

创宇智图数据库审计与防护系统

用户使用手册

2021-05-12

北京知道创宇信息技术股份有限公司

更好更安全的互联网

文档控制

|  |  |
| --- | --- |
| 文档名称 | 创宇智图数据库审计与防护系统用户使用手册 |
| 保密级别 | 内部公开 |
| 拟制 |  |
| 审核 |  |
| 标准化 |  |

版本控制

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 提交日期 | 相关组织和人员 | 版本描述 |
| V1.0 | 2021-05-12 | 辛宇 | 创建 |
|  |  |  |  |

**目 录**

[1 登录与修改密码 4](#_Toc71884728)

[1.1 登录 4](#_Toc71884729)

[1.2 修改密码 4](#_Toc71884730)

[2 首页 5](#_Toc71884731)

[2.1 概览 5](#_Toc71884732)

[2.2 状态监控 6](#_Toc71884733)

[3 审计 8](#_Toc71884734)

[3.1 告警 8](#_Toc71884735)

[3.2 检索 12](#_Toc71884736)

[3.3 会话 14](#_Toc71884737)

[3.4 审计设置 16](#_Toc71884738)

[3.4.1 告警发送 16](#_Toc71884739)

[3.4.2 告警发送查询 21](#_Toc71884740)

[4 分析 21](#_Toc71884741)

[4.1 多维分析 21](#_Toc71884742)

[4.2 用户行为分析 22](#_Toc71884743)

[5 报表 23](#_Toc71884744)

[5.1 预定义报表 23](#_Toc71884745)

[5.2 自定义报表 25](#_Toc71884746)

[5.3 我的报表 26](#_Toc71884747)

[5.4 定时报表 27](#_Toc71884748)

[5.5 报表生成 27](#_Toc71884749)

[6 策略 28](#_Toc71884750)

[6.1 白名单 28](#_Toc71884751)

[6.2 黑名单 31](#_Toc71884752)

[6.3 自定义规则 33](#_Toc71884753)

[6.4 智能告警 36](#_Toc71884754)

[6.4.1 智能告警设置 36](#_Toc71884755)

[6.4.2 用户行为模型 37](#_Toc71884756)

[6.5 SQL注入特征库 39](#_Toc71884757)

[6.6 审计过滤 40](#_Toc71884758)

[6.6.1 IP限制 40](#_Toc71884759)

[6.6.2 数据过滤 42](#_Toc71884760)

[6.7 策略设置 42](#_Toc71884761)

[7 资产 43](#_Toc71884762)

[8 系统 46](#_Toc71884763)

[8.1 基础设置 46](#_Toc71884764)

[8.2 网卡设置 46](#_Toc71884765)

[8.3 插件设置 49](#_Toc71884766)

[8.3.1 插件安装 49](#_Toc71884767)

[8.3.2 插件管理 51](#_Toc71884768)

[8.4 用户管理 52](#_Toc71884769)

[8.4.1 账号管理 52](#_Toc71884770)

[8.4.2 角色管理 54](#_Toc71884771)

[8.4.3 账号审核 55](#_Toc71884772)

[8.5 安全配置 56](#_Toc71884773)

[8.6 系统维护 57](#_Toc71884774)

[8.7 系统授权 58](#_Toc71884775)

[8.8 操作审计 58](#_Toc71884776)

[8.9 备份恢复 59](#_Toc71884777)

[8.9.1 审计日志 59](#_Toc71884778)

[8.9.2 配置数据 62](#_Toc71884779)

[8.10 数据清理 64](#_Toc71884780)

# 登录与修改密码

## 登录

在浏览器中输入“https://管理IP:8441”登录创宇智图数据库审计与防护系统，输入出厂用户名和密码，如图1-1-1所示。



图1-1-1 系统登录

说明

IP地址根据实际情况修改，实际用户名密码请咨询厂家实施人员。

设备默认出厂IP：192.168.0.254，出厂用户名/密码：admin/Admin@123。

浏览器：Chrome、火狐等主流浏览器。

## 修改密码

单击<登录>，进入修改密码界面。首次登陆，为了安全需要修改出厂密码。在图1-2-1中输入原密码、新密码、确认密码，单击<确定>后回到登录界面，使用新密码进行登录。

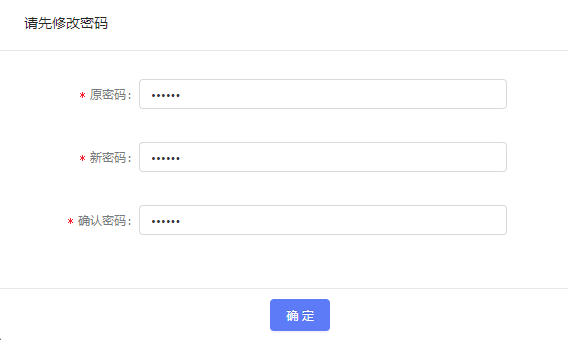


图1-2-1修改密码

# 首页

在首页中可以查看整体或单个数据库的审计统计。

## 概览

单击[首页->概览]后，如图2-1-1和图2-1-2所示，选择资产组或者单一资产，从不同视角查看资产概况、审计信息统计、数据库性能、数据风险分析、用户模型分析和动态告警。

* 资产总数：审计保护的资产总个数。
* 关系型数据库：审计保护的关系型数据库个数。
* 大数据： 审计保护的大数据模块个数。
* 数据请求数：所选数据库近7天的数据请求数统计。
* 告警数：所选数据库近7天的告警数统计。
* 数据库性能：显示按平均时长统计的TOP3数据库，统计的是今天之前的数据。
* 风险评分：随机选取5个资产进行统计，鼠标移动到风险评分图标上则悬浮显示减分项。
* 风险分布：显示所选数据库不同风险类型的告警风险分布统计。
* 风险趋势：显示近1小时、近24小时、近7天统计所选数据库的风险趋势。
* 用户模型分析：统计的资产和风险评分的资产一直，从数据库账号、客户端IP、客户端APP操作命令和操作对象五个方面进行用户模型分析统计。
* 动态告警：动态显示最新的20条告警，循环播放。

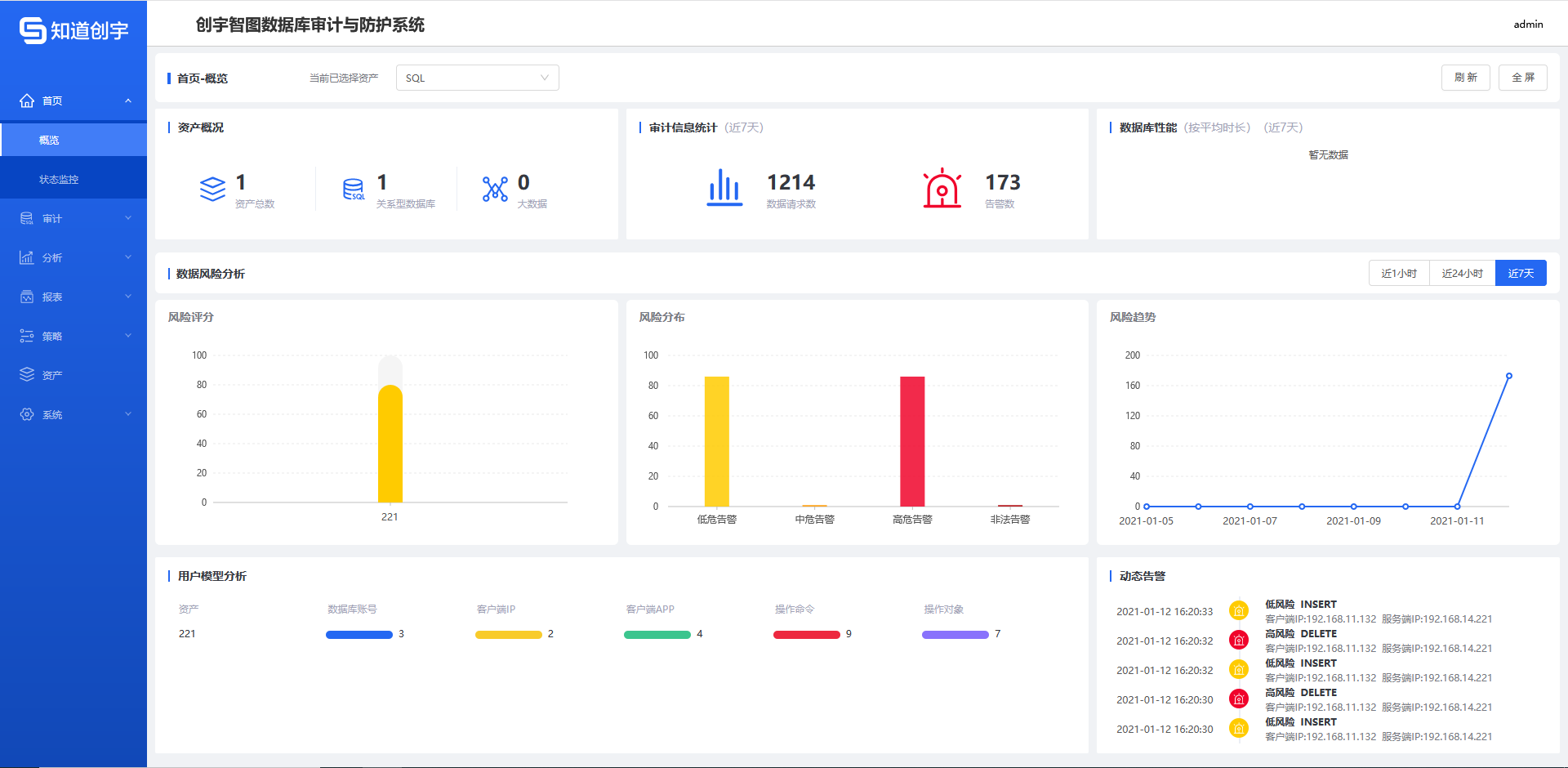


图2-1-1 资产组概览

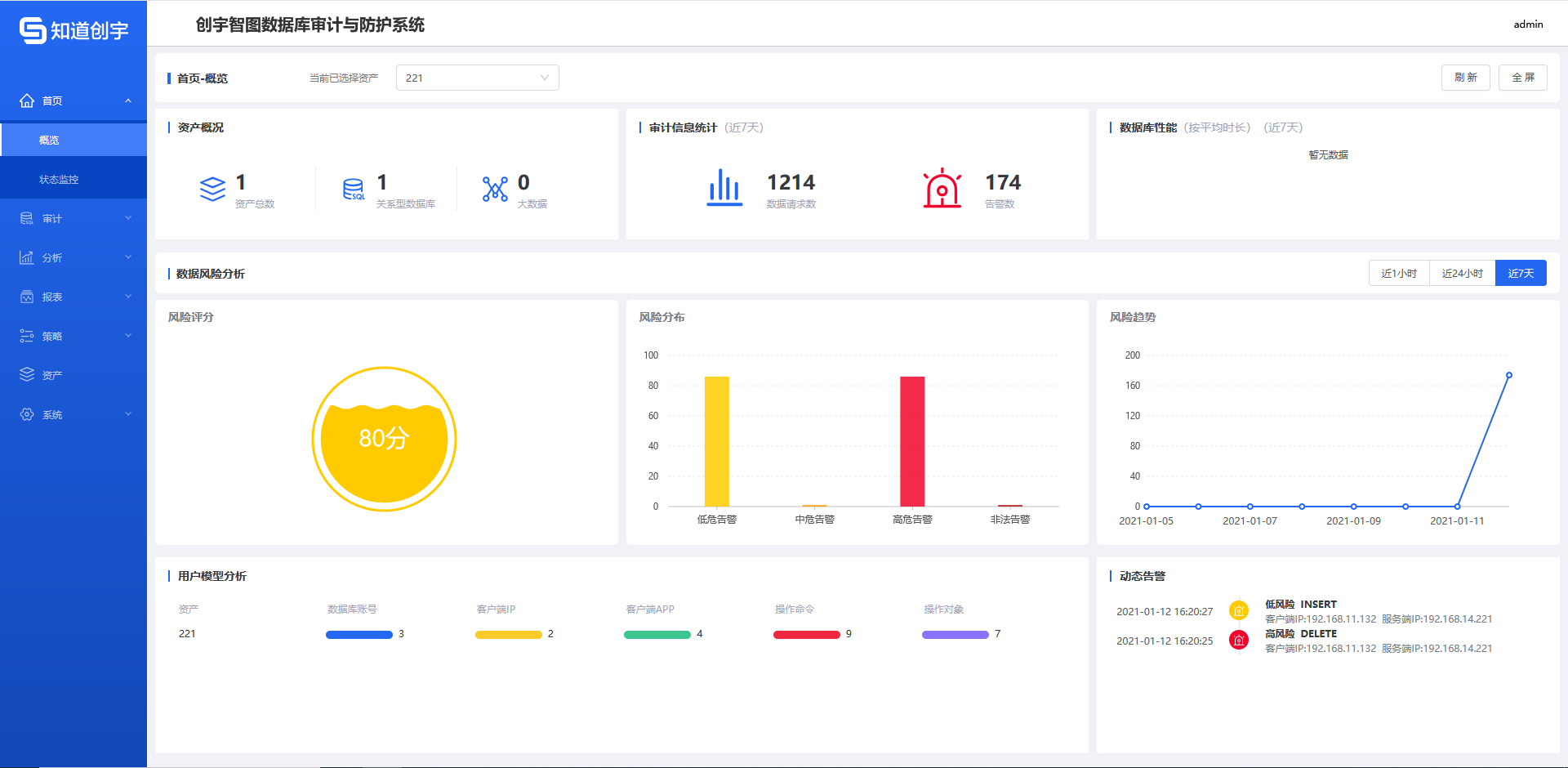


图2-1-2单个资产概览

## 状态监控

在[首页->状态监控]中，可以查看资产组或者某一资产下面的数据流量监控、数据流量排行、最新告警和实时告警，如图2-2-1和图2-2-2所示。

* 实时会话：显示5分钟内所选数据库的实时会话。
* 最新请求：显示5分钟内所选数据库的最新请求。
* 实时流量：显示5分钟内系统网卡的IO。
* 会话数：显示所选数据库的TOP5会话数。
* 请求数：显示所选数据库的TOP5请求数。
* 执行时长：显示所选数据库的TOP5执行时长。
* 最新告警：显示所选数据库的最新告警，如图2-2-3所示。
* 最新请求：显示所选数据库的最新审计日志，单击列表右侧<更多>，如图2-2-4所示，再单击<详情>可以查看某条审计日志的详情信息，如图2-2-5所示。

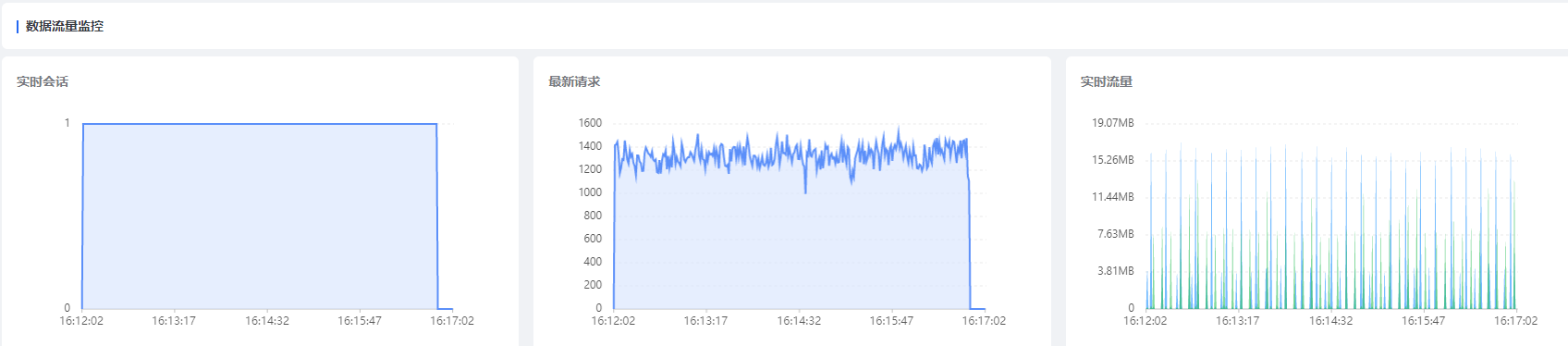


图2-2-1数据流量监控

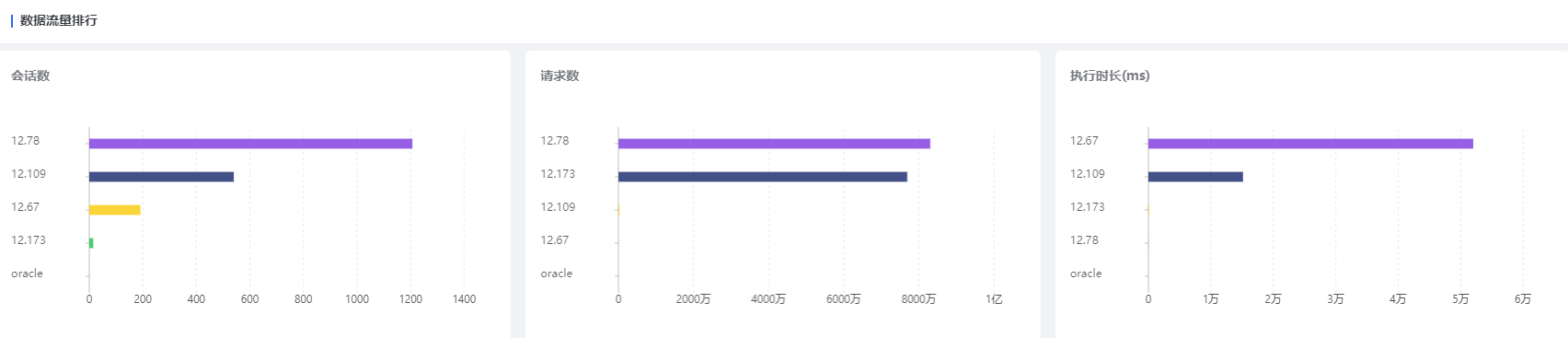


图2-2-2数据流量排行



图2-2-3最新告警



图2-2-4最新请求



图2-2-5 详情

# 审计

## 告警

进入[审计->告警]页面，如图3-1-1所示，在<当前已选择资产>下拉框选择资产组或者单一资产选择需要查看的数据库，可以查看所选数据库的告警统计。

* 风险统计：显示所选数据库非法、高危、中危、低危四种风险等级的告警统计数值。如图3-1-2所示，单击其中一种风险等级，查询条件中自动填充此种风险等级，自动查询此种风险等级下的告警日志，再次单击取消此种风险等级的查询。
* 审阅状态：显示所选数据库下未审阅和已审阅两种情况下的告警统计数值。单击其中一种审阅状态，查询条件中自动填充此种审阅状态，自动查询此种审阅状态下的告警日志，再次单击取消此种审阅状态的查询。
* 默认检索条件：时间范围、风险等级、操作命令、审阅状态。
* 高级检索：单击<高级检索>后，会出现更多查询条件，如图3-1-3所示，输入查询条件后，单击<查询>，可以搜索指定条件下的告警日志；查询完成后，单击<清空>，可以清空查询条件。
* 批量审阅：对告警日志进行查看并进行标记。选中告警日志，单击<批量审阅>，填写审阅意见。
* 导出：输入查询条件，单击查询后，单击<导出>，可以导出此查询条件下的告警日志。
* ：针对审计日志配置策略规则。如图3-1-4所示，单击图标，针对此条告警可以创建自定义规则、白名单规则、黑名单或者用户行为模型，策略中的部分规则根据告警信息自动添加，可以修改。具体的策略规则配置参考[策略]章节。
* ：查看告警日志详情。单击图标，可以查看此条告警日志更详细的信息。
* ：审阅告警日志。如图3-1-5所示，单击图标，可以填写审阅意见和配置审阅规则，对满足审阅规则的已生成的告警会自动添加审阅意见。
* ：回放告警日志中的语句。单击图标，选择时间范围，进行当前或者完整播放，如图3-1-6所示，在播放过程中可以暂停、继续和清屏。

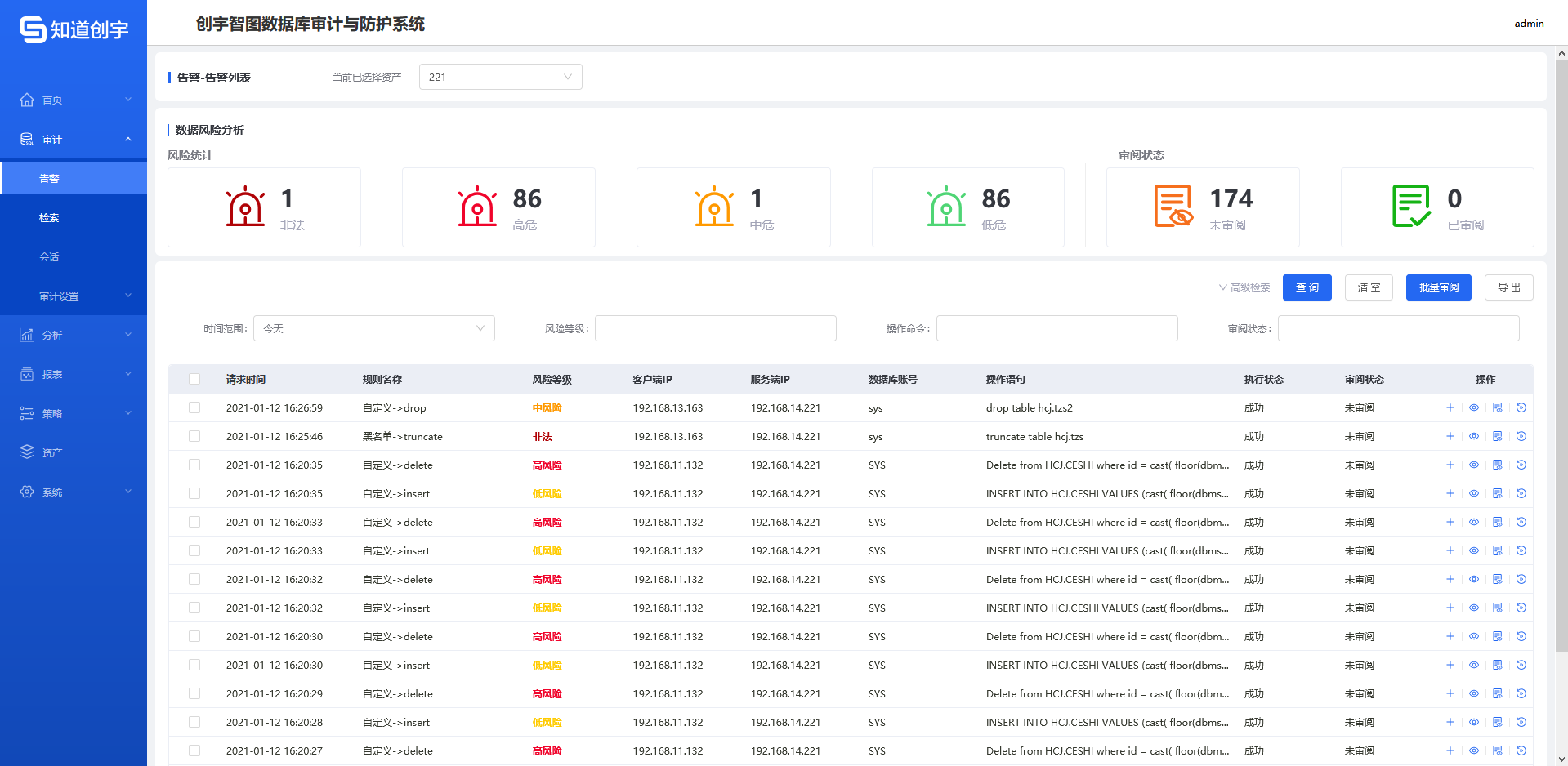


图3-1-1告警

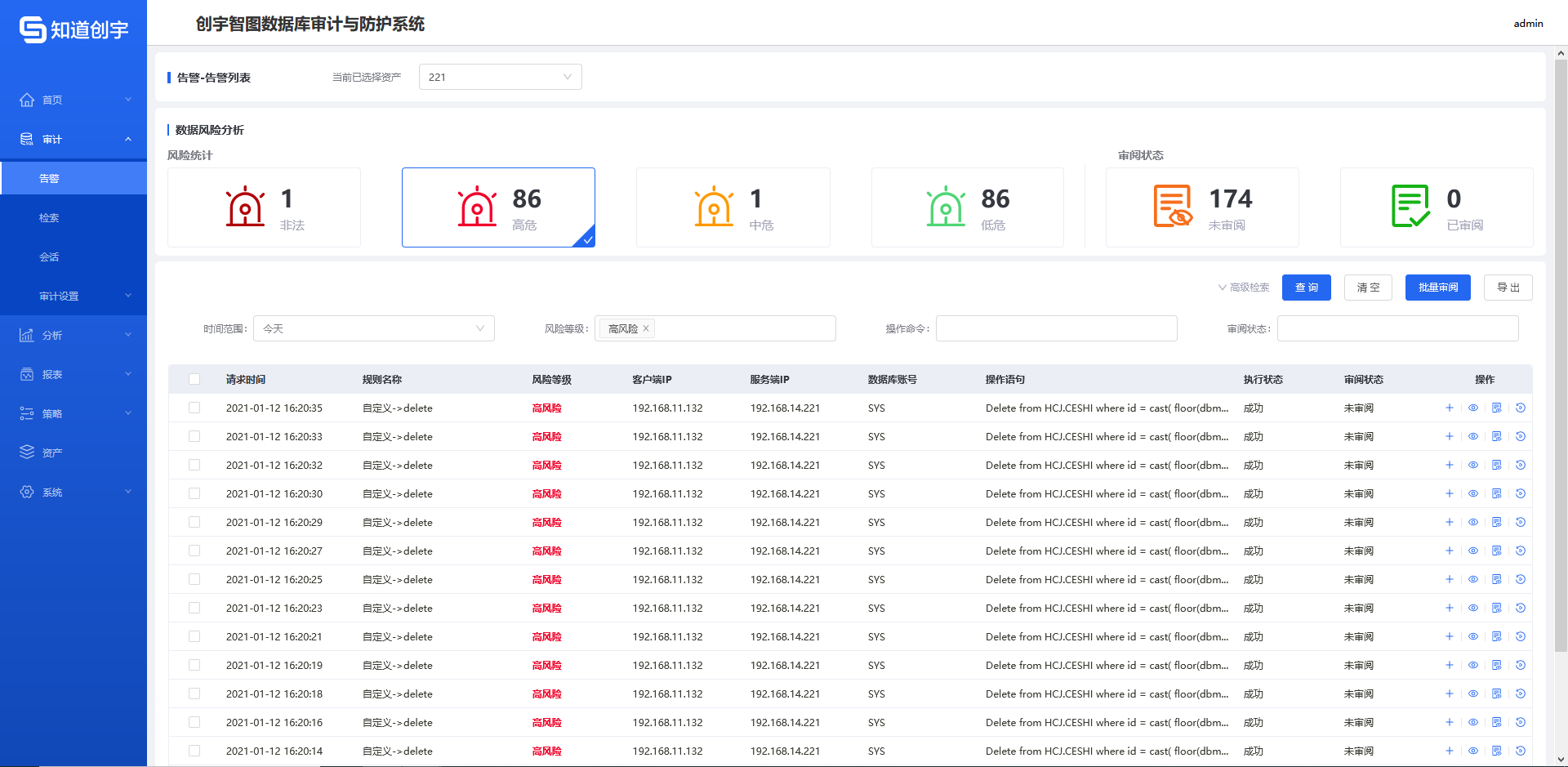


图3-1-2告警查询

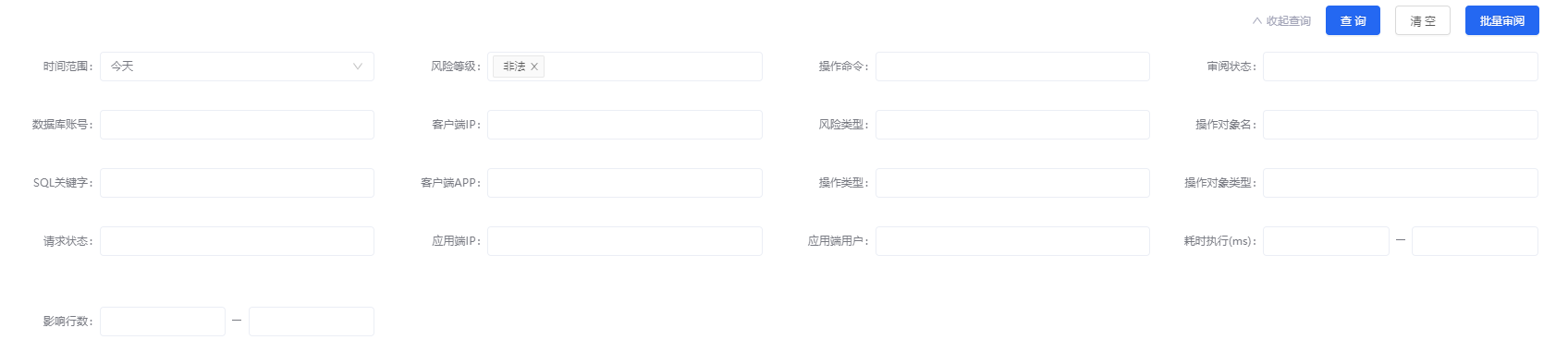


图3-1-3 告警高级检索

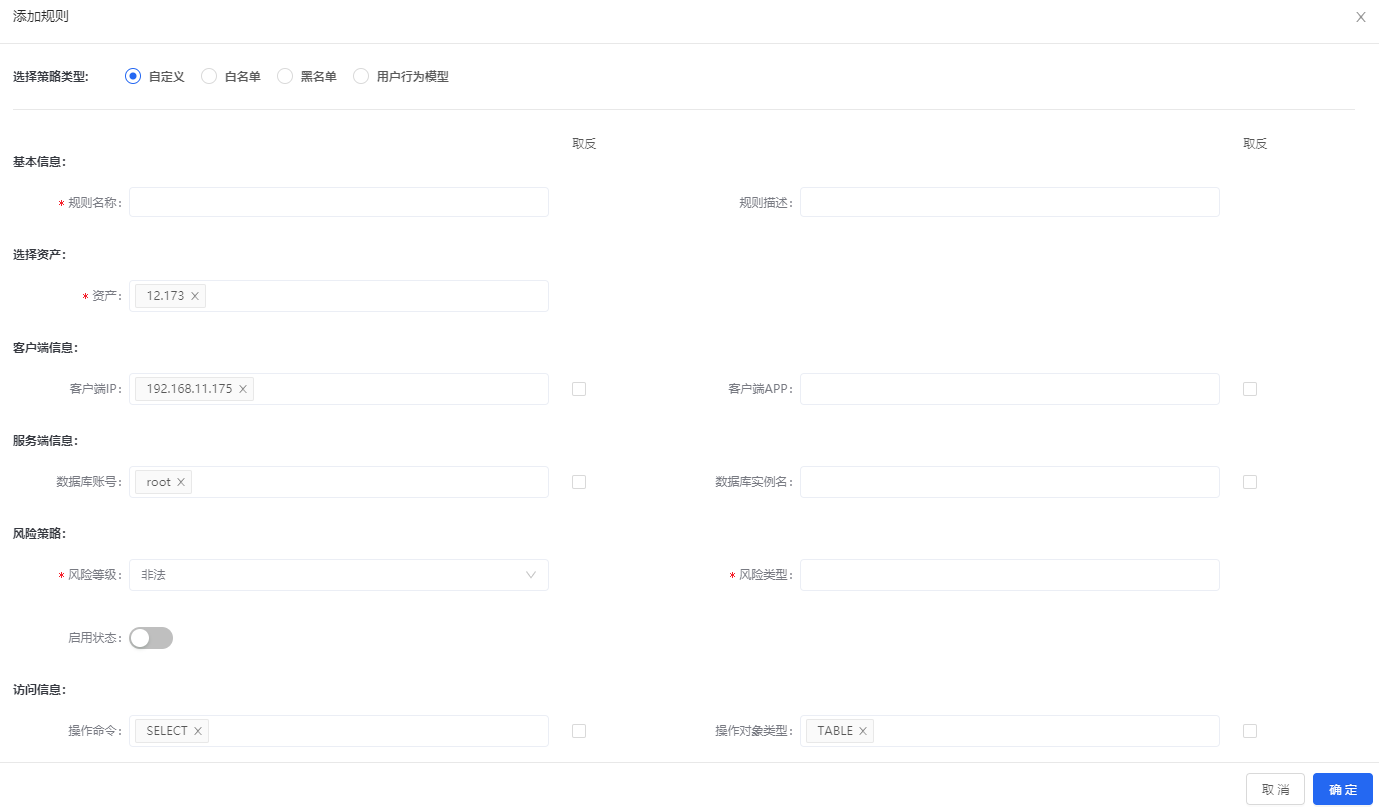
图3-1-4告警添加

图3-1-5 告警审阅

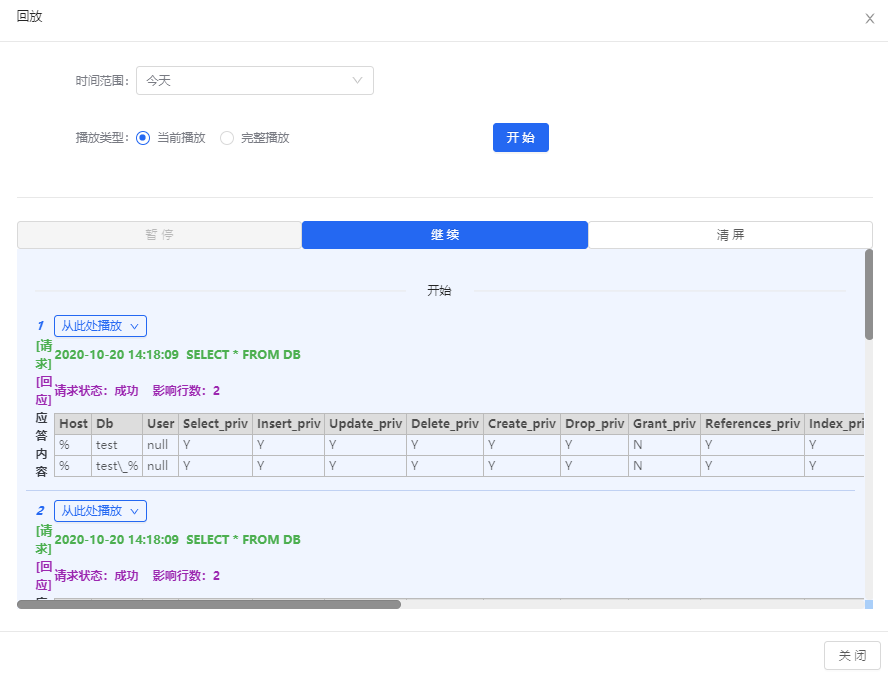


图3-1-6 回放

## 检索

进入[审计->检索]页面，可以查询所选数据库的审计日志，如图3-2-1所示。

* 所有事件：所有事件的统计，登录事件+访问事件。
* 登录事件：所有Login和Logout事件的统计。
* 访问事件：除了登录事件的其它所有请求。
* 默认检索条件：时间范围、风险等级、操作命令。
* 高级检索：单击<高级检索>后，会出现更多检索条件，如图3-2-2所示，输入查询条件后，单击<查询>，可以搜索指定条件下的告警日志；查询完成后，单击<清空>，可以清空查询条件。
* 收藏：将查询条件保存为收藏标签，下次使用相同的查询条件，直接点击收藏标签。
* 导出：输入查询条件，单击查询后，单击<导出>，可以导出此查询条件下的审计日志。
* ：查看审计日志详情。单击图标，可以查看此条审计日志更详细的信息，如图3-2-3所示。
* ：回放审计日志。单击图标，选择时间范围，对审计日志进行当前或者完整播放，如图3-2-4所示，在播放过程中可以暂停、继续和清屏。
* ：针对审计日志配置策略规则。单击图标，针对这条告警可以创建自定义规则、白名单规则、黑名单或者用户行为模型，具体的策略规则配置参考[策略]章节。

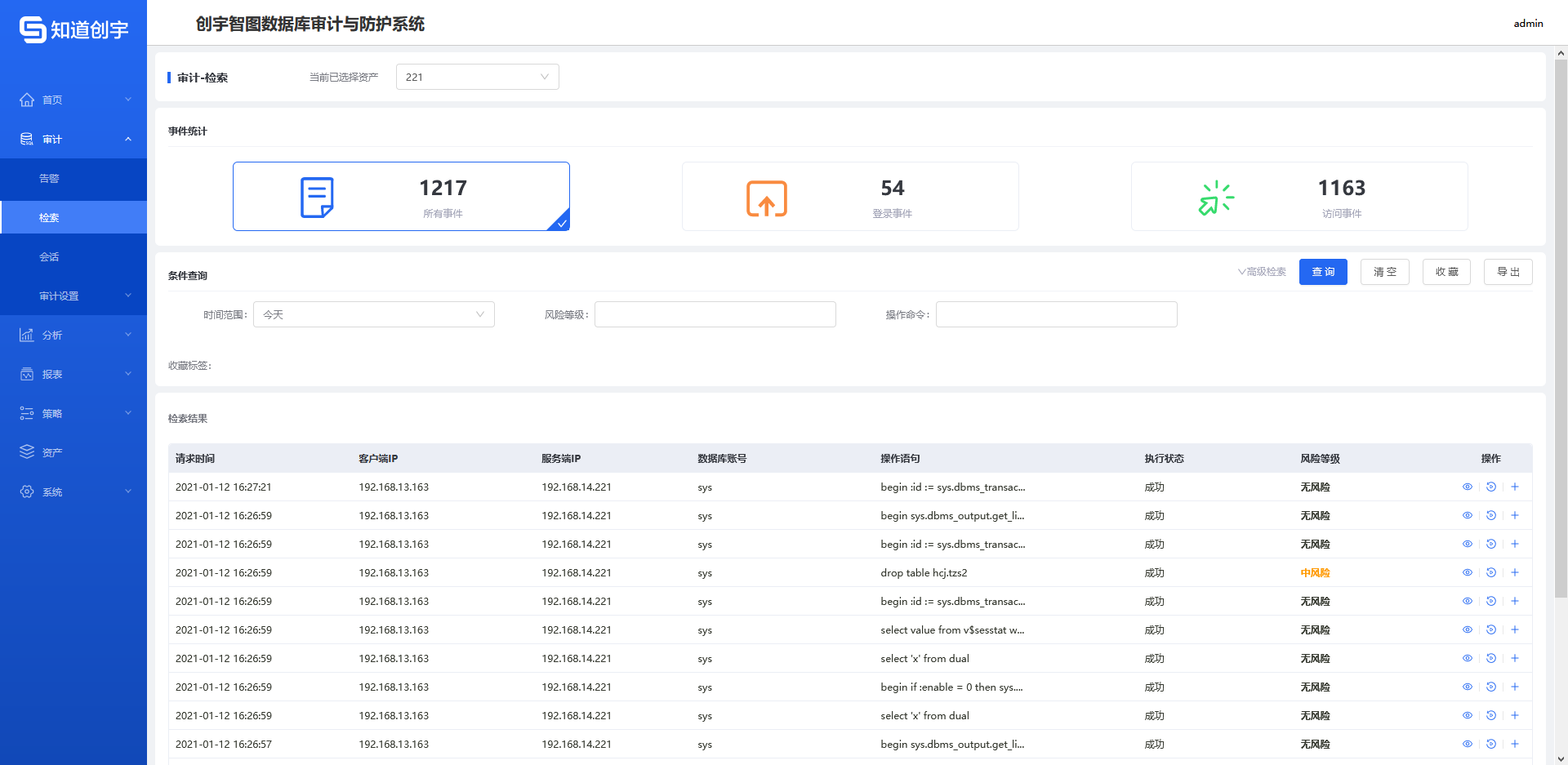


图3-2-1 检索



图3-2-2 高级检索



图3-2-3 检索详情



图3-2-4 回放

说明

检索时间：告警、检索的检索时间默认为今天。

## 会话

进入[审计->会话]页面，如图3-3-1所示，可以查看所选数据库的实时会话。

* 条件查询：输入查询条件，单击<查询>，可以查询满足条件的会话，单击<清空>，清空查询条件。
* ：查看会话详情。单击图标，可以查看此条会话日志更详细的信息，如图3-3-2所示。单击图标，可以查看请求信息详情，如图3-3-3所示。
* ：回放会话。单击图标，选择时间范围，对会话日志进行当前或者完整播放。

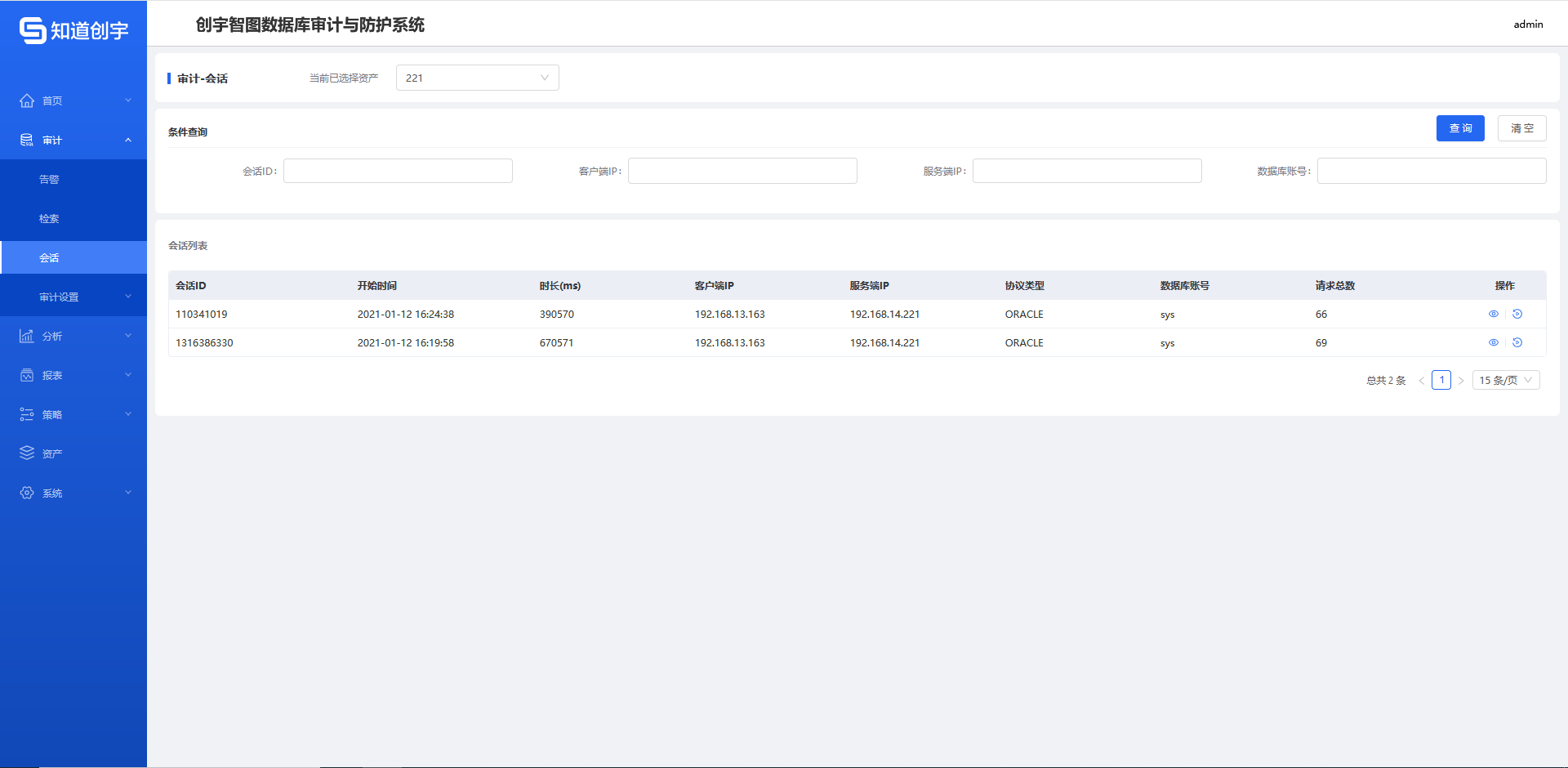


图3-3-1 会话



图3-3-2 会话详情



图3-3-3 会话详情

## 审计设置

### 告警发送

进入[审计->审计设置->告警发送]页面，如图3-4-1所示，配置告警发送，将告警日志以用户指定的方式发送，有FTP、MAIL、SYSLOG和SNMP四种通知方式。单击<>图标，编辑告警发送配置。具体配置参考图3-4-2、图3-4-3、图3-4-4和图3-4-5。

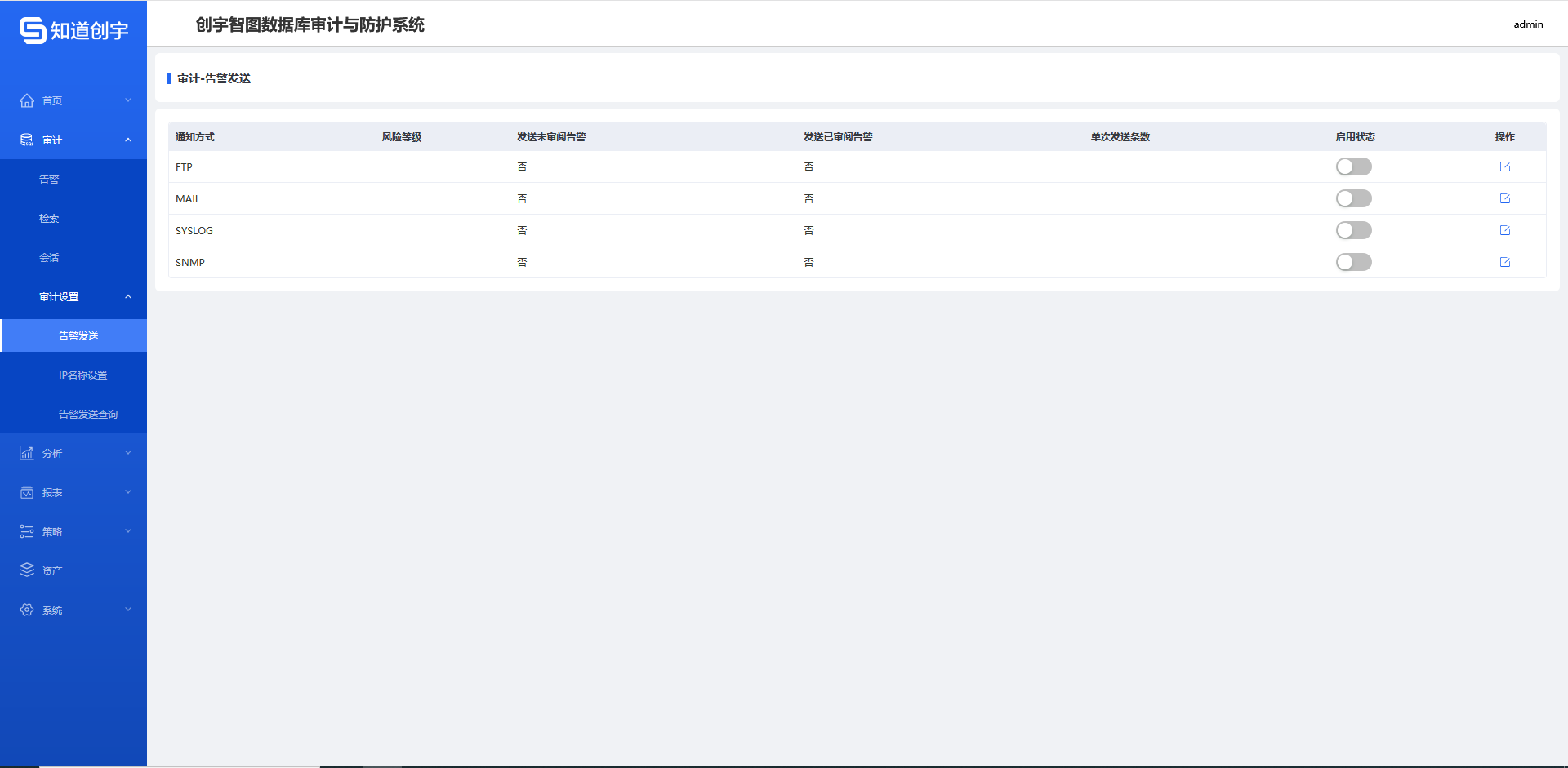


图3-4-1 审计-告警发送



图3-4-2 FTP通知配置

|  |  |
| --- | --- |
| 字段 | 内容 |
| FTP路径 | FTP服务器上存储告警日志的文件路径，不需要写FTP地址 |
| IP地址 | FTP服务器IP地址 |
| 端口 | FTP服务器配置的接收端口，一般是21 |
| 用户账号 | FTP服务器用户名 |
| 密码 | FTP服务器用户密码 |
| 风险等级 | 选择发送告警日志的等级，可以多选 |
| 告警内容 | 选择发送告警日志审阅与否，可以多选 |
| 单次发送条数 | 单次发送告警日志的条数 |
| 时间间隔 | 发送告警日志的时间间隔 |
| 启用状态 | 开启状态发送告警日志，关闭状态停止发送告警日志 |



图3-4-3 邮件通知配置

|  |  |
| --- | --- |
| 字段 | 内容 |
| SMTP服务器 | SMTP服务器地址，登录邮箱，在邮箱设置中查看发送服务器地址 |
| SMTP端口 | SMTP服务器端口，登录邮箱，在邮箱设置中查看发送服务器端口 |
| TLS/SSL | 邮箱发送使用的协议，登录邮箱，在邮箱设置中查看发送服务器支持的协议 |
| 用户账号 | 发件人的邮箱账号 |
| 密码 | 发件人的邮箱密码 |
| 发件人 | 发件人的邮箱账号 |
| 收件人 | 收件人的邮箱账号 |
| 风险等级 | 选择发送告警日志的等级，可以多选 |
| 告警内容 | 选择发送告警日志审阅与否，可以多选 |
| 单次发送条数 | 单次发送告警日志的条数 |
| 时间间隔 | 发送告警日志的时间间隔 |
| 启用状态 | 开启状态发送告警日志，关闭状态停止发送告警日志 |



图3-4-4 Syslog通知配置

|  |  |
| --- | --- |
| 字段 | 内容 |
| IP | SYSLOG日志主机的IP地址 |
| 端口 | SYSLOG日志主机的端口，一般默认是514 |
| 编码 | SYSLOG日志主机支持的编码格式 |
| 风险等级 | 选择发送告警日志的等级，可以多选 |
| 告警内容 | 选择发送告警日志审阅与否，可以多选 |
| 单次发送条数 | 单次发送告警日志的条数 |
| 时间间隔 | 发送告警日志的时间间隔 |
| 启用状态 | 开启状态发送告警日志，关闭状态停止发送告警日志 |



图3-4-5 SNMP通知配置

|  |  |
| --- | --- |
| 字段 | 内容 |
| IP | 网络管理系统的IP地址 |
| 端口 | 网络管理系统的监听端口 |
| OID | 网络管理系统和被测设备之间约定的告警日志的对象标识符 |
| 风险等级 | 选择发送告警日志的等级，可以多选 |
| 告警内容 | 选择发送告警日志审阅与否，可以多选 |
| 单次发送条数 | 单次发送告警日志的条数 |
| 时间间隔 | 发送告警日志的时间间隔 |
| 启用状态 | 开启状态发送告警日志，关闭状态停止发送告警日志 |

### 告警发送查询

进入[审计->审计设置->告警发送查询]页面，如图3-4-5所示，可以查看告警发送状态。如果发送状态是失败 ，可以单击重发。可以通过告警发送方式、时间范围、发送状态进行查询。

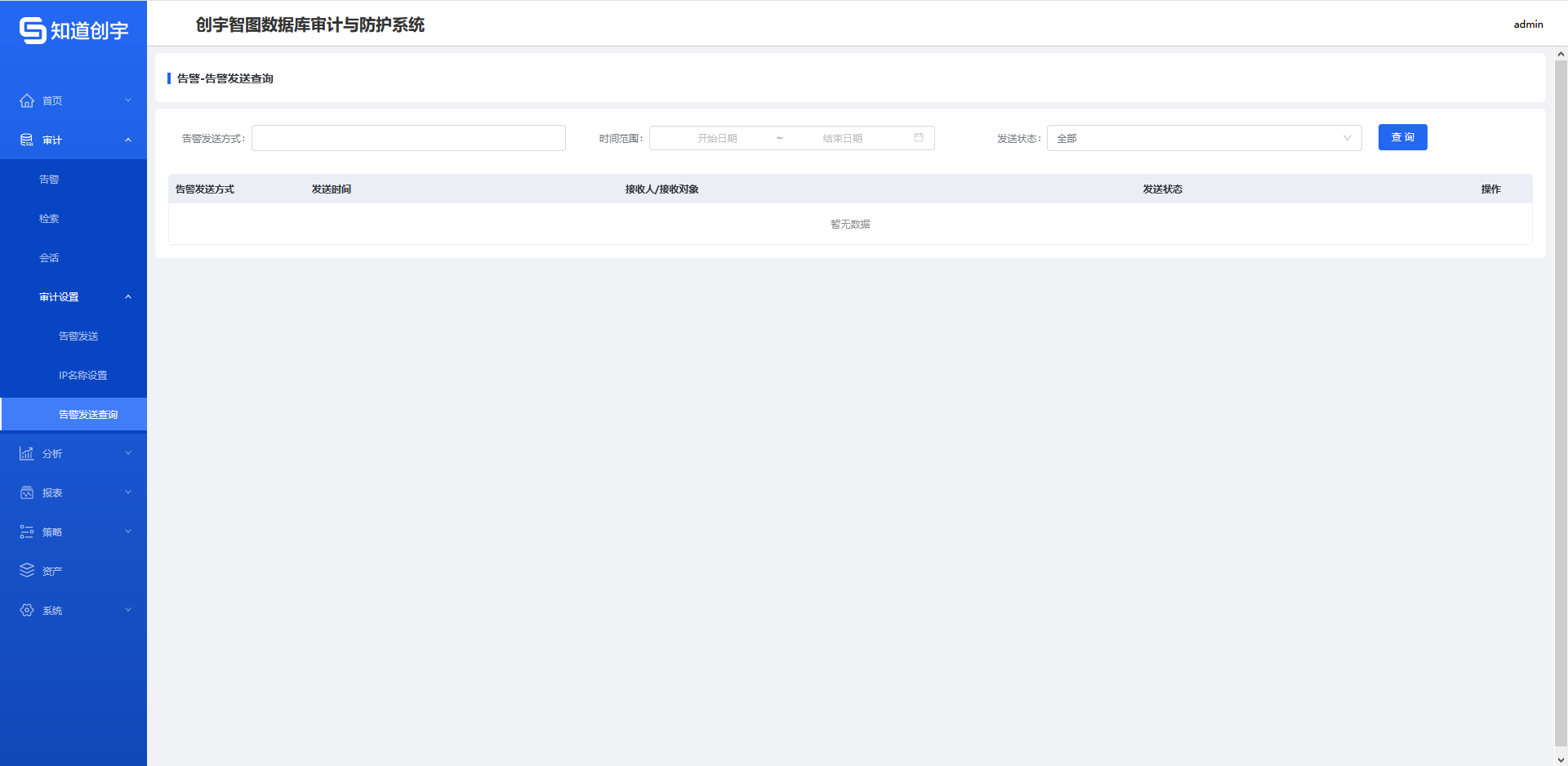


图3-4-5 告警发送查询

# 分析

## 多维分析

进入[分析->多维分析]页面，如图4-1-1所示，选择需要查看的数据库，配置报表时间范围、图标类型、报表维度，单击<下一步>，添加报表维度，可以多次单击下一步。单击<下载分析报告>，可以下载分析报告，单击<生成报表模板>，可以在[报表->自定义报表]中查看模板。

注意

多维分析页面只能选择单一资产，不能选择资产组。

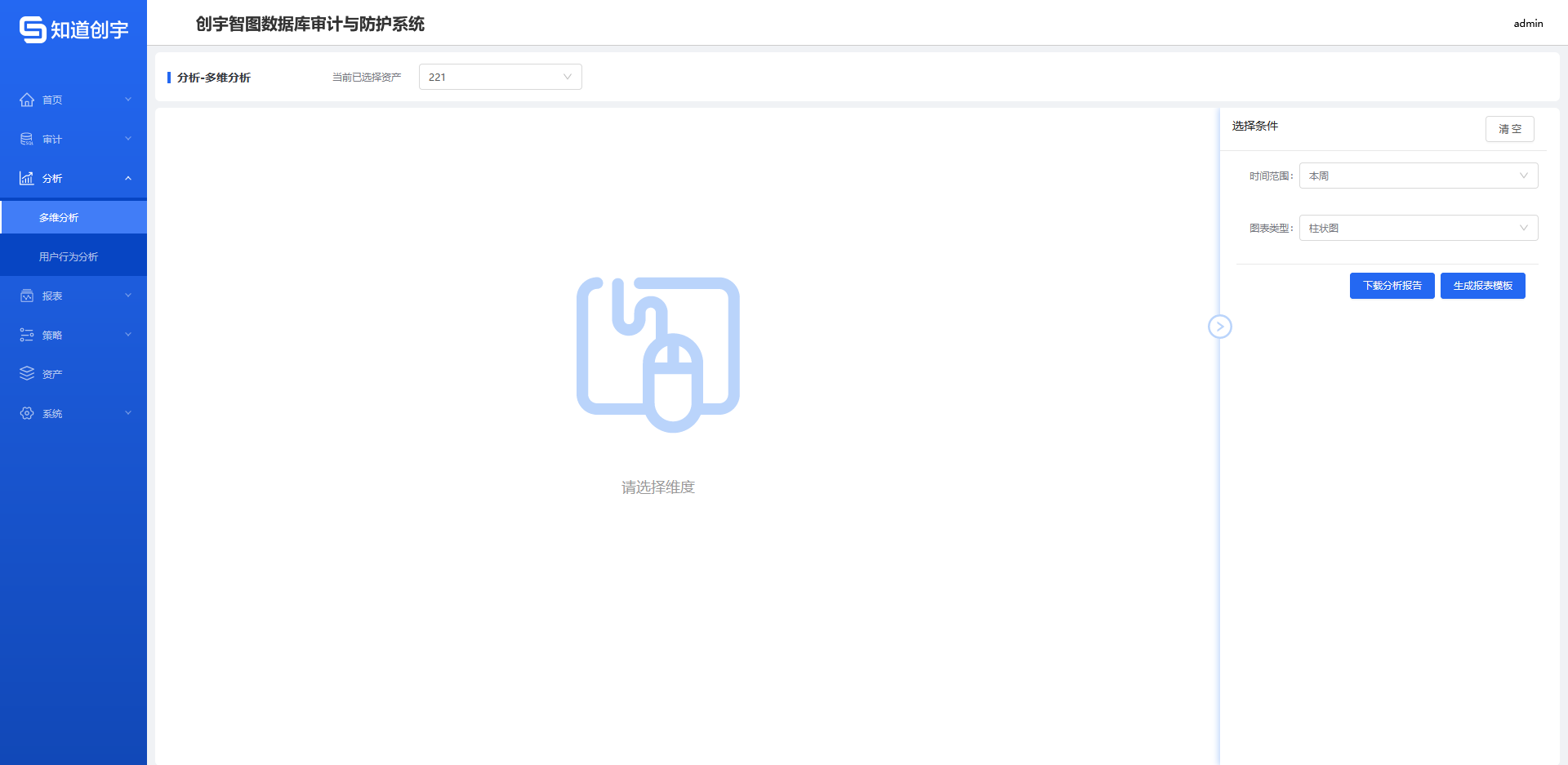


图4-1-1 多维分析

## 用户行为分析

进入[分析->用户行为分析]页面，如图4-2-1所示，选择需要查看的数据库，单击图标，可以展示用户访问行为轨迹。用户行为分析，是从资产、到账号，客户端IP、客户端APP、操作命令、操作对象，形成整个完整的用户访问数据库资产的行为分析，完全模拟用户的真实的操作场景，用图形化来展示用户的访问行为轨迹。

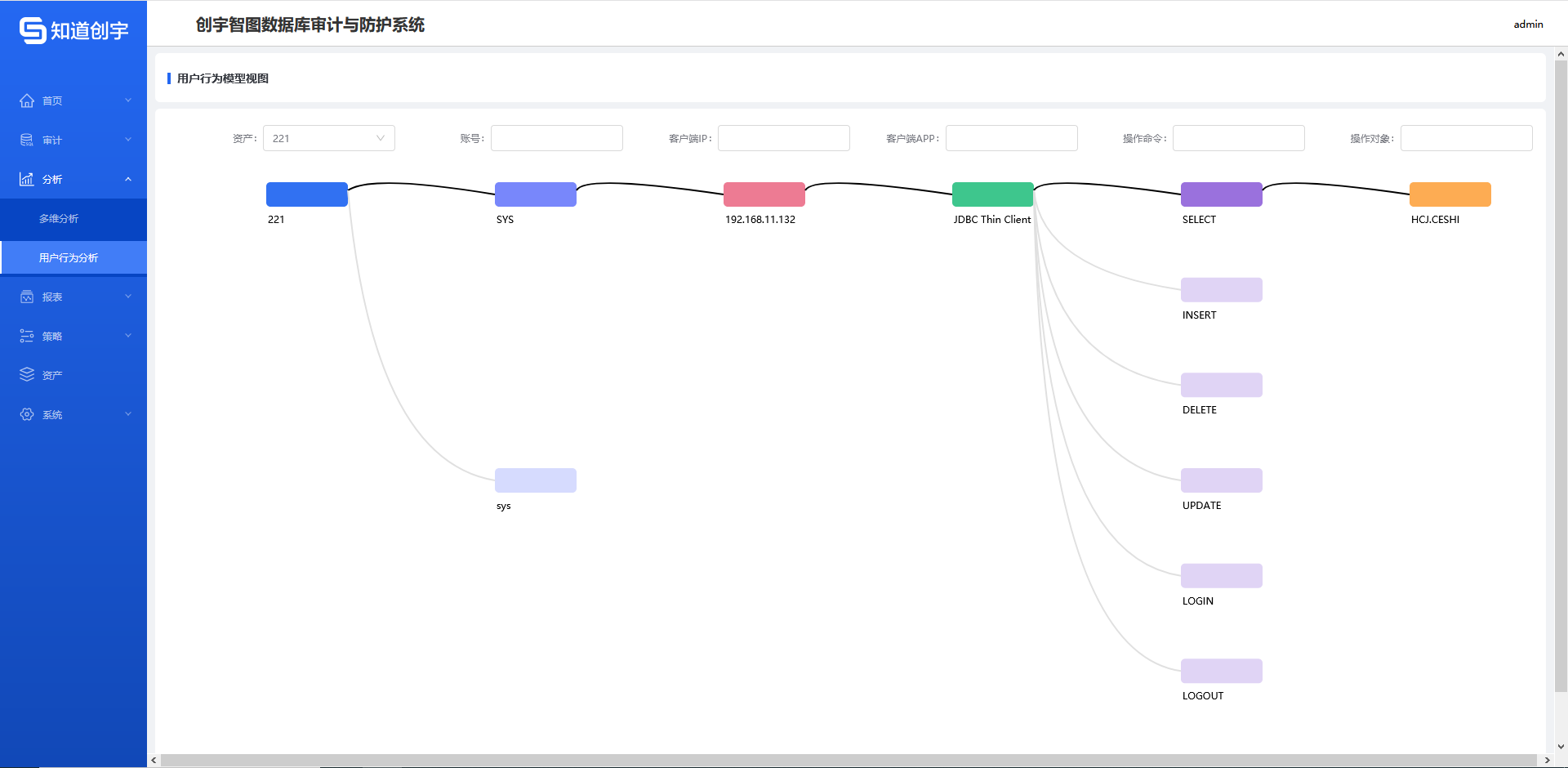


图4-2-1 用户行为分析

# 报表

## 预定义报表

进入[报表->预定义报表]页面，如图5-1-1所示，预定义报表，分为综合、合规性、风险分析和客户端分析等10种类型，内嵌54种报表模板。首先在<当前已选择资产>中选择需要查看的单一资产或者资产组，然后配置时间段和报表类型，时间段支持自定义、昨天、上周、上月、本周和本月，报表类型有PDF和CSV两种，再选择报表类型，单击<>图标，预览报表内容，如图5-1-2所示，单击<返回>回到预定义报表页面；单击<>图标，生成报表，在[报表->报表生成]中可以查看生成的报表任务；单击<>图标，添加到我的报表，在[报表->我的报表]中可以看到添加的报表模板；单击<>图标，配置邮件定时发送报表，如图5-1-3所示，在[报表->定时报表]中查看定时报表任务。

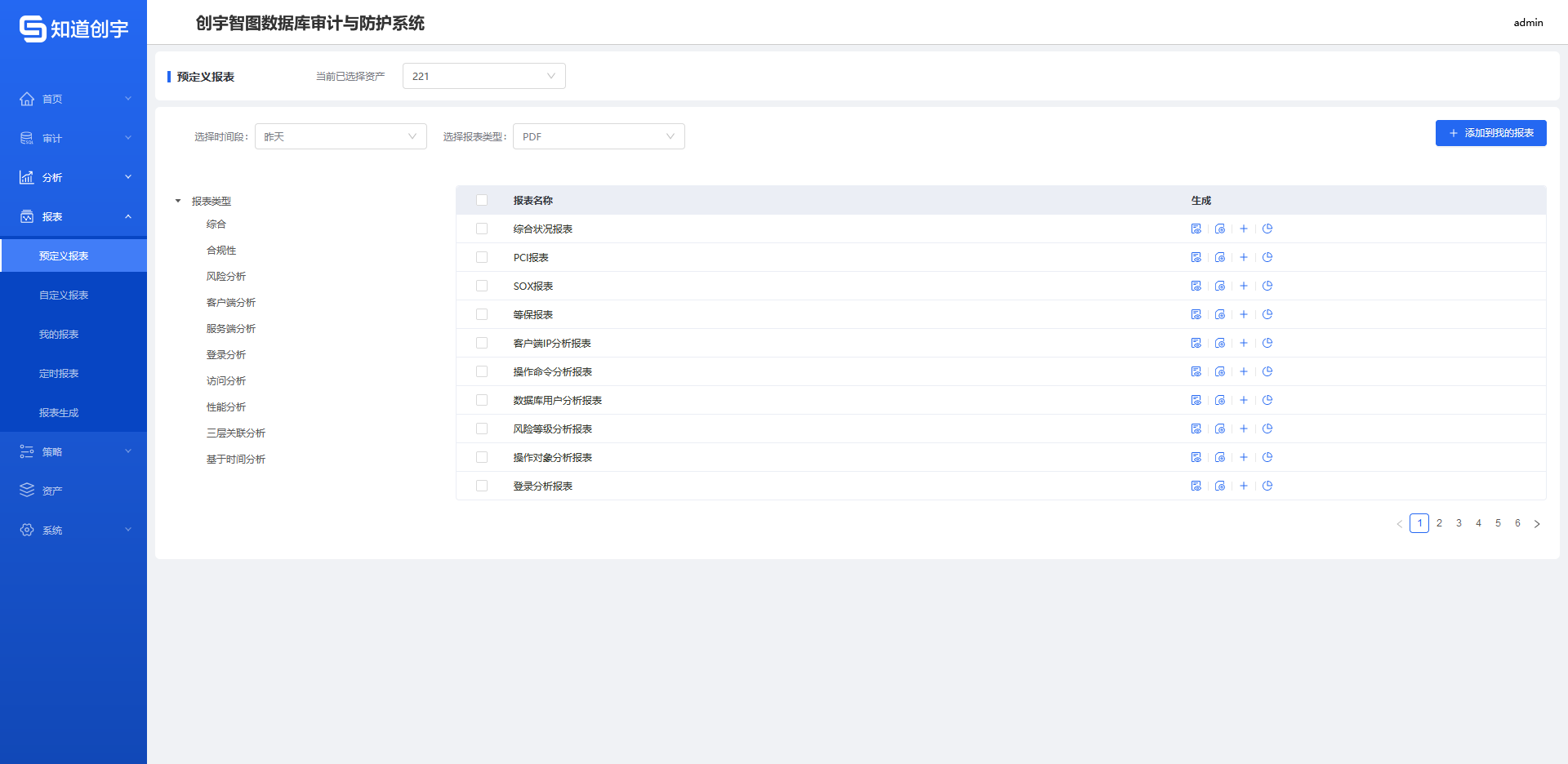


图5-1-1 预定义报表



图5-1-2 报表预览



图5-1-3 添加定时报表

|  |  |
| --- | --- |
| 字段 | 内容 |
| 报表格式 | 定时报表发送的格式，目前只支持发送PDF格式 |
| 审计时间段 | 定时报表发送的审计时间段，支持自定义、每天、每周、每月和每年 |
| 发送时间 | 定时报表发送时间 |
| SMTP服务器 | 发送服务器地址，在邮箱设置中可以查看 |
| SMTP端口 | 发送服务器端口，在邮箱设置中可以查看 |
| TLS/SSL | 发送服务器支持的协议，在邮箱设置中可以查看，注意SMTP端口和TLS/SSL保持一致 |
| 邮箱账号 | 发件人的邮箱账号 |
| 密码 | 发件人的邮箱密码 |
| 发件人 | 发件人的邮箱账号 |
| 收件人 | 收件人的邮箱账号 |

## 自定义报表

进入[报表->自定义报表]页面，如图5-2-1所示，是用户自定义的报表模板，在[分析-多维分析]中选择不同报表维度生成的报表模板。首先在<当前已选择资产>中选择需要查看的单一资产或者资产组，然后配置时间段和报表类型，时间段支持自定义、昨天、上周、上月、本周和本月，报表类型有PDF和CSV两种，再选择报表类型，单击<>图标，预览报表内容，单击<返回>回到自定义报表页面；单击<>图标，生成报表，在[报表->报表生成]中可以查看生成的报表任务；单击<>图标，添加到我的报表，在[报表->我的报表]中可以看到添加的报表模板；单击<>图标，配置邮件定时发送报表，在[报表->定时报表]中查看定时报表任务，具体配置方法参考5.1预定义报表章节对定时发送报表的介绍。选中报表，单击<删除>，可以删除自定义报表模板。

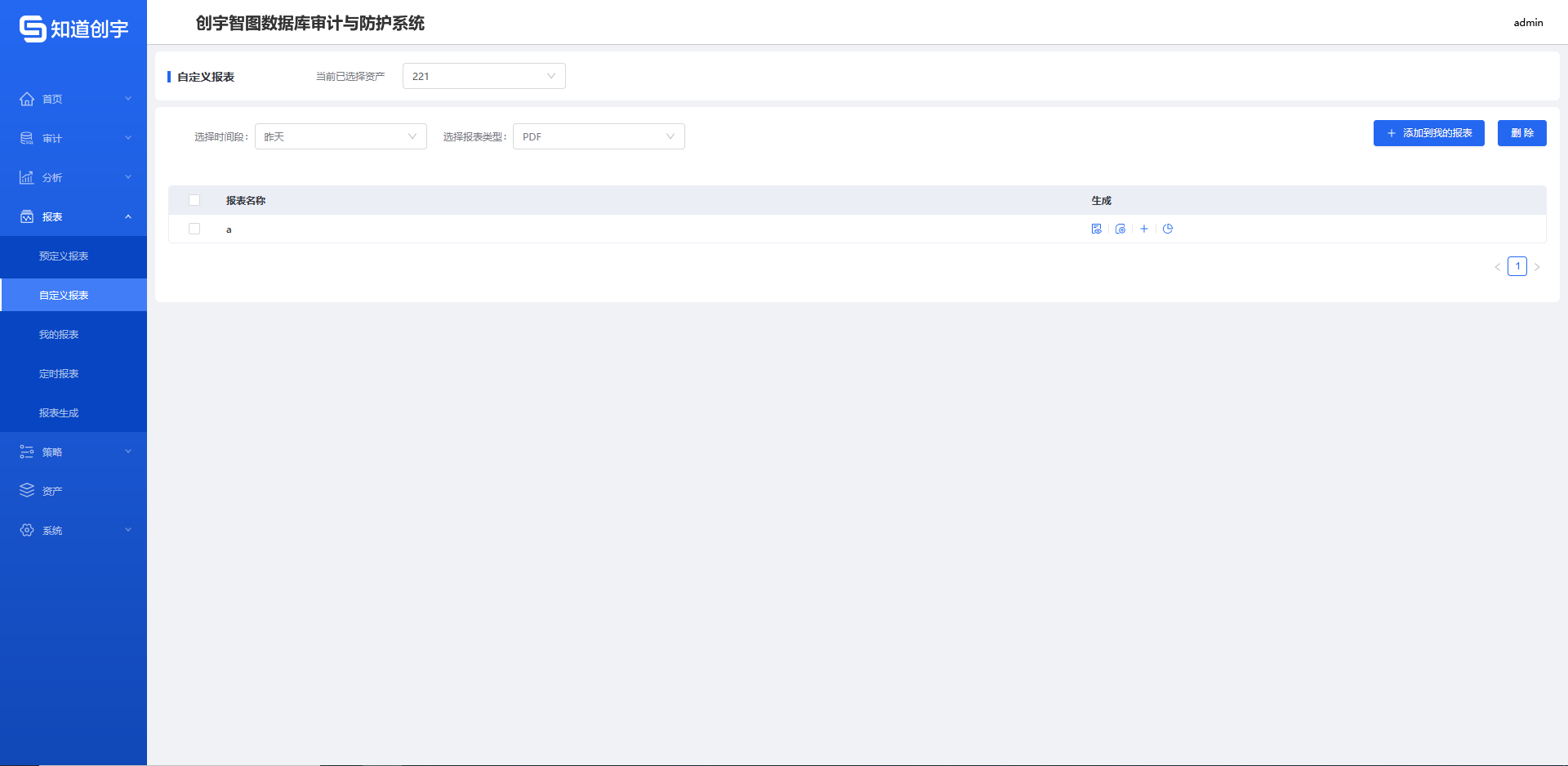


图5-2-1 自定义报表

## 我的报表

进入[报表->我的报表]页面，可以看到用户添加的常用报表模板。首先在<当前已选择资产>中选择需要查看的单一资产或者资产组，然后配置时间段和报表类型，时间段支持自定义、昨天、上周、上月、本周和本月，报表类型有PDF和CSV两种，再选择报表类型，单击<>图标，预览报表内容，单击<返回>回到我的报表页面；单击<>图标，生成报表，在[报表->报表生成]中可以查看生成的报表任务；单击<>图标，配置邮件定时发送报表，在[报表->定时报表]中查看定时报表任务，具体配置方法参考5.1预定义报表章节对定时发送报表的介绍。选中报表，单击<删除>，可以删除报表模板。

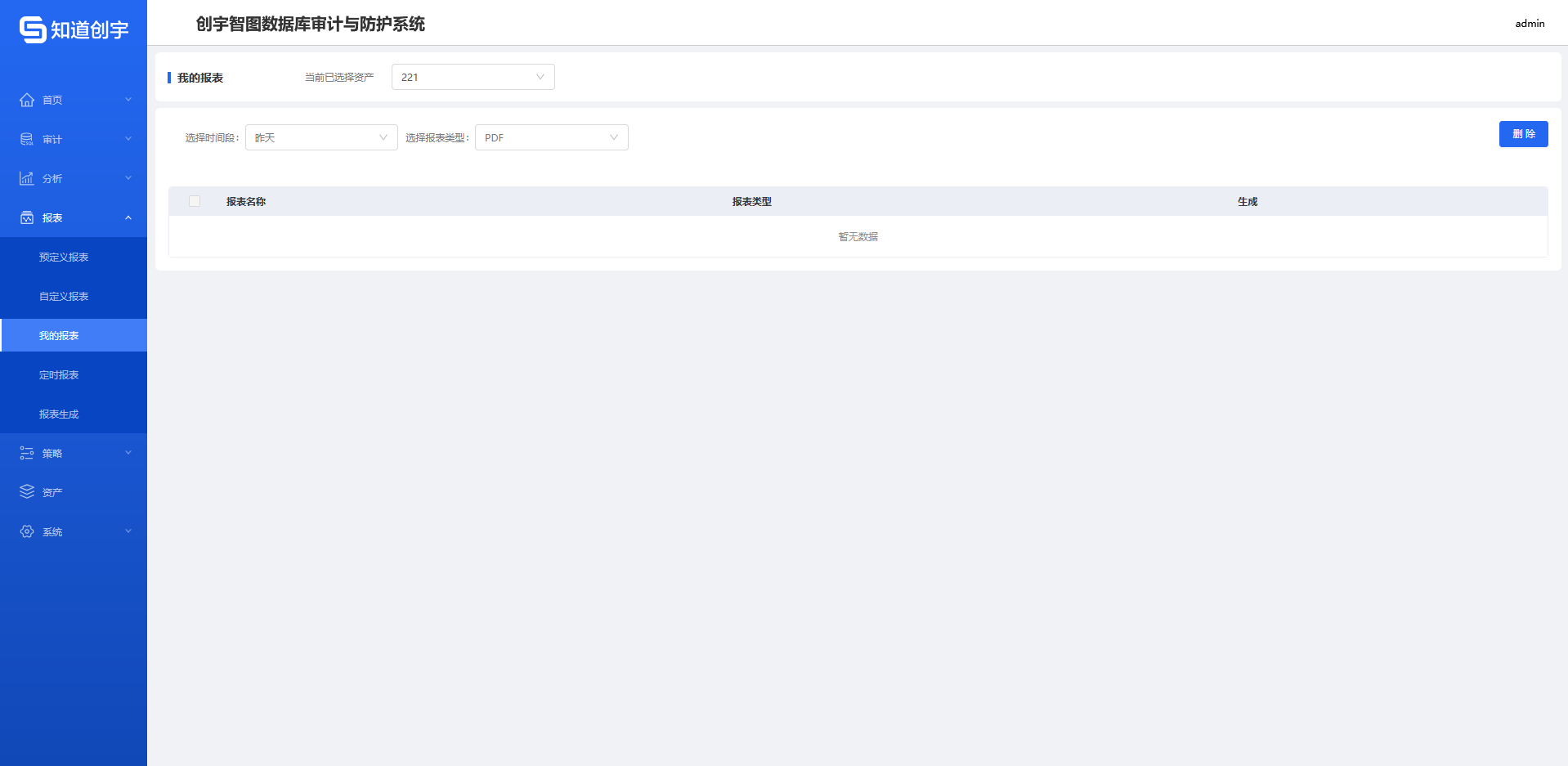


图5-3-1 我的报表

## 定时报表

进入[报表->定时报表]页面，如图5-4-1所示，在<当前已选择资产>中选择需要查看的单一资产或者资产组，可以看到在预定义报表、自定义报表和我的报表中添加的定时报表任务，对定时报表进行管理。单击<>图标，编辑定时报表配置；单击<>图标，删除定时报表。

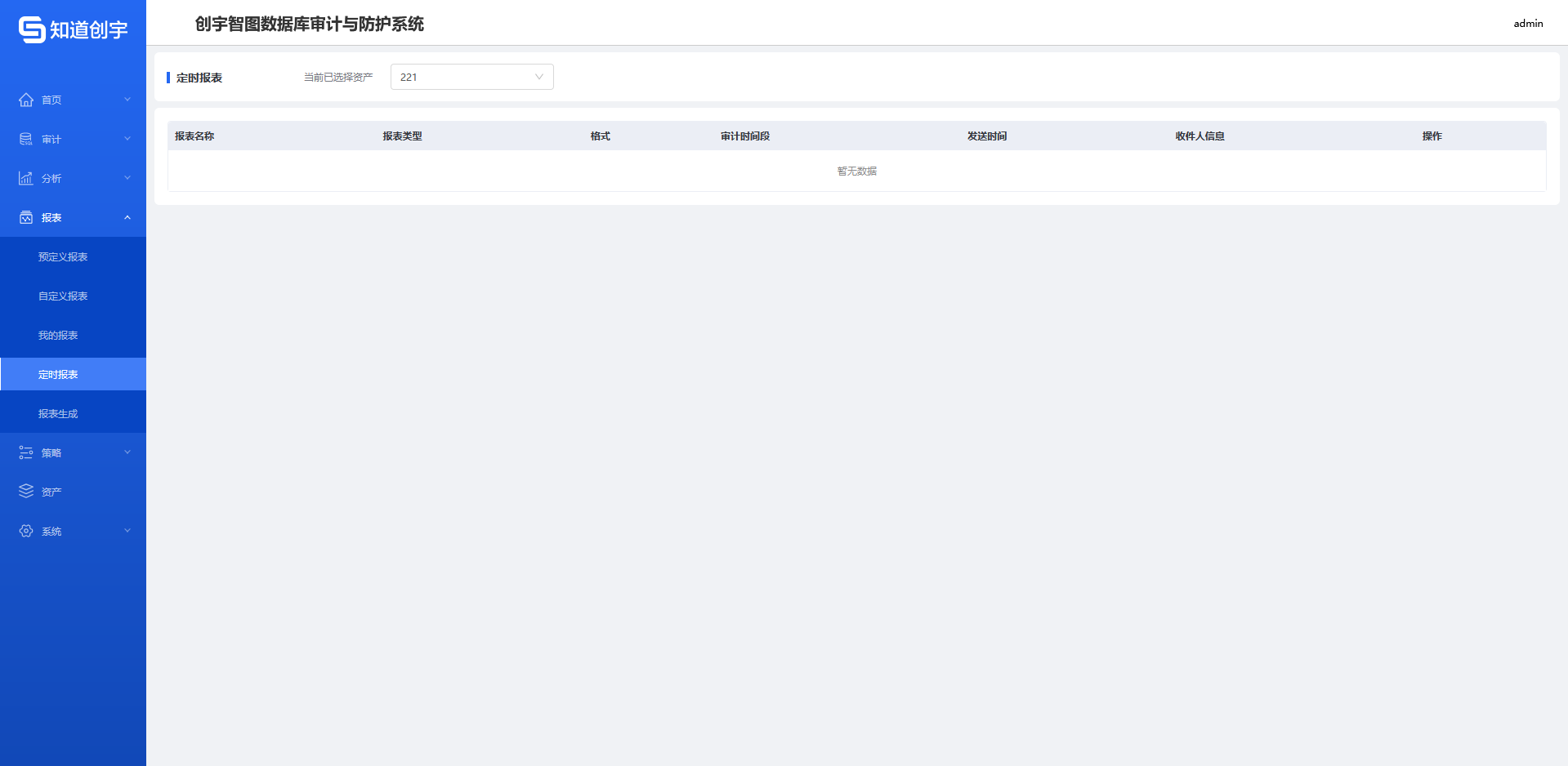


图5-4-1 定时报表

## 报表生成

进入[报表->报表生成]页面，如图5-5-1所示，可以看到在预定义报表、自定义报表和我的报表中添加的生成报表任务，包括报表名称、资产、格式、生成进度、生成方式、审计时间段和下载次数，单击<>图标，下载报表，下载次数更新；如果报表生成失败，单击<>图标，重新生成报表。

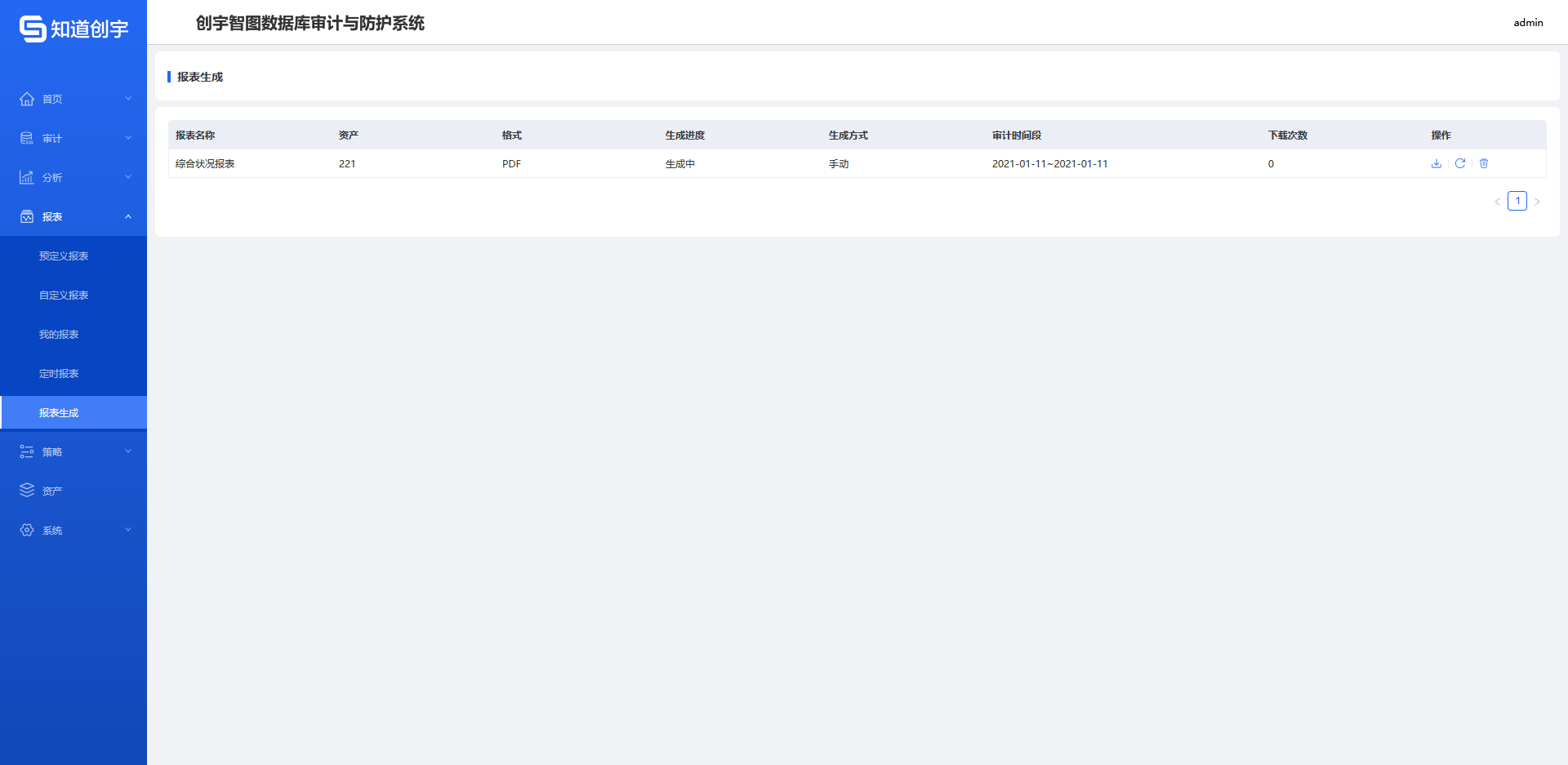


图5-5-1 报表生成

# 策略

## 白名单

进入[策略->白名单]页面，如图6-1-1所示，配置白名单策略后，命中白名单策略的审计日志风险等级会标记为可信。在白名单页面，单击<添加>，可以添加新的白名单策略，如图6-1-2，配置白名单策略命中条件；在白名单配置页面，单击蓝色字体<添加操作语句>，先单击<添加>，然后输入操作语句，勾选是否正则，再单击<提交> ，添加操作语句，如图6-1-3所示，勾选添加后的操作语句可以作为操作语句的命中条件；选中某条策略，单击<>图标，编辑已有的白名单策略；单击<>图标，删除白名单策略。白名单策略查询条件有资产、规则名称、数据库账号和客户端IP，单击<高级检索>，查询条件增多，有操作命令、操作对象类型、操作对象名和操作语句，单击<清空>，可以清空查询条件。

白名单功能生效，状态需要在白名单页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新请求]，查看实时流量检查白名单策略是否生效，如图6-1-4所示。

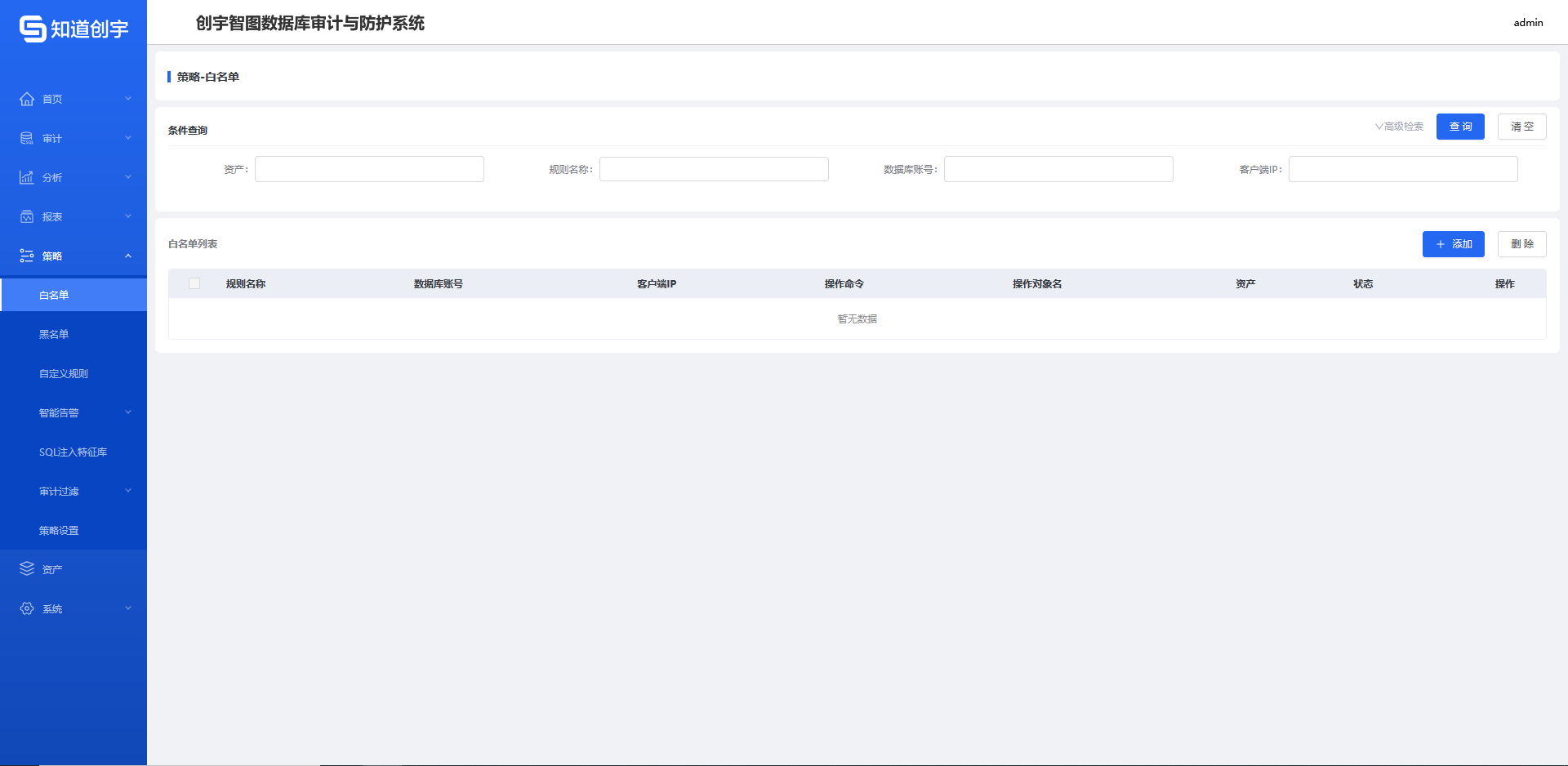


图6-1-1 白名单



图6-1-2 白名单配置

|  |  |
| --- | --- |
| 字段 | 内容 |
| 规则名称 | 策略的名称 |
| 规则描述 | 策略的规则描述 |
| 资产 | 数据库IP名称，单击空白框，出现资产列表，勾选后配置成功 |
| 数据库账号 | 数据库登录账号，可以通过审计-检索-详情，查看审计日志详情，确定数据库账号 |
| 客户端IP | 访问数据库的客户端IP，可以通过审计-检索-详情，查看审计日志详情，确定客户端IP |
| 客户端APP | 访问数据库的客户端APP名称，可以通过审计-检索-详情，查看审计日志详情，确定客户端APP |
| 操作命令 | 访问数据库的SQL关键字，如SELECT、INSERT和DELECT等，不区分大小写，单击空白框，可输入部分单词后选择操作命令，或者输入后单击回车键配置；可以通过审计-检索-详情，查看审计日志详情，确定操作命令 |
| 操作对象类型 | 访问数据库的操作对象类型，单击空白框，出现操作对象类型列表，如TABLE等，不区分大小写，单击空白框，可输入部分单词后选择操作命令，或者输入后单击回车键配置；可以通过审计-检索-详情，查看审计日志详情，确定操作对象类型 |
| 操作对象名 | 访问数据库的操作对象名，不区分大小写，单击空白框，输入后单击回车键配置；可以通过审计-检索-详情，查看审计日志详情，确定操作对象名 |
| 操作语句 | 访问数据库的操作语句，单击添加操作语句，可以先添加或者勾选已有的操作语句 |
| 时间 | 配置审计的时间，支持时间范围、天、周和月四种配置方式 |
| 启用状态 | 配置策略开启和关闭 |



图6-1-3 添加语句操作



图6-1-4 白名单策略命中示例

注意

取反的意思是，除了填写的不能通过之外其他的都可以。

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

## 黑名单

进入[策略->黑名单]页面，如图6-2-1所示，配置黑名单策略后，命中黑名单策略的审计日志风险等级会标记为非法。在黑名单页面，单击<添加>，可以添加新的黑名单策略 ，配置方式参考6.1白名单配置介绍；选中某条策略，单击<>图标，编辑已有的黑名单策略，单击<>图标，删除黑名单策略；查询条件有资产、规则名称、数据库账号和客户端IP，单击<高级检索>，查询条件增多，有操作命令、操作对象类型、操作对象名和操作语句，单击<清空>，可以清空查询条件。黑名单功能生效，状态需要在黑名单页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新请求]或者[首页->状态监控->最新告警]，查看实时流量检查黑名单策略是否生效，如图6-2-2所示。

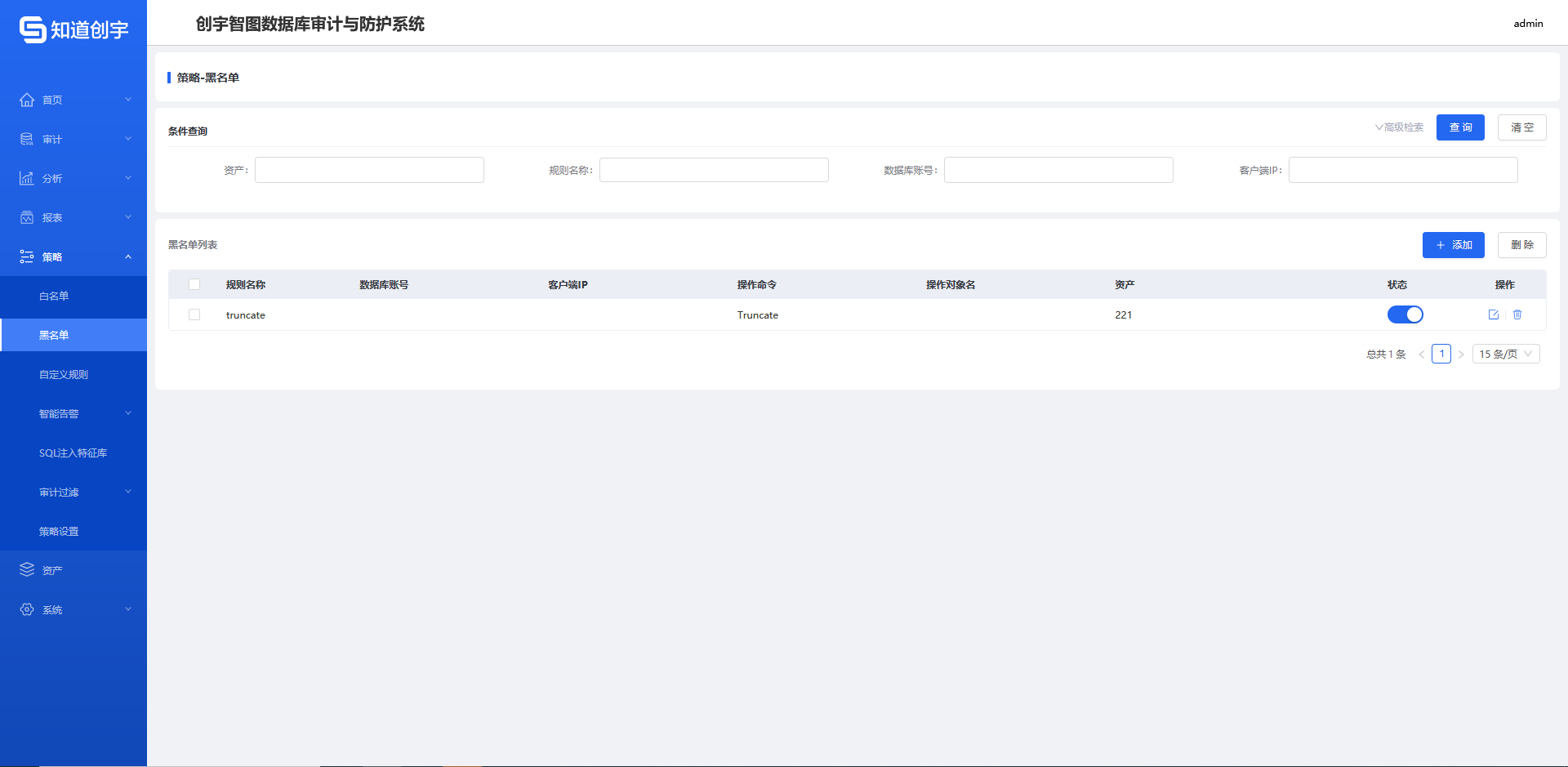




图6-2-1 黑名单



图6-2-2 黑名单策略命中示例

注意

取反的意思是，除了填写的不能通过之外其他的都可以。

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

## 自定义规则

进入[策略->自定义规则]页面，如图6-3-1所示。在自定义规则页面，单击<添加>，可以添加新的自定义规则策略，如图6-3-2所示 ，进行自定义测试配置；选中某条策略，单击<>图标，编辑已有的自定义规则策略，单击<>图标，删除自定义规则策略；查询条件有资产、规则名称、风险等级和风险类型，单击<高级检索>，查询条件增多，有操作命令、操作对象类型、操作对象名和操作语句等，单击<清空>，可以清空查询条件。自定义规则功能生效，状态需要在自定义规则页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新告警]，查看实时流量检查自定义策略是否生效，如图6-3-3所示。

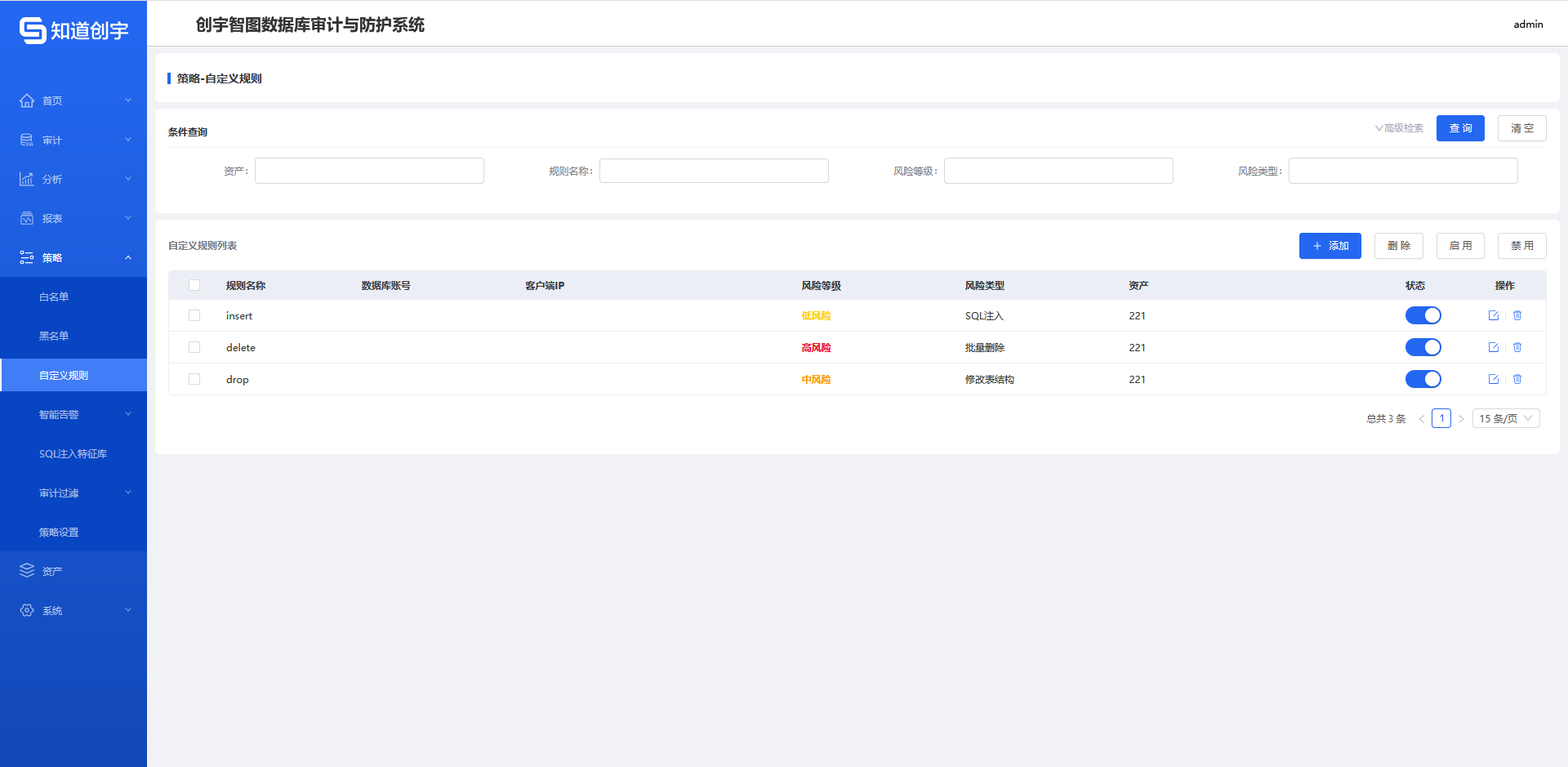
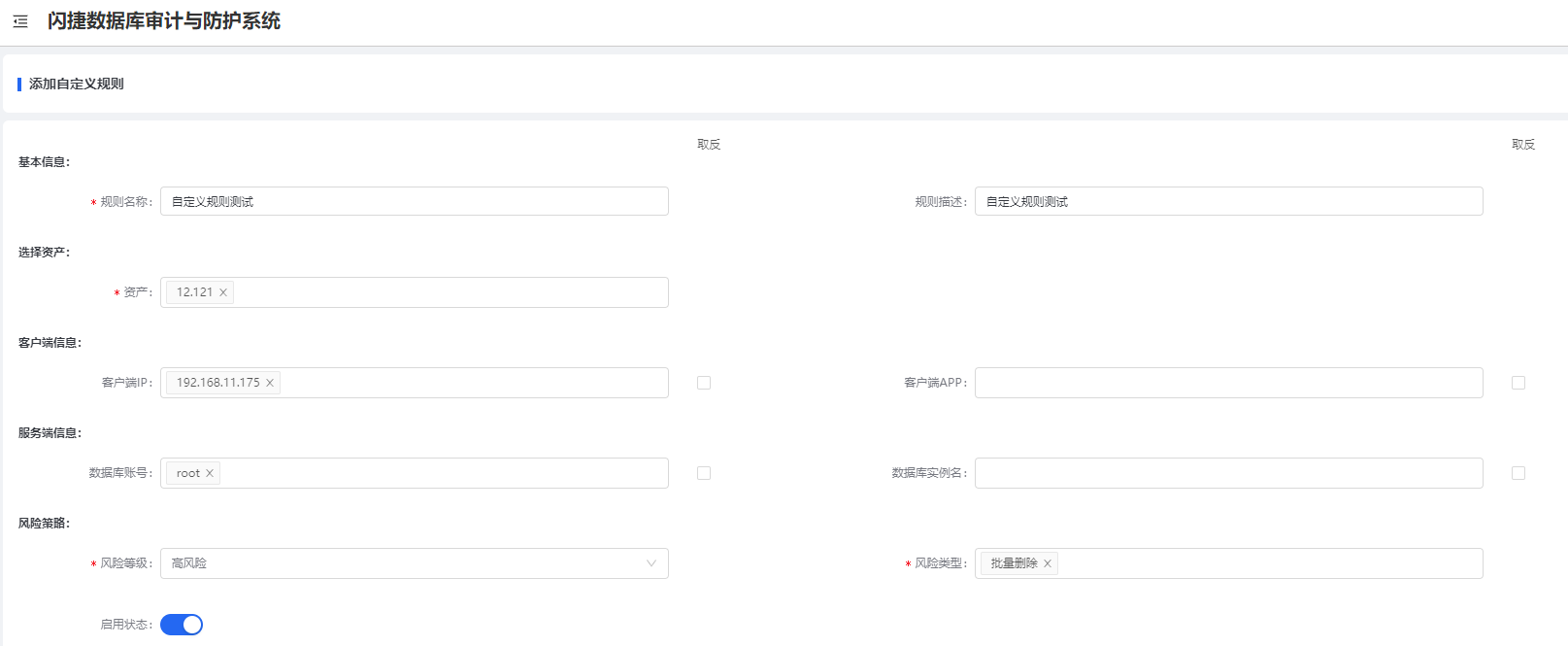
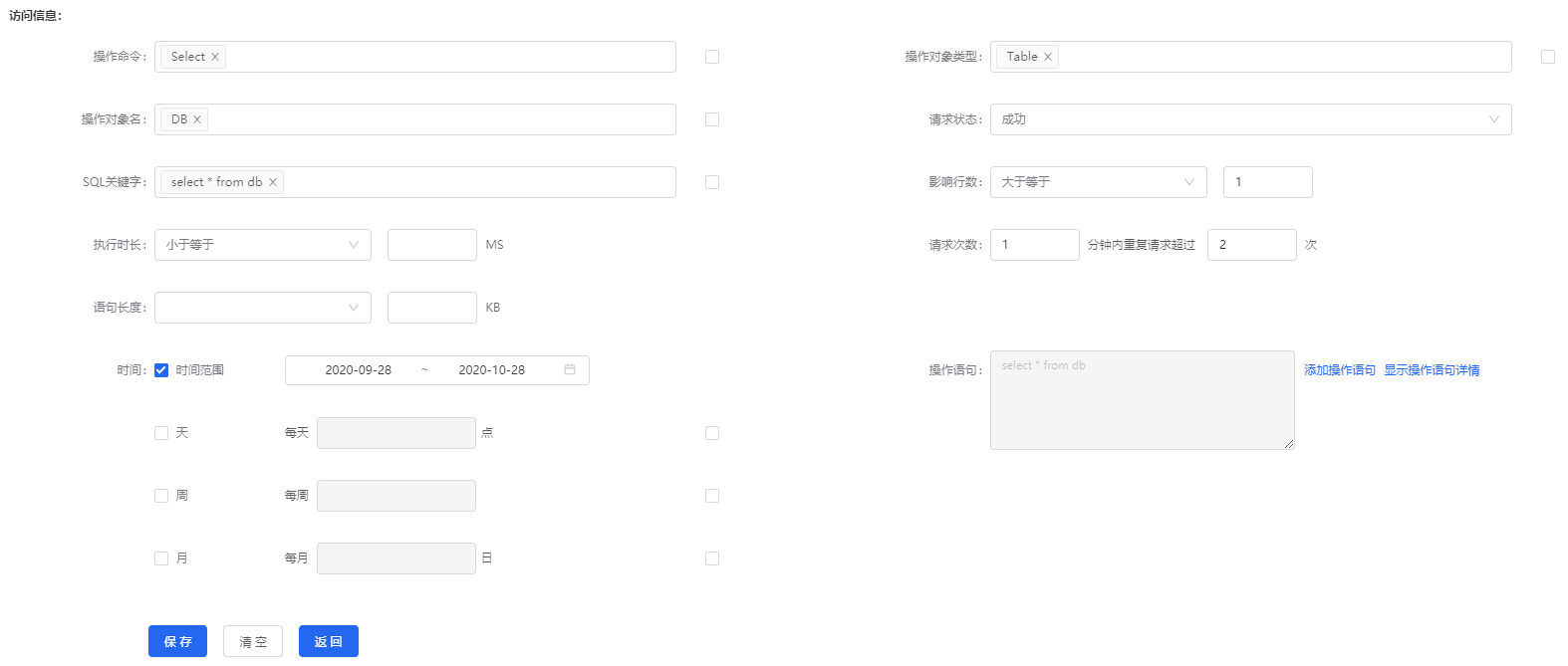


图6-3-1 自定义规则





|  |  |
| --- | --- |
| 字段 | 内容 |
| 规则名称 | 策略的名称 |
| 规则描述 | 策略的规则描述 |
| 资产 | 数据库IP名称，单击空白框，出现资产列表，勾选后配置成功 |
| 客户端IP | 访问数据库的客户端IP，可以通过审计-检索-详情，查看审计日志详情，确定客户端IP |
| 客户端APP | 访问数据库的客户端APP名称，可以通过审计-检索-详情，查看审计日志详情，确定客户端APP |
| 数据库账号 | 数据库登录账号，可以通过审计-检索-详情，查看审计日志详情，确定数据库账号 |
| 数据库实例名 | 数据库登录实例名，可以通过审计-检索-详情，查看审计日志详情，确定数据库实例名 |
| 风险等级 | 配置命中自定义策略的风险等级，有无风险、低风险、中风险和高风险 |
| 风险类型 | 配置命中自定义策略的风险类型，可以选择批量删除、批量修改和登录失败等风险类型，也可以自己配置 |
| 启用状态 | 配置策略开启和关闭 |
| 操作命令 | 访问数据库的SQL关键字，如SELECT、INSERT和DELECT等，不区分大小写，单击空白框，可输入部分单词后选择操作命令，或者输入后单击回车键配置；可以通过审计-检索-详情，查看审计日志详情，确定操作命令 |
| 操作对象类型 | 访问数据库的操作对象类型，单击空白框，出现操作对象类型列表，如TABLE等，不区分大小写，单击空白框，可输入部分单词后选择操作命令，或者输入后单击回车键配置；可以通过审计-检索-详情，查看审计日志详情，确定操作对象类型 |
| 操作对象名 | 访问数据库的操作对象名，不区分大小写，单击空白框，输入后单击回车键配置；可以通过审计-检索-详情，查看审计日志详情，确定操作对象名 |
| 请求状态 | 访问数据库的请求状态，有未知、未应答、成功和失败等，可以通过审计-检索-详情，查看审计日志详情，确定请求状态 |
| SQL关键字 | 访问数据库的请求语句 |
| 影响行数 | 访问数据库返回的应答影响行数，可以通过审计-检索-详情，查看审计日志详情，确定影响行数 |
| 执行时长 | 访问数据库的执行时长，可以通过审计-检索-详情，查看审计日志详情，确定执行时长 |
| 请求次数 | 访问数据库的请求次数，统计配置的时间段内的重复请求次数 |
| 语句长度 | 访问数据库的语句长度 |
| 时间 | 配置审计的时间，支持时间范围、天、周和月四种配置方式 |
| 操作语句 | 访问数据库的操作语句，单击添加操作语句，可以先添加或者勾选已有的操作语句 |

图6-3-2 自定义规则配置



图6-3-3 自定义规则命中示例

注意

取反的意思是，除了填写的不能通过之外其他的都可以。

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

## 智能告警

### 智能告警设置

进入[策略->智能告警->智能告警设置]页面，如图6-4-1所示。在智能告警设置页面，单击<添加>，可以添加资产智能告警，如图6-4-2所示 ，选择资产和学习时间，单击<确定>后开始学习，学习时间结束后，状态开启，智能告警策略生效；选中某条策略，单击<>图标，重新开始学习，单击<>图标，手动停止学习，单击<>图标，查看结果，跳转到[用户行为模型->用户模型列表]，单击<>图标，编辑已有的资产智能告警配置，单击<>图标，删除智能告警策略；查询条件有资产、学习状态和状态，单击<清空>，可以清空查询条件。智能告警功能生效，状态需要在智能告警页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新告警]，查看实时流量检查智能告警策略是否生效，如图6-4-3所示。

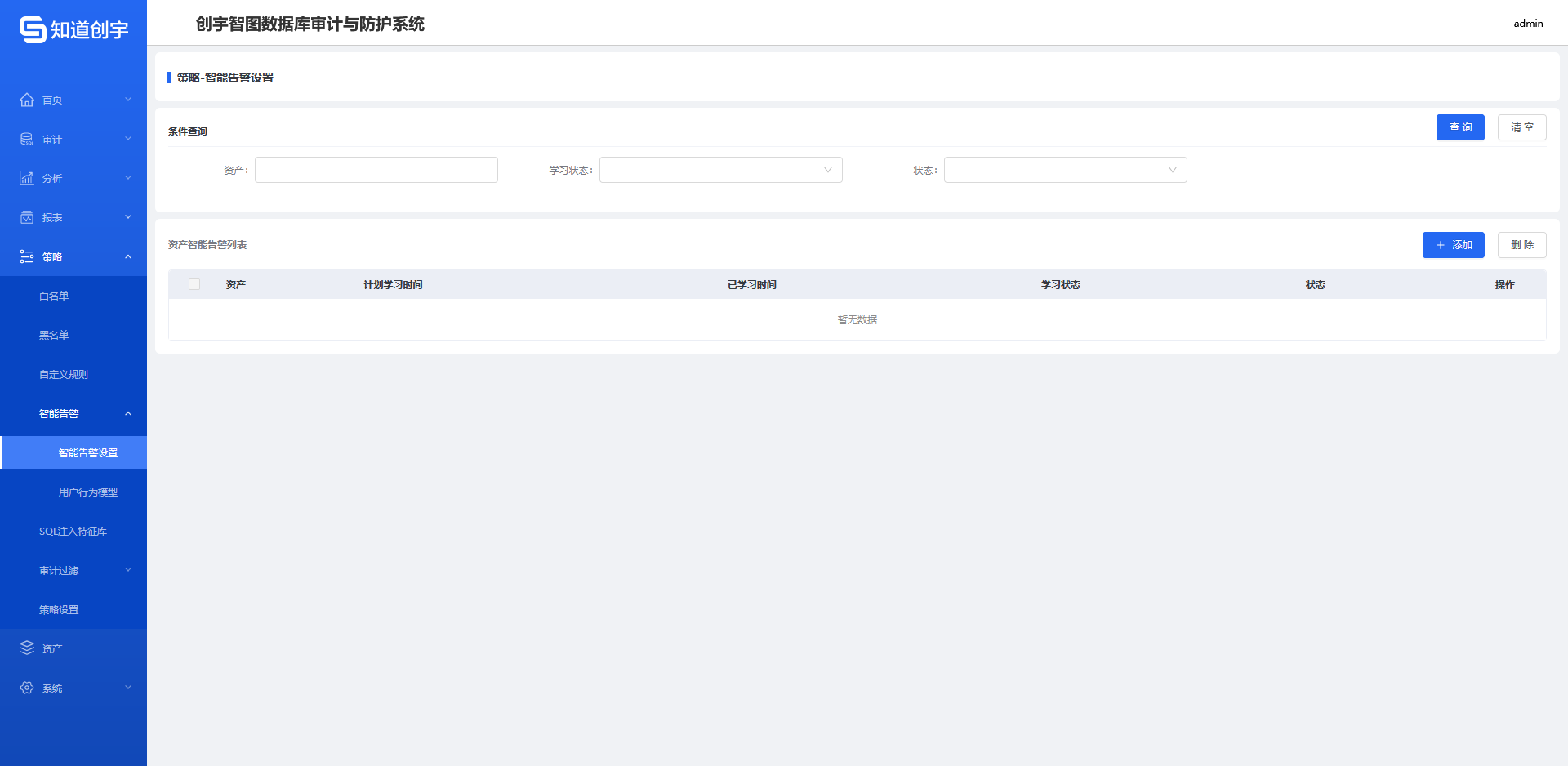


图6-4-1 智能告警



图6-4-2 添加资产智能告警



图6-4-3 智能策略命中示例

注意

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

### 用户行为模型

进入[策略->智能告警->用户行为模型]页面，如图6-4-4所示，有用户模型列表和用户行为列表。在智能告警设置页面，单击<>图标，跳转到[分析->用户行为分析] ，可以查看对应资产的用户行为模型图；单击<>图标，查看对应资产的用户行为列表，如图6-4-5所示；直接进入[策略->智能告警->用户行为模型->用户行为列表]，如图6-4-6所示，显示所有资产的用户行为列表，可以输入查询条件查询用户行为，单击<>图标，将某一用户行为移除基线。

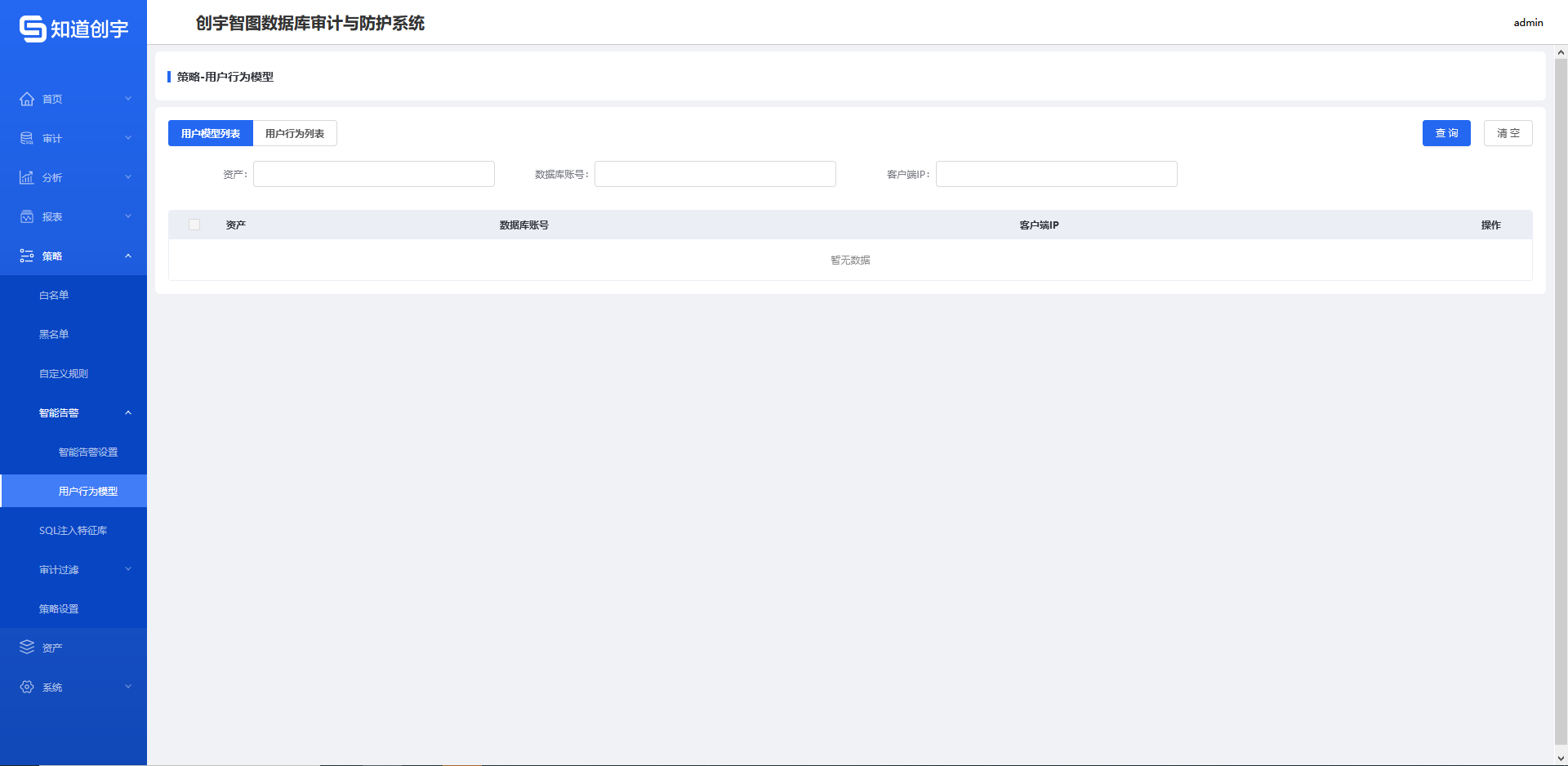


图6-4-4用户模型列表

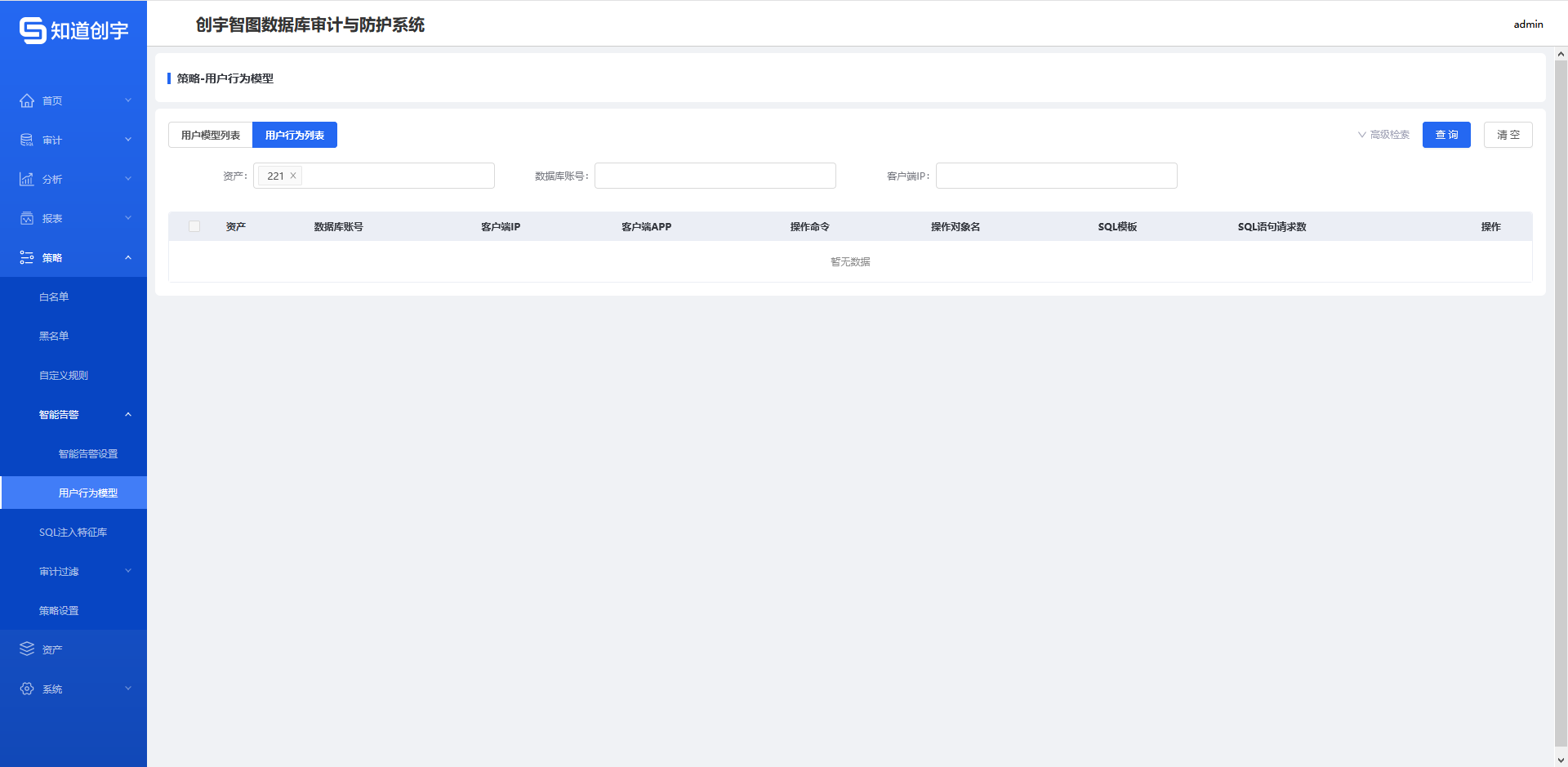


图6-4-5 单个资产的用户行为列表

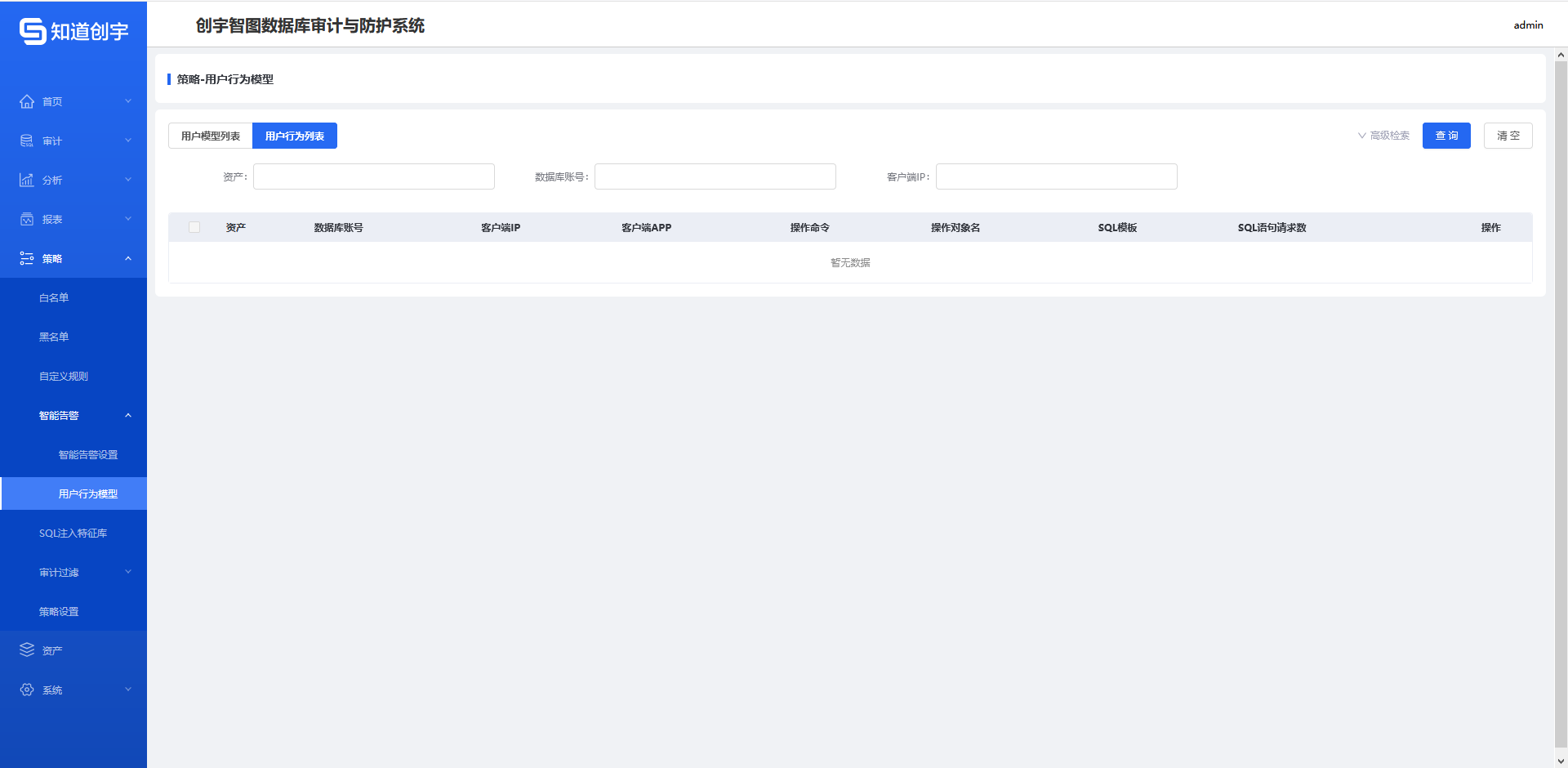


图6-4-6用户行为列表

## SQL注入特征库

进入[策略->SQL注入特征库]页面，如图6-5-1所示，SQL注入特征库有内置45种特征列表，也可以自定义配置。单击<添加>，配置SQL注入特征，如图6-5-2所示。开启状态，SQL注入功能生效；单击<>图标，编辑SQL注入特征库配置，只能调整风险等级和开启状态；单击<>图标，可以删除自定义的SQL注入特征库，但无法删除内置的SQL注入特征库。可以选中SQL注入特征库，单击<启用>和<禁用>，可以批量开启或者关闭SQL注入特征策略，配置SQL注入特征库策略的开启状态；查询条件有规则名称、风险等级、资产类型和状态；单击<清空>，可以清空查询条件。SQL注入特征库功能生效，状态需要在SQL注入特征库页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新请求]，查看实时流量检查智能告警策略是否生效。

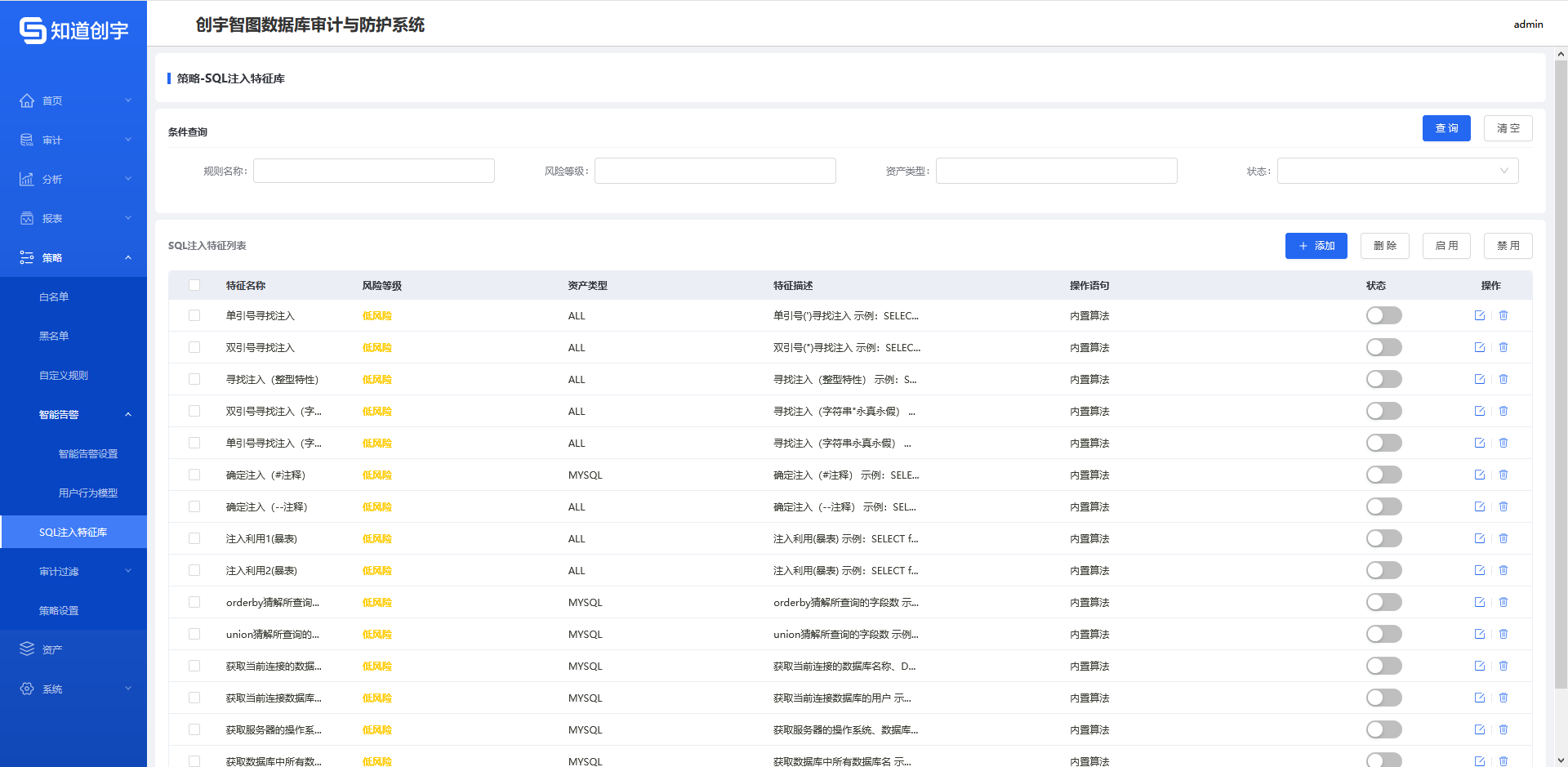


图6-5-1 SQL注入特征库

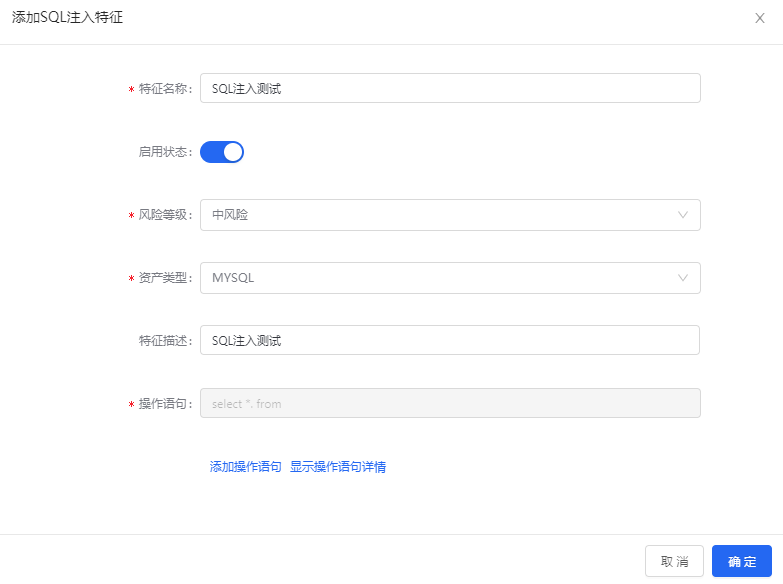


图6-5-2添加SQL注入特征

注意

自定义配置的 SQL注入特征库中操作语句必须配置正则。

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

## 审计过滤

### IP限制

进入[策略->审计过滤->IP限制]页面，如图6-6-1-1所示，审计IP限制模式有IP过滤和IP指定两种，这两种模式同一时间只能存在一种模式。默认是IP过滤模式，单击IP指定，切换到IP指定模式。IP过滤开启后，策略中配置的IP地址（段）在审计系统不进行审计，其它IP段进行审计；IP指定开启后，策略中配置的IP地址（段）进行审计，其它IP段不进行审计。单击<添加>，新增IP限制配置，如图6-6-1-2所示，配置的IP段指的是客户端IP；单击<>图标，编辑IP限制已有配置；单击<>图标，删除IP限制配置；查询条件有IP地址（段）和资产，单击<清空>，可以清空查询条件。IP限制功能生效，状态需要在IP限制页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新请求]，查看实时流量检查IP限制策略是否生效。



图6-6-1-1 IP限制



图6-6-1-2 添加IP限制

注意

IP限制模式有IP过滤和IP指定两种，这两种模式同一时间只能存在一种模式。

IP限制中配置的IP段指的是客户端IP。

### 数据过滤

进入[策略->审计过滤->数据过滤]页面，如图6-6-2所示。匹配数据过滤规则后会在审计系统丢弃，不再进行审计。单击<添加>，新增数据过滤配置，单击<>图标，编辑数据过滤已有配置，单击<>图标，删数据过滤配置；查询条件有规则名称、数据库账号和客户端IP等，单击<清空>，可以清空查询条件。数据过滤功能生效，状态需要在数据过滤页面是开启状态，且在[策略->策略设置]页面也是开启状态。通过[首页->状态监控->最新请求]，查看实时流量检查数据过滤策略是否生效。

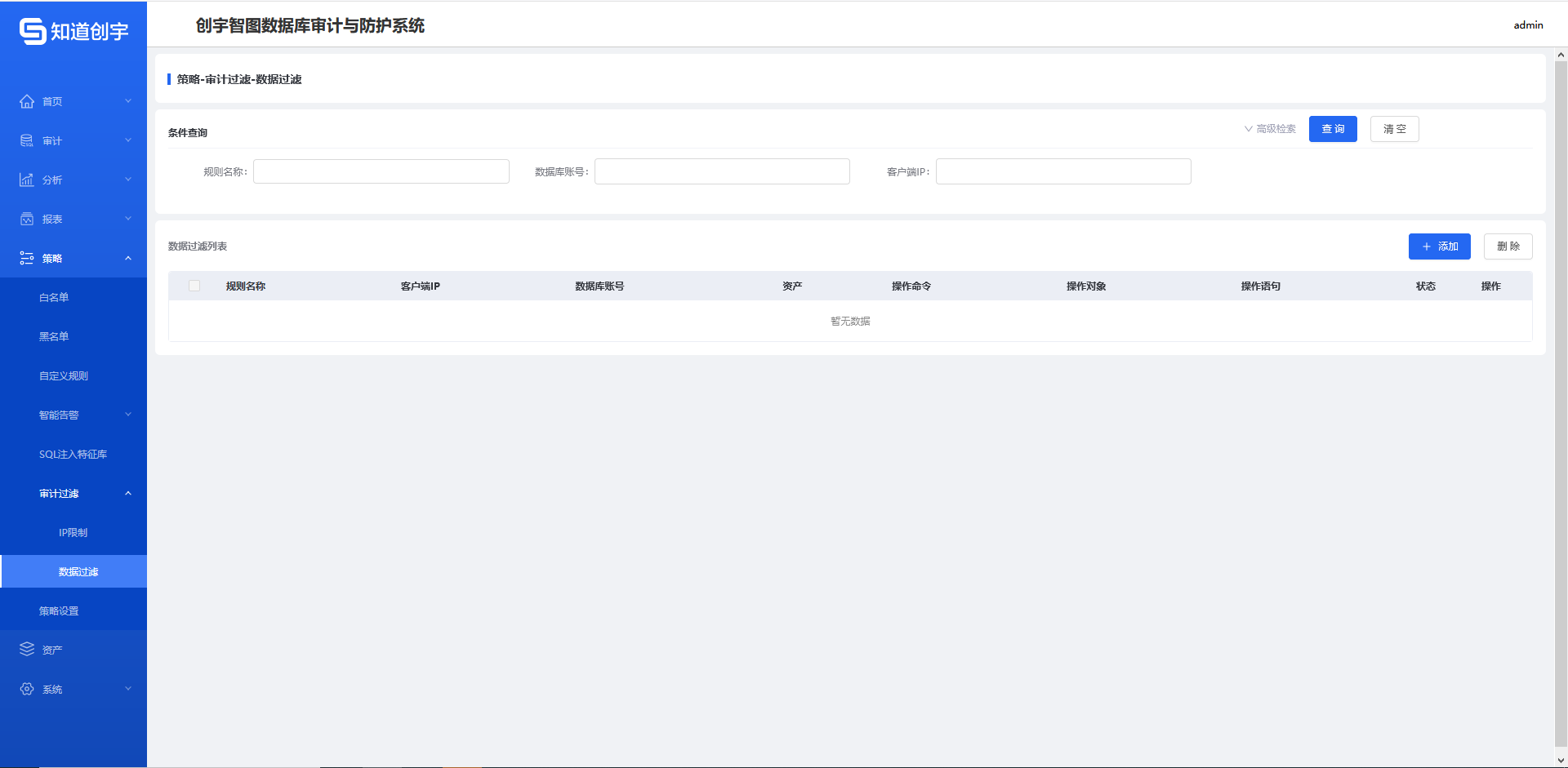


图6-6-2 数据过滤

注意

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

## 策略设置

进入[策略->策略设置]页面，如图6-7-1所示，选择单个资产或资产组，可以看到策略功能优先级顺序，策略命中优先级从高到低分别是审计过滤、白名单、黑名单、自定义规则、SQL注入特征库和智能告警，默认开启白名单、黑名单和自定义规则。如果想要某个策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先。

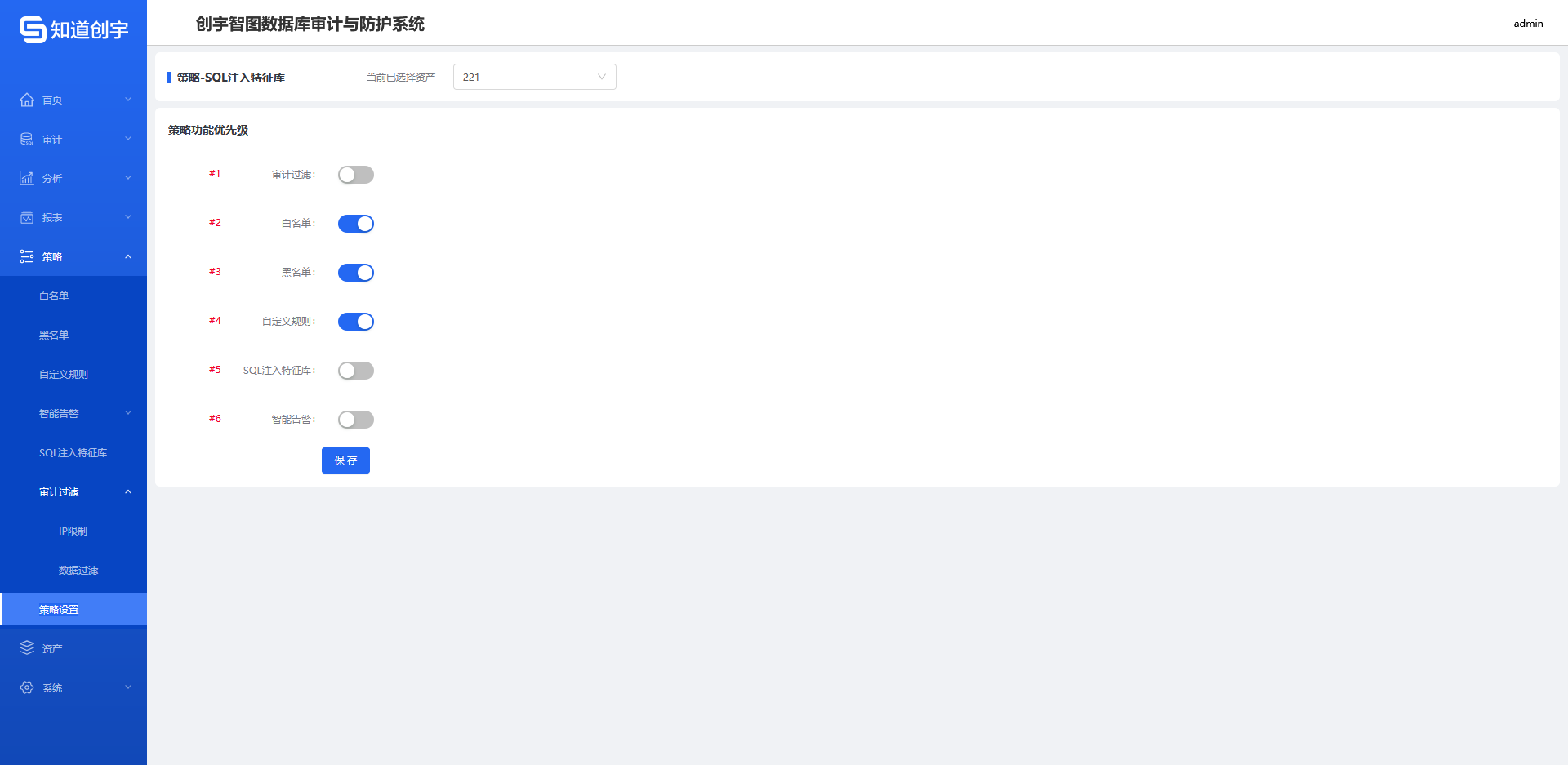


图6-7-1 策略设置

注意

如果想要策略生效，在“策略设置”中策略处于开启状态，同时注意命中优先级。

策略功能优先级：审计过滤 > 白名单 > 黑名单 > 自定义规则 >SQL注入特征库> 智能告警。

# 资产

进入[资产]页面，如图7-1-1所示，添加资产有两种方式，一种是自动发现资产，另外一种是手动添加。

单击<自动发现资产>，如图7-1-2所示，开启自动发现资产功能，选择一级分组和资产类型，在同一网络有数据库流量时可以自动发现资产，资产名称以A+资产IP命名。单击<添加>，如图7-1-3所示，手动添加资产。单击<>图标，编辑资产配置，单击<>图标，删除资产配置。勾选资产，单击<启用>，开启资产保护状态，单击<禁用>，关闭资产保护状态。输入查询条件，可以搜索资产，单击<清空>，清空查询条件。单击<更新地址>，手动更新配置域名的资产地址，默认一天更新一次配置域名的资产地址。



图7-1-1 资产



图7-1-2 自动发现数据库



|  |  |
| --- | --- |
| 字段 | 内容 |
| 资产名称 | 添加资产的名称 |
| 一级分组 | 添加资产的一级分组，有SQL、大数据和网络三类 |
| 二级分组 | 添加资产的二级分组，有ORACLE、SQLSERVER、MYSQL、DB2等 |
| 资产类型 | 添加资产的资产类型，有ORACLE、SQLSERVER、MYSQL、DB2等 |
| 资产地址 | 添加资产的资产地址，支持配置IP地址和域名 |
| 端口 | 添加资产的数据库端口 |
| 编码方式 | 添加资产的数据库使用的编码方式，默认是AUTO，自动识别 |
| 描述 | 添加资产的信息描述 |
| 版本 | 添加资产的数据库版本 |
| 数据库账号 | 添加资产的数据库账号 |
| 密码 | 添加资产的数据库密码 |
| 服务名 | 添加资产的数据库服务名 |
| 是否双向审计 | 选择“是”，则对请求和应答双向进行审计；选择“否”，则只对请求进行单向审计 |
| 是否显示返回集 | 选择“是”，则审计日志中可以看到返回的结果集；选择“否”，则审计日志中不能看到返回的结果集 |
| 是否使用加密 | 选择“是”，上传秘钥文件，则可以对加密的SQLSERVER数据库进行审计；选择“否”，则无法对加密的SQLSERVER数据库进行审计 |
| 保护状态 | 审计开启的开关 |

图7-1-3 添加资产

注意

资产地址支持使用域名，默认一天更新一次地址，可以手动更新。

资产地址配置域名后，需要在网卡设置中的管理口网卡上配置DNS。

# 系统

## 基础设置

进入[系统->基础设置]页面，如图8-1-1所示，看到平台信息，可以看到产品名称、系统版本、引擎版本、系统时间、开机时间、序列号、生成厂商、服务电话、厂商网站和厂商地址。单击<>图标，可以修改系统时间并配置时间同步服务器的IP地址，如图8-1-2所示。

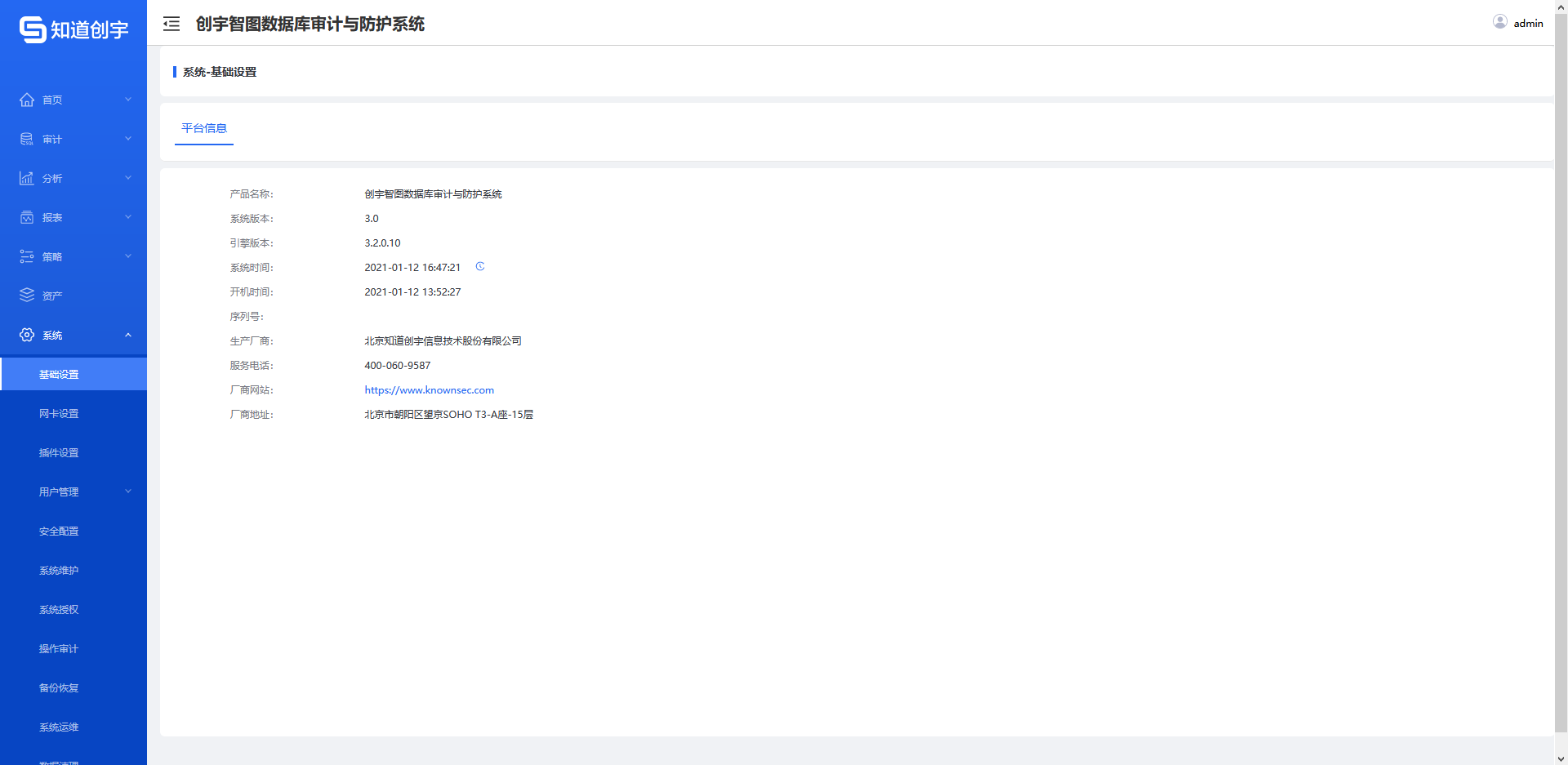


图8-1-1 平台信息

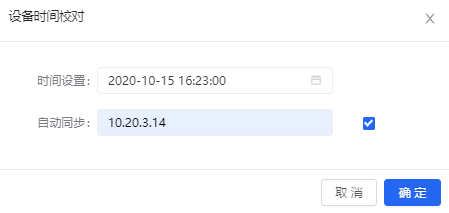


图8-1-2 设备时间校对

## 网卡设置

进入[系统->网卡设置]页面，如图8-2-1所示，通过网卡状态，可以通过图标看出启用状态、网卡类型和连接状态；通过网卡状态列表，可以看到网口名称、网口显示名称、网口类型、IP地址、MAC地址、连接状态和启用状态的详情。单击<>图标，编辑网口配置，如图8-2-2所示，选择网口类型，如果是管理口，网卡类型选择管理口，配置网关地址和掩码，配置主备DNS；如果是旁路审计网口，网卡类型选择审计口。

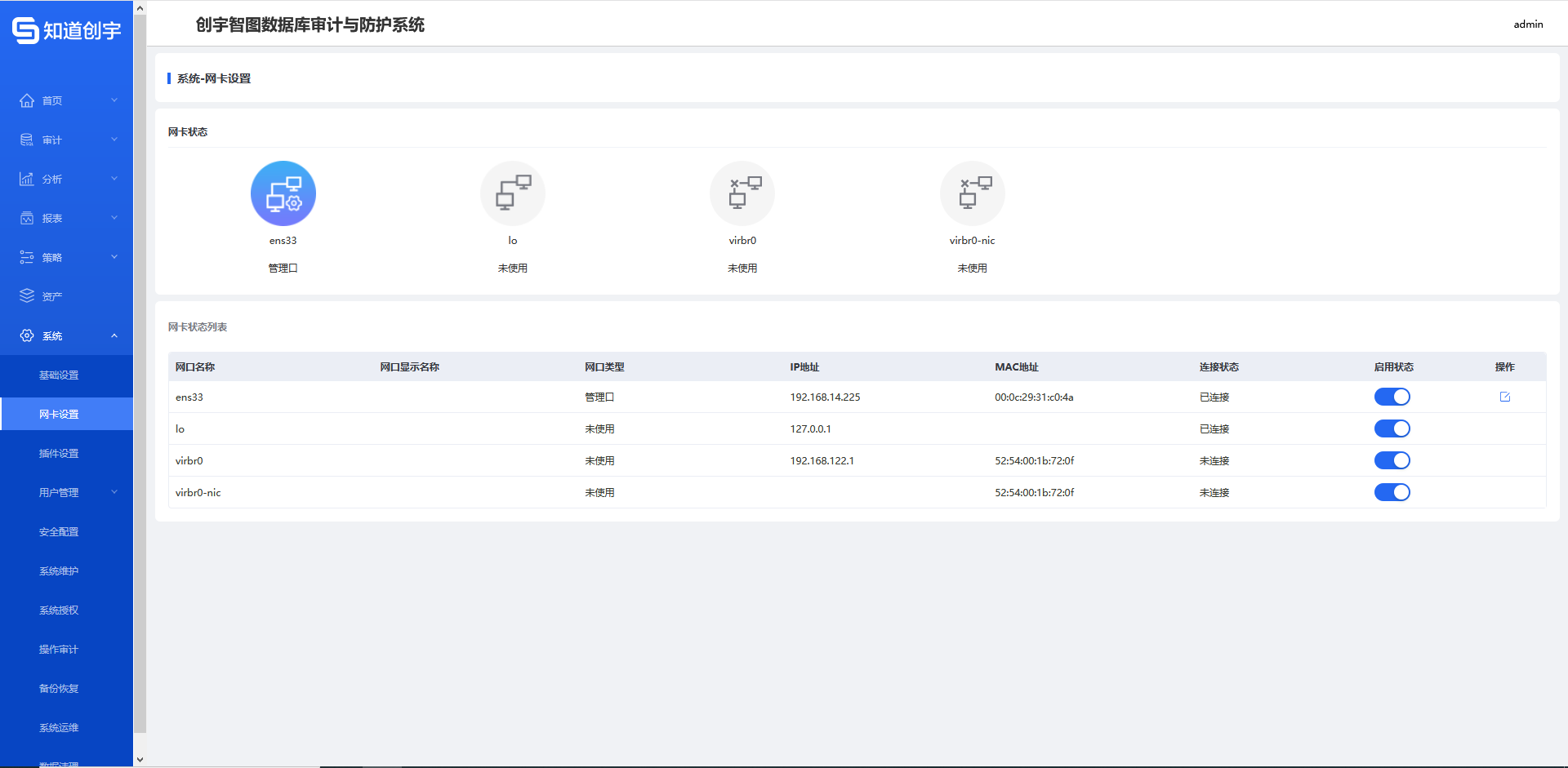


图8-2-1 网卡设置



图8-2-2 编辑网口

## 插件设置

### 插件安装

进入[系统->插件设置->插件安装]页面，如图8-3-1所示，支持Unix、Windows和Linux三种操作系统的插件，单击<下载>，下载不同版本的插件，在不同的客户端下手动安装插件；单击<复制下载地址链接>，打开浏览器，复制地址，下载不同版本的插件，在不同的客户端下手动安装插件。单击<添加插件推送>，可以自动安装插件，可以在推送状态列表看到安装进度和状态。单击<>图标，安装插件；单击<>图标，卸载插件；单击<>图标，编辑插件推送配置；单击<>图标，删除插件推送配置。

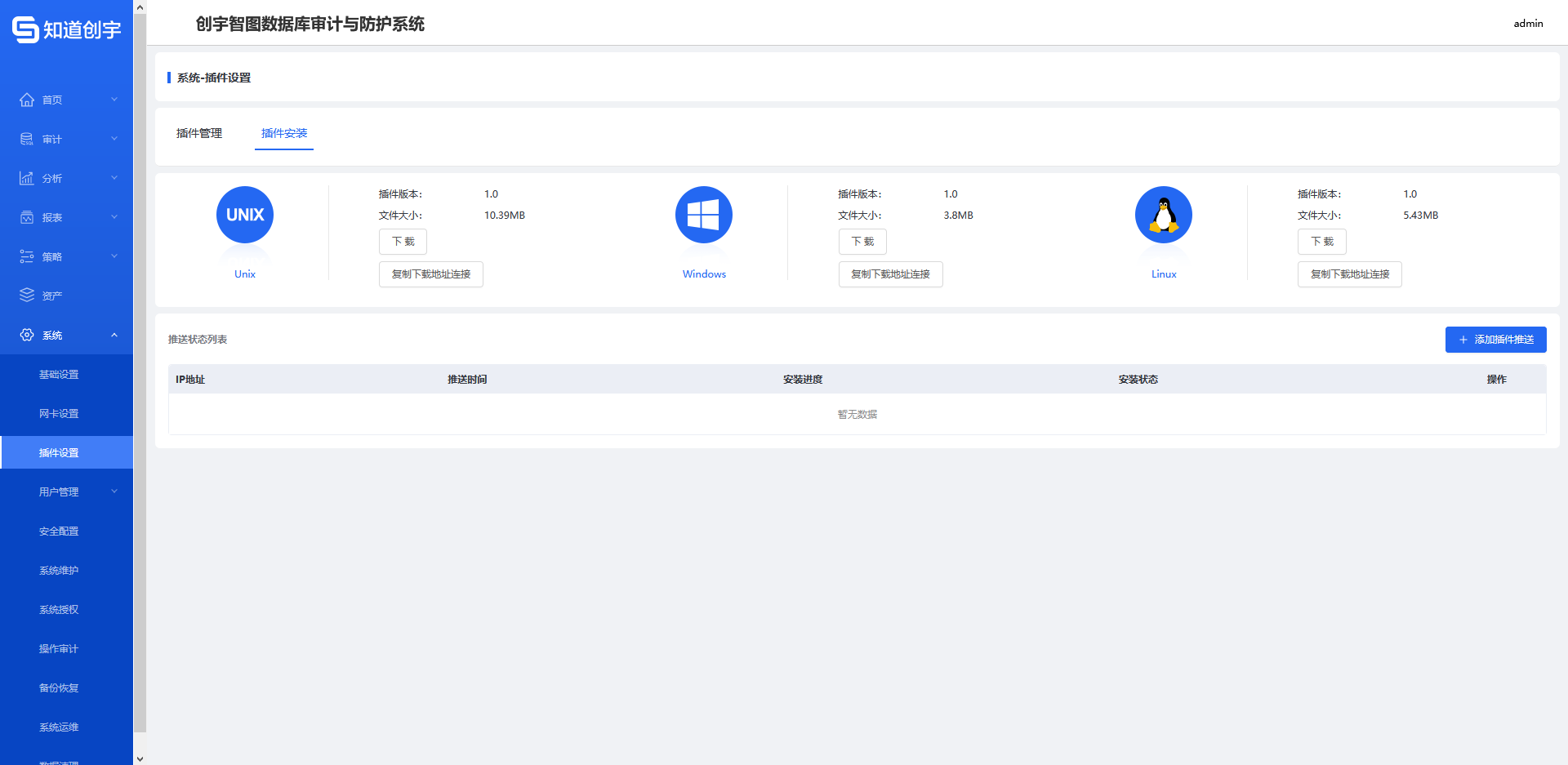


图8-3-1 插件安装



|  |  |
| --- | --- |
| 字段 | 内容 |
| IP地址 | 安装插件的数据库IP地址 |
| 端口 | SSH端口，一般默认是22 |
| 验证方式 | 登录SSH方式，有口令和证书两种 |
| 系统账号 | 安装插件的数据库系统账号 |
| 系统密码 | 安装插件的数据库系统密码 |
| 默认安装 | 勾选后自动安装 |

图8-3-2 添加插件推送

说明

插件手动安装，进入解压后的插件安装包路径，找到readme.txt文件，按照操作步骤进行安装。

### 插件管理

进入[系统->插件设置->插件管理]页面，如图8-3-3所示，插件安装后，在插件管理列表中可以看到安装成功的插件；单击<添加插件推送>，可以自动安装插件，可以在推送状态列表看到安装进度和状态。单击<>图标，查看插件绑定的资产详情，如图8-3-4所示，可以开启关闭插件，并删除资产绑定；单击<>图标，绑定资产，如图8-3-5所示；单击<>图标，设置安装插件数据库的CPU和内存阈值，超过阈值后，不再进行流量采集，如图8-3-6所示；单击<>图标，删除关闭状态的插件。

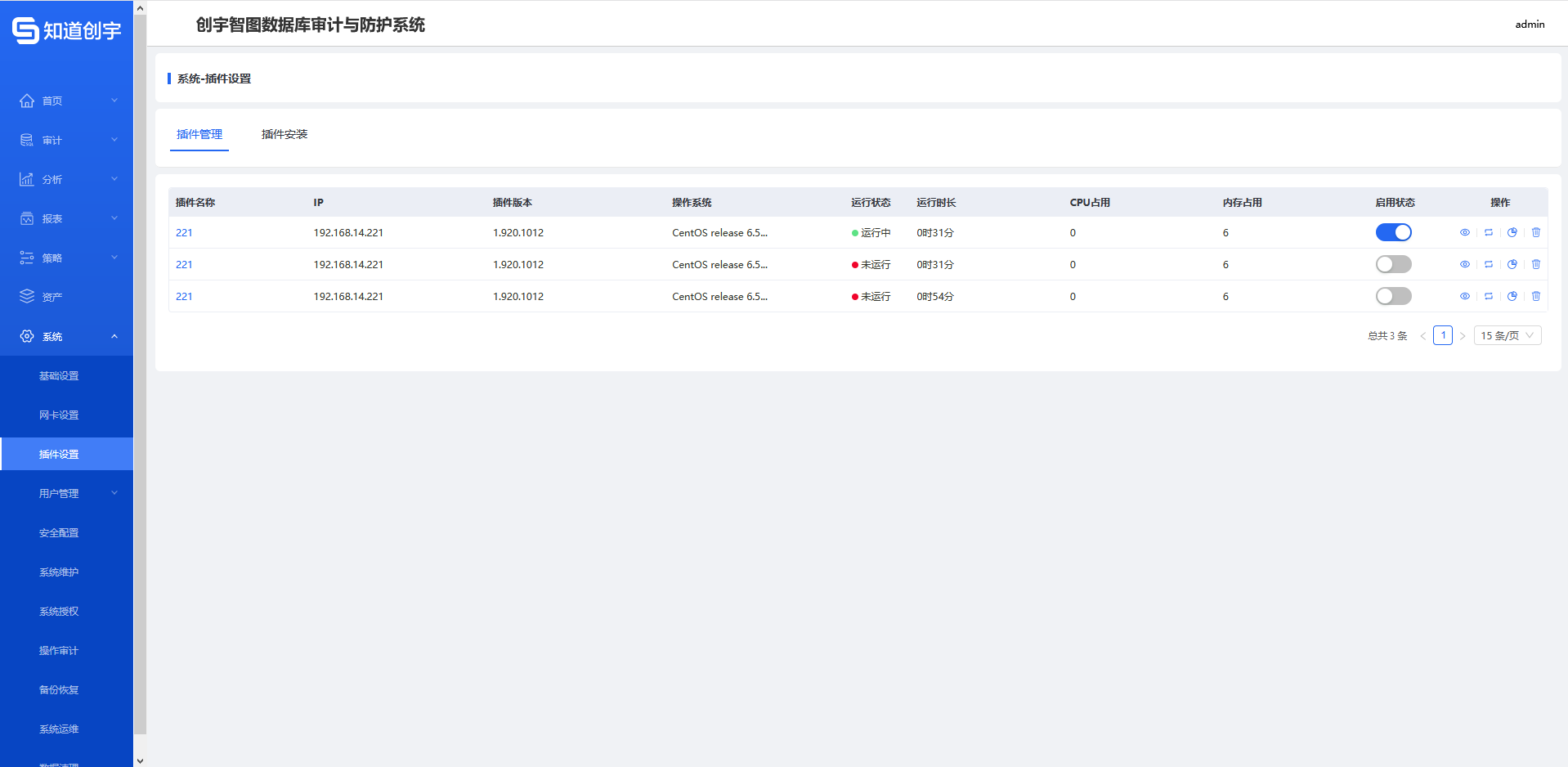


图8-3-3 插件管理

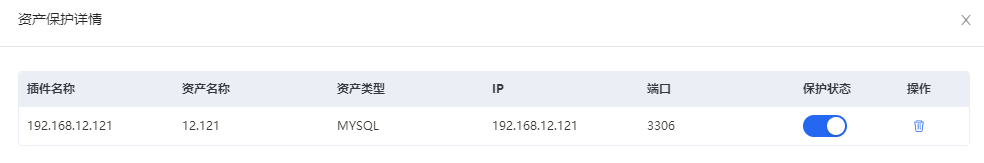


图8-3-4 资产保护详情

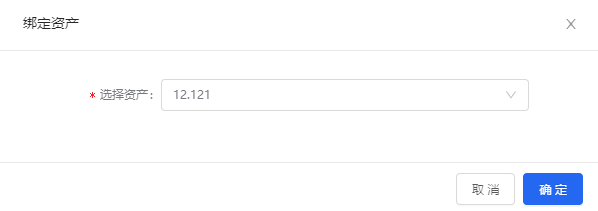


图8-3-5 绑定资产

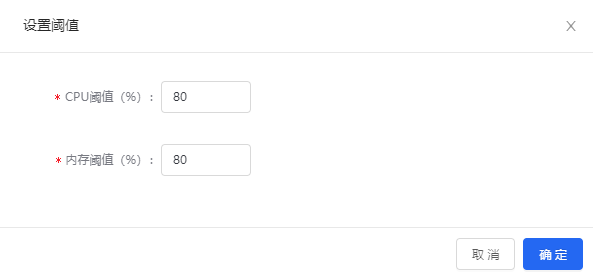


图8-3-6 设置阈值

## 用户管理

### 账号管理

进入[系统->用户管理->账号管理]页面，如图8-4-1所示，系统存在4个默认的本地用户账号，角色不同，不能进行账号编辑和删除。单击<创建账号>，配置新账号，如图8-4-2所示；单击<导入>，下载导入账号模板，批量导入账号，如图8-4-3所示；选中用户创建的账号，单击<删除>，删除账号；单击<>，刷新页面；单击<>，编辑账号列表列展示的内容；单击<>，设置账号列表行高；单击<>，编辑用户创建的账号；单击<>，删除用户创建的账号。新建的账号当前状态是“未审核”时，在[平台管理->账号审核->手动审核]，选中账号单击<通过>或者<拒绝>。搜索条件有账号、角色、使用人和时间范围。用户创建的账号忘记密码时，单击<初始化密码>，将用户创建的账号密码初始化到123456。

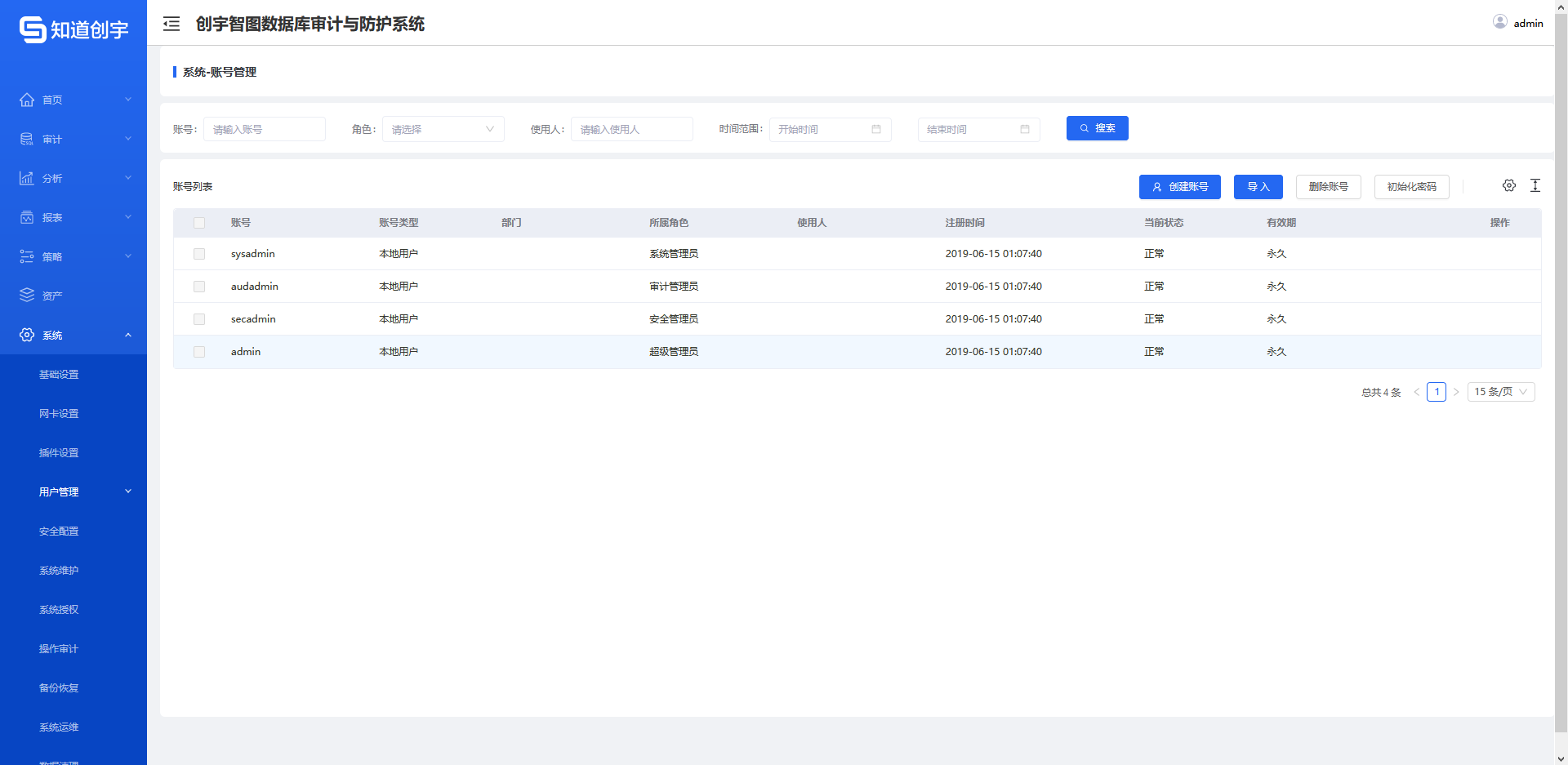


图8-4-1 账号管理



图8-4-2 创建账号



图8-4-3 导入账号信息

注意

新建的账号需要在[系统->用户管理->账号审核]中手动审核通过才会生效。

### 角色管理

进入[系统->用户管理->角色管理]页面，如图8-4-5所示，系统存在4个默认的角色，角色权限不同，不能进行角色编辑和删除。单击<创建角色>，配置新角色；选中用户创建的角色，单击<删除角色>，删除角色；单击<>，刷新页面；单击<>，编辑角色列表列展示的内容；单击<>，设置角色列表行高；单击<查看角色权限>，查看角色对应的权限；单击<>，编辑用户创建的角色；单击<>，删除用户创建的角色。搜索条件有角色名称、创建者和时间范围。

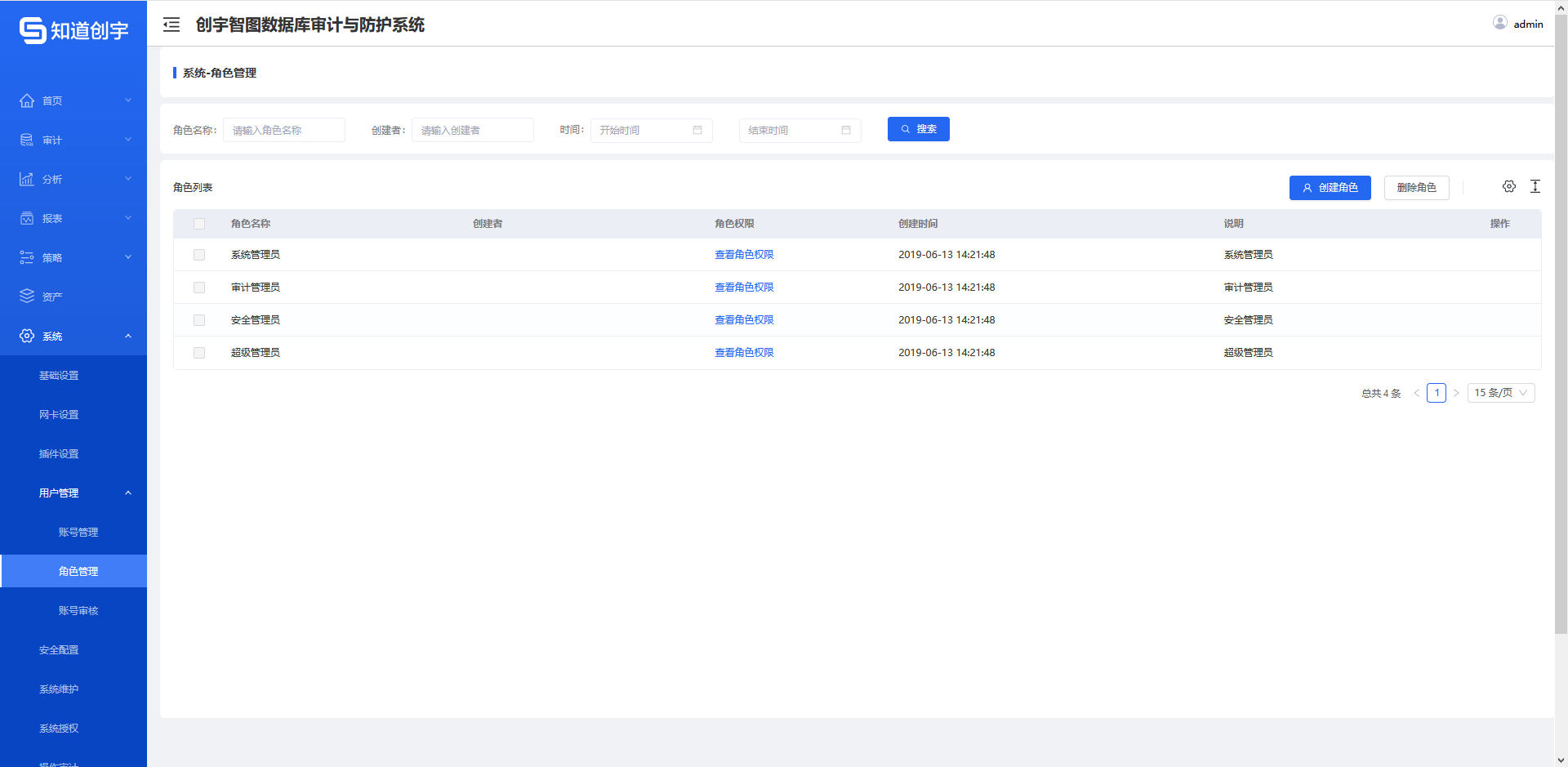


图8-4-5角色管理

### 账号审核

进入[系统->用户管理->角色管理]页面，如图8-4-6所示，在账号管理中用户创建的账号需要手动审核或者自动审核。

在自动审核页面，如图8-4-7所示，选中账号，单击<自动审核>，自动审核状态从“否”变为“是”，使用此账号登录创建的账号状态自动审核通过，不需要手动审核；单击<撤销自动审核>，自动审核状态从“是”变为“否”，使用此账号登录创建的账号状态需要手动审核才能使用；单击<>，刷新页面；单击<>，编辑账号列表列展示的内容；单击<>，设置账号列表行高。搜索条件有账号、所属角色、使用人和创建者。

在手动审核页面，单击<通过>，账号管理页面账号的当前状态从“未审核”变为“正常”，账号可以使用；单击<拒绝>，账号管理页面账号的当前状态从“未审核”变为“审核不通过”，账号不可以使用；单击<>，刷新页面；单击<>，编辑账号列表列展示的内容；单击<>，设置账号列表行高。搜索条件有角色名称、创建者和时间范围。

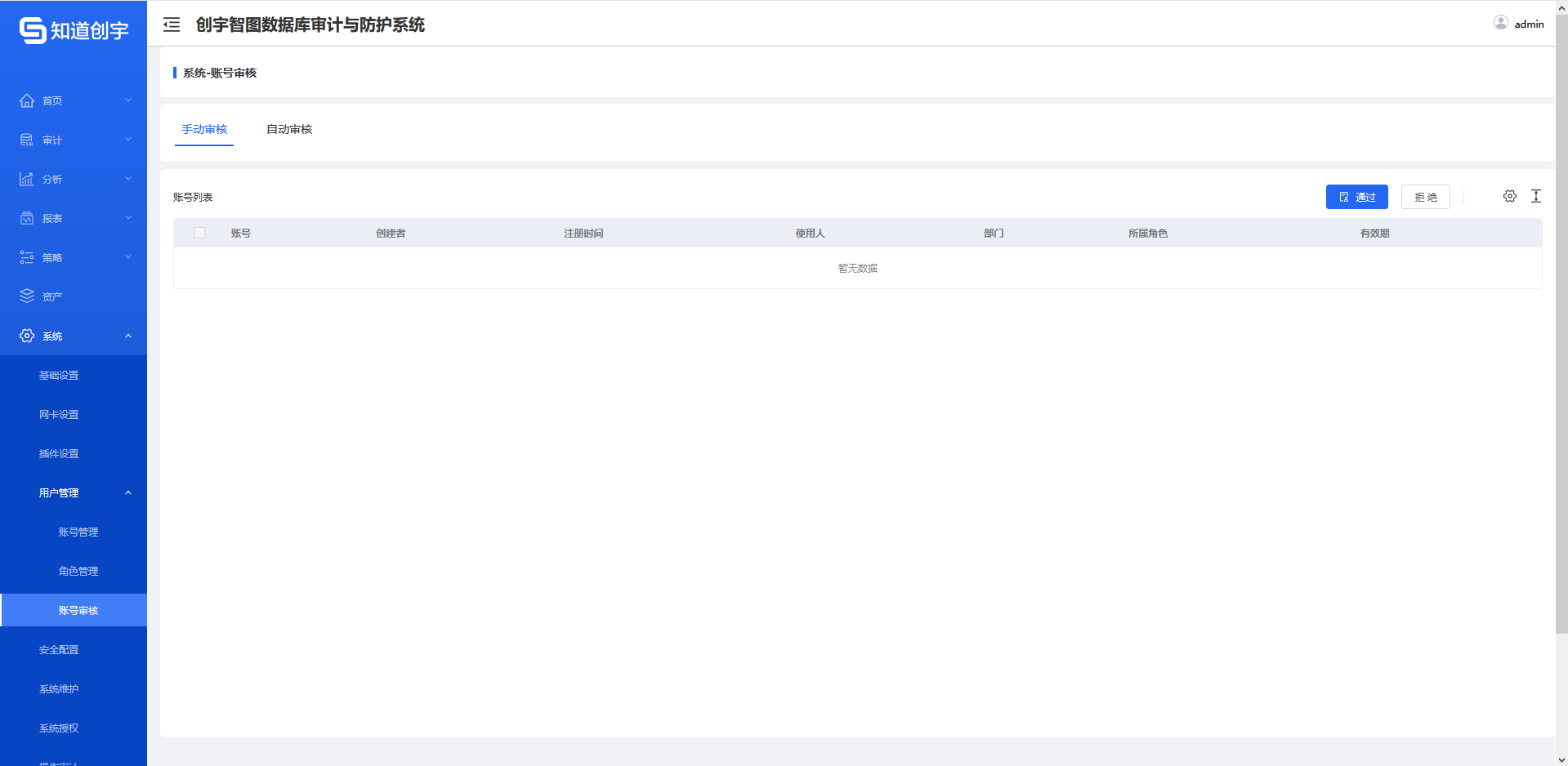


图8-4-6 账号审核-手动审核

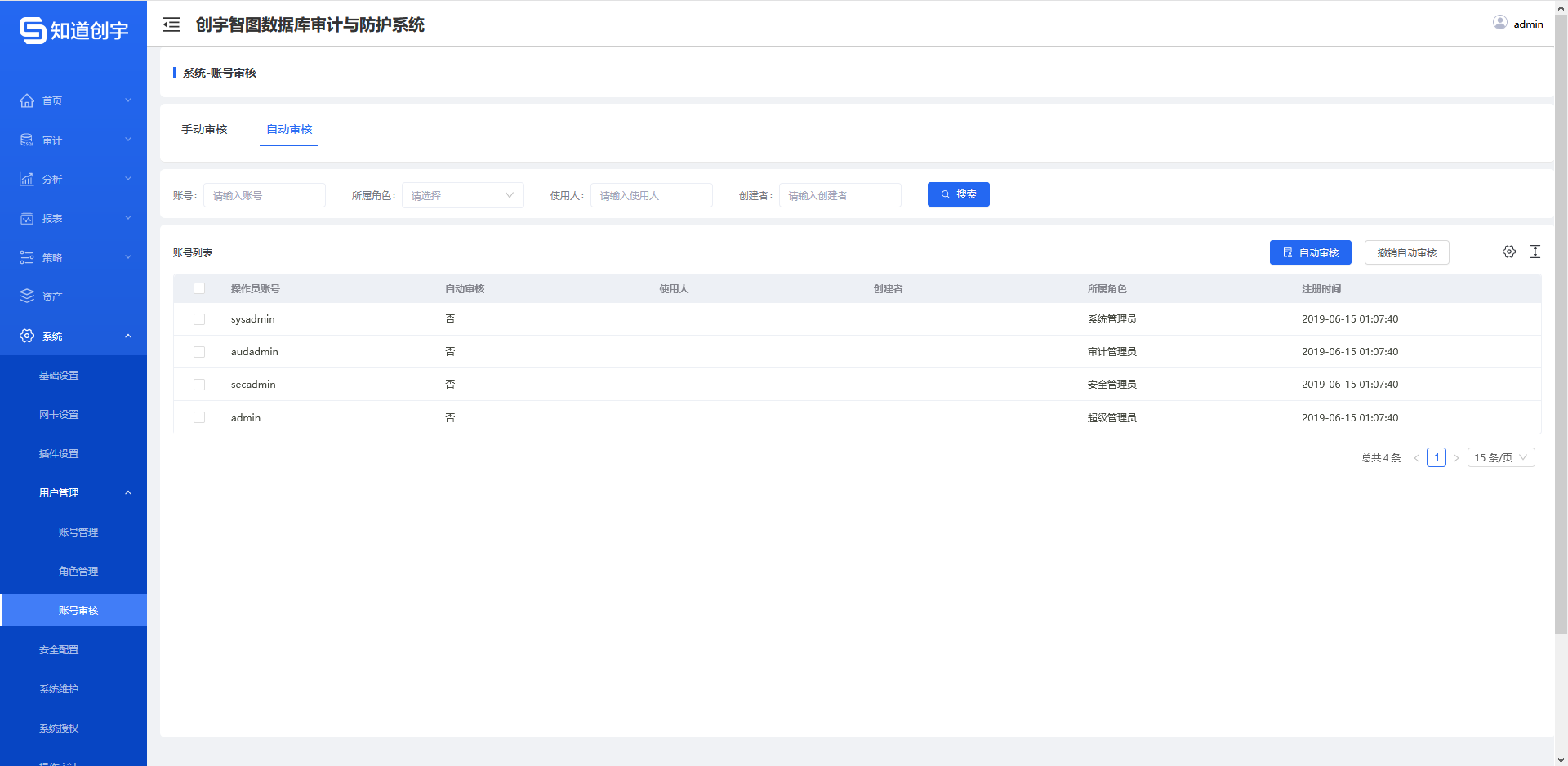
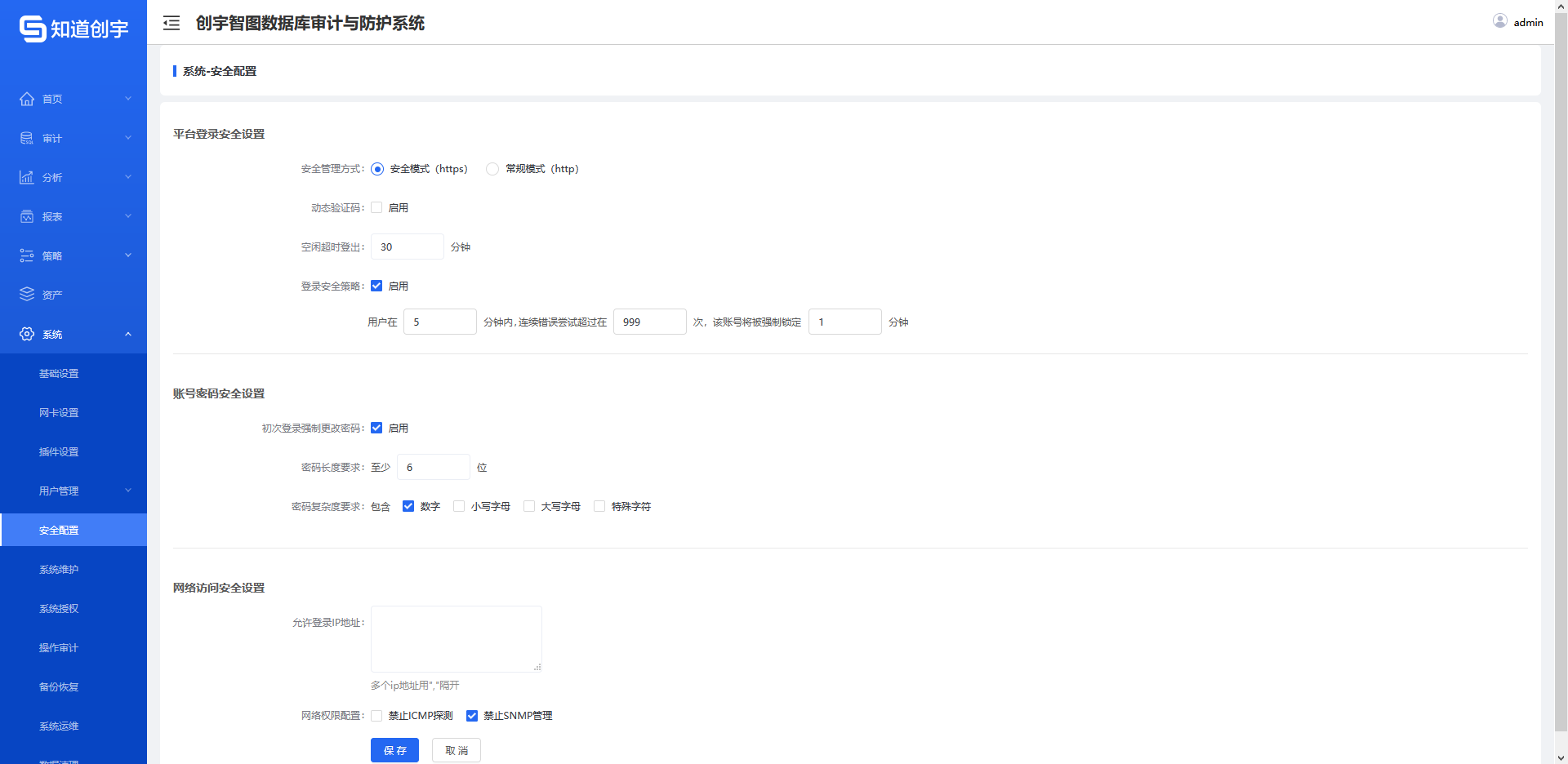


图8-4-7账号审核-自动审核

## 安全配置

进入[系统->安全配置]页面，如图8-5-1所示，对系统进行安全配置。



|  |  |
| --- | --- |
| 字段 | 内容 |
| 安全管理方式 | 系统登录方式有HTTPS和HTTP两种，默认使用https安全模式 |
| 动态验证码 | 启用后，系统登录时，输入正确的动态验证码是必要条件之一，可以防暴力破解密码 |
| 登录闲时超出 | 配置登录超时时间 |
| 登录安全策略 | 启用登录安全策略后，可以防暴力破解密码 |
| 初次登录强制更改密码 | 默认启用，增加账号安全 |
| 密码长度要求 | 对登录密码长度要求，建议至少6位 |
| 密码复杂度要求 | 出于安全考虑，建议包含数字、小写字母、大写字母和特殊字符，设置密码时不满足要求会有提示 |
| 允许登录IP地址 | 设置登录IP白名单，白名单内的可以登录成功，白名单外的不可以登录 |
| 网络权限配置 | 禁止后，关闭ICMP和SNMP功能 |

图8-5-1 安全配置

## 系统维护

进入[系统->系统维护]页面，如图8-6-1所示，对系统进行操作维护。单击<重启服务>，服务重启；单击<重启设备>，设备重启；单击<关闭设备>，设备关机。

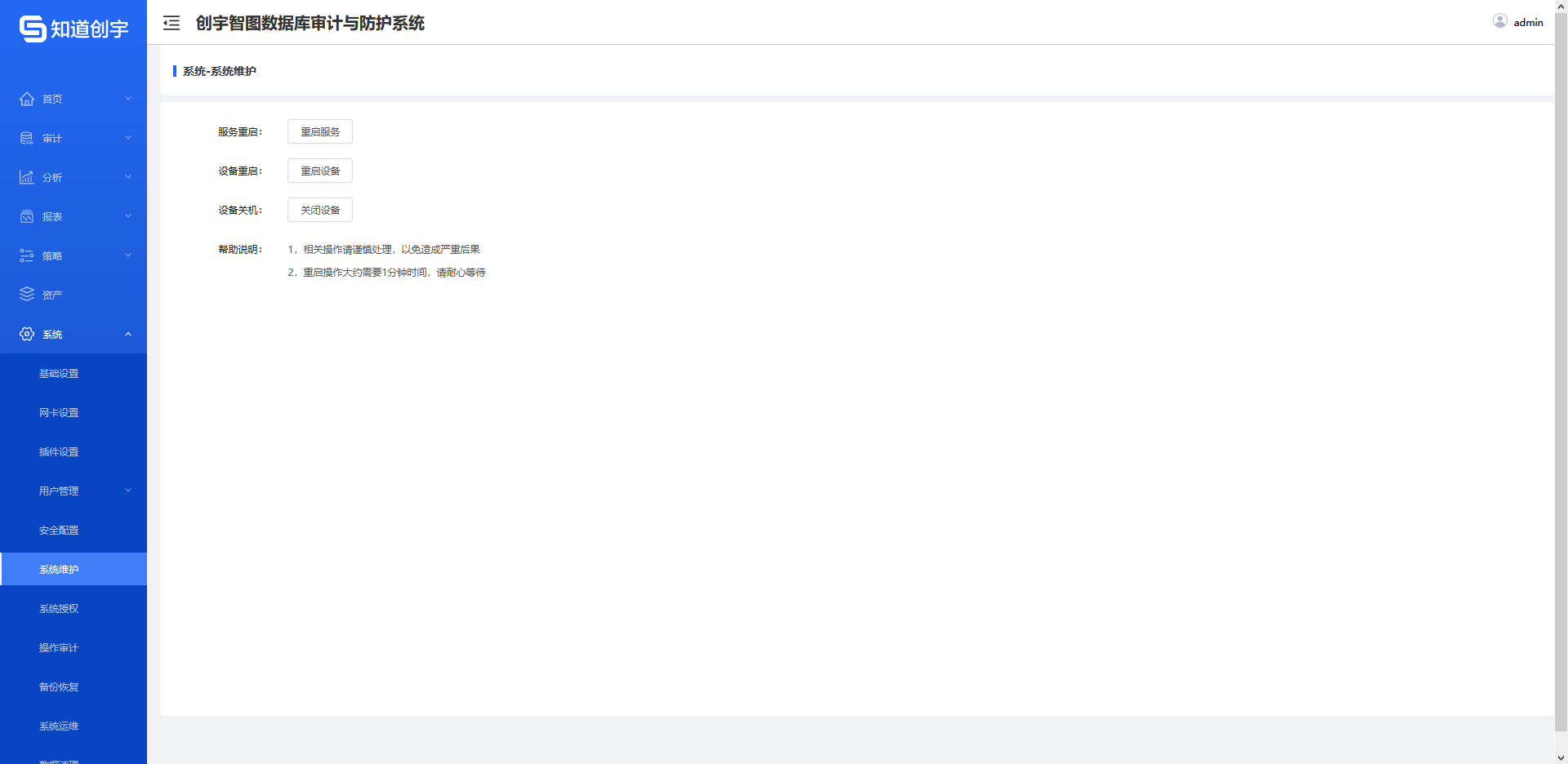


图8-6-1 系统维护

## 系统授权

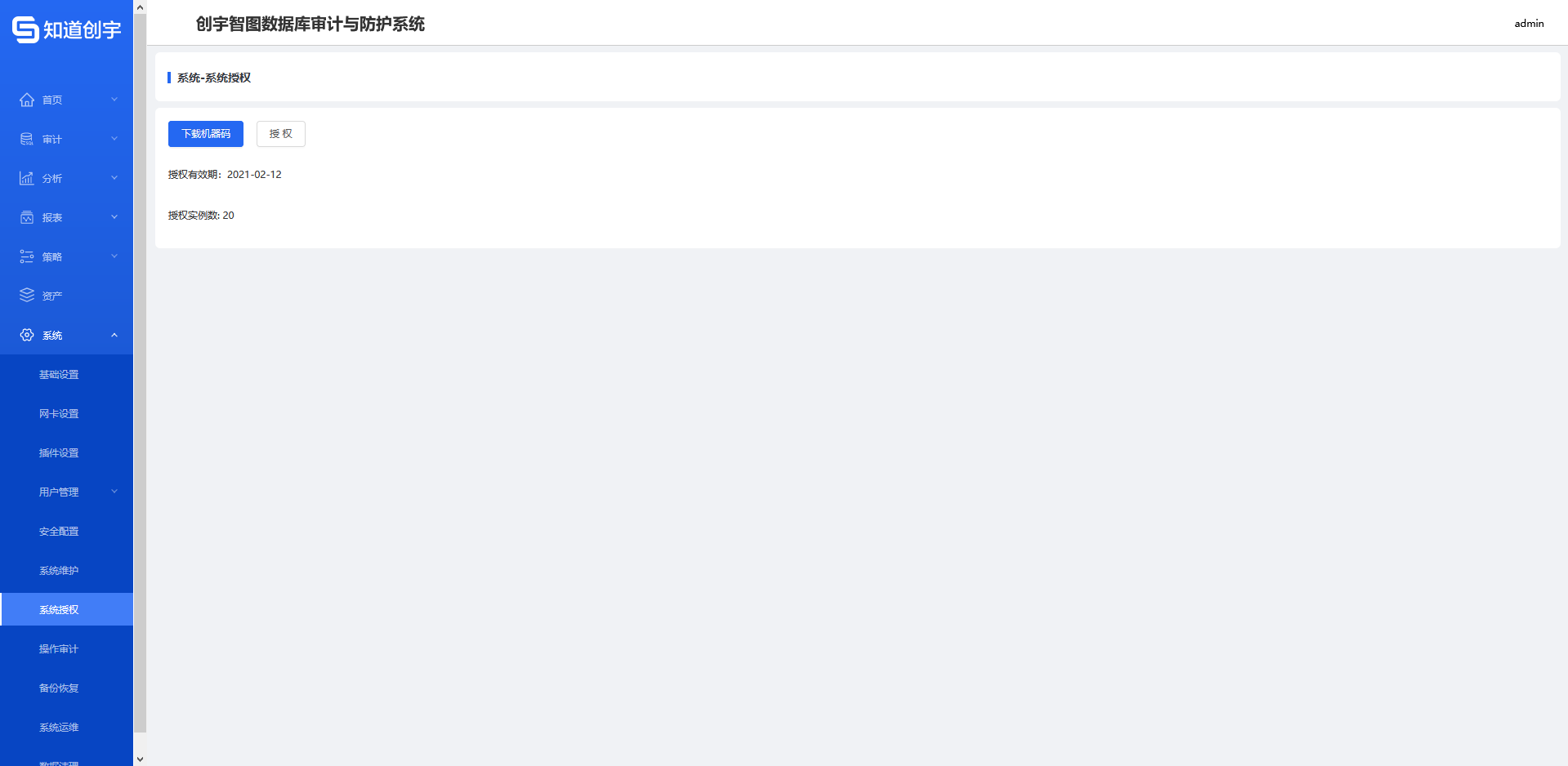


图8-7-1 系统授权

## 操作审计

进入[系统->操作审计]页面，如图8-8-1所示，可以查看系统操作日志。通过账号、使用人、IP地址、关键字、开始时间或结束时间搜索操作日志。单击<详情>，查看操作日志详情，如图8-8-2所示。单击<>图标，刷新页面；单击<>图标，设置列展示；单击<>图标，设置行间距，支持中等、默认和大三种间距。

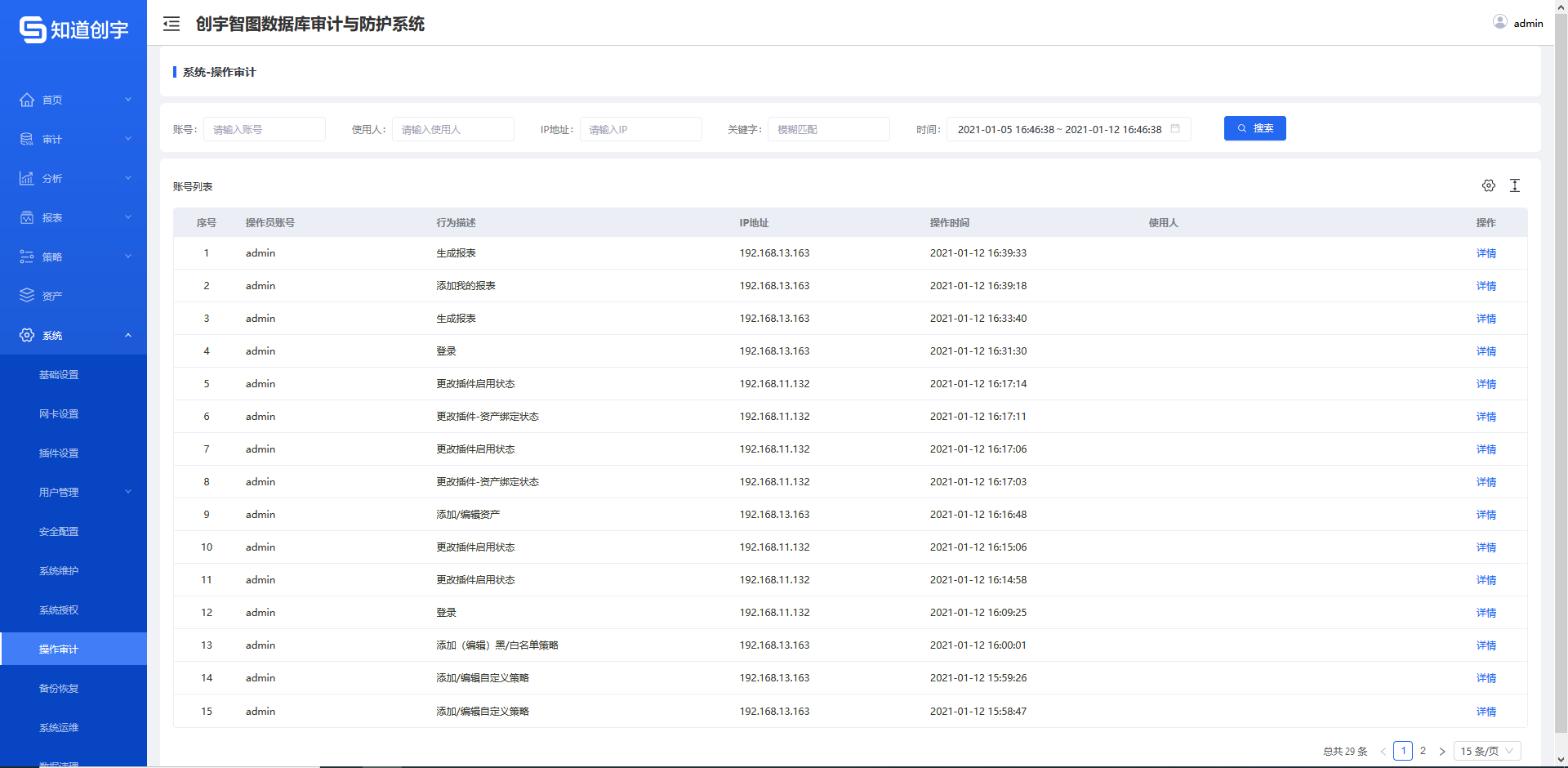


图8-8-1 操作审计

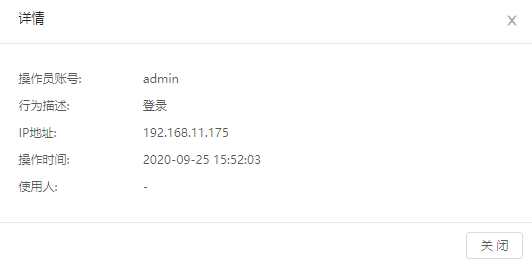


图8-8-2 操作审计详情

## 备份恢复

### 审计日志

进入[系统->审计日志]页面，如图8-9-1所示，支持通过FTP方式进行异地备份和恢复审计日志。单击<异地备份配置>，配置审计日志异地备份，如图8-9-2所示；单击<异地恢复配置>，配置审计日志异地恢复；如图8-9-3所示；选中审计日志备份记录，单击<删除备份>，删除审计日志备份记录。

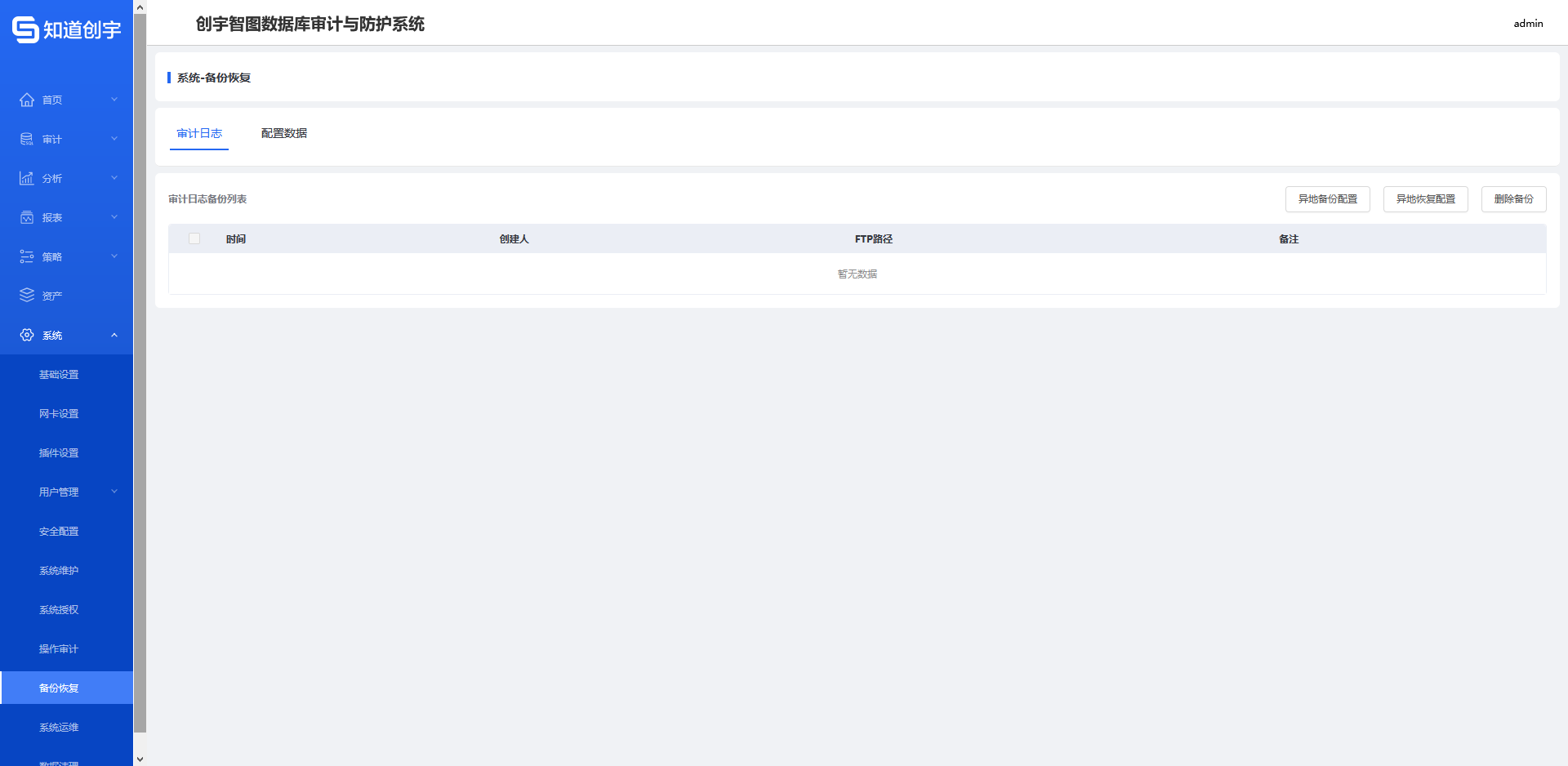
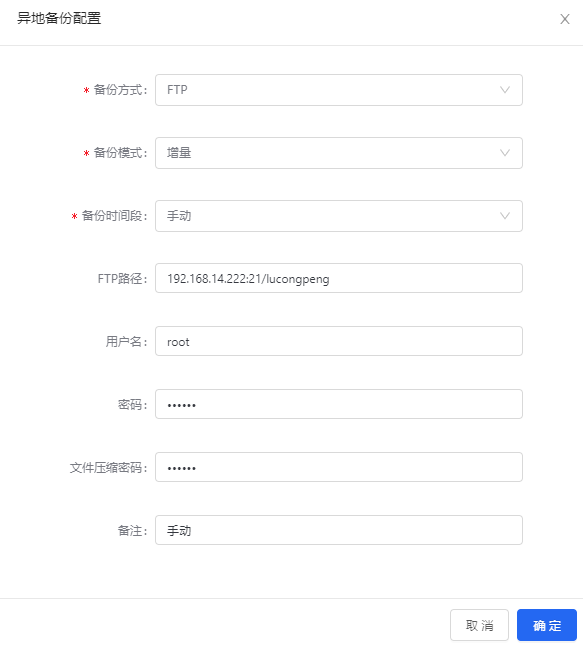


图8-9-1 备份恢复-审计日志



|  |  |
| --- | --- |
| 字段 | 内容 |
| 备份方式 | 审计日志异地备份方式，目前通过FTP方式 |
| 备份模式 | 审计日志异地备份模式，支持全量和增量两种方式 |
| 备份时间段 | 审计日志异地备份时间段 |
| FTP路径 | FTP路径格式：ip:port/path（无中文） |
| 用户名 | FTP服务器用户名 |
| 密码 | FTP服务器密码 |
| 文件压缩密码 | 审计日志文件压缩密码，在上传审计日志恢复时使用 |
| 备注 | 对此次异地备份配置的注解说明 |



|  |  |
| --- | --- |
| 字段 | 内容 |
| 备份方式 | 审计日志异地恢复方式，目前通过FTP方式 |
| FTP路径 | FTP路径格式：ip:port/path（无中文）/filename |
| 用户名 | FTP服务器用户名 |
| 密码 | FTP服务器密码 |
| 文件压缩密码 | 审计日志文件压缩密码 |

图8-9-3 审计日志异地恢复配置

### 配置数据

进入[系统->审计日志]页面，如图8-9-4所示，支持通过FTP方式进行异地备份和本地备份配置数据。单击<添加备份>，如图8-9-5所示，进行本地备份数据配置，输入备份备注和文件压缩密码，在恢复备份的时候需要输入文件压缩密码，在图8-9-4中，单击配置数据文件，可以下载到本地；单击<异地备份配置>，配置数据异地备份，如图9-9-6所示；单击<上传备份并恢复>，配置数据本地恢复，如图8-9-7所示；选中数据备份记录，单击<删除备份>，删除数据备份记录。

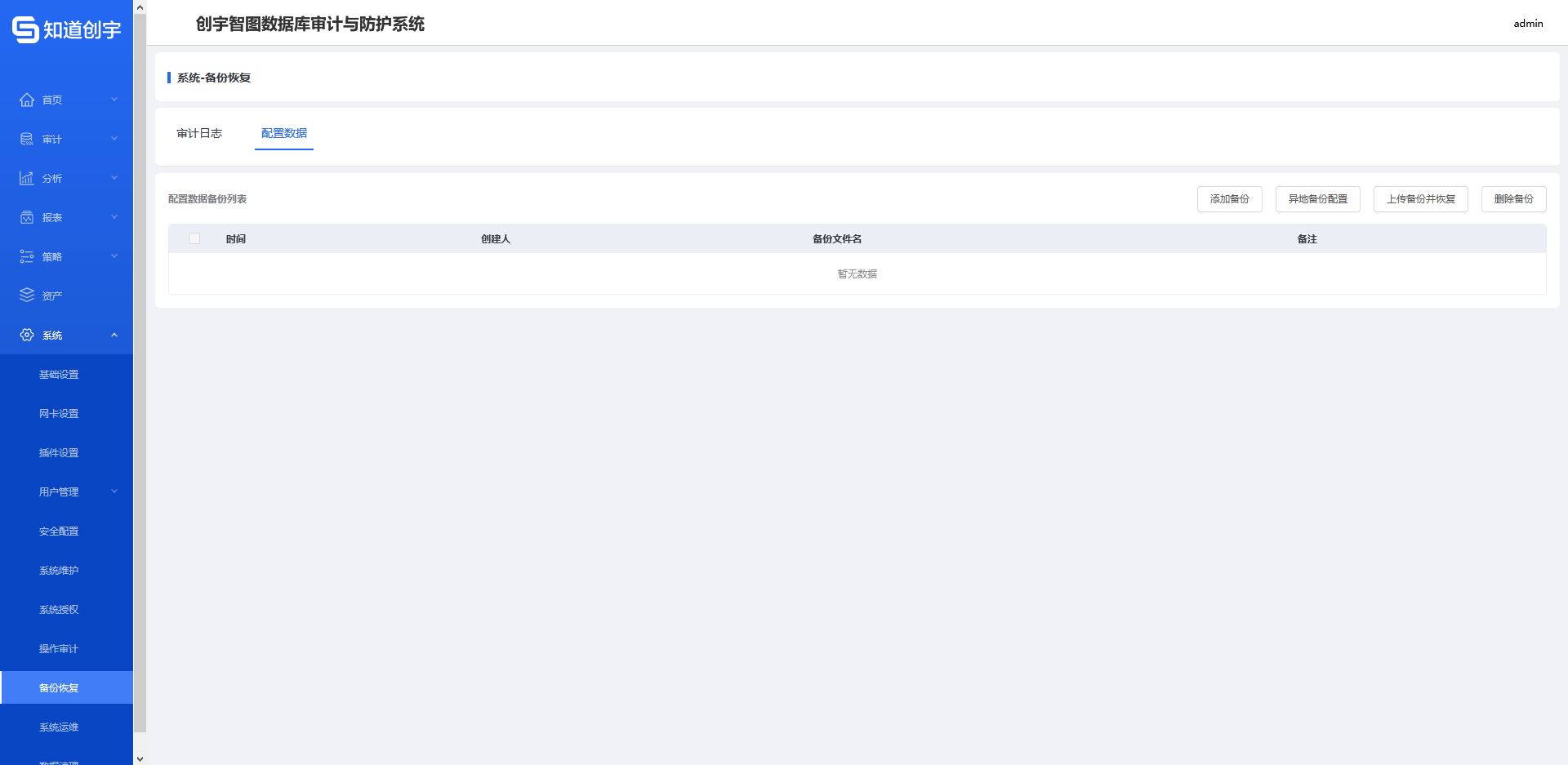


图8-9-4 配置数据

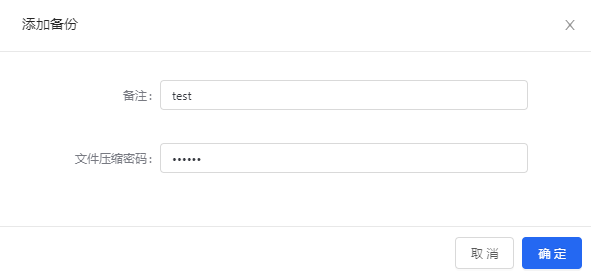
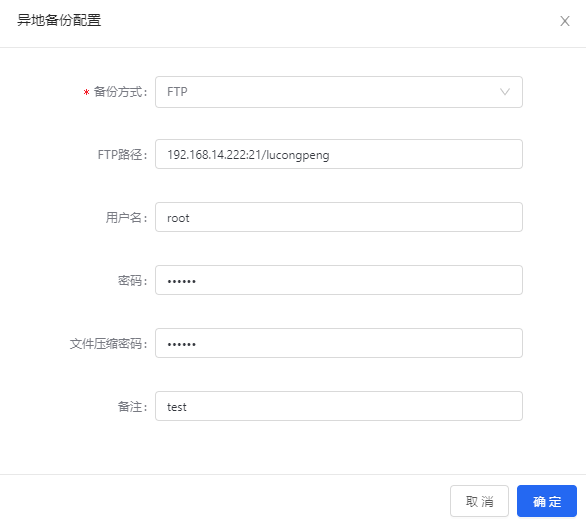


图8-9-5添加备份



|  |  |
| --- | --- |
| 字段 | 内容 |
| 备份方式 | 审计配置数据异地备份方式，目前通过FTP方式 |
| FTP路径 | FTP路径格式：ip:port/path（无中文） |
| 用户名 | FTP服务器用户名 |
| 密码 | FTP服务器密码 |
| 文件压缩密码 | 审计配置数据文件压缩密码 |
| 备注 | 对此次异地备份配置的注解说明 |

图8-9-6数据异地备份配置

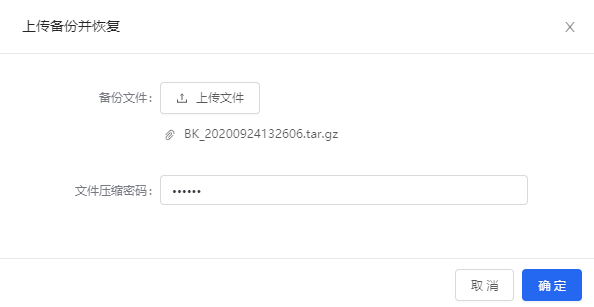


图8-9-7 上传备份并恢复

## 数据清理

进入[系统->数据清理]页面，如图8-10-1所示，可以手动或者自动清理备份文件、运行日志和审计日志，释放内存空间。

手动清理：选择日期，清理日期前的本地备份文件、运行日志和审计日志，单击<清理>，立即清理。

自动清理：设置超过阈值，超过阈值后，会自动清理日志，如果勾选了转储，会转储后再清理，转储配置如图8-10-2所示。设置小于阈值，低于阈值后悔自动停止清理。到了配置的天数后，不管阈值在什么范围，会自动清理审计日志。

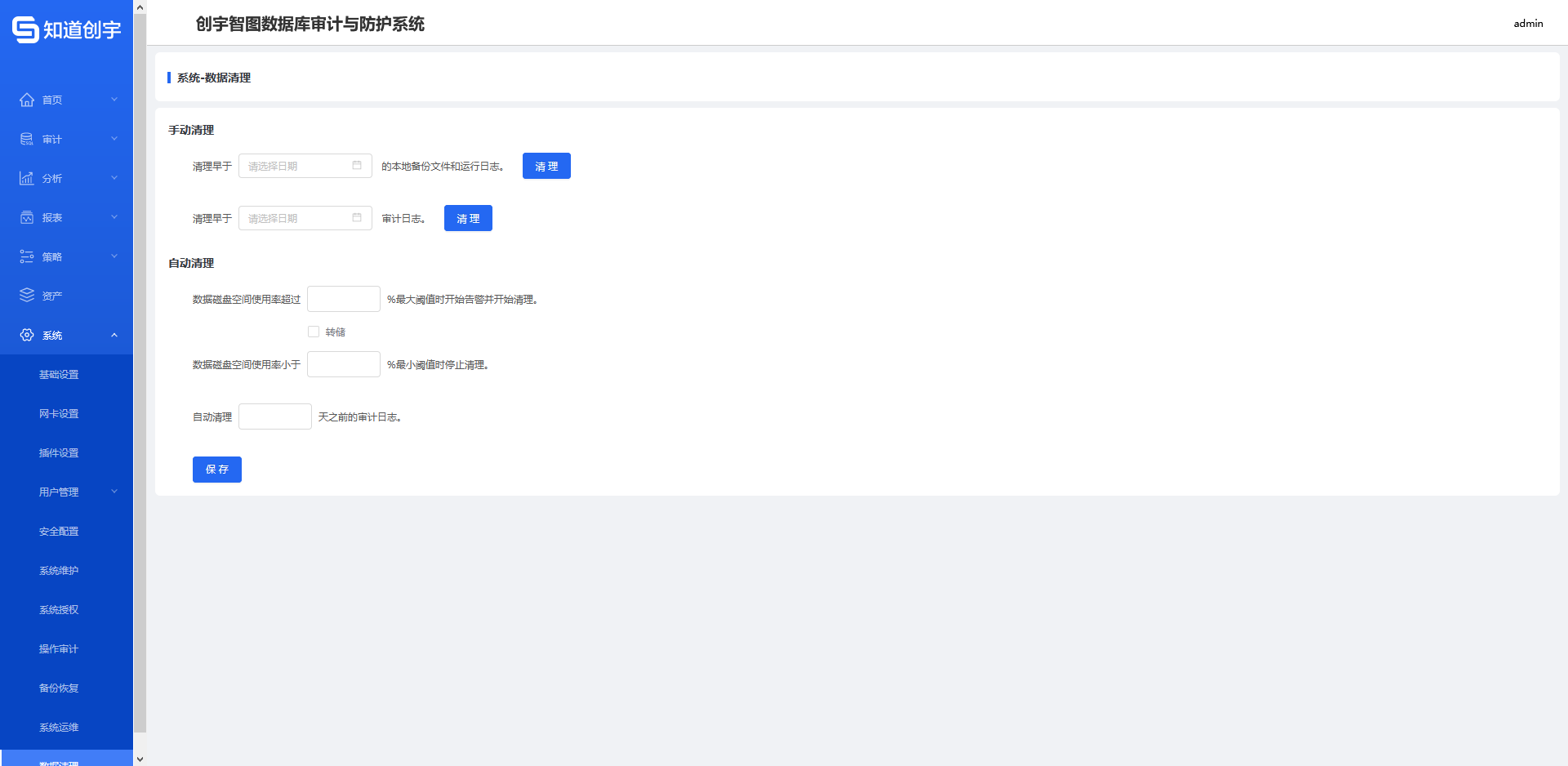


图8-10-1 数据清理



图8-10-2 转储配置