

数据库审计系统

用户手册

Copyright © 2012-2017 UCloud

上海优刻得信息科技有限公司

目录

| | |
|---------------------|----|
| 一、系统管理平台 | 2 |
| 1、登陆 | 2 |
| 2、系统管理平台整体预览 | 2 |
| 3、数据维护 | 3 |
| 3.1 自动备份 | 3 |
| 3.2 数据恢复 | 5 |
| 3.3 磁盘告警 | 6 |
| 3.4 手动清理 | 7 |
| 4、通知服务 | 8 |
| 4.1 SNMP 配置 | 8 |
| 4.2 SYSLOG 配置 | 8 |
| 5、系统升级 | 9 |
| 6、日志管理 | 9 |
| 7、系统管理 | 10 |
| 7.1 安全设置 | 10 |
| 7.2 FTP 配置 | 11 |
| 8、基本配置 | 12 |
| 8.1 证书管理 | 12 |
| 8.2 管理口配置 | 12 |
| 8.3 审计口配置 | 12 |
| 8.4 名称配置 | 13 |
| 8.5 NTP 配置 | 13 |
| 8.6 节点配置 | 14 |
| 8.7 邮件服务器配置 | 14 |
| 8.8 短信平台配置 | 15 |
| 8.9 设备维护 | 15 |
| 8.10 出厂设置 | 15 |
| 二、规则管理平台 | 16 |
| 1、规则管理平台整体预览 | 16 |
| 2、全局参数设置 | 17 |

| | |
|-----------------------|-----------|
| 2.1 审计对象别名 | 17 |
| 2.2 访问者别名 | 17 |
| 2.3 隐秘数据设置 | 18 |
| 2.4 审计控制 | 19 |
| 2.5 通知策略 | 20 |
| 3、访问者信息配置 | 21 |
| 3.1 进程配置 | 21 |
| 3.2 驱动级 IP 过滤 | 22 |
| 3.3 IP 监控 | 22 |
| 3.4 规则生效时间 | 23 |
| 4、对象设置 | 24 |
| 4.1 子对象 | 24 |
| 4.2 审计对象 | 25 |
| 4.3 通知对象 | 27 |
| 5、规则配置 | 28 |
| 5.1 操作类型 | 28 |
| 5.2 组合规则 | 29 |
| 5.3 规则管理 | 30 |
| 5.4 白名单管理 | 31 |
| 5.5 规则组管理 | 31 |
| 5.6 系统语句 | 32 |
| 三、审计管理平台 | 33 |
| 1、审计管理平台预览 | 33 |
| 2、风险管理 | 34 |
| 2.1 风险查询 | 35 |
| 3、审计管理 | 37 |
| 3.1 日常行为查询 | 37 |
| 3.2 白名单管理 | 38 |
| 3.3 事件回放 | 38 |
| 3.4 使用工具监控 | 39 |
| 3.5 阻断 IP | 40 |

| | |
|--------------------|----|
| 4、报表管理 | 41 |
| 4.1 等级保护报表 | 41 |
| 4.2 用户登录注销报表 | 42 |
| 4.3 表对象访问情况报表..... | 42 |
| 4.4 用户操作情况统计 | 43 |
| 4.5 访问失败次数排行 | 44 |
| 4.6 用户访问情况统计 | 45 |
| 4.7 每天平均数据统计 | 46 |
| 4.8 月度风险统计报表 | 47 |
| 4.9 自定义报表设置 | 48 |
| 5、日志管理 | 49 |
| 5.1 操作日志 | 49 |
| 6、系统管理 | 49 |
| 6.1 用户管理 | 49 |
| 6.2 系统状态 | 50 |

一、系统管理平台

系统管理平台主要是针对审计系统的整体配置，包括系统基本配置、数据维护、系统日志、通知服务等。

1、登陆

打开 web 浏览器，在地址栏输入审计设备的管理 IP 地址或输入 https://IP，IP 为审计设备的 IP 地址，打开登陆界面。初始的登陆账号和登陆密码为：admin。

如需有关浏览器支持的浏览器的信息，请参阅第 1 页中支持的浏览器信息。



图 2 登陆界面

2、系统管理平台整体预览

分为两大块，左边为导航菜单，中间部分为系统状态（系统实时状态、满足规则的 sql 语句数量、实时流量状态）。

系统管理平台整体预览：

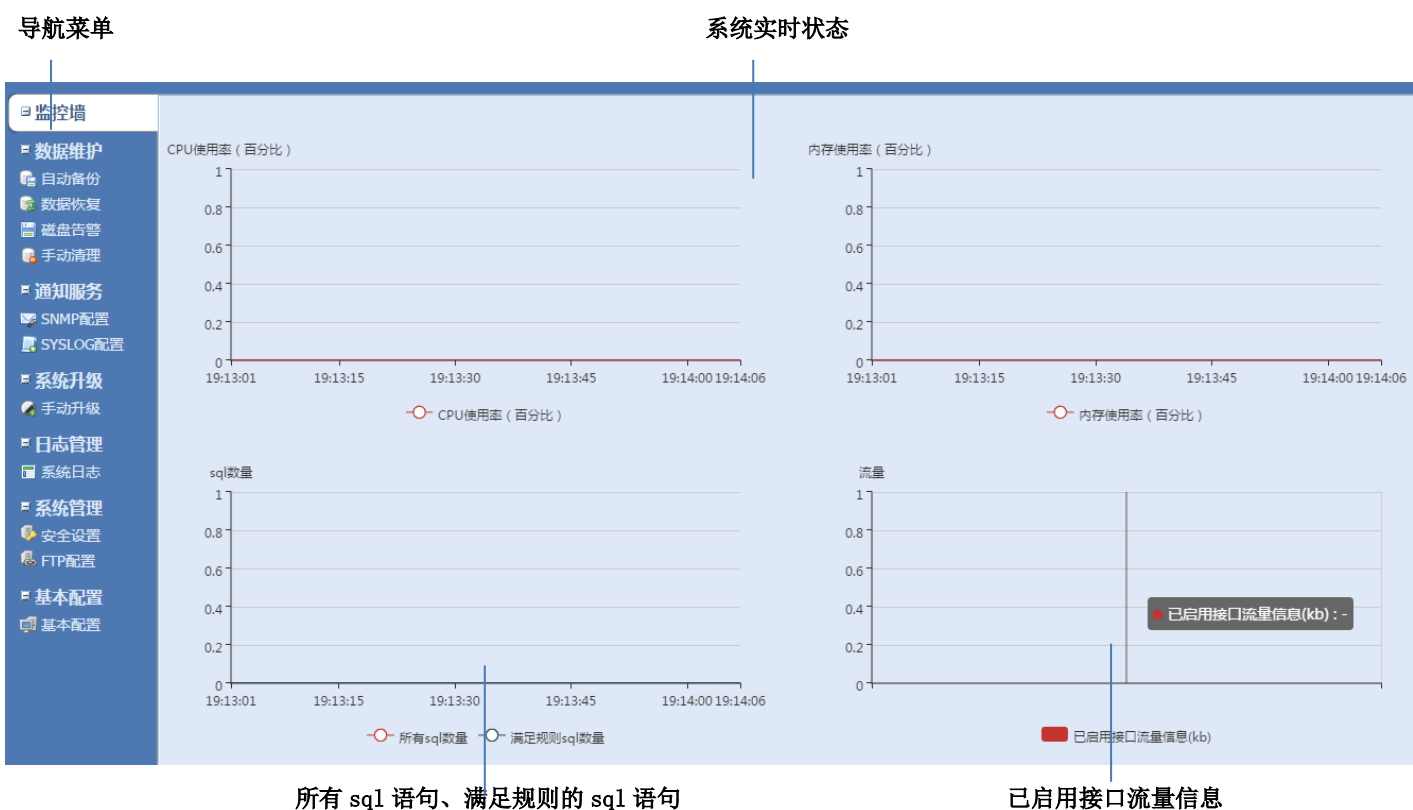


图 3 系统管理平台预览

模块介绍:

| 登陆安全参数 | 说明 |
|------------------------------|---|
| 导航菜单 | 各功能模块及子菜单，详细信息请查看各功能模块描述。 |
| 系统实时状态 | 以折线图的方式显示设备 CPU 使用率和内存使用率。 |
| 已启用接口流量信息 | 以柱状图的方式实时显示配置的已启用接口的流量情况 |
| 所有 sql 语句、满足规则 的 sql 语句数量 | 以折线图的方式显示所有审计到的所有 sq 语句数量及满足规则的 sql 语句数量。 |

3、数据维护

此模块是对审计设备的数据的备份、恢复、磁盘告警、清理等的设置。

3.1 自动备份

点击“数据维护”-“自动备份”，打开“自动备份”界面，

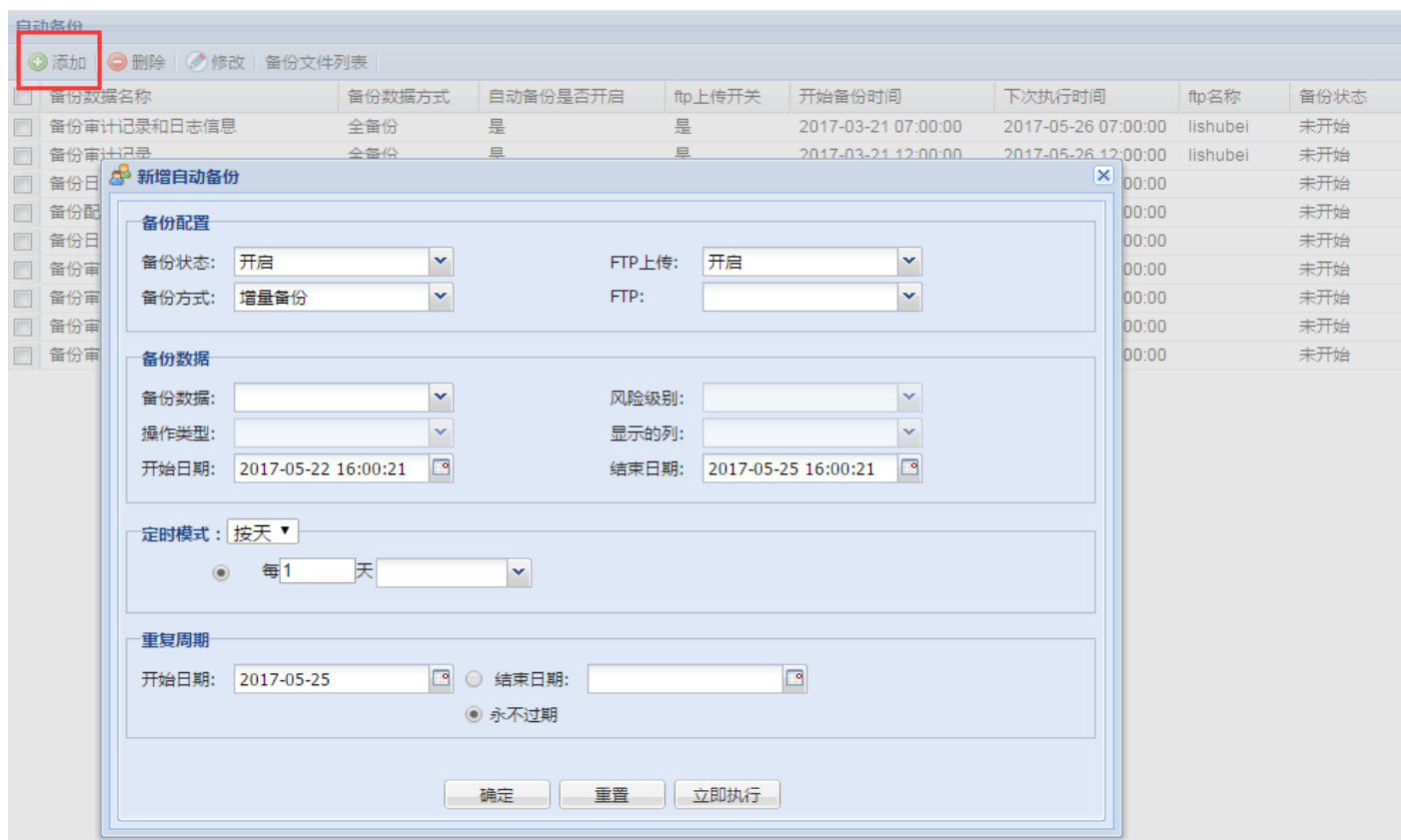


图 4 自动备份主要内容

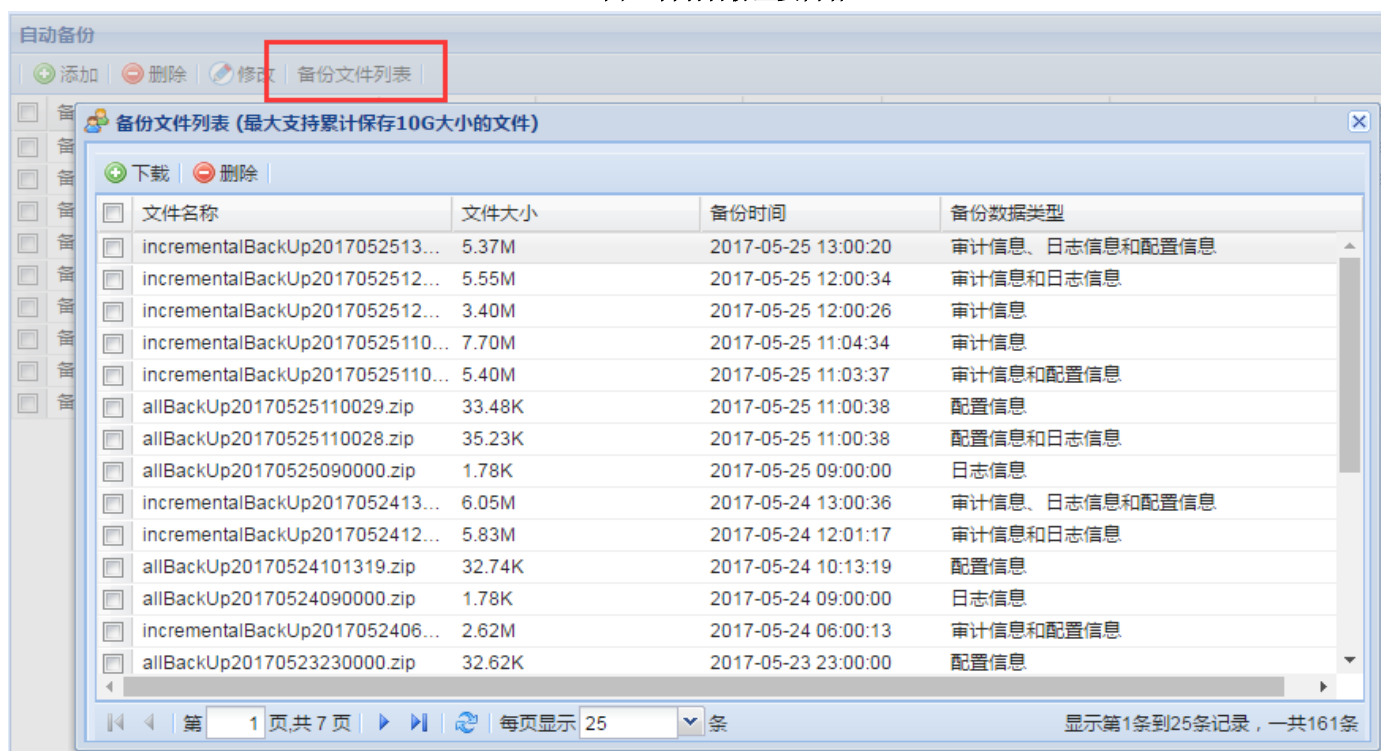


图 5 备份文件列表

此功能是设置是否开启自动备份，若开启自动备份，需要同时开始 FTP 上传功能，以及备份的时间、备份的模式、备份的数据、重复周期等的设置，备份好的数据可以在本分文件列表中进行下载。

开启 FTP 上传功能时，需要进入“系统管理”里进行 FTP 设置。



注意：备份数据时，开启自动备份时，需要同时开启 FTP 功能，且对 FTP 服务器进行设置。

备份的内容主要有：

| 名称 | 说明 |
|------|--------------|
| 审计记录 | 审计设备审计到的记录 |
| 日志信息 | 系统的操作日志和系统日志 |
| 配置信息 | 审计设备的所有配置信息 |

备份方式：

| 名称 | 说明 |
|------|-----------------|
| 全备份 | 将所有数据全部一次性备份 |
| 增量备份 | 跟上次相比，增加的部分进行备份 |

3.2 数据恢复

点击“数据维护”-“数据恢复”，点击“导入”，就可以将备份到 FTP 服务器的备份数据，导入系统中，然后进行恢复，同时可以根据恢复状态进行查找。

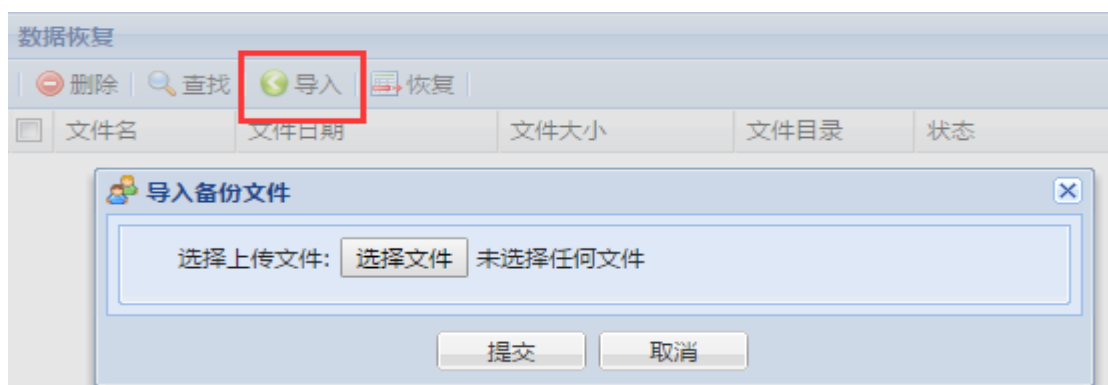


图 6 导入恢复文件

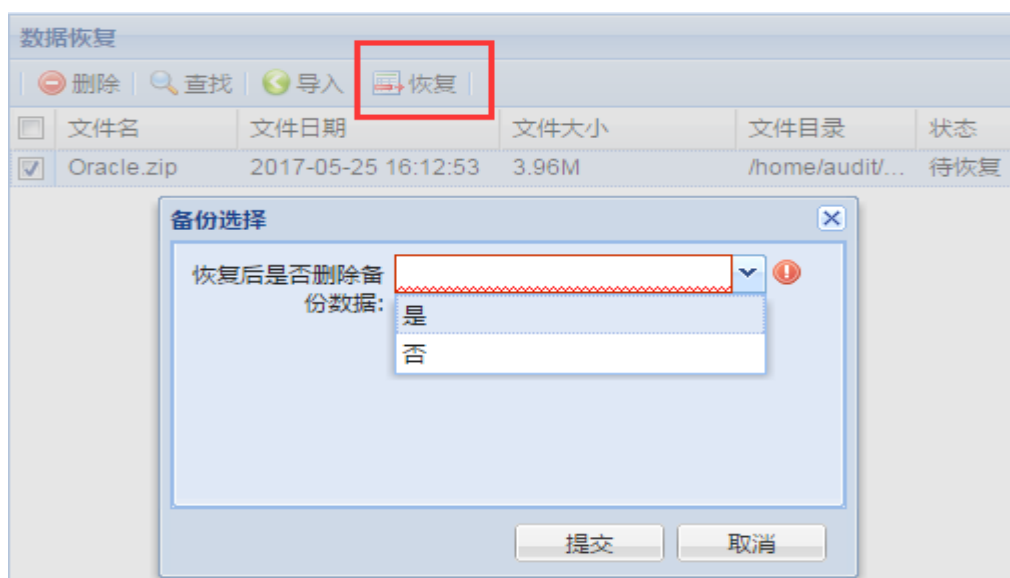


图 7 数据恢复



注意：所有备份的数据均为.gz、.zip、.ibd 扩展名的文件。

功能简介：

| 名称 | 说明 |
|----|---|
| 查找 | 点击“查找”，可以根据数据恢复的状态，分别是待恢复、恢复中、恢复成功及恢复失败进行查看 |
| 导入 | 将备份的审计数据、配置信息、日志等导入系统，进行恢复 |
| 恢复 | 选中导入的数据，然后选择是否删除备份数据，进行恢复。 |

此项功能对已备份并删除的数据，可在此进行恢复。

3.3 磁盘告警

点击“数据维护”-“磁盘告警”，打开“磁盘告警”设置界面，

磁盘信息

| | |
|----------|----------|
| 磁盘空间总量: | 566.214G |
| 已占用磁盘空间: | 73.329G |
| 剩余空间可使用: | 492.884G |

设置

告警阈值设置:

说明: (告警阈值是磁盘已经使用多少百分比后就会报警和清理数据，以短信和邮件的方式提醒管理员。)

数据处理

是否开启: ☒ 是 ☐ 否

处理方式: ☒ 转存 ☐ 覆盖

FTP:

保留最近数据(天):

说明：系统将使用“处理方式”中的策略对数据进行处理,清理数据优先按你设置的阈值去清理，清理最早的数据直到磁盘已用空间到阈值以下，然后再按保存天数去覆盖和转存，当磁盘剩余空间不到10%时，系统将强制清理磁盘最早的数据。提示：不会清理风险数据。

图 8 磁盘告警功能界面

功能说明：

| 名称 | 说明 |
|------|--|
| 磁盘信息 | 显示当前磁盘总量、已占用和剩余磁盘空间 |
| 设置 | 定义磁盘告警阈值、当磁盘容量达到或超过这个阈值时，就会已邮件或短信方式通知管理员，并进行相应的“数据处理”。 |

| | |
|------|--------------|
| 数据处理 | 开启或关闭数据处理功能。 |
|------|--------------|

数据处理功能:

| 名称 | 说明 |
|--------|--|
| 转存 | 当磁盘空间达到设定阈值，就转存到配置好的 FTP 服务器 |
| 覆盖 | 覆当磁盘空间达到设定阈值，就以覆盖的形式，覆盖早期的数据，保留定义最近多少天的数据。 |
| 保留最近数据 | 根据规定天数的数据系统不会进行清理 |

此功能是针对磁盘达到阈值时，通过“数据处理”功能进行相应的处理。



注意：转存的话，需要配置 FTP 服务器

3.4 手动清理

点击“数据维护”-“手动清理”，打开“手动清理”界面，

| 风险级别 | 开始时间 | 结束时间 | 审计对象 | 运行时间 | 状态 |
|------|-----------------|-----------------|------------------|------|-----------|
| 低风险 | 2017-05-10 1... | 2017-05-25 1... | 43orcl,orcl12... | 0分 | 清理数据正在... |

图9 手动清理界面

手动清理功能:

| 名称 | 说明 |
|-----------|------------------------|
| 风险级别 | 可以针对不同风险级别进行清理 |
| 开始时间/结束时间 | 定义需要清理数据的时间段 |
| 审计对象 | 可以针对某个审计对象进行清理，也可以不选择。 |

此功能是在磁盘空间不足的情况下，对旧风险数据或者可以删除的非风险数据进行手动清理。



注意：对于大数据的处理，建议联系本公司工程师进行咨询。

4、通知服务

此模块的功能在产生风险时，是能以 SNMP、SYSLOG 的方式通知管理员。

4.1 SNMP 配置

点击“通知服务”-“SNMP 配置”，打开“添加”界面。



The image shows the 'SNMP配置' (SNMP Configuration) window. At the top, there are three buttons: '添加' (Add), '删除' (Delete), and '修改' (Modify), each with a corresponding icon. Below these buttons is a table with columns: '服务器IP' (Server IP), '团体名' (Community Name), '版本号' (Version), '发送频率' (Send Frequency), and '是否启用' (Whether Enabled). The table contains one row with the following values: '192.168.10.174', 'public', '3', '2', and '是'. Below the table is a '新增SNMP' (Add New SNMP) dialog box. This dialog box has several fields: '是否启用' (Whether Enabled) with a dropdown menu set to '是' (Yes); '服务器IP' (Server IP) with a text box containing '192.168.10.207'; '发送频率' (Send Frequency) with a dropdown menu set to '4' and a unit '秒/次' (seconds/time); 'SNMP版本' (SNMP Version) with a dropdown menu set to 'V1'; and '服务器团体名' (Server Community Name) with a text box containing 'public'. At the bottom of the dialog box is a '确定' (Confirm) button.

图 10 SNMP 配置

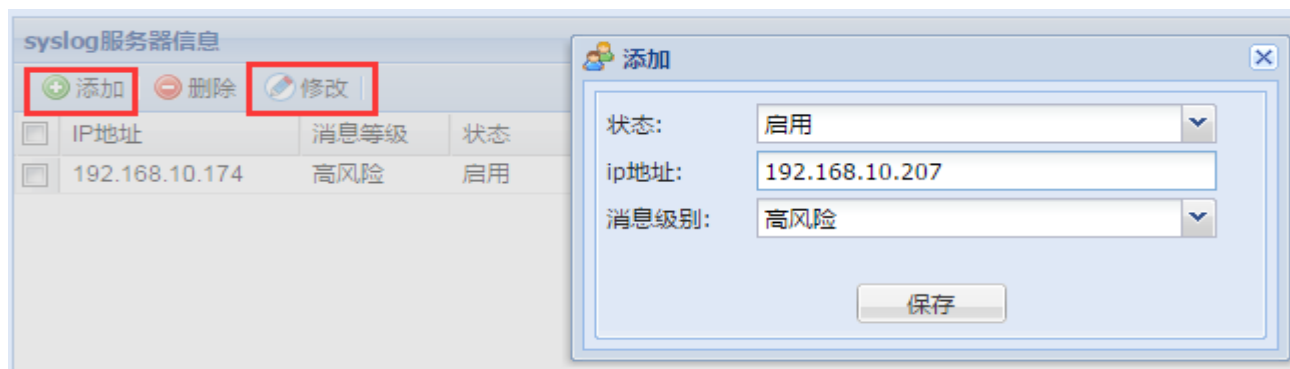
此项是针对 SNMP 服务器的配置，包括状态（是否启用）、SNMP 版本、服务器 IP、服务器团体名、发送频率。



SNMP 称为简单网络管理协议，由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资源对象。SNMP 发送端会传送出一个小的文字信息到 SNMP 接收端。

4.2 SYSLOG 配置

点击“通知服务”-“SYSLOG 设置”，打开“添加”界面。



The image shows the 'syslog服务器信息' (SYSLOG Server Information) window. At the top, there are three buttons: '添加' (Add), '删除' (Delete), and '修改' (Modify), each with a corresponding icon. Below these buttons is a table with columns: 'IP地址' (IP Address), '消息等级' (Message Level), and '状态' (Status). The table contains one row with the following values: '192.168.10.174', '高风险' (High Risk), and '启用' (Enabled). Below the table is an '添加' (Add) dialog box. This dialog box has three fields: '状态' (Status) with a dropdown menu set to '启用' (Enabled); 'ip地址' (IP Address) with a text box containing '192.168.10.207'; and '消息级别' (Message Level) with a dropdown menu set to '高风险' (High Risk). At the bottom of the dialog box is a '保存' (Save) button.

图 11 SYSLOG 配置

此项是针对 SYSLOG 服务器的配置，包括状态（是否启用）、IP 地址、消息级别等。



Syslog 称为系统日志或系统记录，是一种用来在互联网协议（TCP/IP）的网络中传递记录档信息的标准。syslog 发送端会传送出一个小的文字信息（小于 1024 字节）到 syslog 接收端（通常称为 syslog 服务器）。

消息级别内容：

| 消息级别名称 | 说明 |
|--------|-----|
| Emerg | 高风险 |
| Crit | 中风险 |
| Notice | 低风险 |

5、系统升级

点击“系统升级”-“手动升级”，打开“手动升级”界面，

图 12 手动升级

“手动升级”选择需要进行升级的文件，同时也可以对历史的升级记录进行查看。手动升级的文件应该是以 .zip、.sql 或以 audit.tar.gz 结尾的文件。

6、日志管理

点击“日志管理”-“系统日志”，打开“系统日志”界面，

系统日志

详细

查询

导出服务及数据库日志

导出excel

导出pdf

| 时间 | 日志类型 | 事件级别 | 内容 | 描述 |
|---|------|------|----|--|
| <input type="checkbox"/> 2017-05-23 19:55:59 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 19:37:58 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 19:28:37 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 17:47:02 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 17:03:39 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 16:58:28 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input checked="" type="checkbox"/> 2017-05-23 16:44:16 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 16:34:51 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 15:31:12 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 15:28:30 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 15:14:21 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 14:09:12 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 14:08:54 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 13:43:24 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 13:17:40 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 13:12:42 | 其他日志 | 一般事件 | 成功 | 启动审计引擎 |
| <input type="checkbox"/> 2017-05-23 13:00:01 | 其他日志 | 一般事件 | 成功 | 自动备份成功，备份文件名：incrementalBackUp20170523130000 |
| <input type="checkbox"/> 2017-05-23 12:00:02 | 其他日志 | 一般事件 | 成功 | 自动备份成功，备份文件名：incrementalBackUp20170523120000 |
| <input type="checkbox"/> 2017-05-23 12:00:02 | 其他日志 | 一般事件 | 成功 | 自动备份成功，备份文件名：incrementalBackUp20170523120000 |
| <input type="checkbox"/> 2017-05-23 10:59:34 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 10:48:40 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 10:42:12 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 10:16:27 | 其他日志 | 一般事件 | 成功 | 守护进程成功启动 |
| <input type="checkbox"/> 2017-05-23 09:00:00 | 其他日志 | 一般事件 | 成功 | 自动备份成功，备份文件名：allBackUp20170523090000 |
| <input type="checkbox"/> 2017-05-23 06:00:01 | 其他日志 | 一般事件 | 成功 | 自动备份成功，备份文件名：incrementalBackUp20170523060000 |

图 13 系统日志管理

“系统日志”可以针对域名（包括审计引擎、备份引擎、守护进程、监听进程、动作引擎等），日志类型（异常日志、其他日志）、处理状态（处理中、未处理等）、事件级别（一般事件、致命告警）等多个查询条件查询系统日志。

7、系统管理

此模块主要是对系统的安全、FTP 的配置。

7.1 安全设置

点击“系统管理”-“安全设置”，打开“安全设置”界面，

安全设置

登录控制

限制登录时间: 45秒

限制登录次数: 3

锁定用户时间: 60秒

超时退出时间: 3600秒

密码控制

密码最短长度: 8

密码最长长度: 30

密码过期时间: 14天

密码过期状态: 禁用

保存

取消

web登录IP白名单:

web登录IP黑名单: 1.1.1.1

说明: 多个IP使用符号"&&"分隔开; 如果是地址段, 地址段的起始地址和终止地址使用符号"="隔开, 多个地址段使用";"隔开; 不能同时存在"&&"和"="符号, 配置地址段时使用英文分号";"结束。

保存

取消

图 14 系统安全设置

安全设置的功能是对尝试登录并登录失败的用户进行限制和密码的安全设置，并可以对一些确认安全用户 IP/网段添加到白名单，对非法用户 IP/网段添加到黑名单以限制登录。

登陆安全参数设置：

| 登陆安全参数 | 说明 |
|--------|--|
| 限制登陆时间 | 与限制登陆次数结合，即在限制登陆时间内限制登陆次数 n 次。 |
| 限制登陆次数 | 参照限制登陆时间说明，尝试登陆但是登陆失败 |
| 锁定用户时间 | 配合限制登陆时间、限制登陆次数，在限制登陆时间内，超过限制登陆（登陆失败）次数，账户即被锁定多长时间 |

安全退出时间 在界面无任何的操作下，超过此时间将退出，保护界面信息不被泄露。

密码长度参数设置：

| 密码长度参数 | 说明 |
|--------|------------------|
| 密码最短长度 | 设置密码时，最短不能少于该长度。 |
| 密码最长长度 | 设置密码时，最长不能大于该长度。 |
| 密码过期时间 | 设置的密码将在多长时间内过期。 |
| 密码过期状态 | 密码过期之后是继续使用还是禁用。 |

web 登录 IP 白名单：设置某个 IP/网段可以登录 web 系统管理平台

web 登录 IP 黑名单：设置某个 IP/网段不可以登录 web 系统管理平台

7.2 FTP 配置

点击“系统管理”-“FTP 配置”，打开“添加”界面，



图 15 FTP 服务器配置

此功能是对 FTP 服务器进行配置，设置 FTP 名称、地址、FTP 用户名、密码和存放路径，可以存放备份数据和系

统转存数据。

8、基本配置

此模块是对系统证书、管理口、审计口、名称、NTP、节点、邮件服务器、短信平台等的配置，还可以对系统进行设备维护和出厂设置。

8.1 证书管理

点击“基本管理”-“证书管理”，打开“证书管理”界面，



图 16 证书管理

此功能对审计设备系统证书进行管理，文件格式是以_audit.lic 结尾。

8.2 管理口配置

点击“基本配置”-“管理口配置”，打开“管理口配置”界面，

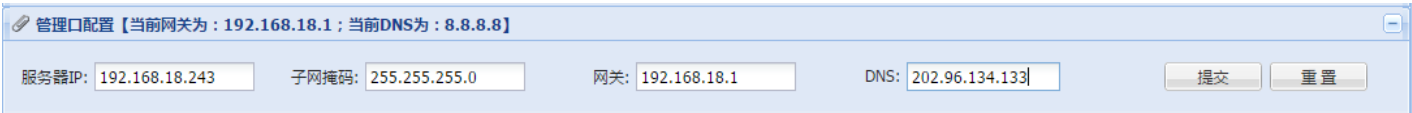


图 17 审计设备管理口

管理口配置是对管理口的各项网络信息，包括 IP、子网掩码、网关、DNS 等进行配置。



注意：修改这里的 IP 等信息之后，需要在地址栏中输入新的 IP，重新登录。

8.3 审计口配置

点击“基本配置”-“审计口配置”，打开“审计口配置”界面，

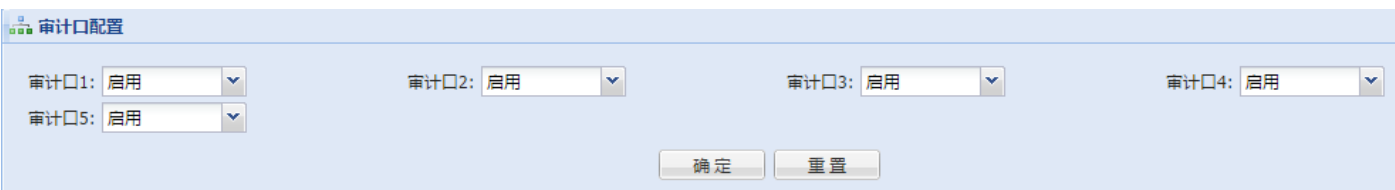


图 18 审计设备的审计口配置

“审计口配置”主要是针对审计口是否启用进行相应的配置。启用某个审计口并且该审计口有流量进入时，将对该部分数据进行审计；禁用之后，该审计口的数据将不做审计。



注意：在审计口拔线告警过于频繁时，可以将该审计口设置为“禁用”。

8.4 名称配置

点击“用户管理”-“名称配置”，打开“名称配置”界面，

名称配置

系统名称: UCloud 数据库审计系统

提交

图 19 平台名称配置

此功能是对系统的名称的标题进行更改。

8.5 NTP 配置

点击“系统配置”-“NTP 配置”，打开“NTP 配置界面”，

NTP配置【当前系统时间：2017-05-27 10:48:24 AM | 时钟同步周期: 每10分钟;】

手动设置系统时间 更新时钟同步周期 更新NTP服务器地址

图 20 平台 NTP 配置

系统时间设置

系统时间:

说明：时间格式为:YYYY-MM-DD H:M:S
例如：2013-05-09 23:32:09

提交 重置

图 21 系统时间设置

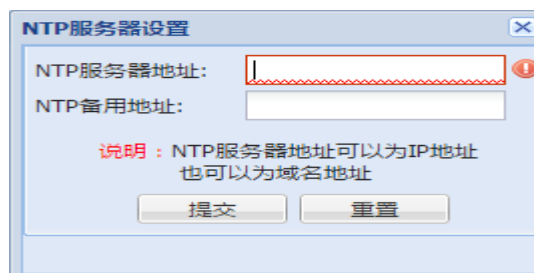
时钟同步周期设置

同步周期: 月 周 天 小时 分

周期详情: 星期 点 分

提交 重置

图 22 系统同步周期设置



NTP服务器设置

NTP服务器地址:

NTP备用地址:

说明: NTP服务器地址可以为IP地址
也可以为域名地址

提交 重置

图 23 NTP 服务器设置

NTP 即 Network Time Protocol，是用来使计算机时间同步的一种协议，这里的功能是设置 NTP（时间）服务器地址、同步周期以及设置系统时间。

功能简介:

| 名称 | 说明 |
|--------------|-----------------------------|
| 更新时钟同步周期 | 与 NTP 时间服务器同步的周期，隔多长时间同步一次。 |
| 手动设置系统时间 | 手动设置审计设备的系统时间。 |
| 更新 NTP 服务器地址 | 修改更新 NTP 时间服务器地址。 |



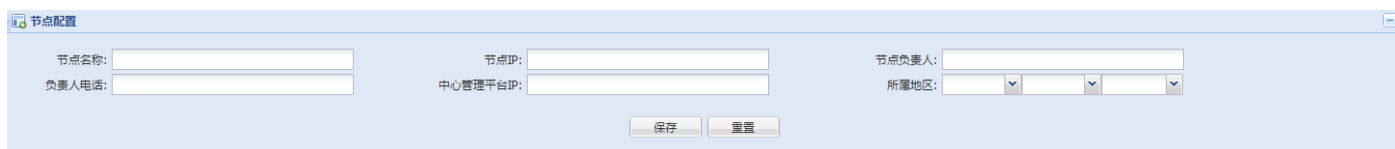
注意：对于加密的 SQL Server 数据库，需要保证数据库服务器的时间与审计设备的时间误差不能超过五分钟，否则将审计不到进程名、操作系统主机名、登录用户名等。

8.6 节点配置



注意：此项功能只有在使用集中管理平台时才需要配置。

点击“基本配置”-“节点配置”，打开“节点配置”界面，



节点名称:

节点IP:

节点负责人:

负责人电话:

中心管理平台IP:

所属地区:

保存 重置

图 24 集中管理平台-节点配置

“节点配置”主要是针对这个节点的信息，包括节点 IP、负责人及中心管理平台的 IP 进行配置。

| 名称 | 说明 |
|------------|------------------------|
| 节点名称 | 定义该节点的名称，方便用户直观看到是哪个节点 |
| 节点 IP | 该节点的审计设备 IP 地址 |
| 节点负责人 | 节点的主要负责人，可设置为该节点的管理员 |
| 负责人电话 | 根据实际情况填写 |
| 中心管理员平台 IP | 集中管理平台中心设备的 IP |
| 所属地区 | 定义该节点是哪个省、市、区域 |

8.7 邮件服务器配置

点击“基本配置”-“邮件服务器配置”，打开“邮件服务器配置”界面，

图 25 邮件服务器配置

此功能是对系统的测试以及受到告警信息的邮箱进行配置。

8.8 短信平台配置

点击“基本配置”-“短信平台配置”，打开“短信平台配置”界面，

图 26 短信平台配置

此功能是对系统的短信平台行配置。

8.9 设备维护

点击“基本配置”-“设备维护”，打开“设备维护”界面，

图 27 设备维护界面

8.10 出厂设置

点击“基本配置”-“出厂设置”，打开“出厂设置”界面，

图 28 出厂设置界面

二、规则管理平台

主要功能是针对规则的设置管理、别名的设置、审计对象的设置等。

登录界面请参照第 3 页系统管理平台的登录。默认的策略管理员的用户名为 ruleadmin，密码为 12345678。

1、规则管理平台整体预览

分为三大块，左边部分为导航菜单，中间部分规则适用情况，右边部分包括审计状态和 IP 过滤名单。

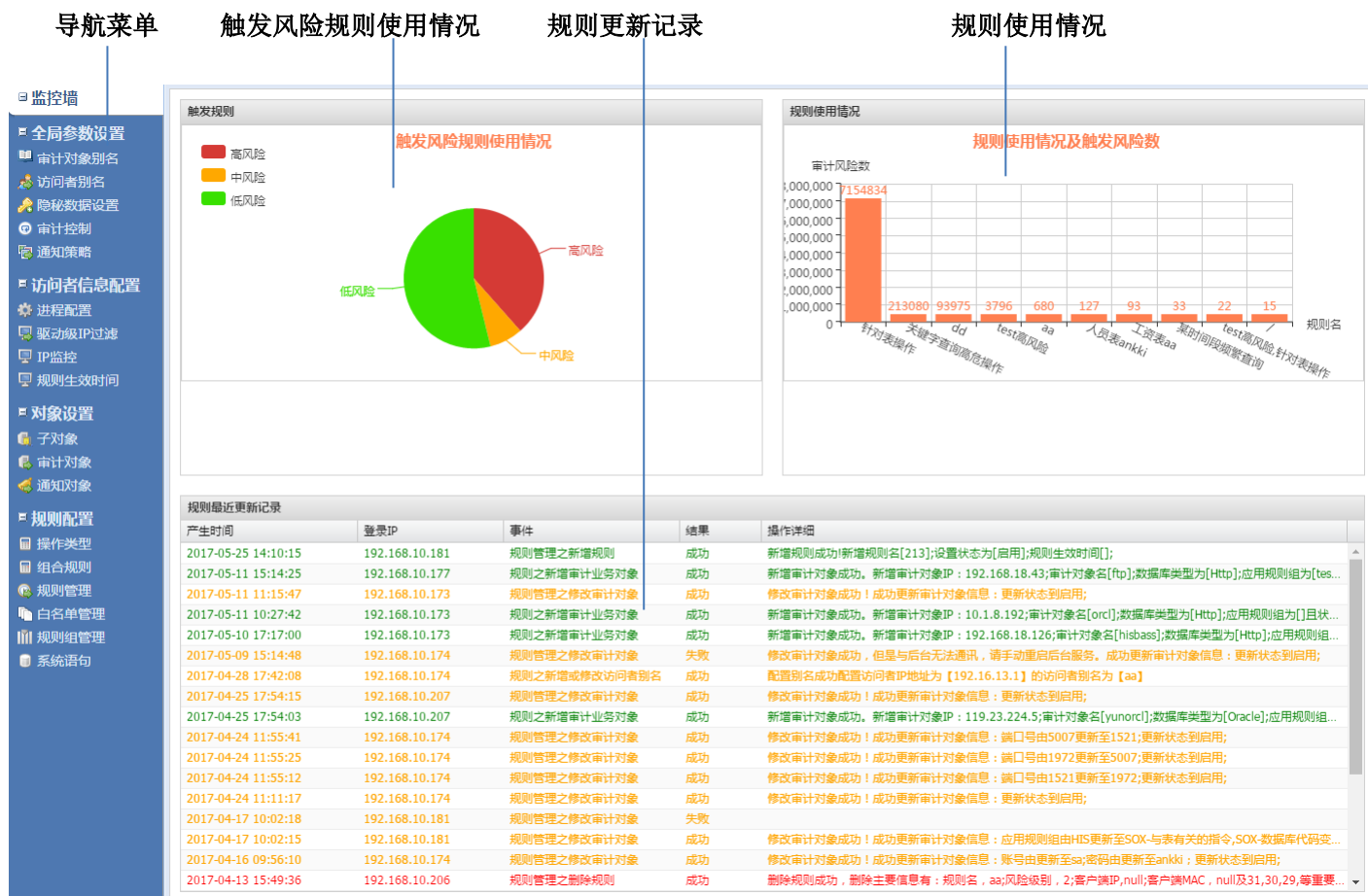


图 29 策略管理平台预览

说明:

| 名称 | 说明 |
|------------|---------------------------|
| 导航菜单 | 各功能模块及子菜单，详细信息请查看各功能模块描述。 |
| 规则使用情况 | 列出目前系统中已使用的规则数量及被触发的风险条数。 |
| 触发风险规则使用情况 | 已触发的规则条数统计。 |
| 规则最近更新记录 | 规则更新记录。 |

2、全局参数设置

2.1 审计对象别名

点击“全局参数设置”-“审计对象别名”，打开“审计对象别名”界面，点击“添加”，对审计对象的一些敏感的表、字段、关键字或客户端进程设置一个别名，系统可以进行翻译，设置关键字的目的是因为数据库语句中有些英文字符既不是表，也不是字段，这个时候如果要设置别名，就可以通过关键字来定义。

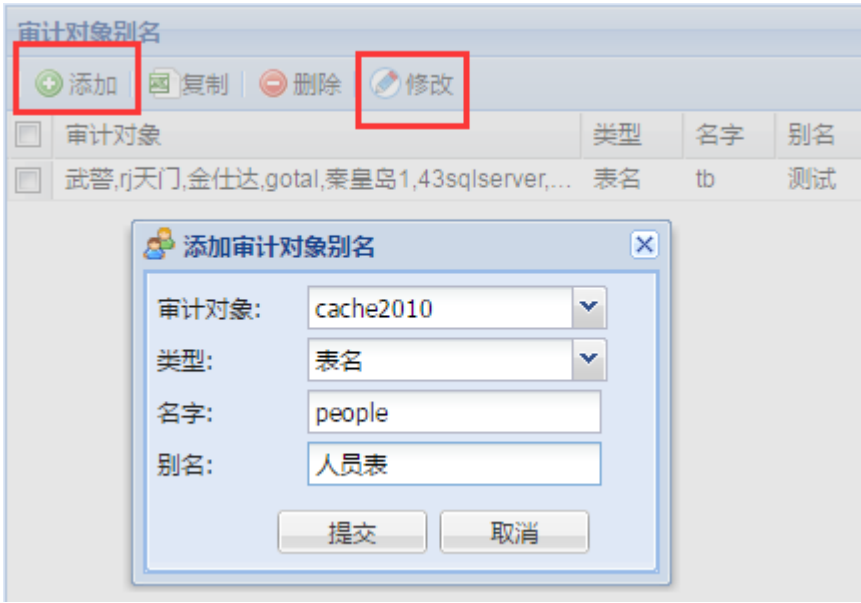


图 30 审计对象别名配置

针对表名、字段名和、关键字或客户端进程设置别名设置，也就是翻译，这里设置的别名会在风险查询和日常行为查询中出现相应的表名、字段名、关键字或客户端进程进行标注翻译之后的，方便识别和查看。

2.2 访问者别名

点击“全局参数设置”-“访问者别名”，打开“访问者别名”界面，访问者别名设置，将访问者的 IP 地址、MAC 地址、操作系统用户名、操作系统主机名、数据库账户、客户端进程翻译成别名，方便在审计结果中直观的看到是谁操作了数据库。



图 31 访问者别名配置

访问者别名管理是对客户端访问者设置别名，方便识别，设置某个 IP 的别名为 A，这样在审计结果中出现这个 IP 的将会显示别名 A。

2.3 隐秘数据设置

点击“全局参数设置”-“隐秘数据设置”，打开“隐秘数据设置”界面，

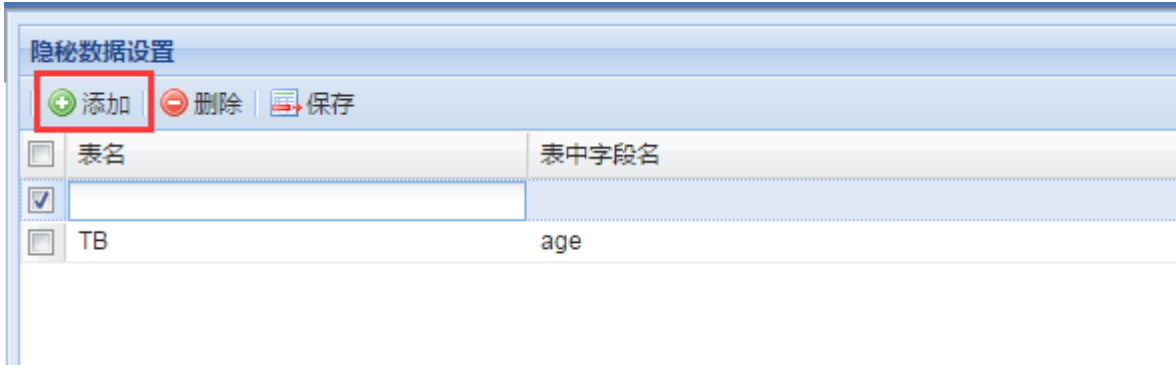


图 32 隐秘数据配置

对审计结果中的某些关键字段和敏感字段进行隐秘设置，防止二次泄密，这里设置之后，在审计结果中将会以加密星号（*）显示。

查询结果

详情

| 客户端IP | 服务端端口 | 数据库名 | 语句执行回应 | 发生时间 | 操作类型 |
|----------------|-------|------|--------|---------------------|------------|
| 192.168.10.207 | 1521 | orcl | 成功 | 2017-05-26 10:11:01 | select(查询) |
| 192.168.10.207 | 1521 | orcl | 成功 | 2017-05-26 10:11:01 | select(查询) |
| 192.168.10.207 | 1521 | orcl | 成功 | 2017-05-26 10:11:01 | select(查询) |
| 192.168.10.207 | 1521 | orcl | 成功 | 2017-05-26 10:11:01 | select(查询) |

客户端信息

服务端信息

操作语句

语句分析

客户端IP及端口：192.168.10.207:54066 发生时间：2017-05-26 10:11:01 操作系统主机名：魏晴
操作系统用户名：Administrator 源MAC地址：B0:F9:63:13:92:C0 客户端进程：plsqldev.exe 应用账户：/ 数据库账户：system

服务端IP及端口：192.168.18.43:1521 服务端MAC地址：00:E0:4C:F8:14:47

select * from tb where age=20;

全屏查看

对测试表中满足条件为：age等于20的所有数据进行了统计

操作发生在：2017-05-26 10:11:01,使用的电脑IP为:192.168.10.207,电脑物理地址（MAC地址）为：B0:F9:63:13:92:C0,电脑名称为：魏晴

| ID | NAME | SEX | AGE | JOB | DEPTNO | SAL | JOB1 | DEPTNO1 | SAL1 | JOB2 | DEPTNO2 | SAL2 | JOB3 | DEPTNO3 | SAL3 |
|----|------|-----|-------|-------|--------|-----|--------|---------|------|--------|---------|------|--------|---------|-------|
| 1 | deng | nan | ***** | ceshi | 20 | 100 | ceshi1 | 30 | 1000 | ceshi2 | 10000 | 1111 | ceshi3 | 10 | 10100 |
| 3 | den | nan | ***** | | | | | | | | | | | | |
| 4 | 等 | man | ***** | | | | | | | | | | | | |
| 5 | 等 | man | ***** | | | | | | | | | | | | |
| 6 | 等 | man | ***** | | | | | | | | | | | | |
| 7 | 等 | man | ***** | | | | | | | | | | | | |
| 8 | 等 | man | ***** | | | | | | | | | | | | |
| 9 | 等 | man | ***** | | | | | | | | | | | | |
| 10 | 等 | man | ***** | | | | | | | | | | | | |
| 11 | 等 | man | ***** | | | | | | | | | | | | |
| 12 | 等 | man | ***** | | | | | | | | | | | | |
| 13 | 等 | man | ***** | | | | | | | | | | | | |
| 14 | 等 | man | ***** | | | | | | | | | | | | |
| 15 | 等 | man | ***** | | | | | | | | | | | | |
| 16 | 等 | man | ***** | | | | | | | | | | | | |
| 17 | 等 | man | ***** | | | | | | | | | | | | |

图 33 隐秘数据实现效果

2.4 审计控制

点击“全局参数设置”-“审计控制”，打开“审计控制”，

审计控制

审计选项

控制选项: ☒ 全部审计 ☐ 按规则审计

最大返回结果长度 (字节): 30000

最长操作语句长度 (字符): 30000

保存 重置

零告警通知选项

零告警通知: ☒ 启用 ☐ 禁用

保存 重置

图 34 审计状态控制

该模块是进行“全部审计”还是进行“按规则审计”，以及返回结果长度，对审计的结果进行过滤。

两种审计状态：

全部审计：对所有的操作数据进行审计操作，并将所有操作数据进行保存；

按审计规则：只有满足审计规则的数据才会被审计到。

零告警通知：启用该功能后，每天早上 10 点（程序定义）发送一条告警短信到管理员手机中，让管理员知悉前一天的风险告警情况，有无告警系统都会发送。

2.5 通知策略

点击“全局参数设置”-“通知策略”，打开“添加”按钮

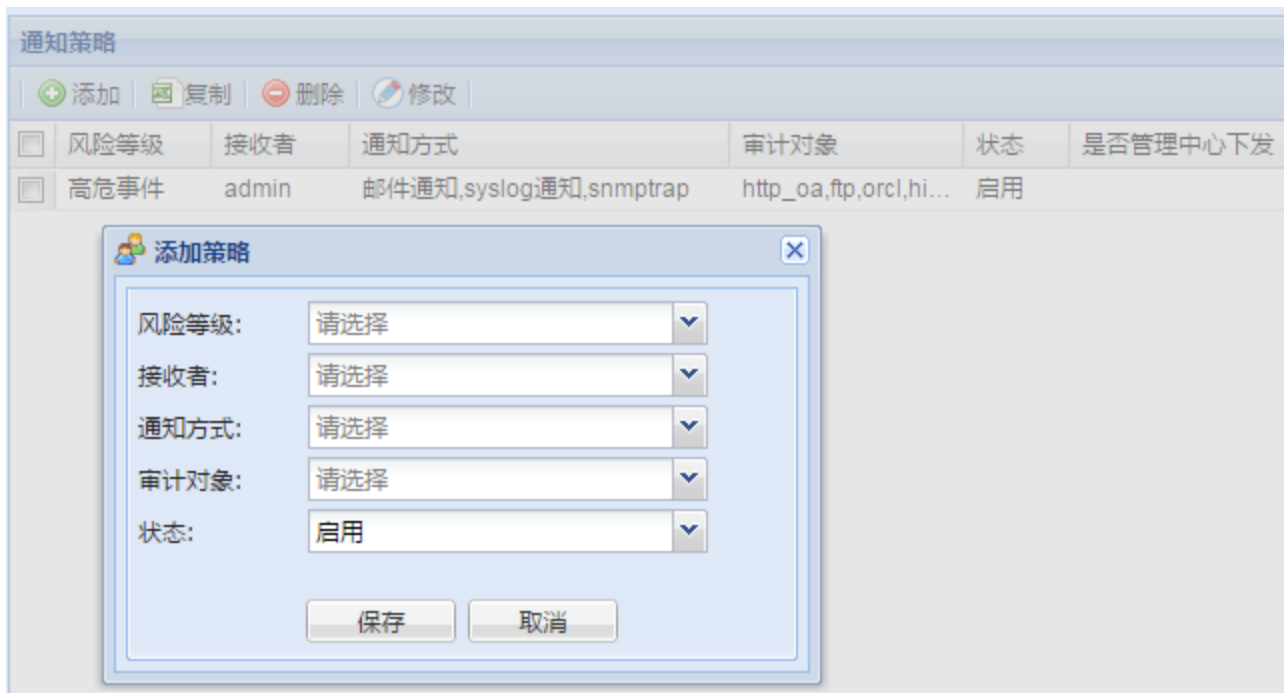


图 35 通知策略

“添加”选项：

| 名称 | 说明 |
|------|-----------------------------------|
| 风险等级 | 高危事件、中危事件、低危事件分别对应规则设置时的高、中、低。 |
| 接收者 | 在“审计管理平台-系统管理-用户管理”中的用户，或者其它新增的用户 |
| 通知方式 | 五种：邮件、syslog、SNMP、短信通知、短信平台。 |
| 审计对象 | 选择需要告警通知的审计对象，可多选。 |
| 状态 | 启用还是禁用。 |

3、访问者信息配置

对访问者的客户端进程、驱动级 IP 过滤，IP 监控和规则生效时间的设置。

3.1 进程配置

点击“访问者信息配置”-“进程配置”，打开“进程配置”界面，添加进程集合，进程集合名可以自定义，这里配置为“第三方工具”，然后点“客户端进程”的下拉选项，选择“plsqldev.exe”，最后点“添加”按钮。一个集合中可以添加多个进程。

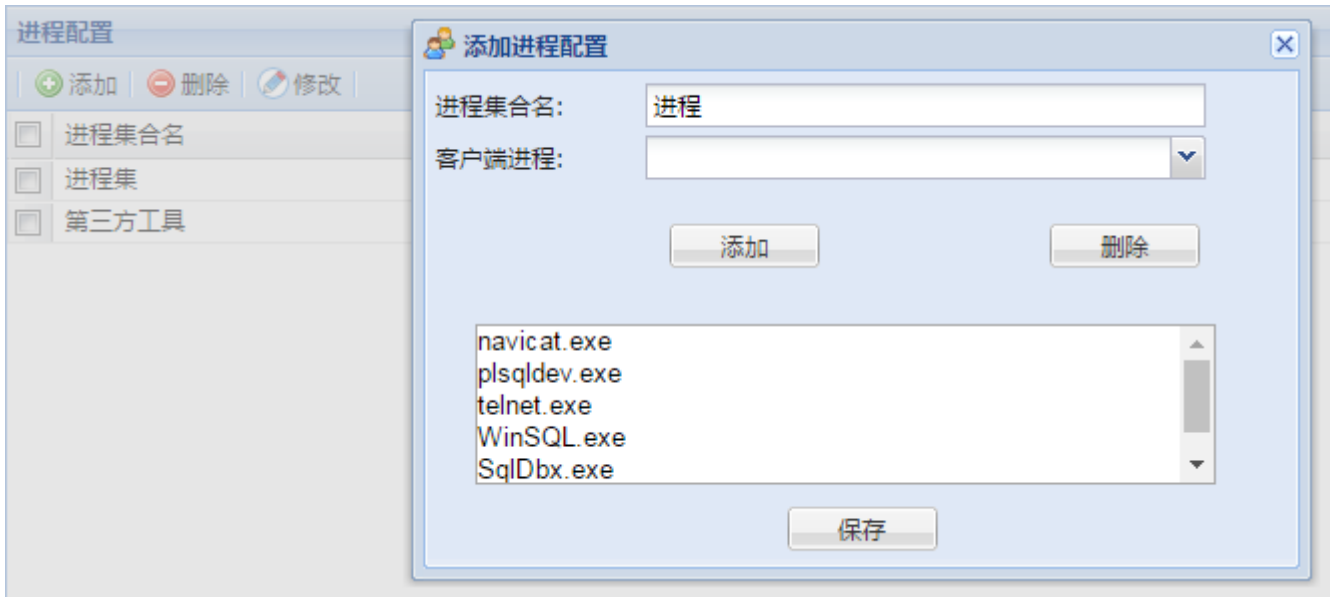


图 36 进程配置

配置相应的进程集合，可以对该进程集合添加到相应规则管理做处理。

3.2 驱动级 IP 过滤

点击“访问者信息配置”-“驱动级 IP 过滤”，打开“驱动级 IP 过滤”界面，

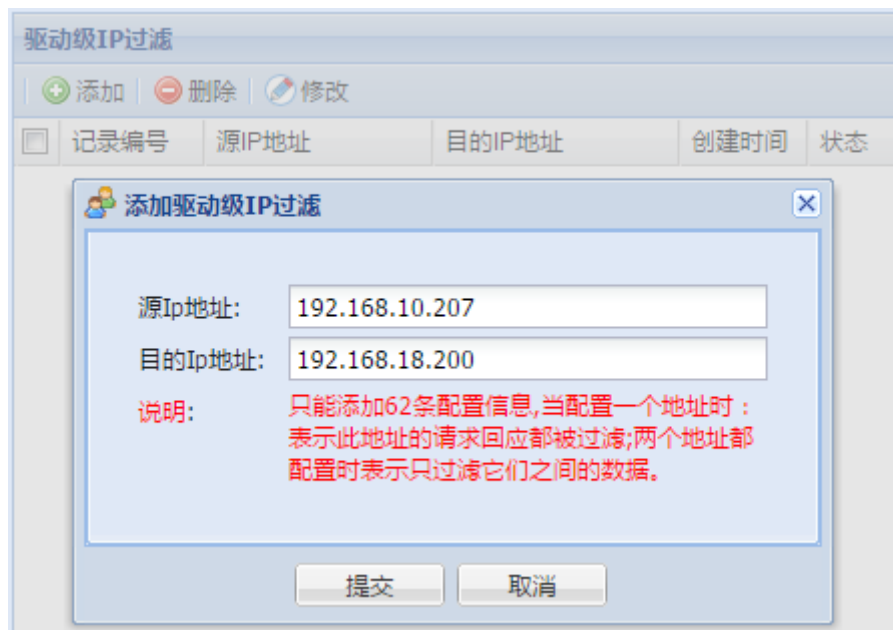


图 37 驱动级 IP 过滤信息

设置过滤某些 IP 后，将不对其 IP 产生的数据进行审计。

3.3 IP 监控

点击“访问者信息配置”-“IP 监控”，打开“IP 监控”配置界面（应用到规则管理，在审计控制中选择按规则审计，

就可以监控这个 IP 或 IP 段)，

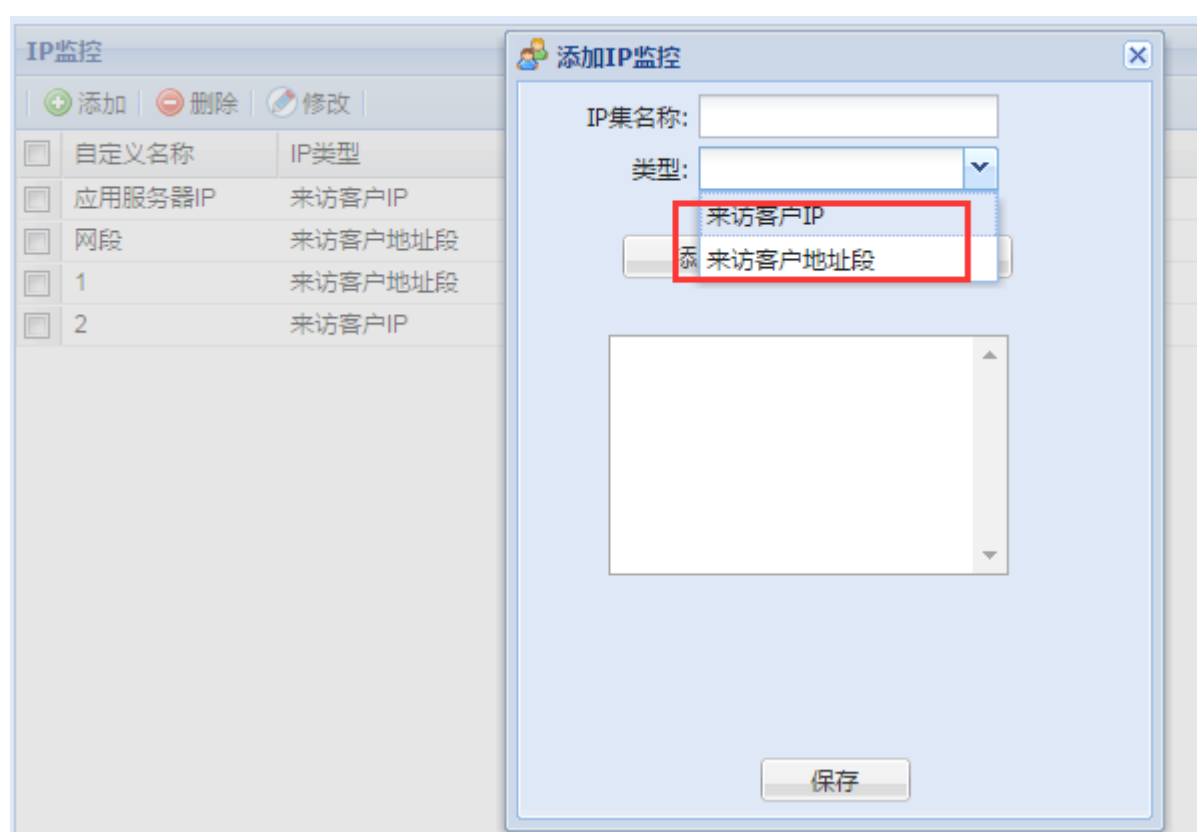


图 38 IP 监控信息配置

这部分功能是设置相应的客户端 IP 集合，将一些 IP 加入某个集合中，在设置规则时可以针对该集合配置规则。

先添加应用服务器 IP，选择“来访客户 IP”，输入应用服务器的 IP 地址“192.168.10.207”，点“添加”，再点“保存”；继续添加上面需求中提到的 IP 网段，1.1.1.1-192.168.10.206，类型选择“来访客户网段”，把起始 IP 和终止 IP 输入后，点击添加，保存即可。

关于类型的说明：

| 类型名称 | 说明 |
|---------|----------------------|
| 来访客户 IP | 客户端 IP |
| 来访客户地址段 | 客户地址段，配置起始 IP 和终止 IP |

3.4 规则生效时间

点击“访问者信息配置”-“规则生效时间”，打开“添加”配置界面，

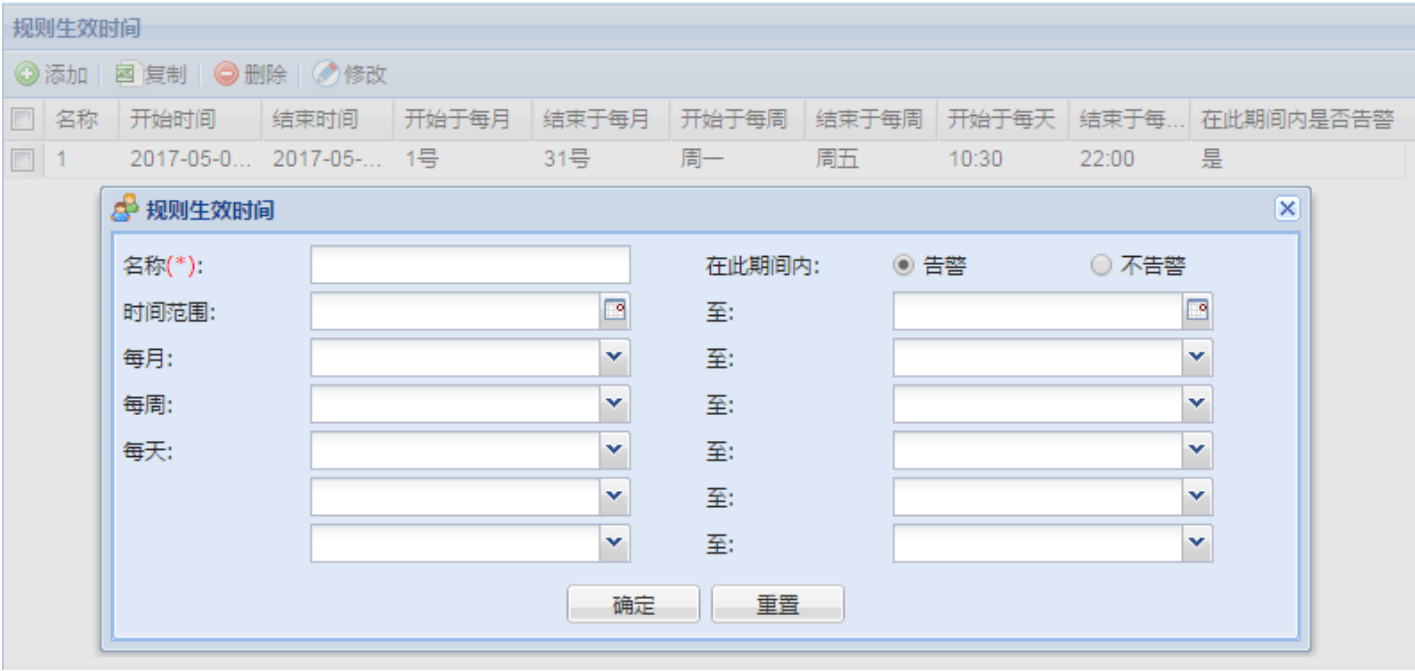


图 39 规则生效时间

此功能是定义规则生效时间，可以定义某个时间段内，规则处于告警或者不告警的状态。

4、对象设置

4.1 子对象

点击“对象设置”-“子对象”，打开“子对象”界面，根据需求中若多个表和多个字段，同时满足时告警，他们之间是与（&）的关系，可以在子对象中进行设置。多张表或字段用“&”符合隔开，点击保存即可，

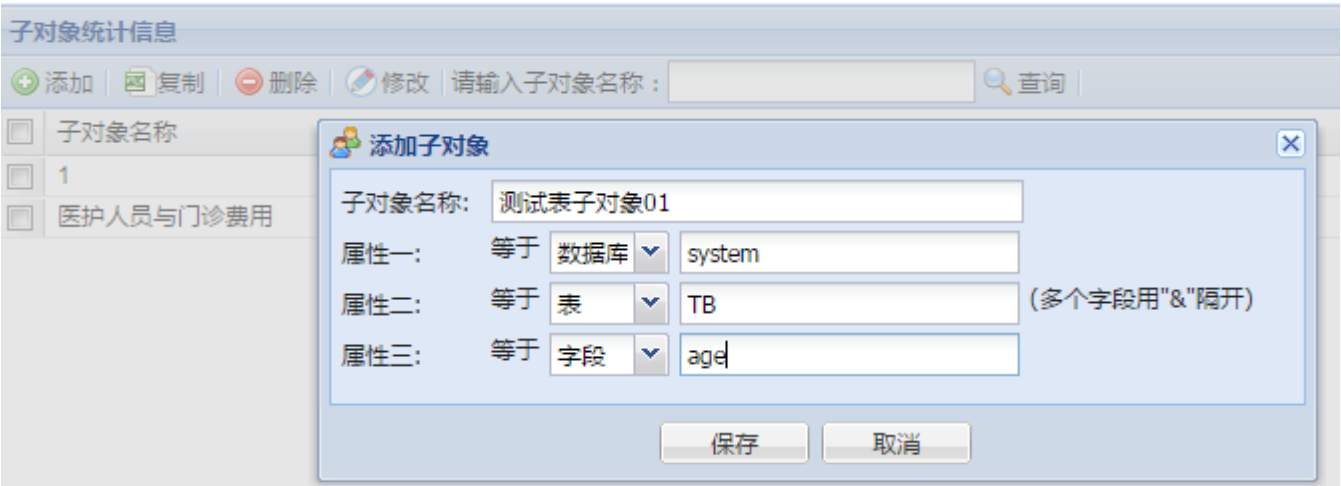


图 40 子对象配置界面

此项是设置规则的子对象名称，这里的子对象即为访问者的用户名或数据库名，即需要审计的数据库中的敏感表、包、函数、过程、视图、字段、索引等，其中包括以下内容：

| 名称 | 说明 |
|-----|---------------------|
| 属性一 | 包括数据库及用户名 |
| 属性二 | 包括数据库中的表、包、函数、过程、视图 |
| 属性三 | 包括数据库中的字段和索引 |

4.2 审计对象

点击“对象设置”-“审计对象”，打开“审计对象”配置界面，B008 版本合入的 HIS 有：杭创，键讯，金蝶慧通，用友，中联，阳光用药，天健，厦门智业，科进，中天，天网，方正，东华，总计 13 个。

注意：系统默认为东华 HIS，故配置审计对象时无需选择 HIS，选择相对应的数据库即可。

图 41 审计对象配置



注意：这里阻断 IP 要配合防火墙使用。

此项是配置要审计的对象即数据库的信息，包括以下内容：

| 名称 | 说明 |
|--------|---|
| 审计对象名称 | 设置业务对象的名称，可以自定义，建议设置的名称最好体现该对象的特点。 |
| 状态 | 禁用还是启用。 |
| 数据库类型 | 选择数据库类型，如 Oracle、Cache、SQL Server、Sybase 等等 |
| 版本号 | 选定数据库服务器类型后，这里选择数据库的版本号。 |
| 服务地址 | 数据库服务器所在的 IP 地址。 |
| 端口 | 数据库服务器设置的数据库的端口号，默认 SQL Server：1433； |

HTTP: 80; Oracle: 1521; MySQL: 3306。

| | |
|--------|---|
| 应用规则组 | 规则组设置，请参阅 5.5 规则组管理 |
| 数据库编码 | 根据数据库服务器数据库设置的编码字符集选择。 Oracle: GB2312; SQLServer: 936; 其他: UTF-8 |
| 应用部门 | 默认选择根部门。 |
| 关联对象 | 可将该审计对象与其他的审计对象进行关联。 |
| HIS 厂商 | 每个医院都会有一个 HIS 系统，用于管理医院信息。 |



注意：对于加密 SQL Server 数据库，需要在扩展配置中加入连接数据库的账号和用户名，这样有利于查看审计结果。

(1) 方正 HIS，键讯 HIS，天网 HIS 数据库类型选择中间件，端口号为 0

The screenshot shows the '添加审计对象' (Add Audit Object) dialog box. The following fields are highlighted with red boxes:

- 审计对象名: 东直门
- 数据库类型: 中间件
- 服务地址: 10.21.15.30
- 应用规则组: 关键字查询高危操作
- 应用部门: 根部门
- HIS厂商: 方正his
- 状态: 启用
- 版本号: 1.0
- 端口: 0
- 数据库编码: UTF-8
- 关联对象: (empty)

At the bottom, there is a checkbox for '扩展配置' (Advanced Configuration) and two buttons: '保存' (Save) and '重置' (Reset).

(2) 阳光用药数据库类型选择 portal, 端口号根据实际填写

The screenshot shows the '添加审计对象' (Add Audit Object) dialog box. The following fields are highlighted with red boxes:

- 审计对象名: 阳光用药
- 数据库类型: Portal
- 服务地址: 192.168.8.126
- 应用规则组: 关键字查询高危操作
- 应用部门: 根部门
- HIS厂商: 阳光用药
- 状态: 启用
- 版本号: Portal2010
- 端口: 80
- 数据库编码: UTF-8
- 关联对象: (empty)

At the bottom, there is a checkbox for '扩展配置' (Advanced Configuration) and two buttons: '保存' (Save) and '重置' (Reset).

(3) 中天 HIS 数据库类型选择 HTTP，端口号据实填写

The screenshot shows the '添加审计对象' (Add Audit Object) dialog box. The following fields are highlighted with red boxes:

- 审计对象名: 湘西州
- 数据库类型: Http
- 服务地址: 192.168.30.4
- 应用规则组: 关键字查询高危操作
- 应用部门: 根部门
- HIS厂商: 中天his
- 状态: 启用
- 版本号: Http
- 端口: 2001
- 数据库编码: UTF-8
- 关联对象: (empty)

At the bottom, there is a checkbox for '扩展配置' (Advanced Configuration) and two buttons: '保存' (Save) and '重置' (Reset).

(4) 其他 HIS 是什么数据库就选择对应的数据库类型及端口号，HIS 厂商即可
如天健 HIS，数据库类型选择 ORACLE，端口号 1521，HIS 厂商选择天健 HIS

The screenshot shows the '添加审计对象' (Add Audit Object) dialog box for Tianjian HIS. The following fields are highlighted with red boxes:

- 审计对象名: 长庆油田
- 数据库类型: Oracle
- 服务地址: 192.168.18.43
- 应用规则组: 关键字查询高危操作
- 应用部门: 根部门
- HIS厂商: 天健his
- 状态: 启用
- 版本号: Oracle 11g
- 端口: 1521
- 数据库编码: UTF-8
- 关联对象: (empty)

At the bottom, there is a checkbox for '扩展配置' (Advanced Configuration) and two buttons: '保存' (Save) and '重置' (Reset).

4.3 通知对象

点击“通知对象”-点击添加，添加后的通知对象可以运用到通知策略的接收者中

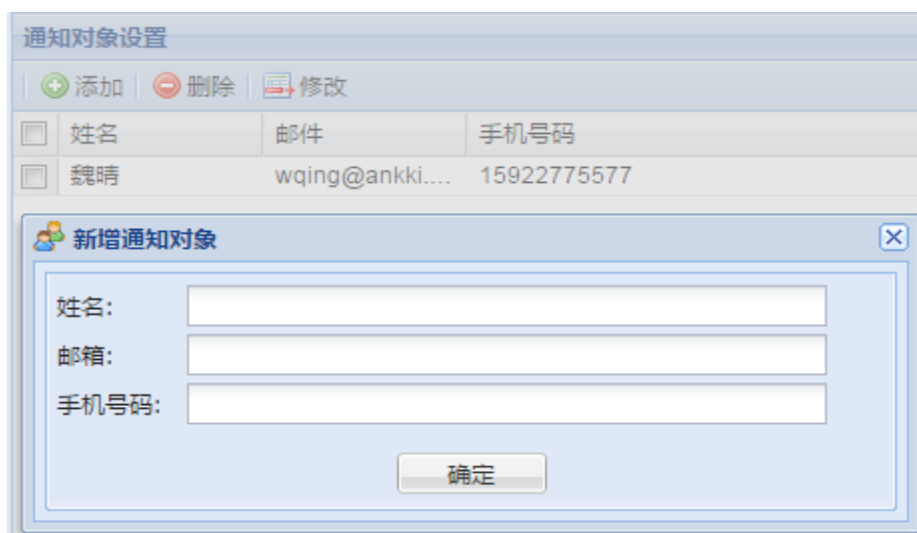
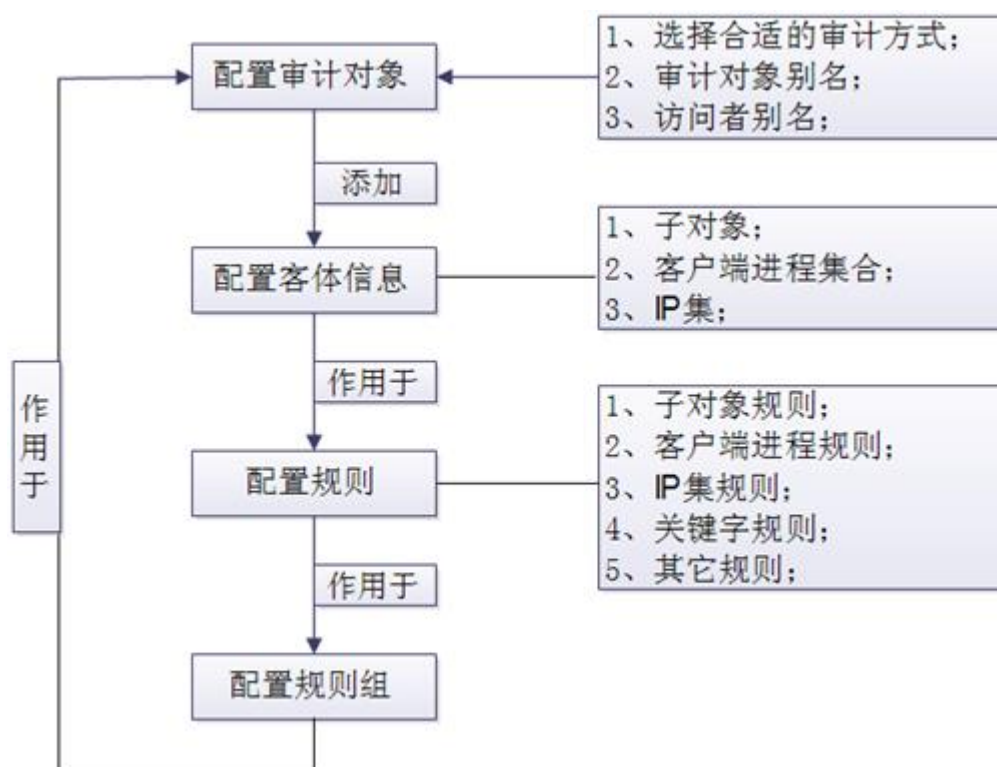


图 42 通知对象设置界面

此项是配置通知对象，可以将审计到的不同级别的风险发送给管理员，以便管理随时了解是否有人操作数据库。

5、规则配置

模块主要功能是规则管理和规则组管理。规则配置流程如图所示：



5.1 操作类型

点击“规则配置”-“操作类型”，打开“操作类型”界面（应用到规则管理）

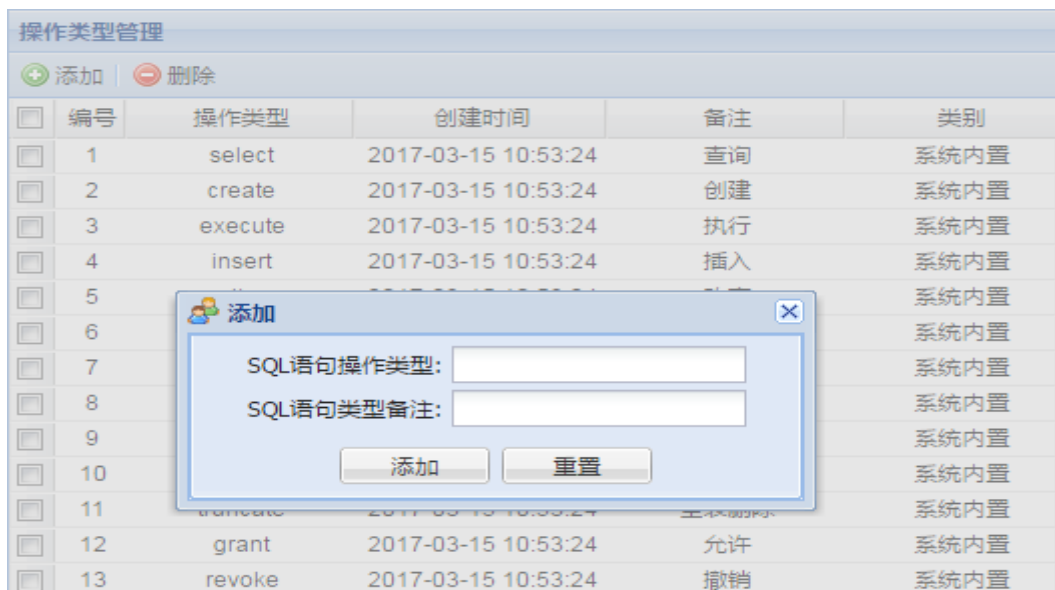


图 43 操作类型管理

此项是配置操作类型，有系统内置操作类型，用户也可以手动添加。

5.2 组合规则

点击“规则配置”-“组合规则”，打开“组合规则”界面，

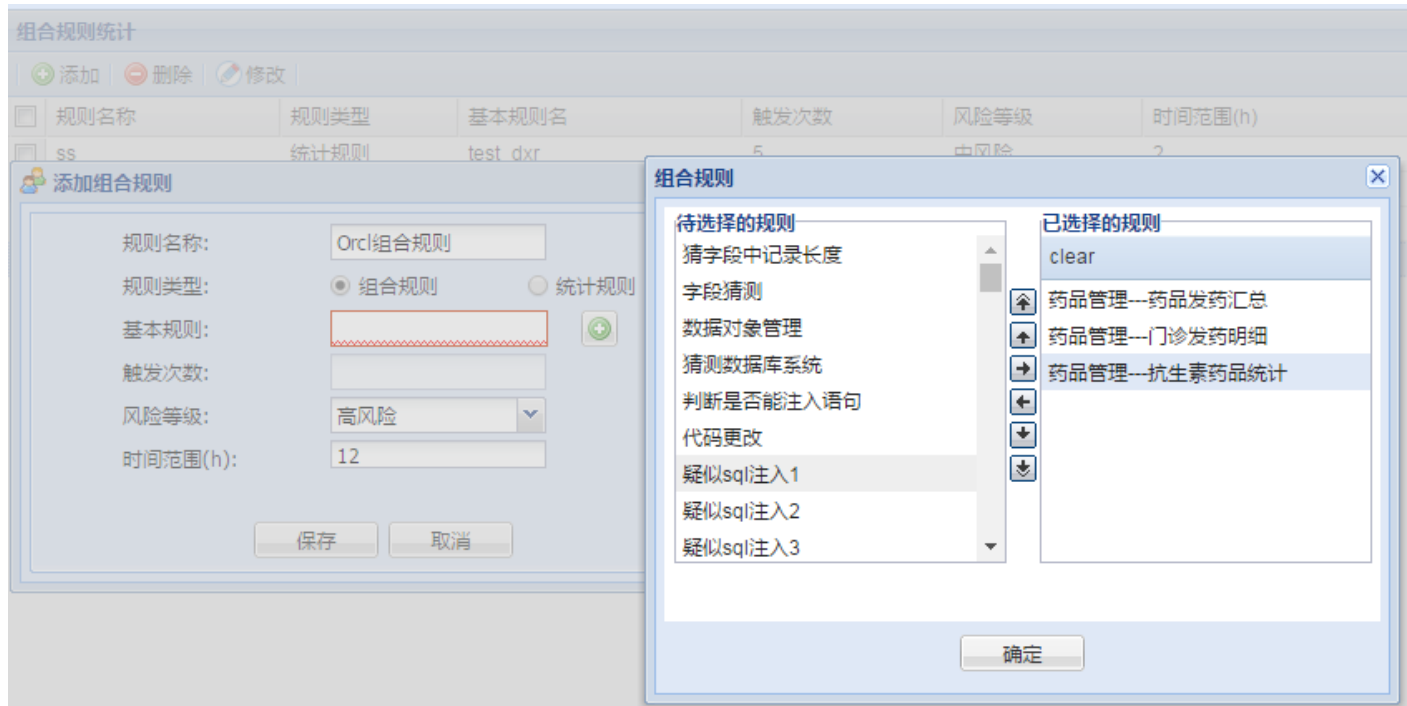


图 44 组合规则设置界面

此项是配置组合规则或统计规则。组合规则是根据几个规则在一定时间段内被触发是就会触发风险；统计规则是一定时间内一条规则达到触发的次数就会触发风险。

5.3 规则管理

点击“规则配置”-“规则管理”，打开“规则管理”界面，

规则列表

针对数据库的操作

规则属性设置

设置风险级别

规则管理

添加

复制

删除

修改

请输入规则名称：

查询

导入

导出

| 规则名称 | 规则级别 | 状态 | 更新时间 |
|----------|------|----|---------------------|
| 213 | 中风险 | 启用 | 2017-05-25 14:10:15 |
| test_dxr | 高风险 | 启用 | 2017-05-26 10:01:07 |

添加规则

基本配置

规则名(*):

操作类型:

关键字审计:

级别(*):

状态:

启用

高级配置

语句执行回应:

等于

进程集合名:

等于

子对象名:

请选择

客户端MAC:

等于

返回内容:

操作系统主机名:

等于

操作系统用户名:

等于

返回行数阈值:

语句执行时间(毫秒):

客户端IP集:

等于

请选择

来访客户网络:

等于

请选择

规则生效时间:

数据库账户:

等于

最大操作语句长度(字节):

大于

请输入数字

保存设置

重置

图 45 规则管理界面

此功能是设置规则，包括风险的级别、何种操作类型以及针对的对象（操作系统主机名、子对象、客户端 IP 集、客户端进程集、关键字等）。

针对数据库的操作：各种操作语句，例 select、insert、update 等，在审计结果中触发对应的操作时，出现告警。

风险级别：高风险、中风险、低风险、关注行为、一般行为、高级白名单。

规则属性内容：

| 名称 | 说明 |
|----------|---------------------------------|
| 操作系统主机名 | 客户端的操作系统主机名。 |
| 操作系统用户名 | 客户端的操作系统用户名。 |
| 客户端 MAC | 客户端的网卡地址。 |
| 子对象名 | 详细信息 4.1 子对象设置。 |
| 进程集合名 | 详细信息 3.1 进程配置。 |
| 客户端 IP 集 | 详细信息请参阅 3.3IP 监控配置中的来访客户 IP 配置。 |

| | |
|----------|---|
| 数据库账户 | 数据库服务器的账户 |
| 来访客户网络 | 详细信息请参阅 3.3IP 监控配置中的来访客户网段的配置。 |
| 最大操作语句长度 | 客户端的最大的操作语句长度，超过此值时，出现告警。 |
| 语句执行回应 | 客户端操作数据库的 SQL 语句的执行回应，结果为成功或失败。 |
| 返回内容 | 查询结果返回的行数大于该值时，将报警。 |
| 返回行数或阈值 | 设置一个返回结果的行数，当审计到的返回结果行数一致时出现报警。 |
| 语句执行时间 | SQL 语句中表的操作，当审计结果中执行时间大于该值时，出现告警。 |
| 规则生效时间 | 详细信息请参阅 3.4 规则生效时间配置。 |
| 关键字审计 | 关键字之间使用“&”和“ ”符号连接，分别表示“与”和“或”的关系，设置关键字后，在审计结果中出现对应的关键字时，会告警。 |

5.4 白名单管理

点击“规则配置”-“白名单管理”，打开“白名单管理”界面，

图 46 白名单管理

功能是将某个 IP、MAC 地址、疑似风险经确认正常的操作语句等加入白名单，在以后的审计中将不做审计，这样可以方便管理员对真正的风险的处理，提高工作效率。手动添加或者在审计结果中右键添加。

5.5 规则组管理

点击“规则配置”-“规则组管理”，打开“规则组管理”界面，

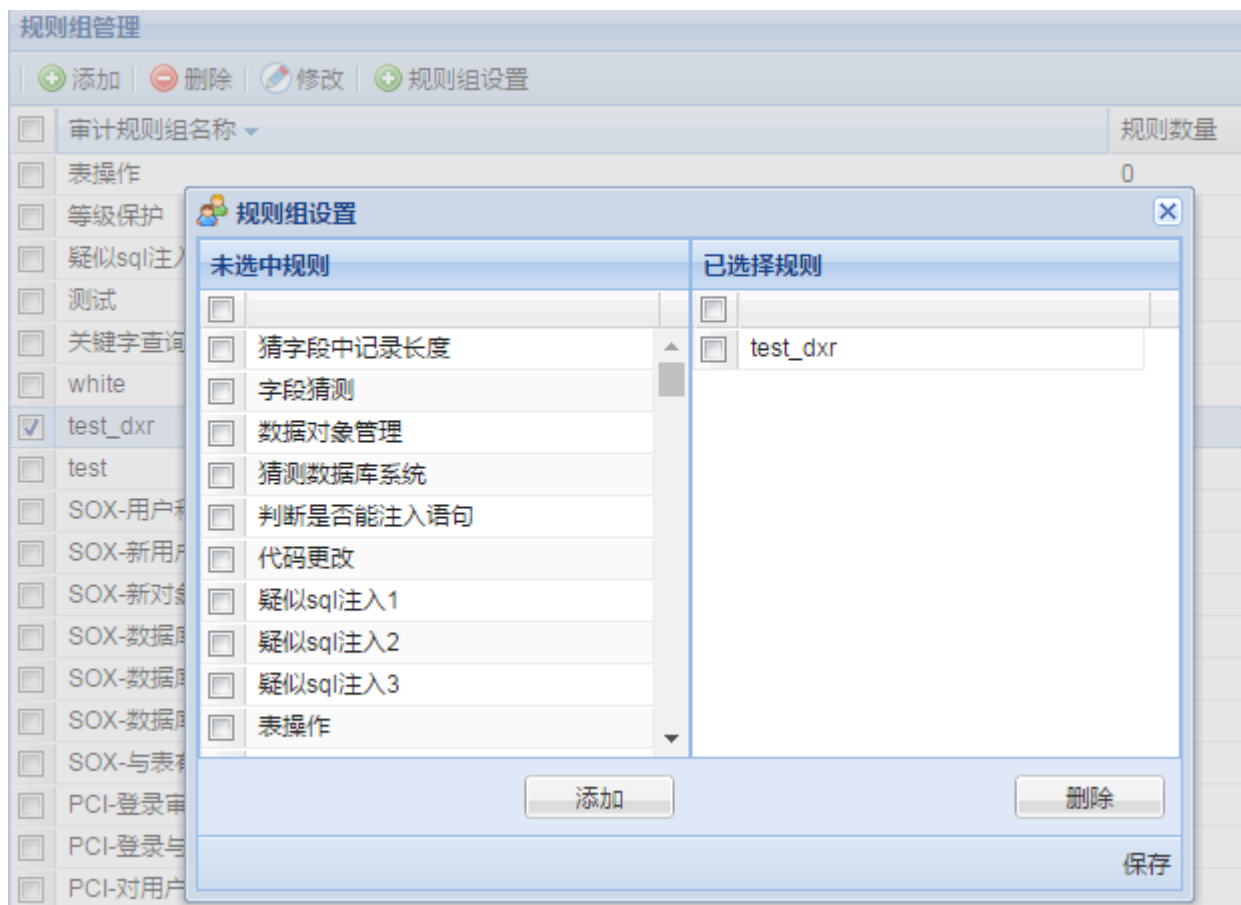


图 47 规则组管理

“规则组管理”是方便对规则的管理，可以将几个规则一起加入规则组，然后在“对象设置”-“审计对象”中加入该规则组，则规则启用。

5.6 系统语句

点击“规则配置”-“系统语句”，打开“系统语句”界面，

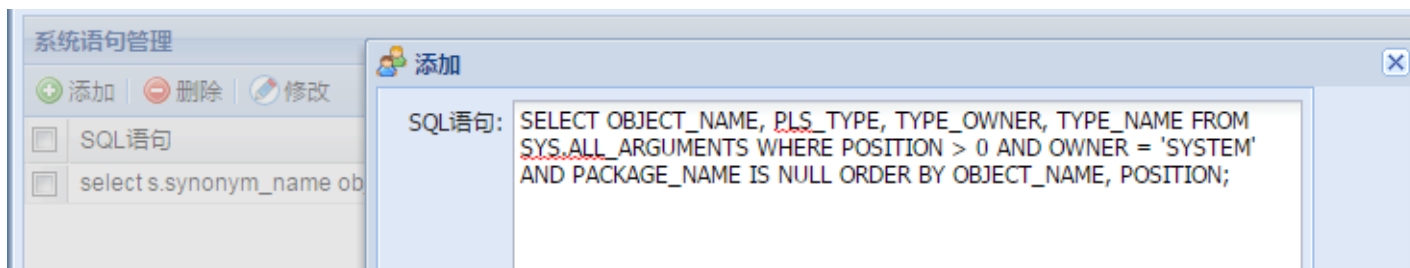


图 48 系统语句

“系统语句”是将确认正常的操作的 sql 语句标注为系统语句，在以后的审计中将不做审计，这样可以方便管理员对真正的风险的处理，提高工作效率。

三、审计管理平台

此平台主要是进行风险的查询和处理。

登录请参照第 3 页系统管理平台的登录。默认的审计管理员的用户名为 auditadmin，密码为 12345678。

1、审计管理平台预览

分为三大块，左边为导航菜单，中间部分为本月风险级别分布，右下角部分为最近系统事件。

其中，位于标题处的“告警事件统计”是当前系统中存在的未处理的风险数。



图 49 标题报警事件统计



图 50 消息提醒

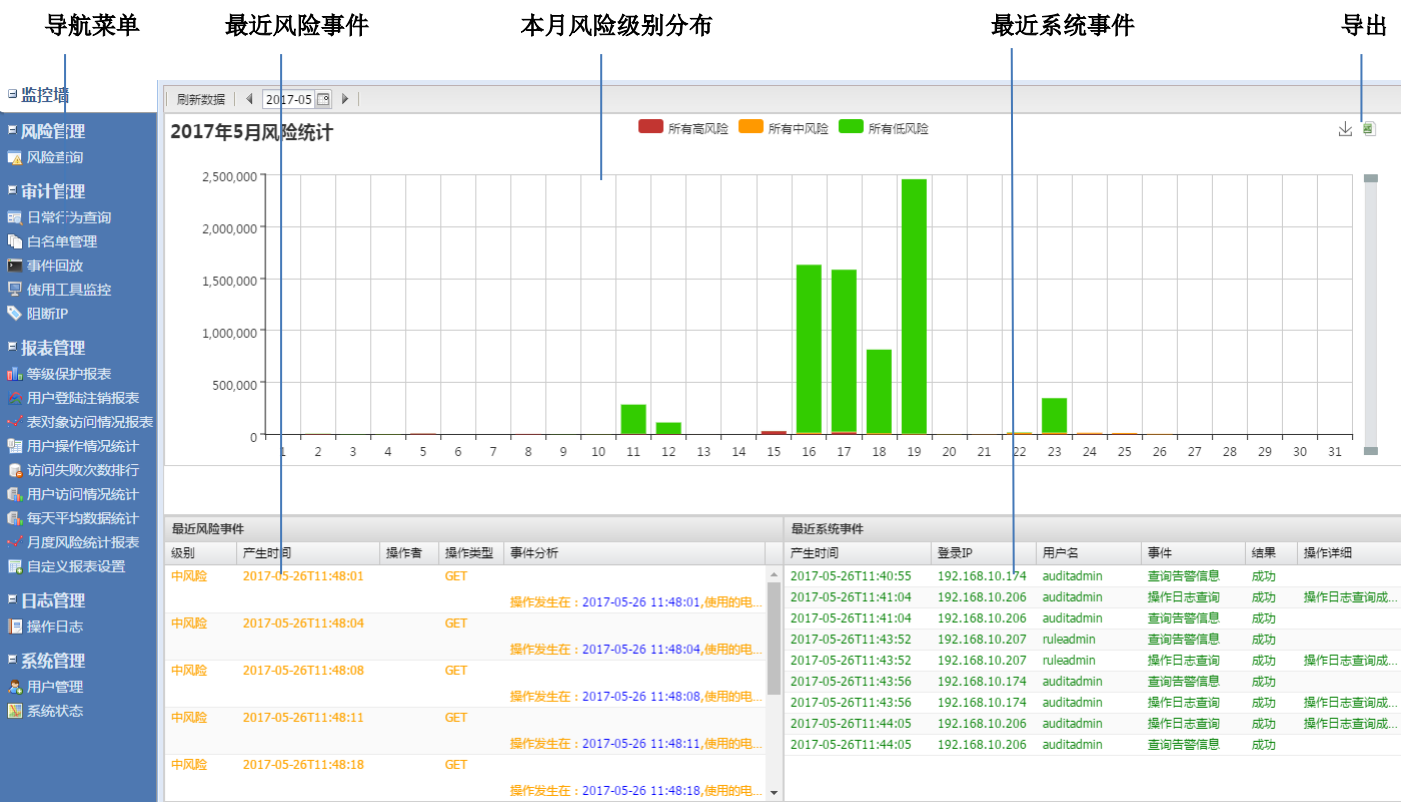


图 51 审计管理平台预览

点击柱形图，对当天产生的风险数据进行详细查看。

详细风险查询

开始日期: 2017-05-19 结束日期: 2017-05-19 IP地址: 搜索 导出数据 高风险: 399 | 中风险: 7466 | 低风险: 1701511

| IP地址 | 数据库账号 | 访问者 | 数据库名 | 访问对象 | 高风险 | 中风险 | 低风险 | 操作 |
|----------------|-------|-----|---------------------|----------|-----|------|-----|----|
| 192.168.10.174 | N/A | 邓筱莠 | orcl | orcel | 252 | 0 | 0 | 详细 |
| 192.168.10.184 | N/A | | ORCL | orcel | 147 | 0 | 0 | 详细 |
| 10.1.1.2 | / | | / | http_oa | 0 | 860 | 0 | 详细 |
| 192.168.10.184 | / | | / | http2 | 0 | 0 | 187 | 详细 |
| 192.168.10.173 | / | | / | http2 | 0 | 0 | 366 | 详细 |
| 192.168.10.164 | root | | / | 218mysql | 0 | 119 | 0 | 详细 |
| 192.168.10.164 | root | | mysql | 218mysql | 0 | 125 | 0 | 详细 |
| 192.168.10.171 | / | | / | http2 | 0 | 0 | 51 | 详细 |
| 192.168.10.176 | / | | / | http_oa | 0 | 879 | 0 | 详细 |
| 192.168.10.162 | root | | / | 218mysql | 0 | 157 | 0 | 详细 |
| 192.168.10.162 | root | | information_sche... | 218mysql | 0 | 6 | 0 | 详细 |
| 192.168.10.162 | root | | mysql | 218mysql | 0 | 63 | 0 | 详细 |
| 192.168.10.204 | / | | / | http_oa | 0 | 1666 | 0 | 详细 |
| 192.168.10.174 | / | 邓筱莠 | / | http2 | 0 | 0 | 152 | 详细 |

第 1 页, 共 3 页 显示 1 - 25 条, 共 68 条

关闭

图 52 详细风险查询

2、风险管理

模块功能主要是风险的查询和处理。

2.1 风险查询

点击“风险管理”-“风险查询”，打开“风险查询”界面，在基本配置中，可以根据查询条件进行风险查询。

基本配置

高级配置

审计查询结果现实的列

基本配置

高级配置

审计查询结果现实的列

基本配置

高级配置

审计查询结果现实的列

基本配置

高级配置

审计查询结果现实的列

图 53 风险查询界面

配置好查询条件，点击“查询”，打开“查询结果”界面，查询结果会打开一个新的页面，选择一条结果，下方会显示详细的信息，包括客户端信息、服务器端信息、操作语句、回应信息等

同时可以将查询结果“导出 word”、“导出 excel”、“导出 pdf”、文件导出。

查询结果

风险处理

报表导出菜单

文件导出

| | 客户端IP | 客户端... | 服务端... | 数据库名 | 数据库类... | 表名 | 字段名 | 操作语句 | 语句长度 | 语句执行... | 数据库账... | 应用账户 | 发生时间 | 操作类型 | 语句执行... | 访问者 | 处理状态 |
|----|------------|--------|--------|------|-------------|------|-----|---------------|-------|---------|---------|------|------------|-------------|------------|-----|------|
| 1 | 127.0.0.1 | 0 | 0 | / | / | / | / | 提示:eth... | | | | | 2017-05... | eth0管理... | 0ms | | 未处理 |
| 2 | 127.0.0.1 | 0 | 0 | / | / | / | / | 提示:eth... | | | | | 2017-05... | eth4审计... | 0ms | | 未处理 |
| 3 | 127.0.0.1 | 0 | 0 | / | / | / | / | 告警:eth... | | | | | 2017-05... | eth4审计... | 0ms | | 未处理 |
| 4 | 192.168... | 50101 | 1521 | orcl | Oracle 1... | dual | 'X' | select 'X'... | | | N/A | / | 2017-05... | select 查... | 0.85ms | | 未处理 |
| 5 | 192.168... | 50101 | 1521 | orcl | Oracle 1... | dual | 'X' | select 'X'... | | | N/A | / | 2017-05... | select 查... | 0.058ms | | 未处理 |
| 6 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | / | / | logout | 6字节 | 成功 | N/A | / | 2017-05... | logout登... | 1000.35... | | 未处理 |
| 7 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | dual | 'X' | select 'X'... | 21字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.197ms | | 未处理 |
| 8 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | dual | 'X' | select 'X'... | 21字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.058ms | | 未处理 |
| 9 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | / | / | select va... | 75字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.171ms | | 未处理 |
| 10 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | / | / | select va... | 75字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.058ms | | 未处理 |
| 11 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | / | / | select va... | 75字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.169ms | | 未处理 |
| 12 | 192.168... | 50061 | 1521 | orcl | Oracle 1... | / | / | select va... | 75字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.058ms | | 未处理 |
| 13 | 192.168... | 50101 | 1521 | orcl | Oracle 1... | / | / | begin if... | 126字节 | 成功 | N/A | / | 2017-05... | begin | 0.044ms | | 未处理 |
| 14 | 192.168... | 50101 | 1521 | orcl | Oracle 1... | kai | / | select *fr... | 17字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.166ms | | 未处理 |
| 15 | 192.168... | 50101 | 1521 | orcl | Oracle 1... | kai | / | select *fr... | 17字节 | 成功 | N/A | / | 2017-05... | select 查... | 0.058ms | | 未处理 |

客户端信息

服务器端信息

操作语句

客户端IP及端口 : 192.168.10.206:50061 发生时间 : 2017-05-26 11:23:41 操作系统主机名 : /

操作系统用户名 : / 源MAC地址 : B0:F9:63:13:92:C0 客户端进程 : plsqldev.exe 应用账户 : / 数据库账户 : N/A

服务器端IP及端口 : 192.168.18.200:1521 服务器端MAC地址 : 40:8D:5C:FA:B1:DA

logout

全屏查看

35

图 54 查询结果

选择一条记录，右键“事件分析”，弹出“事件分析”对话框，通过此对话框也可以查看

| 事件分析 | | | |
|---------|---|---------|---------|
| 风险级别： | 高风险 | 访问者： | N/A |
| 访问时间： | 2017-05-26 11:10:47 | 访问数据库： | orcel |
| 涉及关键表： | dual | | |
| 涉及关键字段： | 'x' | | |
| 语句执行结果： | 成功 | 语句执行时间： | 0.197ms |
| 满足规则： | 关键字查询高危操作 | 操作类型： | 查询 |
| 语句分析： | 对dual表中'x'进行了统计 操作发生在：2017-05-26 11:10:47,使用的电脑IP为:192.168.10.206,电脑物理地址 (MAC地址) 为：B0:F9:63:13:92:C0,电脑名称为：/ | | |
| 事件分析： | 对dual表中'x'进行了统计 操作发生在：2017-05-26 11:10:47,使用的电脑IP为:192.168.10.206,电脑物理地址 (MAC地址) 为：B0:F9:63:13:92:C0,电脑名称为：/ | | |
| 处理状态： | 未处理 | 处理人： | N/A |
| 行为状态： | 未处理 | 处理时间： | N/A |
| 处理描述： | 无 | | |

图 55 事件分析

会话开始>>>

[请求] 2017-03-15 11:21:24 > 告警: eth4 审计口被启用, 但是没插上网线

[回应] 2017-03-15 11:21:24 > success

[请求] 2017-03-15 11:23:12 > 提示:eth3审计口网线已连接 2017-03-15 11:23:12

[回应] 2017-03-15 11:23:12 > success

[请求] 2017-03-15 14:18:42 > 提示:eth1审计口网线已连接 2017-03-15 14:18:42

[回应] 2017-03-15 14:18:42 > success

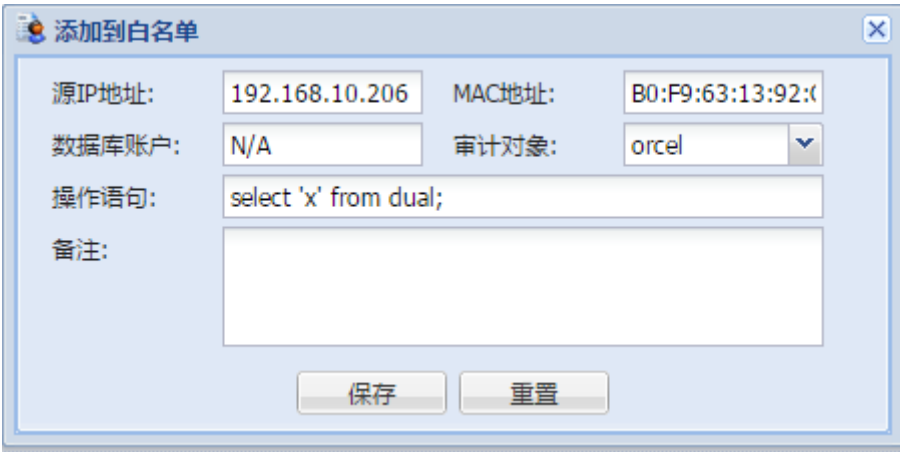
会话基本信息

客户端IP:默认回放所有IP记录

审计对象: /

请求次数:52

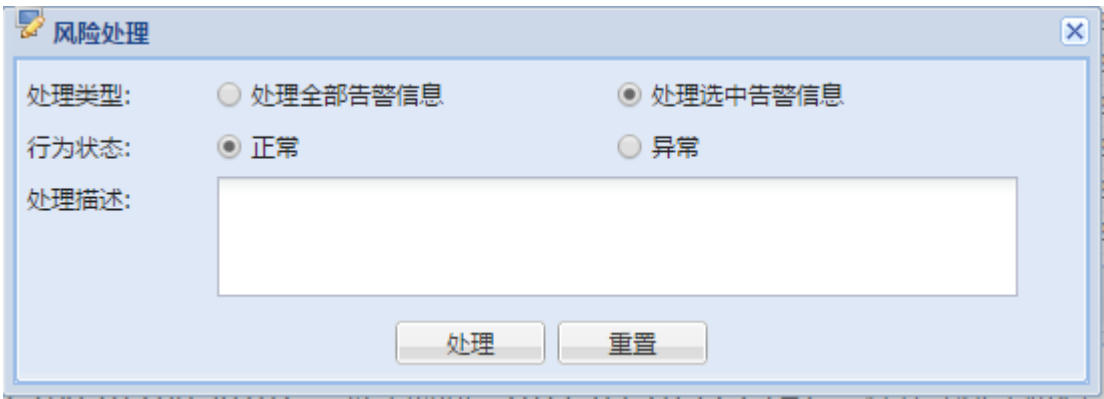
图 56 回放



The dialog box titled "添加到白名单" (Add to Whitelist) contains the following fields and controls:

- 源IP地址 (Source IP Address): 192.168.10.206
- MAC地址 (MAC Address): B0:F9:63:13:92:0
- 数据库账户 (Database Account): N/A
- 审计对象 (Audit Object): orcel (dropdown menu)
- 操作语句 (Operation Statement): select 'x' from dual;
- 备注 (Remarks): (empty text area)
- Buttons: 保存 (Save), 重置 (Reset)

图 57 添加到白名单



The dialog box titled "风险处理" (Risk Handling) contains the following fields and controls:

- 处理类型 (Handling Type):
 - ☐ 处理全部告警信息 (Handle all alert information)
 - ☒ 处理选中告警信息 (Handle selected alert information)
- 行为状态 (Behavior Status):
 - ☒ 正常 (Normal)
 - ☐ 异常 (Abnormal)
- 处理描述 (Handling Description): (empty text area)
- Buttons: 处理 (Handle), 重置 (Reset)

图 58 风险处理界面

3、审计管理

此模块功能是进行日常的查询、结果的回放以及客户端进程的统计信息。

3.1 日常行为查询

点击“审计管理”-“日常行为查询”，打开“日常行为查询”界面，

基本配置

审计对象:

时间选择:

最近五分钟

客户端IP:

等于

关键字一过滤:

等于

不计算总数:☒

勾选上之后可以增加查询的速度。

风险级别:

开始时间:

进程名:

关键字二过滤:

操作类型:

结束时间:

先选择时间，再选择日期

数据库账户:

等于

高级配置

操作系统主机名:

等于

返回行数:

等于

操作系统用户名:

等于

会话ID:

等于

语句执行时间(毫秒):

等于

客户端MAC:

等于

规则名:

等于

客户端端口号:

等于

语句长度(字节):

等于

记录编号:

等于

语句执行回应:

等于

数据库名:

等于

服务器端口:

等于

返回内容:

等于

规则组名:

审计查询结果显示的列

☒ 发生时间

☒ 客户端IP

☒ 服务端端口

☒ 操作类型

☒ 语句执行时间

☒ 语句执行回应

☒ 数据库名

☐ 数据库类型

☐ 表名

☐ 字段名

☐ 操作语句

☐ 语句长度

☐ 客户端端口

☐ 数据库账户

☐ 应用账户

☐ 进程名

☐ 服务端IP

☐ 规则名

☐ 风险级别

☐ 会话ID

☐ 记录编号

查询

重置

图 59 日常行为查询界面

详细信息请参照 2.1 风险查询。

3.2 白名单管理

同规则管理平台中的白名单管理。

3.3 事件回放

点击“审计管理”-“事件回放”，打开“事件回放”界面，

基本配置

审计对象:

时间选择:

自定义时间

客户端IP:

等于

关键字过滤:

等于

回放排序:

正排序

开始时间:

2017-05-26 14:51:32

进程名:

等于

操作类型:

结束时间:

2017-05-26 14:51:32

数据库账户:

等于

高级配置

操作系统主机名:

等于

规则名:

等于

客户端端口号:

等于

返回内容:

等于

客户端MAC:

等于

操作系统用户名:

等于

服务器端口号:

等于

语句执行时间(毫秒):

等于

语句执行回应:

等于

会话ID:

等于

语句长度(字节):

等于

回放

重置

图 60 事件回放界面



图 61 回放记录界面

结果回放是针对已发生的风险操作进行回放，展示详细的操作过程，方便之后的追溯和取证。

通过记录的回放，对于风险的详细操作过程展示给管理员。

3.4 使用工具监控

点击“审计管理”-“使用工具监控”，打开“使用工具监控”界面，可针对使用工具、使用某个工具的 IP 数以及某 IP 使用工具进行统计。

| 工具使用统计 | | |
|--|---------------------------|---------------------------|
| 时间选择: 本月 | 开始时间: 2017-05-01 00:00:00 | 结束时间: 2017-05-26 15:16:59 |
| 工具: enter search term | 开始统计 | |
| 使用工具 | 使用此工具的IP数 | 工具访问数据库次数 |
| ADMIT.exe | 1 | 1 |
| Apache-HttpClient/4.2.6 | 3 | 21 |
| CSTUDIO.EXE | 2 | 2082 |
| DavClnt | 1 | 3 |
| DesignRpt | 1 | 2 |
| DOCTOR.E | 1 | 4 |
| JDBC.exe | 4 | 1740 |
| Jetty/9.2.11.v20150529 | 7 | 36 |
| KK | 1 | 6 |
| Microsoft JDBC Driver for SQL Server | 1 | 1249 |
| Microsoft SQL Server Management Studio | 2 | 81 |
| Microsoft-WebDAV-MiniRedir/6.1.7601 | 1 | 1 |

图 62 使用工具监控界面

点击“审计管理”-“使用工具监控”，打开“使用某个工具的 IP 数统计”界面，可针对一个相应的数据库工具的使用 IP 数及 IP 的访问次数进行统计。

| 使用某个工具的IP数统计 | |
|---|--|
| 时间选择: 本月 | 开始时间: 2017-05-01 00:00:00 结束时间: 2017-05-26 15:16:59 工具: enter search term 开始统计 |
| 使用此工具的IP地址 工具访问数据库次数 | |
| 使用工具: ADMIT.exe (1 Item) | |
| 10.180.51.78 | 1 |
| 使用工具: Apache-HttpClient/4.2.6 (3 Items) | |
| 10.1.8.83 | 10 |
| 10.1.8.84 | 9 |
| 10.1.8.97 | 2 |
| 使用工具: CSTUDIO.EXE (2 Items) | |
| 192.168.10.174 | 726 |
| 192.168.10.207 | 1356 |

图 63 使用某个工具的 IP 数统计界面

点击“审计管理”-“使用工具监控”，打开“某个 IP 使用的工具统计”界面，可针对一个相应的 IP 地址所使用的数据库工具及访问数据库次数进行统计。

| 某个IP使用工具统计 | |
|--------------------------|--|
| 时间选择: 本月 | 开始时间: 2017-05-01 00:00:00 结束时间: 2017-05-26 15:16:59 IP地址: 开始统计 |
| 使用工具 工具访问数据库次数 | |
| IP地址: 10.1.1.2 (2 Items) | |
| Mozilla/5.0 | 1222 |
| Shockwave Flash | 2 |
| IP地址: 10.1.1.3 (1 Item) | |
| Mozilla/5.0 | 388 |
| IP地址: 10.1.1.4 (1 Item) | |
| Mozilla/5.0 | 526 |
| IP地址: 10.1.1.5 (1 Item) | |
| Mozilla/5.0 | 143 |
| IP地址: 10.1.1.6 (1 Item) | |
| Mozilla/5.0 | 102 |

图 64 某个 IP 使用的工具统计界面



注意：这里的需要选择一个时间段，然后系统会收集统计改时间段内的详细情况。

3.5 阻断 IP

点击“审计管理”-“阻断 IP”，打开“阻断 IP”界面，选择一条记录点击“释放所选记录”，便可删除这条阻断 IP 记录。

| + 释放所选记录 | | | | | | | |
|-------------------------------------|----------------|----------------|-------------------|--------|-----|------|---------------------|
| | IP | AgentIP | MAC | 用户名 | 合法性 | 处理状态 | 产生时间 |
| <input type="checkbox"/> | 192.168.10.169 | 0.0.0.0 | B0:F9:63:13:92:C0 | / | 非法 | 未处理 | 2017-03-15 11:29:54 |
| <input type="checkbox"/> | 192.168.10.177 | 0.0.0.0 | B0:F9:63:13:92:C0 | / | 非法 | 未处理 | 2017-03-15 15:44:59 |
| <input checked="" type="checkbox"/> | 192.168.10.207 | 192.168.18.238 | B0:F9:63:13:92:C0 | system | 非法 | 未处理 | 2017-05-25 14:53:28 |

图 65 阻断 IP 界面



注意：这里阻断 IP 要配合防火墙使用，在审计对象中 agent 状态设置为启用。

4、报表管理

报表管理是对审计结果进行分类统计，并以图形和图标的方式展示给管理员，便于管理员查看；同时可以将报表“导出 word”、“导出 excel”、“导出 pdf”。

4.1 等级保护报表

以柱形图的方式将“数据库账户/访问次数”展示出来，并在下方显示详细的信息，包括数据库账户、数据库名、操作类型、结果、操作次数。



图 66 等级保护报表

4.2 用户登录注销报表

以柱形图的方式将“数据库账户/用户登录注销次数”展示出来，而在下方会显示数据库账户、访问者 IP、数据库名、操作类型、结果、操作次数等详细信息。



图 67 用户登录注销报表

4.3 表对象访问情况报表

对某 IP 在一段时间内对数据库中哪些表进行了哪些操作，以及操作了多少次，以柱形图的形式展现出了。



图 68 表对象访问情况报表

4.4 用户操作情况统计

这里是使用某个数据库账户操作次数，详细信息以柱形图的形式展示出来。



图 69 用户情况操作统计

4.5 访问失败次数排行

对使用数据库账户访问数据库，并且是失败的情况进行汇总。



图 70 访问失败次数排行

4.6 用户访问情况统计

对于客户端（IP）访问数据库的次数进行统计分析。



图 71 用户访问情况统计

4.7 每天平均数据统计

对审计对象在当天访问数据库产生数据的级别和次数进行统计。

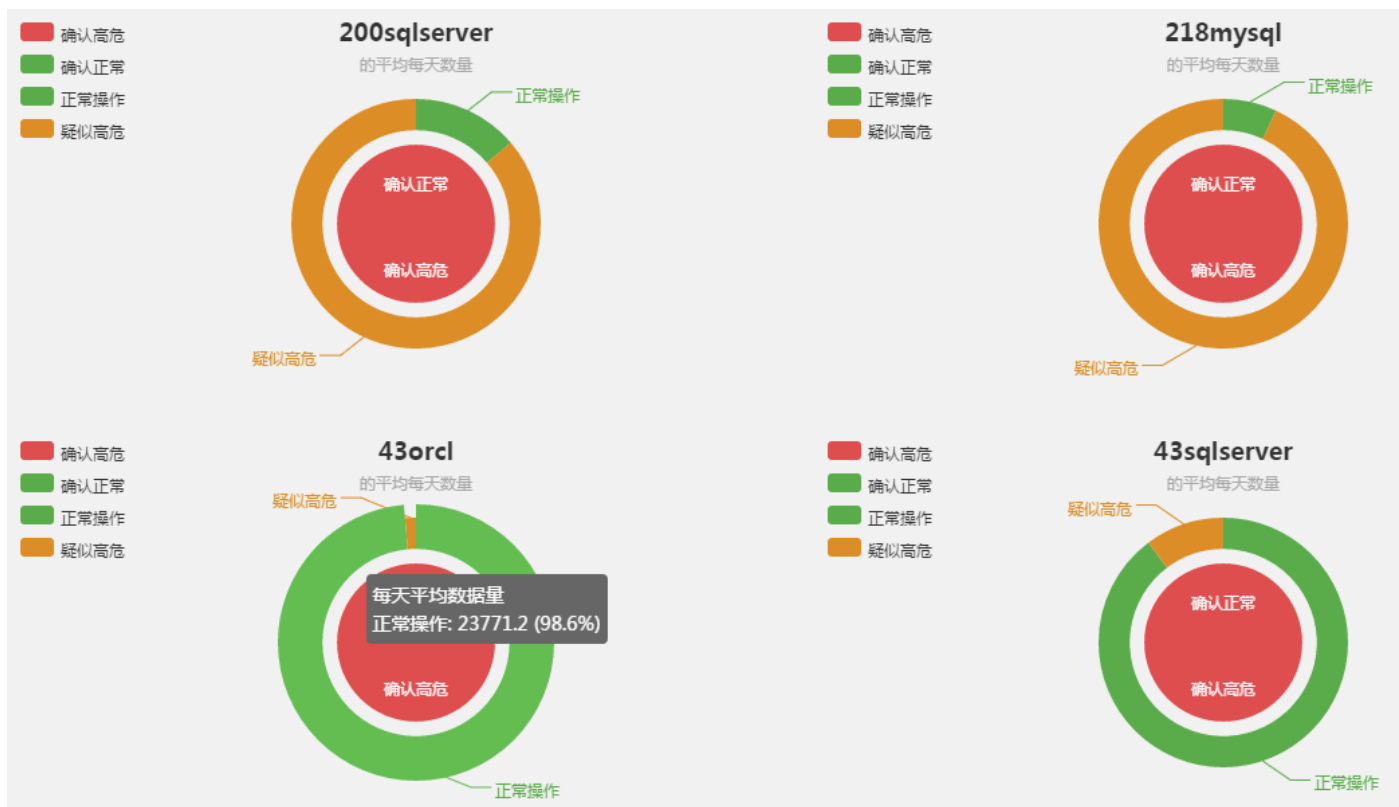


图 72 每天平均数据统计

4.8 月度风险统计报表

查询当月高风险数以及高风险占有所有风险的比例和返回行数大于 50 以及所占的比例，并在报表中详细显示。



图 73 每天平均数据统计

4.9 自定义报表设置

用户可以根据自己需求，自定义字段，显示想要看到的报表。

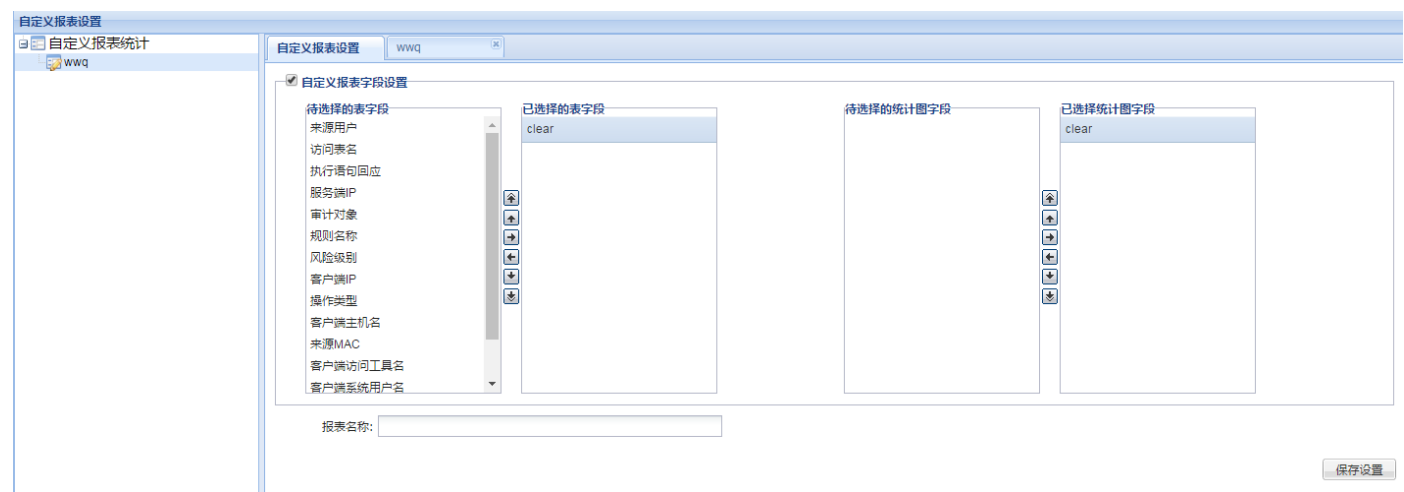


图 74 自定义报表设置

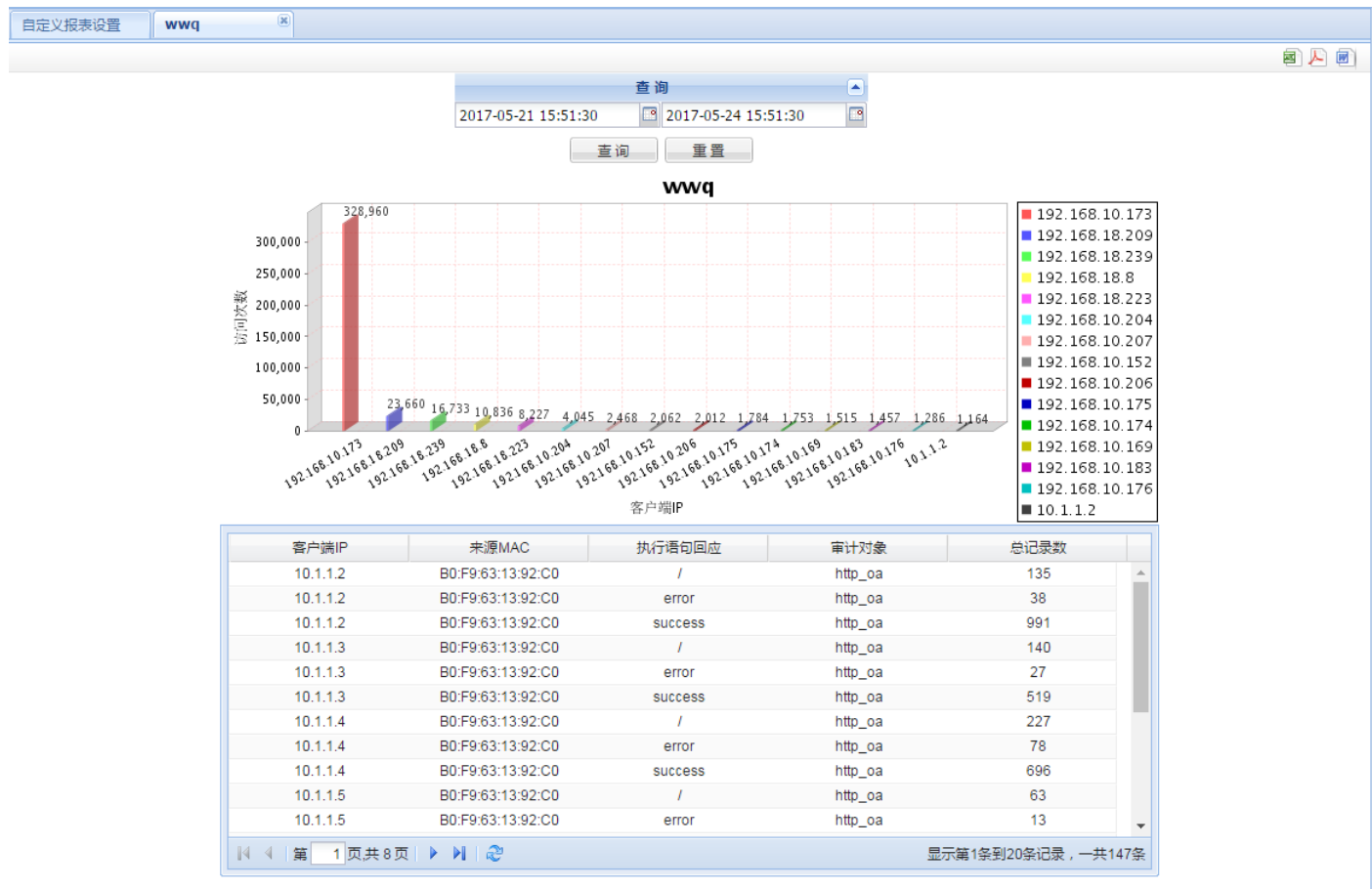


图 75 自定义报表

根部门用户权限介绍——在根部门下创建用户可以指定用户角色（系统管理员、规则管理员、审计管理员），默认能查看所有审计对象的规则配置、审计结果等信息；

子部门用户权限介绍——在根部门下添加子部门后，并在子部门内添加用户，该用户仅能查看本部门配置的审计对象的审计信息，用户角色仅能设置为审计管理员。

6.2 系统状态

系统情况查看，详细信息可以参照第 3 页系统管理平台中的“系统管理员平台整体预览”。