**云集数据库审计系统**

**用户手册**

北京云集至科技有限公司

目录

[1. 引言 2](#_Toc29075)

[1.1. 术语和缩写 2](#_Toc25304)

[2. 产品简介 4](#_Toc25373)

[2.1. 产品背景 4](#_Toc17159)

[2.2. 产品特点 5](#_Toc10831)

[2.3. 产品功能 5](#_Toc9170)

[3. 网络端口说明 6](#_Toc7137)

[4. 使用操作 6](#_Toc28121)

[4.1. 系统管理 6](#_Toc20916)

[4.1.1. 管理计算机连接方式 6](#_Toc16458)

[4.1.2. 登录系统 6](#_Toc28614)

[4.1.3. 设置最基本的审计策略 8](#_Toc21133)

[4.2. 查询分析 13](#_Toc28083)

[4.2.1. 审计查询 13](#_Toc19520)

[4.2.2. SQL类型统计 14](#_Toc29011)

[4.2.3. 事件类型统计 15](#_Toc3544)

[4.2.4. SQL流量统计 16](#_Toc27449)

[4.2.5. 风险级别统计 16](#_Toc30646)

[4.2.6. 系统审计 17](#_Toc27668)

[4.2.7. 报表预览 18](#_Toc27241)

[4.2.8. 报表定时参数配置 19](#_Toc8779)

[4.3. 安全配置 20](#_Toc21106)

[4.4. 资产配置 20](#_Toc10570)

[4.5. 来源规则配置 21](#_Toc25292)

[4.6. 时间规则配置 22](#_Toc24661)

[4.7. 内容规则配置 22](#_Toc31999)

[4.8. 证书管理 23](#_Toc27873)

[4.9. 过滤配置 24](#_Toc31373)

[4.9.1. 地址过滤 24](#_Toc27839)

[4.9.2. 语句过滤 25](#_Toc27381)

# 引言

## 术语和缩写

1. **数据库审计**

数据库审计是通过对数据库的操作记录下来作为审计记录，反映出数据库被使用的状况；数据库审计支持把通过网络访问方式对数据库的操作及内容进行实时的监控审计。

1. **审计类型**

审计类型指数据库审计系统支持的数据库类型，包括：Oracle、DB2、MSSql、MySql、Sybase、Infomix。

1. **数据库sql操作类型**

数据库审计支持的sql操作类型，包括

* 插入操作（Inserts）

数据插入操作（INSERT， SELECT … INTO）

* 新建数据表、数据库、视图、索引等操作（CREATE TABLE， CREATE DATABASE， CREATE VIEW， CREATE INDEX， …）
* 查询操作（Selects）

数据查询操作（SELECT）

数据表结构查询操作（show/desc）

* 删除操作（Deletes）

删除数据操作（DELETE， TRUNCATE TABLE， TRUNCATE DATABASE， …）

删除数据表、数据库、视图、索引等操作（DROP TABLE， DROP DATABASE， DROP VIEW， DROP INDEX， …）

* 更新操作（Updates）

数据更新操作（UPDATE）

数据表结构更新操作（ALTER， RENAME … TO …， MERGE INTO … USING …）

* 用户访问（Access）

用户登录

* 特权操作（Privilege）

用户权限改变（GRANT， DENY， REVOKE）

* 用户建立与删除

备份与恢复操作（BACKUP， RESTORE）

事务操作（COMMIT， ROLLBACK TO）

* 数据库特有操作

Microsoft SQL Server特有操作：DBCC，SP\_\*， OPENDATASOURCE， …

ORALCE特有操作

* 其他操作

特定字符串审计

1. **审计服务器**

审计服务器指数据库服务器。

1. **审计客户端**

审计客户端指访问审计服务器的用户终端。

1. **审计记录**

用户访问审计服务器产生的每一个sql操作或运维操作记录下来的行为及内容作为一条审计记录。

1. **策略**

对监控数据进行处理，生成审计记录以及执行某种操作的集合。

# 产品简介

## 产品背景

数据库是每个企业数据管理的基础，尽管这些系统的数据完整性和安全性是相当重要的，但对数据库采取的安全检查措施的级别还比不上操作系统和网络的安全检查措施的级别。许多因素都可能破坏数据的完整性并导致非法访问，这些因素包括密码安全性较差、误配置、未被察觉的系统后门以及自适应数据库安全方法的强制性常规使用等。

针对以上破坏数据完整性的威胁都来自于数据库本身的安全策略的漏洞和使用方面的问题，然而对于数据库合法用户的违规操作，以及内部用户对数据资源的故意泄露或破坏等问题，对企业带来的危害会更加严重，损失也会相当巨大。当然，数据库系统本身会提供一些日志审计功能，但是想要审计较为细致的操作日志就必然要影响到数据库服务器的性能，一般应用数据库的企业用户 ，都不愿意开设多一些的日志审计功能，这样必然会对数据库的安全埋下了安全隐患。

当产生数据安全问题时，为了寻找案件线索，执法机构需要从网络上寻找犯罪嫌疑人的活动和留下的痕迹并获取可靠的犯罪证据，对于侦破犯罪案件，保障社会稳定，维护公民利益具有十分重要的意义。

因此，安全管理要从网络系统安全和应用安全两个方面推进，才能有效地全面解决安全问题。数据库网络安全审计是网络安全管理工作中的一个重要组成部分，它可以通过对网络数据库的“信息活动”实时地进行监控审计，使管理者对网络数据库的“信息活动”一目了然，能够及时掌握数据库服务器的应用情况，及时发现客户端的使用问题，存在着哪些安全问题和隐患并予以纠正，预防应用安全事件的发生，即便发生了也能够可以快速查证并追根寻源。

## 产品特点

数据库审计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，对网络中的各种应用行为和应用内容进行监控、报警、记录。

数据库审计系统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。

## 产品功能

* 数据库行为和数据库运维监控、审计、报警

能够对网络数据库的各种操作进行记录审计并报警，提供详细的审计信息（4W：何时 When 、何地 Where 、何人 Who以及何种行为 What）查询功能和邮件、syslog报警方式。同时提供多种审计条件，实现分类审计或组合审计。

* 数据库事件审计分析

能够对网络数据库接收发送的流量包数进行统计，并提供详细的统计条件（如：时间、IP地址、协议类型等），并根据历史的数据库操作数量做出基于：天、周、月的趋势分析。

* 日志信息查询

能够对网络中其他设备发来的syslog和SNMP日志信息进行接收和查询，并提供多种查询条件，实现分类或组合查询。

* 报表系统

可以实现手动报表和自动定制报表邮件发送功能。

* 自身日志

支持完善的自身日志记录和查询功能。

# 网络端口说明

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 源→目标 | 端口 | 备注 |
| 1 | 终端→审计产品 | 443 |  |
| 2 | 审计产品→数据库 | 8101 |  |
| 3 | 数据库→审计产品 | 8288 |  |

# 使用操作

## 系统管理

### 管理计算机连接方式

产品为B/S架构，使用IE浏览器软件即可以对产品进行配置和管理。将管理计算机连接数据库审计设备的通信口或者和通信口IP可达即可对设备进行管理。

### 登录系统

使用IE浏览器，在地址栏中输入：https://审计中心IP （此处的审计中心IP指审计中心通信口的IP） 如：https:// 192.168.99.60 按照以下步骤进行即可登录系统。

通信口IP地址：192.168.99.60

掩码： 255.255.255.0

网关： 192.168.99.1

端口开放：

终端至产品 443端口

产品至数据库 8101

数据库至产品8288

登录方式：使用浏览器访问https://ip

账户:

sysadmin/sysadmin@1234 系统管理员

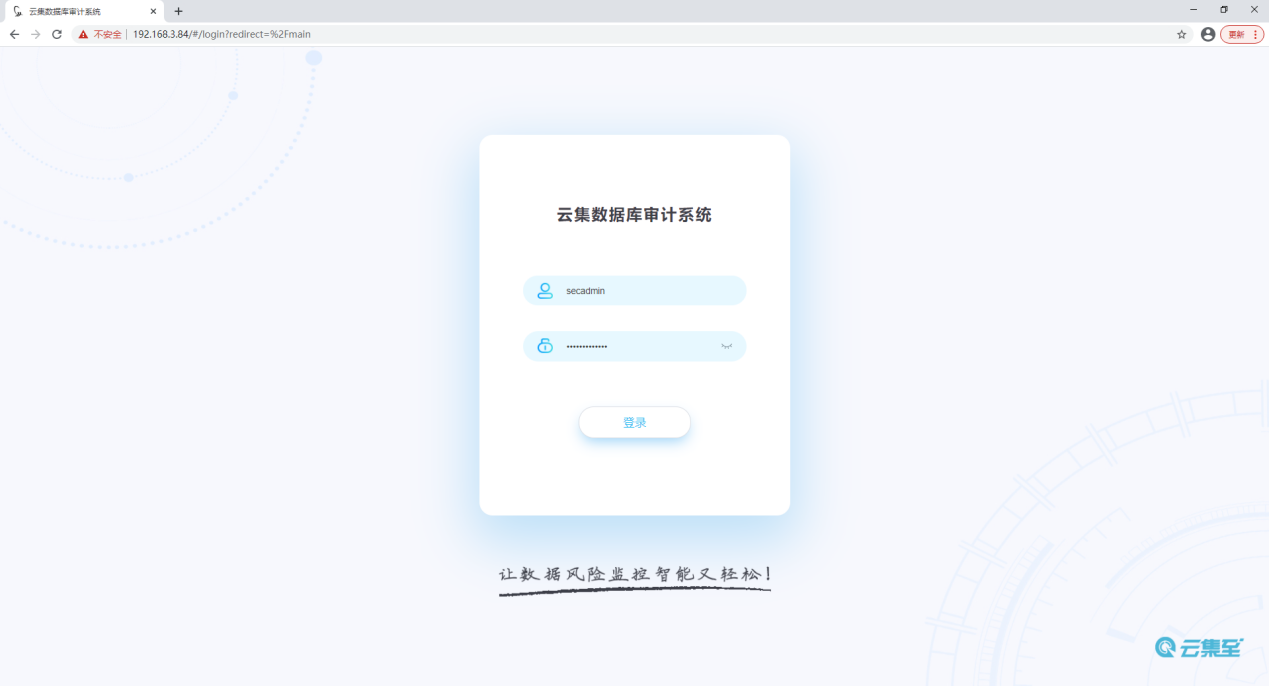
secadmin/secadmin@1234 安全管理员

audadmin/audadmin@1234 审计管理员

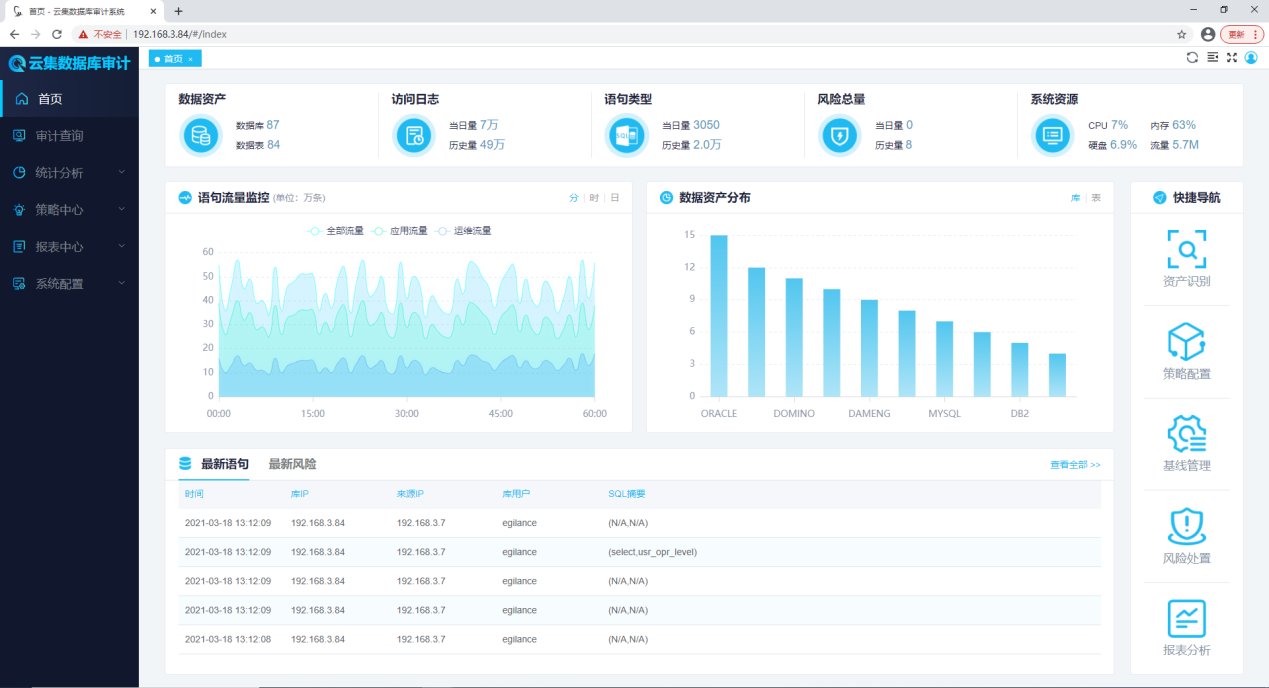
系统内置用户和密码：

|  |  |  |  |
| --- | --- | --- | --- |
| **内置默认用户** | **用户名** | **密码** | **权限** |
| 系统管理员 | sysadmin | sysadmin@1234 | 系统管理、用户权限管理、策略配置、报表配置 |

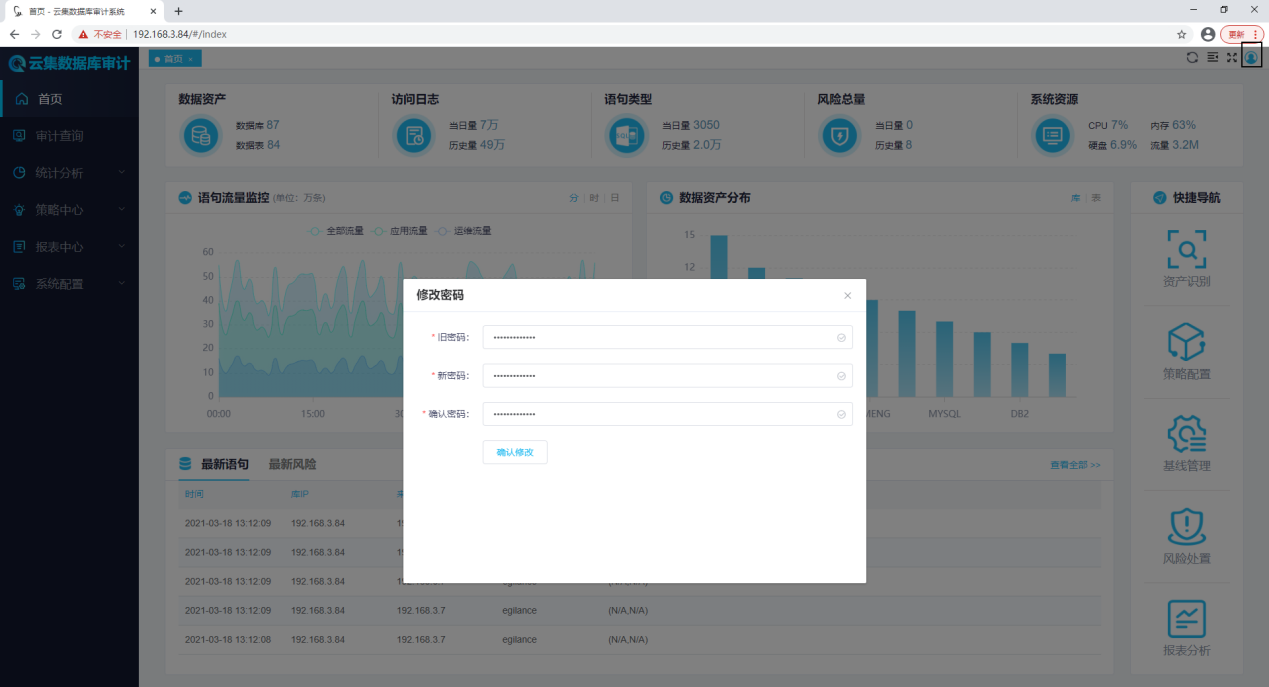
当用户成功安装数据库审计系统系统后，使用IE浏览器，在地址栏中输入：https://审计中心IP （此处的审计中心IP指审计中心通信口的IP） 如：https://192.168.99.60。显示页面如下图：



首次安装部署的数据库审计系统应以系统管理员身份登录系统，系统管理员默认用户名和密码为secadmin，secadmin@1234。登入后界面如下图所示：



登入后界面在右上角头像处点击下拉按钮可以进行密码修改，修改密码时输入先前旧密码，在输入新密码和再次确认新密码，密码长度必须为6-18位！

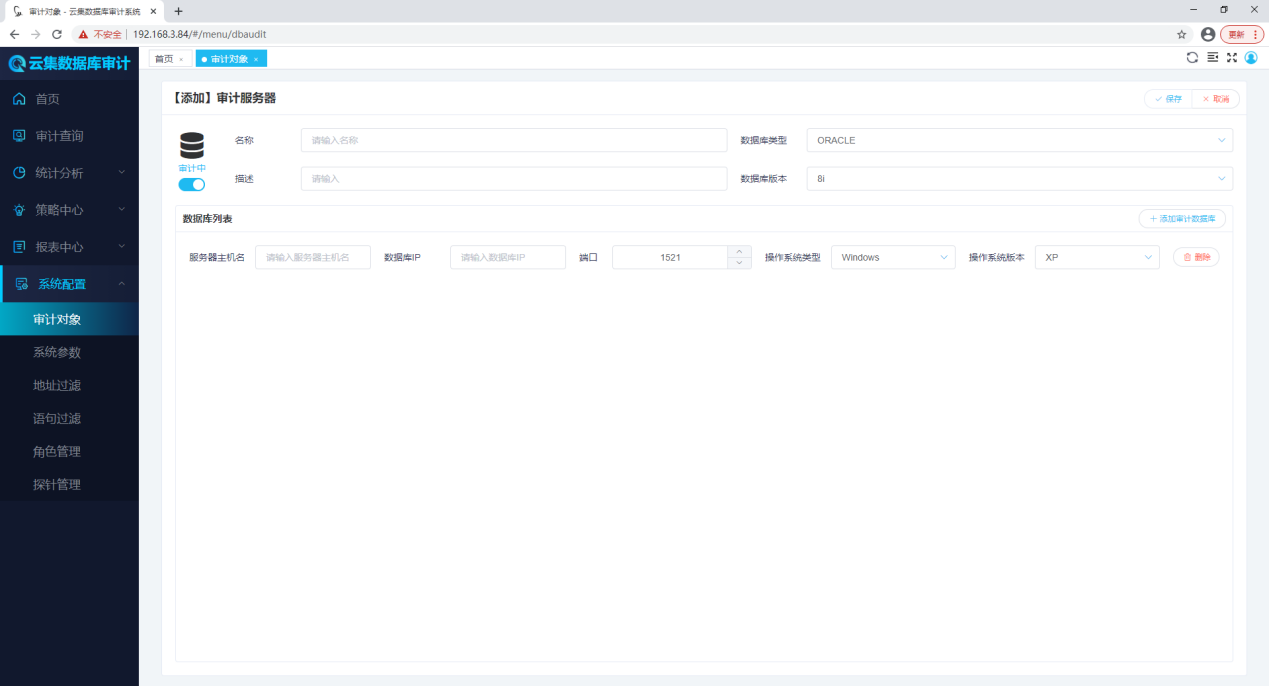


### 设置最基本的审计策略

为了数据库审计系统可以审计到关注数据库的数据库操作，以系统管理员secadmin登录，配置以下内容：

#### 添加审计服务器

鼠标左键点击左侧导航栏中的“系统配置->审计对象”，进入审计服务器页面界面。点击审计服务器页面左上角的添加按钮，进入添加审计服务器页面。在此页面中编辑审计服务器的参数，点击“保存”，完成新审计服务器的添加，点击“取消”不添加新的审计服务器，如下图所示：



#### 添加审计策略

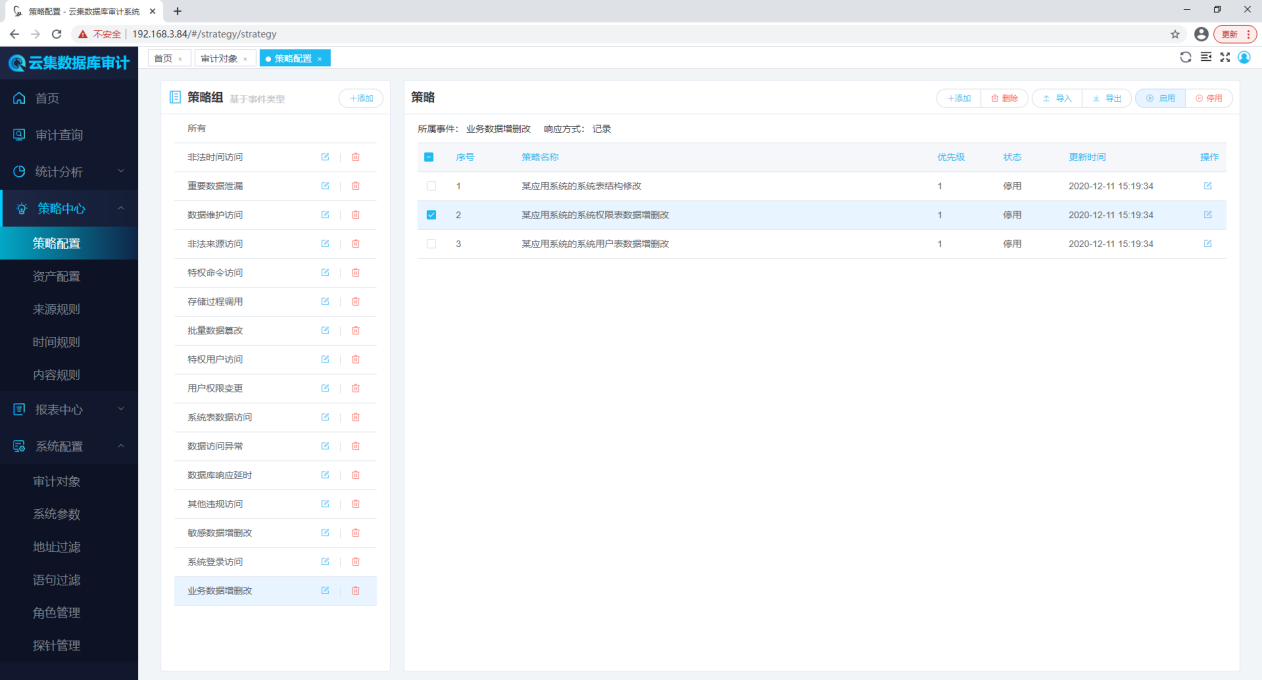
鼠标左键点击左侧导航栏中的“策略中心->策略配置”，进入“策略配置”界面。如下图所示：

启用：点击此选项，选中的审计策略启用

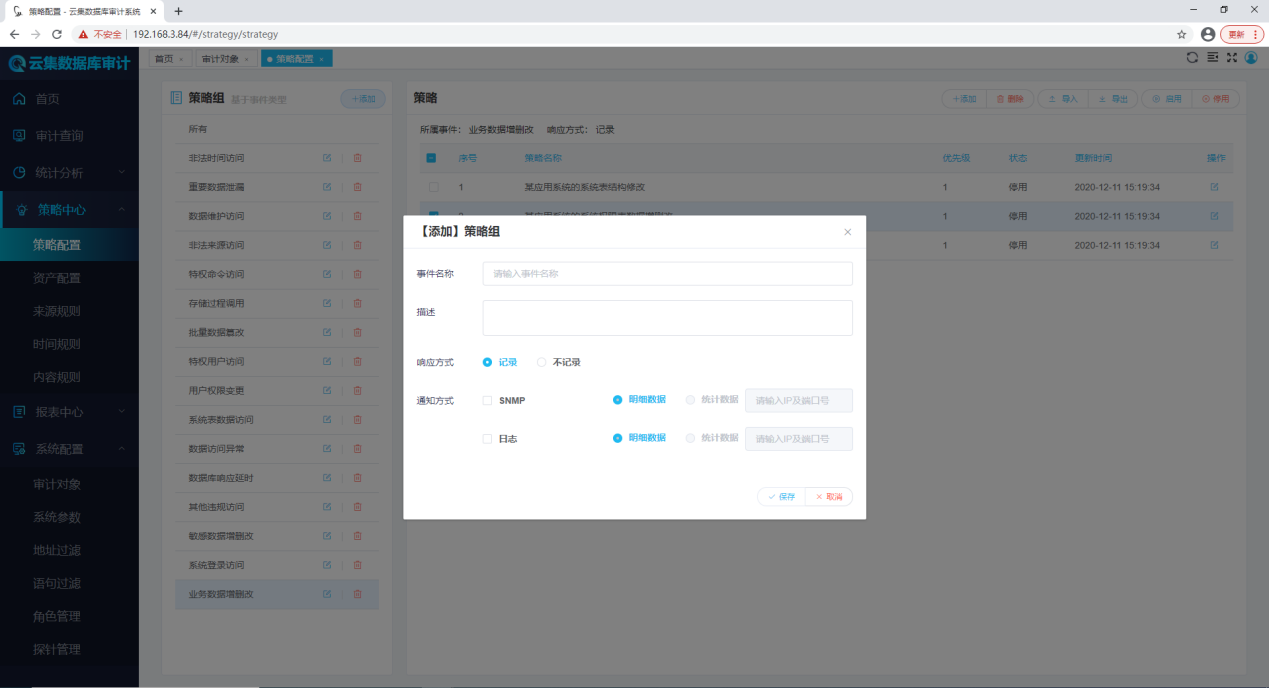
停用：点击此选项，选中的升级策略停用

删除：删除所选中的策略

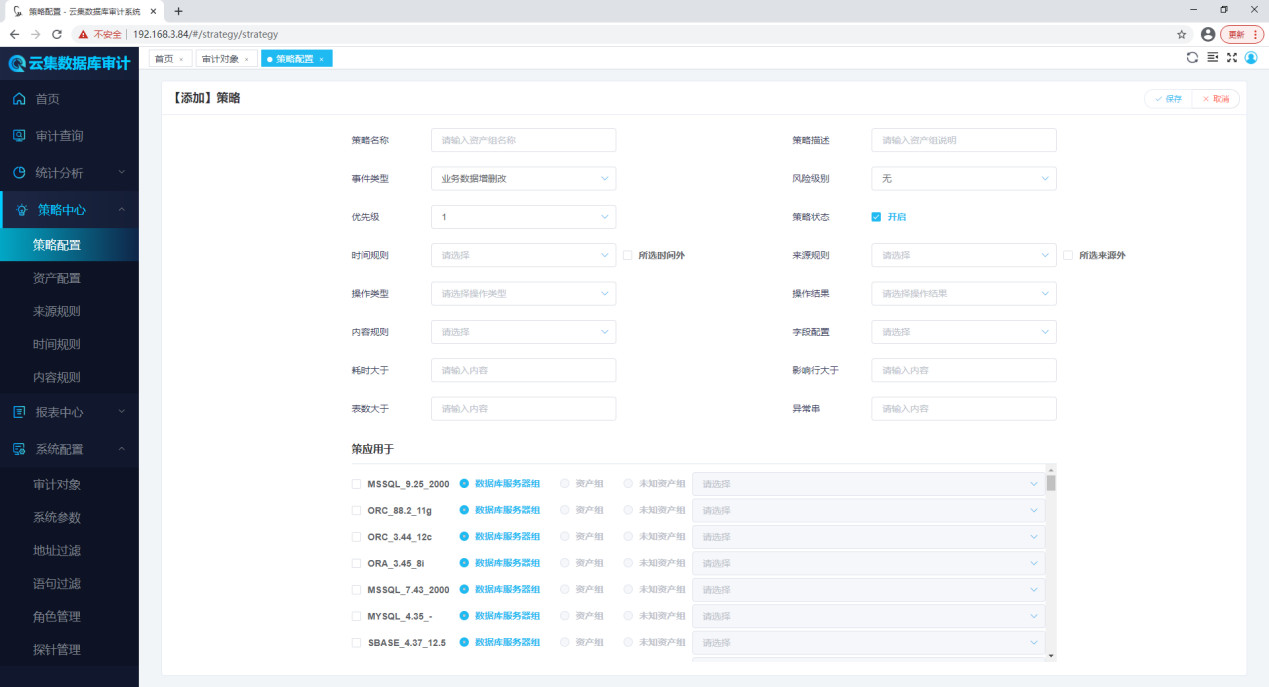
编辑：编辑当前所选中的此策略



点击此页面左上角添加策略组，弹出“【添加】策略组”对话框，正确填写各项信息，点击“保存”完成新策略组添加，如下图所示：

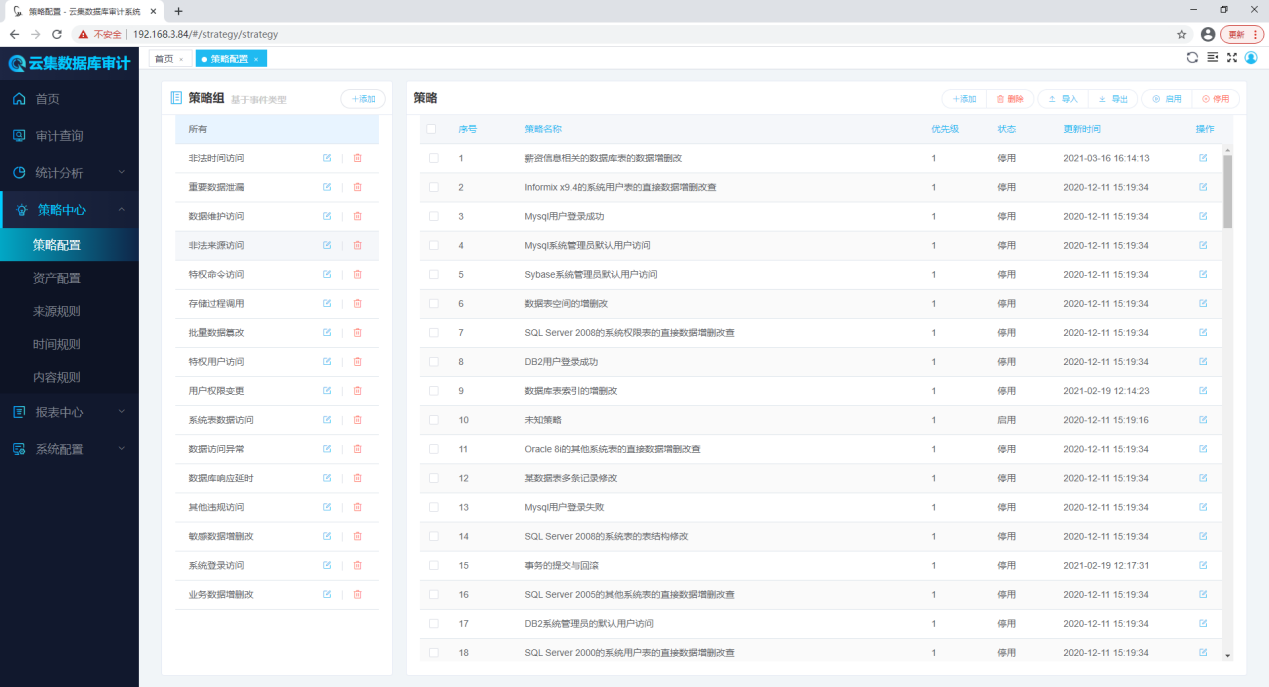


点击页面中下新建策略，打开“添加策略”界面。正确填写各项信息，点击“保存”完成新审计策略添加，如下图所示：

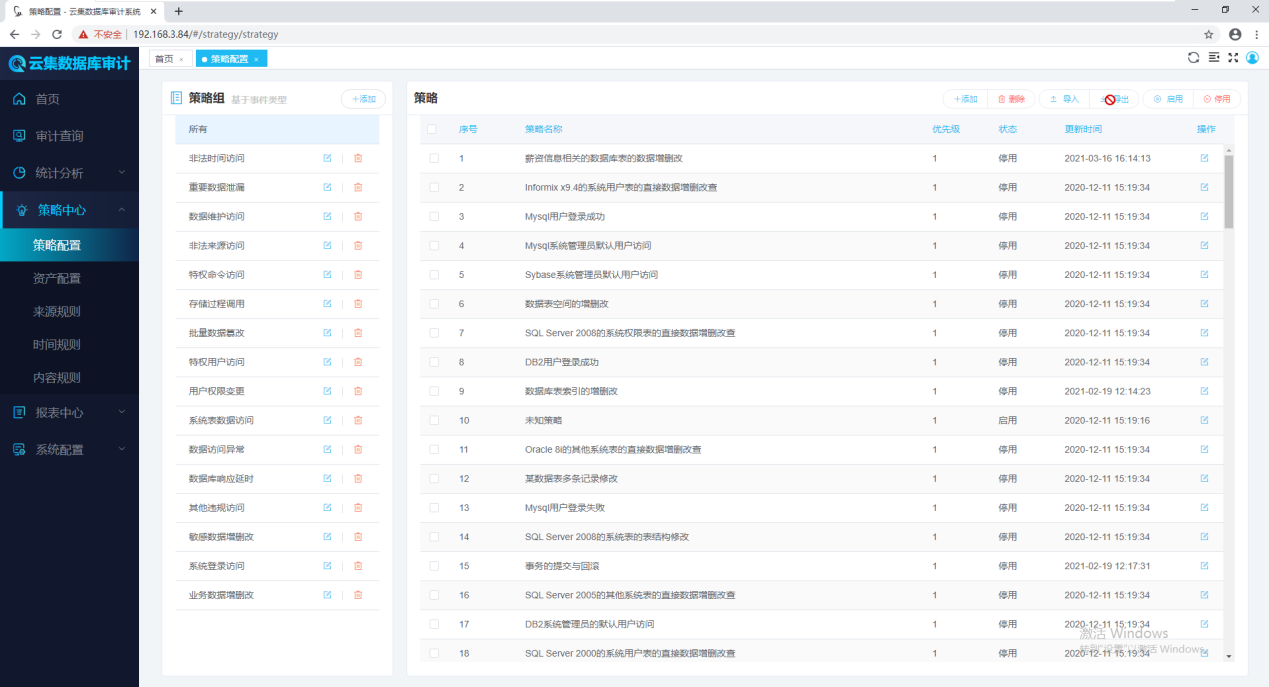


#### 查询结果导出

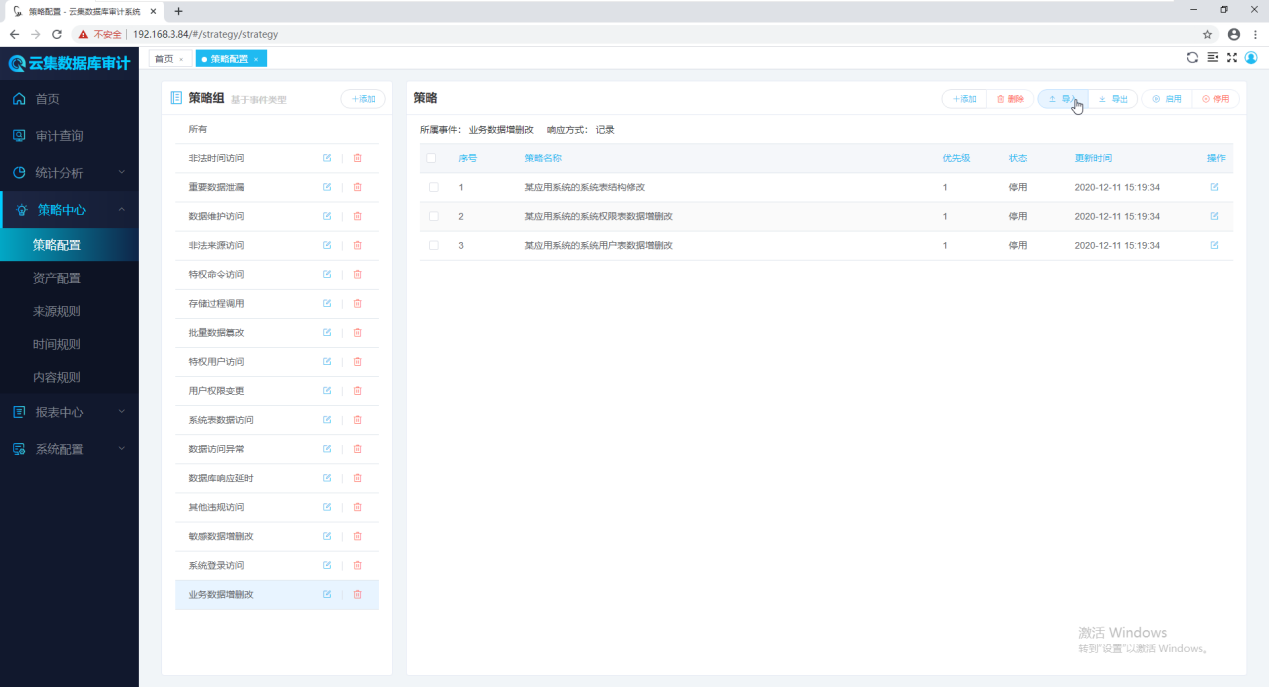
以拥有数据库行为操作权限的用户登录系统，鼠标左键点击左侧导航栏中的“策略中心->策略配置”，进入“策略配置”界面，如下图所示：



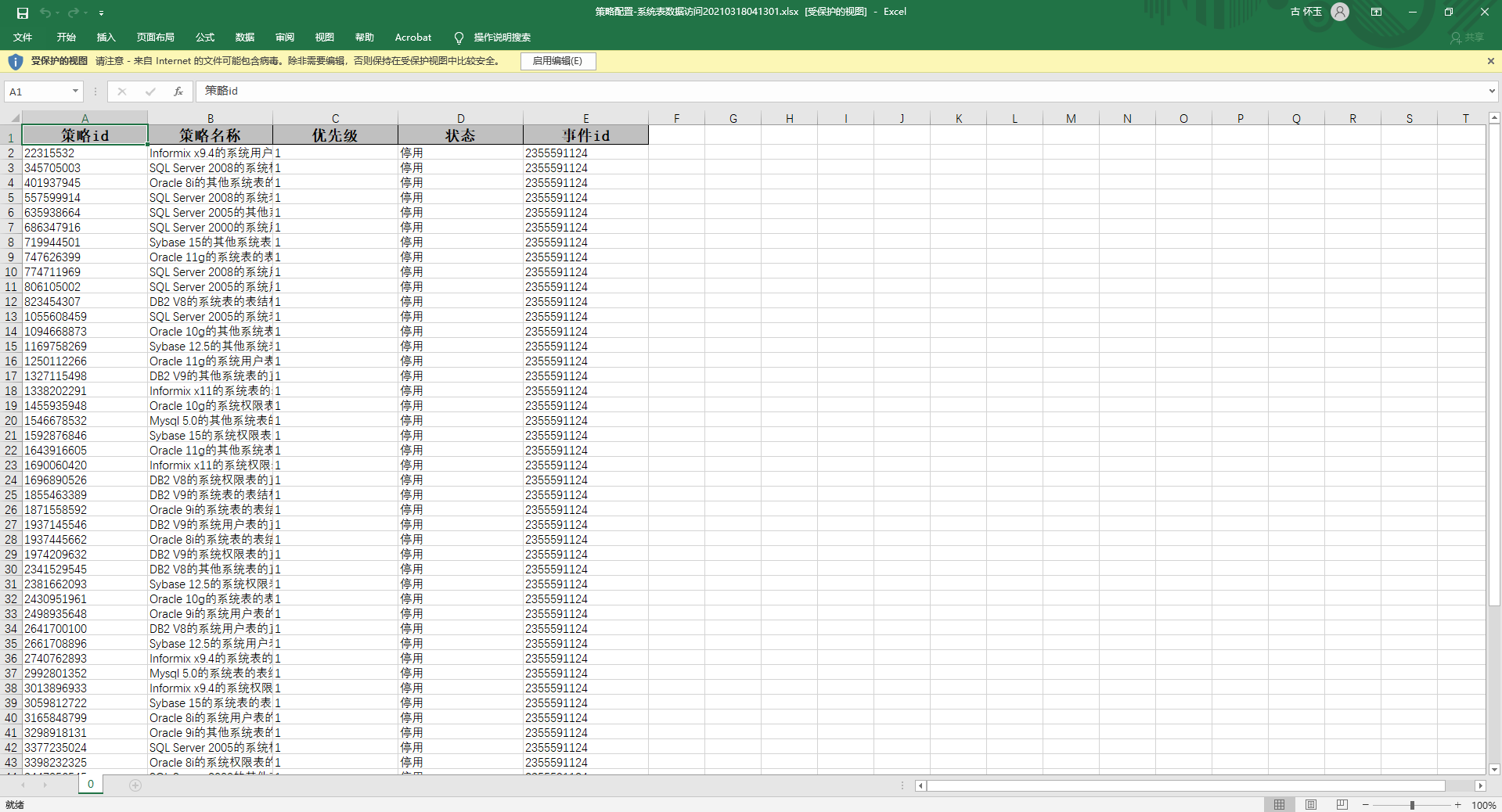
查询结果导出格式为“Excel”格式，当未选策略组或策略组没有内容时，鼠标放到“导入”和“导出”上方，为禁止点击状态



当选中数据，“导入”，“导出”可以进行点击，如下图所示：



1.导出模式默认为“xlsx”格式的Excel文件，下载成功，然后用Excel工具打开查看文件。如下图所示：



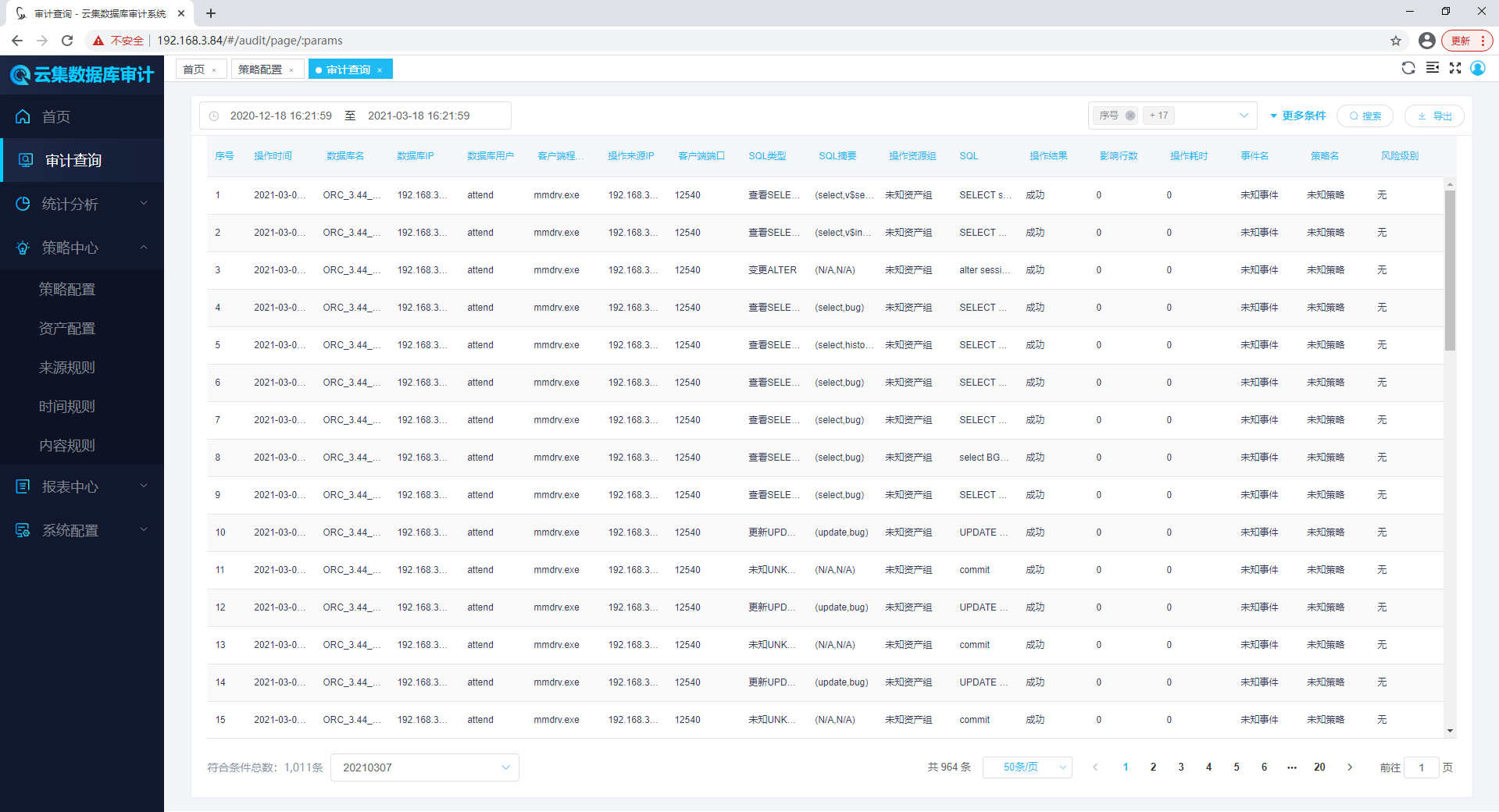
导入默认格式为“xlsx”文件格式，点击导入，选中编辑好的“xlsx”文件将其导入。

“来源规则”，“时间规则”，“内容规则”的查询结果导出与“策略配置”一至。

## 查询分析

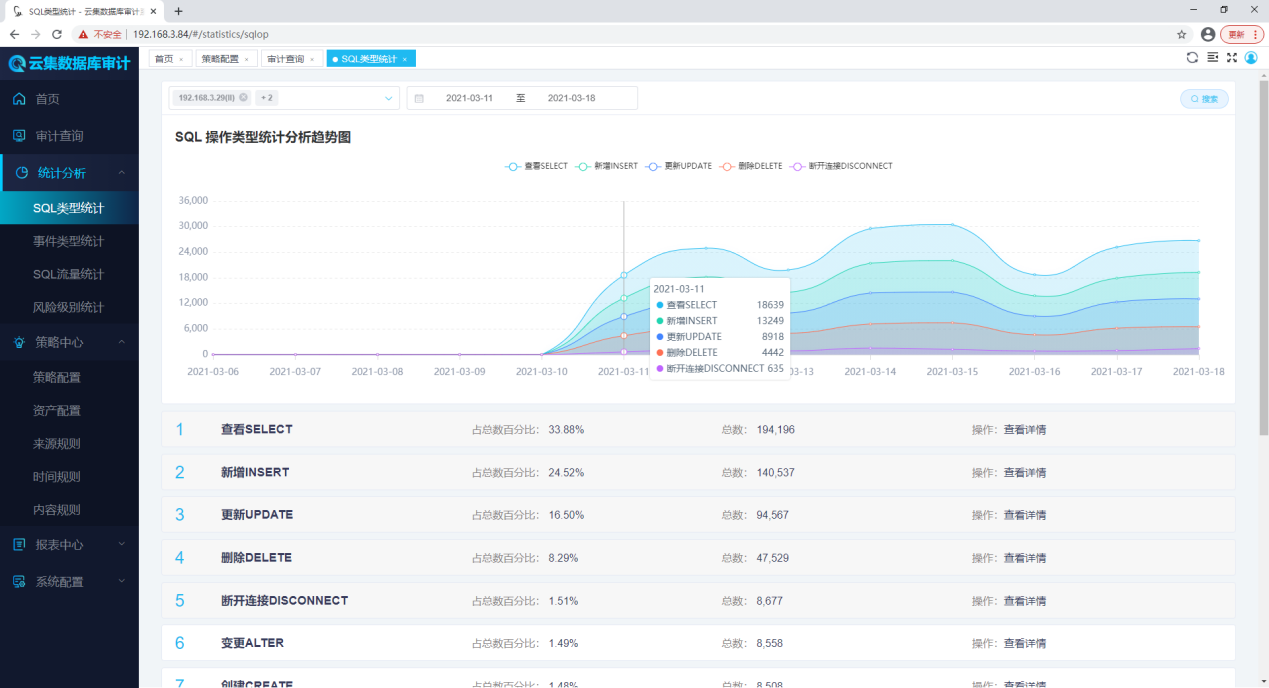
### 审计查询

审计查询，可以设置各种条件进行监测、查询。点击检索出的某一条数据，在右侧可以查看此条信息的详细内容。如下图所示：

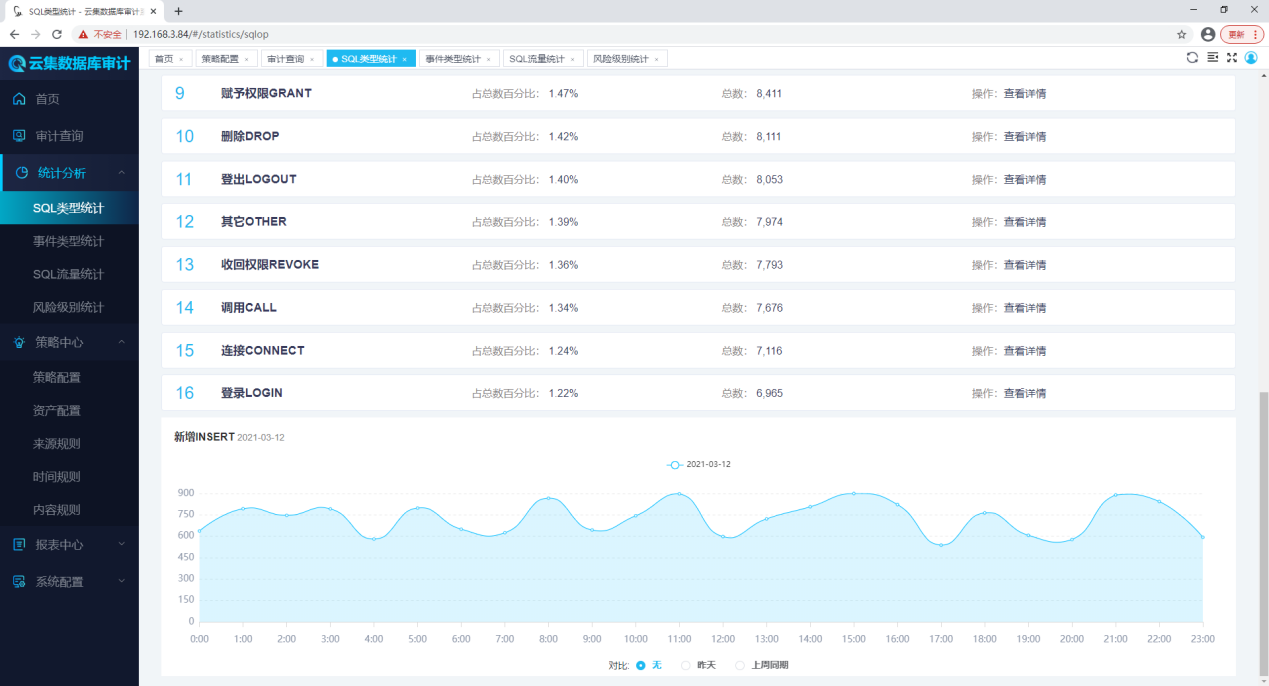


### SQL类型统计

以拥有数据库操作查询权限的用户登录系统，鼠标左键点击左侧导航栏中的“统计分析->SQL类型统计”，进入“数据库类型统计”界面，如下图所示：

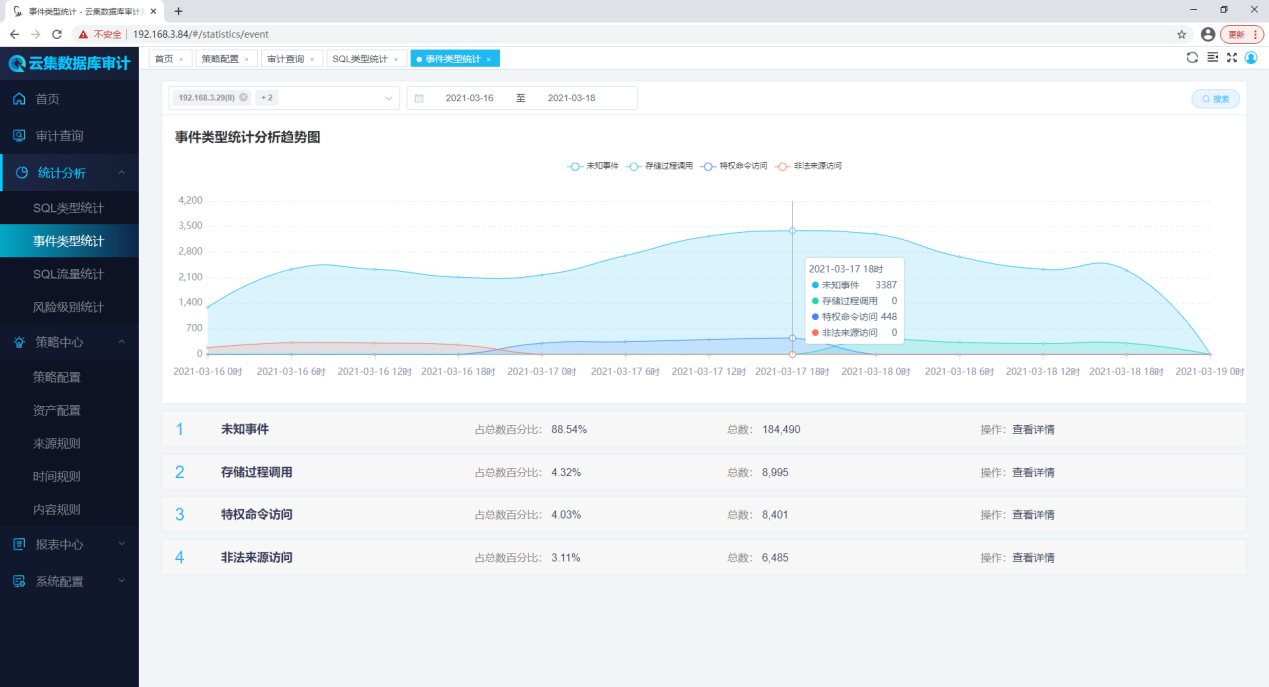


点击其中的日期，可以查看点击日期一天以小时为单位的数据模型

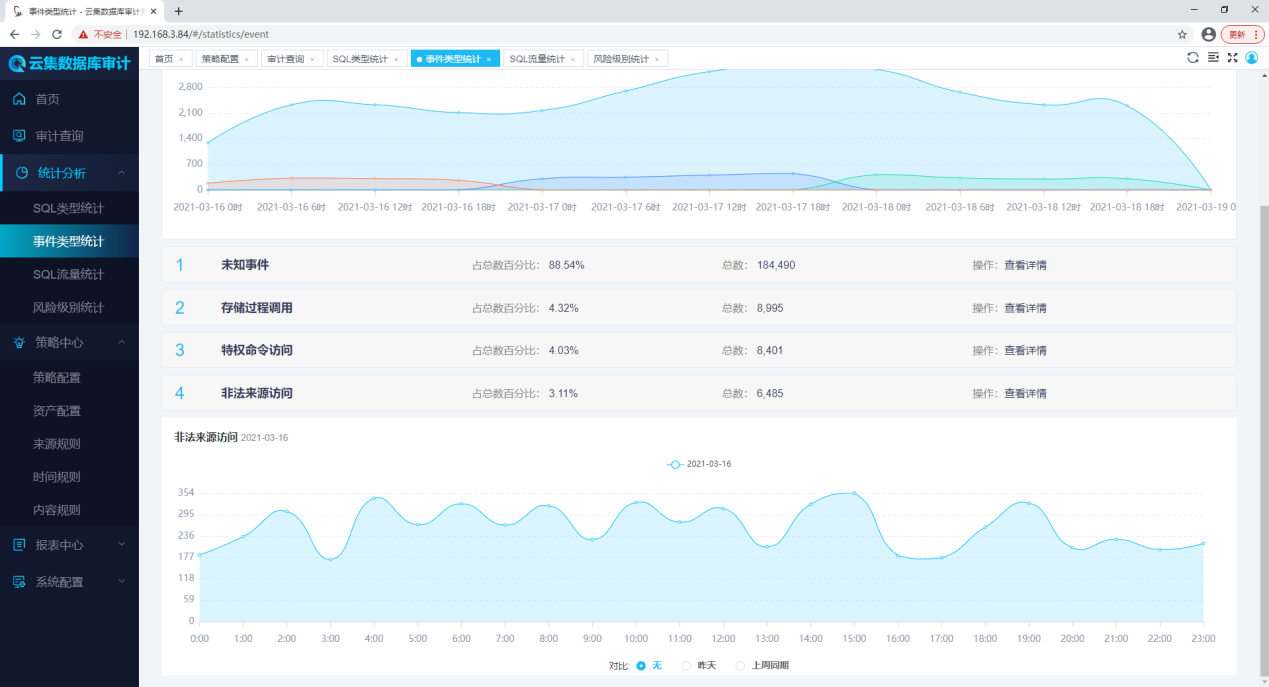


### 事件类型统计

已拥有数据库操作查询权限的用户登录系统，鼠标左键点击左侧导航栏中的“统计分析->事件类型统计”，进入“事件类型统计”页面，如下图所示：

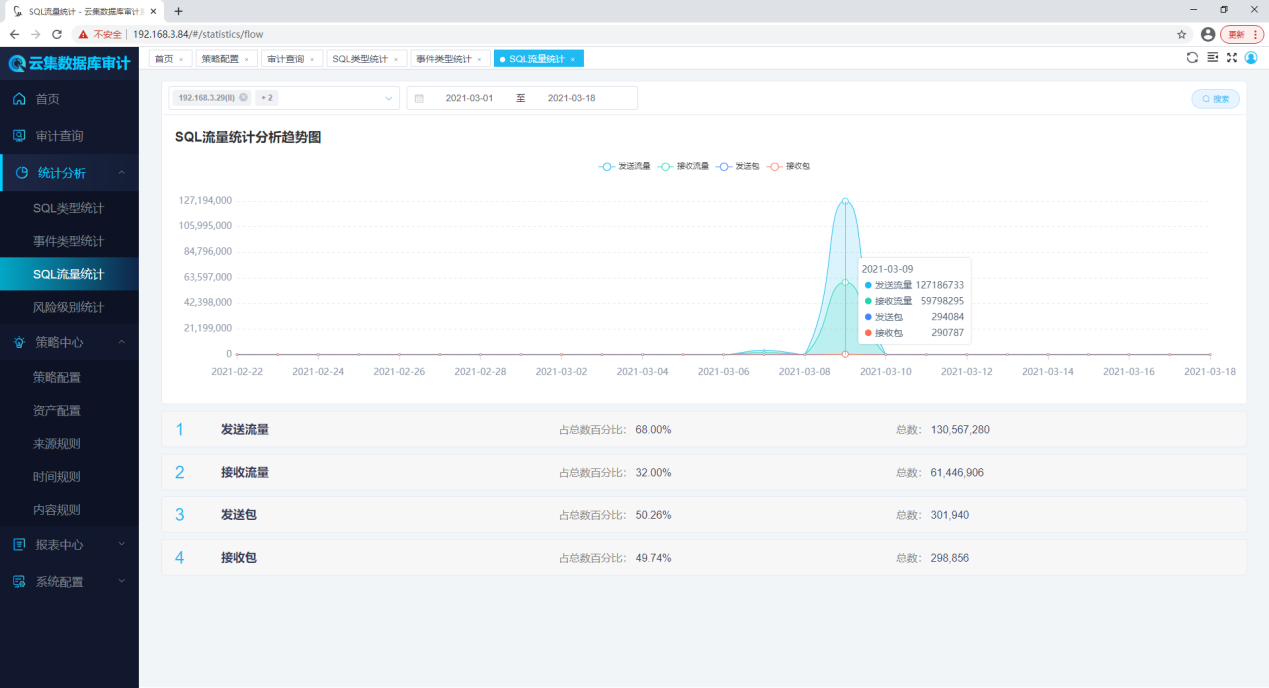


点击其中的日期，可以查看点击日期一天以小时为单位的数据模型



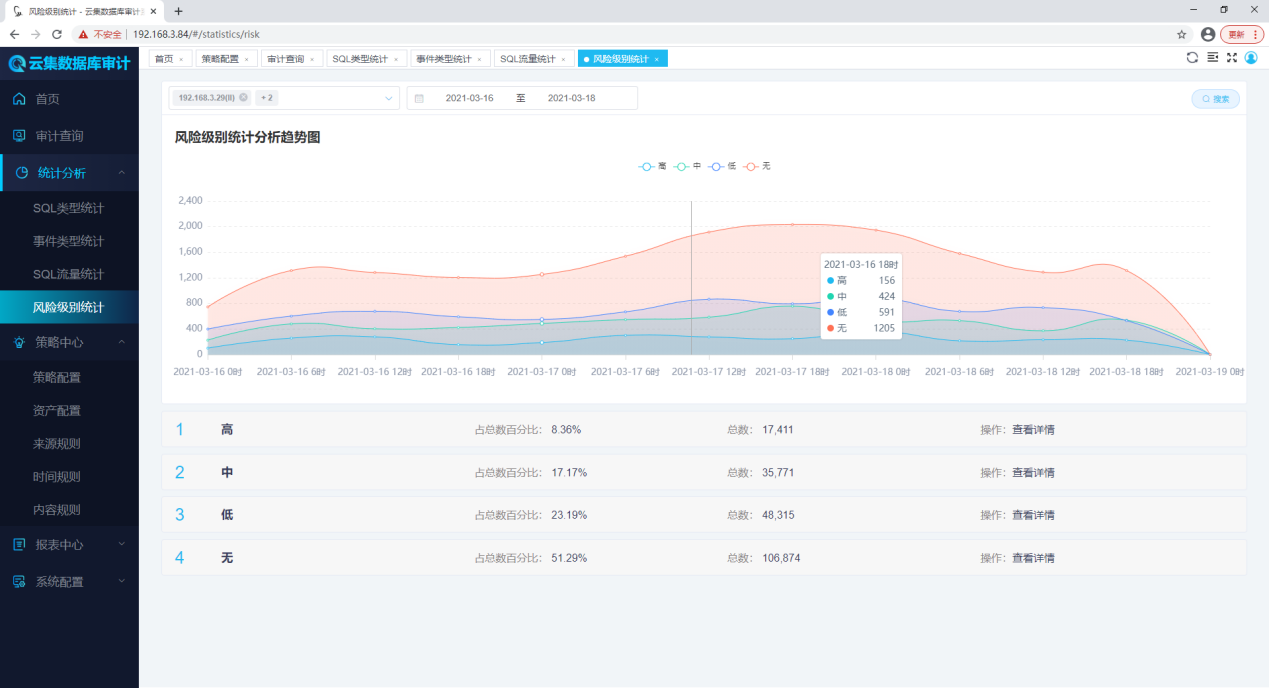
### SQL流量统计

已拥有数据库操作查询权限的用户登录系统，鼠标左键点击左侧导航栏中的“统计分析->SQL流量统计”，进入“SQL流量统计”页面，如下图所示：

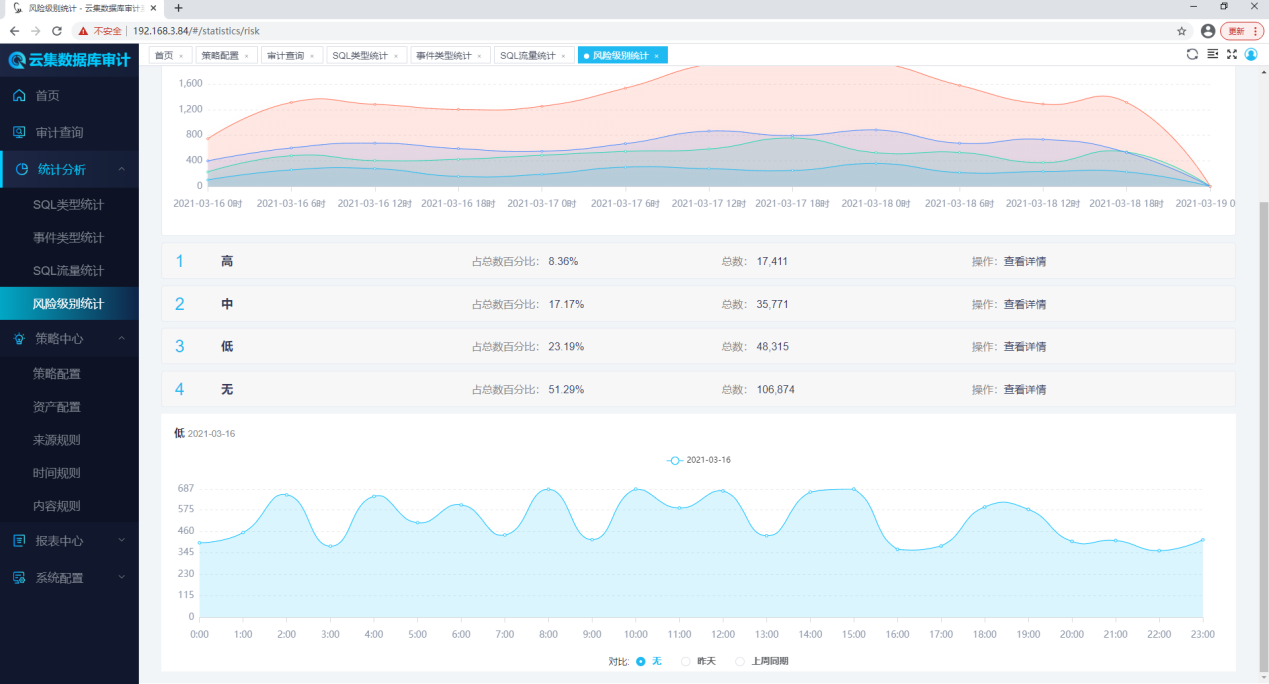


### 风险级别统计

已拥有数据库操作查询权限的用户登录系统，鼠标左键点击左侧导航栏中的“统计分析->风险级别统计”，进入“风险级别统计”页面，如下图所示：

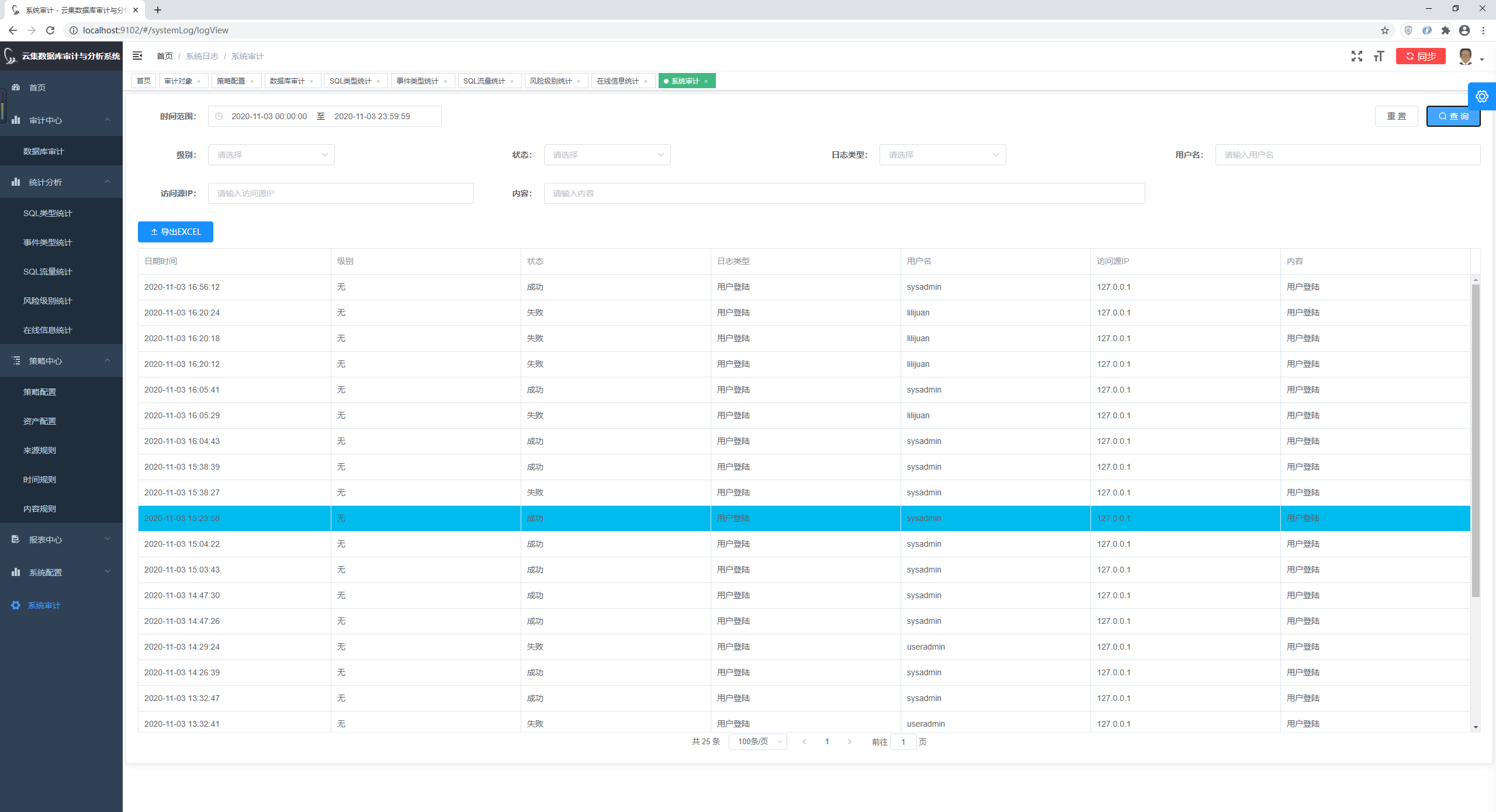


点击其中的日期，可以查看点击日期一天以小时为单位的数据模型



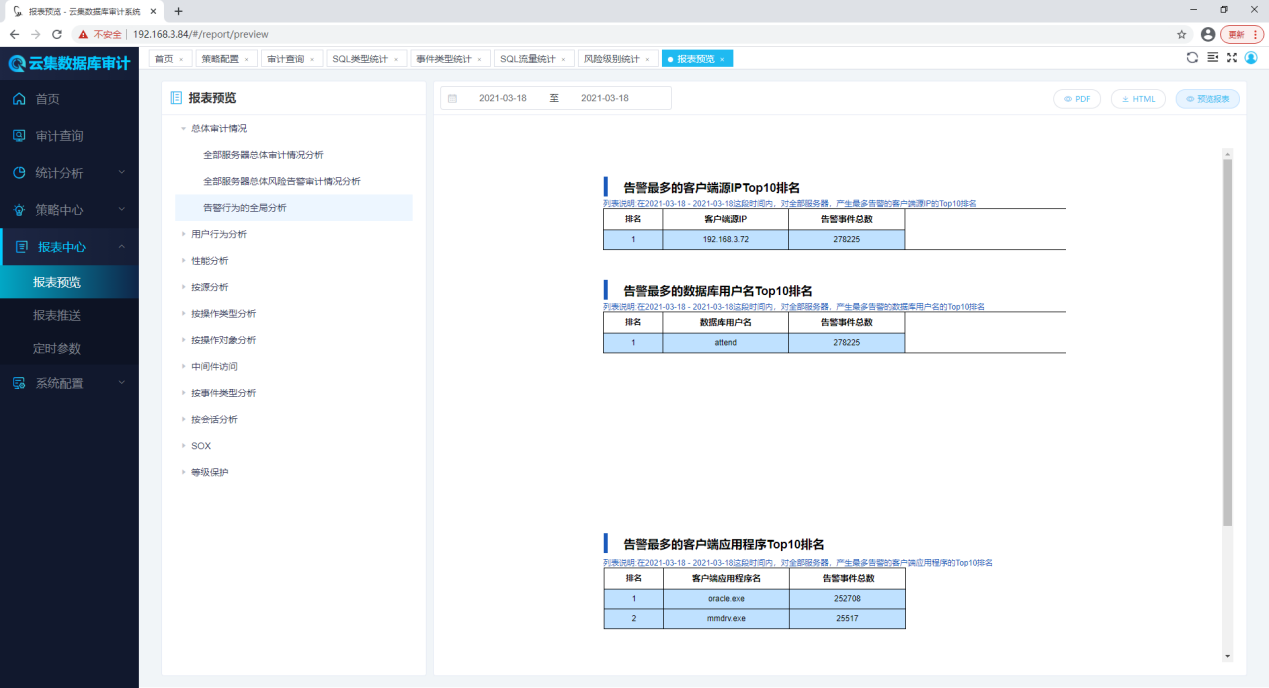
### 系统审计

已拥有数据库操作查询权限的用户登录系统，鼠标左键点击左侧导航栏中的“系统审计”，打开系统审计页面，填写相应的检索要求，查询出所有的系统审计数据，表单可以在左上角以EXCEL导出，如下图所示：



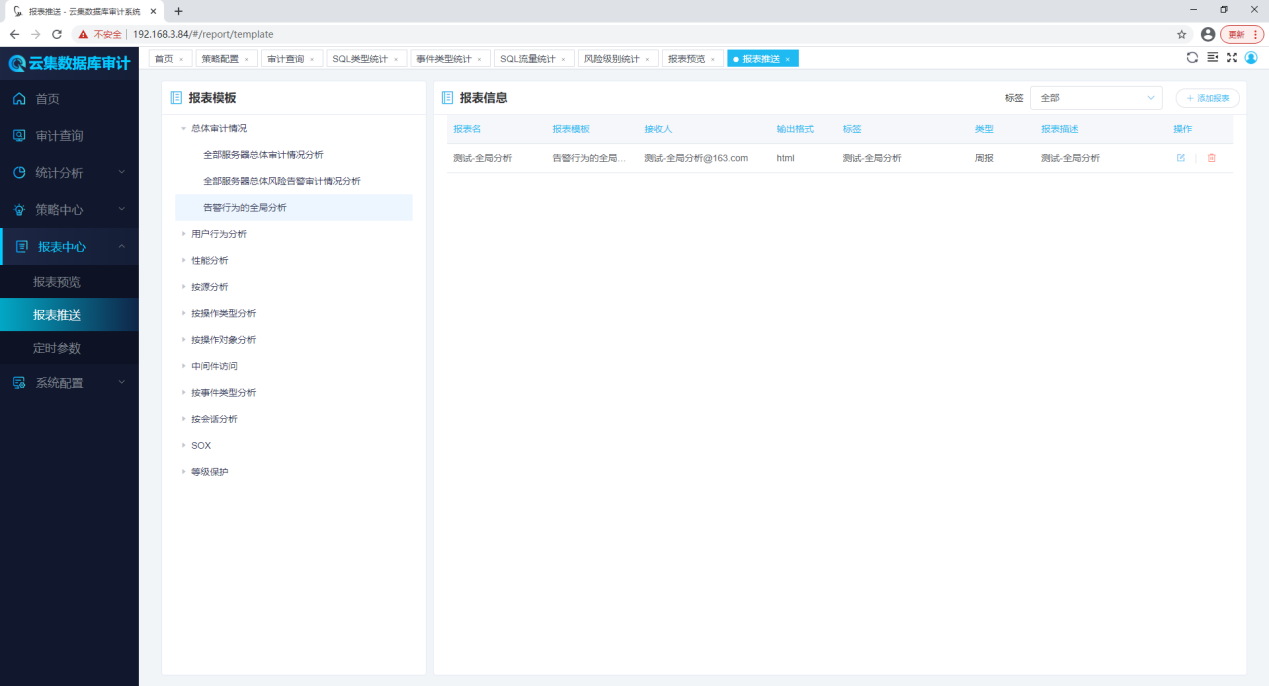
### 报表预览

已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“报表中心->报表预览”，进入“报表预览”页面，选中左侧的报表分类的某一项，填入检索条件，点击预览报表，以“折线统计图”，“饼状图”，“表单”方式显示，还可以通过“pdf”，“html”方式查看，如下图所示：



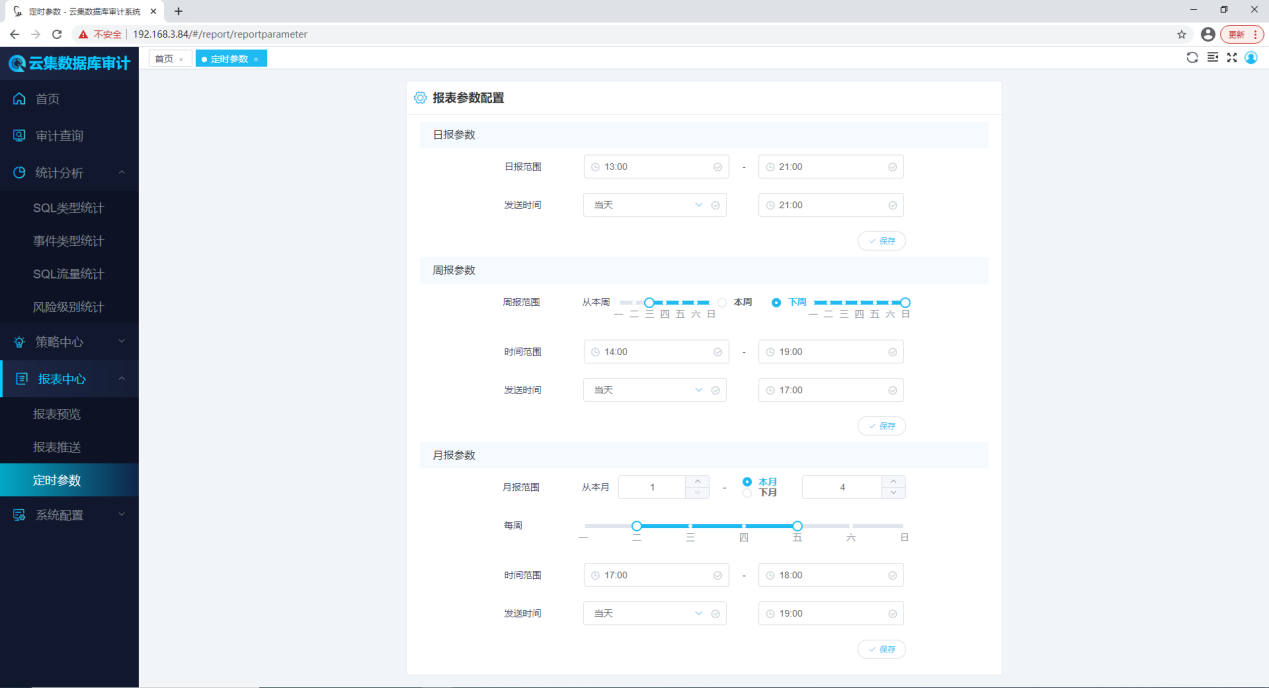
报表推送管理

鼠标左键点击左侧导航栏中的“报表中心->报表推送”，进入“报表推送”页面，选中页面中左侧的报表模板的某一项，点击左上角添加报表，跳入添加报表页面，填入相应的信息，进行添加报表信息。如下图所示：



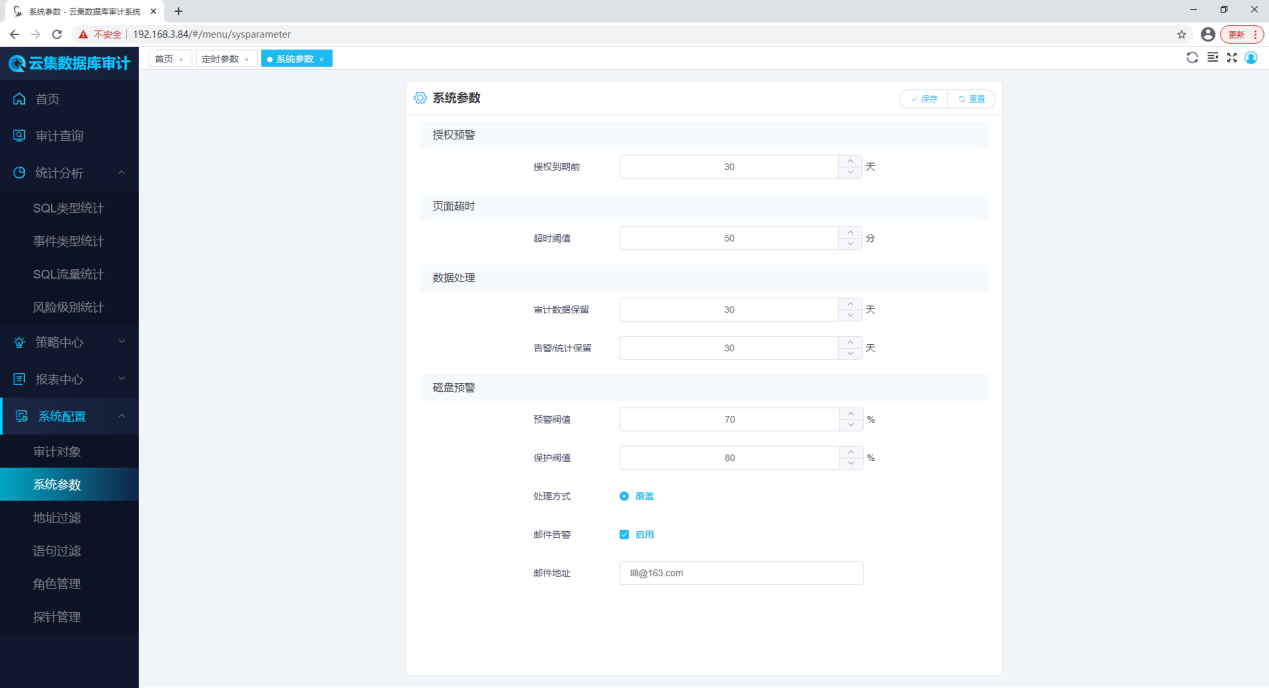
### 报表定时参数配置

接收自动报表，首先要进行报表配置，鼠标左键点击左侧导航栏中的“报表中心->定时参数”，进入“定时报表配置”页面。此页面分为日报，周报，月报三部分，对于这三部分进行选择，每一部分进行点击保存，进行每一段的时间报表配置。如下图所示：



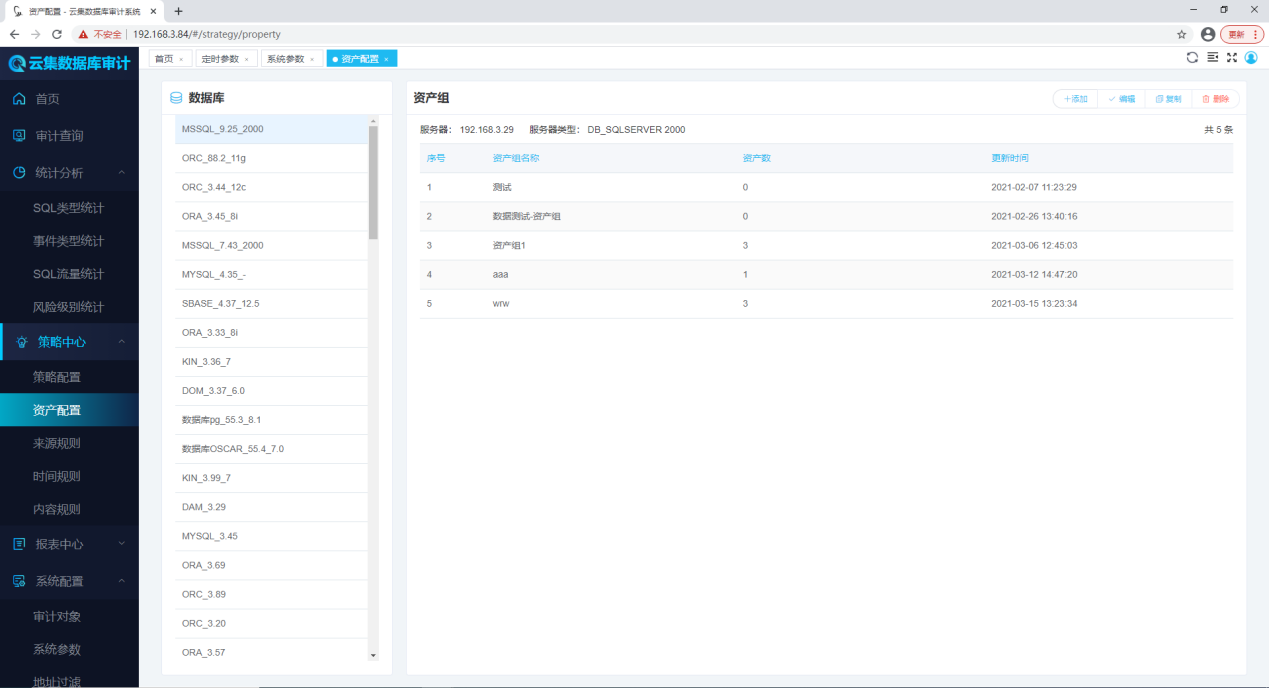
## 安全配置

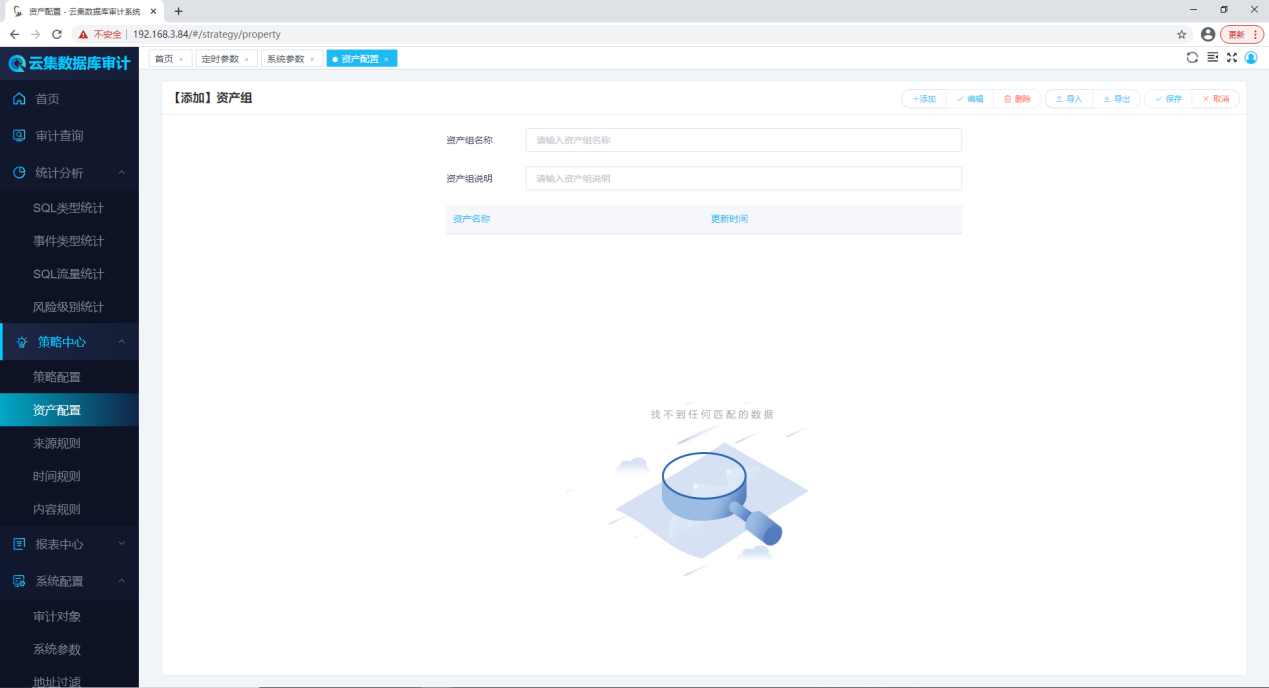
已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“系统配置”，可以进行“授权预警”与“页面超时”配置，在安全登录页面，可以进行“连续登陆失败”、“系统锁定时间”、“账户密码长度”，“密码修改时间”配置，在“页面超时”页面可以配置用户在该设定时间段内未作出操作的页面超时时间设置。如下图所示：



## 资产配置

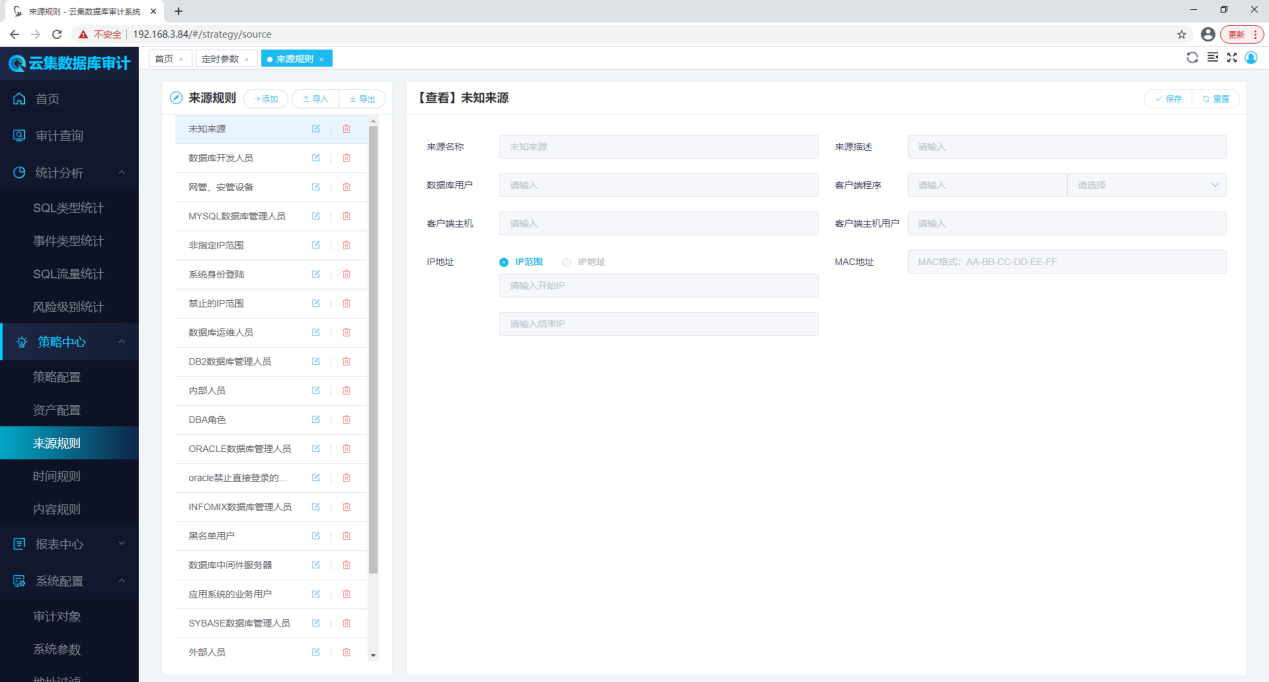
已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“策略中心->资产配置”显示所有的审计数据库服务器与每个服务器的详细信息，左上角可以添加数据库服务器，可以对每个服务器中的资产组进行新建，复制，编辑，删除，如下图所示：





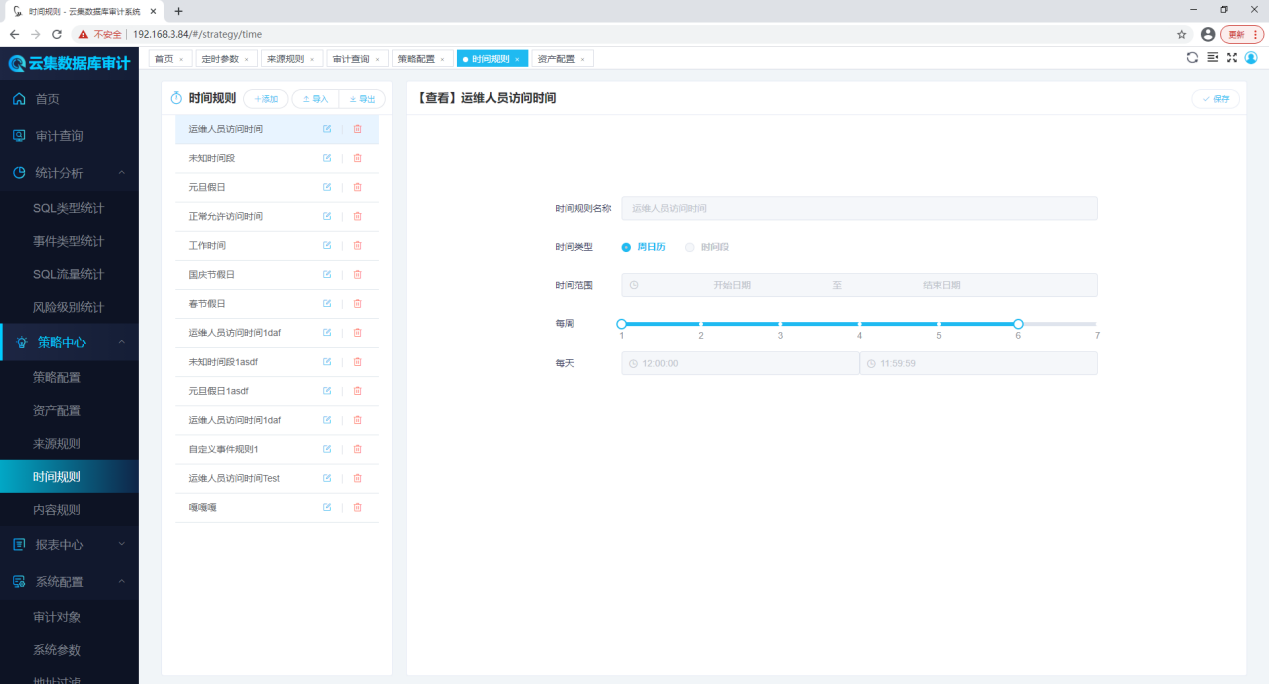
## 来源规则配置

已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“策略中心->来源规则”显示来源规则列表与列表内数据的详细信息，在列表上方有“导入”“导出”按钮，可以导入或导出规则列表中所有数据，点击某一条数据的编辑在右侧可以进行数据的修改，在左下角点击新建来源，在右侧添加数据点击保存添加至规则列表，如下图所示：



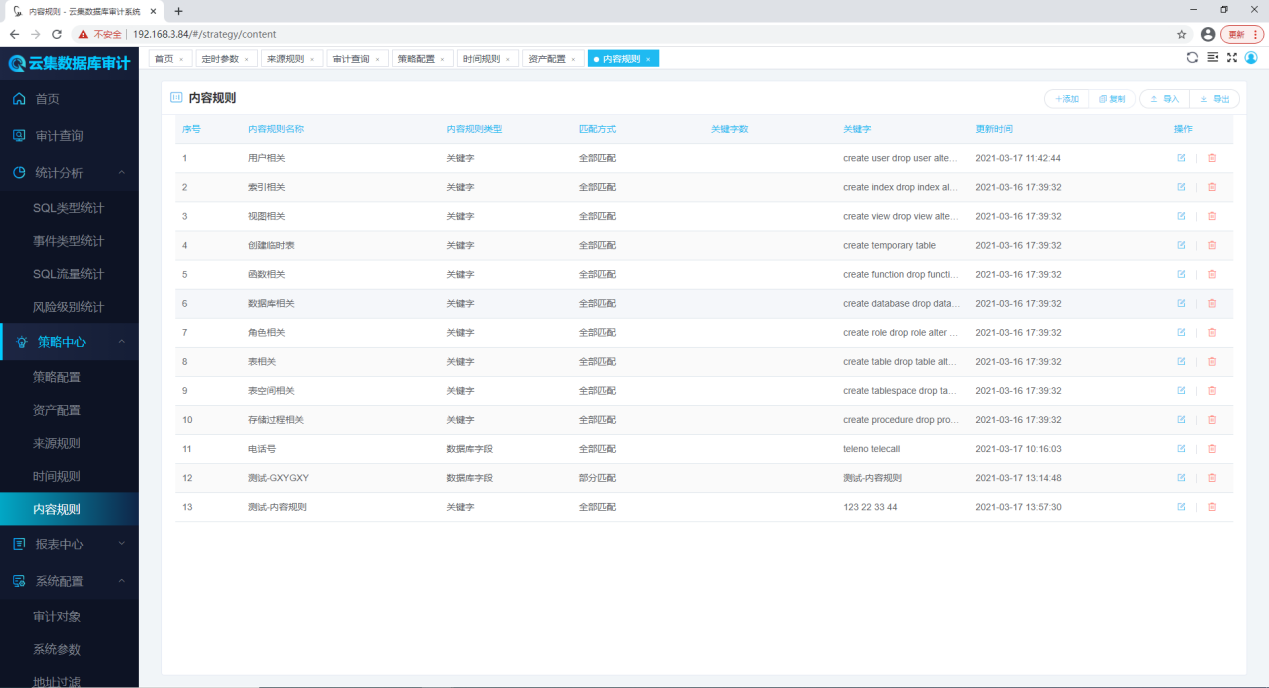
## 时间规则配置

已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中的“策略中心->时间规则”可以新建时间规则列表，也可以对选中的时间进行时间段的调整。



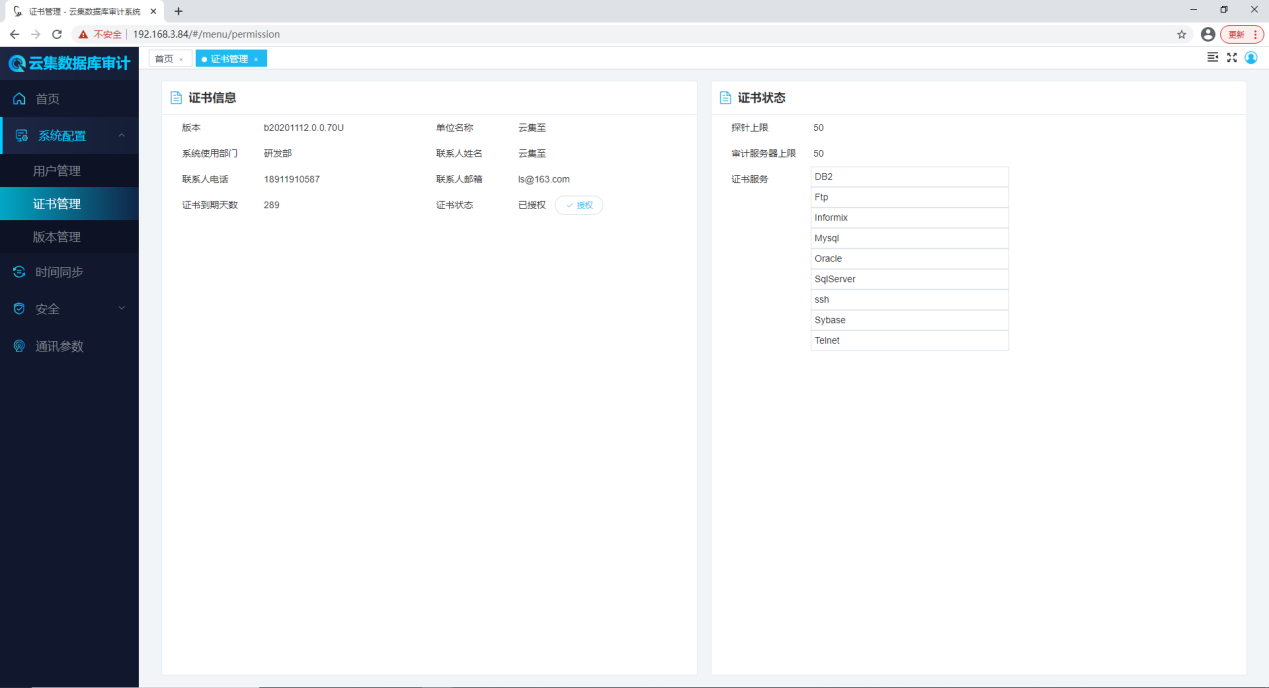
## 内容规则配置

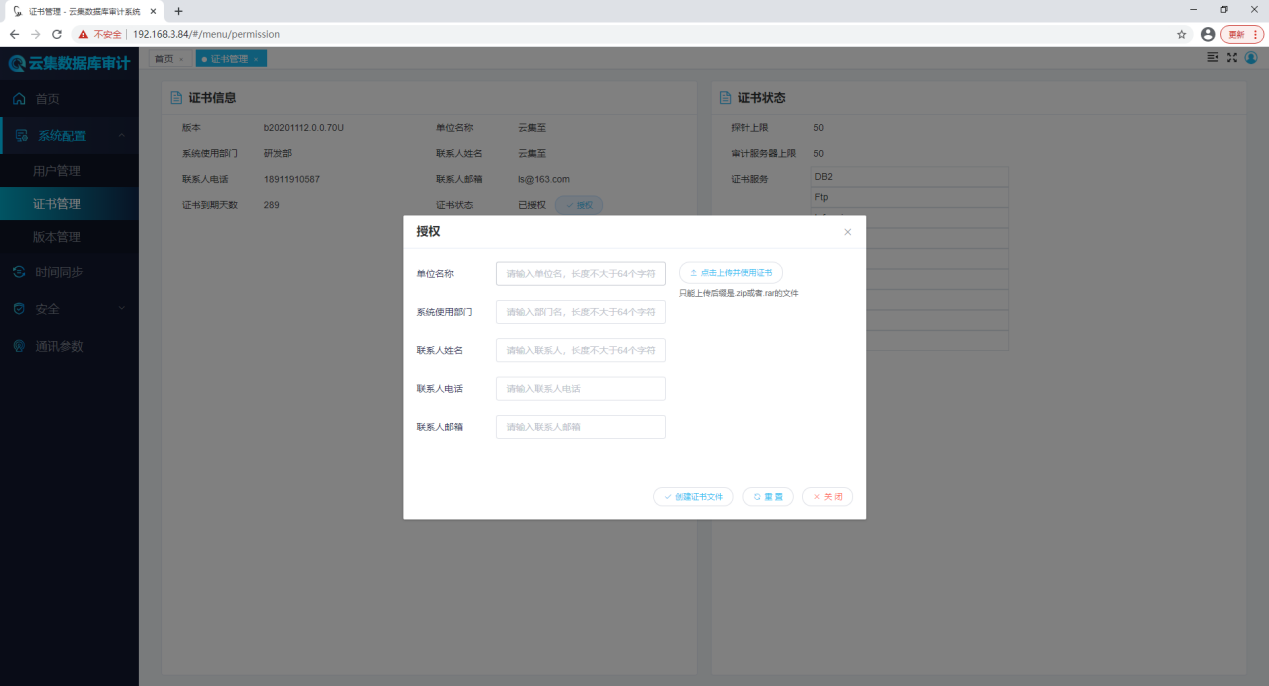
已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“策略中心->内容规则”显示内容规则列表，可以进行编辑、删除某一条详细信息，新建内容规则，导入和导出内容规则列表：



## 证书管理

已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“证书管理”，页面包含两部分“证书信息”和“证书状态”。在“证书信息”证书状态为未授权，点击“授权”按钮填入相应的信息对证书进行授权操作





## 过滤配置

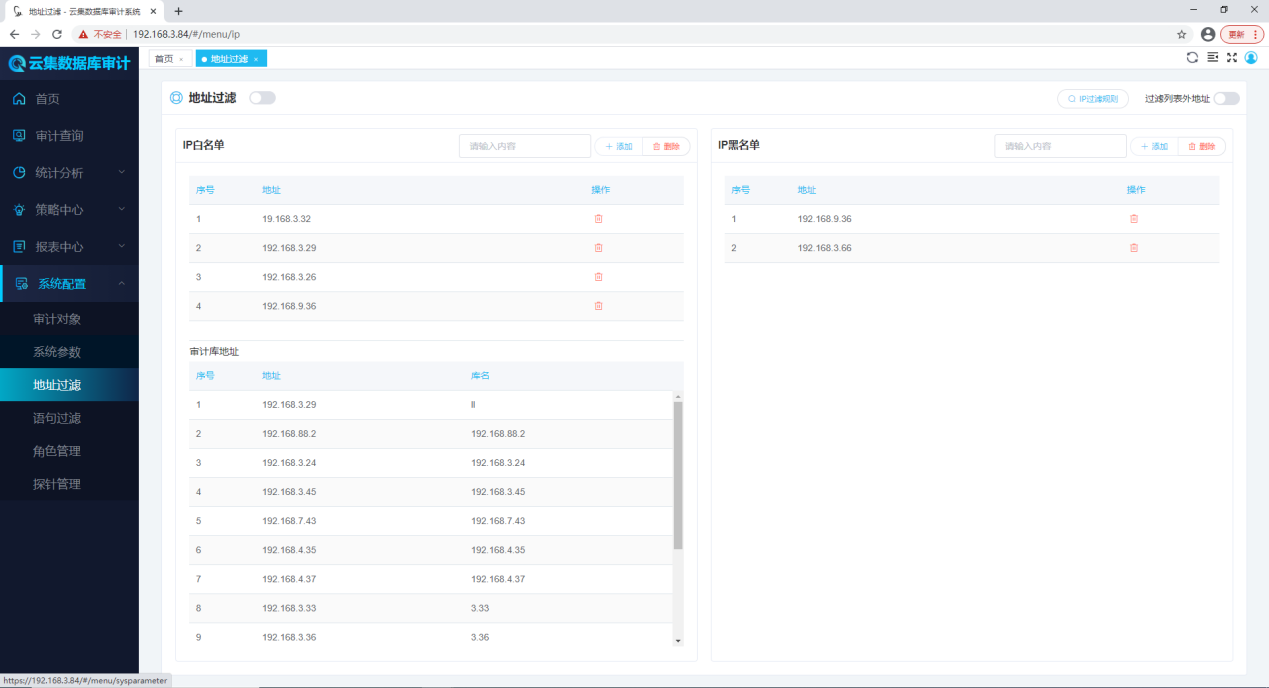
过滤分为“地址过滤”和“语句过滤”两种

### 地址过滤

设置当过滤条件没有命中时的操作，有两种类型的操作可选：

不采集：即当数据包没有被过滤条件命中时丢弃该数据包

采集：即当数据包没有被过滤条件命中时将该数据包提交给后续模块处理



### 语句过滤

已拥有数据库行为风险分析系统权限的用户登录系统，鼠标左键点击左侧导航栏中“系统配置->语句过滤”点击选中数据库类型，在右侧SQL语句过滤配置中在此数据库类型中添加SQL语句。

说明：开启SQL语句采集条件时，将自动过滤掉含有这些SQL语句的数据

