文档中心

数据安全解决方案 UDSS

产品文档

目录

概览

- 数据库审计升级说明
- 产品手册下载
- 产品价格
- FAQ
  - 验证码不显示

概览

- 数据库审计升级说明
- 产品手册下载
- 产品价格
- FAQ
  - 验证码不显示

产品概述

云数据库审计系统(Udas),首创双向审计机制,全面覆盖应用、中间件、数据库,达到“事前预防+事中防范十事后取证”的立体防御效果。审计系统采用数据库深度报文协议解析技术DPI及流煤体分析技术DFI等,将数据库的各种访问操作,解析还原为数据库级的操作语句,通过预置的安全规则匹配,即可智能分析和监控访问者的各种操作,进行实时威胁预警,并对事件进行统计分析记录,多重身份定位,有效支持电子取证。

审计系统对审计和事务日志进行审查,从而跟踪各种对数据库操作的行为。一般审计主要记录对数据库的操作、对数据库的改变、执行该项目操作的人以及其他的属性。这些数据库被记录到审计系统独立的平台中,并且具备较高的准确性和完整性。针对数据库活动或状态进行取证检查时,审计可以准确的反馈数据库的各种变化,对我们分析数据库的各类正常、异常、违规操作提供证据。

系统采用三权分立的模式,包括三个平台,系统管理平台、安全管理平台、审计管理平台,各平台的功能与职责不同,权限不同,相互监督。如系统管理员负责设备的运行设置;安全管理员负责查看相关审计记录及规则违反情况;审计日志员负责查看整体设备的操作日志情况。

产品价值

- 精准可视，安全可控

  过人性化界面按总分结构直观展示当前审计结果，帮助用户快速了解自身系统的风险情况，并根据当前的风险情况快速确认以及审视，当存在异常，如流量突变、会话突然增多的情况时，通过审计页面快速排查风险来源，避免遭遇危险攻击。

- 溯源分析，精准定责

  通过业务关联功能和审计功能，从各个维度进行统计分析、结合原始用户操作审计记录，提供原始数据的快速检索能力，让用户能快速确认问题的来源，并将安全事件进行精准定位、追责到人，溯源取证。

- 资产数据安全防护

  通过对用户访问数据库行为的记录、分析和汇报，帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

- 访问权限控制

  可针对那些持有特权账号进行了误操作或者不法行为时，特别是运维人员，可对该用户的部分操作进行阻断控制并及时告警，从而降低影响以及损失。同样也可以通过控制只有特定的访问IP范围才能对数据库进行访问，从而阻断那些非法分子进行访问。提高数据资产安全。

- 满足合规要求

  帮助用户满足等保、分保等合规要求，各政府及行业对于信息安全越来越重视，也提出了很多的相关标准来确保各单位的网络安全。政府的行政事业单位或者国有企业则有遵循等保护、分保的合规性要求。UCloud提供了一套独立的审计方案，有助于完善组织的内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过审计。

支持范围

数据库支持类型

(1)、关系型数据库:Sqlserver、oracle、Sybase、DB2、Informix、PostgreSQL、 MariaDB、XUGU(虚谷

(2)、国产数据库:达梦、人大金仓、神通数据库、南大通用

(3)、后关系型数据库:Caché DB

(4)、内存数据库:HANA 、Redis

(5)、大数据数据库:RECORD_HIVE、SPARK_JAVA_API、Hive、HIVE_HSQL、Record_Hive、ES、GaussDB(华为高斯)、LibrA、HBASE_SHELL、Solr、MongoDB

(6)、工控实时数据库:IP21_API、IP21_APIIP21_WEBSERVICE

(7)、特殊云数据库:阿里云_PostgreSQL-目前版本不支持、RDS

说明

云上数据库审计只支持审计功能,不支持命令阻断功能;且需要在访问数据库的应用服务客户端部署agent。

agent:转发数据库协议流量发送至审计端,从而实现审计操作,支持多个审计对象上同时配置并进行引流

浏览器兼容性

本系统采用B/S架构,支持IE10及以上浏览器、Chrome浏览器、Firefox火狐浏览器。为了保证良好的浏览效果,推荐使用Chrome浏览器。

功能特性

平台高可用性设计

审计平台异常操作记录和告警:当有人非法操作或者破坏设备时,系统会实时发送短信或邮件,并作详细记录。24小时自动监控。

系统运营监控: 监控数据库审计系统运行状态,当设备出现问题或者磁盘空间不足时,将通知相关负责人处理。

数据库审计功能

智能规则库:支持自定义规则,通过不同规则配置让系统更加符合每个企业不同的管理要求。

多维度身份指纹:系统支持工号、源IP、MAC、用户名、进程、操作系统类型、操作系统用户名、身份标识和审计,多重定位。

数据库异常操作记录和回溯:记录数据库上的所有详细操作,何时、何人、何种方式操作,支持事件的回溯。

审计日志:支持审计日志的查询、分析、统计和打印等。

三权分立:提供审计管理员、规则管理员、系统管理员,实现三权分立,互相制约,满足等保要求。

统计报表:包括源IP访问排行、数据库登录失败排行等。

高级审计:支持绑定变量及嵌套语句的复杂组合的数据库命令审计。支持三层模糊关联和HTTP协议的审计。

审计加密协议的MS SQL:支持MS SQL Server加密身份信息破译,解决MS SQL Server 2005及以上数据库看不到身份的难题。

管理范围

支持自建数据库

支持UCloud的UDB数据库

提供Openstack接口方案,支持对大数据平台的安全审计

数据盘说明

1、磁盘计算方式

根据数据库的sql条数来计算，10000条/秒的SQL，一个月的数据量，按照峰值计算约150G，客户案例预估是100G左右

2、磁盘存储说明

数据库审计的审计日志存储时长取决于数据盘空间大小，默认规则为不删除日志

磁盘空间不足时将自行覆盖最早审计日志，客户也可手动根据日期选择需要删除的日志

数据库审计快速上手指导

数据库审计快速上手指导文档【6.0】

一、 部署前说明

1、注意点:云数据库环境配置，需要在agent的引流下完成审计的整个过程，整个部署时间需要1-2天，产品购买满3个月后支持自行删除退费

2、agent部署模式:

(1)、客户端模式:

云数据库/自建数据库:agent部署在访问数据库的应用服务端(客户端)

(2)、服务端模式: agent部署在数据库的底层操作系统上（服务端），但会占用底层主机的性能（CPU、内存阀值不超过主机整体的5%,超过阀值会自动重启），部署前需先评估业务流量大小机底层主机性能

云数据库:业务端后台部署agent

自建数据库:客户自行部署agent

3、数据库审计、数据库、应用服务器建议在同一内网环境，不推荐外网访问（数据转发为明文传输）

4、数据库审计不支持到期前删除退费（使用满3个月支持删除）

5、数据库审计6.0各平台默认账号密码：默认首次登陆强制改密

系统管理员sysadmin/3edc$RFV

安全管理员secadmin/3edc$RFV

审计管理员auditadmin/3edc$RFV

6、数据库审计需要开放的外网防火墙端口：

8443:web页面登陆验证码使用

443: 前端 https前端页面访问

22: 后台登录-非必要不需要开放

二 、部署数据库审计

1. 购买数据库审计

目前支持的可用区包括：国内常用区域；如需特殊区域部署上线，请联系技术支持申请！

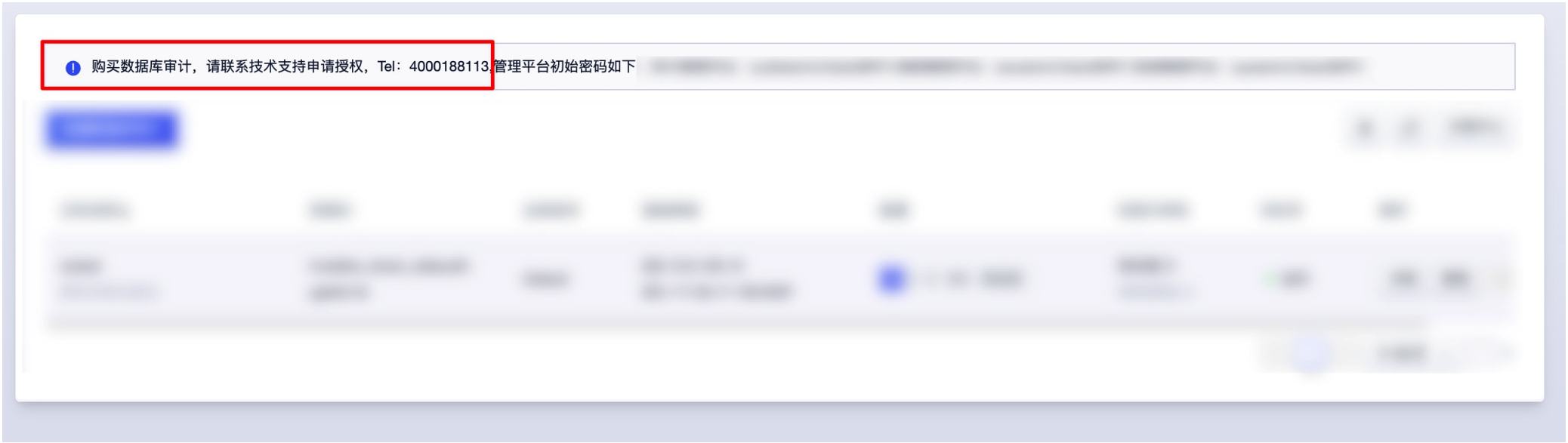
访问路径：产品-\>安全合规-\>数据安全解决方案

点击购买数据库审计，并选择相应的配置，完整支付及自动创建（大约5分钟）

数据盘大小估算参考：https://docs.ucloud.cn/udas/concepts/shujupan 同步支持后期弹性扩容

2. 申请并导入授权

默认创建的数据库审计是没有license授权的，需提供注册文件，联系技术支持/产品负责人申请



打开浏览器,在地址栏输入设备https://EIP,登录系统管理平台,下载注册信息文件,将授权给到申请人。

系统管理平台:sysadmin/3edc$RFV

3. 导入授权

拿到授权文件进行文件导入，导入之后就可以看到数据库审计具体的实例个数和有效时间

4.下载并部署agent（UDB上部署agent，请联系业务人员处理）

4.1、下载agent

系统管理平台-部署方式，下载对应版本的agent，目前支持支持Linux和windows版本的agent

4、2部署agent

参考对应版本agent部署文档：

- 《Linux_agent部署指导-V6.0》
- 《windows_agent部署指导-V6.0》
- agent部署指导手册

5. 配置审计规则及审计对象

打开浏览器，在地址栏输入https://EIP，在弹出的登陆页面输入规则用户名/密码：安全管理员secadmin/3edc$RFV后，安全管理平台。

点击‘保护对象’，点击“添加”，输入需要被审计数据库服务器的相关信息，输入完成以后点击保存，如下图所示：

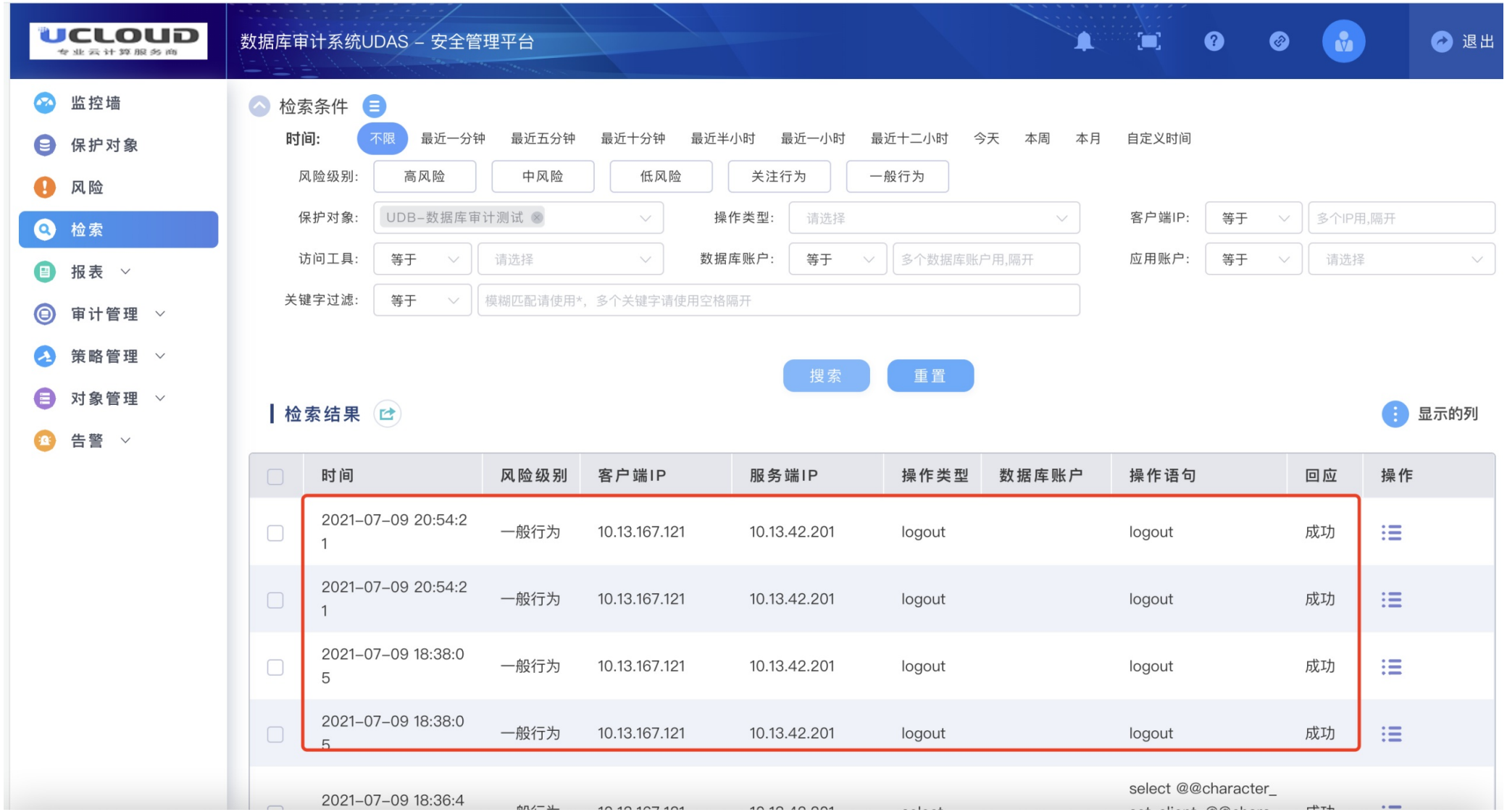
注：操作日志全量审计，审计策略为出发对应规则的风险告警

6. 查看审计结果

在目前的安全管理平台，检索模块，选择对应的检索条件（默认不选为全选），点击检索

查询审计日志

审计结果展示



1、登录系统

打开浏览器，在地址栏输入审计设备的管理IP地址或输入 https://数据库审计IP

- 6.0版本外网IP登陆请放开443,8443端口
- 5.0版本外网IP登陆放开443端口

初始的登陆账号和登陆密码为：

5.0版本初始登陆账号和登陆密码

- 审计管理平台：auditadmin/!1fw@2soc#3vpn
- 规则管理平台：ruleadmin/!1fw@2soc#3vpn
- 系统管理平台：admin/!1fw@2soc#3vpn

6.0版本初始登陆账号和登陆密码

- 系统管理员sysadmin/3edc$RFV
- 安全管理员secadmin/3edc$RFV
- 审计管理员auditadmin/3edc$RFV

2、监控墙

查看设备运行的实时状况，主要为五部分（引擎状态、磁盘信息、cpu和内存、接口流量、平均负载）.

引擎模块

反应系统的运行情况，如有任何一个引擎异常，都会导致系统不能正常地进行工作。如证书未上传或证书过期，解析引擎和规则引擎会为黄色停止转动状态，如下图。如证书在有效期内出现

异常可尝试在系统管理-系统维护中重启引擎或者直接联系相关的技术人员。

磁盘信息

显示当前磁盘总量、已占用和剩余磁盘空间。

cpu和内存

显示当前设备最近一分钟的cpu和内存的使用情况。

接口流量

以折线图的方式实时显示接口的流量情况，用户可通过接口流量判断该接口是否为审计口

平均负载

快速查看系统整体性能，反映了整体设备的负载情况 显示当前磁盘总量、已占用和剩余磁盘空间。

3、部署方式

1）网口配置

通过网口配置查看设备的网口信息，包括数量，网口运行状态。主要是针对网口是否启用进行相应的配置。启用某个网口并且该网口有流量进入时，将对该部分数据进行审计；禁用之后，该网口的数据将不做审计。

2）管理口配置

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。网络测试可以检测ip是否可用，网关是否能连通，帮助用户判断是否可以修改管理口信息。

3）部署方式

部署方式默认Agent引流，agent引流更多用于云上审计环境或者没有做端口镜像的场景。

4）Agent引流

通过在审计对象的系统上安装agent，将所需要的流量导入审计设备，从而实现审计操作。此外agent可以在多个审计对象上同时配置并进行引流，关于agent的使用方法可以查看具体的使用文档。

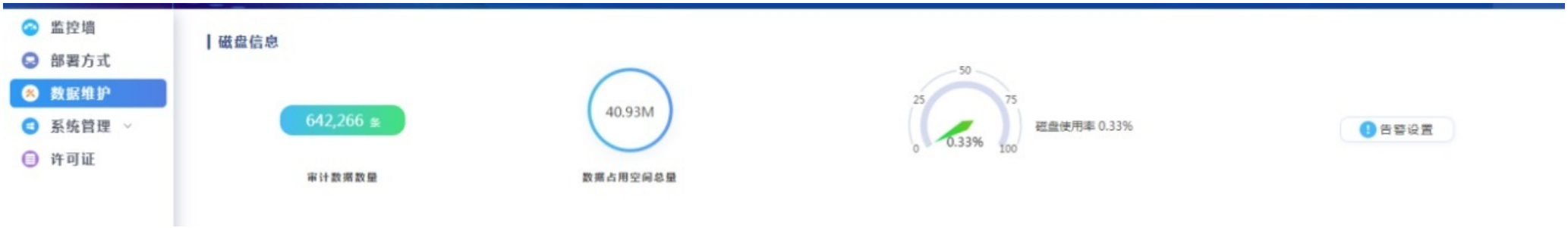
注：服务器与设备之间agent监听端口都需要开放，且两者之间网络可通信。默认设备是9999端口且已开放该端口。

4、数据维护

该模块主要是对审计数据进行管理维护的，主要的操作为备份、清理、恢复。其次还能在此模块查看关于审计数据的磁盘信息。

1）网口配置

查看审计数据（风险、非风险）的总数据量条数，审计数据占用的空间总量以及磁盘的使用率。可根据数值评估是否需要设置告警或者进行数据维护相关操作，保证设备运行在最佳状态。点击“告警设置”按钮会自动跳转到系统告警。



2）数据备份

根据指定的条件对指定的数据进行指定方式的备份，分为自动备份和手动备份两种方式。自动备份最多支持10个任务同时进行，手动备份状态同时只能一个任务进行且下一个任务必须在上一个任务完成后才能添加。

3）数据清理

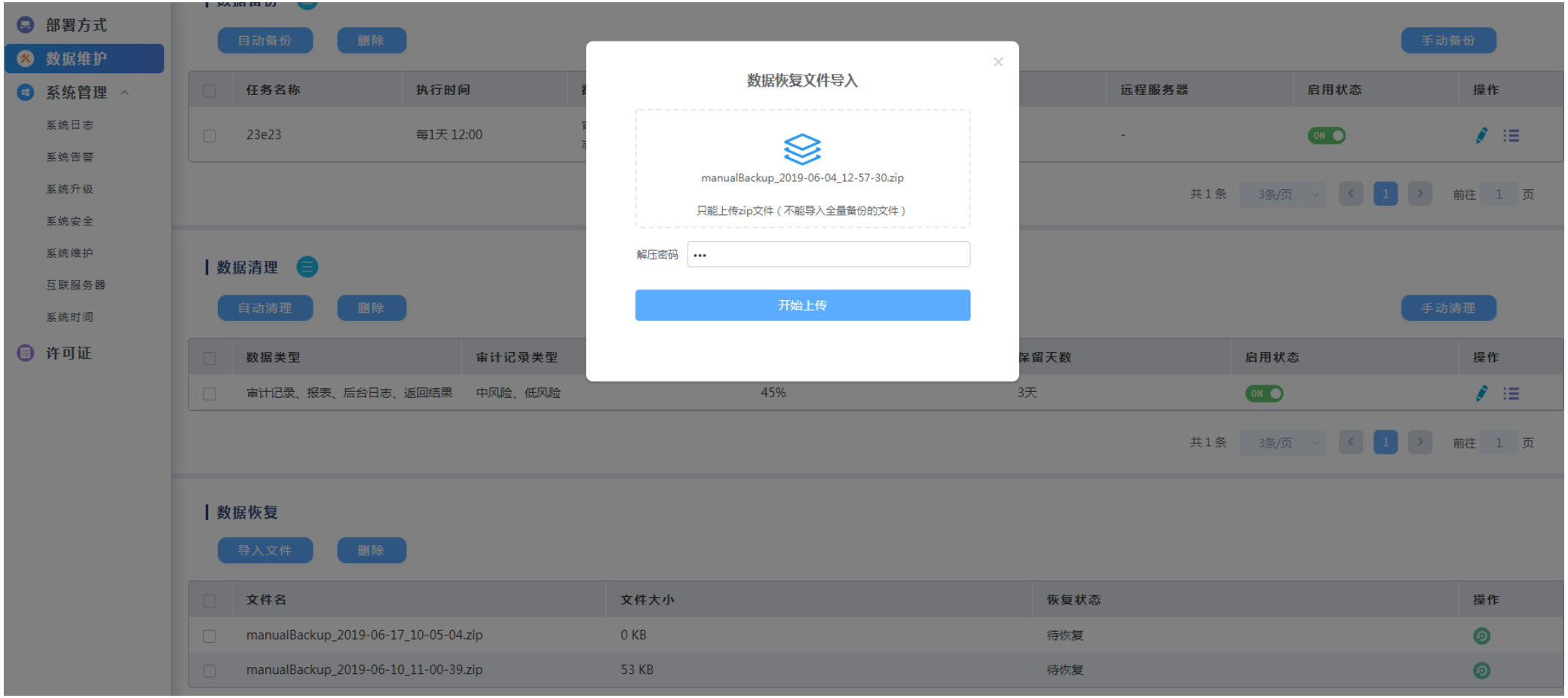
根据指定的条件对指定的数据进行清理，分为自动清理和手动清理两种方式。自动清理只能添加一条配置信息，手动清理只能有一个任务进行且下一个任务必须在上一个任务完成后才能添加。注：自动清理、手动清理以及强制清理执行过程中，会将检索引擎和入库引擎关掉。完成任务后会将程序恢复到正常运行状态。

4）数据恢复

当数据量过大时，或者暂不需要某一段时间的数据，用户可选择将数据备份下来，在需要用到的情况下再对数据进行恢复，保证设备运行状态最佳。

导入文件

导入加密文件需要输入加密的密码，再点击开始上传，上传文件不校验密码是否正确。



不支持全量恢复，且导入的文件大小限制为5G，必须是zip压缩，文件名带有“increment、manual”关键字，不可存在中文。

恢复导入文件

点击恢复图标时，会校验密码是否正确。导入没有加密的文件，不管是否有输入密码，不影响恢复。当有任务在进行恢复时不可以再进行其他文件的恢复，界面上恢复图标会消失

数据恢复

导入文件 删除

文件名	文件大小	恢复状态	操作
manualBackup_2019-06-17_10-05-04.zip	0 KB	失败	
manualBackup_2019-06-04_12-57-30.zip	4.07 MB	待恢复	
manualBackup_2019-06-10_11-00-39.zip	53 KB	恢复中	

共 3 条 3条/页 1 前往 1 页

5、系统管理

1）系统日志

用户可通过系统日志查看设备是否一直正常运行，中途是否有在界面上执行关闭系统或者重启等系统维护操作。设备基础信息是否有修改，如部署方式，管理口ip修改等。也可查看告警日志是否发送成功，是否发送给了正确的接受者。可以针对指定条件查询系统日志，支持对系统日志的导出。

2）系统告警

配置系统告警，有利于实时监控设备运行状态是否正常，能够在设备异常时收到告警信息并及时做出措施，防止重要审计日志的丢失。告警方式包括邮件、短信、syslog、snmp告警，关于告警方式的配置详见4.4.6互联服务器。如果选择了邮件和短信告警方式，告警接收人需要配置邮箱和手机号码，详见4.5用户管理，进行配置，更改配置后需要点击下方的保存按钮才会生效。

系统告警属于高风险告警，添加syslog服务器时的消息等级需要选择高风险。

3）系统升级

支持用户在前台界面进行多种类型（版本、补丁、引擎）的升级以及回退。展示升级记录，对升级记录可追踪，什么时候升级的，升级是否成功等。对升级过程可视化，当升级记录提示升级失败时，用户可下载升级日志文件，将日志发送给相关的技术人员查看失败原因。升级文件需要相关的技术人员提供。

注意:升级或者回退版本后需要清空浏览器缓存,防止浏览器缓存机制导致操作失败。

4）系统安全

安全等级有默认的高中低三种,用户也可自定义选择各个条件组合成适合自己的安全策略。更改配置后需要点击下方保存按钮才可生效。

5）系统维护

设备管理

提供在web界面上对设备直接进行操作，用户可在此处对审计系统进行重启关闭等操作，也提供审计引擎的重启以及关闭。对系统的重启以及关闭需要输入登录密码，该部分任意功能的实现都会影响审计功能，建议用户慎重使用。

配置信息收集

此功能与数据备份中备份配置信息一致，配置信息内容都是一样的，唯一差别是，备份出来的配置信息是脚本，可视化差。配置信息收集导出的是Excel文档，可视化高，且用户可在文档上进行个人编辑后再导入。导出Excel内容包括配置信息：保护对象、策略管理、对象管理（不包括工号提取）以及各个配置之间的引用关系。

6）互联服务器

该模块主要是用来配置与设备通信的外部服务，大多是用于告警通知方式的发送方和接收方，需要保证设备与各个服务之间是可通信的。

6、许可证

第一次使用系统或者需要续期时，进入该界面，将设备的机器码下载后发送给相关的技术人员，技术人员会返回一份以lic结尾的文件。上传该文件后，先查看授权时间、功能是否正确，再查看5.1监控墙引擎模块是否都正常，如某一个引擎没起来可以尝试在4.4.5.1 设备管理模块重启引擎，还有问题可向相关技术人员寻求帮助。

注意返回的证书文件编码是否与发送的一致，例如：下载的机器码：clientInfoFile44F88EF60861CF37.info 返回的证书文件：44F88EF60861CF37_audit.lic

上传证书时先确保系统时间是否正确，如在系统时间不正确情况下上传证书会导致证书校验不通过。

1、监控墙

对设备的整体审计情况进行查看，用户可通过监控墙了解到设备审计状态是否正常，能有效把控风险的数量，及时做出有效措施。

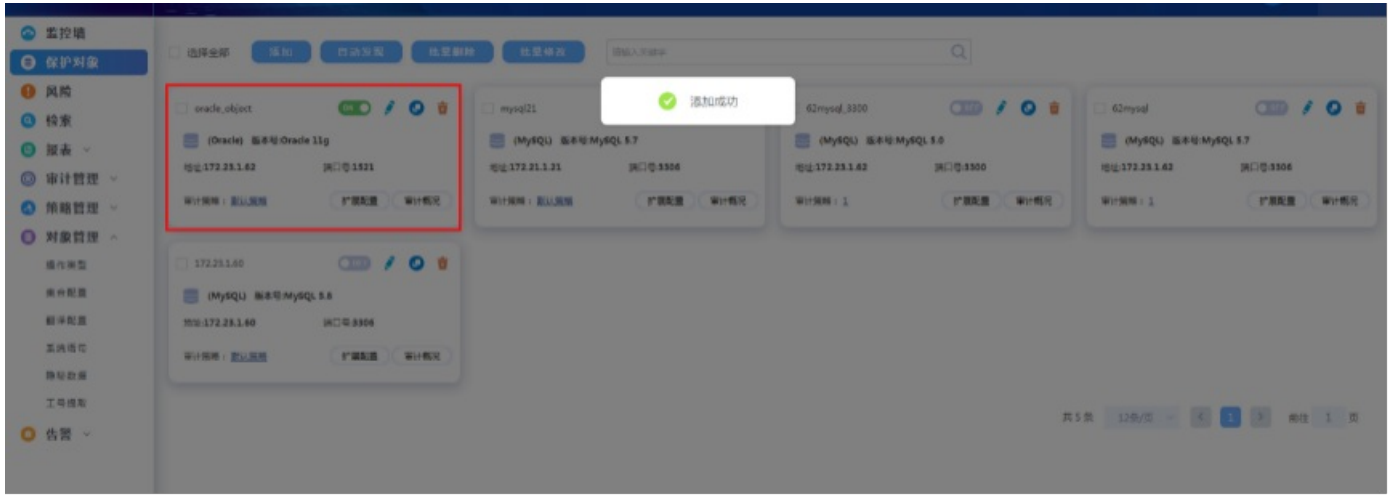

监控墙
保护对象
风险
检索
报表
审计管理
策略管理
对象管理
告警
15,610
117,531
流量
会话
入库速率
规则匹配度
select
test

2、保护对象

配置需要保护的数据库，支持十几种数据库类型审计，包括后关系型数据库cache，HBASE、MongoDB等大数据审计，达梦、人大金仓等国产数据库的审计。审计对数据库进行操作的行为，配置相应的策略将危险性行为特别标注出来，帮助用户快速发现危险操作行为，及时作出处理措施。

1）保护对象配置

点击界面“添加”按钮，弹出添加保护对象对话框



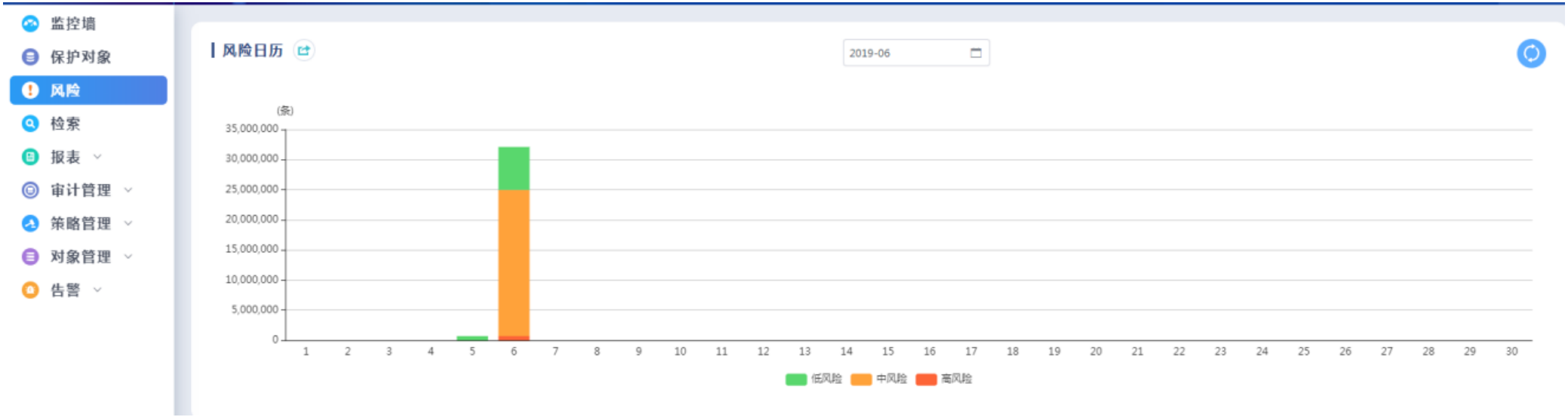
2）自动发现

如果用户存在较多资产都需要配置保护对象的时候，手动进行配置显然不是一个好方法，那么我们通过自动发现功能，实现资产的批量添加，从而提高操作效率。点击保护对象中的自动发现按钮，弹出配置界面。地址范围，任务执行时间和数据库类型可以根据实际情况进行填写，发现类型包括“全部”和“端口扫描”，填写完成后即可开始扫描。

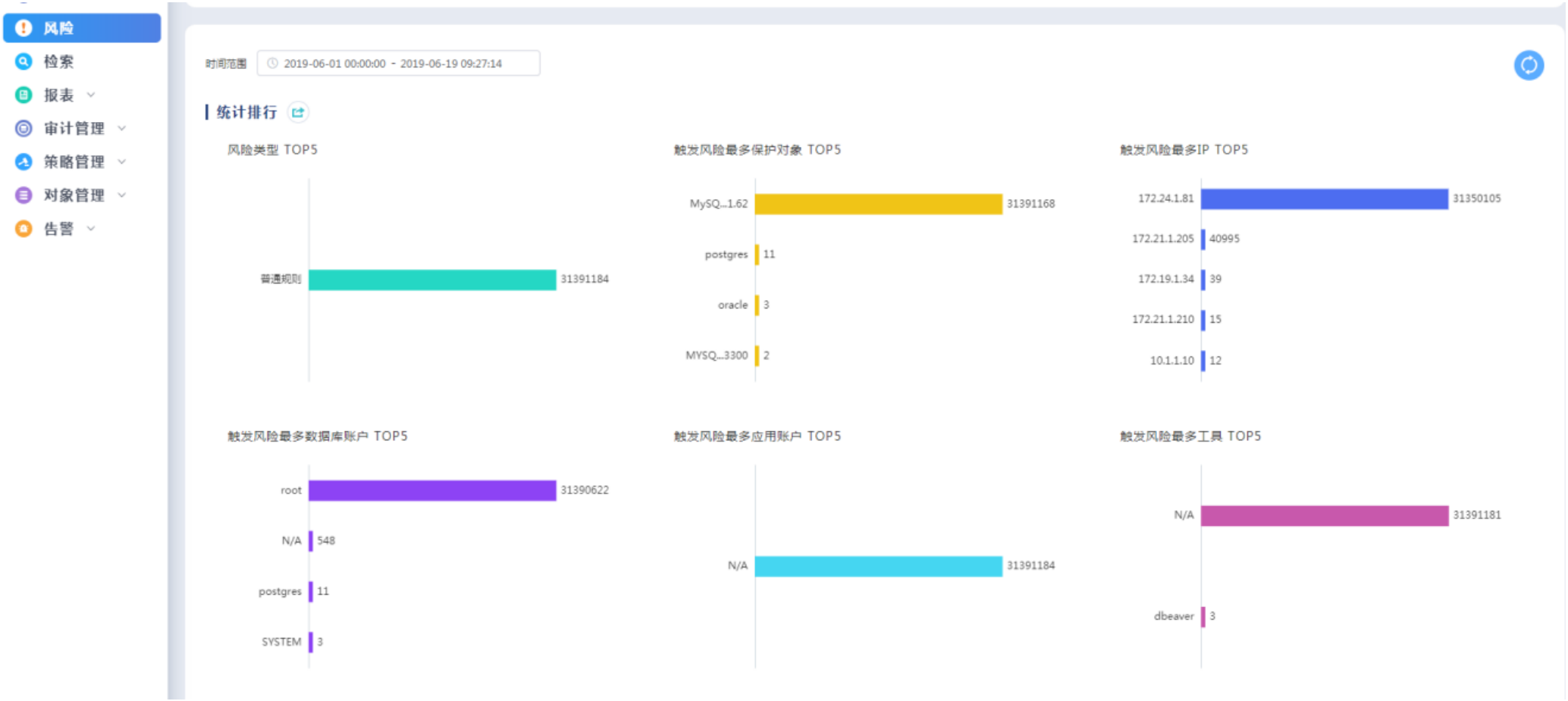
扫描完成后可以点击完成资产的批量添加，或者点击实现单台添加；另外扫描的结果也是可以查询的，通过输入对应的地址，数据库类型，任务执行时间段还有处理状态来进行查询。

3、风险

该界面主要分为两部分，第一部分为风险日历，展示一个月每一天风险产生的情况。直观看见风险趋势图，以及各类风险占的总比例。可直接点击柱状图跳转至当天风险的检索列表。



第二部分为TOP5，统计时间范围里风险类型TOP5、触发风险最多保护对象TOP5、触发风险最多IP TOP5、触发风险最多数据库账户TOP5、触发风险最多应用账户TOP5，触发风险最多工具TOP5。用户可根据TOP5评估该风险行为是否造成了影响。



4、检索

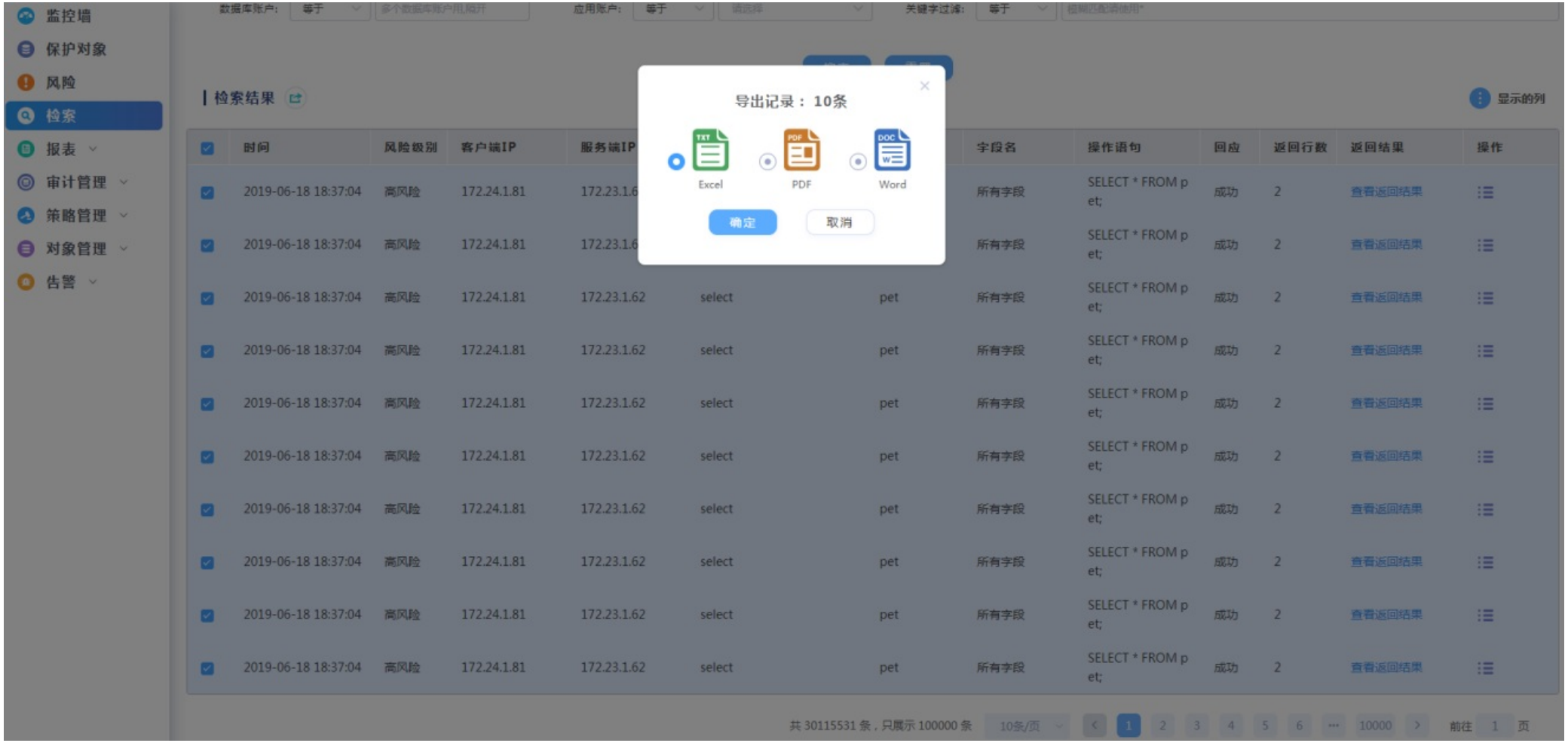
检索可以让用户对审计日志进行查询，通过各种查询条件的搭配，帮助用户完成审计日志的精确查询。进入审计日志的检索界面，该界面包括检索条件和检索结果两个模块。

1）检索条件

其中检索条件包括基本检索和高级检索。默认显示的为基本检索，点击检索条件右边的图标，弹出的检索条件为高级检索条件，可勾选条件后点击确认，加入到界面上。

2）检索结果

检索结果显示的列也可以通过手动去选择，点击显示的列左边的图标，弹出显示检索列，可自行勾选要在界面上显示出来的列选项。支持检索结果的导出，点击按钮进行导出，导出选项包括导出选中和导出全部，导出的文件形式包括Excel，PDF，Word。


监控墙
保护对象
风险
检索
报表
审计管理
策略管理
对象管理
告警
检索结果
显示的列
导出记录：10条
Excel
PDF
Word
确定
取消
时间
风险级别
客户端IP
服务端IP
字段名
操作语句
回应
返回行数
返回结果
操作
2019-06-18 18:37:04
高风险
172.24.1.81
172.23.1.62
select
pet
所有字段
SELECT * FROM pet;
成功
2
查看返回结果
共 30115531 条，只展示 100000 条
10条/页
前往 1 页

5、报表

1）分析报表

被监测的数据库:该部分数据主要是针对数据库的连接信息进行报表统计，旨在给客户提供其数据库的访问情况。数据库服务性能:该部分数据主要是针对数据库本身的查询参数进行统计，旨在给客户提供其数据库查询性能的相关参数。

2）合规报表

本报表参考《中国国家信息安全保护检验标准》完成设计，针对国家等级保护的检测要求进行审计数据统计，能够帮助数据库管理人员、审计人员对各种异常行为和违规操作及时发现，快速定位分析，为整体信息安全管理提供决策依据。

数据库审计状态

该报表主要是数据库审计概要内容展现，帮助用户快速了解当前数据库审计状态，主要包括了“保护对象名”，“访问者数量”，“数据库账户数量”，“审计总量”。

保护对象名	访问者数量	数据库账户数量	审计总量
62mysql	7	2	29818056
172.21.1.21	2	1	196
62mysql_3300	3	1	150
mysql21	1	1	6

客户端访问分析

展示数据库是否存在可能的非法客户端访问，及访问状态分析，主要包括“保护对象名”，“访问者工具”，“访问者IP”，“数据库账户”，“登录数量”。

保护对象名	访问者工具	访问者IP	数据库账户	登录数量
62mysql	plsql	172.24.1.61	root	69
62mysql	dbeaver	172.19.1.34	root	6
62mysql	navicat	172.21.1.205	root	6
172.21.1.21	navicat	172.21.1.205	root	5
62mysql_3300	sqlplus	172.21.1.202	root	4

审计日志统计分析

展示所有被审计数据库产生的操作次数，帮助审计人员进行趋势分析。

保护对象名	访问者IP	操作次数
62mysql	172.24.1.81	29966359
62mysql	172.24.1.106	145803
62mysql	172.22.1.89	1989
62mysql	172.24.1.61	469
62mysql	172.21.1.205	318

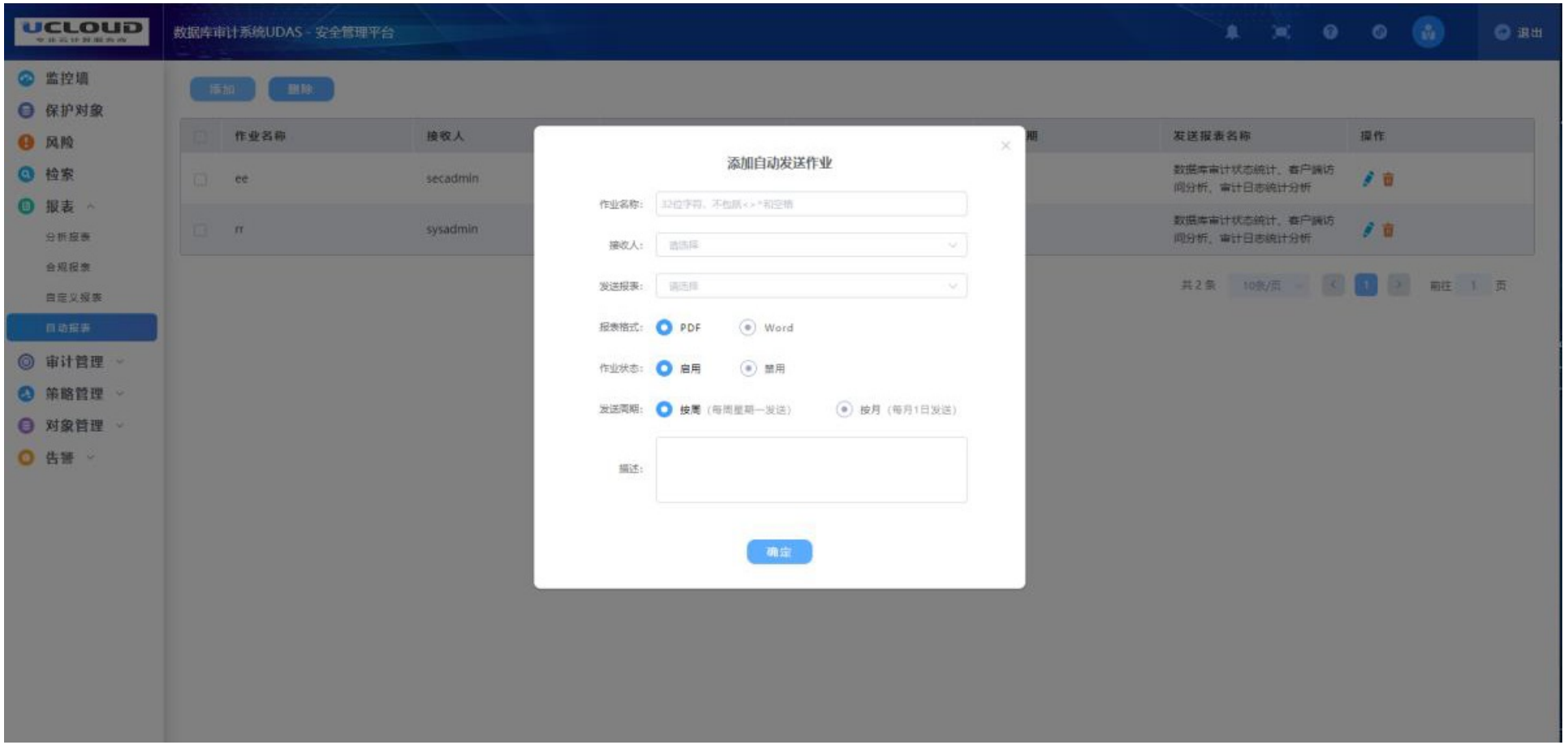
3）自定义报表

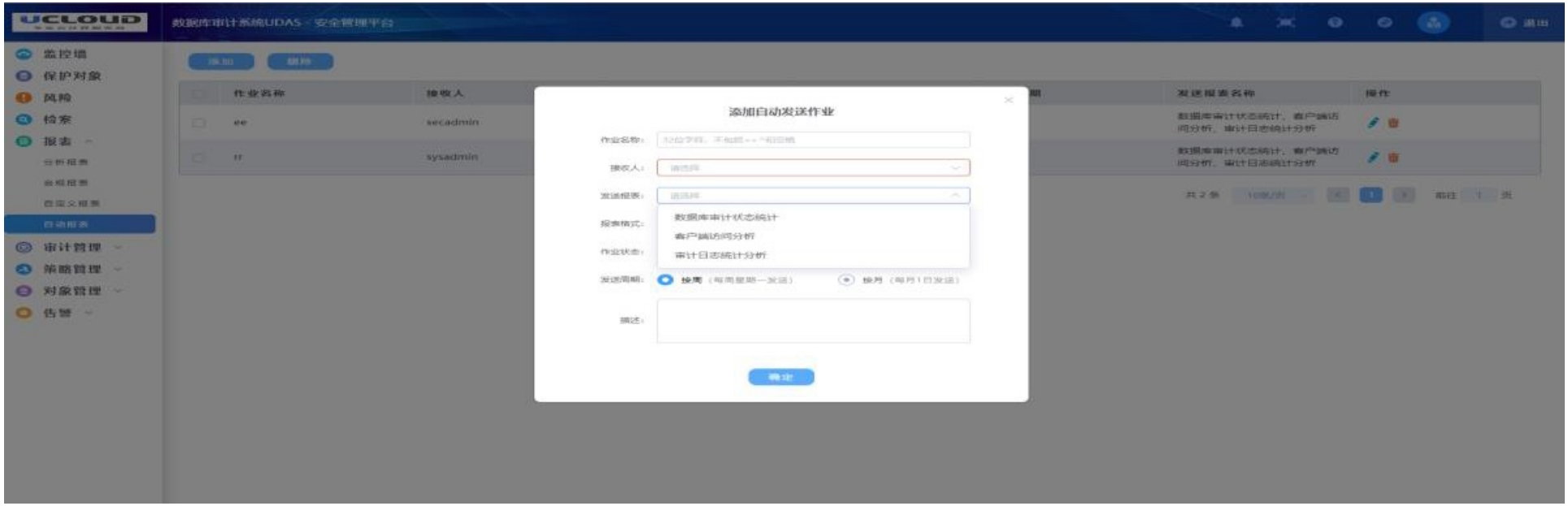
自定义报表可以让用户灵活地定制自己所需的内容,统计维度包含了时间,保护对象,客户端ip, 服务端ip, 访问工具,操作类型,数据库账户,数据库名,表明,执行回应

4）自动报表

在一级菜单报表，二级菜单自定义报表下方新添加自动报表选项卡，页面显示添加、删除两个按钮和已经添加好的自动发送报表任务列表。在点击添加按钮后，会弹出一个弹框，弹框会显示

要添加的任务名、邮件的接收人、要发送的报表、报表的格式、任务状态、任务周期和任务描述。其中邮件的接收人必须要用户在个人信息添加邮件后才会有数据显示，要发送的报表和二级菜单合规报表相对应，报表的格式只有pdf和word两种格式，任务周期只有一周发送一次和一月发送一次。




数据库审计系统UDAS - 安全管理平台
监控墙
保护对象
风险
检索
报表
审计管理
策略管理
对象管理
告警
作业名称
接收人
发送报表名称
操作
ee
secadmin
tt
sysadmin
添加自动发送作业
作业名称：
接收人：
发送报表：
报表格式：
作业状态：
发送周期：
描述：
数据库审计状态统计
客户端访问分析
审计日志统计分析
按周（每周星期一发送）
按月（每月1日发送）
确定

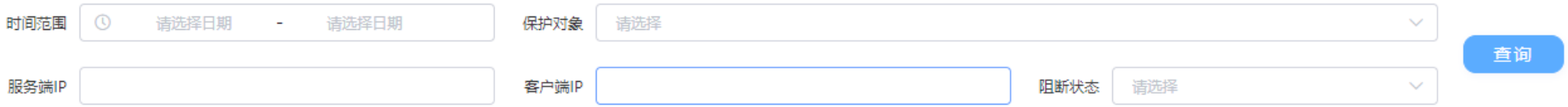
6、审计管理

1）阻断管理

阻断管理包含所有已被阻断的客户端IP，管理者查看阻断记录，并对阻断客户端ip进行管理。阻断ip的产生是由于客户端操作了动作为严格阻断的规则并且审计策略开启了阻断，则该客户端ip除非从阻断管理中释放，否则不能继续操作数据库。

查询

阻断记录的查询条件包含“时间范围”，“保护对象”，“服务端IP”，“客户端IP”，“阻断状态”五种



通过选择对应的查询参数后，点击查询按钮即可完成阻断记录的查询和筛选。

释放

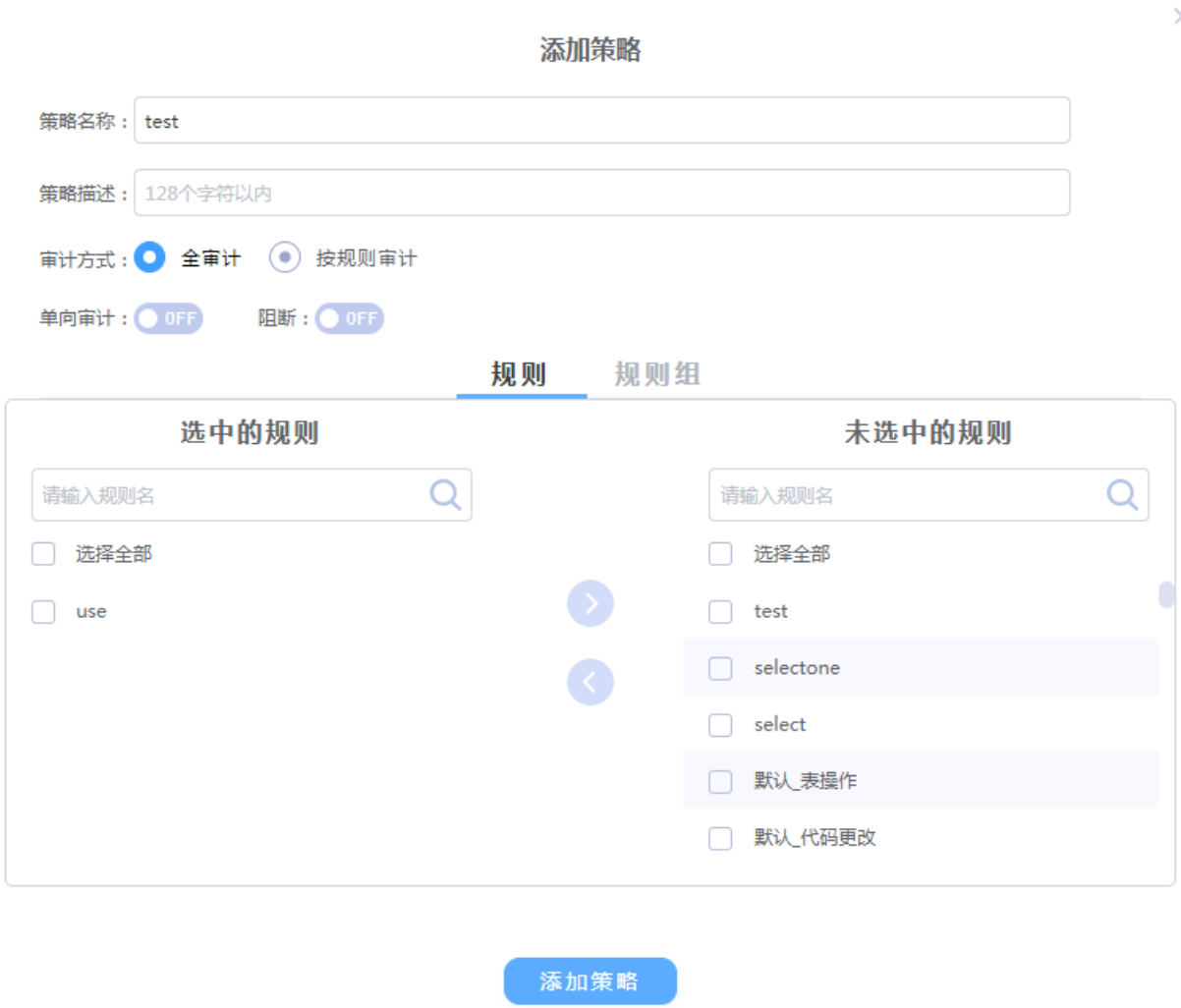
对于已阻断的客户端ip，可以对其进行勾选，然后点击释放按钮即可释放被阻断的客户端ip，该客户端ip就可以继续操作数据库，如果继续触发了阻断的规则，还是会被阻断。阻断记录的查询条件包含“时间范围”，“保护对象”，“服务端IP”，“客户端IP”，“阻断状态”五种

时间	保护对象	服务端IP	服务端端口	客户端IP	阻断状态
2019-06-18 16:30:16	obj1	2.2.2.2	11223	1.1.1.1	阻断中

7、策略管理

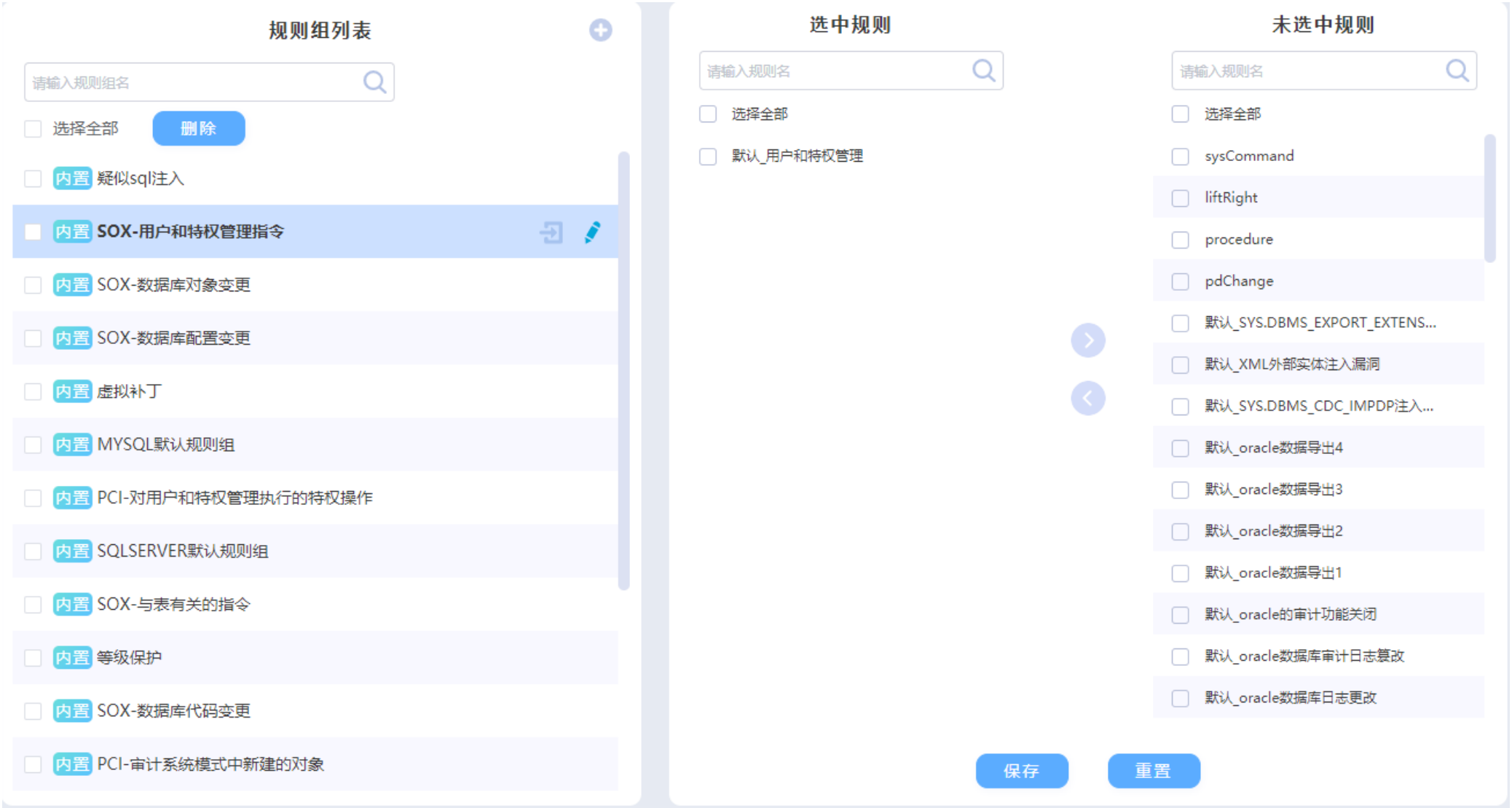
1）审计策略

审计策略是规则组和规则的集合，它是审计过程中的核心所在，审计对象通过应用不同的审计策略，从而实现不同的审计效果。系统内置一个默认策略，不包含任何规则和规则组，审计方式为全审计。



2）规则组

规则组是若干规则的集合，通过对规则进行整合，可以让审计对象批量应用规则，同时也方便用户对规则进行管理。



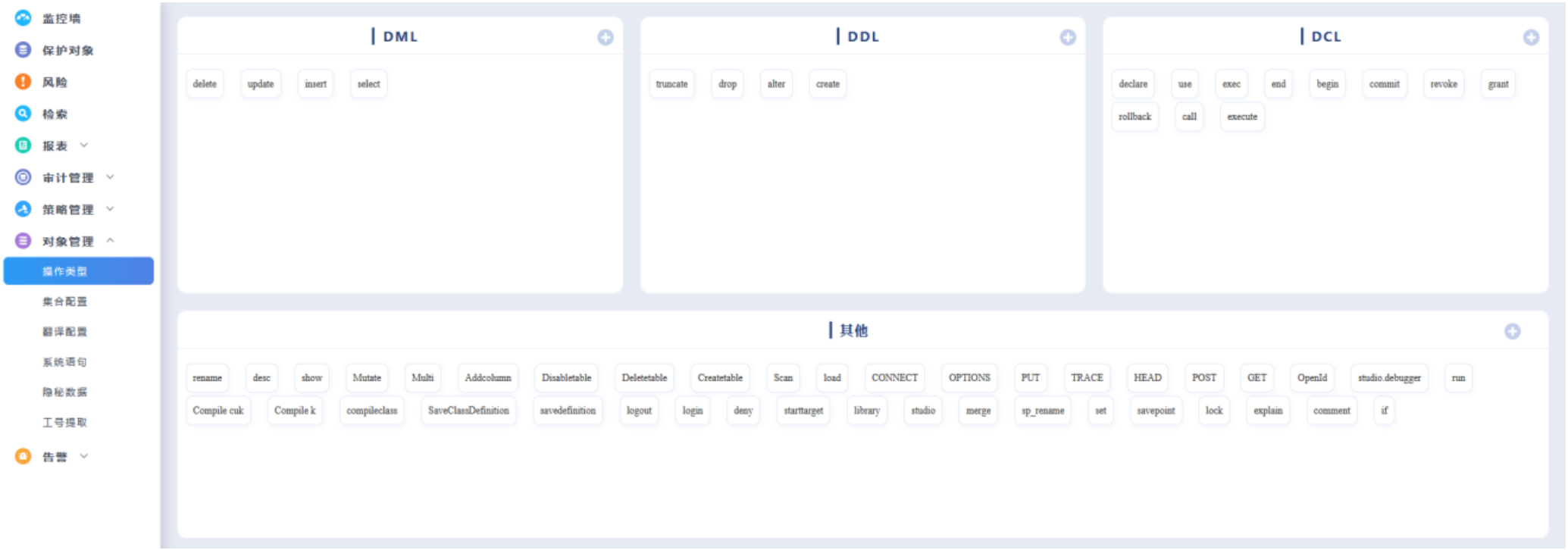
3）规则

规则是审计的核心所在，也是策略中的最小单位，所有审计都是通过配置对应的规则来完成触发，灵活运用规则可以大大提高审计的效率和准确性。

8、对象管理

1）操作类型

系统内置了多个常见的DML（数据操作语言）、DDL（数据定义语言）、DCL（数据控制语言）和其他操作类型，也可以根据需求自行添加上述类别的操作语言，自行添加的操作类型可在规则中选择引用。



2）集合配置

集合配置中关于访问工具、IP地址、客户端MAC、操作系统主机名、操作系统用户名、应用账户名的集合和基础元素配置，可以方便在检索中作为搜索条件过滤审计结果，也可以应用到6.7.3规则中作为规则的高级配置项。集合配置可以做添加、删除、修改、搜索等操作，基础元素可以添加到集合中.

3）翻译配置

保护对象别名

保护对象别名会在检索结果中对相应的表名、字段名、关键字进行标注翻译，方便识别和查看。保护对象别名规则可以做添加、删除、修改、搜索操作。

数据库

数据库类型： MySQL

地址： 172.21.1.24：3306

数据库名： test

操作类型： select

表名： students

字段名： 所有字段

操作回应： 成功

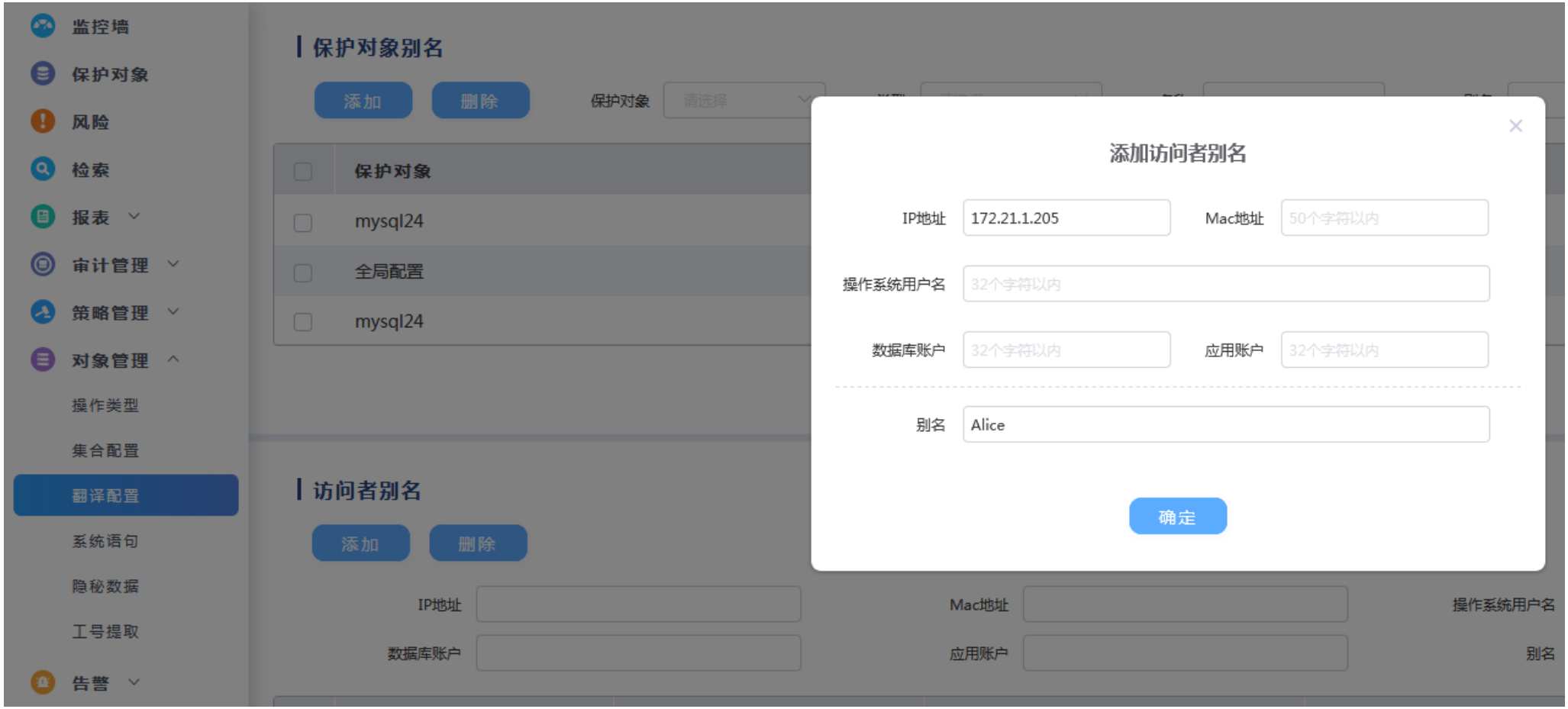
操作耗时： 0.084毫秒

操作描述： 用户对test数据库[学生信息]表所有字段进行了查询操作；操作发生在：2019-06-19 09:49:02，使用的电脑IP为：172.21.1.205，电脑物理地址（MAC地址）为：38:D5:47:13:2D:77

操作语句： SELECT * FROM test.students LIMIT 0,1000

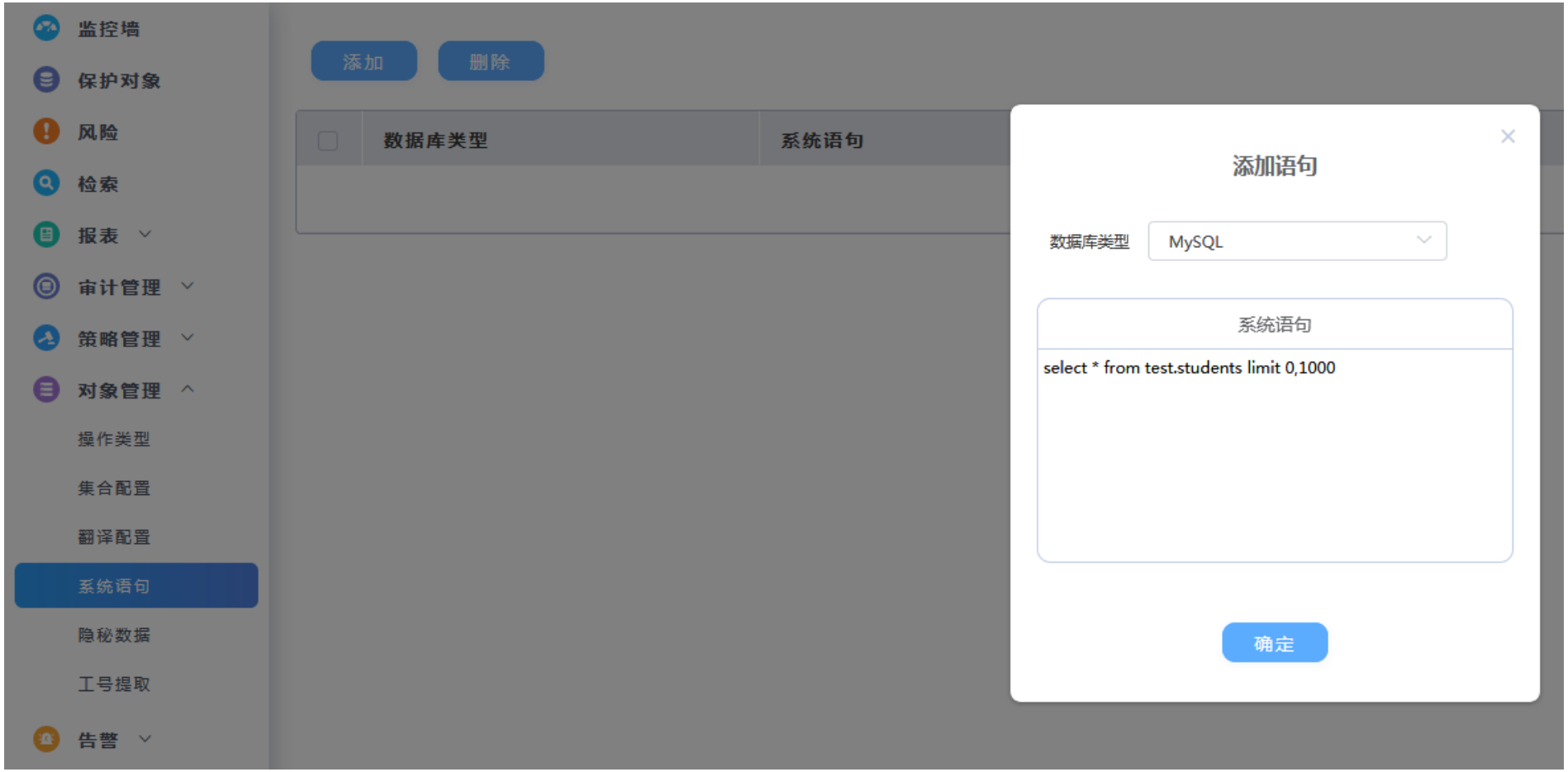
访问者别名

访问者别名可以在检索结果中直观的看到了是谁操作了数据库。访问者别名规则可以做添加、删除、修改、搜索操作。



4）系统语句

系统语句可以将确认正常操作的sql语句进行标注，在以后的审计中不做审计，在检索结果中不显示。系统语句规则可以做添加、删除、修改、搜索操作。



添加完成后，对已有的mysql类型的保护对象执行上述操作语句，在检索中查看审计结果，不包含该条语句。

5）隐秘数据

隐秘数据可以将保护对象中的关键数据（表名和字段），在返回的审计结果中做隐秘处理，防止二次泄密。隐秘数据规则可以做添加、删除、修改、搜索操作。

返回结果

id	class_id	name	gender	score
1	1	******	M	90
2	1	******	F	95
3	1	******	M	88
4	1	******	F	73
5	2	******	F	81
6	2	******	M	55
7	2	******	M	85
8	3	******	F	91
9	3	******	M	89

确定

添加完成后，查询保护对象的students数据，在检索中查看返回结果中的name字段的记录已被隐藏。

6）工号提取

工号提取把需要的工号提取出来，对应的是检索结果中的应用账户，能够让用户根据现场环境自定义配置，不需要定制化需求。工号提取规则可以做添加、删除、修改操作。

对保护对象进行登录操作，查看审计检索结果，能提取到工号（应用账号）。

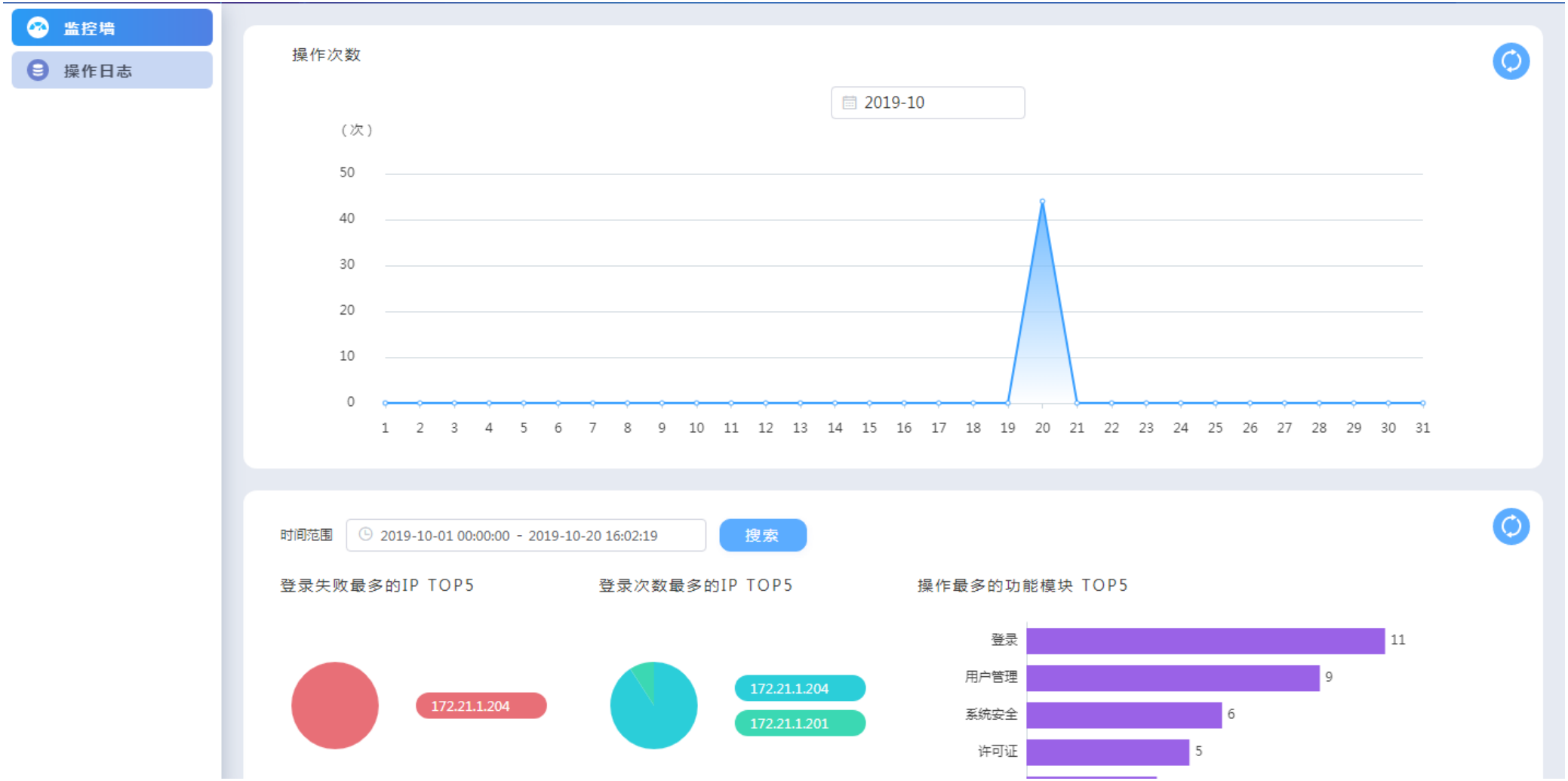
9、告警

1）告警策略

告警策略是对审计事件实时告警的方法，用户通过对告警的事件，告警方式，告警的接收者进行配置告警策略。将告警策略应用到保护对象中，一旦有符合告警策略的审计记录产生，就会实时告警通知，从而协助安全人员快速识别安全事故。

1、监控墙

整体显示设备的登录和操作信息，主要为四部分（操作次数、登录失败最多的IP TOP5、登录次数最多的IP TOP5、操作最多的功能模块TOP5）

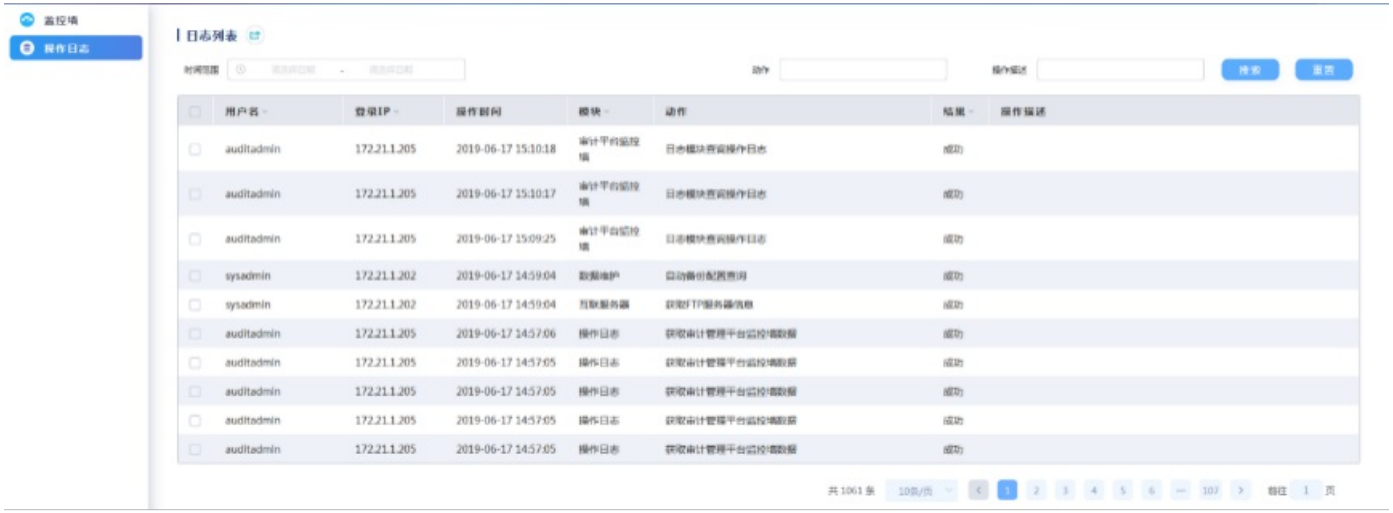


a.操作次数：显示所选年份和月份的每一天内，设备的操作次数。b.登录失败最多的IP TOP5：显示搜索时间范围内，登录设备失败次数最多的前五名的IP地址，含详细次数和所占百分比，点击饼状图中的任意IP，可以跳转到操作日志来查看对应IP登录失败的时间、用户名等详细信息。c.登录次数最多的IP TOP5：显示搜索时间范围内，登录设备次数最多的前五名的IP地址，含详细次数和所占百分比，点击饼状图中的任意IP，可以跳转到操作日志来查看对应IP登录的时间、用户名、登录成功或失败等详细信息。操作最多的功能模块TOP5：显示搜索时间范围内，设备操作次数最多的功能模块的前五名，点击任意功能模块的条形图，可以跳转到操作日志来查看对应功能模块的操作时间、用户名、登录IP、动作等详细信息。系统内置了多个常见的DML（数

据操作语言）、DDL（数据定义语言）、DCL（数据控制语言）和其他操作类型，也可以根据需求自行添加上述类别的操作语言，自行添加的操作类型可在规则中选择引用。

8、操作日志

操作日志展示了三大平台的用户的操作情况，可以查看详细操作日志信息，以保证审计设备自身安全。



默认显示设备所有的操作日志，可以通过配置时间范围，输入动作或操作描述来搜索满足条件的操作日志。用户名、登陆IP、模块、结果可以通过下拉按钮来进行筛选，筛选后仅显示满足筛选条件的操作日志。操作日志可以导出所有日志或选中的日志为Excel或PDF。系统内置了多个常见的DML（数据操作语言）、DDL（数据定义语言）、DCL（数据控制语言）和其他操作类型，也可以根据需求自行添加上述类别的操作语言，自行添加的操作类型可在规则中选择引用。

数据库审计版本升级说明

线上版本：6.3.2版本

修复问题：

暂无。

新增功能：

互联服务器新增OSS远程备份存储服务器。

删除特性：

暂无

产品手册下载

最新版用户手册

数据库审计系统v6.3.2用户手册.docx

快速购买配置指南及Agent部署指导手册

老版用户手册

数据库审计系统用户手册1.0.pdf

快速配置指南及Agent部署指导手册

产品价格

使用注意事项

版本适用范围：高级版、企业版、旗舰版

1. 不支持退费；

2. 购买后我们会为您部署，部署时需要人工操作，一般为1-2个工作日内完成，如需加急，请与您的客户经理或者技术支持联系。

计费模式

注意，数据库审计购买满3个月后才支持客户自行删除退费。

付费方式： 底层主机+磁盘+license（资源管理费用）

计费标准： 以数据库审计的型号为计费标准

计费周期： 高级版/企业版/旗舰版：支持按年、3个月、6个月、9个月；允许续费和升级；不允许提前删除退费。

预付/后付：

所有版本：所有费用预付。

例如：购买国内机房华北一可用区C的“高级版”数据盘300G数据库审计，则费用为：主机+磁盘+license=481+120+3300=3901元/月；如果需要扩展磁盘则在原有基础上补磁盘的价格。

镜像费用

支持按年购买，按月购买（按月至少购买3个月，可选3个月、6个月或9个月）

镜像版本-普通授权	镜像价格 元/月	镜像价格 元/年
高级版-3个实例	3300	33000
企业版-8个实例	6600	66000
旗舰版-32个实例	22000	220000

镜像版本-普通授权+大数据授权模块	镜像价格 元/月	镜像价格 元/年
高级版-3个实例	4800	48000
企业版-8个实例	9600	96000
旗舰版-32个实例	30000	300000

普通数据库授权模块包括：

1、关系型数据库：Mysql、Sqlserver、oracle、Sybase、DB2、Informix、PostgreSQL、 MariaDB、XUGU（虚谷）

2、国产数据库：达梦、人大金仓、神通数据库、南大通用

大数据库授权模块包括：

1、后关系型数据库：Caché DB

2、内存数据库：HANA 、Redis

3、大数据数据库：RECORD_HIVE、SPARK_JAVA_API、Hive、HIVE_HSQL、Record_Hive、ES、GaussDB（华为高斯）、LibrA、HBASE_SHELL、Solr、MongoDB

4、工控实时数据库：IP21_API、IP21_APIIP21_WEBSERVICE

普通磁盘

可用区	价格
所有区域	4元/10G/月

主机费用（以控制台实际价格为准）

主机类型	可用区	价格 元/月
4核8G-linux-标准型-60G硬盘（高级版-3个实例）	一般国内	481
	金融云	865
8核16G-linux-标准型-60G硬盘（企业版-8个实例）	一般国内	1000
	金融云	1680
16核32G-linux-标准型-60G硬盘（旗舰版-32个实例）	一般国内	1901
	金融云	3152

产品性能

版本	底层主机	性能参数	数据库实例数
高级版	4核8G-linux-标准型-60G硬盘	峰值:8000条SQL语句/秒级吞吐量,300万/小时入库速度;在线SQL语句存储8亿条(日志可实现网络转存)	3
企业版	8核16G-linux-标准型-60G硬盘	峰值:20000条SQL语句/秒级吞吐量,500万/小时入库速度;在线SQL语句存储16亿条(日志可实现网络转存)	8
旗舰版	16核32G-linux-标准型-60G硬盘	峰值:30000条SQL语句/秒级吞吐量,1000万/小时入库速度;在线SQL语句存储16亿条,360亿条SQL语句归档存储支持(日志可实现网络转存)	32

访问数据库审计系统时，验证码无法加载出来，

答:数据库审计外网防火墙开放8443端口