

**玖玖盾数据库防火墙系统**

**V3.0**

**用户使用手册**

2021年3月

**目 录**

[一. 华为云操作步骤 3](#_Toc72866941)

[二. 系统概述 6](#_Toc72866942)

[1. 简介 6](#_Toc72866943)

[2. 关键性特点简介 7](#_Toc72866944)

[3. 使用限制和约束 8](#_Toc72866945)

[三. 操作指导 8](#_Toc72866946)

[1. 系统管理 8](#_Toc72866947)

[2. 操作指南 8](#_Toc72866948)

[安全防护类 9](#_Toc72866949)

[2.1. 资产管理 9](#_Toc72866950)

[2.2. 策略防护 11](#_Toc72866951)

[2.3. 日志检索 32](#_Toc72866952)

[2.4. 风险管控 34](#_Toc72866953)

[2.5. 报表分析 39](#_Toc72866954)

[系统管理类 41](#_Toc72866955)

[2.6. 设备管理 41](#_Toc72866956)

[2.7. 日志管理 47](#_Toc72866957)

[2.8. 用户管理 48](#_Toc72866958)

[系统审计类 52](#_Toc72866959)

[2.9. 操作审计 52](#_Toc72866960)

[3. 系统常用操作 53](#_Toc72866961)

[3.1. 业务启动 53](#_Toc72866962)

[3.2. 业务停止 53](#_Toc72866963)

[3.3. 上电断电 53](#_Toc72866964)

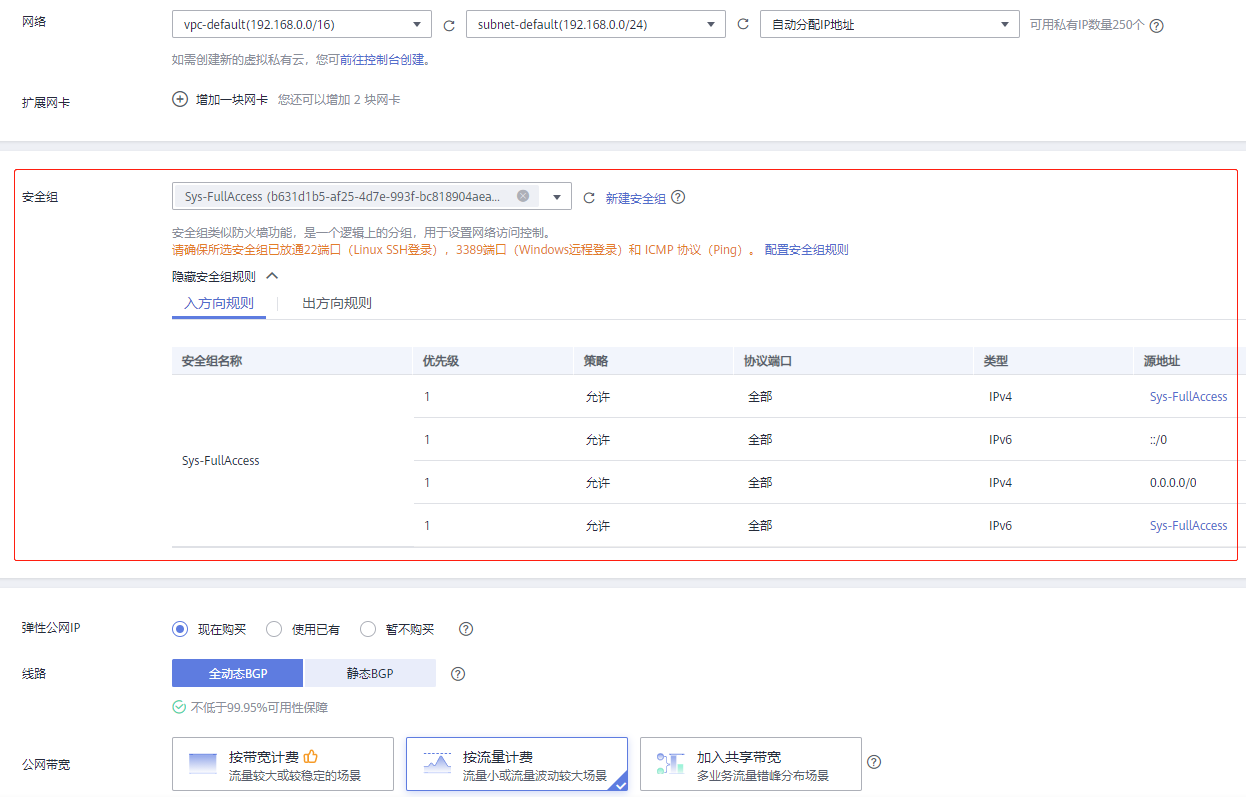
[4. 快速入门 53](#_Toc72866965)

# 华为云操作步骤

1.购买防火墙镜像或云服务器



2.安全组注意端口放行



3.设置云服务器的账号密码



4.购买完成后，在控制台处选择远程登录-VNC登录



5.新建用户（可跳过）

因镜像禁止使用root用户通过ssh访问，如有远程登录需要，可通过一般用户登录后，再切换root用户。

相关命令如下：

Adduser sirius *//添加一个新用户，名字叫Sirius*

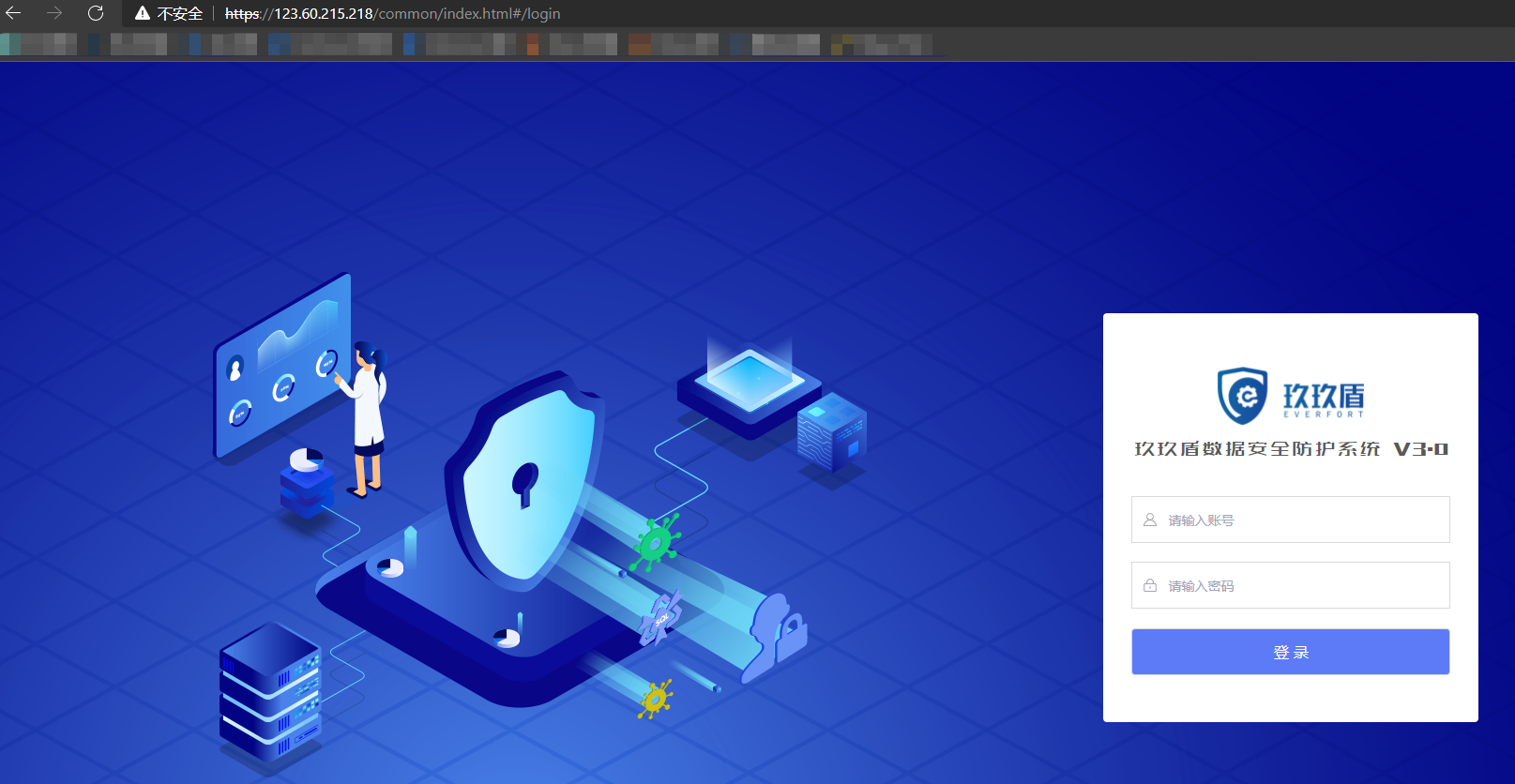
passwd sirius *//设置用户密码*

su root *//切换root用户*

6.重启NetworkManager服务

systemctl restart NetworkManager

7.通过<https://ip>访问系统



# 系统概述

## 简介

玖玖盾数据库防火墙系统，是由玖玖盾数据科技有限公司开发的具有完全自主知识产权的数据库防护产品。能够对数据库所面临的风险进行多方位的评估，以直路或旁路方式部署在数据库之前，隔离应用于运维环境。采用透明网桥的形式对数据库的所有访问行为进行监控分析，并根据策略阻断未授权、高危操作。

玖玖盾数据库防火墙主要适用场景大体分为三部分：

1、应对黑客攻击，拦截多种类型的攻击场景，如：SQL注入攻击、数据库漏洞攻击、拖库、撞库等。

2、数据库高权限管控场景，主要针对数据库访问操作进行细粒度的访问控制和限制，阻止不同操作行为的风险。

3、运维风险管控场景：运维内部经常发生删库、批量数据操作和数据库高危操作等，管控运维内部人员的危险行为。

## 关键性特点简介

1.独立访问控制

玖玖盾数据库防火墙通过接管数据库访问，并针对SQL协议进行解析，实现独立于数据库权限体系之外的访问控制功能。支持添加内置和自定义访问控制规则、支持经典的黑白名单以及基于机器学习的智能动态基线机制。

2.SQL注入攻击防御

玖玖盾数据库防火墙通过分析SQL语法来识别SQL注入攻击的不同特征，同时构建SQL注入特征库，对外来SQL注入攻击进行特征库匹配。同时基于玖玖盾数据独有的SQL序列智能检测发明专利，快速有效的对SQL注入攻击进行拦截阻断。支持sqlmap攻击防御。

3.漏洞攻击防护

基于传统数据库补丁升级带来的业务影响，玖玖盾数据库防火墙有针对性的开发虚拟补丁功能。通过内置缓冲区溢出、拒绝服务等多种数据库虚拟补丁规则，涵盖数十种数据库类型，在数据库外层构建漏洞攻击的专项防护，有效规避数据库被攻击的风险。

4.风险检测与处置

玖玖盾数据库防火墙对识别的风险访问行为记录高风险告警日志，并进行阻断。告警信息根据匹配的策略进行分类后统计汇总。对于系统产生的误报警，可以分别进行处理，提高防护策略的精确性，支持告警日志外发：SYSLOG、SNMP。

5.全面日志审计

玖玖盾数据库防火墙能够对访问数据库的行为进行详细的特征识别，包括：数据库用户名、源应用程序名、IP地址、请求的数据库、表、执行的语句，风险等级等信息。并提供灵活的查询分析功能。

## 使用限制和约束

1. 切勿自行更换操作系统
2. 切勿随意卸载数据库防火墙软件
3. 切勿任意登录到系统后台对系统文件进行修改
4. 不建议在服务器系统安装杀毒软件
5. 不建议在服务端使用第三方缓存工具，例如SuperCache等软件，这可能导致服务异常出现一系列异常状况

# 操作指导

## 系统管理

数据库防火墙系统采用B/S架构，通过浏览器对系统进行管理。系统默认管理URL为<https://19.168.0.254>。

数据库防火墙系统WEB页面基于三权分立原则设计，具有三个不同权限的管理员，分别负责不同的功能配置，具体权限分配如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 用户名 | 缺省密码 | 角色 | 负责功能模块 |
| **sysadmin** | everfort123 | 系统管理员 | 1、首页  2、资产管理  3、策略防护  4、日志检索  5、风险管控  6、报表分析 |
| **secadmin** | everfort123 | 安全管理员 | 1、设备管理  2、日志管理  3、用户管理 |
| **audadmin** | everfort123 | 审计管理员 | 1、操作审计 |

## 操作指南

数据库防火墙系统的主要功能分为三大类：安全防护、系统管理、系统审计。三大类别的功能分别对应三个管理员sysadmin、secadmin、audadmin。配置安全防护类功能需要使用sysadmin用户，配置系统管理类功能需要使用secadmin用户，配置系统审计功能需要使用audadmin用户。

系统管理类的主要功能项有：首页、资产管理、策略防护、日志检索、风险管控、报表分析。其中策略防护包括：策略设置、客户端过滤语句白名单、自定义策略、智能防护基线、虚拟补丁；风险管控包括：风险扫描、风险管理、风险发送；报表分析包括：报表配置、报表查看。

安全管理类的主要功能项有：设备管理、日志管理、用户管理。其中设备管理包括基础设置、时间配置、网卡配置、设备维护、升级恢复、高可用配置、服务配置；日志管理包括日志配置、备份还原；用户管理包括角色管理、账号管理、账号审核、安全配置。

系统审计类主要功能项有：操作审计。

## 安全防护类

使用sysadmin登录系统，可以对以下功能进行配置与管理。

### 资产管理

#### 资产配置

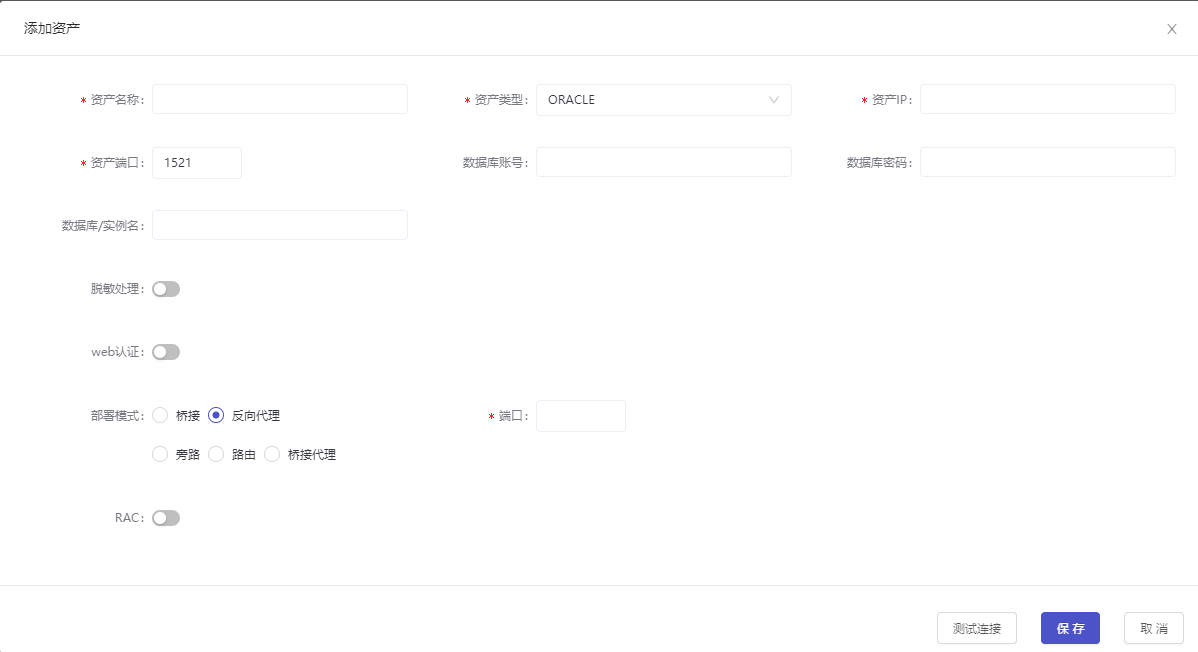
* **准备工作**

1、被防护的资产IP地址、端口号、资产类型、数据库账号、数据库密码、数据库名/实例名；

2、已经配置好的数据来源。

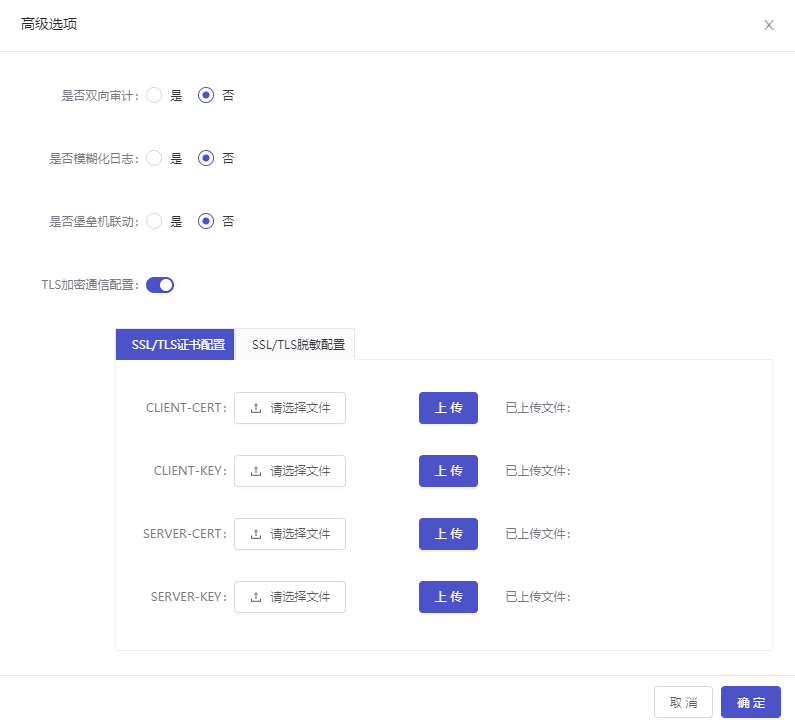
* **操作步骤**

1. 进入“资产管理”页面，单击“添加”，在弹出的对话框中输入资产名称、资产IP地址、端口号、资产类型、数据库账号、数据库密码、数据库名/实例名、资产节点IP、端口、域名等；选择数据库防火墙部署模式（如选择代理部署，需填写端口号9000-10000之间），单击“确定”，完成本次操作；



2、检查保护状态是否开启；

3、通过高级配置项可对已添加资产配置双向审计功能、模糊化日志功能、堡垒机联动功能和TLS加密通信配置。注：该TLS加密通信配置仅限于oracle资产。



#### TLS加密通讯配置

* **准备工作**

数据源访问经过TLS加密保护。

* **操作步骤**

1、进入“资产管理-TLS加密通讯配置”页面

2、按页面提示逐一输入TLS相关信息；

3、点击“保存”按钮完成配置。



### 策略防护

#### 策略设置-基本配置

* **准备工作**

1、已添加需要防护的资产

2、已配置防护规则（自定义策略、智能防护基线、虚拟补丁）

* **操作步骤**

1. 进入“基本配置”页面，选择需要策略防护的资产
2. 勾选已配置防护规则相对应的策略；



1. 点击勾选策略后的编辑按钮，进入规则选择页面；



4、勾选已配置的防护规则或选择该策略属性，点击“确定”按钮；

5、点击“基本配置”页面的“策略应用”按钮使策略生效。

#### 策略设置-集合配置

##### IP集

* **准备工作**

已知访问的客户端IP地址或客户端IP地址段

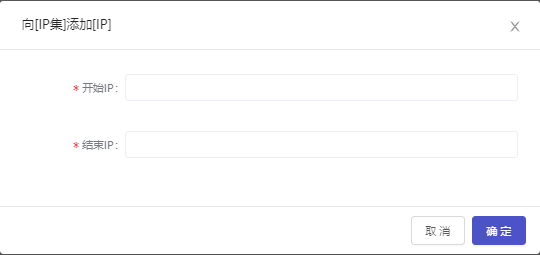
* **操作步骤**

1、进入“集合配置”页面；

2、单击“IP集”，单击“添加”按钮；



3、在弹出的对话框中输入“开始IP”、“结束IP”，单击“确定”按钮。



##### 源应用程序集

* **准备工作**

已知访问资产的客户端名称。

* **操作步骤**

1、进入“集合配置”页面；

2、单击“源应用程序集”，单击“添加”按钮；



3、在弹出的对话框中输入“应用程序名称”，单击“确定”按钮。



##### 操作系统用户集

* **准备工作**

已知的访问资产的操作系统用户名。

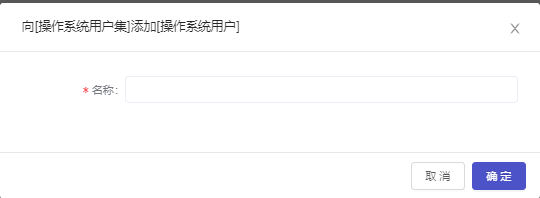
* **操作步骤**

1、进入“集合配置”页面；

2、单击“操作系统用户集”，单击“添加”按钮；



3、在弹出的对话框中输入用户名，单击“确定”。



##### 操作系统主机集

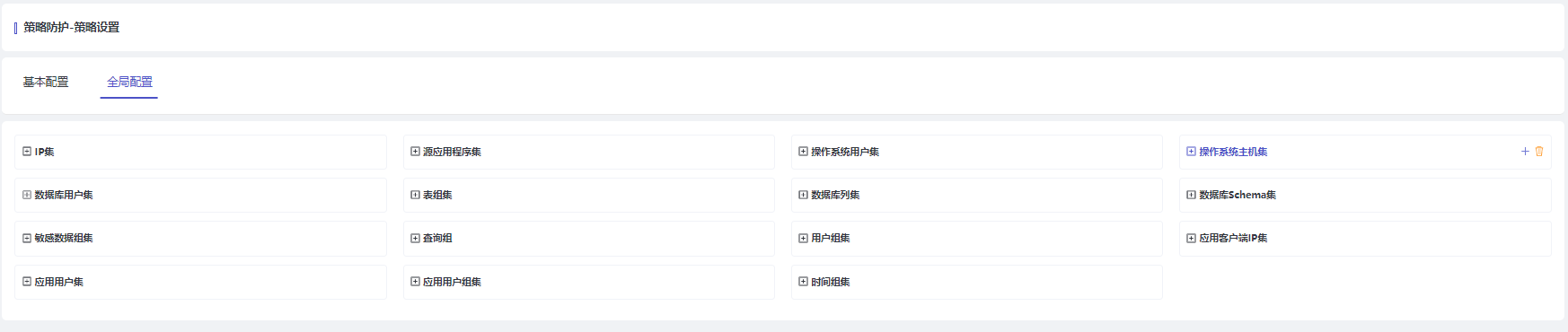
* **准备工作**

已知的访问资产的主机名

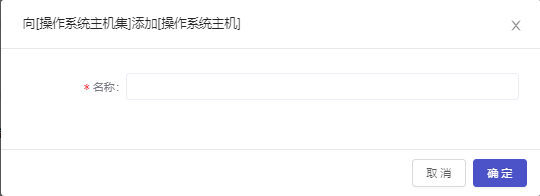
* **操作步骤**

1、进入“集合配置”页面；

2、单击“操作系统主机集”，单击“添加”按钮；



3、在弹出的对话框中输入主机名，单击“确定”按钮。



##### 数据库用户集

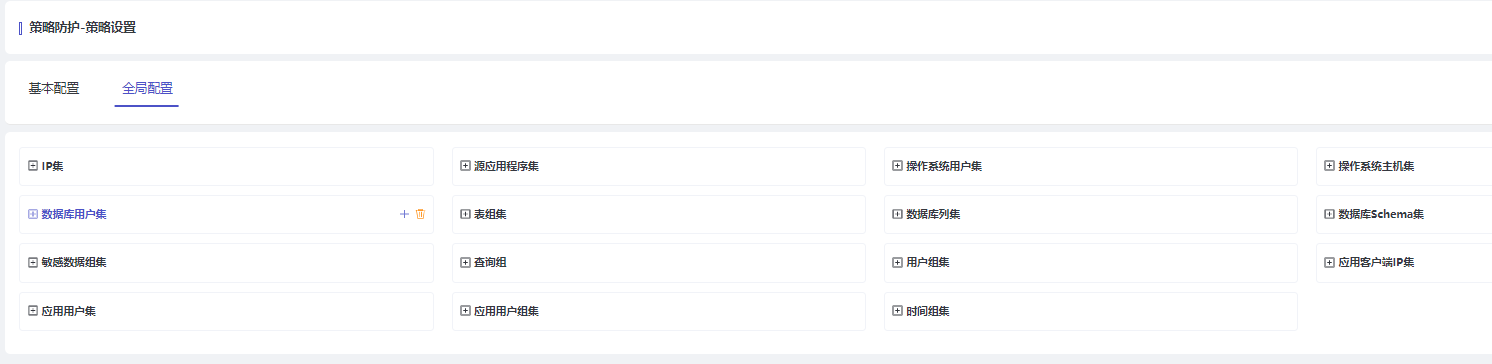
* **准备工作**

已知的资产用户名

* **操作步骤**

1、进入“集合配置”页面；

2、单击“数据库用户集”，单击“添加”按钮；



3、在弹出的对话框中输入数据库用户名，单击确定。



##### 表组

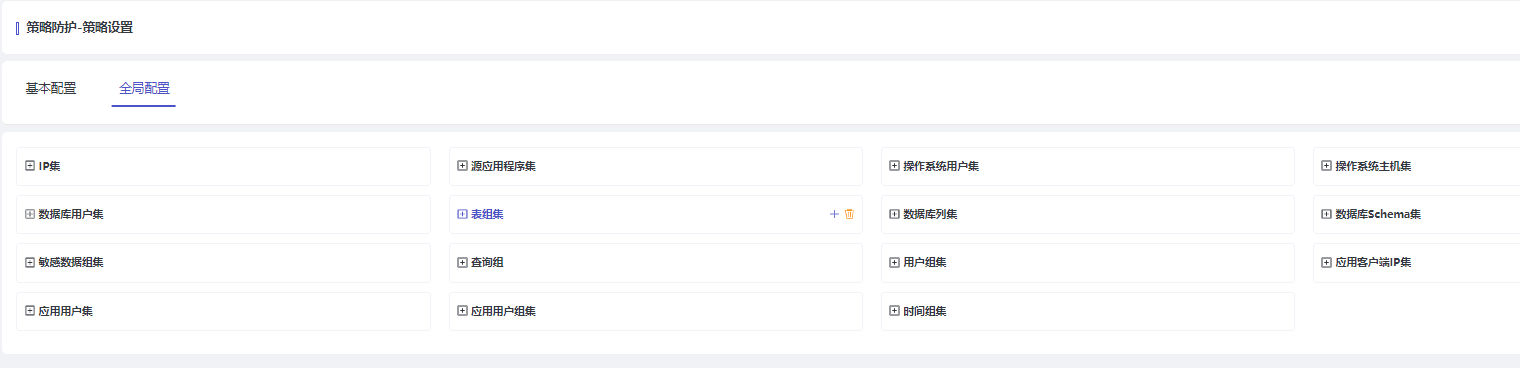
* **准备工作**

已知的表名称。

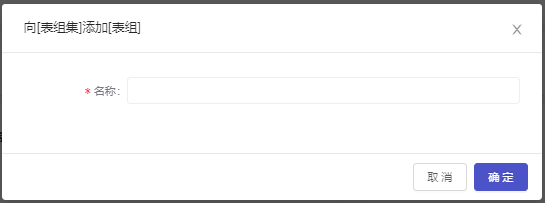
* **操作步骤**

1、进入“集合配置”页面；

2、单击“表组集”，单击“添加”按钮；



3、在弹出的对话框中输入表组名称，单击“确定”按钮；



##### 数据库列集

* **准备工作**

已知的列名称。

* **操作步骤**

1、进入“集合配置”页面；

2、单击“数据库列集”，单击“添加”按钮；



3、在弹出的对话框中输入列名，单击“确定”按钮。



##### 数据库Schema集

* **准备工作**

已知的数据库实例名、用户名。

* **操作步骤**

1、进入“集合配置”页面；

2、单击“数据库schema集”，单击“添加”按钮；



3、在弹出的对话框中数据库实例名、数据库用户，单击“确定”按钮。



##### 敏感数据集

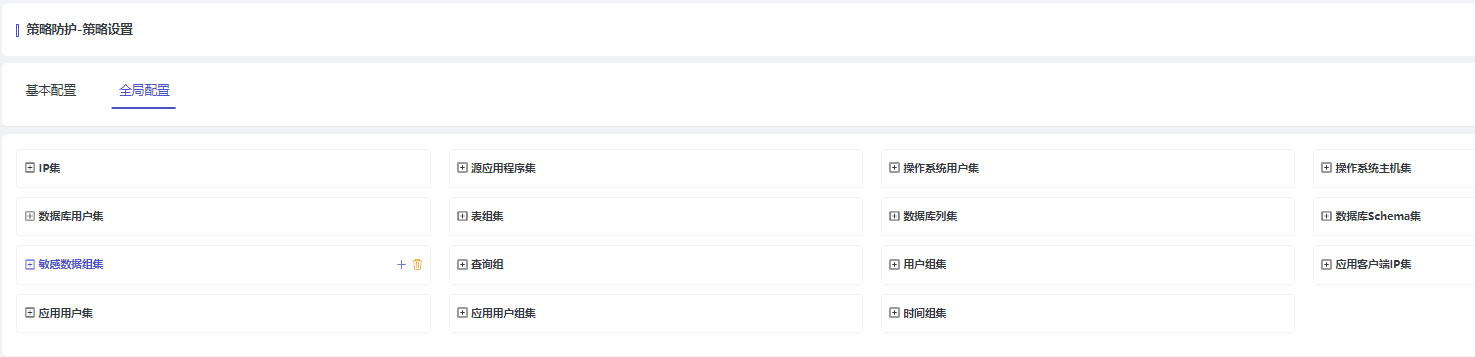
* **准备工作**

已知的敏感表名。

* **操作步骤**

1、进入“集合配置”页面；

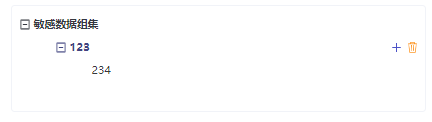
2、单击“敏感数据集”，单击“添加”按钮；



3、在弹出的对话框中输入敏感表集名称，单击“确定”按钮；



4、单击已经添加的敏感集名称，单击“添加”按钮。添加敏感数据；



##### 查询组集

* **准备工作**

**已知的表、操作。**

* **操作步骤**

1、进入“集合配置”页面；

2、单击“查询组集”，单击“添加”按钮；



3、在弹出的对话框中选择“资产类型”，输入SQL语句，单击“确定”按钮。



##### 用户组集

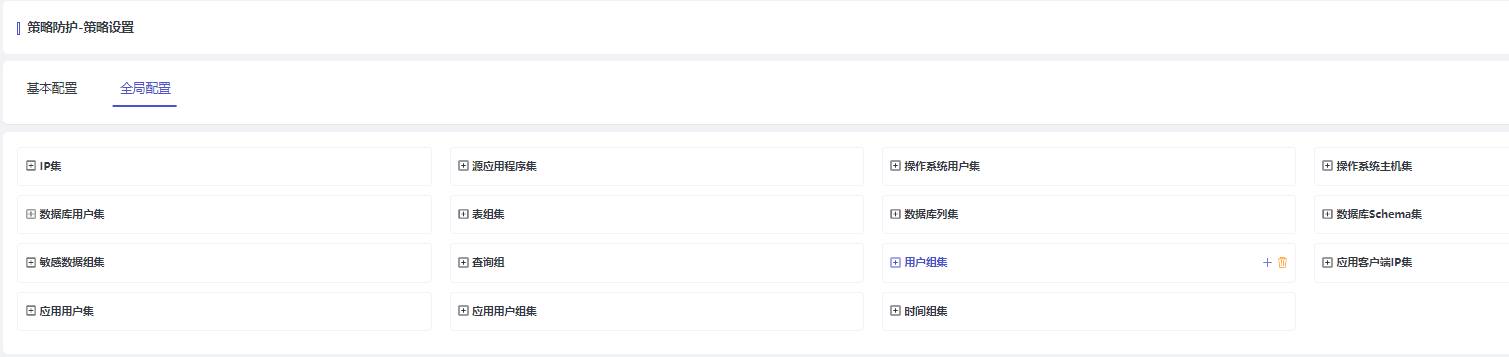
* **准备工作**

已知的资产用户。

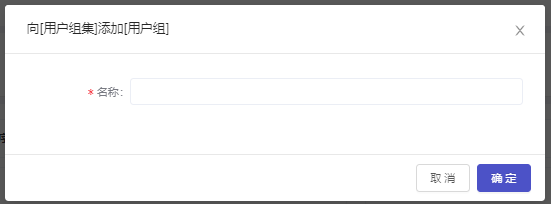
* **操作步骤**

1、进入“集合配置”页面；

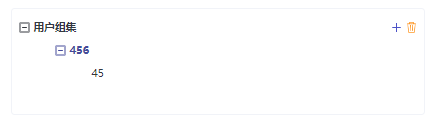
2、单击“用户集”，单击“添加”按钮；



1. 在弹出的对话框中输入用户组名称，单击“确定”按钮。



4、单击已添加的用户组集名称，添加数据库用户：



##### 应用客户端IP集

* **准备工作**

已知访问的应用系统客户端IP地址或应用系统客户端IP地址段

* **操作步骤**

1、进入“集合配置”页面；

2、单击“应用客户端IP集”，单击“添加”按钮；



3、在弹出的对话框中输入“开始IP”、“结束IP”，单击“确定”按钮。



##### 应用用户集

* **准备工作**

已知访问的应用用户

* **操作步骤**

1、进入“集合配置”页面；

2、单击“应用用户集”，单击“添加”按钮；



3、在弹出的对话框中输入应用用户名称，单击“确定”按钮。



##### 应用用户组集

* **准备工作**

已知的应用用户。

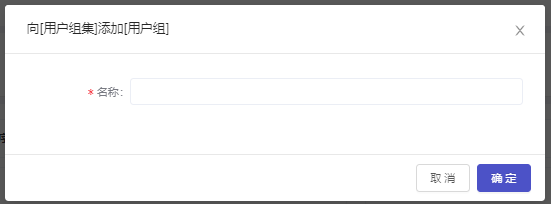
* **操作步骤**

1、进入“集合配置”页面；

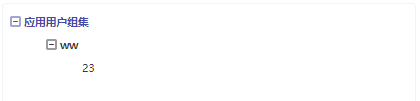
1. 单击“应用用户组集”，单击“添加”按钮；



3、在弹出的对话框中输入应用用户组名称，单击“确定”按钮。



4、单击已添加的应用用户组集名称，添加数据库用户：



##### 时间组集

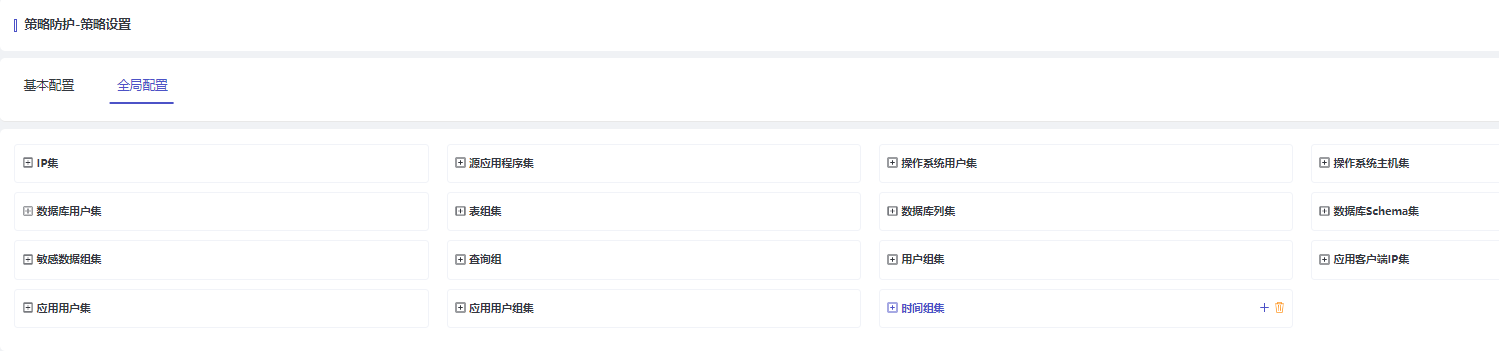
* **准备工作**

已知所需的时间段

* **操作步骤**

1、进入“集合配置”页面；

2、单击“时间组集”，单击“添加”按钮；



1. 在弹出的对话框中配置所需的时间段，单击“确定”按钮。



#### 超级白名单

* **准备工作**

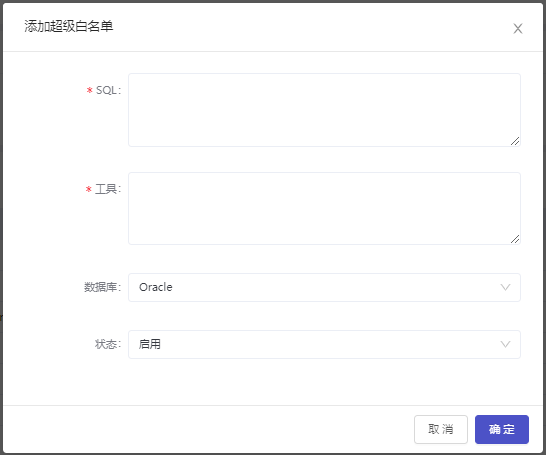
访问数据库的客户端工具；需过滤的客户端语句。

* **操作步骤**

1、进入“超级白名单”页面；

2、单击“添加”按钮；

3、弹出添加提示窗，根据页面提示信息填写需要过滤的语句信息。



1. 添加完成后可对列表中的语句信息进行编辑和删除操作。

#### 自定义策略

##### 添加策略与规则

* **准备工作**

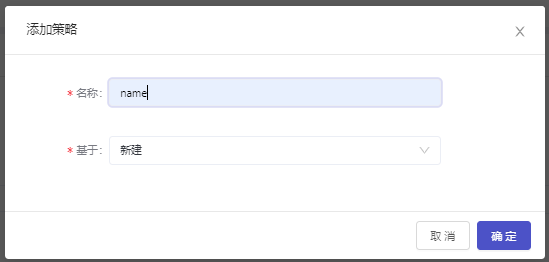
用户对数据库访问控制的实际需求

* **操作步骤**

1、进入“自定义策略”页面；

2、单击“SQL策略-添加策略”按钮；

3、弹出添加提示窗，填写策略名称，默认选择新建。



4、单击“确定”按钮，在页面左侧策略栏中显示新增的策略name



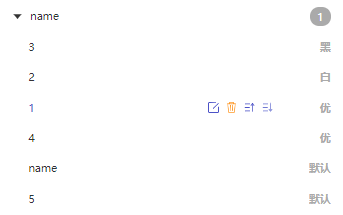
1. 点击name策略中的添加图标，添加防护规则。



1. 弹出添加提示窗，填写规则名称，规则防护类型为黑名单、白名单、优先级、默认。四种防护类型的优先级由高到低。



1. 单击“确定”按钮，在页面左侧策略栏中显示新增的规则



说明：

1. 优先级规则之间可通过上移或下移图标进行规则优先级调整。
2. 点击“自定义策略-hbase策略”进入hbase策略配置，配置方式同“SQL策略”配置。

##### 配置防护规则

* **准备工作**

已添加的策略和策略中的防护规则

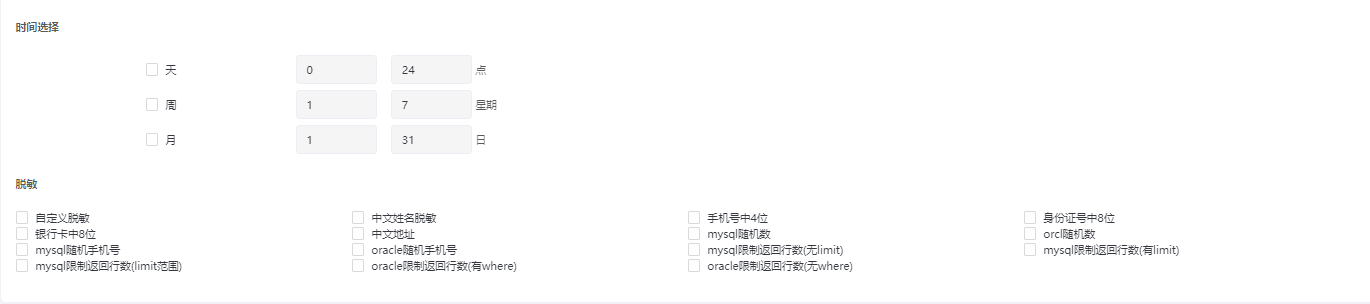
* **操作步骤**

1、进入“自定义策略-SQL策略”页面；

2、单击展开已添加的策略；

3、单击选择该策略下需要配置的防护规则，显示具体的配置项





1. 用户可根据具体的防护需求根据页面配置规则进行定义配置。

说明：

点击“自定义策略-hbase策略”进入hbase策略配置，防护规则配置方式同“SQL策略”配置。

#### 智能防护基线

##### 基线管理

* **准备工作**

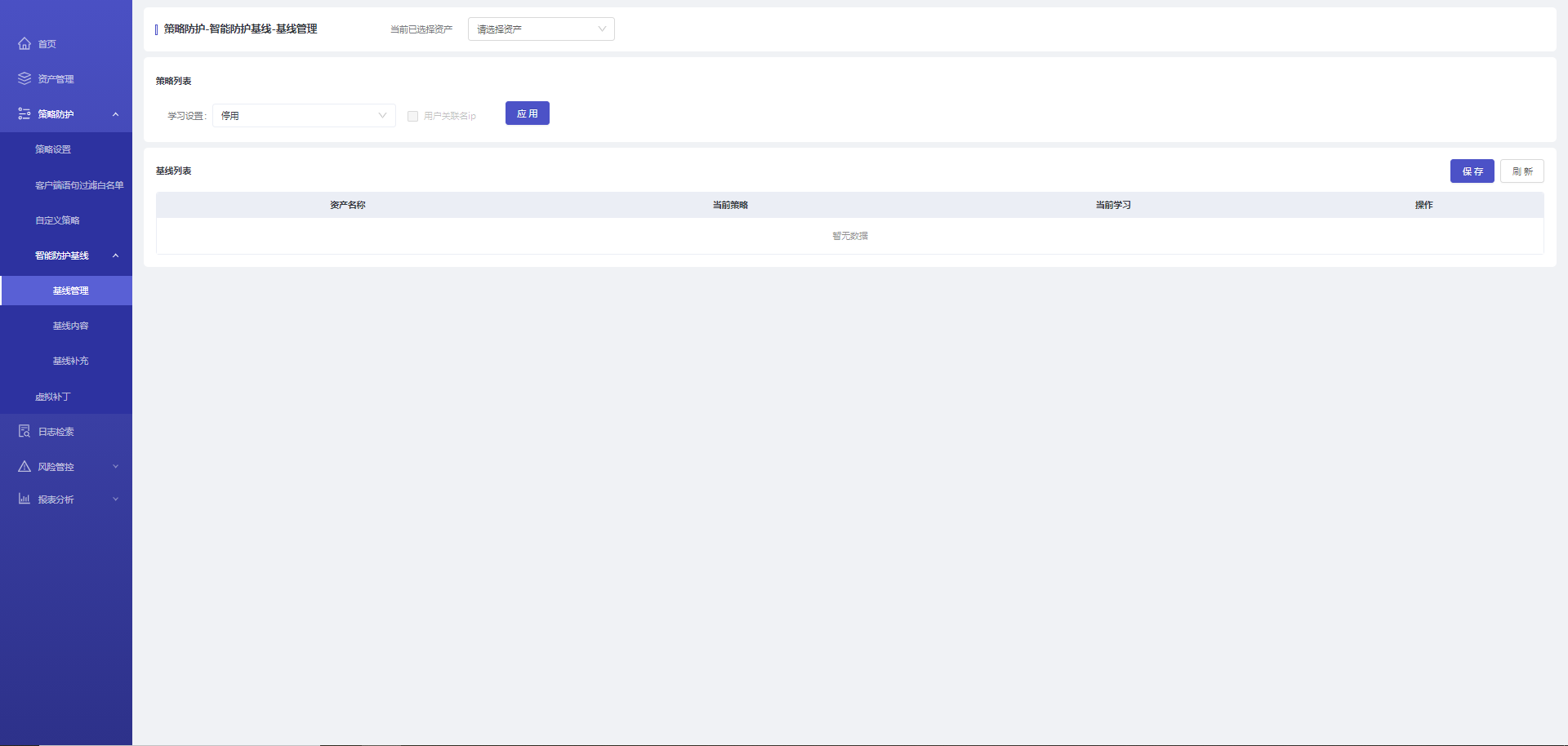
已选择的需要学习的资产

* **操作步骤**

1、进入“基线管理”页面；

2、单击学习设置选择启用基线学习，勾选“用户关联名ip”；

3、单击应用，开始学习数据库操作



##### 基线内容

* **准备工作**

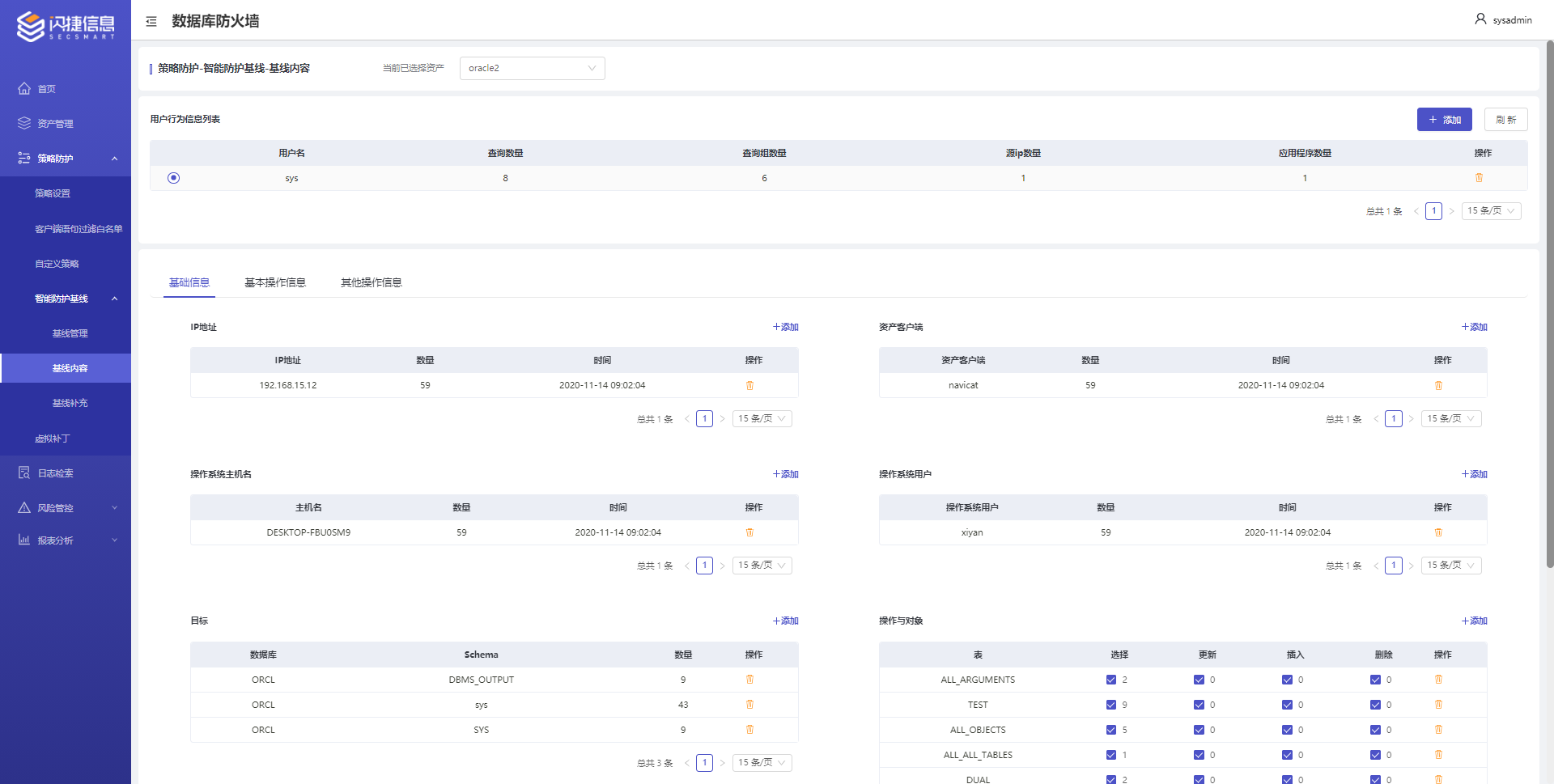
选择要查看的资产，并该资产已进行智能学习。

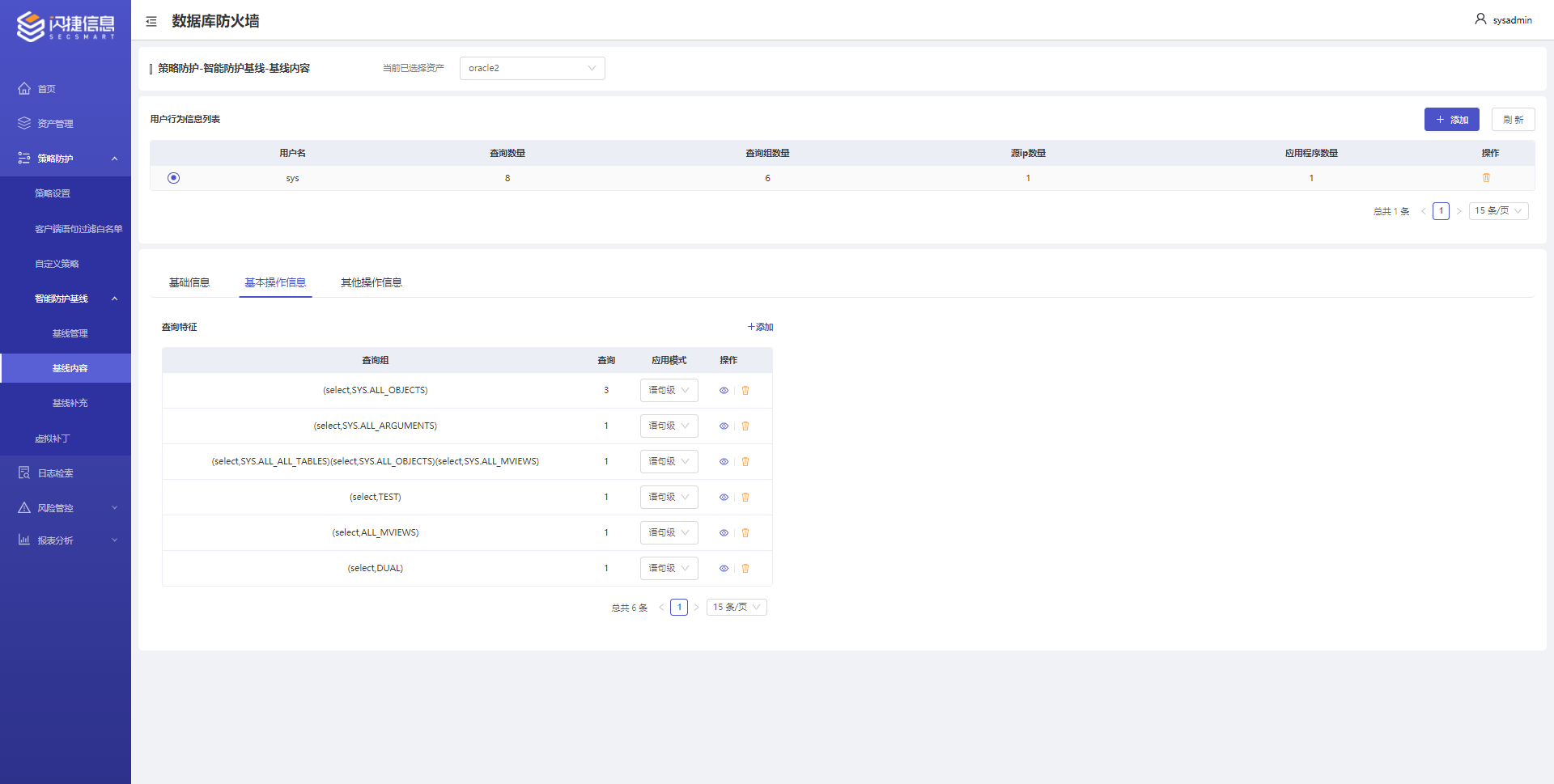
* **操作步骤**

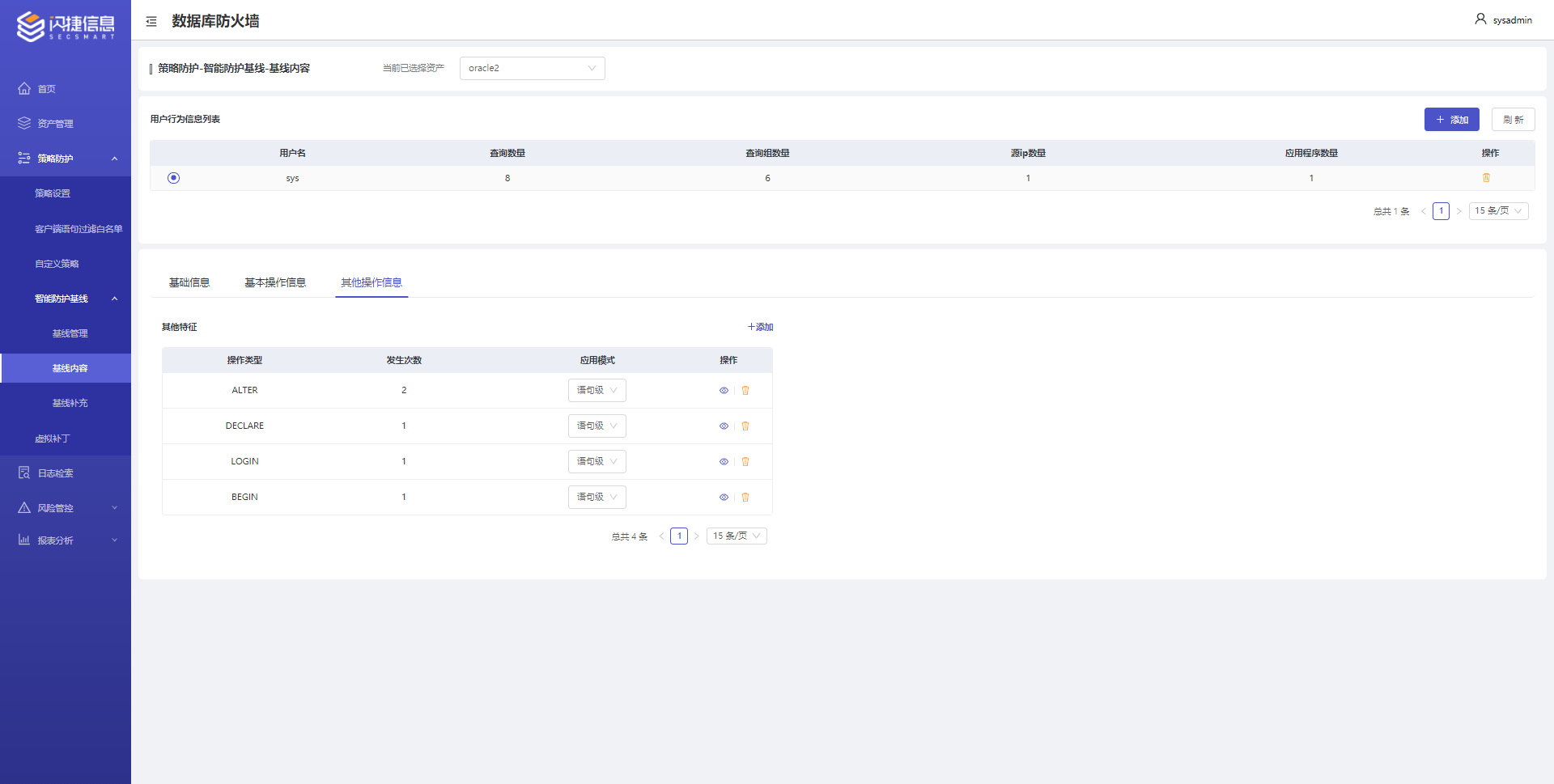
1、进入“基线内容”页面；

2、选择当前需要查看的资产，点击用户行为信息列表中的学习基线

3、在下方的“基础信息”、“基本操作信息”、“其他操作信息”中可查看学习内容的详情







##### 基线补充

* **准备工作**

选择要进行策略配置的资产。

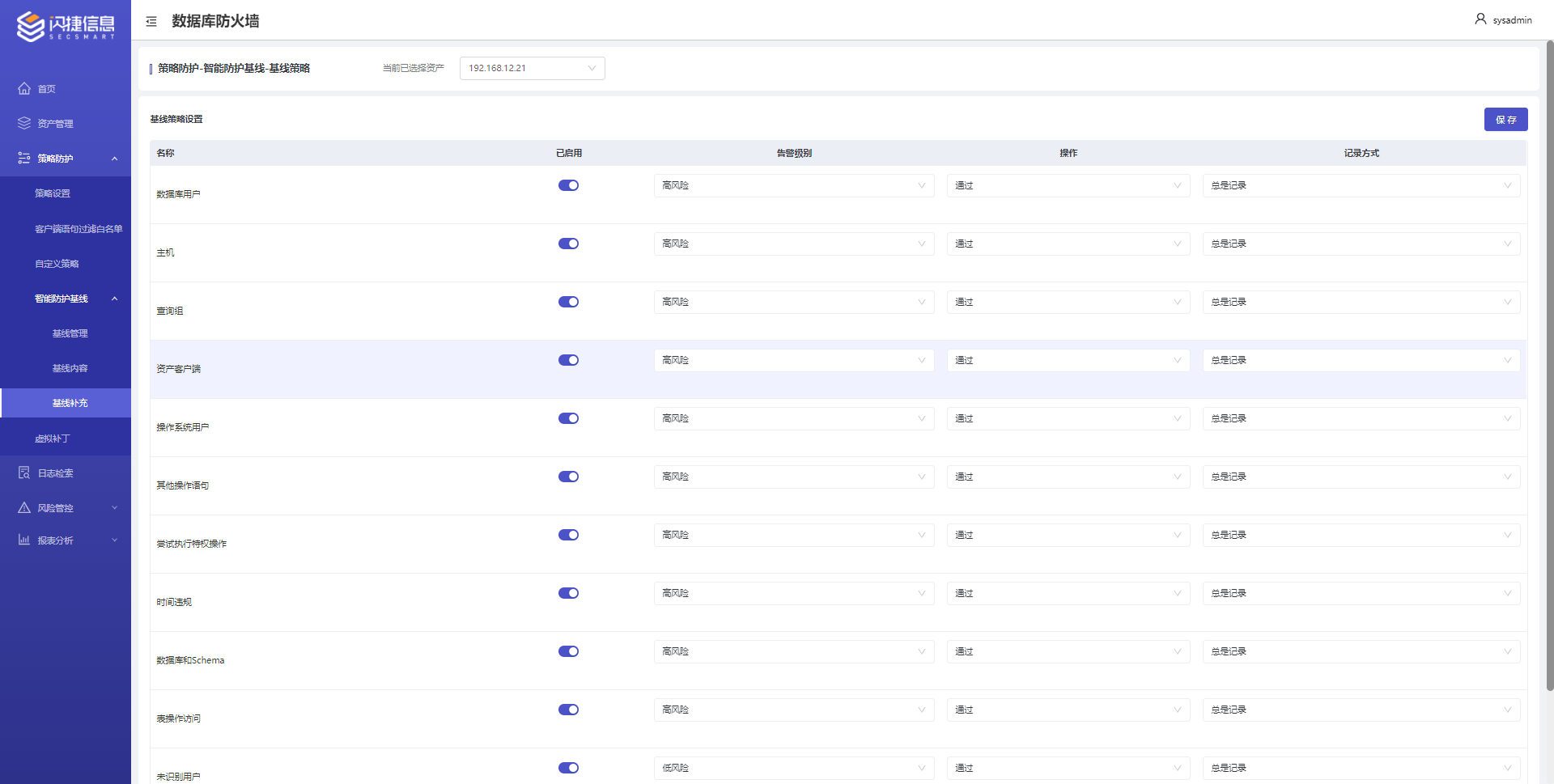
* **操作步骤**

1、进入“基线补充”页面；

2、选择当前需要自定义策略配置的资产

3、根据需要选择相应策略字段，并进行启用/停用、告警级别、通过/阻断、记录方式等详细配置

4、点击保存。



说明：该版本hbase资产暂不支持智能防护基线规则

#### 虚拟补丁

##### 虚拟补丁规则

* **准备工作**

选择要进行虚拟补丁防护的资产。

* **操作步骤**

1、进入“虚拟补丁-虚拟补丁规则”页面；

2、查找需要配置的虚拟补丁策略

3、点击该策略进行编辑



1. 点击确定进行保存。

说明：该版本hbase资产暂不支持虚拟补丁规则

##### 虚拟补丁规则例外

* **准备工作**

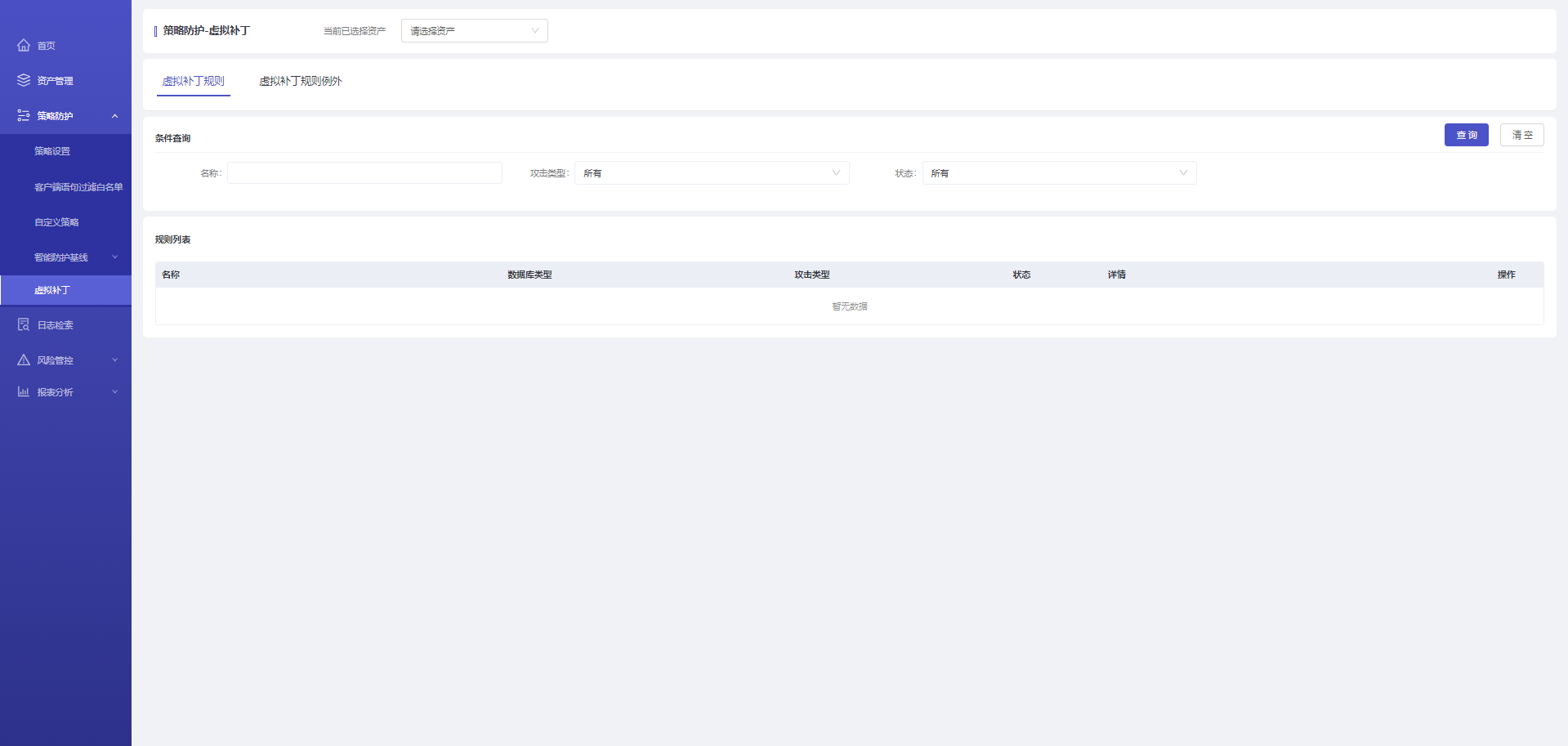
已在风险管控-风险管理中存在触发虚拟补丁策略的告警信息，并加入虚拟补丁规则例外

* **操作步骤**

1、进入“虚拟补丁-虚拟补丁规则例外”页面；

2、查看已加入的虚拟补丁例外规则

3、点击详情进行可对该规则进行删除操作



### 日志检索

#### 最新日志

* **准备工作**

已与数据库连接正常

* **操作步骤**

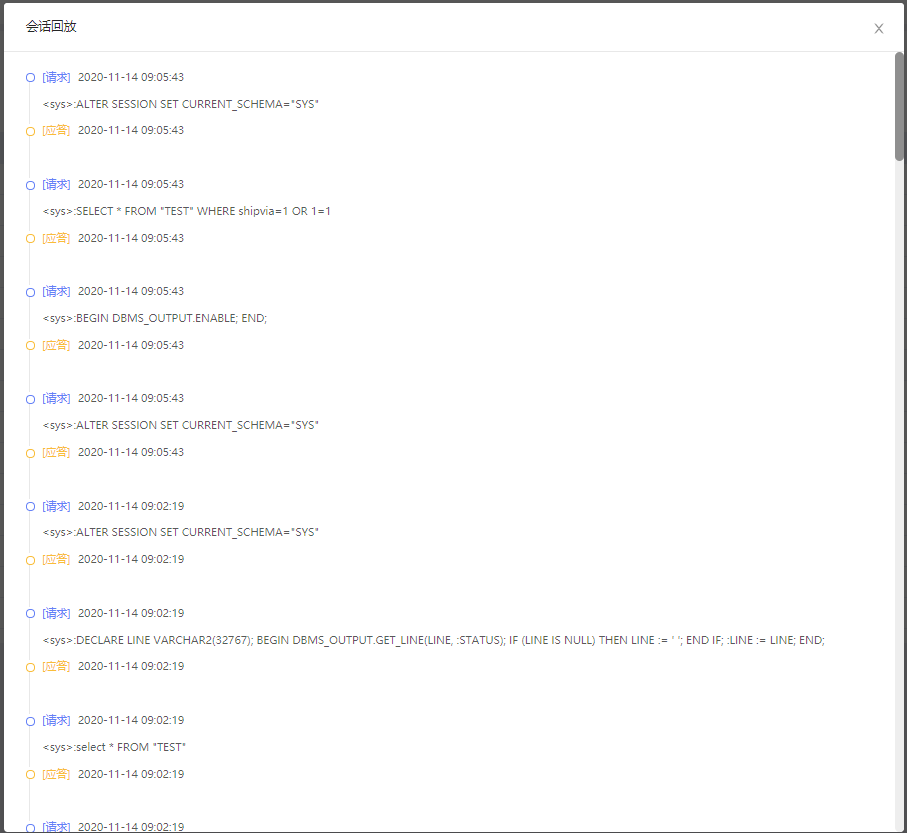
1、进入“日志检索-SQL日志-最新日志”页面；

2、查看已审计到的数据库操作日志

3、点击详情可查看该日志详细信息



4、点击回访可查看该日志的会话和操作记录



#### 检索列表

* **准备工作**

已产生审计日志

* **操作步骤**

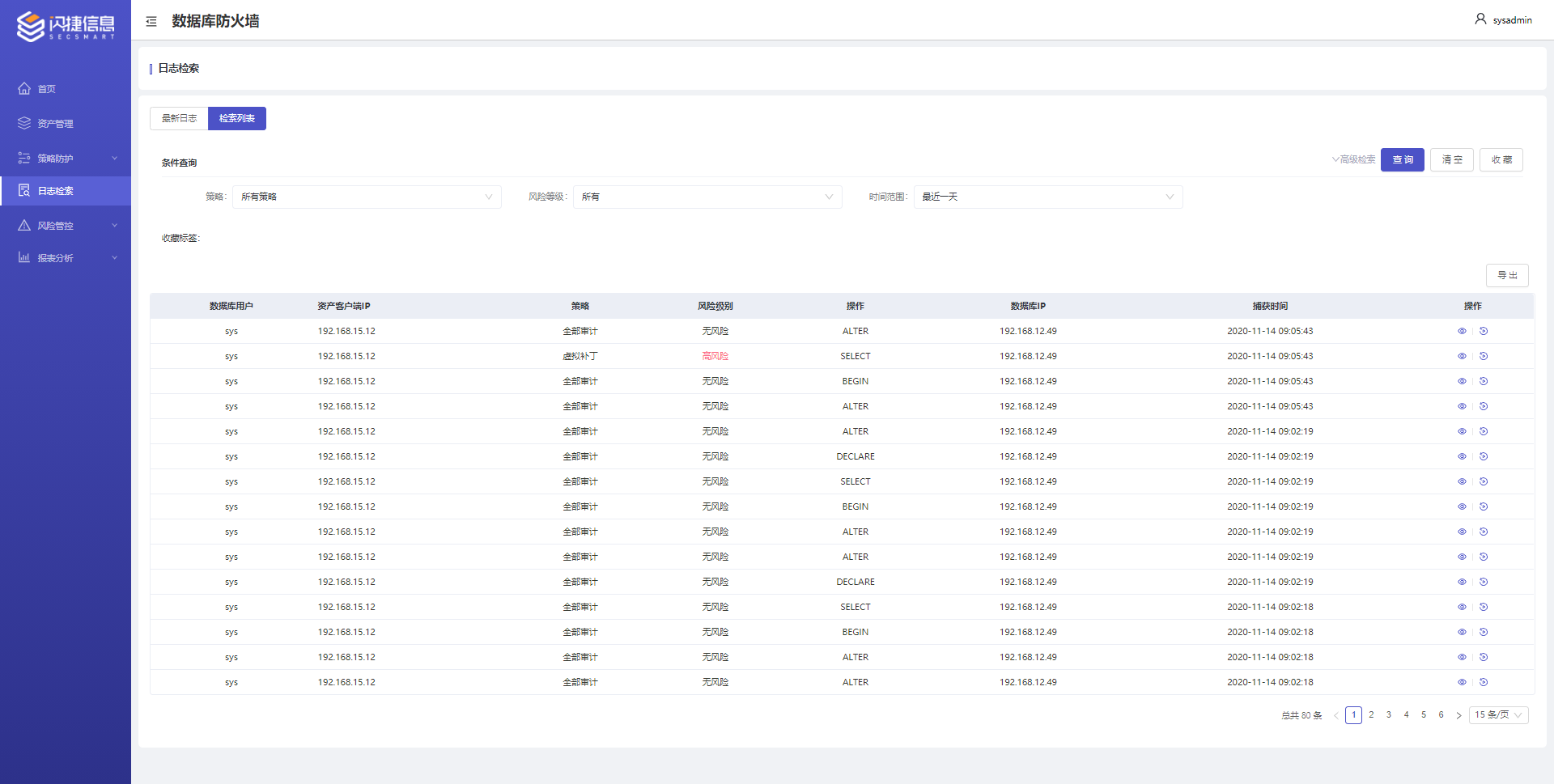
1、进入“日志检索-检索列表”页面；

2、点击高级检索功能，自定义检索条件进行配置

3、点击收藏按钮，对当前检索条件设置进行标签收藏



3、点击查询可看到检索结果



说明：如需查看hbase资产相关业务日志，需进入“日志检索-HBASE日志-最新日志/检索列表”页面进行查看和检索

### 风险管控

#### 风险扫描

* **准备工作**

已正确填写数据库（oracle、mssql、sybase）的登录信息并保证测试连接正常

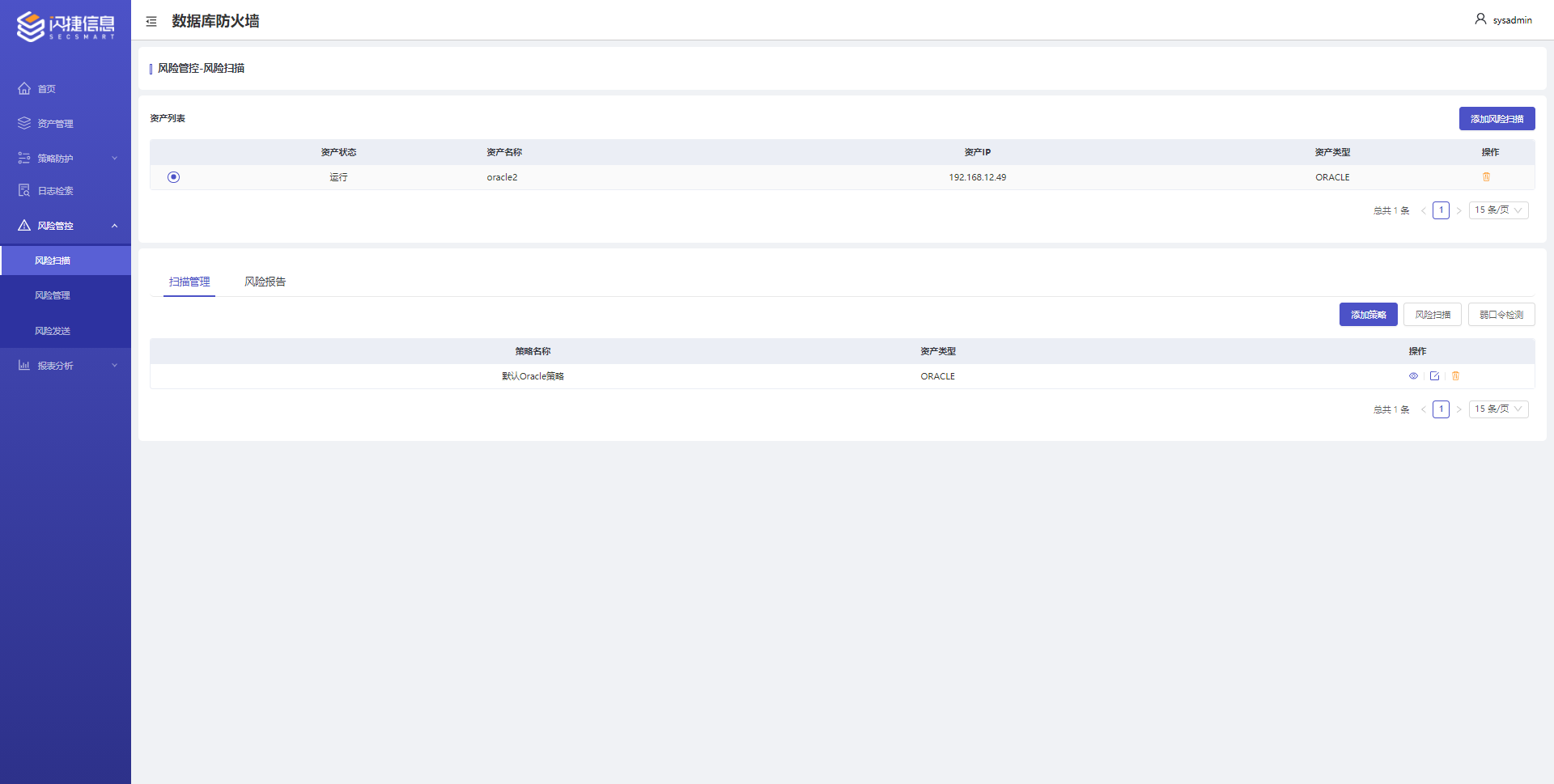
* **操作步骤**

1、进入“风险管控-风险扫描”页面；

2、点击添加风险扫描按钮，进行资产选择



3、点击确定按钮，添加完成



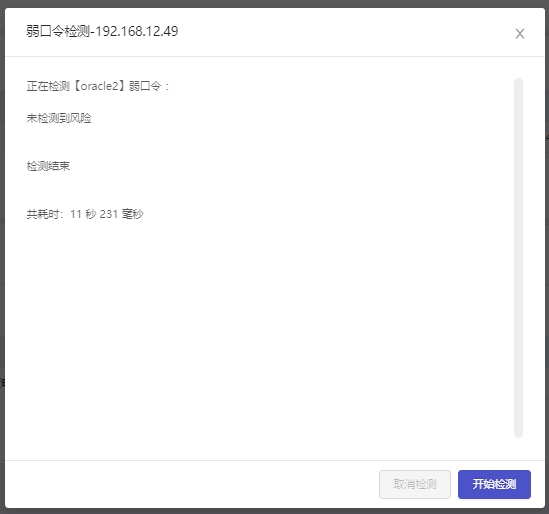
1. 对已添加资产进行风险扫描策略配置，点击添加策略进行配置。



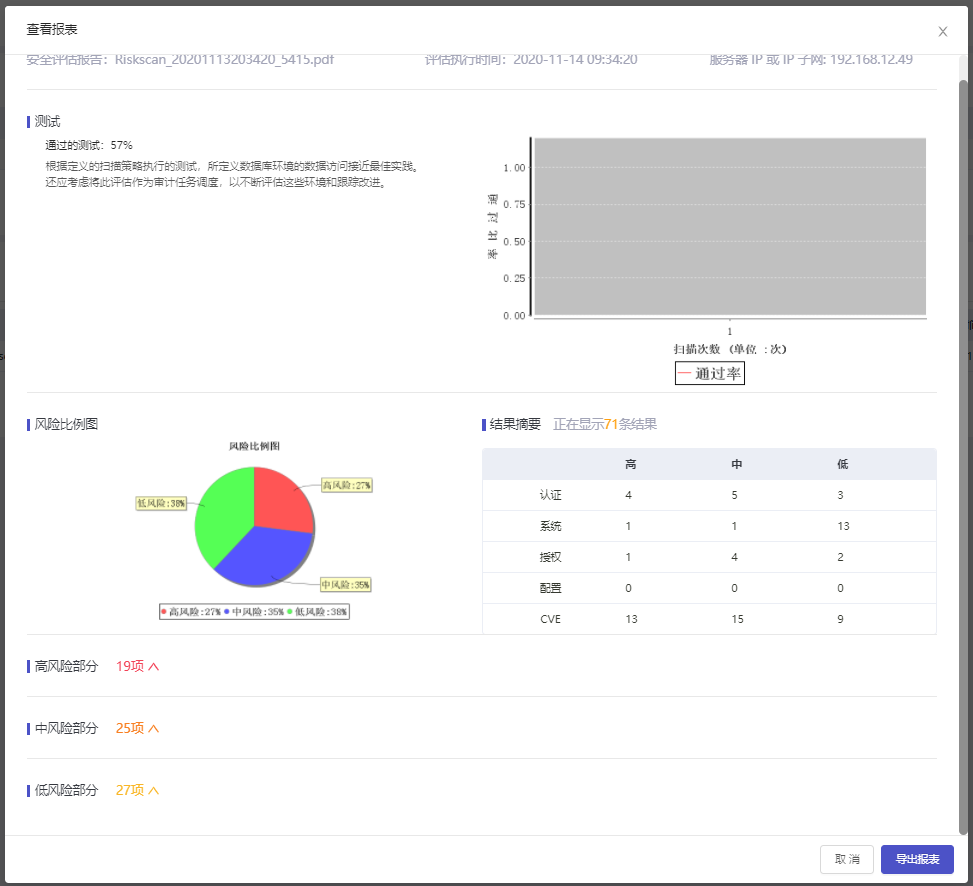
5、点击风险扫描按钮，在弹出框中选择扫描资产和策略，点击开始扫描



6、点击弱口令检测按钮，对当前选择的资产进行弱口令检测



7、点击风险报告进入页面，列表中显示出生成的风险扫描报告，点击详情进行报告查看，并可以导出报表



#### 风险管理

* **准备工作**

已产生风险告警信息

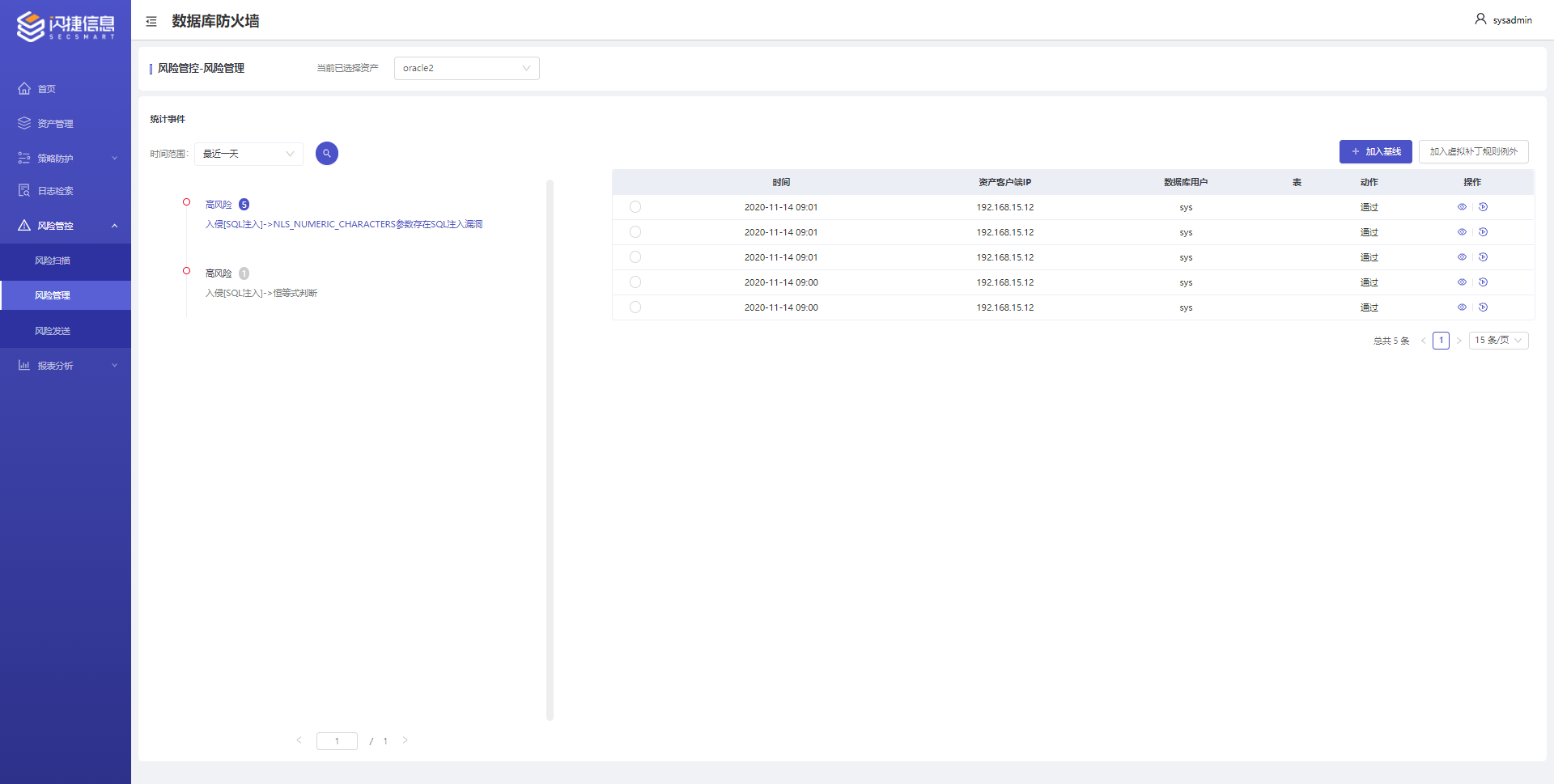
* **操作步骤**

1、进入“风险管控-风险管理”页面；

2、点击时间范围进行风险告警检索

3、选中告警，可进行详情查看和回放查看（同日志检索-最新日志功能）

4、可对选中的风险告警进行加入基线或加入虚拟补丁规则例外



#### 风险发送

* **准备工作**

已产生风险告警信息

* **操作步骤**

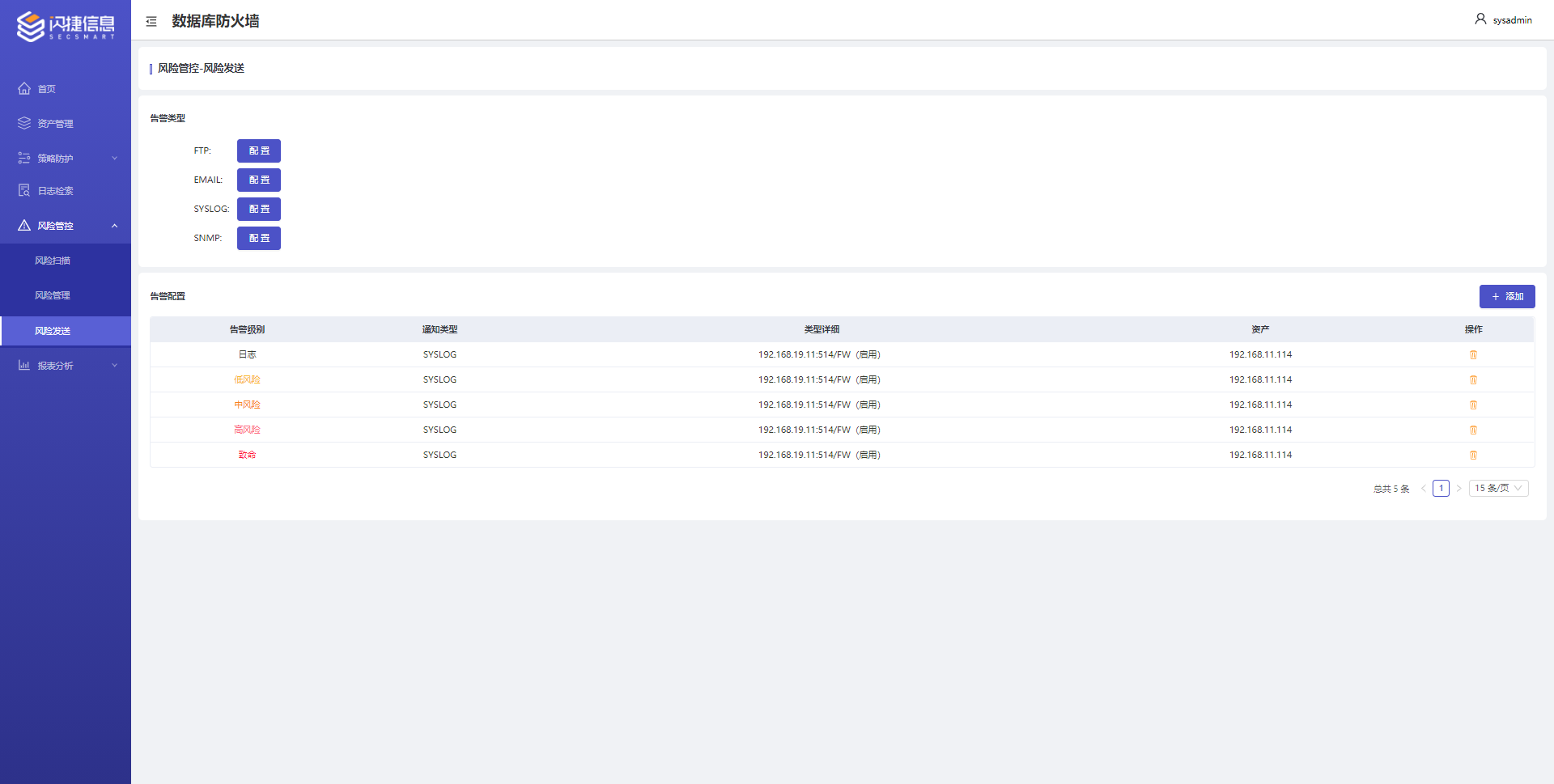
1、进入“风险管控-风险发送”页面；

2、根据需要进行告警类型配置（FTP、EMAIL、SYSLOG、SNMP）

3、点击添加按钮，基于告警类型配置告警发送详情



4、点击确定按钮在在告警配置列表中显示告警发送信息



### 报表分析

#### 报表配置

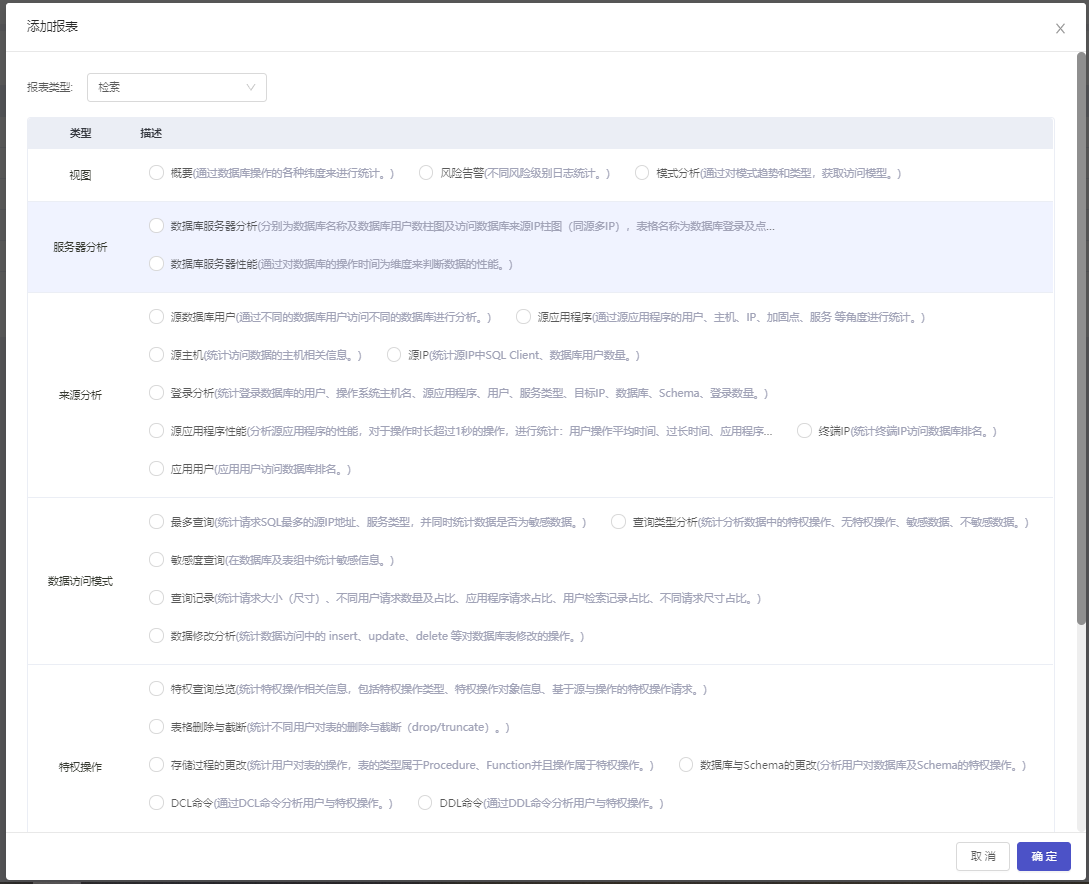
* **准备工作**

已产生日志或风险告警等信息

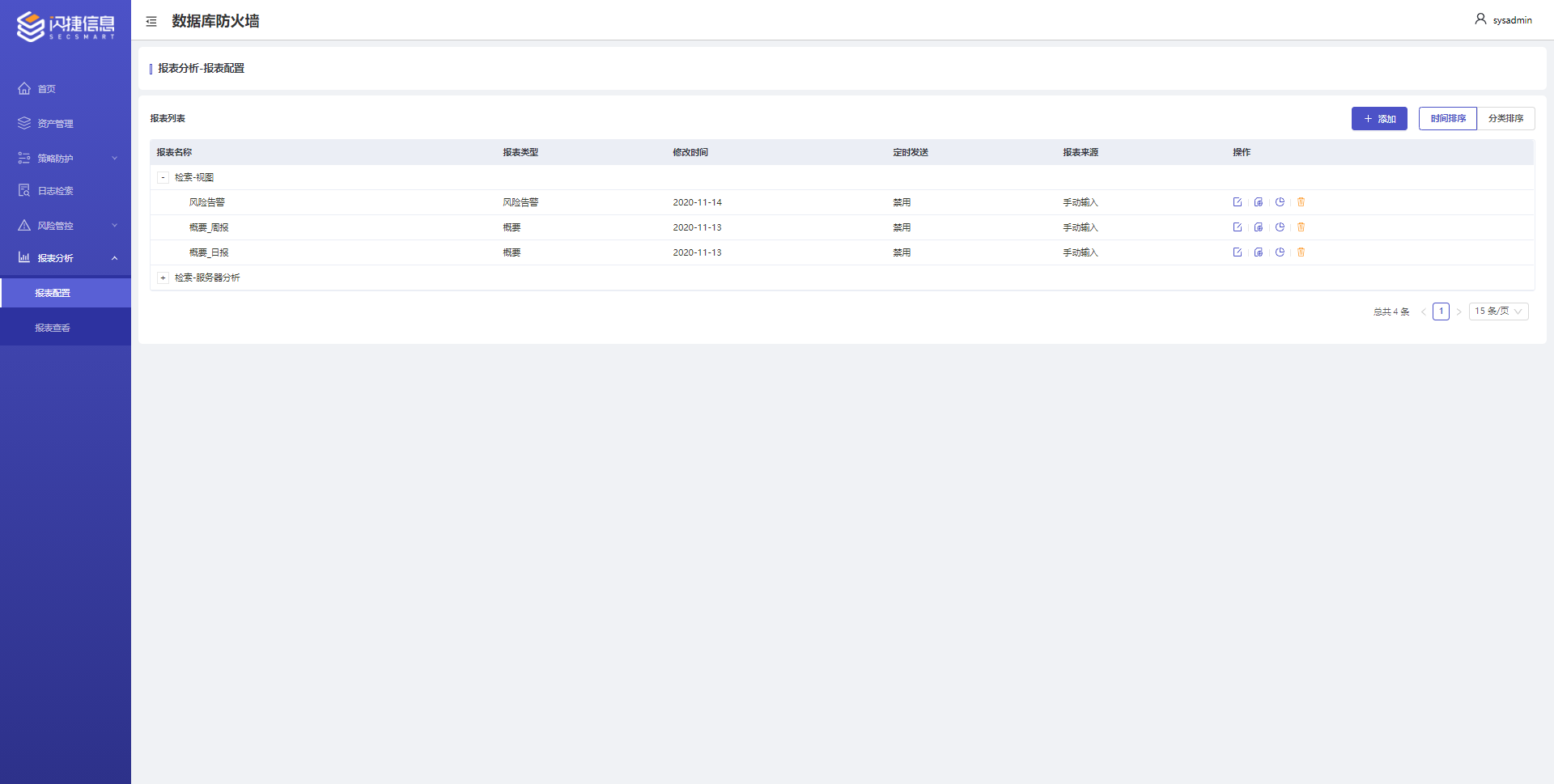
* **操作步骤**

1、进入“报表分析-报表配置”页面；

2、点击添加进行报表模板选择



3、点击确定可在报表列表里查看已添加的报表信息，可对报表进行编辑、报表生成、定时发送、删除等操作。



#### 报表查看

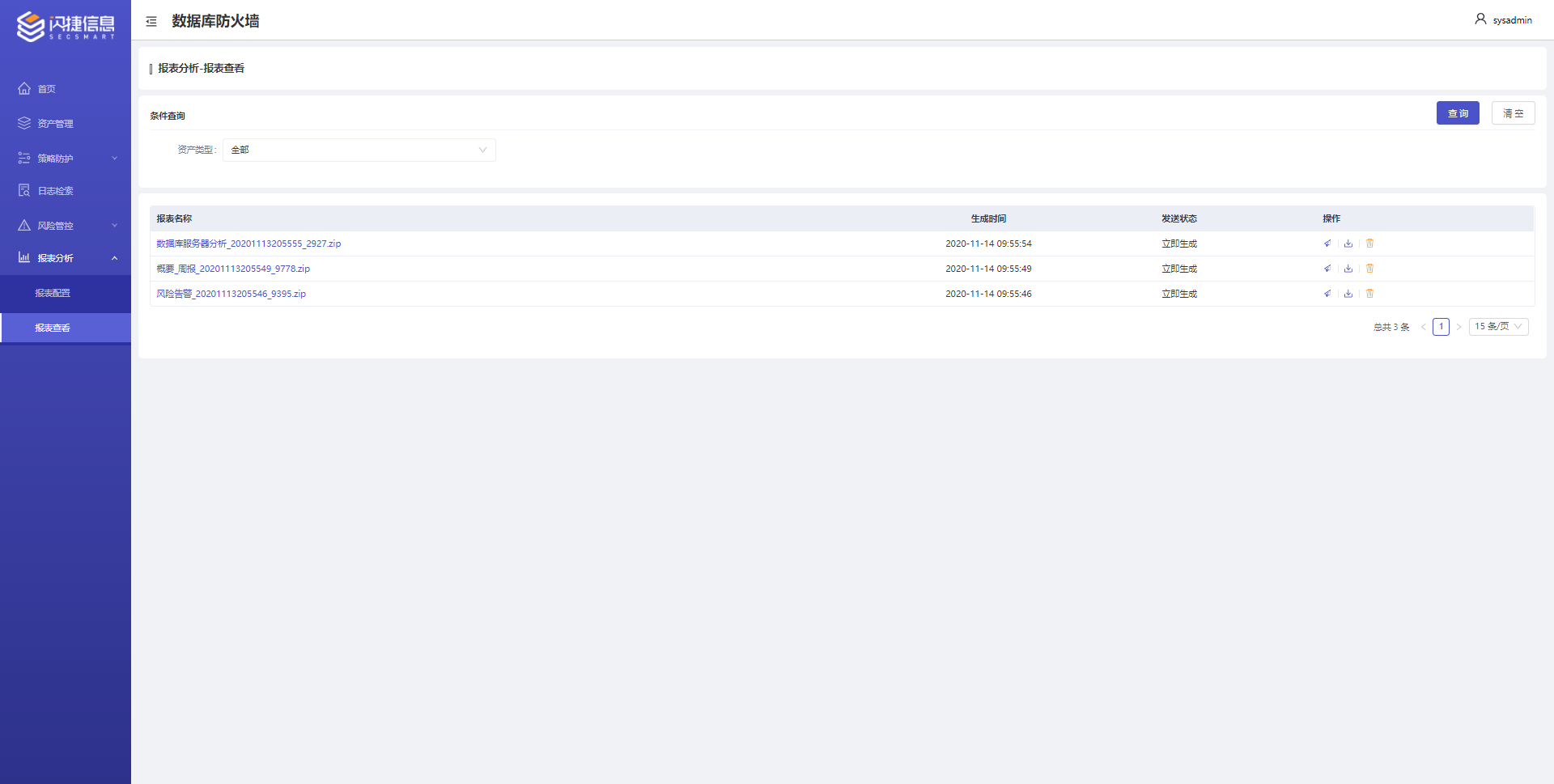
* **准备工作**

已配置完成报表模板

* **操作步骤**

1. 进入“报表分析-报表查看”页面；
2. 可通过资产类型选项进行报表检索

3、可在报表列表中看到已生成的报表信息，根据需要进行报表发送、报表下载和删除等操作



## 系统管理类

使用secadmin用户登录系统，可以对以下功能进行配置与管理。

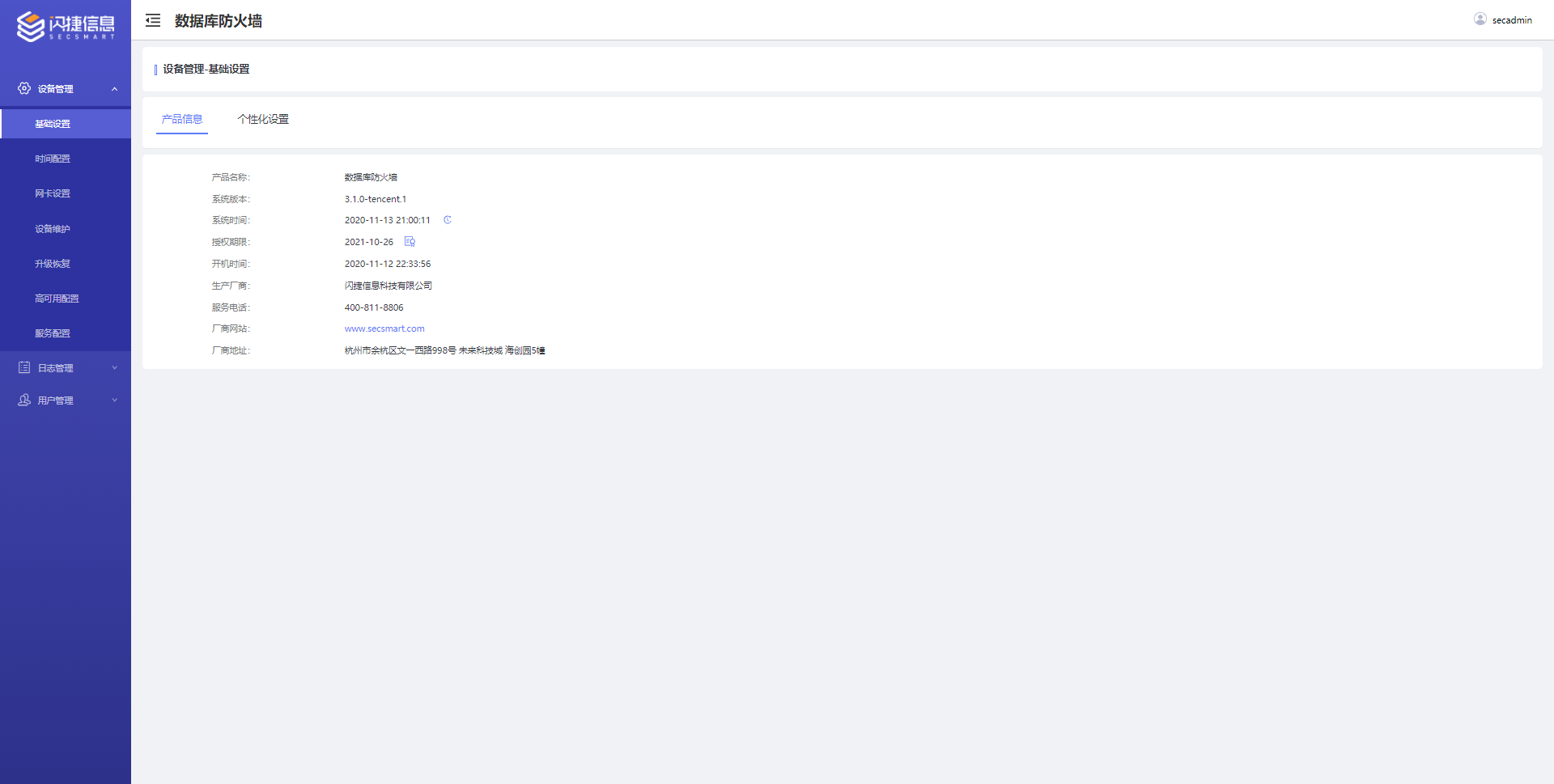
### 设备管理

#### 基础信息

* **操作步骤**

1、 进入“设备管理-基础设置”页面

2、 单击产品信息进入该页面，显示当前产品信息，可进行授权和系统时间设定操作。



#### 时间设置

* **操作步骤**

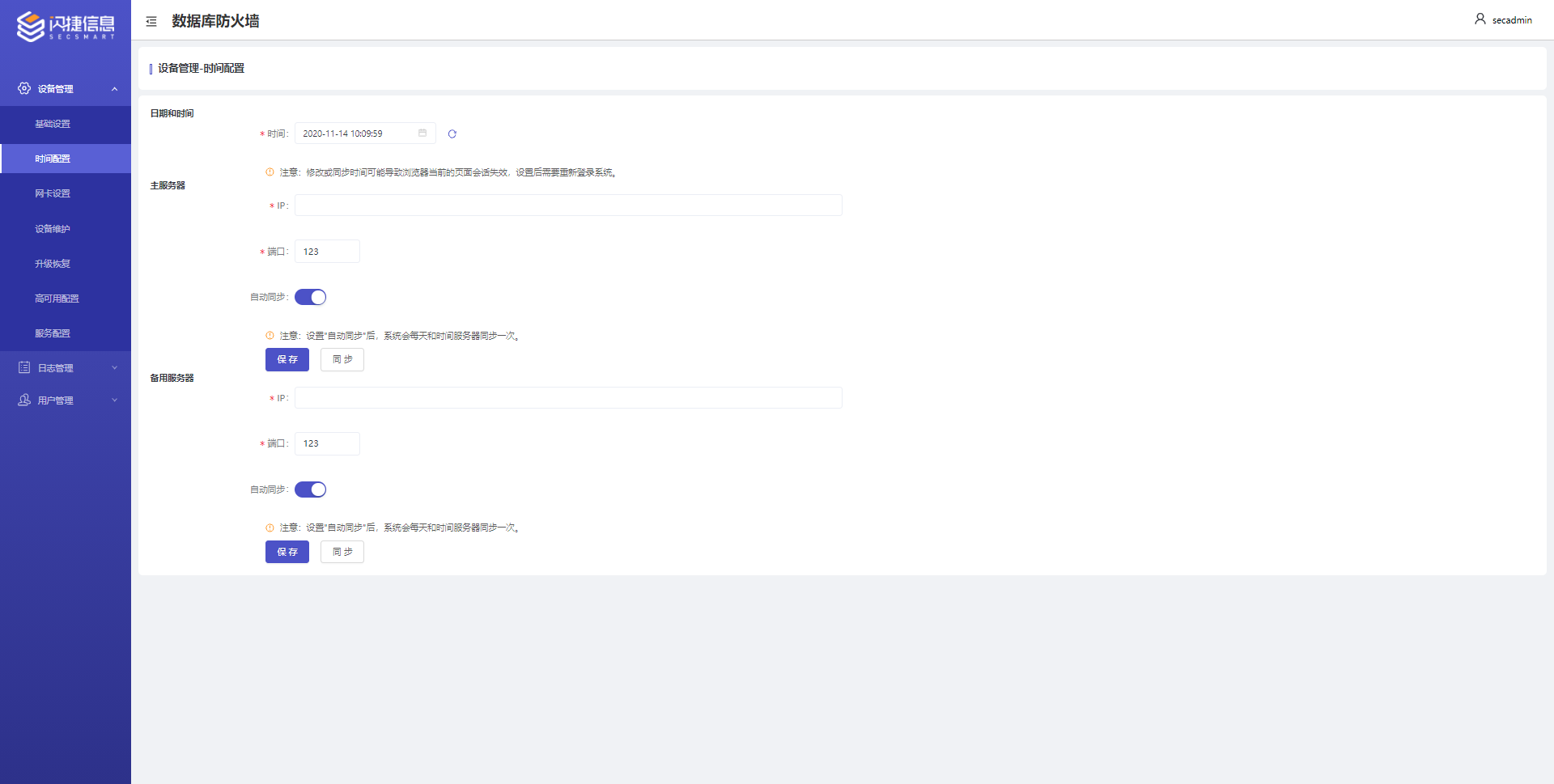
1、进入”设备管理-时间配置”页面；

2、单击按钮，在弹出的下拉框内调整时间值，确定后，单击“更新”按钮。

3、在主服务器、备服务器分别输入NTP服务器的地址；

4、单击“同步”按钮，系统自动与输入的NTP服务器进行时间同步；

5、同步完成后，勾选“自动同步”，单击保存。系统即可自动与NTP服务器进行同步。

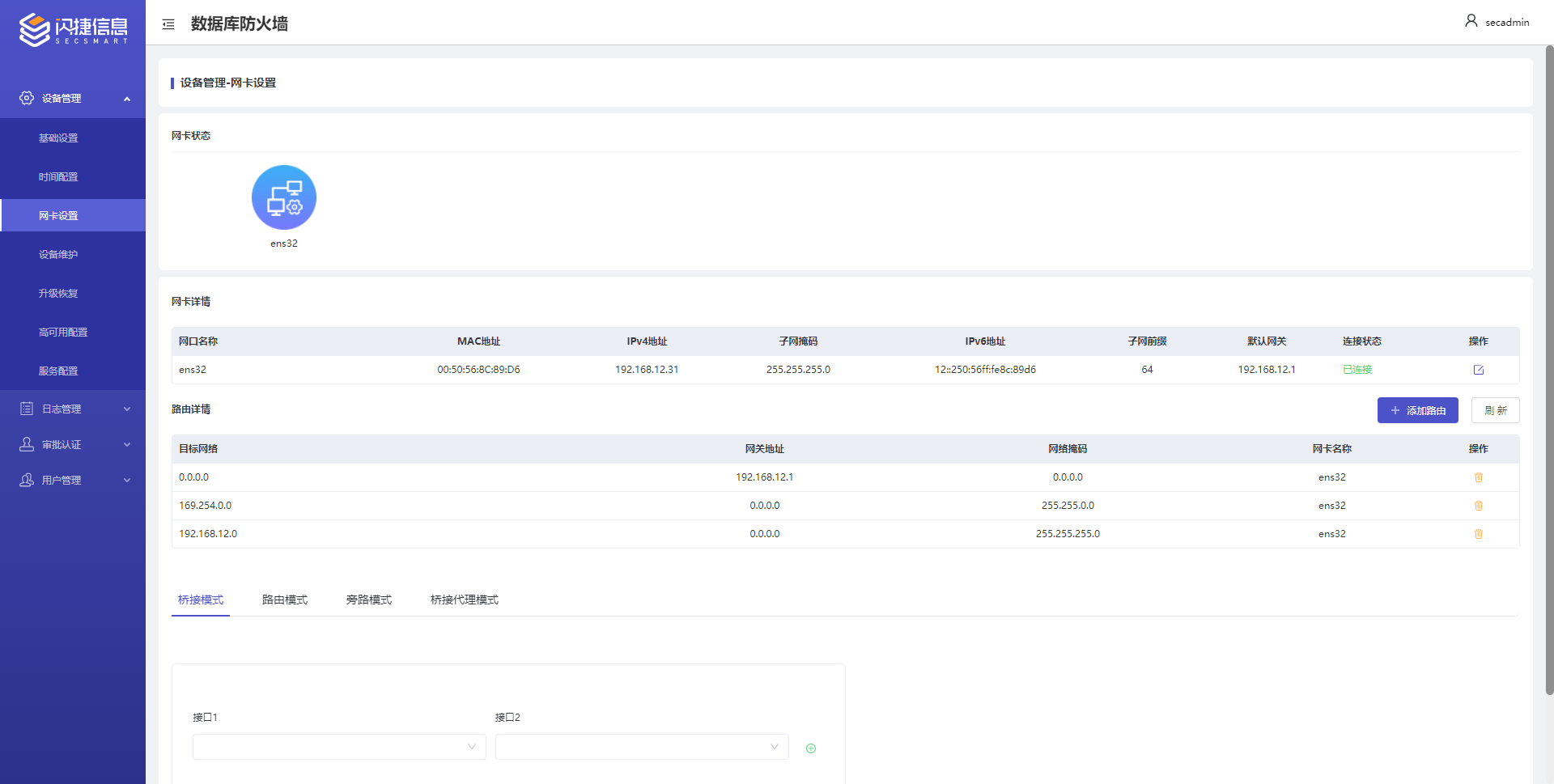


#### 网卡设置

* **操作步骤**

1、进入”设备管理-网卡配置”页面；

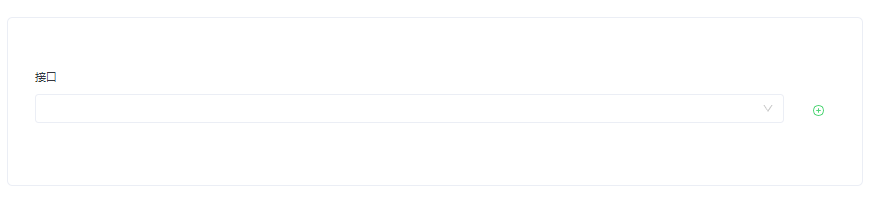
2、可查看当前网卡连接状态和详细信息。



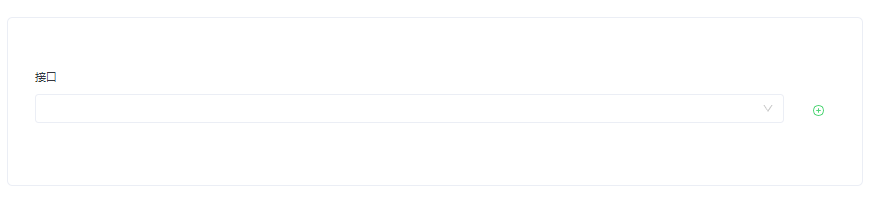
3、点击桥接模式接口配置，对桥接的网口进行桥接配置



4、点击路由模式接口配置，对路由网口进行配置



1. 点击旁路模式接口配置，对旁路镜像网口进行配置



1. 点击桥接代理模式接口配置，对桥接网口进行配置



#### 设备维护

* **操作步骤**

1、进入”设备管理-设备维护”页面；

2、点击重启设备按钮对设备进行重启。

3、点击关闭设备按钮对设备进行关闭。

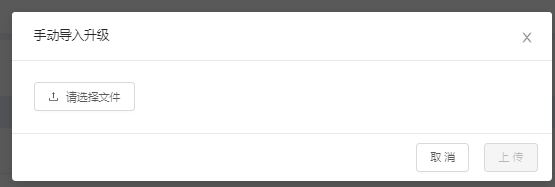


#### 升级恢复

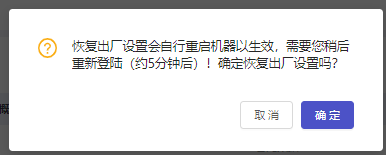
* **操作步骤**

1、进入”设备管理-升级维护”页面；

2、点击手动导入升级按钮选择升级文件进行升级。



3、点击恢复出厂设置按钮对系统进行恢复出厂设置。

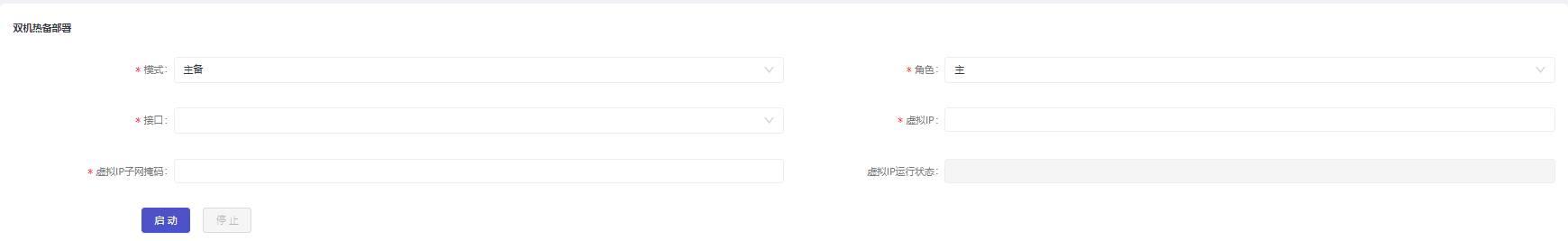


#### 高可用配置

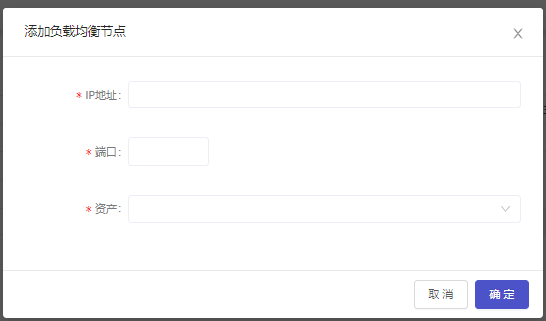
* **操作步骤**

1、进入”设备管理-高可用配置”页面；

2、根据页面提示信息配置双机热备部署。



3、根据页面提示信息配置负载均衡部署

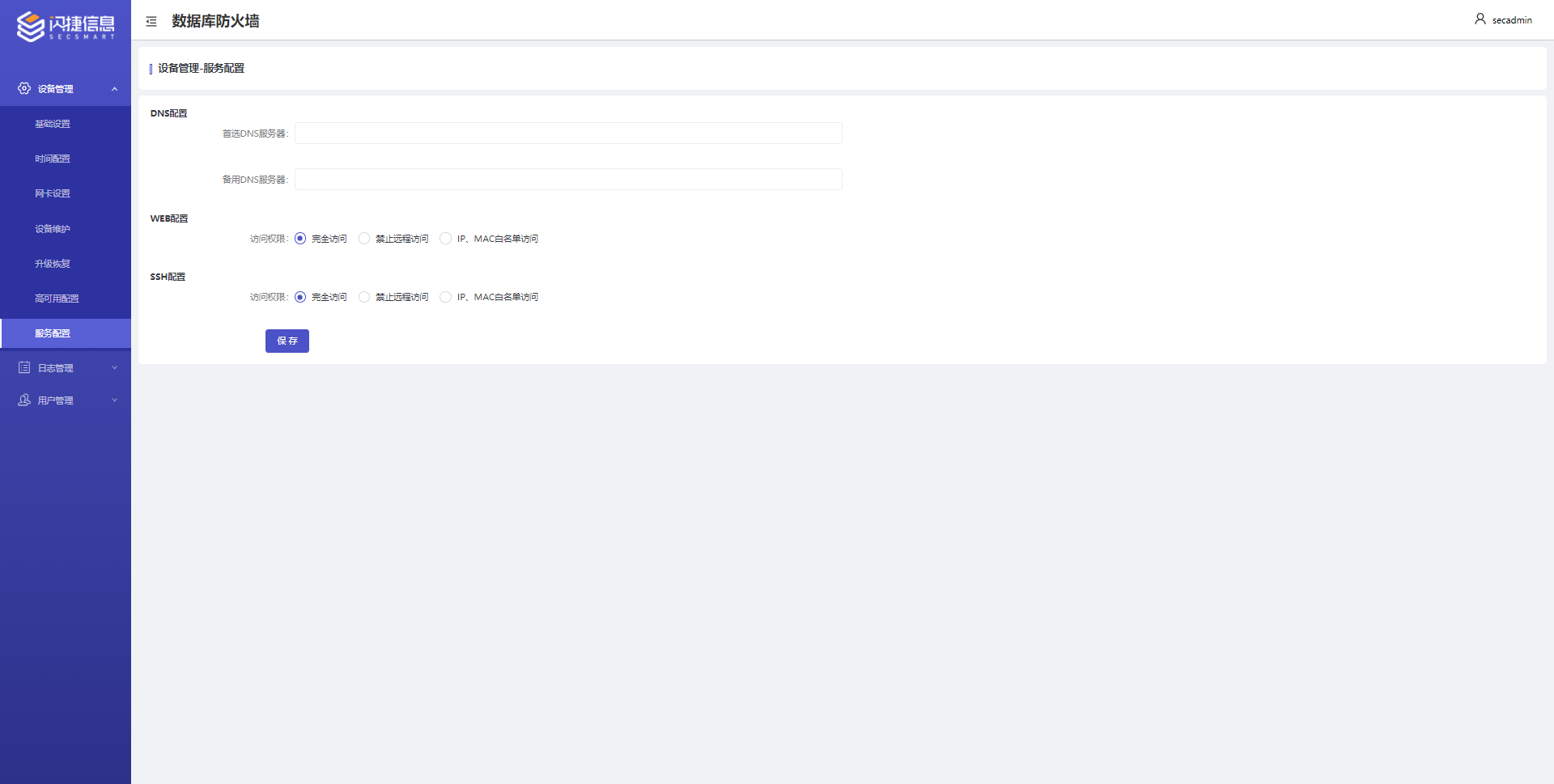


#### 服务配置

* **操作步骤**

1、进入”设备管理-服务配置”页面；

2、根据页面提示信息配置DNS配置、WEB配置、SSH配置。



### 日志管理

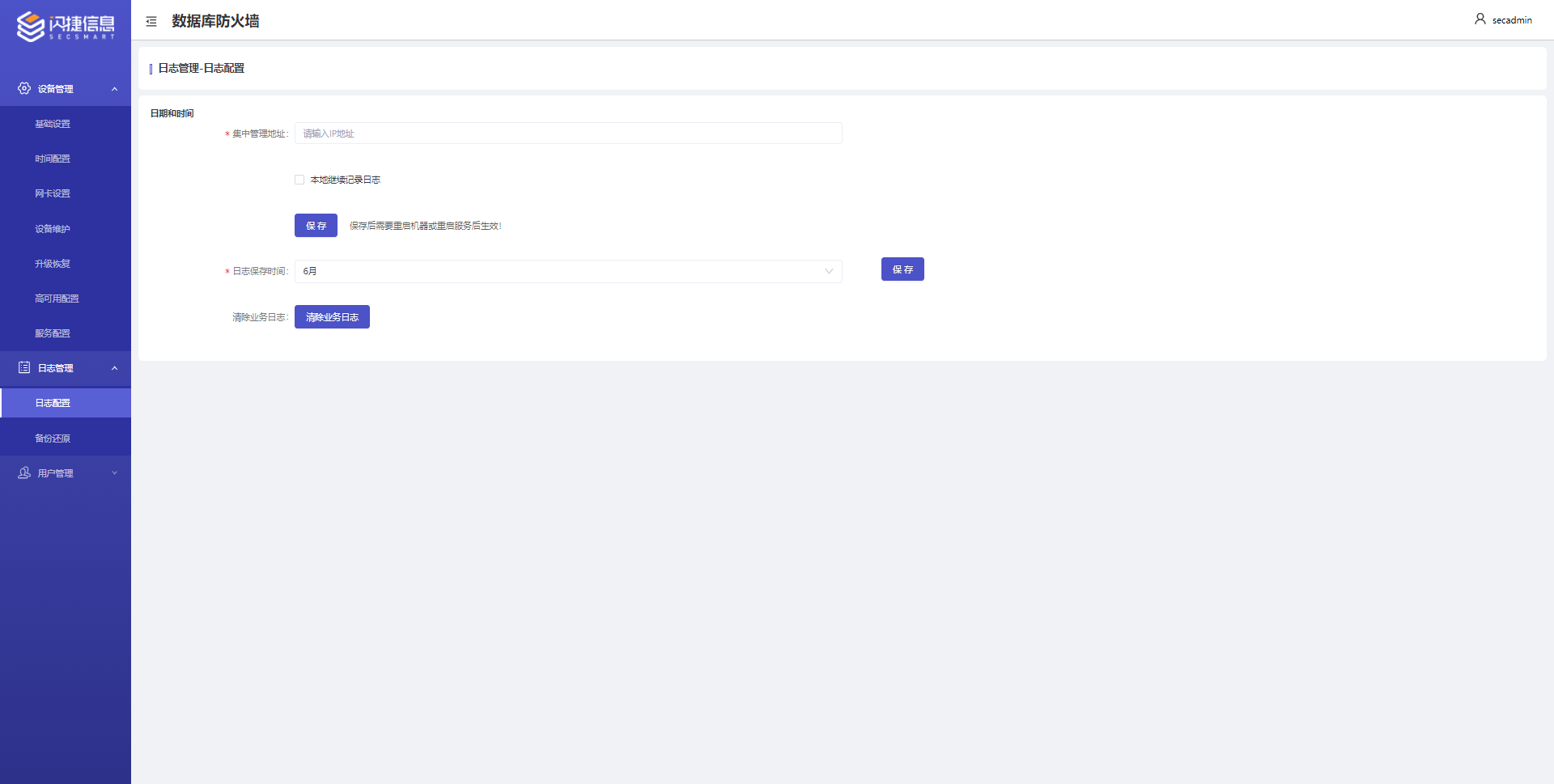
#### 日志配置

* **操作步骤**

1、进入“日志管理-日志配置”页面

2、进行集中管理地址设定。

3、可对日志保存时间进行配置，并根据需要清除业务日志

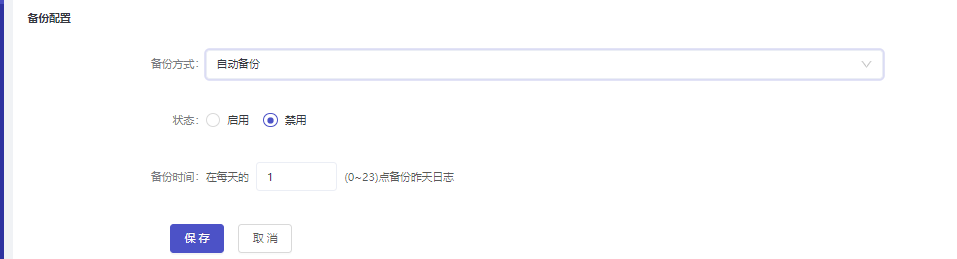


#### 备份还原

* **操作步骤**

1、进入“日志管理-备份配置”页面

2、根据需要对备份方式进行选择-自动备份、手动备份、远程备份







3、在备份列表中可对备份文件进行备份上传、备份还原和删除等操作



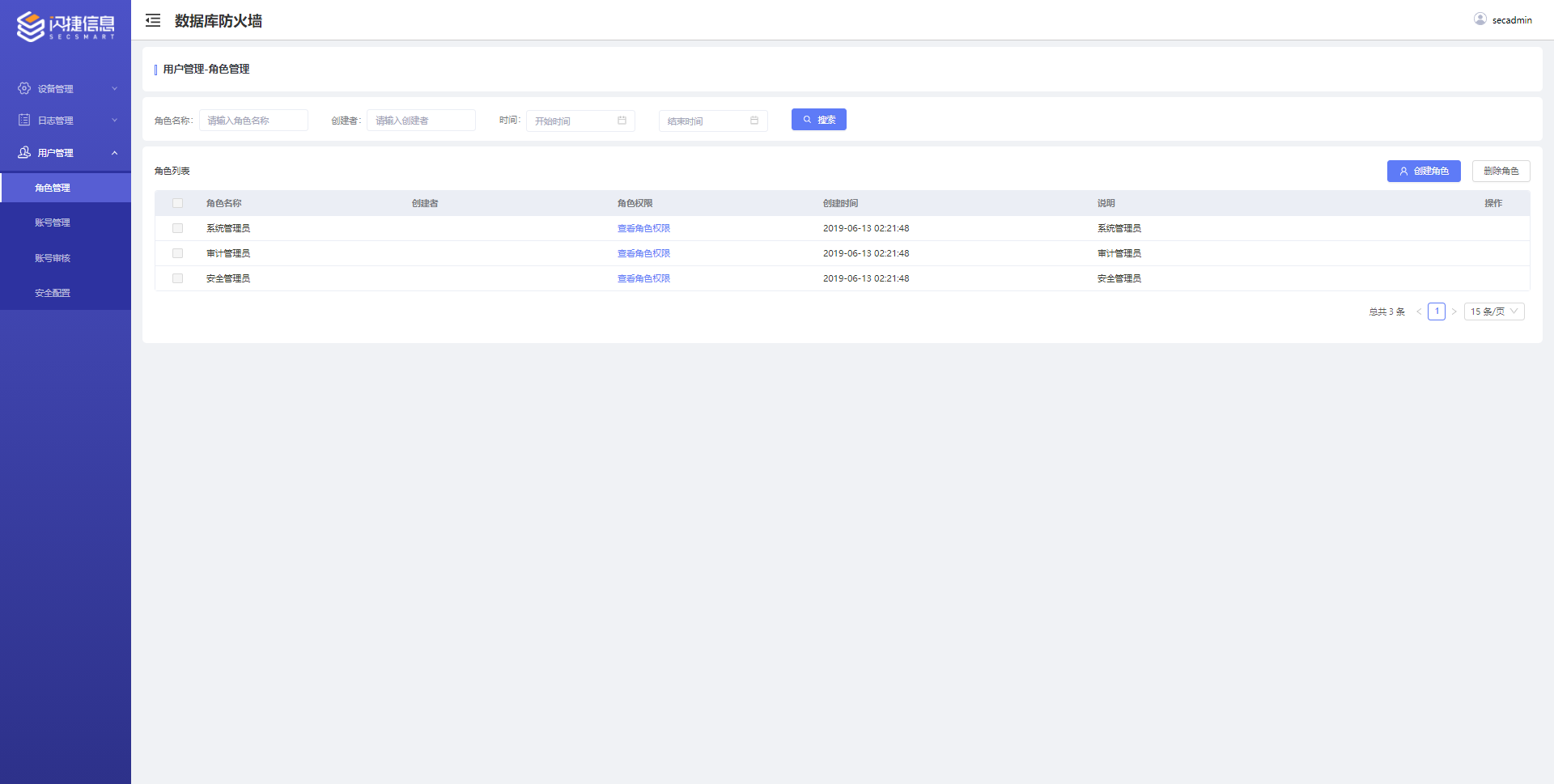
### 用户管理

#### 角色管理

* **操作步骤**

1、进入“用户管理-角色管理”页面

2、根据角色名称、创建者、时间进行角色检索



3、点击创建角色对用户角色进行创建，管理员可对新建角色进行模块授权配置



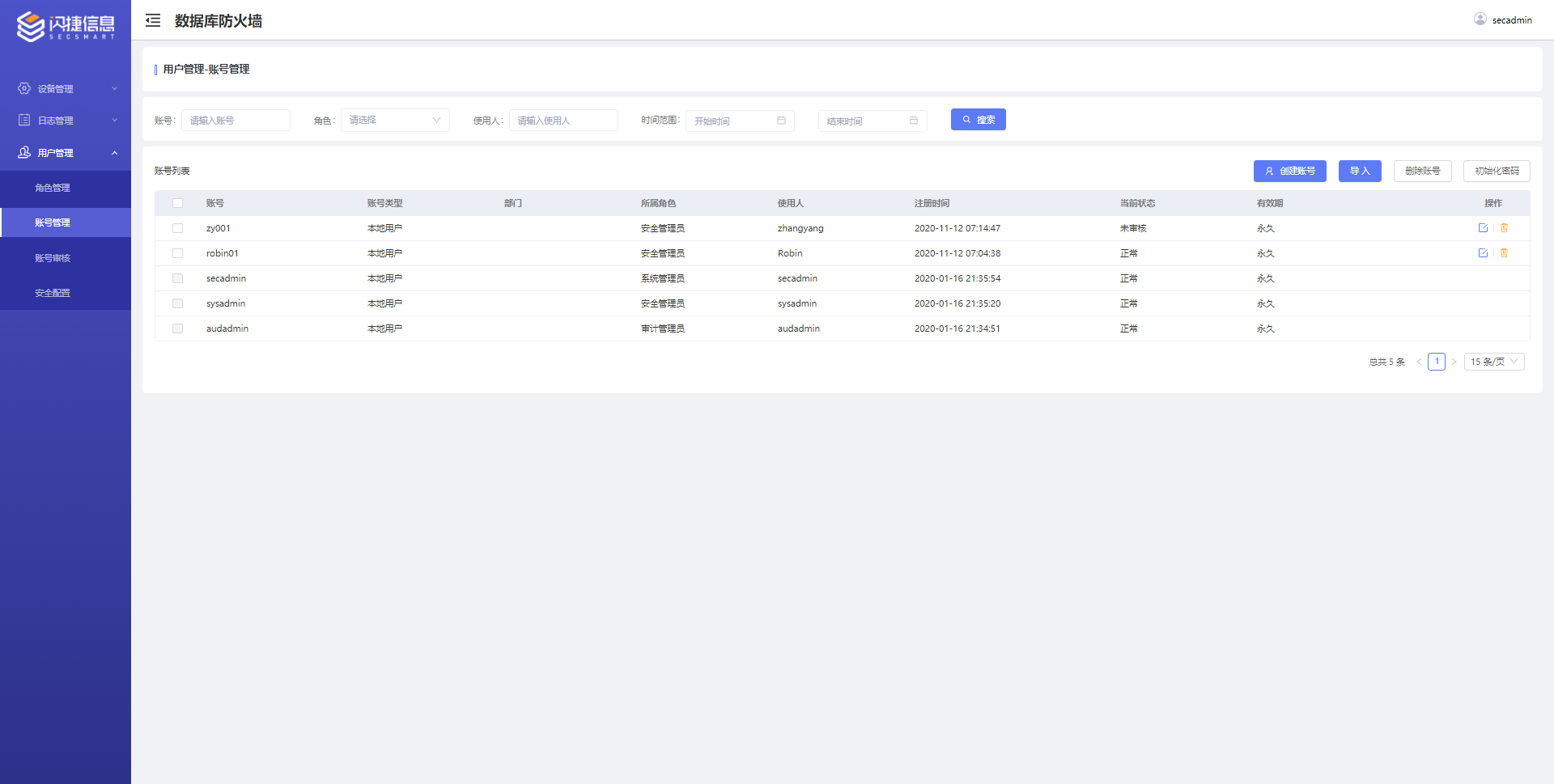
4、点击删除角色对新建角色进行删除

#### 账号管理

* **操作步骤**

1、进入“用户管理-账号管理”页面

2、根据账号名称、角色、使用人、时间进行角色检索



3、点击创建账号对用户账号进行创建，管理员可根据提示窗信息对新建账号进行配置



1. 可对新建账号进行删除和初始化密码操作

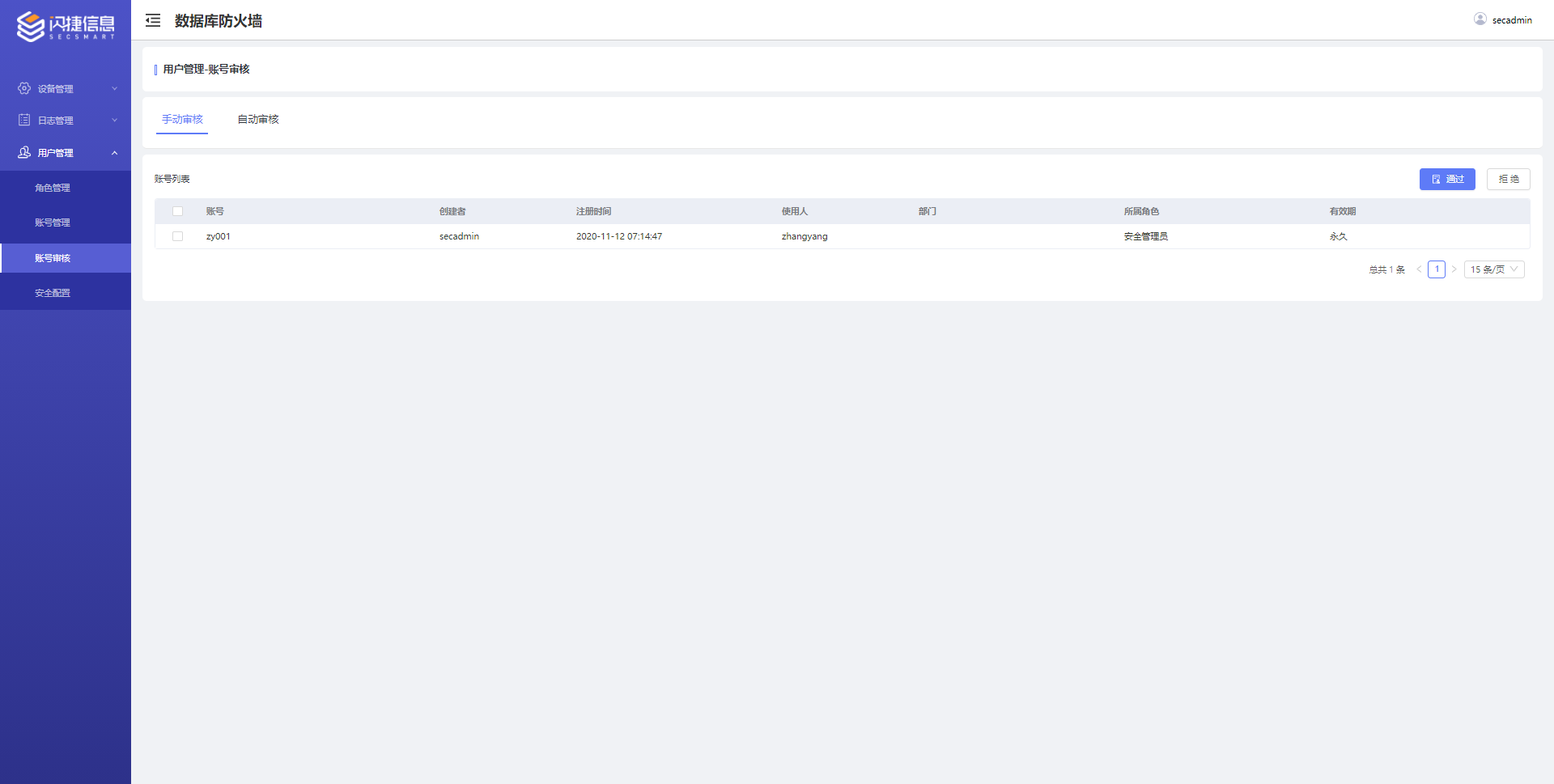
#### 账号审核

* **操作步骤**

1、进入“用户管理-账号审核”页面

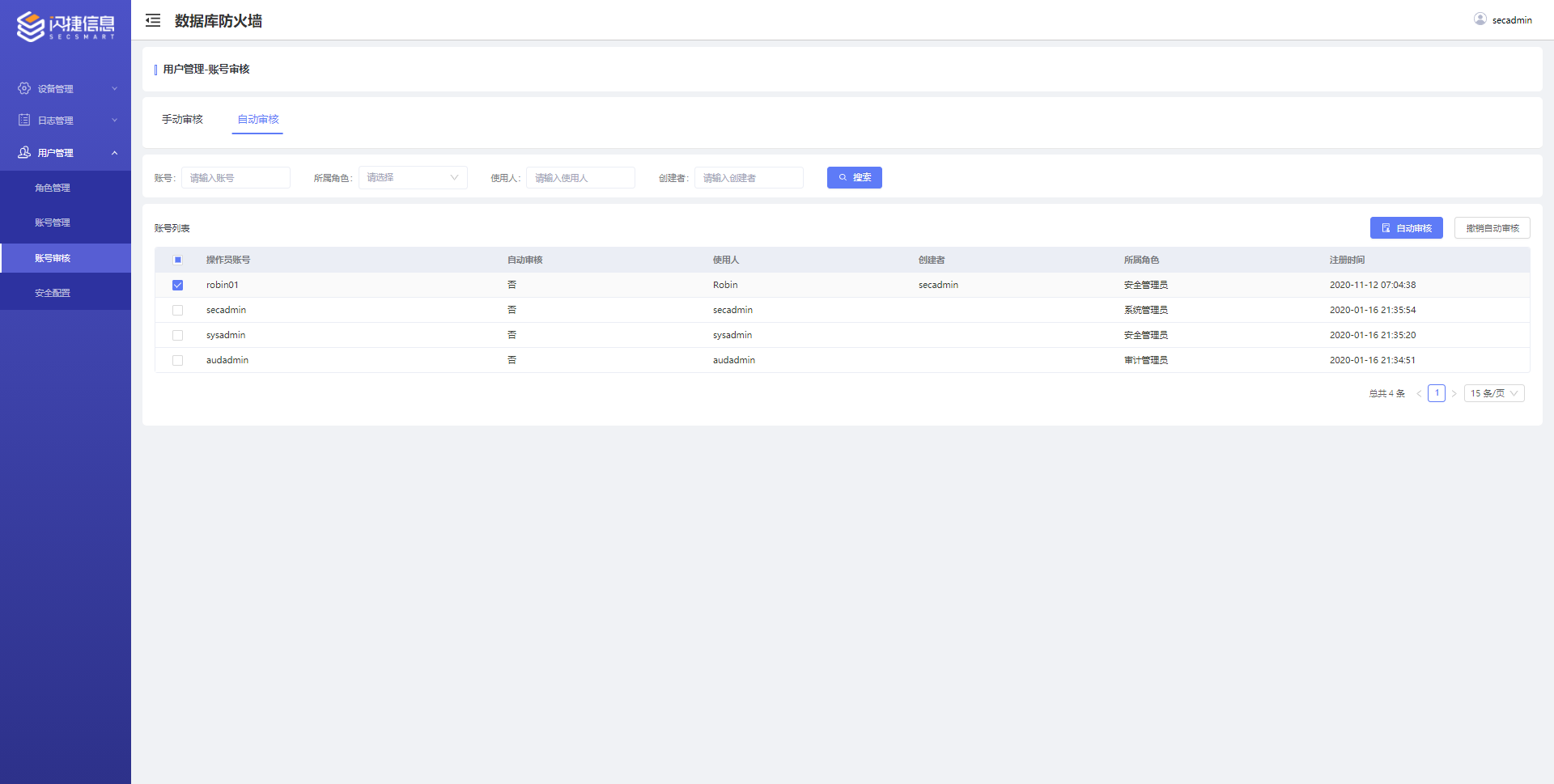
2、点击手动审核进入该页面，在账号列表中看到已新建账号

3、选中该账号，点击通过或拒绝对账号进行手动审核。



4、点击自动审核进入该页面，选中需要自动审核的账号

5、点击自动审核或撤销自动审核对账号进行自动审核功能

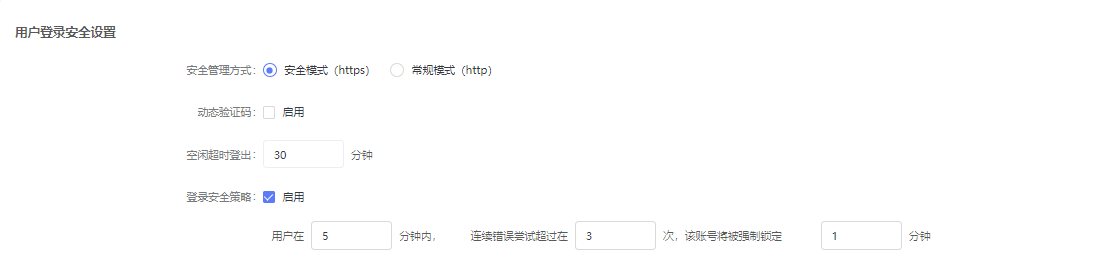


#### 安全配置

* **操作步骤**

1、进入“用户管理-安全配置”页面

2、用户登录安全设置，可对安全管理方式、动态验证码、空闲超时登出、登陆安全策略选项进行安全配置



3、账号密码安全设置，可对初次登录强制更改密码、密码长度要求、密码复杂度要求进行安全配置



## 系统审计类

### 操作审计

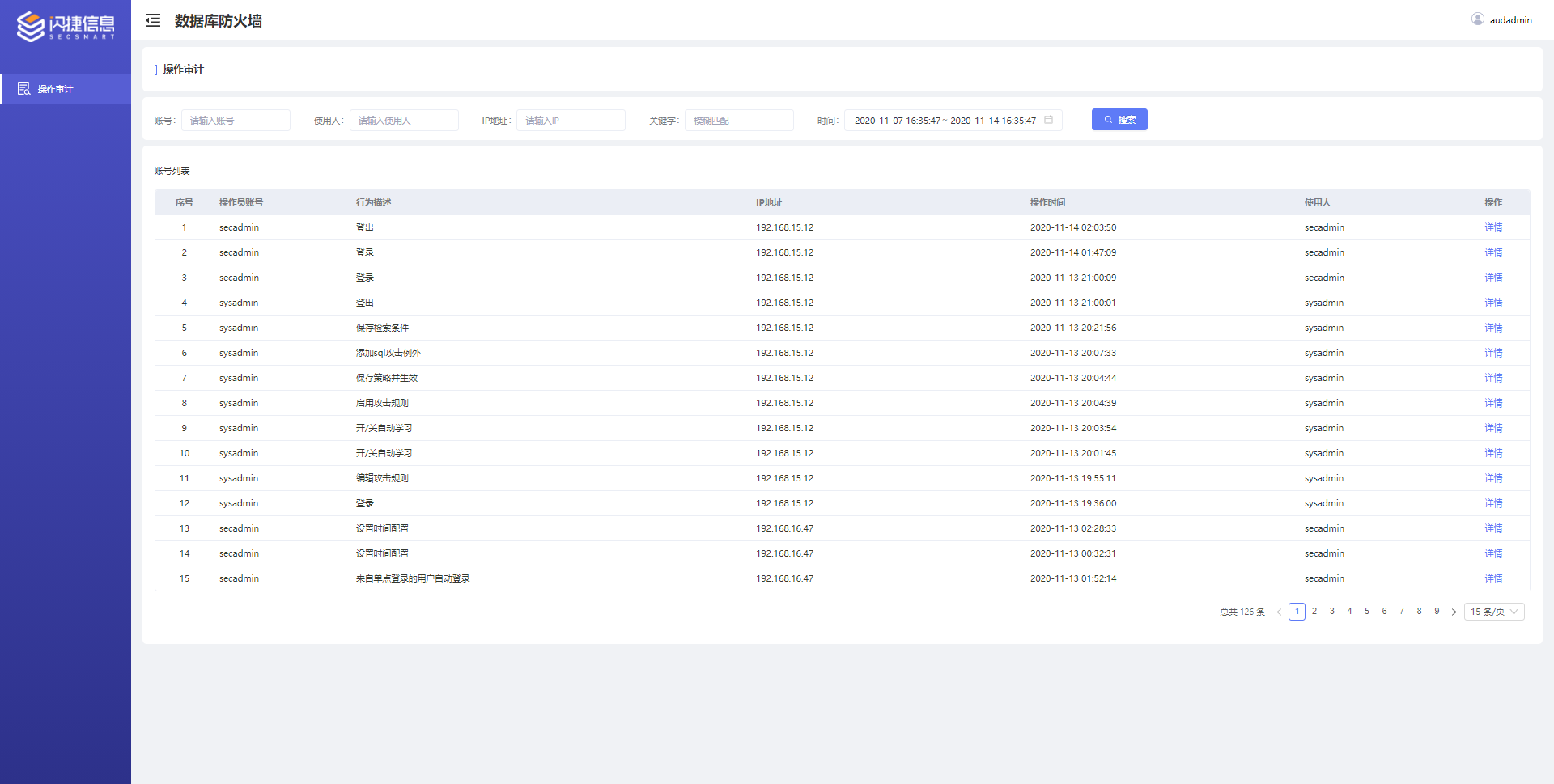
* **操作步骤**

1、使用审计管理员（Auditor）登录，进入“操作审计”页面，单击查询按钮；

2、可以使用账号、使用人、IP地址、关键字、时间进行查询具体记录。

3、查询结果可在下方账号列表中显示

4、点击详情查看该操作的详细信息



## 系统常用操作

### 业务启动

1. 按下设备开机键
2. 待系统启动后自动进入到操作系统
3. 用一台网络可达的PC机，打开谷歌浏览器，输入设备地址后打开业务

### 业务停止

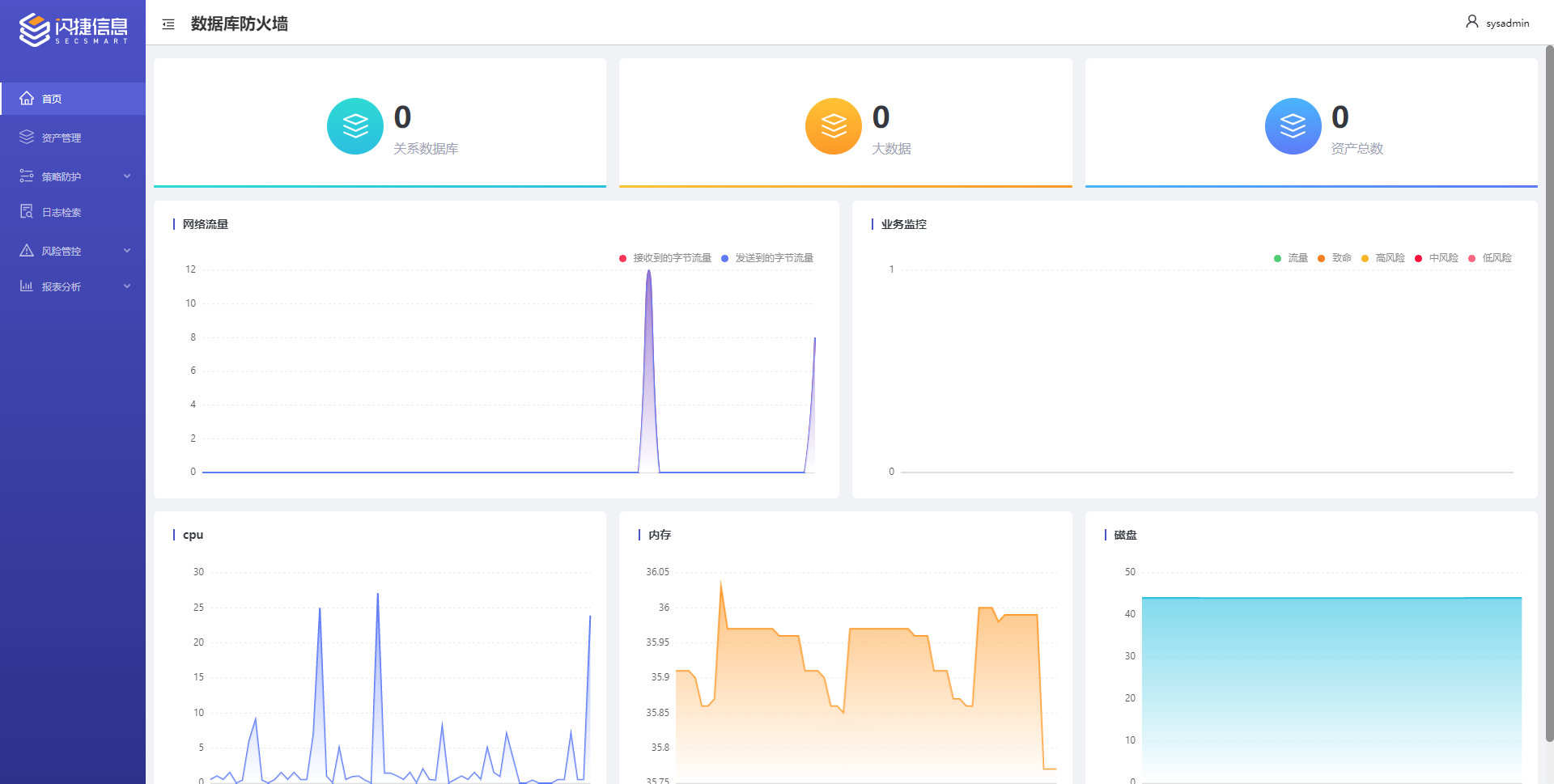
1. 确保停止数据库防火墙系统后不会影响当前业务
2. 关闭网页
3. 按下设备关机键关机

### 上电断电

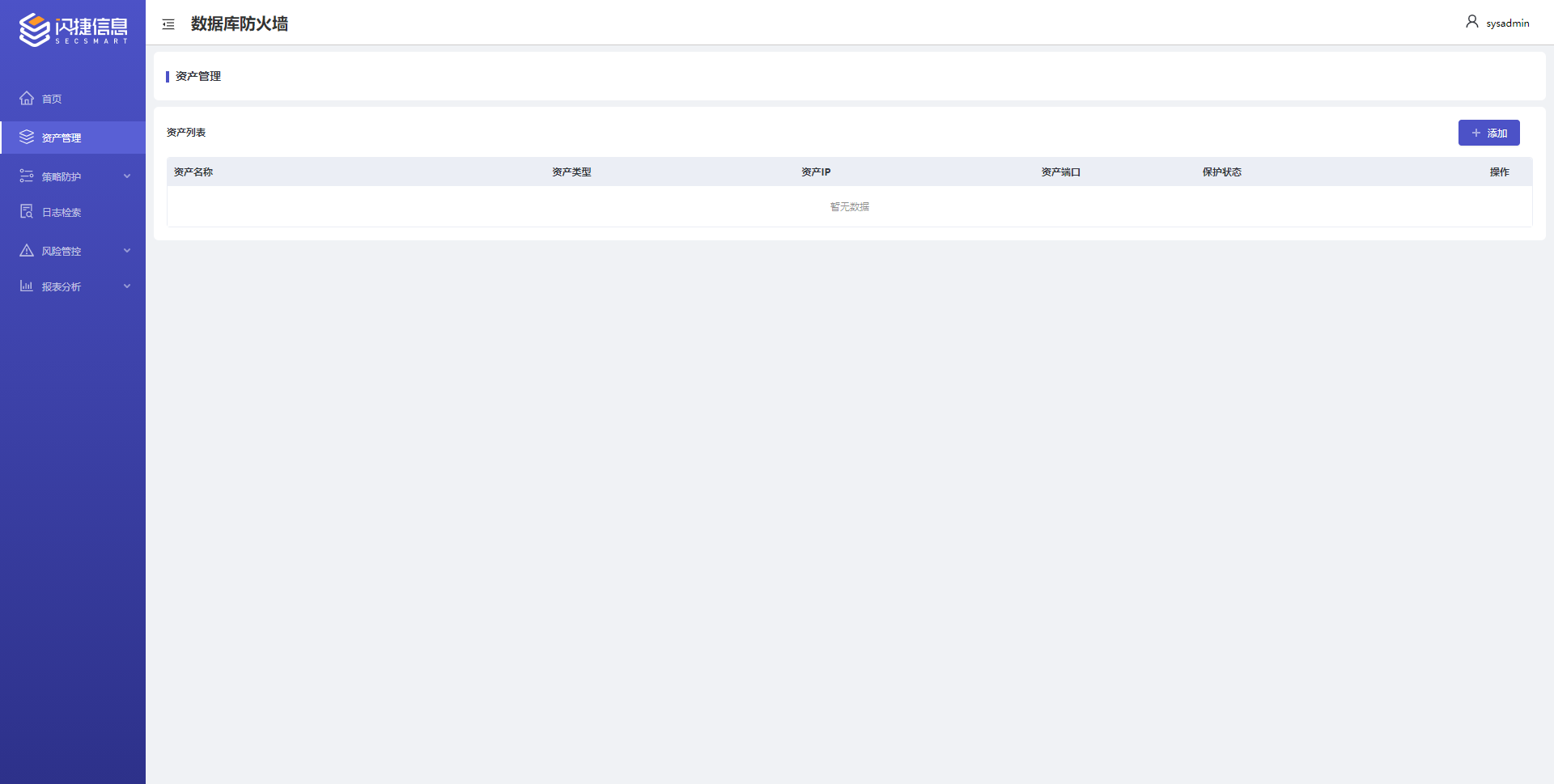
1. 为设备接入电源线进行上电
2. 观察上电后设备能否正常启动和运行
3. 当需要为设备断电时，进行2.3.2 业务停止操作
4. 拔下电源线断电

## 快速入门

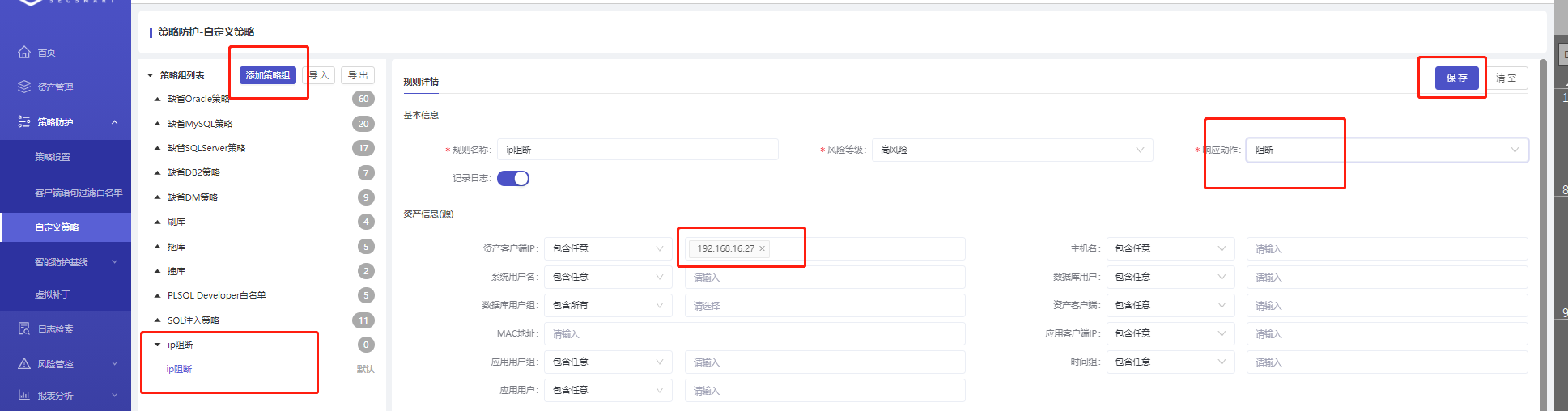
1、开机后进入系统登录页，输入用户名和密码进入业务界面，如下图



1. 点击“资产管理”页面进行资产添加配置，如图：

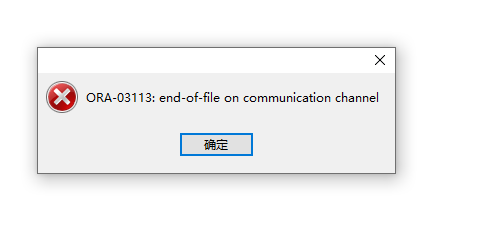
1. 点击“策略防护-自定义策略”添加“ip阻断策略和相应规则”，配置需要阻断的ip地址后点击保存，如图



1. 点击“策略设置”页面，勾选“自定义策略”，点击编辑按钮后，在弹窗内选择“5”中新建的策略后，点击“策略应用”



1. 通过策略设置中阻断的ip地址所在的PC机访问数据库，无法访问，阻断该会话，如图



1. 点击“日志检索”，查看最新的阻断日志信息，如图

