修改规则

勾选某条记录前的复选框，点击<修改>按钮修改规则，在弹出的[修改数据库应用规则]窗口中对规则各项参数调整。如下图所示：

图5-23 修改




## 4. 删除规则

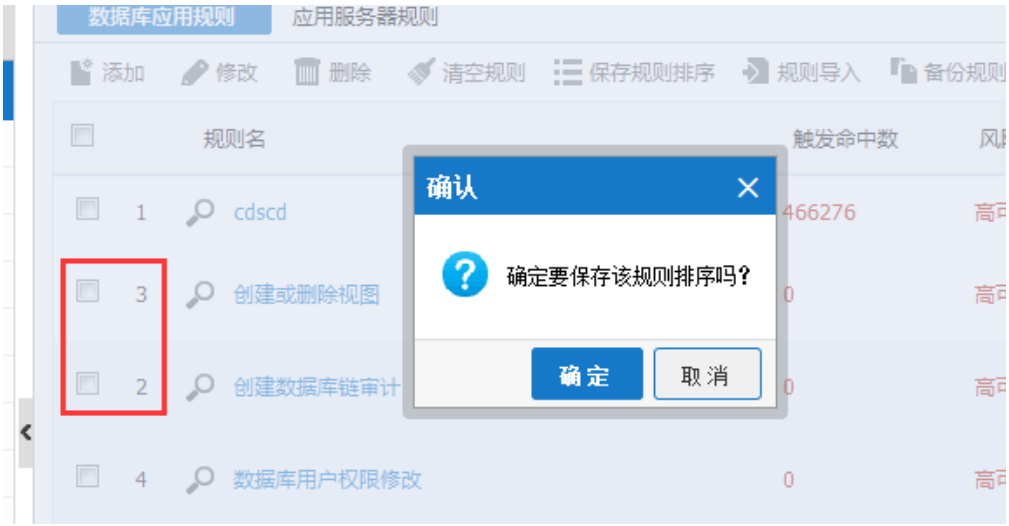
勾选一条或多条记录前的复选框，单击<删除>按钮，在弹出[确认]的对话框中选择确定即可删除。如下图所示：

图5-24 删除

## 5. 规则排序

事件的识别是按照规则列表中的排列顺序逐条匹配。即排在前面的规则优先生效。用户可以根据情况点击规则后的上下箭头按钮或选中拖动来重新排列规则，然后单击<保存规则排序>，在弹出[确认]的对话框中点击<确定>，排序生效。如下图所示：

图5-25 规则排序



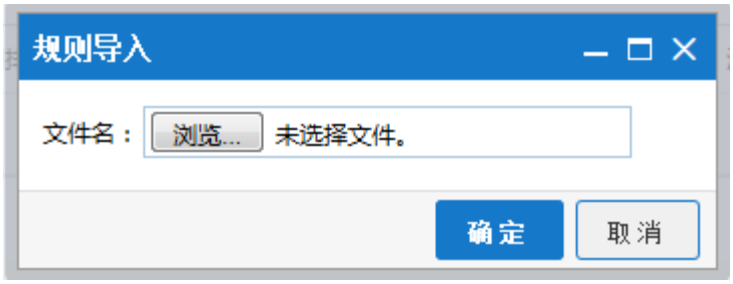

选择确定。排序生效，如下图所示：

图5-26 排序


## 6. 规则导入

首先要下载了需要导入的规则，然后点击<规则导入>按钮，选择需要导入文件的路径即可。如下图所示：

图5-27 规则导入




说明

导入的文件要求是.tgz 文件，无需解压。

### 7. 备份规则

选择一条或多条规则后点击<备份规则>按钮进行备份，填入备注信息后，系统提示备份成功即可，如下图所示：

图5-28 备份规则


### 8. 备份规则文件管理

对所有的规则备份文件管理，可以对其进行删除、恢复、下载操作。如下图所示：

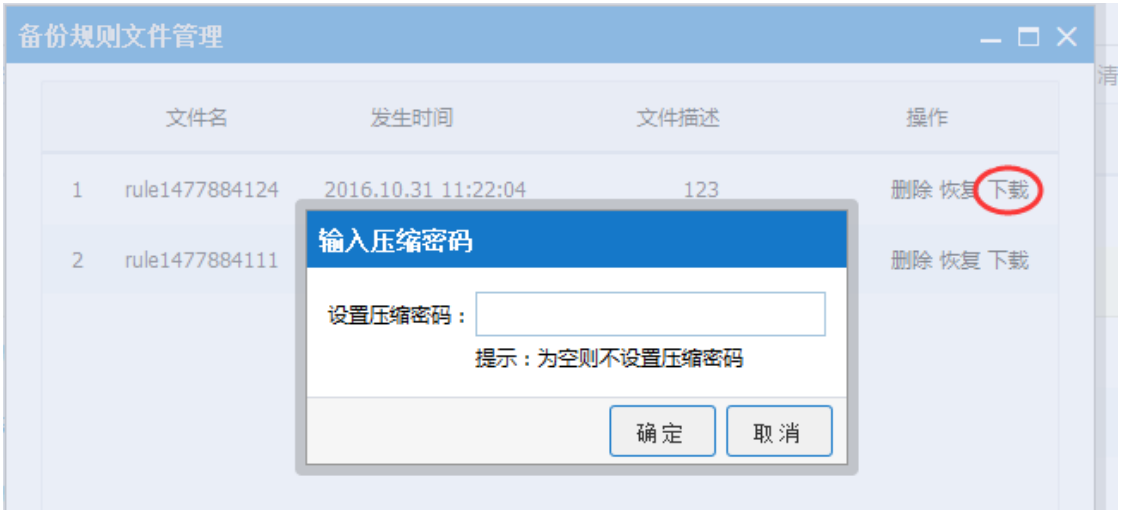
图5-29 备份


说明

当在规则列表中删除一条或多条规则后，如果实现有对其进行备份，只需要点“恢复”即可将规则添加到自定义识别规则列表中。

规则导出提供压缩加密功能，点击<下载>按钮即可填写密码，如下图所示：

图5-30 下载




## 9. 清空单条规则触发命中数

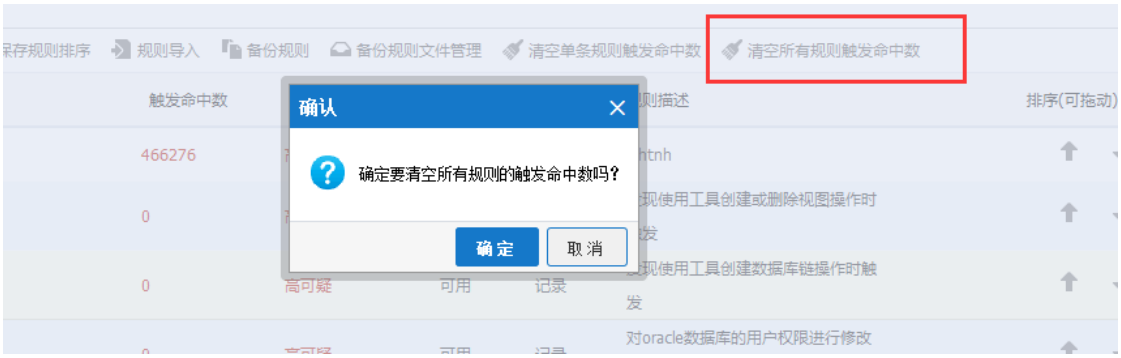
勾选一条记录前的复选框，单击<清空单条规则触发命中数>按钮，在弹出[确认]的对话框中选择<确定>即可清空。如下图所示：

图5-31 清空单条规则触发命中数


### 10. 清空所有规则触发命中数

单击<清空所有规则触发命中数>按钮，在弹出[确认]的对话框中选择<确定>即可清空所有规则的触发命中数。如下图所示：

图5-32 清空所有规则触发命中数




## 5.3.3 应用服务器规则

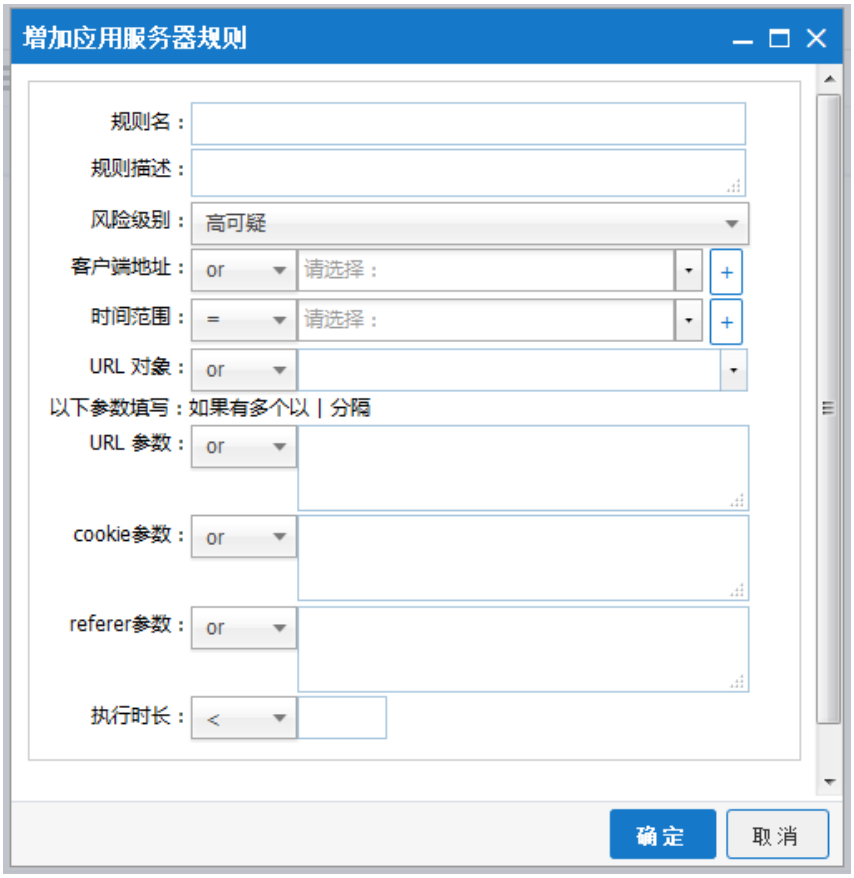
针对应用服务器的审计规则，操作与数据库服务器规则类似，只是规则的内容不同。如下图所示：

图5-33 应用服务器规则


### 2. 添加规则

点击<添加>按钮新建识别规则。主要设置项如下图所示：

图5-34 添加规则




应用服务器规则的其他操作与数据库服务器规则相似，此处不再赘述，具体的可以参考数据库服务器规则部分。

## 5.4 对象管理

包含系统正常运行，风险事件识别所需要的各种对象，可以对对象进行添加、删除、修改。主要对象包括：地址池、时间域、数据库名、数据库用户名、操作表名、程序名、操作内容、操作方式、计算机名、错误代码。

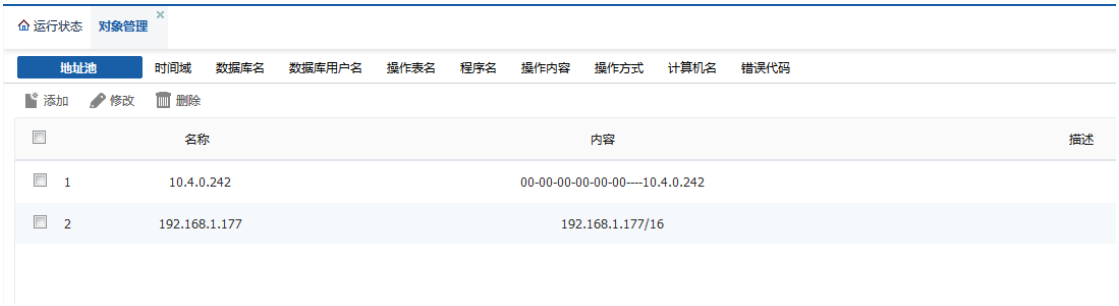
图5-35 对象管理


每种信息的含义和操作方式将在下文中描述。

### 5.4.2 地址池

点击左栏菜单中“地址池”进入地址池管理页面：

图5-36 地址池




点击<添加>按钮，输入地址池对象名称，描述，选择 IPMAC 列表类型，填写对应的 IP 地址与 MAC 地址到列表，点击<添加>确定>即可加入；

图5-37 添加 IPMAC


点击<添加>按钮，输入地址池对象名称，描述，选择网段类型，填写对应的 IP 地址子网掩码类型，点击<添加>确定>即可加入；

图5-38 添加网段


当选定已有的某条记录，点击<修改>进行编辑，修改完成后点击<添加/保存>完成修改。

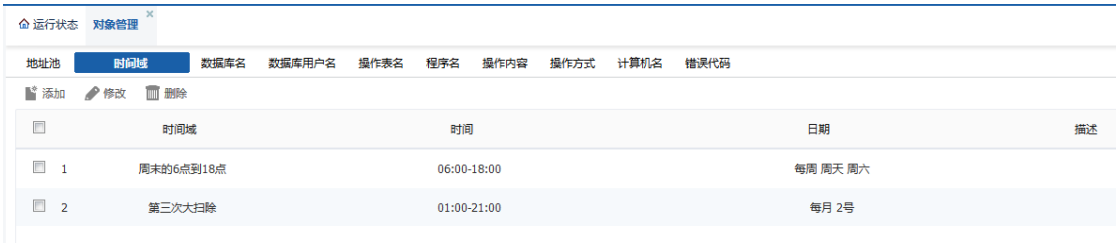
选定已有的某条记录，点击<删除>，即可把已经存在的某个对象删除。如下图所示：

图5-39 删除

### 5.4.3 时间域

点击栏菜单中“时间域”进入时间域管理页面：

图5-40 时间域

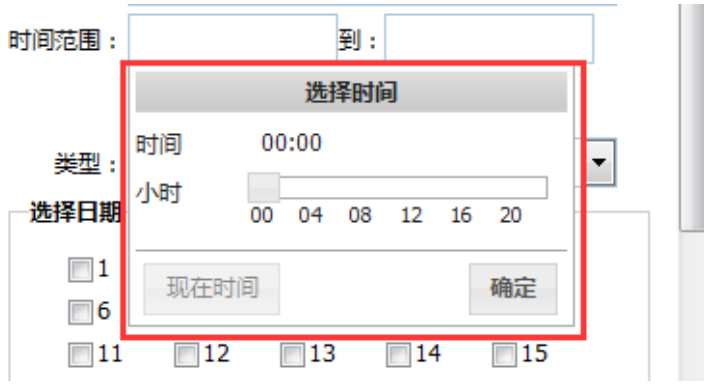



点击左栏菜单中时间域进入时间对象管理，选择添加进入时间对象添加界面：

图5-41 添加

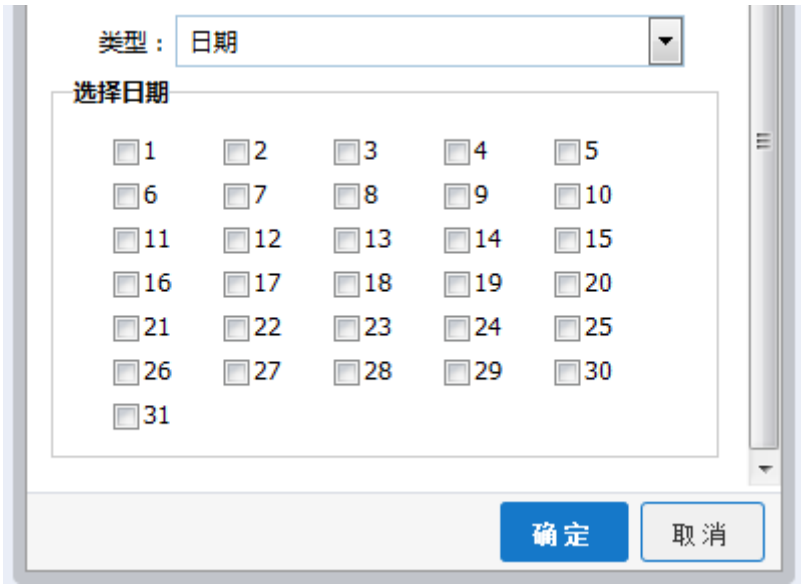

时间对象名称，描述，然后将光标移至时间范围左侧的文本框处，通过拖动滑块设置开始时间。同样的方法可以设置终止时间；如下图所示：

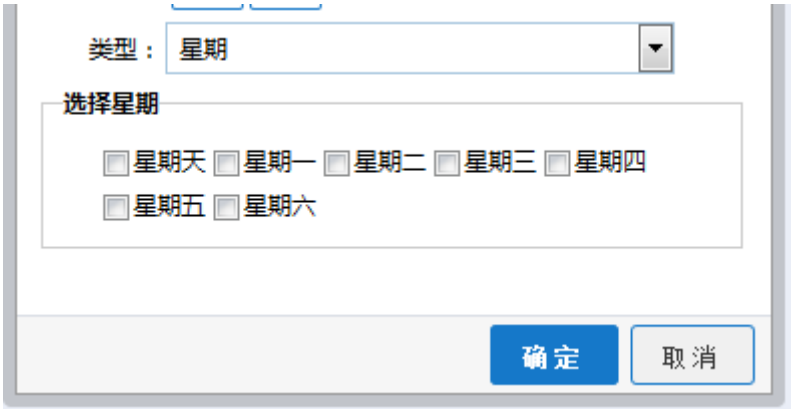
图5-42 选择时间

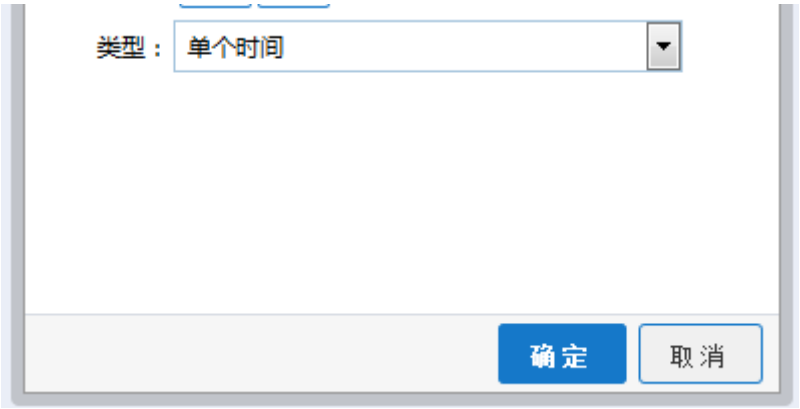



时间类型的选择，可以选择日期、星期、单个时间。

图5-43 时间类型






时间域的编辑和删除操作与地址池一致，只需选择某记录后点击<编辑、删除>按钮进行操作后点击<确定>即可。

### 5.4.4 数据库名

数据库名即与业务相关的数据库实例名。用户可以对其进行添加、删除、编辑等操作。

图5-44 数据库名


点击界面中的<添加>按钮，在弹出[添加数据库名]窗口中录入相关数据，点击<确定>按钮即可添加成功。如下图所示：

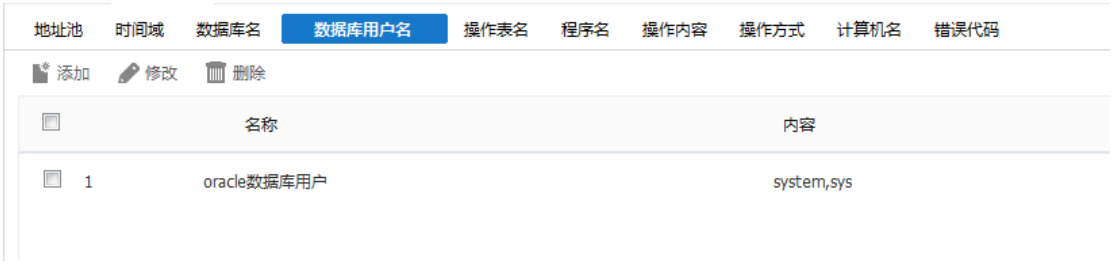
图5-45 添加


删除与编辑操作与其他对象的操作类似，此处不再赘述。

### 5.4.5 数据库用户名

数据库的用户，管理员在此进行用户的添加、删除、修改。数据库用户名可用于规则中

图5-46 数据库用户名




点击界面中的<添加>按钮，在弹出[添加数据库用户名]对话框中录入相关数据后点击<确定>按钮即可添加成功。如下图所示：

图5-47 添加


删除与编辑操作与其他对象的操作类似，此处不再赘述。

### 5.4.6 操作表名

操作表名，用于规则定义，可以对操作表名进行添加、删除、修改操作。

图5-48 操作表名


操作表名的添加、修改、删除与其他对象的操作方式一直，在此不在累述。

### 5.4.7 程序名

业务系统中存在的程序名，可以是合法或非法的，用于定义识别规则。若是合法的程序名则常用于过滤规则，若是非法的，常用于识别各类风险事件。

图5-49 程序名


程序名的添加、修改、删除与其他对象的操作方式一直，在此不在累述。

## 5.4.8 操作内容

操作内容是 SQL 操作方式的具体参数，如某个表、某个字段、甚至是某个对象的具体的值。界面如下图所示：

图5-50 操作内容


操作内容的添加、修改、删除与其他对象的操作方式一直，在此不在累述。

## 5.4.9 操作方式

预先定义规则中会引用到的操作方式，并对其进行增加、删除、编辑、等操作，如下图所示：

图5-51 操作方式


操作方式的添加、修改、删除与其他对象的操作方式一直，在此不在累述。

### 5.4.10 计算机名

计算机名称，定义规则时，主要用于设置客户端触发条件。界面如下图所示：

图5-52 计算机名


计算机名的添加、修改、删除与其他对象的操作方式一直，在此不在累述。

### 5.4.11 错误代码

错误代码，即与业务相关的数据库的错误代码。用户可以对其进行添加、删除、编辑等操作。如下图所示：

图5-53 错误代码


错误代码的添加、修改、删除与其他对象的操作方式一直，在此不在累述。

## 5.5 客户端信息

系统收集了业务环境中所有客户端信息，包括：使用者，他的业务账号，办公的科室和房间号等等。在追踪定位事件时可以快速的定位到发生时间的客户端信息，即事件的主体。

图5-54 客户端信息


用户可以逐条添加客户端信息外，可以通过批量导入的方法添加客户端信息。如下图所示：

图5-55 导入


说明

导入导出目前只支持扩展名为.csv 的文档。

## 5.6 敏感信息

敏感信息主要应用与规则，定义业务系统中的用户非常关心的重要信息。包含关键表、关键字段、医生 ID 对应表、药品 ID 对应表、应用程序对应表等。

用户可根据具体信息如医生 ID、关键表名将其设置为敏感信息，敏感信息起到翻译作用，并且是产生统方事件的必要因素之一。

图5-56 敏感信息


为了让用户能一目了然的获取事件的信息，系统还对业务系统中的关键信息进行了映射，即数据库中的数据翻译成对应的中文描述。用户可以逐条添加敏感信息外，可以通过导入已有的.CSV 文档快速添加关键表，关键字段信息。如下图所示：

图5-57 导入


说明

用户可自定义敏感信息是否启用，若启用将会影响事件识别规则，反之，不影响。

## 5.7 事件响应

系统将识别到的事件分三个等级：高可疑、中可疑、低可疑三级。响应策略主要有：windows 报警、syslog 告警、snmp 告警、发送邮件、短信猫五种。

### 5.7.1 风险响应策略

为各类风险事件设置统一响应策略，并以列表形式展示设置结果，如下图所示：

图5-58 风险响应策略


修改响应策略：选择某类事件后点击<确定>按钮可以修改该类事件的响应策略，如下图所示：

图5-59 修改


说明

在配置或修改响应策略时，若想选择某种响应策略，需要在[风险响应规则/响应策略配置]页面中先对其进行配置，否则会被告知无法设置。

## 5.7.2 响应策略配置

各类响应策略的参数配置。主要内容如下图所示：

图5-60 响应策略配置


## 2. Windows 报警配置

当触发该响应策略时，系统会按照设置好的事件间隔向指定 IP 主机发送弹出式 WINDOWS 消息提示框。告知用户并采取相应措施。配置参数如下图所示：

图5-61 Windows 报警配置


参数配置后请点击<测试>按钮进行测试配置是否成功，成功后请点击<保存配置>。

## 3. syslog 告警配置

需要配置 syslogo 服务器 IP 及端口号，当风险事件发生时，系统会发送 SYSLOG 日志给 SYSLOG 服务器：

图5-62 syslog 告警配置

### 4. 邮件服务器配置

当触发该响应策略的条件时，系统会向指定的邮件服务器发送邮件提醒。各项参数如下图所示：

图5-63 邮件服务器配置


### 5. SNMP 配置

配置 SNMP 告警的基本信息，如下图所示：

图5-64 SNMP 配置


- IP 地址：配置 SNMP 服务器的 IP 地址。
- 端口：配置 SNMP 端口信息。
- 版本：配置 SNMP 相对应的版本信息。
- 团体名称：配置 SNMP 的 PUBLIC 号。

说明

可将 SNMP 的告警信息发送到 SNMP 服务器上，方便查阅！

### 6. 短信猫配置

当触发该响应策略的条件时，系统会向指定的电话号码发送短信提醒。配置参数如下图所示：

图5-65 短信猫配置


## 5.8 三层关联

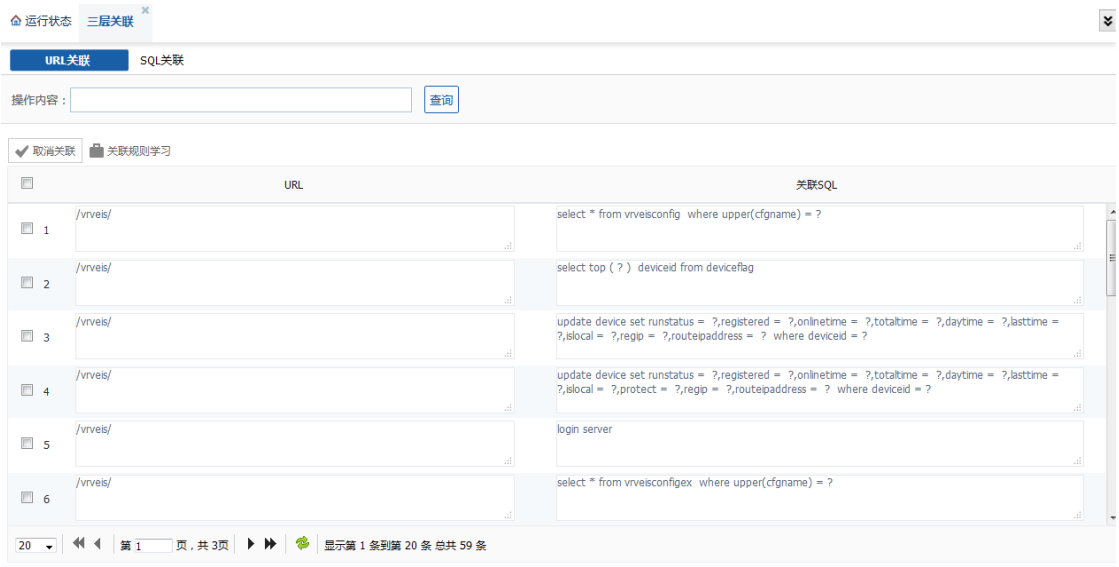
三层关联是对三层审计到的 SQL 语句及三层审计进行关联规则学习，主要功能是：

(1) 学习用户业务环境中已发生的 URL 和 SQL 语句的对应关系

(2) 通过学习，建立三层审计的关联规则库，将 SQL 语句与 URL 进行精确关联

三层关联从两个角度进行关联：与 URL 关联的 SQL，与 SQL 关联的 URL。点击[策略中心/三层关联]，打开界面如下图所示：

图5-66 三层关联




说明

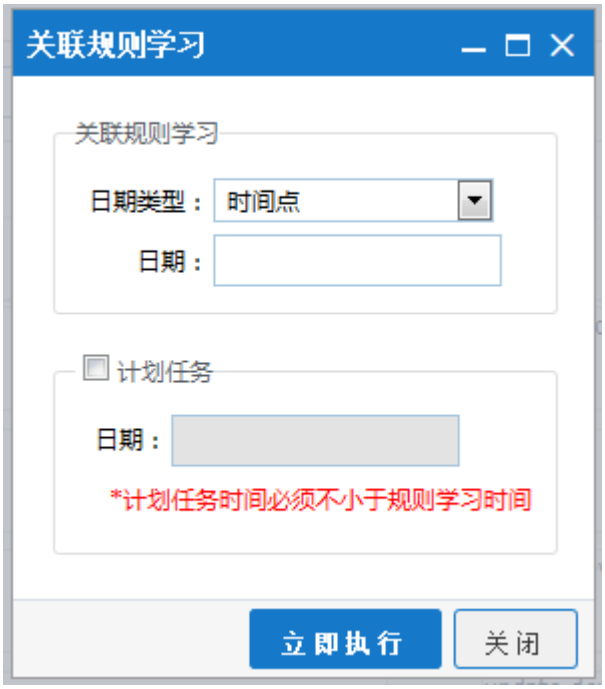
建立的关联规则库将在“三层关联”页面中引用，对 SQL 语句与 URL 进行精确关联后展示给用户。

### 5.8.2 URL 关联

#### 1. 关联规则学习

点击<关联规则学习>按钮，在弹出[关联规则学习]窗口中进行参数设置，如下图所示：

图5-67 关联规则学习




- 时间类型

  选择要学习的数据源(时间)，可以对某天或某段时间发生的三层审计数据进行学习。

---

说明

学习的数据源必须是过去的、已发生的。

---

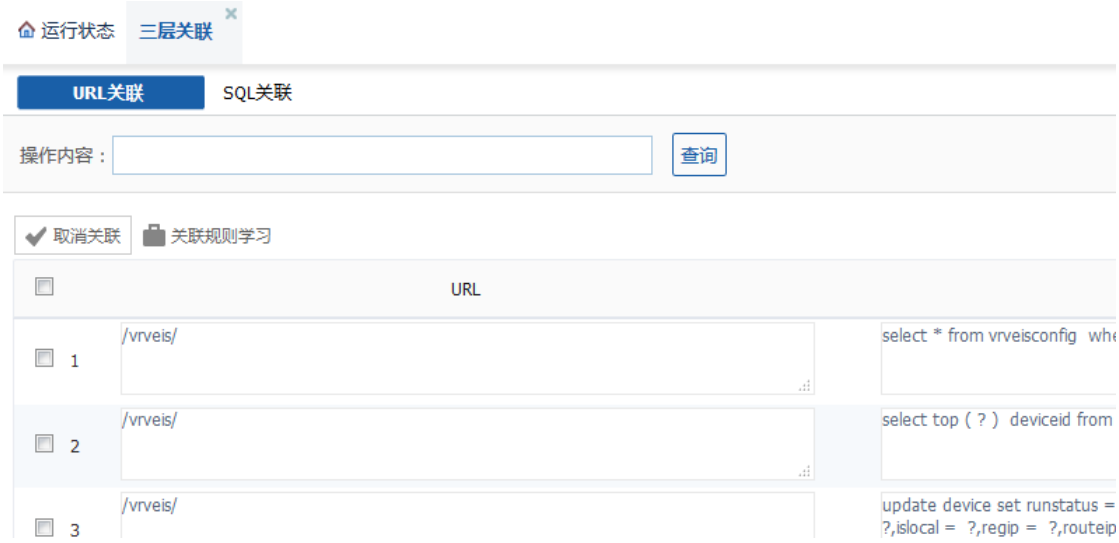
- 计划任务

  若不勾选此项，任务默认是立即执行。若勾选该项该项，并设置执行的时间，点击<计划执行>按钮，系统将在用户设置的日期开始对选定的数据源进行关联分析。

### 2. 关联结果查询

系统已执行了关联规则学习后，对之前设置的数据源进行 URL 与 SQL 语句关联的结果将会在三层关联界面中展示，在文本框中输入操作内容可以对结果进行查询。如下图所示：

图5-68 关联结果查询




### 3. 取消关联

选择某条 URL 记录后点击<取消关联>按钮，在弹出[确认]对话框中点击<确定>将会取消该关联。

图5-69 取消关联

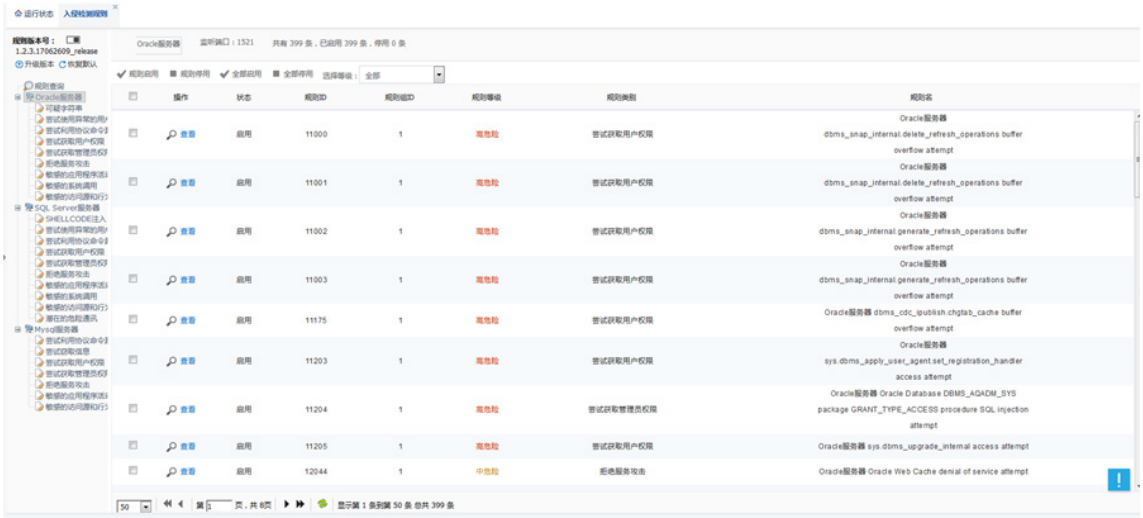

## 5.8.3 SQL 关联

展示与 SQL 关联的 URL 数据，也提供了关联规则学习和取消关联的功能。具体操作请查阅本节中的“URL 关联”部分。

# 5.9 入侵检测规则

入侵检测规则提供了针对 ORACLE、SQL Server、MySQL 三种类型数据库的检测入侵。用户根据需要启用或禁用规则。打开入侵检测规则，如下图：

图5-70 入侵检测规则



## 2. 启用、停用入侵检测规则库

点击  ，选择确定即可启用入侵检测规则库，如下图所示：

图5-71 启用

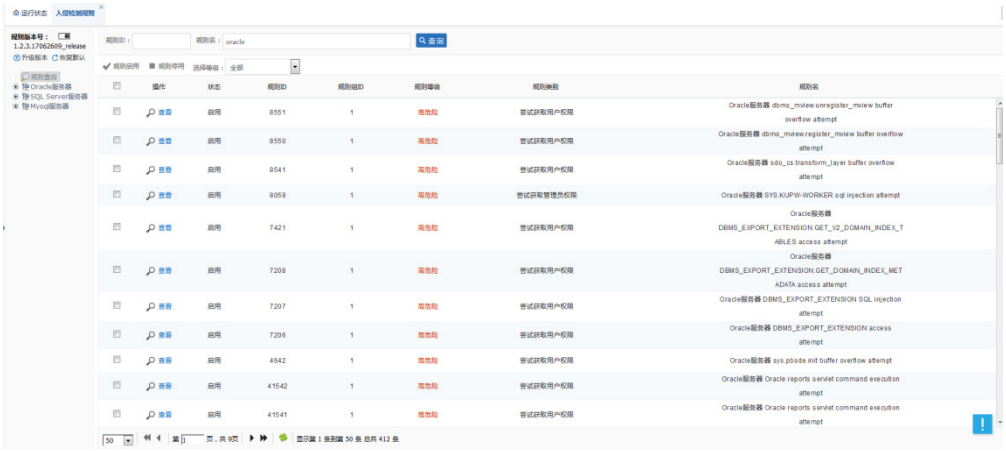

点击  ，选择确定即可停用入侵检测规则库，如下图所示：

图5-72 停用


### 3. 规则查看

点击 规则查询 ，可以根据规则 ID、规则名等关键字查询相关规则，并进行规则的启用和停用操作。

图5-73 规则查看



在检索列表右侧点击 查看 ，可以在新窗口中查看该规则更详细的信息。主要有：规则信息，报文特征信息、处理方式信息，及 CVE、URL 的参考信息等。如下图所示：

图5-74 规则详情

| 规则详情 | | |
|---|---|---|
| 规则信息 | 规则ID： 8551 | 规则等级： 高危险 |
| | 规则名： Oracle服务器 dbms_mview.unregister_mview buffer overflow attempt | |
| 报文特征 | 内容中包含"dbms_mview.unregister_mview"；并且需要匹配正则表达式"/((\w+)[\r\n\s]*\x3a=[\r\n\s]*(\x27[^\x27]{150,}\x27\|\x22[^\x22]{150,}\x22)[\r\n\s]*\x3b.*mviewsite[\r\n\s]*=>[\r\n\s]*\2\|mviewsite\s*=>\s*(\x27[^\x27]{150,}\|\x22[^\x22]{150,}))\|(\s*((\x27[^\x27]*\x27\|\x22[^\x22]*\x22)\s*,\s*){2}(\x27[^\x27]{150,}\|\x22[^\x22]{150,}))/si"。 | |
| 规则描述 | 当试图利用Oracle数据库的已知漏洞时，生成此事件。 | |
| 影响 | 严重，可能导致SQL注入和执行任意代码。 | |
| 判断 | 请根据告警信息中的时间和IP地址向设备拥有者进行核对，若该时段无对应操作或该主机为闲置主机，则可能该主机被作为"跳板"进行入侵行为。 | |
| 处理方式 | 应用合适的供应商提供的补丁。 | |
| 参考 | CVE： | |
| | URL： www.appsecinc.com/resources/alerts/oracle/2004-0001/25.html | |

## 4. 系统默认规则

系统自带规则，只能启用或者停用，不能添加或者修改。在左侧选择攻击类型，然后在右侧设置相应的规则，具体的操作有以下几种：

- 规则启用

  用户可以在右侧中选择不同攻击规则，然后点击<规则启用>即可启用列表中所选规则。

图5-75 规则启用


规则被启用并生效后，会提示启用成功，并在规则状态显示启用，如下图所示：

图5-76 状态


- 规则停用

  用户可以在右侧中选择已启用的攻击规则，然后点击<规则停用>即可停用列表中所选中的正在生效的规则。

图5-77 规则停用


- 全部启用

  用户点击<全部启用>按钮，在弹出[确认]框中点击<确定>即可启用列表中所有规则。

图5-78 启用


- 全部停用

  右侧显示的是当前启用的规则列表，可以点击<全部停用>按钮禁用所有正在生效的规则。

图5-79 停用


## 5.10 交换机信息

用户通过三层设备访问数据库时，其真实 MAC 地址将被隐藏，通过交换机信息模块，获取与交换机连接终端的真实 IP 及 MAC 地址。通过预先设置的 snmp 口令，获取交换机上存储的 CAM 信息。点击<开始扫描>前，需要指定扫描对象，即“激活”交换机。扫描行为将每隔一分钟获取一次数据，新数据将覆盖现有数据。

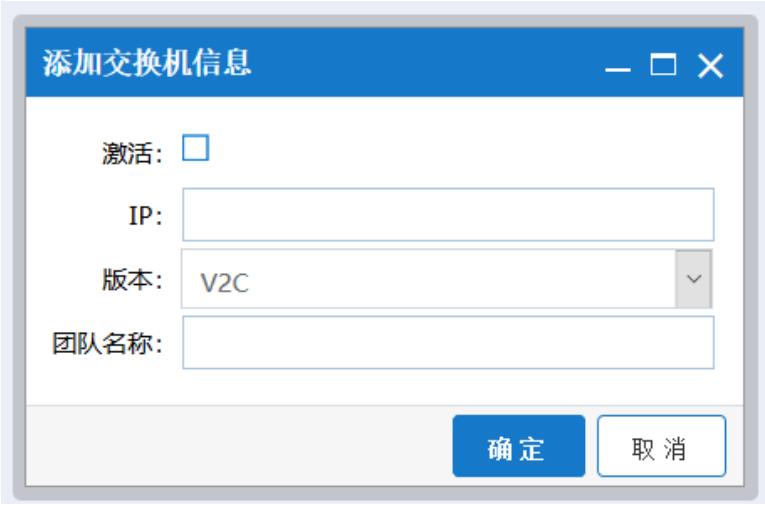
界面中列出了用户添加的交换机信息。主要信息包括交换机 IP、版本号、团队名称以及交换机的状态。如下图所示：

图5-80 交换机信息

### 2. 添加交换机

点击<添加>按钮，在弹出[添加交换机信息]框中输入交换机相关信息后点击<确定>即可添加成功。如下图所示：

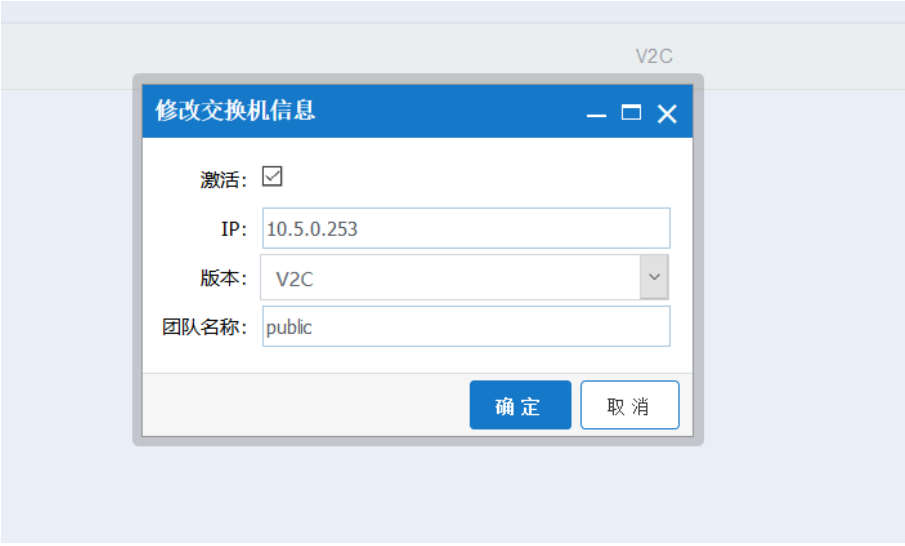
图5-81 添加交换机




### 3. 修改交换机信息

勾选列表中需要编辑的记录，点击<修改>按钮，在弹出[修改交换机信息]对话框中进行修改后确定即可。

图5-82 修改交换机




### 4. 删除交换机

当不需要使用该交换机时，勾选列表前面复选框后点击<删除>按钮，在弹出[确认]框中点击<确定>即可。

图5-83 删除交换机


## 5. 交换机扫描

交换机扫描主要是对连接到交换机上的PC终端进行扫描，获取PC终端真实的IP、MAC对应关系，并在事件追踪界面中展示中客户端 MAC 地址一栏展示。如下图所示：

图5-84 交换机扫描


交换机的状态有两种：已激活、未激活。已激活的状态是一把已打开的锁，如下图所示：

图5-85 状态

(2)　开始扫描

对交换机进行扫描前，请确认交换机的状态是激活的。然后点击界面中<开始扫描>按钮，在弹出[确认]框中点击<确定>后系统提示开始扫描成功，并对列表中已激活的交换机每隔一分钟自动扫描一次。界面中<开始扫描>按钮自动变更为<停止扫描>。

图5-86 扫描



(3)　停止扫描

不需要扫描时，点击界面中<停止扫描>按钮即可。

# 6 系统管理

## 6.1 概述

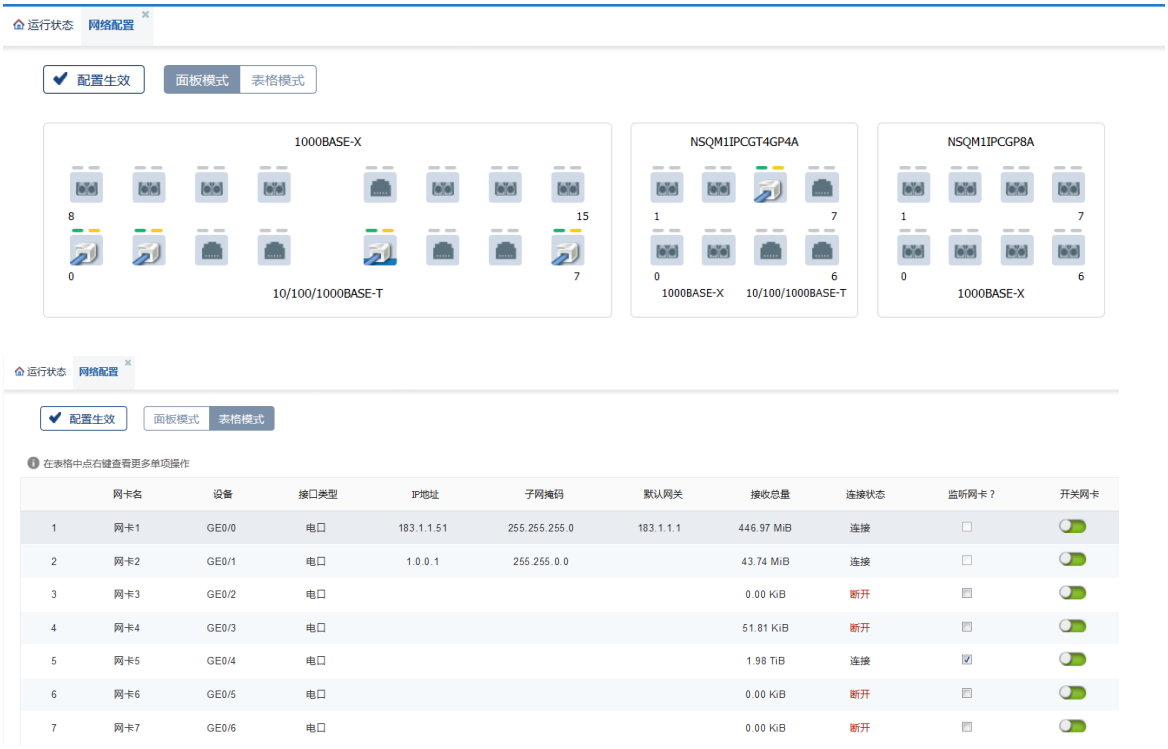
系统管理主要介绍如何了解当前系统的运行状态，系统正常运行需要进行哪些基本配置，介绍系统运行中的各种日志数据，以及审计到的数据如何保管。具体可以分为这几个部分：网络配置、用户管理、进程管理、运行日志、日志响应、调试工具、配置备份、系统信息、管理主机等。

图6-1 系统管理


## 6.2 网络配置

设备的网口配置，可以将网口设置为管理口、监听口。有面板模式和表格模式，面板模式展示与物理设备面板一一对应的网卡模拟展示图，根据实际连线情况实时展示网卡当前接线状态，并以水量方式展示网卡当前负载，鼠标移至网卡会显示该网卡的详细信息。点击左栏菜单[系统管理/网络配置]进入配置界面，如下图所示：

图6-2 网络配置




(2) 设置/修改 IP

面板模式下选择 设置/修改IP 按钮；表格模式下，选择某个网卡，右击选择 设置/修改IP 按钮后，在弹出[设置/修改 IP]窗中修改 IP 信息，如下图所示：

图6-3 修改

提示

一般监听网卡建议不设置 IP。

(3) 删除 IP

面板模式下选择 删除IP 按钮；表格模式下，选择某个监听网卡，右击选择 删除IP 按钮后，在弹出[确认]窗口中点击<确定>即可删除该网卡 IP，如下图所示：

图6-4 删除


(4) 配置生效

网卡设置 IP 后并未马上生效，需要点击 配置生效 按钮，系统提示“配置生效成功”才算是生效。如下图所示：

图6-5 配置生效


(5) 监听网卡设置

设置是否监听该网卡，如下图所示：

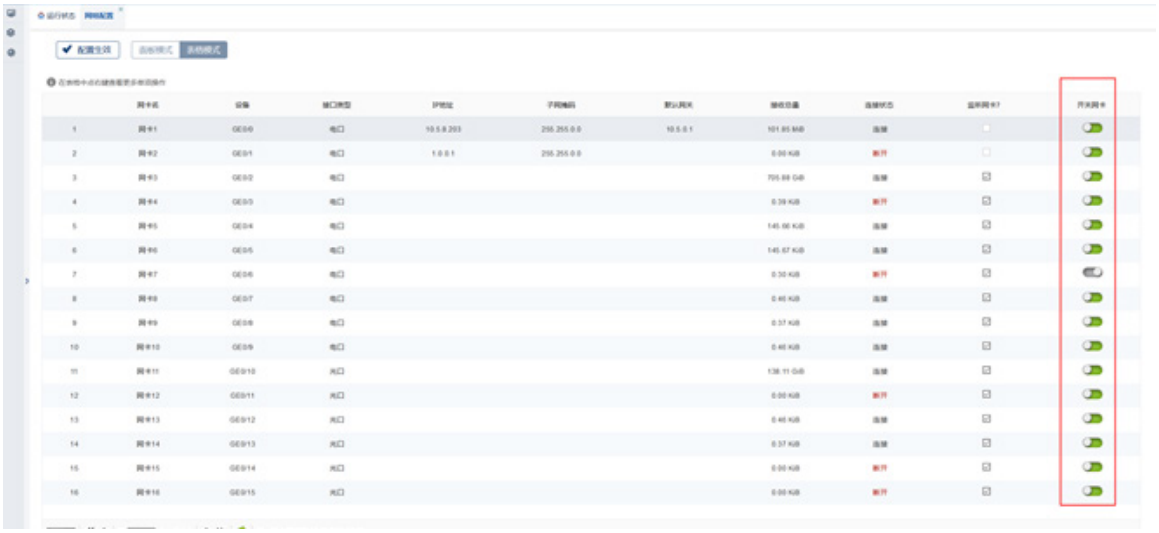
图6-6 监听网卡设置

| | 网卡名 | 设备 | 接口类型 | IP地址 | 子网掩码 | 默认网关 | 接收总量 | 连接状态 | 监听网卡？ | 开关网卡 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 网卡1 | GE0/0 | 电口 | 183.1.1.51 | 255.255.255.0 | 183.1.1.1 | 447.30 MiB | 连接 | ☐ | |
| 2 | 网卡2 | GE0/1 | 电口 | 1.0.0.1 | 255.255.0.0 | | 43.79 MiB | 连接 | ☐ | |
| 3 | 网卡3 | GE0/2 | 电口 | | | | 0.00 KiB | 断开 | ☐ | |
| 4 | 网卡4 | GE0/3 | 电口 | | | | 51.81 KiB | 断开 | ☐ | |
| 5 | 网卡5 | GE0/4 | 电口 | | | | 1.98 TiB | 连接 | ☑ | |
| 6 | 网卡6 | GE0/5 | 电口 | | | | 0.00 KiB | 断开 | ☐ | |

(6) 开关网卡设置

设置网卡禁用和启用的操作，如下图所示：

图6-7 监听网卡设置



## 6.3 用户管理

### 1. GB/T 18336.2-2001 中管理员角色规定

系统的管理体系的划分遵循了 GB/T 18336.2-2001 中的安全管理规定，GB/T 18336.2-2001 其等有效采用 ISO/IEC 15408 Common Criteria for IT Security Evaluations (CC)，相关说明部分摘录如下：

- FMT_SMR.1 安全角色

  在 FMT_SMR.1.1 中，PP/ST 作者应规定系统所认同的角色，就安全而言这些角色是用户可以拥有的角色。例如：拥有者、审计员和管理员。

- FMT_SMR.2 安全角色限制

  在 FMT_SMR.2.3 中，PP/ST 作者应规定制约角色分配的条件。这些情况的例子如：“一个账户不能同时具有审计员和管理员两种角色”或“具有助理角色的用户也必须具有拥有者角色。”

- FMT_SMR.3 承担角色

  在 FMT_SMR.3.1 中，PP/ST 作者应规定需要作出明确请求才能承担的角色。例如：审计员和管理员。

## 2. 用户权限划分

系统根据用户的不同角色提供不同的命令集合。

(1) 系统管理员（sys）：系统默认用户名及密码为：sys/sys，对应 GB/T 18336 中提到的管理员，权限如下：

- 个人信息管理。
- 系统运行参数配置。
- 查看系统运行状态。
- 无权操作其他角色功能。

(2) 系统审计员（audit）：系统默认用户名及密码为：audit/audit，对应 GB/T 18336 中提到的审计员，权限如下：

- 个人信息管理。
- 查看系统运行状态。
- 系统自身运行日志信息。
- 无权操作其他角色功能。

(3) 系统安全员（sec）：系统默认用户名及密码为：sec/sec，对应 GB/T 18336 中提到的安全员，负责权限如下：

- 个人信息管理。
- 与业务有关的操作及信息查看。
- 查看系统状态。
- 无权操作其他角色功能。

(4) 监察员（mon）：系统默认用户名及密码为：mon/mon。负责权限如下：

- 个人信息管理。
- 与业务有关的操作及信息查看。
- 无权操作其他角色功能。

四类角色具有的权限范围不同，具体的权限分配请参考“表 1-1 各类角色权限分配表”

## 3. 用户管理

系统内置了以下四类用户的超级用户，每个用户只能对本组的用户权限管理。例如，系统内置的 sys 用户只能对系统管理员的用户进行增、删、改，权限分配等管理操作。

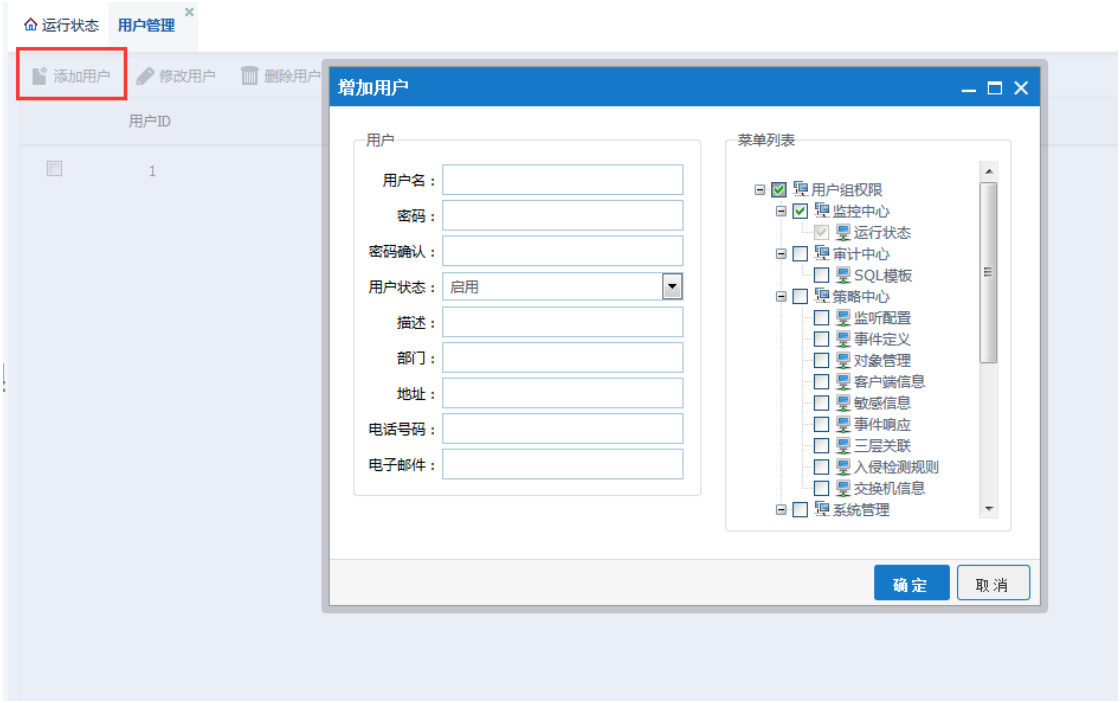
点击[系统管理/用户管理]，进入当前登录用户所属角色类型的用户列表，如下图所示是系统管理员 sys 用户列表：

图6-8 用户管理


(2) 添加用户

进入添加用户的操作界面：

图6-9 增加用户

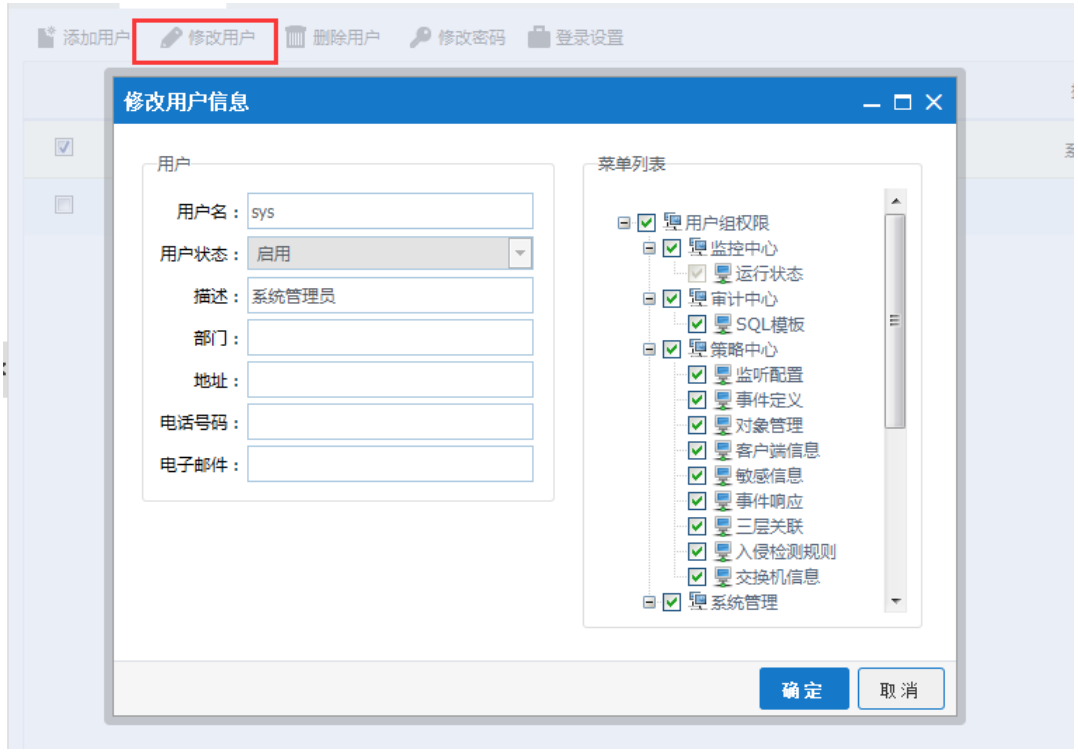



左侧是用户基本信息，右侧是权限列表。正确填写各项信息后点击<确定>即可。

(3) 修改用户

选择某个已存在的用户，点击<修改用户>按钮,即可对其基本信息和系统权限修改，修改完毕后点击<确定>即完成修改，如下图所示：

图6-10 修改用户




(4) 删除用户

选择一个或多个已存在的用户，点击<删除用户>按钮，在弹出[确认]框中选择<确定>，将立即删除该用户，如下图所示：

图6-11 删除用户

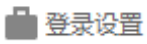

(5) 用户状态修改

将鼠标放置在用户状态字段下的锁的图标时，可以修改用户状态，如下图所示：

图6-12 修改状态

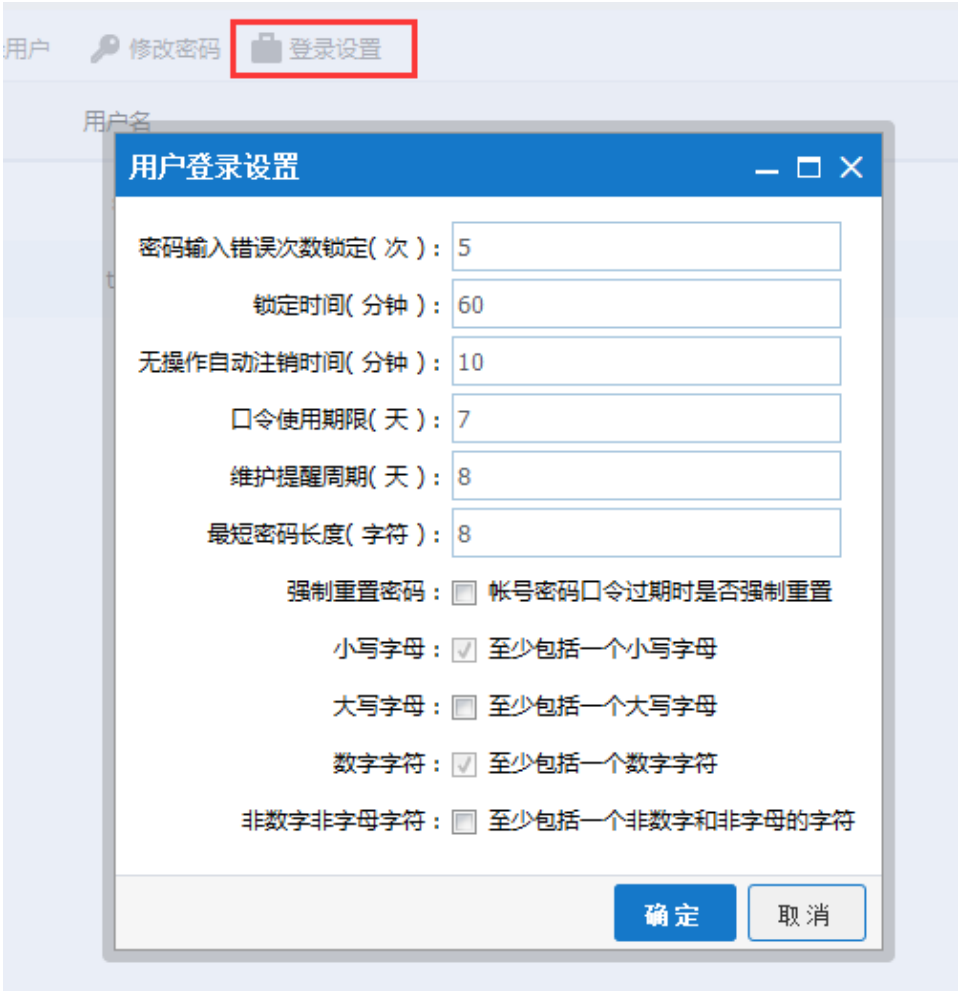

- 未锁定：图标的锁是打开的  ，该用户可以正常使用。
- 锁定：图标的锁是锁住的  ，表示该用户已经被锁定，无法使用。

(6) 登录设置

该功能只有系统管理员（sys）角色才拥有，在此可以对系统所有角色用户的登录进行设置。点击用户列表上的 

按钮，对系统所有用户进行登录设置。主要内容如下图所示：

图6-13 用户登录设置



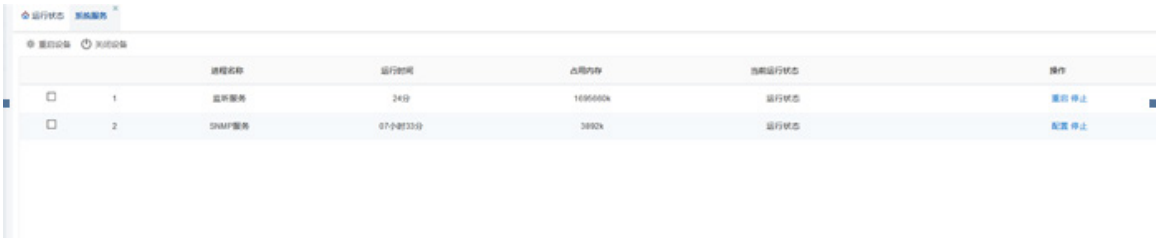
- 密码输入错误次数锁定：用户在登录界面上输入密码错误的次数，如果超过该次数，该用户即被锁定，在锁定时间内无法继续登录。
- 锁定时间：用户被锁定后需要经过 N（N 是大于 1 的整数）分钟后才能使用。
- 误操作自动注销时间：用户登录成功后，无操作动作的时间，超过该时间，用户自动注销。
- 口令使用期限：用户口令可使用天数，可设置 1-30 天。
- 维护提醒周期：周期性（建议每 7 天）提醒管理员维护配置（登录配置）。
- 最短密码长度：管理员可设置用户设立密码的最短长度（字符）。
- 管理员可配置用户设立密码的复杂度：强制重置密码、小写字母数、大写字母数、数字字符数、非数字非字母字符数。

## 6.4 系统服务

类似我们操作系统中的服务管理器，对系统运行产生各种服务进行启用、停用管理和配置。

点击右上角的“系统管理”，然后在左侧菜单栏中点[系统管理/系统服务]进入界面，如下图所示：

图6-14 系统服务



### 2. 重启设备

点击 重启设备，可以重启系统。

### 3. 关闭设备

点击 关闭设备，可以关闭系统。

### 4. 监听服务

点击监听服务操作栏上的重启或者停止按钮，可以对监听服务进行重启和停止。

### 5. SNMP 服务

点击 SNMP 服务操作栏上的配置按钮，可对 SNMP 服务进行配置，如下图所示：

图6-15 SNMP 服务配置


## 6.5 运行日志

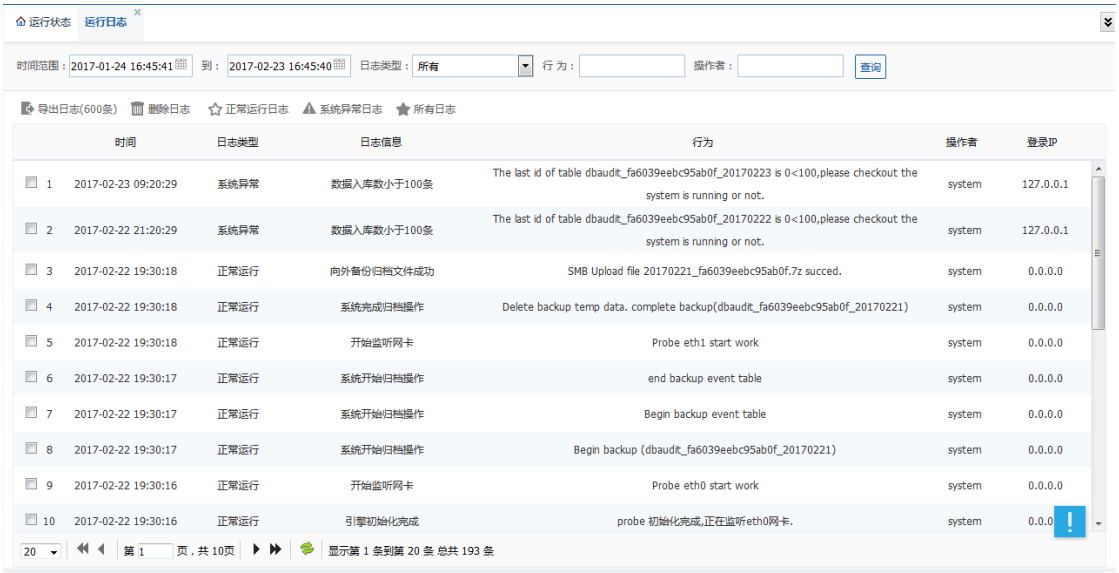
运行日志记录了系统自身运行过程中的日志，包括正常运行日志、系统异常日志。在此页面可以分类查询，或导出、删除日志。

(1) 正常运行日志：系统 CPU、内存、存储空间等系统运行参数正常，系统正常运行。

(2) 系统异常日志：系统无法正常运行。

点击[系统管理/运行日志]，进入界面如下图所示：

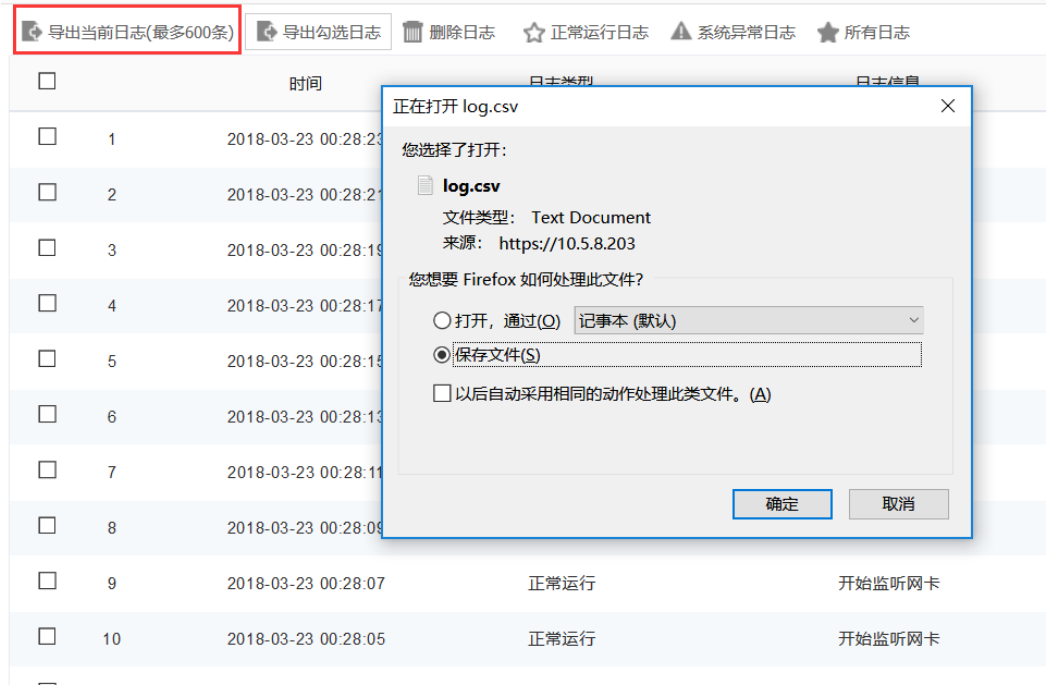
图6-16 运行日志




### 2. 导出日志

点击<导出日志>按钮，可以最多导出 600 条当前所有系统日志包括正常运行及系统异常日志，导出日志的格式为 CSV 格式。

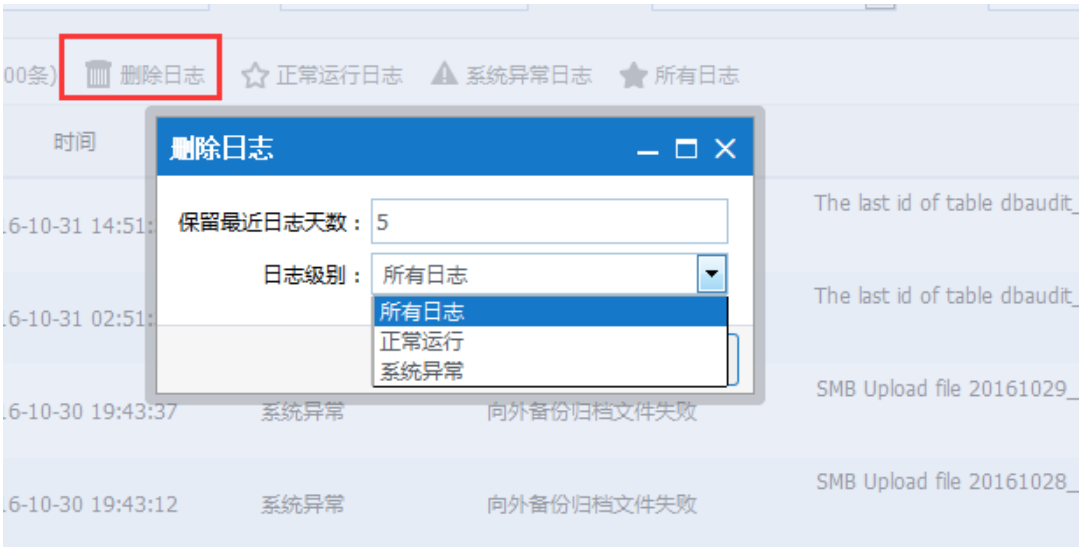
图6-17 导出




### 3. 删除日志

点击<删除日志>按钮，在弹出[删除日志]框中选择需要保留的最近 N（整数）天日志（即删除 N 天之前的所有日志），再选择删除的日志类型，点击<确定>后立即执行删除操作。

图6-18 删除



说明

日志可以被删除，但是删除日志的行为将会被记录到操作日志。

### 4. 分类查看系统日志

鼠标点击 正常运行日志 系统异常日志 所有日志 这三个按钮可以在列表中展示对应的日志内容。

## 6.6 日志响应

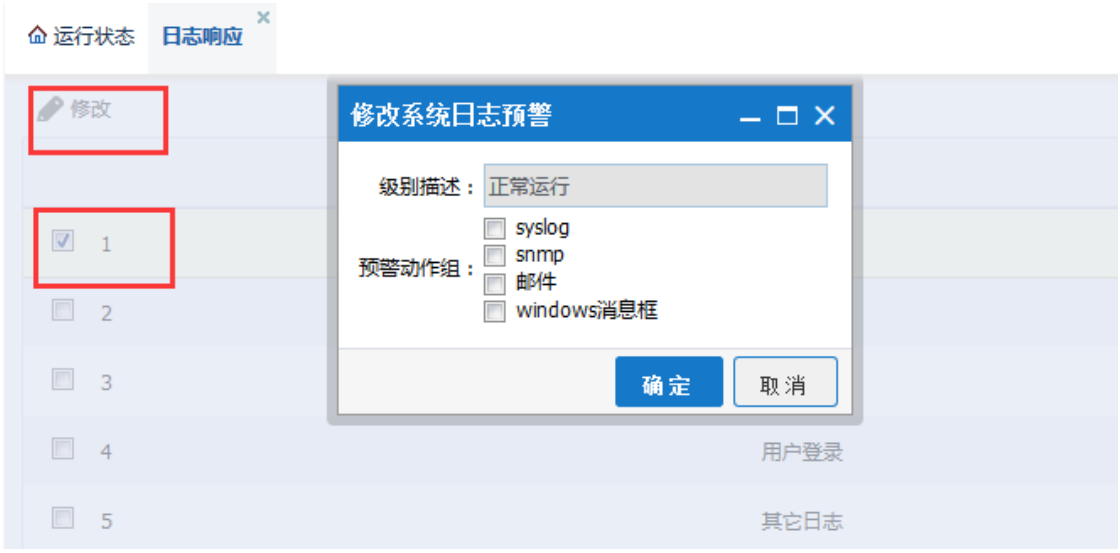
为不同类型的系统日志设置预警方式，一旦发现危险的日志行为将会发出告警。点击左栏菜单中的[系统管理/日志响应]，进入界面如下图所示：

图6-19 日志响应


### 2. 修改日志响应策略

选择某类日志级别后，点击<修改>按钮在弹出[修改系统日志预警]框中修改预警动作，点击<确定>按钮后即可保存配置如下图所示：

图6-20 修改

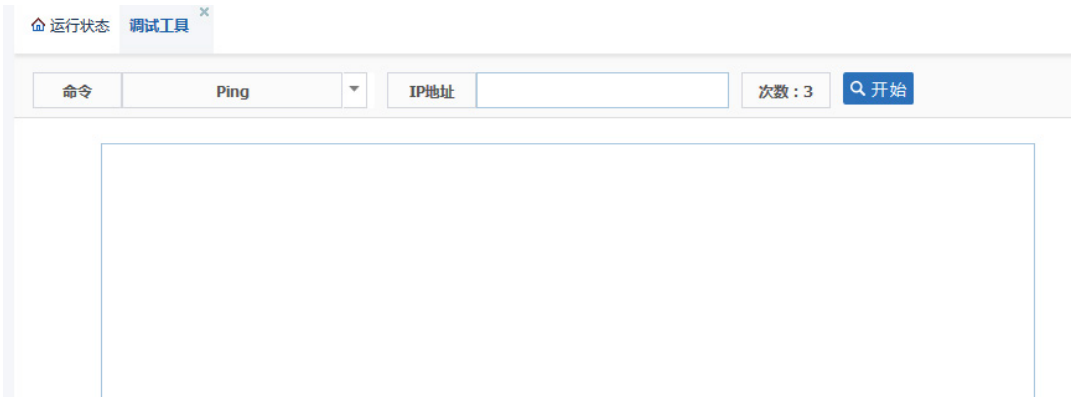



## 6.7 调试工具

系统为管理员提供了两个调试工具分别是 ping 和 sniffer。

点击右上角的“系统管理”，然后在左栏菜单[系统管理/调试工具]进入界面，如下图所示：

图6-21 调试工具

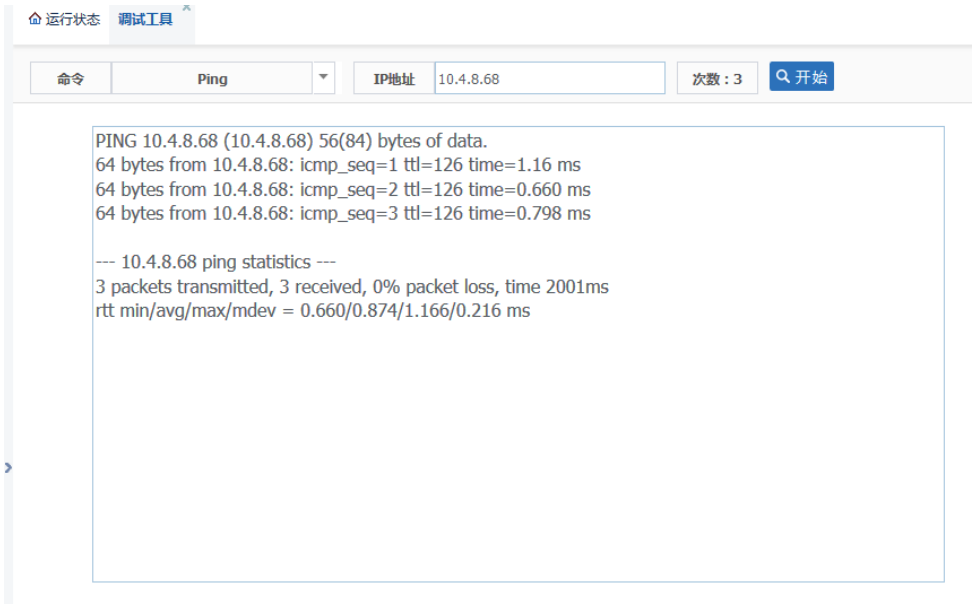



具体作用如下：

### 2. Ping

填入相关查询参数后点击<开始>按钮进行查询分析。如下图所示：

图6-22 分析结果




### 3. Sniffer

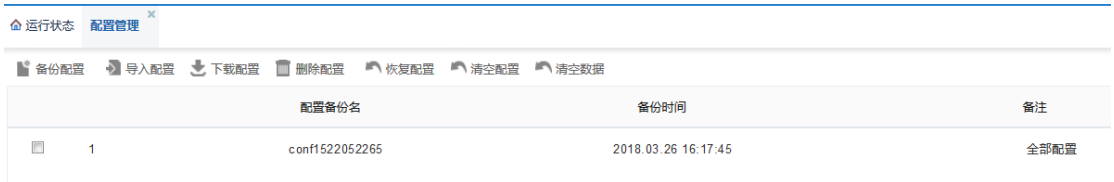
填入相关查询参数后点击<开始>按钮进行查询分析。如下图所示：

图6-23 分析结果


## 6.8 配置管理

对系统各项基本参数进行备份管理。点击[系统管理/配置管理]进入配置管理界面,如下图所示：

图6-24 配置管理

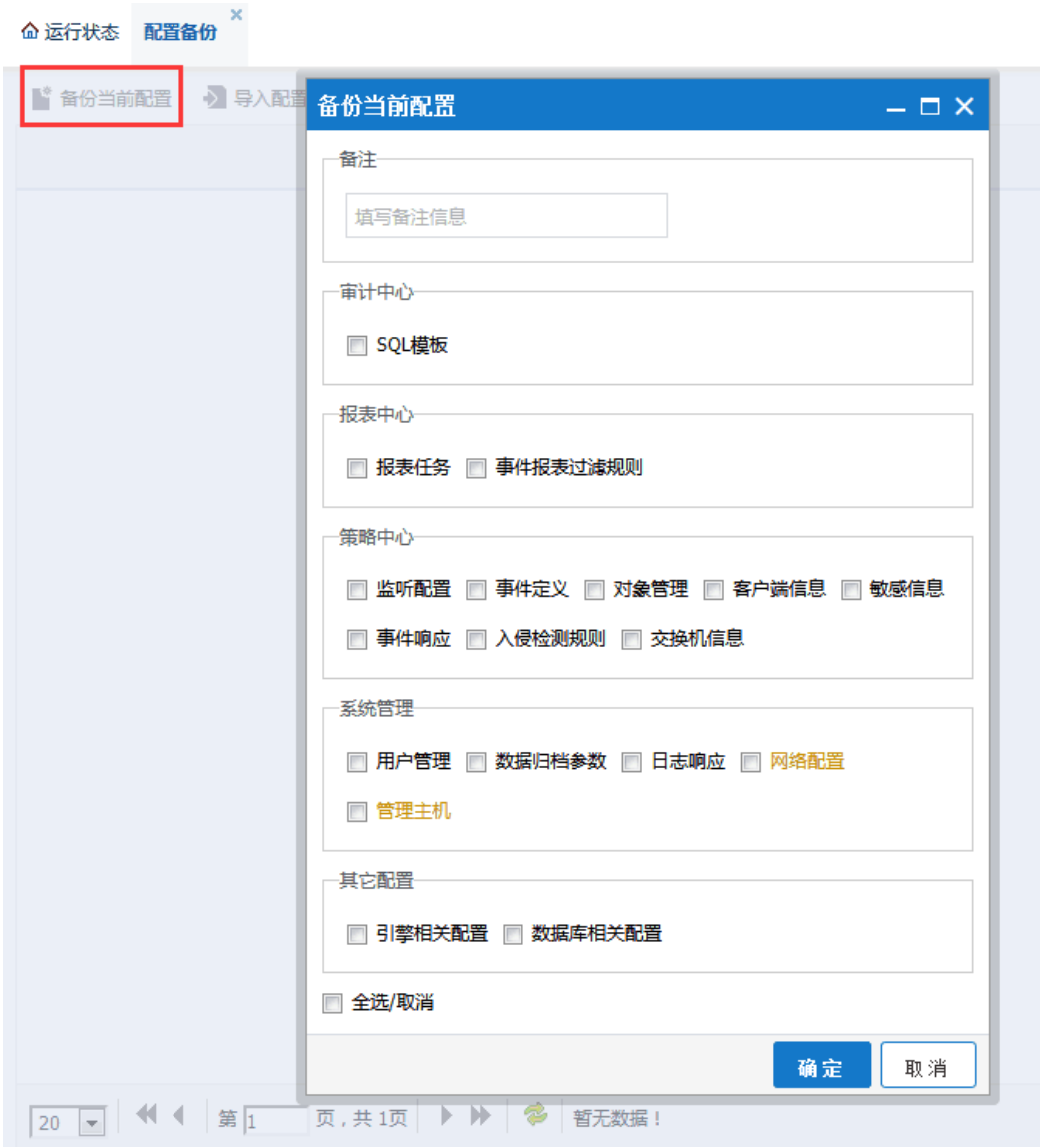



具体作用如下：

## 2. 备份配置

备份当前所有的配置，方便下次恢复。支持备份项的自由选择，可根据所需进行备份。

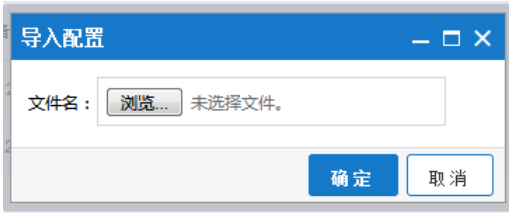
图6-25 备份




## 3. 导入配置

导入之前的备份配置文件。

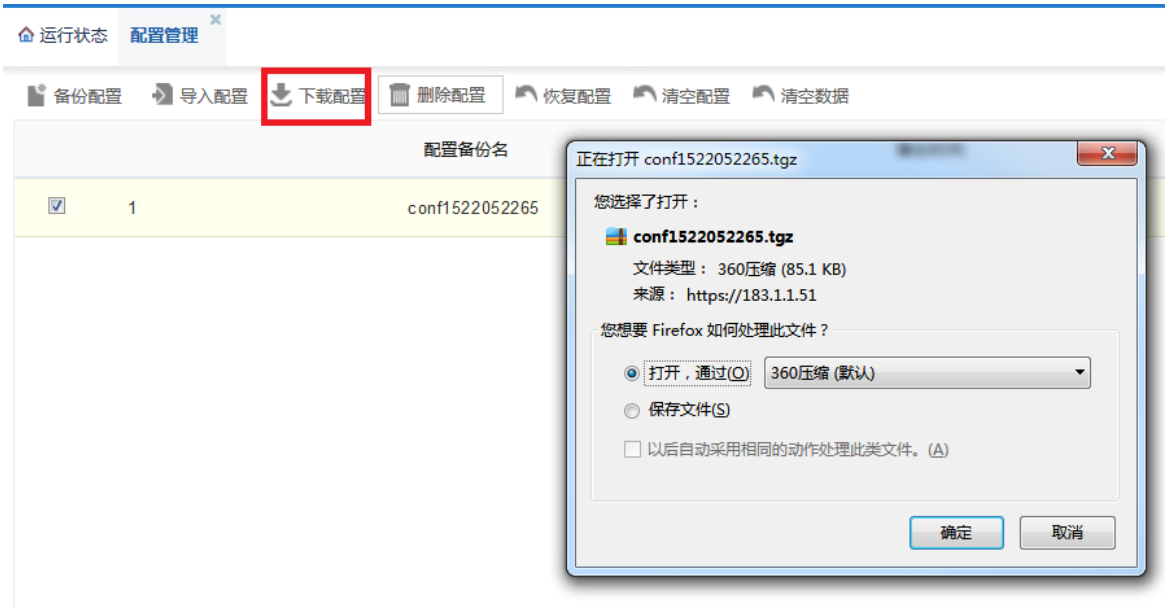
图6-26 导入




## 4. 下载配置

下载系统已有的备份文件，用于下次恢复到某时期的系统配置。勾选某备份的配置记录，点击<下载配置>在弹出框中点击<保存>，将配置文件保存到指定目录中。

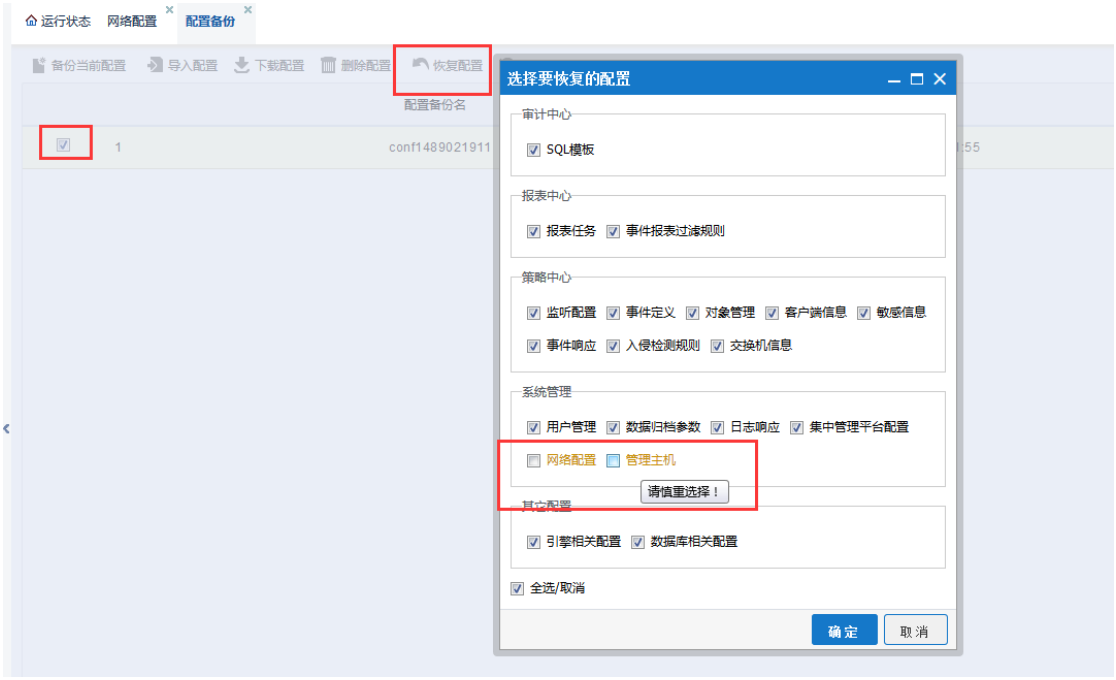
图6-27 下载




## 5. 恢复配置

将系统的配置恢复到某个版本。选择某个配置备份记录，点击<恢复配置>在弹出[选择要恢复的配置]选择相应项，然后点击<确认>，当前的系统配置将恢复到该配置。默认不选择网络配置、管理主机的配置，恢复可能导致系统无法访问，需谨慎选择。

图6-28 恢复配置




## 6. 删除配置

删除配置文件。选择某个配置备份记录后，点击<删除配置>后，将会在系统中删除该配置备份文件。

图6-29 删除


## 7. 清空配置

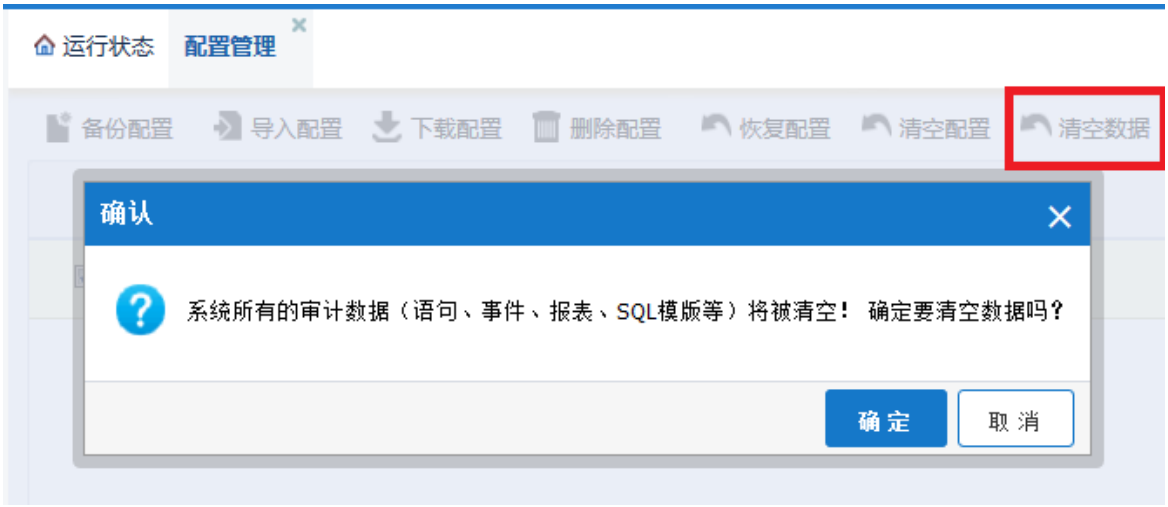
将系统的配置清空，恢复到出厂设置。点击<清空配置>后，在弹出[确认]框中点击<确定>，系统将恢复到默认配置。

图6-30 清空配置


### 8. 清空数据

将系统的审计数据全部清空。点击<清空数据>后，在弹出[确认]框中点击<确定>，系统将清空全部的审计数据。

图6-31 清空数据




## 6.9 系统信息

展示系统的基本信息，包括系统时间，产品信息。用户可以在此修改系统时间，升级和注册系统。

### 1. 系统时间

展示系统的当前的时间，若不准确可以<更改>按钮在弹出[更改日期和时间设置]对话框中更改，弹出的界面如下图所示：

图6-32 系统时间

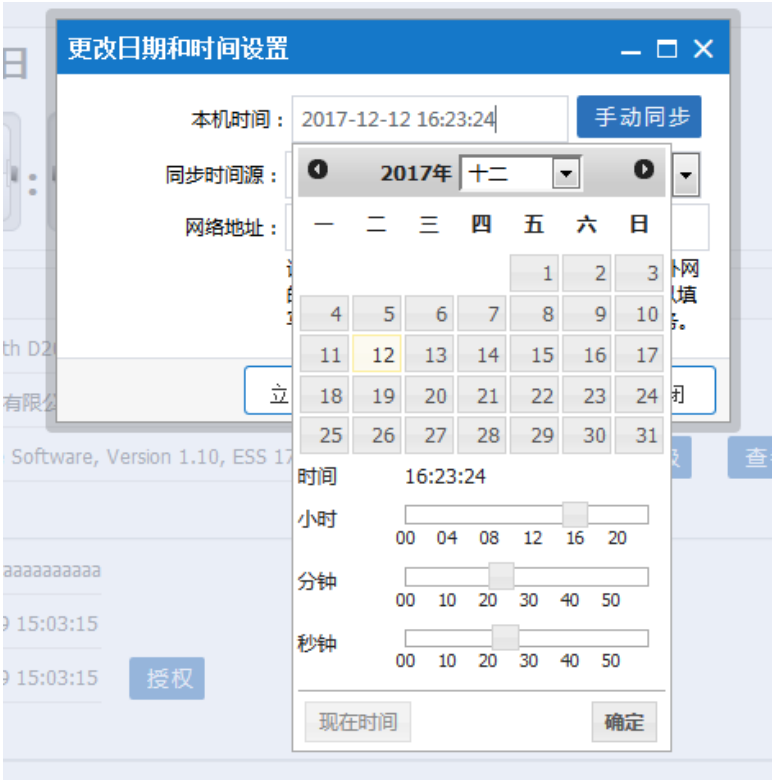

说明

系统时间的准确性，将直接影响采集数据的时间戳。

(2) 手动同步

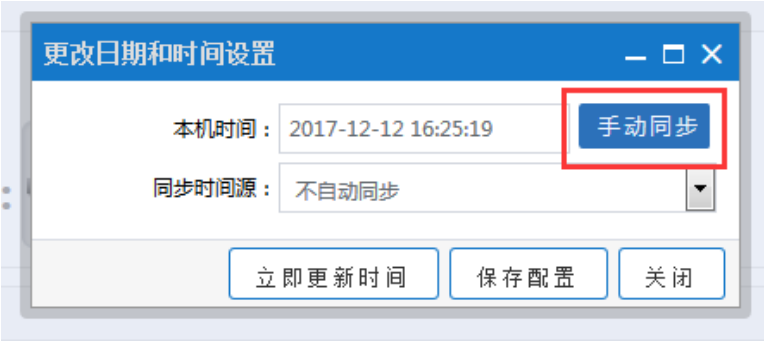
单击弹出框中的“本机时间”输入框，在下拉的列表中设置时间，如下图所示：

图6-33 本机时间




分别设置时、分、秒后点击<确定>按钮后点击<手动同步>按钮，系统时间开始更新时间，并提示更新成功，如下图所示：

图6-34 手动同步




(3) 自动同步

可以有两种同步时间源：从网络上同步、从数据库服务器上同步。不论哪种自动同步，系统将会每天自动在 6:00 和 18:00 分别与同步时间源同步两次时间，确保系统时间准确性。

- 从网络上同步

  需要设置同步时间源的时间服务器，可以是外网的也可以是本地的时间服务器，本地的需要先设置好 NTP 服务，具体内容如下图所示：

图6-35 NTP 服务


- 从数据库服务器上同步

  需要设置同步时间源的相关参数，具体内容如下图所示：

图6-36 更改


配置好同步参数后，点击<保存配置>后关闭串口即可，用户也可以点击<立即更新时间>马上进行时间同步。

(4) 不自动同步

若不希望系统时间自动同步，则可设置为不自动同步。

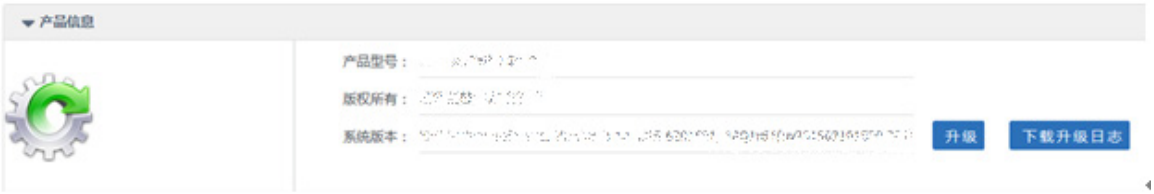
## 2. 产品信息

产品信息中可以对系统进行升级和硬件注册。

(1) 系统升级

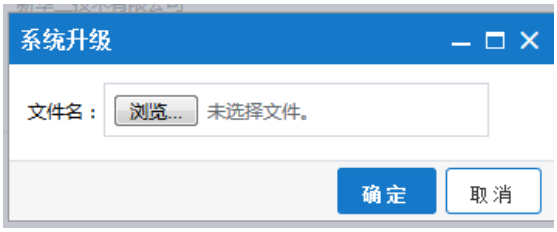
点击界面中的<升级>按钮，可以找到本地已有的升级文件，对系统进行升级，如下图所示：

图6-37 系统升级




点击产品信息中<升级>按钮，会弹出[系统升级]界面，如下图所示：

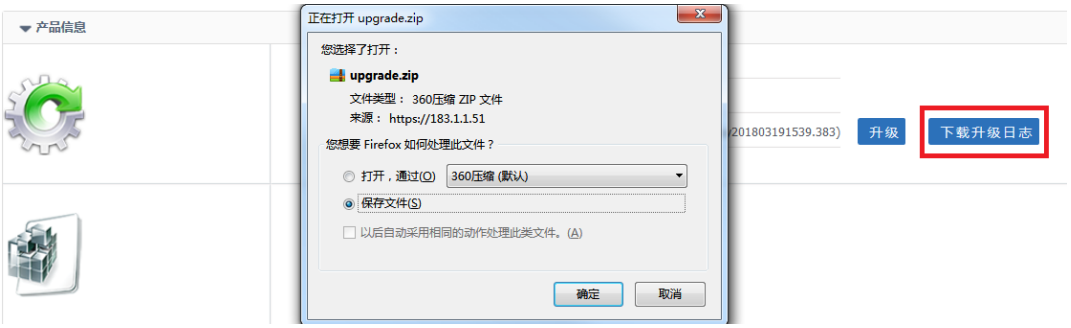
图6-38 升级



(2)　下载升级日志

产品信息中可以下载系统更新日志，点击<下载升级日志>按钮，会弹出界面，如下图所示：

图6-39 查看日志




(3)　系统授权

注册前，需要修正设备系统时间，然后才能硬件信息更新、引擎注册、初始化硬盘等操作。

图6-40 系统授权


## 6.10 管理主机

对主机进行管理，点击左栏菜单[系统管理/管理主机]进入界面，如下图所示：

图6-41 管理主机

## 2. 添加管理主机

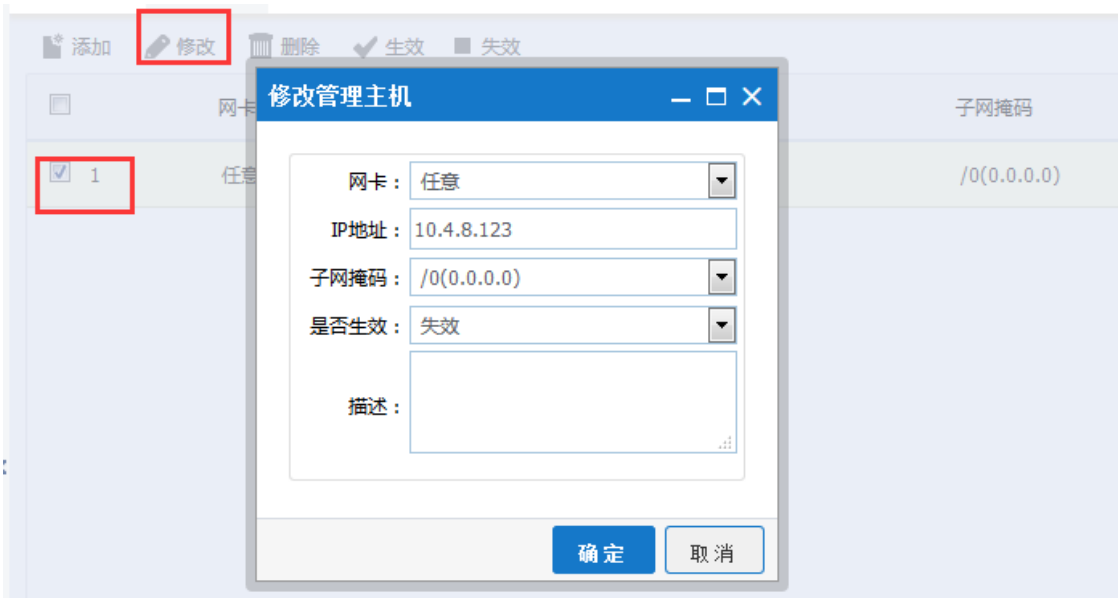
点击<添加>按钮后，填入网卡名、IP 地址、子网掩码、描述即可。如下图所示：

图6-42 添加


## 3. 修改管理主机

选择某个管理主机，点击<修改>按钮后，在弹出[修改管理主机]窗中修改主机信息，如下图所示：

图6-43 修改




### 4. 删除管理主机

选择某个管理主机，点击<删除>按钮后，在弹出[确认]窗口中点击<确定>即可删除该管理主机，如下图所示：

图6-44 删除

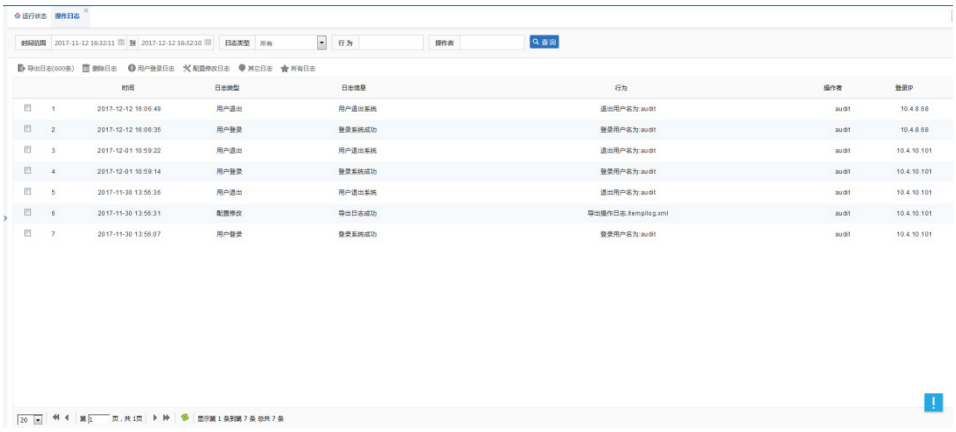

### 5. 生效

对于某管理主机设置后并未马上生效，需要点击<生效>按钮，系统提示“生效成功”才算是生效。点击<失效>按钮，确定该管理主机失效。

## 6.11 操作日志

记录了所有角色的所有用户的操作，主要包括：登录系统日志、配置修改日志、其他日志。点击[系统管理/操作日志]，进入界面如下图所示：

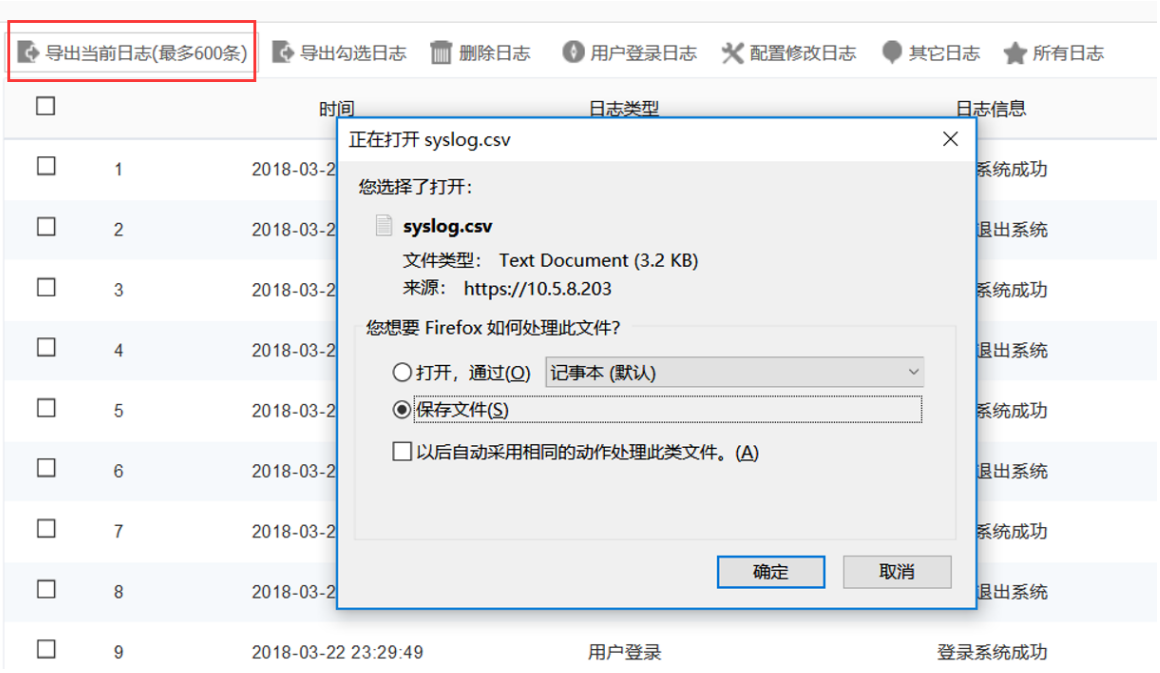
图6-45 操作日志



## 2. 导出日志

点击<导出日志>按钮，可以最多导出 600 条当前所有系统日志，包括用户登录日志及配置修改日志，导出日志的格式为 CSV 格式。

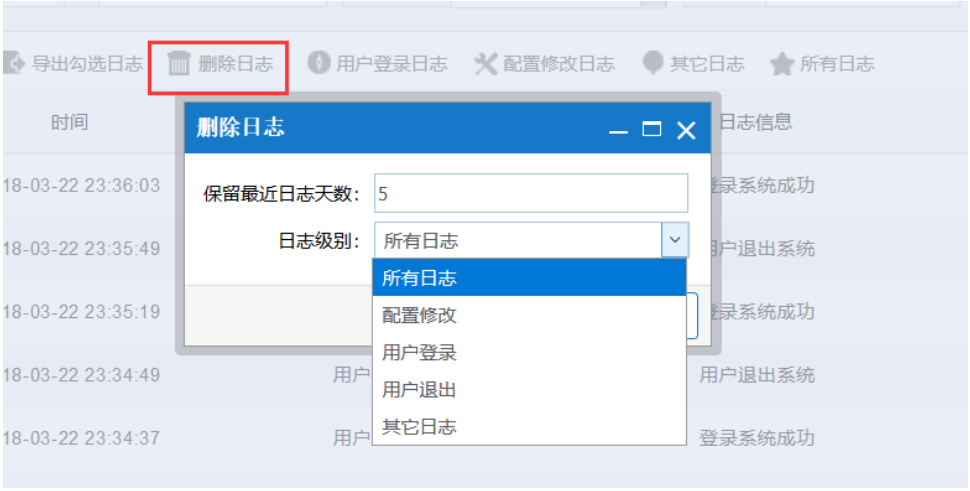
图6-46 导出




## 3. 删除日志

点击<删除日志>按钮，在弹出[删除日志]框中设置删除条件即可删除对应的日志信息。如下图所示：

图6-47 删除日志




### 4. 分类查看各类操作日志

通过鼠标点击 用户登录日志 配置修改日志 其它日志 所有日志 这四个按钮可以查看各类操作日志，各类操作日志内容主要是：

(1) 登录系统日志：系统所有用户登入、登出系统的所有动作将记录于此。

(2) 配置修改日志：用户的系统配置操作内容都将被记录下。

(3) 其他日志：除登录系统日志、配置修改日志外的其他所有日志。

## 6.12 数据归档

实现归档数据的管理，包括三个方面的内容：归档参数配置、归档文件管理。主要是配置归档文件的保留参数，归档文件的下载、删除。

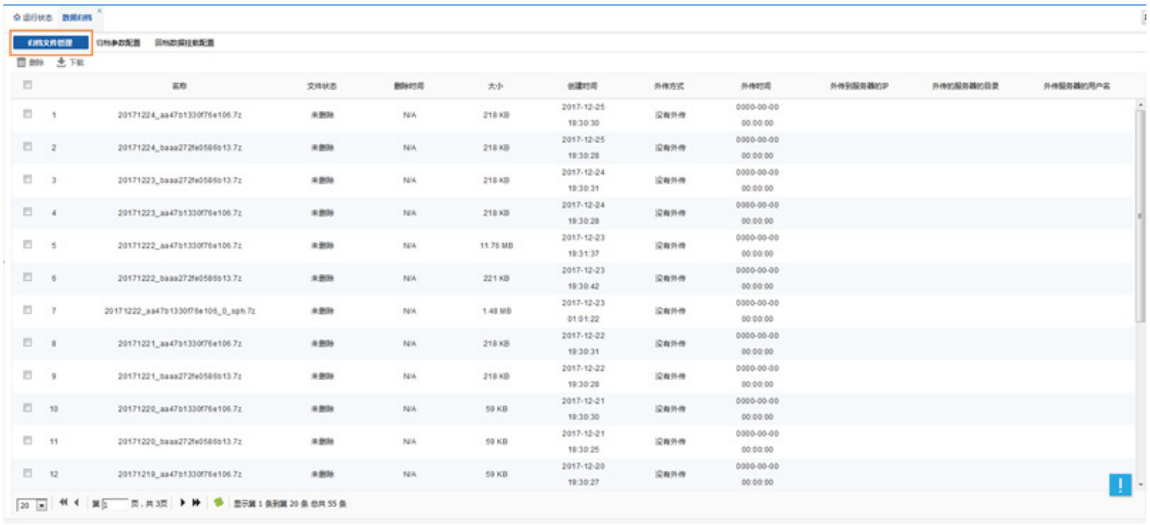
点击[系统管理/数据归档]，界面如下图所示：

图6-48 数据归档

### 6.12.2 归档文件管理

以列表的形式展示归档的文件，还能手动对归档文件进行删除和下载。如下图所示：

图6-49 管理



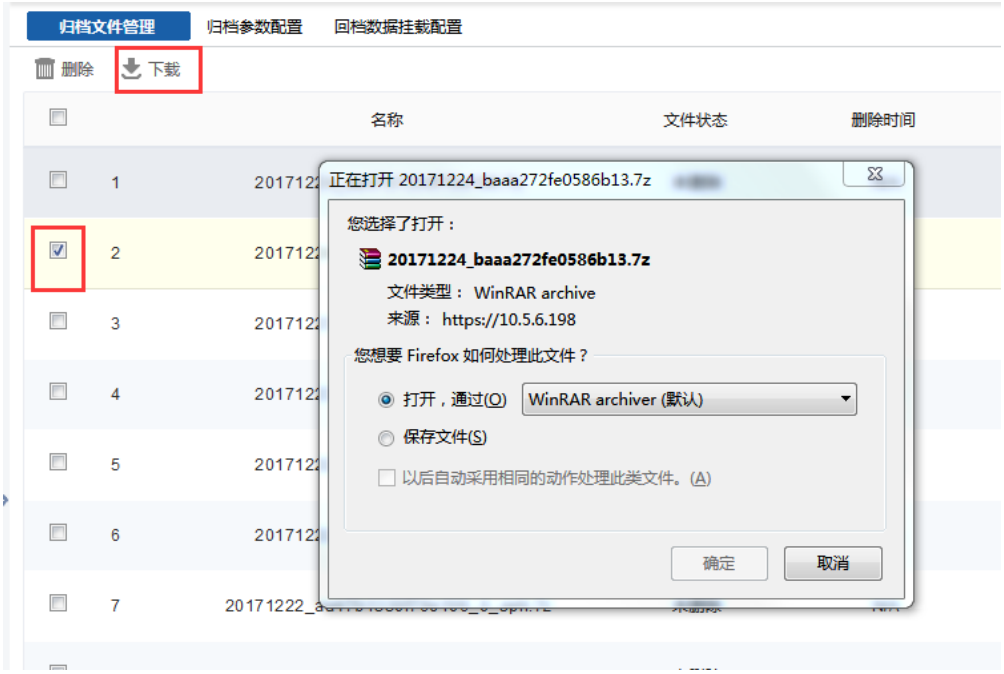
#### 2. 删除归档文件

在列表中勾选某个归档文件后，点击<删除>按钮，在弹出框中选择确定即可删除该归档文件。

#### 3. 下载归档文件

在列表中选择一个归档文件，点击<下载>，如下图所示：

图6-50 下载



### 6.12.3 归档参数设置

图6-51 归档参数配置


主要是设置归档文件外传的设置，各项参数如上图。正确填写各项参数后点击<保存配置>按钮即可，页面会提示结果。

此外系统目前系统默认每天凌晨两点执行归档操作。

### 6.12.4 回档数据挂载配置

图6-52 回档数据挂载配置


主要是配置回档数据挂载的设置，各项参数如上图。正确填写个性参数后点击<挂载>按钮即可，页面会提示结果。