★完全公开

奇安信网神数据库审计与防护系统 V6.0（6.5.7）用户手册 V1.0

创建时间：2025 年 8 月 6 日

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：100044

● 版权声明

奇安信集团，保留所有权利。
奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。
对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。
由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（**“本声明”**）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称**“本产品”**）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**
2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**
3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**
4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**
5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品，**奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**
6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传**

输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利： **在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**
8. 本声明受中华人民共和国法律的约束并依据其解释。
9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	新建	赵康驰	李超	2025/06/10

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据（Y）	内部数据（）	普通商秘（）	核心商秘（）

*数据分级标注及说明：

1、文档编写前，应标注数据安全级别，默认为内部；

2、请根据文档内容评估数据安全级别，在对应数据级别（）中填写（Y）；

3、分级 TIPS：

【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；

【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；

【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；

【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。

更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips

目录

1 产品概述 10
1.1 产品简介 10
1.2 产品功能 10
1.3 适用产品 11
1.4 读者对象 11
1.5 配套手册 11
1.6 符号约定 11
2 系统登录 13
2.1 兼容性 13
2.2 登录信息 13
2.3 登录异常告警提醒 13
3 导航栏 15
3.1 消息盒子 15
3.2 锁屏 15
3.3 帮助 16
3.4 关于我们 16
3.5 用户管理 17
3.5.1. 个人信息 17
3.5.2. 修改密码 18
3.5.3. 用户管理 18
4 系统管理平台 21
4.1 监控墙 21
4.2 系统管理 22
4.2.1. 部署方式 22
4.2.2. 系统告警 27
4.2.3. 系统安全 27
4.2.4. 互联接口 30
4.2.5. 系统时间 35
4.2.6. 许可证 38
4.2.7. 审计日志外发 38
4.3 系统维护 39
4.3.1. 系统维护 39
4.3.2. 系统升级 43

4.3.3. 系统日志 43
5 安全管理平台 45
5.1 监控墙 45
5.2 态势感知 50
5.3 保护对象 53
5.3.1. 保护对象配置 53
5.3.2. Agent 管理 65
5.4 风险 71
5.5 检索 72
5.6 报表 77
5.6.1. 分析报表 77
5.6.2. 自定义报表 94
5.6.3. 自动报表 97
5.7 敏感监控 98
5.7.1. 敏感数据 98
5.7.2. 敏感发现 102
5.7.3. 敏感分析 110
5.8 拦截管理 114
5.9 策略管理 116
5.9.1. 审计策略 116
5.9.2. 规则组 118
5.9.3. 规则 121
5.10 配置管理 125
5.10.1. 集合参数 125
5.10.2. 业务字典 133
5.10.3. 翻译配置 136
5.10.4. 隐秘数据 152
5.10.5. 工号提取 153
5.10.6. 系统语句 162
5.10.7. 驱动级 IP 过滤 162
5.10.8. 白名单管理 165
5.11 数据维护 167
5.11.1. 外置存储 167
5.11.2. 数据备份 167
5.11.3. 数据清理 171

5.11.4. 数据恢复 173
5.12 告警 174
5.12.1. 告警策略 174
5.12.2. 告警通知日志 175
5.13 操作日志 175
6 审计管理平台 177
6.1 监控墙 177
6.2 操作日志 177
7 FAQ 179
8 注释 182
8.1 缩略语 182
8.2 术语 182
9 附录 184
9.1 企业微信对接流程 184
9.2 钉钉对接流程 189

1 产品概述

1.1 产品简介

奇安信网神数据库审计与防护系统是一款软硬一体化产品，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。数据库审计与防护系统采用数据库深度报文协议解析技术 DPI 及流媒体分析技术 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。

奇安信网神数据库审计与防护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数据库审计与防护系统独立的平台中，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;审计管理员负责查看整体设备的操作日志情况。

1.2 产品功能

本产品涵盖以下几大功能：

- 审计
  - 通过对网络行为进行记录，可用来分析网络状况和确定网络使用者的相关责任。
- 策略：根据业务需求，制定网络行为分析引擎。
  - 产品的核心功能，对网络行为进行采集，使用分析引擎过滤出有用的数据包后，提供给审计功能使用。
  - 具有丰富的审计策略配置功能。

- 告警：包含告警规则设置和告警事件的查看功能。
  - 告警规则：针对符合策略的事件进行关联分析，抽取出对于安全管理人员真正有用的安全信息，提供实时告警，从而协助安全管理人员快速识别安全事故。
  - 告警事件：查看由告警规则产生的事件。
- 报表：包含系统内置报表，能够将业务分析情况以报表的形式提交给指定的部门。
  - 内置报表：常见通用报表，例如：基本的合规报表。
- 系统管理：对系统内部进行相关的设置，并进行统一的管理。
  - 系统配置：配置系统运行参数，包含：服务器配置、安全等级以及数据维护等功能。
  - 系统维护：对系统的自身的维护信息，包含地址管理、许可证导入、时间同步等。

1.3 适用产品

适用于奇安信网神数据库审计系统 V6.0（6.5.7.9.0）。

1.4 读者对象

本手册适用于 DAS 产品使用人员。包括企业和组织的领导层、企业安全负责人以及安全管理人员、安全分析员和安全运维人员。

通过阅读本文档，系统管理员、安全管理员、审计管理员可以独自完成以下工作：

- DAS 的基本配置
- 针对企业业务制定审计策略
- 对数据库、主机的操作行为进行审计
- 针对业务特性制定告警规则
- 数据综合分析，生成审计报表

1.5 配套手册

无。

1.6 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号名称	说明
警告	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

2 系统登录

2.1 兼容性

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

本系统仅保证屏幕水平方向像素范围为 1366 到 1920 时的显示效果，推荐使用屏幕分辨率 1920 x 1080（即 1080p）以获得最佳显示体验。

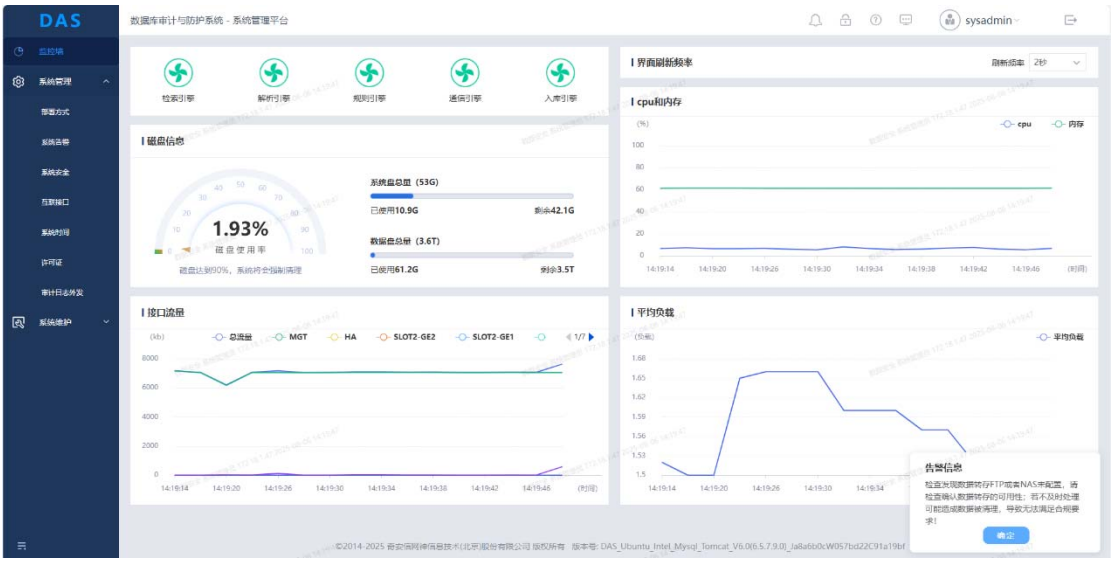
2.2 登录信息

系统采用三权分立的模式，各平台的功能与职责不同，权限不同，相互监督。进入登录页面后，输入用户名、密码、验证码进行登录，首次登录需要修改密码。首次登录的默认信息如下：

角色	用户名	密码	基本权限
系统管理员	sysadmin	!1fw@2soc#3vpn	许可证、部署方式等
安全管理员	secadmin	!1fw@2soc#3vpn	保护对象、策略管理、配置管理等
审计管理员	auditadmin	!1fw@2soc#3vpn	监控墙、操作日志

2.3 登录异常告警提醒

登录页面右下角弹框提醒，每种异常系统配置一个弹框告警。如下图：



告警类型：

1、磁盘容量不足告警，告警格式:【告警】磁盘空间不足，请检查确认数据转存的可用性；若不及时处理可能造成数据被清理，导致无法满足合规要求；

2、CPU 超过阈值进行告警，告警格式:【告警】CPU 负载过高，请确定服务正常；若不及时处理可能造成审计不及时

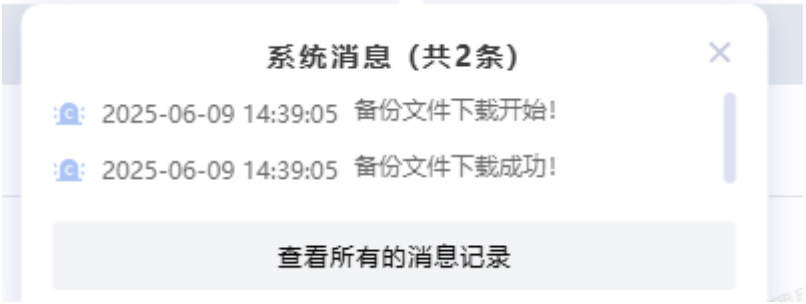
3、FTP、NAS 未配置告警及清理时，达到最高阈值时且无法再清除时，进行告警，告警格式:【告警】检查发现数据转存 FTP 或者 NAS 未配置，请检查确认数据转存的可用性；若不及时处理可能造成数据被清理，导致无法满足合规要求！

3 导航栏

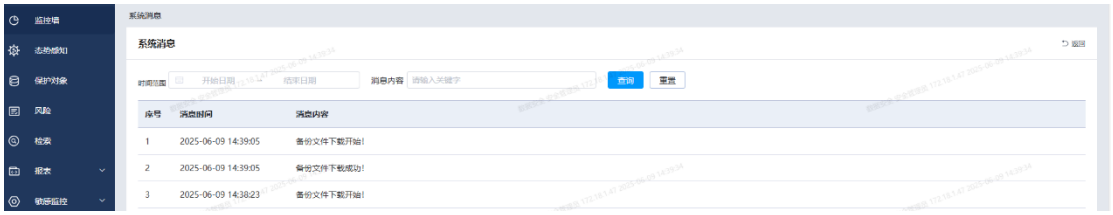
三大平台均有导航栏，用户可在导航栏中进行锁屏、修改密码、用户管理、退出等操作。

3.1 消息盒子

点击导航栏按钮，可以查看系统消息。

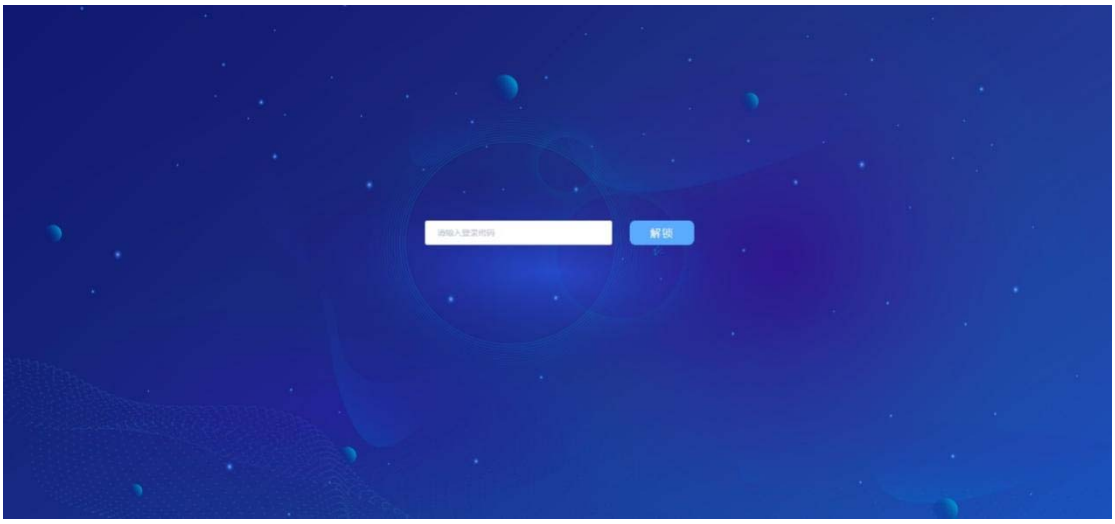


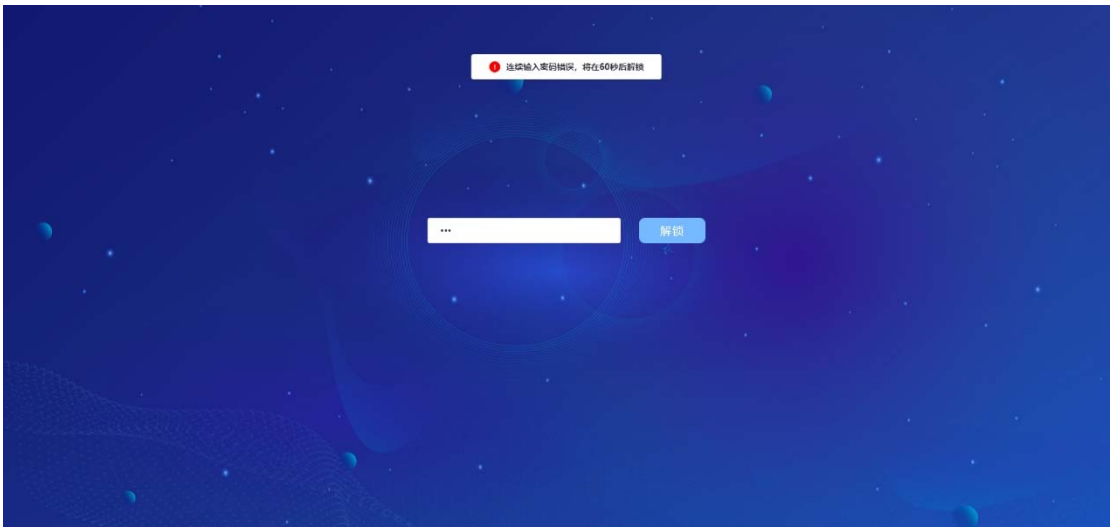
点击“查看所有的消息记录”进入所有产生的消息记录列表页面，可以根据时间范围以及关键字进行指定记录查找。



3.2 锁屏

为确保短暂离开客户机时信息不被泄露，可以采用锁屏方式，将屏幕锁定。点击导航栏，进入锁屏界面。解锁时，输入该平台的密码，连续输错时会锁定登录，具体允许登录密码错误次数和禁止登录时间配置详见【安全等级】。





3.3 帮助

对系统功能不熟悉的，可以点击导航栏 ，查看该系统的帮助手册，帮助用户快速了解平台的使用。

3.4 关于我们

在导航栏中点击 ，可以查看产品的基本信息，包括产品名称、产品型号、版本号。还可以通过以下方式联系我们提出问题及改进建议。

3.5 用户管理

点击导航栏用户图标，弹出列表展示个人信息，用户管理两个菜单。

注意：管理员用户才有用户管理功能，子用户没有。

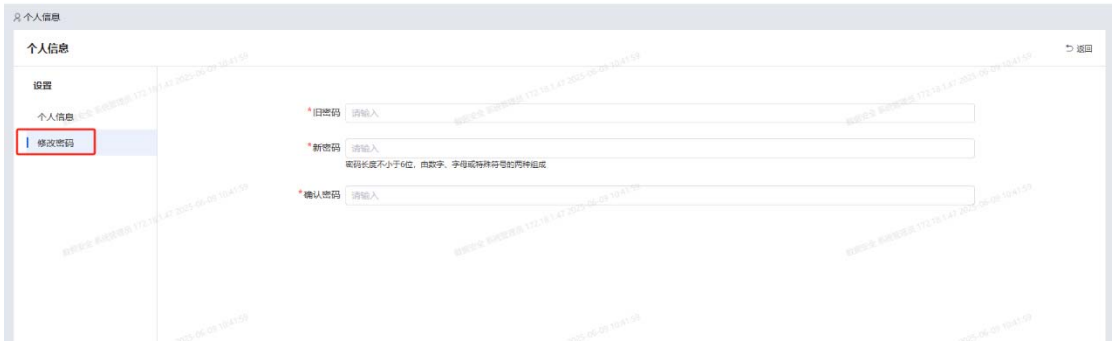
3.5.1. 个人信息

点击进入个人信息页面，能看到该用户的基本信息和拥有的功能权限。用户可在此界面编辑自己的个人信息。如果要将此用户作为告警或短信的接收者，需要配置邮件或者手机号码。

点击编辑按钮，对个人信息进行修改。每个平台的管理员可以对子用户的权限进行修改，详见【用户管理】。

3.5.2. 修改密码

点击修改密码，进入修改密码界面。用户需要输入正确的旧密码且新密码必须满足密码强度。



注意：新密码的要求可以在系统管理平台中的“系统管理-系统安全”进行修改。

3.5.3. 用户管理

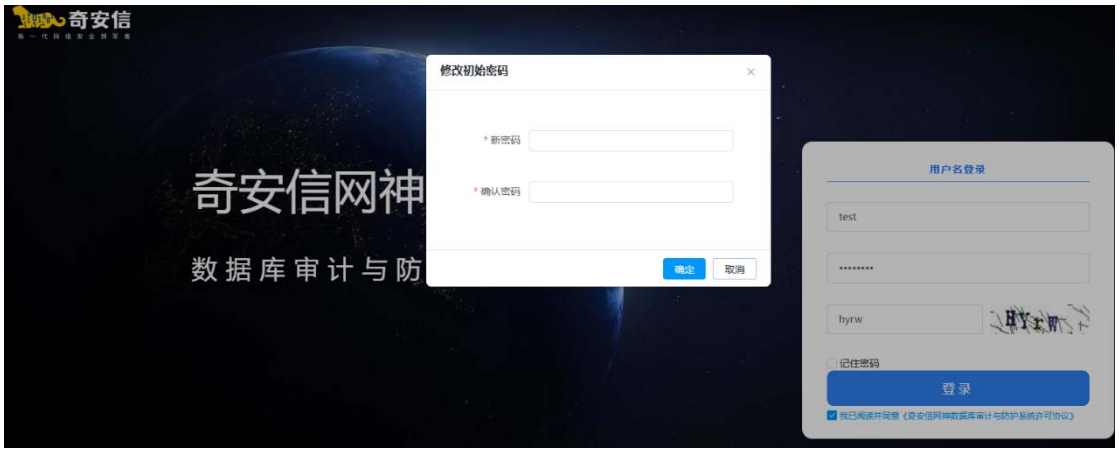
点击用户管理，进入用户管理界面，可以对所属平台的子用户进行添加修改删除等基本操作，并可对子用户进行权限的分配和修改。每个子用户只能拥有管理员分配的固定权限，无法越权操作。

1、添加用户：

添加新用户时，只能分配给新用户自己平台的权限，比如系统管理员只能创建具有部署方式、系统维护等权限的用户，可按需分配权限。点击页面添加按钮，弹出对话框，在对话框中依次输入新用户信息，示例如下：

点击保存后会提示给该用户分配的初始密码，如图：

打开浏览器，使用新用户及初始密码进行登录，首次登录需要修改密码。



修改密码并登录成功后，展示页面信息与分配的权限一致。

2、编辑用户

a. 修改：点击编辑按钮，弹出该子用户的信息框，可对用户的信息以及基本权限进行修改。

b. 重置密码：点击重置密码按钮，子用户忘记密码时可以向管理员申请重置密码，使用重置密码登录后再进行个人密码的修改。

c. 删除：点击更多中的删除按钮，删除对应的子用户，也可以勾选后点击删除按钮，此方式支持批量删除。

d. 查看详情：点击更多中的详情按钮，对子用户的基本信息进行查看。

e. 锁定状态：打开指定用户的锁定状态，该用户被锁定不能登陆。

锁定新创建的用户

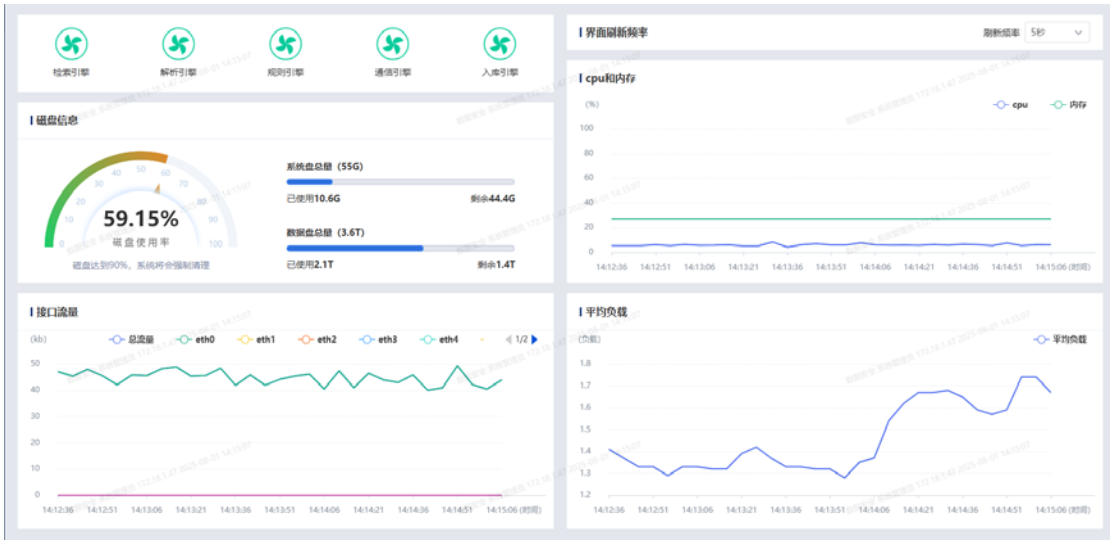
退出登录账号，使用新用户及密码进行登录，提示如下

注意：可以对在线用户进行修改、重置密码、删除和锁定操作。修改、重置密码、删除会在子用户进行下一步操作时自动返回登录页面，锁定会在下一次登录生效。

4 系统管理平台

4.1 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）



a. 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。如证书在有效期内出现异常可尝试在【设备管理】中重启引擎或者直接联系相关的技术人员。

b. 页面刷新频率：页面默认每 2 秒刷新一次，用户也可以根据需求手动选择刷新频率（2、3、5、10 秒），灵活控制数据更新速度。

c. 磁盘信息：显示当前磁盘使用率、已占用和剩余磁盘空间。
d. 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。
e. 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

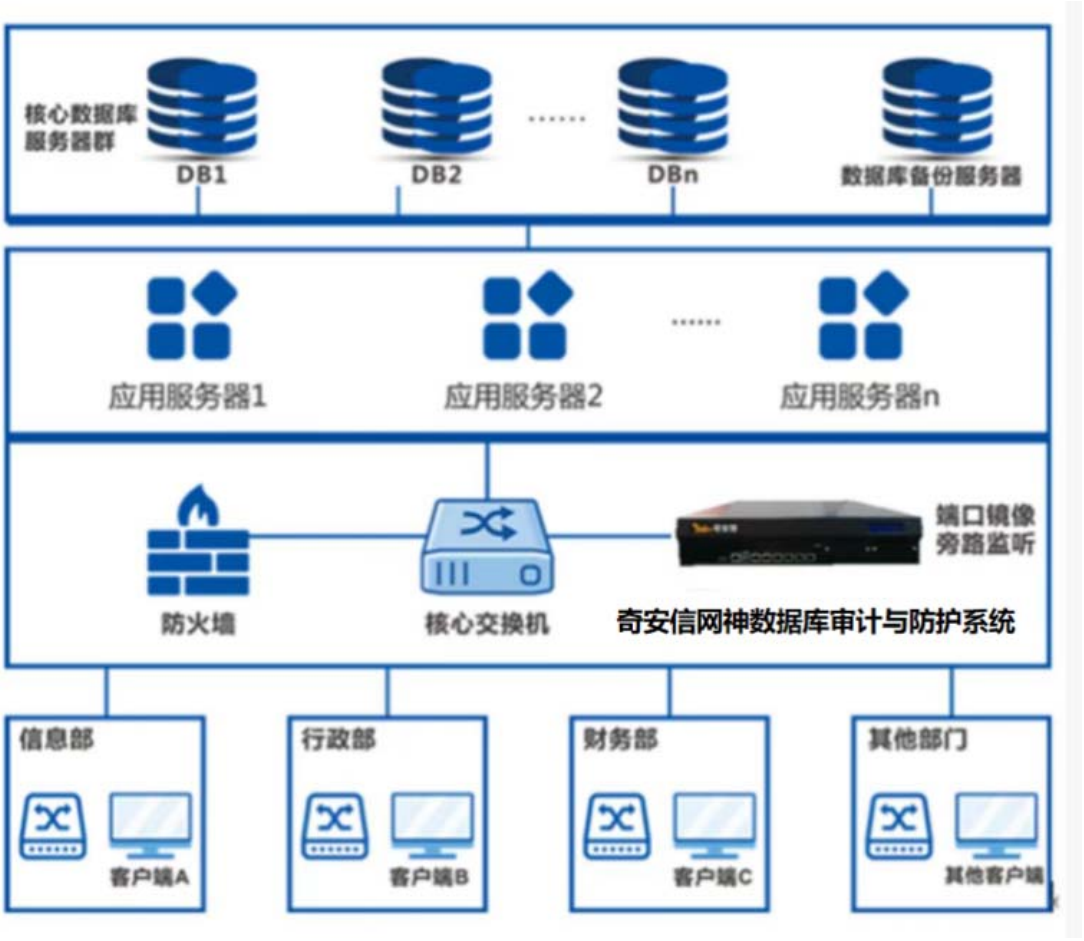
断该接口是否为审计口。

f. 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。

4.2 系统管理

4.2.1. 部署方式

采用旁路接入的方式，通过对交换机做镜像的方式来获取流量报文。在核心交换机上设置端口镜像模式或采用 TAP 分流监听模式，使安全审计引擎能够监听到所有用户通过交换机与数据库进行通讯的全部操作。如图所示为设备部署图：



部署方式页面支持查看及设置网口配置、管理口配置、部署方式。

4.2.1.1. 网口配置

通过网口配置查看设备的网口信息，包括数量、运行状态。启用某个网口并且该

网口有流量进入时，将对该网口流量数据进行审计；禁用之后，该网口的数据将不做审计。

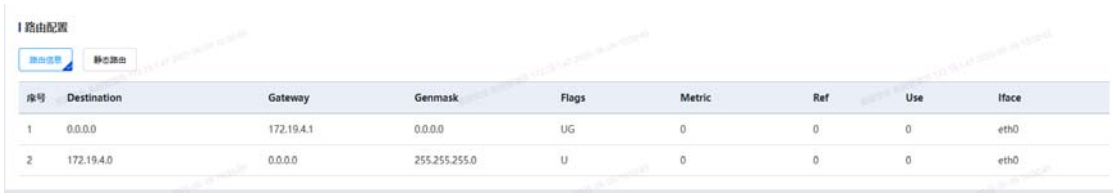
4.2.1.2. 管理口配置

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。

注意：修改并保存 ip 后，页面会提示需要重新登录。

4.2.1.3. 路由配置

静态路由是一种手动配置的路由方式，用于指定数据包到达特定目的地时应采用的路径。支持手动添加及展示静态路由信息。



目的 IP	输入目的 IP 地址或子网（如 192.168.1.0/24）。
下一跳转 IP 地址	输入下一跳路由器的 IP 地址（如 192.168.1.1）。
出接口	选择数据包离开本地设备时所使用的网口（如 eth0、eth1）。
描述	（可选）输入对该条路由规则的描述，便于识别（如前往内网服务器的路由）。

4.2.1.4. hosts 配置

数据库审计与防护系统通过 Kafka 向外部系统推送日志时，若 Kafka 服务通过域名提供访问，由于域名无法在内网环境中被解析，需配置域名映射，将目标域名指向内网 IP 地址，以确保跨网通信正常进行。

4.2.1.5. 部署方式

部署方式可共存也可只配置其中一种，默认旁路镜像，确定部署方式后需要点击下方保存按钮后才会生效。旁路镜像一般用于可做端口镜像的场景，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。如果两种方式都有共同的审计对象流量，会自动丢弃重复的审计流量。

4.2.1.5.1. 旁路镜像

设备接入审计对象所连接的交换机，通过端口镜像的方式将流量引到审计设备。该部署方式不会影响用户的正常业务。

4.2.1.5.2. Agent 引流

通过在审计对象设备上安装 agent，将所需要的流量导入审计设备。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。

注意：设备默认使用 9999 端口。支持在页面中更换成其他端口，更换后需要在设备后台开放新的端口。

4.2.1.6. 节点配置

通过节点配置部署单台审计环境或多台审计环境。默认单机，即只接入一台审计设备进行审计操作。中心节点和子节点配置用于部署多台审计环境，即接入多台审计设备，其中一台设备作为中心节点，其他设备作为子节点，分别进行审计操作。在子节点上可选择不同数据类型的审计记录上传到中心节点，对于上传到中心节点的数据，可选择在子节点上保存或不保存。

4.2.1.6.1. 单机

只接入一台审计设备进行审计操作。

4.2.1.6.2. 中心节点

接入多台审计设备，其中一台设备作为中心节点。

4.2.1.6.3. 子节点

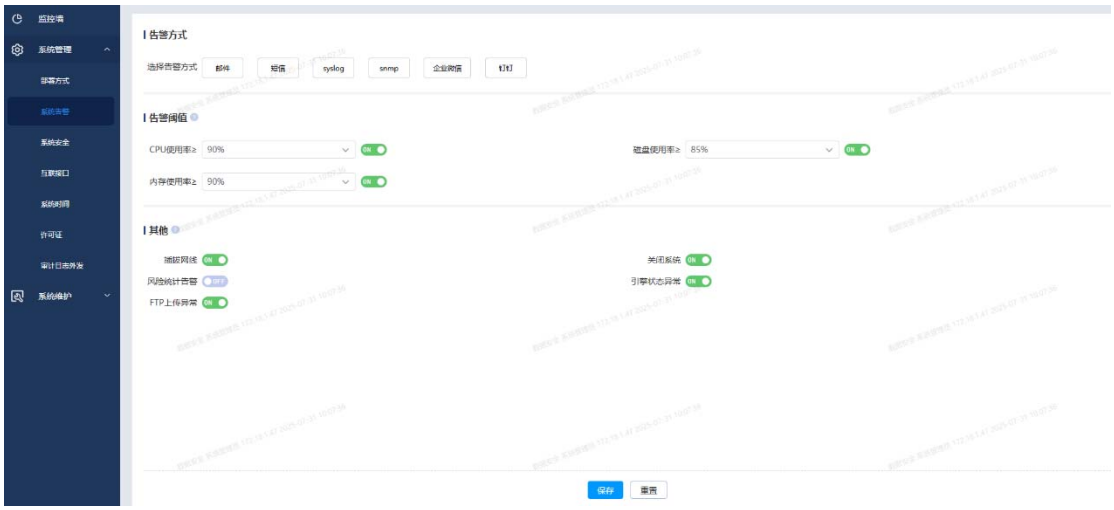
接入多台审计设备，除中心节点设备外，其他设备作为子节点。选择设备类型为子节点，输入子节点名称、负责人、电话、地区，选择上传数据类型，选择是否保存数据，输入中心节点 IP。进行测试连接，检测子节点和中心节点是否网络互通。

配置项	描述
子节点名称	当前子节点名称
负责人	当前子节点负责人
电话	当前子节点负责人电话
地区	当前子节点所属地区
上传数据类型	当前子节点需要上传到中心节点的风险数据类型，可多选
是否保存数据	是：当前子节点保存上传的数据类型；否：当前子节点不保存上传的数据类型。
中心节点 IP	当前子节点对接的中心节点 IP

4.2.2. 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【互联接口】。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，配置方式详见【用户管理】，更改配置后需要点击下方的保存按钮才会生效。



4.2.3. 系统安全

4.2.3.1. 安全等级

安全等级默认内置高中低三种类型，也可以根据需要自定义选择不同的安全条件，更改配置后点击下方保存按钮生效。

历史密码记录数：为增强账户安全性，新密码不能与最近使用的 N 次旧密码相同（N）。例如，若设置为“3”，则新密码不能与最近三次修改过的密码重复。

密码过期时间：选项为 7 天、14 天、21 天、28 天、3 月、6 月、12 月。选择具体值 X 天，包括当前时间 X 天后，密码过期，此时打开登录界面，输入用户名密码，页面会跳转到强行修改密码界面，必须使用新密码才可以继续登录。

密码复杂度：支持分别选择高、中、低进行配置。修改密码时，新密码必须要满足设置的复杂度才可修改成功。

高：密码长度不小于 15 位，需要由数字、大写字母、小写字母或其他特殊符号当中的三种以上组成。

中：密码长度不小于 12 位，需要由数字、大写字母、小写字母或其他特殊符号当中的两种组成。

低：密码长度不小于 8 位，需要由数字、大写字母、小写字母或其他特殊符号当中的一种组成。

连续失败登陆：可选择 2 次、3 次、5 次。连续登录选定的次数后，会禁止登录。禁止登录的时长根据选择的锁定时间进行限制。

锁定：选项为 60 秒、180 秒、300 秒、600 秒、1800 秒、3600 秒。禁止登录后需要等选定时间秒数后才能登录成功。

界面：选项为 300 秒、600 秒、1800 秒、3600 秒。判断界面在选定时间内没有操作就会超时退出。

连接方式：当前仅支持 HTTPS 方式访问。

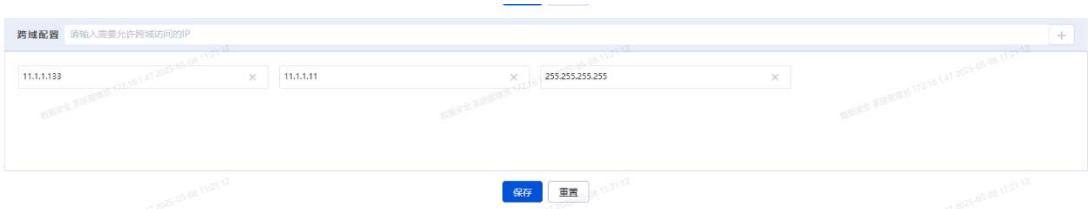
账号同时登录：关闭时单账号仅允许一个在线会话，新登录将强制登出前一个 开启时需设定“同时在线数”，达到上限后禁止新登录

同时在线数：限制单个账号的最大同时在线数量,限制范围 1-500

登录并发会话数：限制系统所有用户同时登录会话的最大总数，限制范围 1-500

双因子登录：默认为关闭状态。修改为开启状态时，需要确保已配置了短信猫或短信服务器，且每个用户都已配置了手机号码。修改为开启状态后，登录页面需要填写正确的短信验证码后才能登录成功。

4.2.3.2. 跨域配置



在不同网络域之间进行通信时，往往需要进行跨域配置，明确允许特定 IP 地址进行访问，以确保合法的网络通信顺畅进行。

在跨域配置输入框中输入需要允许访问的 IP 地址,点击右边的 + 号完成配置。

4.2.3.3. 黑白名单

为了控制具体的不同 IP 地址的登录权限，用户可采用黑白名单的方式进行访问限制。即使密码被泄露，但 PC 端 IP 无登录权限也无法使用，双层保障信息不会被泄露。用户可配置平台所有的管理员子用户使用的 PC 端 IP 为白名单。配置白名单后，将只允许白名单中的 IP 地址访问，配置黑名单后，将不允许黑名单中的 IP 地址访问系统。例如配置 172.18.1.47 为白名单，172.18.1.7 为黑名单，则 172.18.1.47 可以访问，172.18.1.7 不能访问。

注意：以黑名单优先，比如黑名单设置 1.1.1.1-1.1.1.10，白名单设置 1.1.1.2，此时 1.1.1.2 同时设置为黑名单和白名单，以黑名单优先，所以 1.1.1.2 不允许登录。

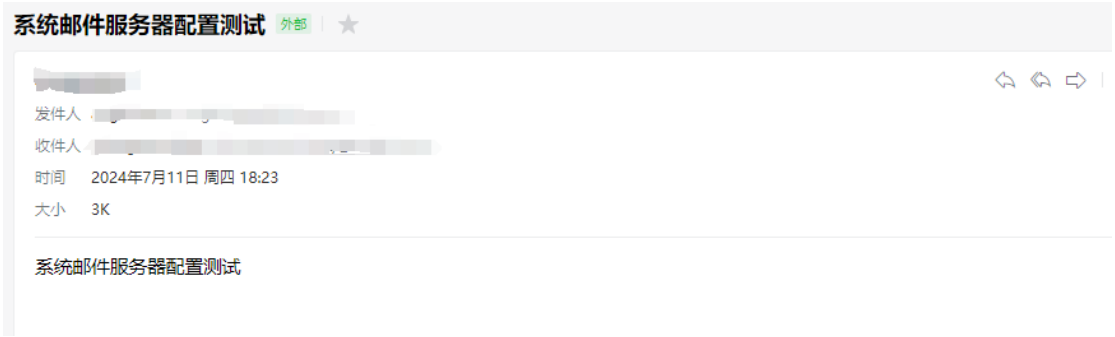
4.2.4. 互联接口

该模块主要是用来配置与设备通信的外部服务器信息，需要保证设备与各个服务之间通信正常。

4.2.4.1. 邮件服务器

邮件服务器主要是用来配置邮件告警方式的发件人信息。支持配置备用邮件服务器，当主邮件服务器因为其他因素不可使用时，自动采用备用邮件服务器，保证告警信息能够及时发送。以主邮件服务器为例，填写局域网的邮件服务器配置：

配置后可点击“测试”按钮，测试该配置是否可用，前台界面会展示测试成功，且测试邮箱还能收到邮件。



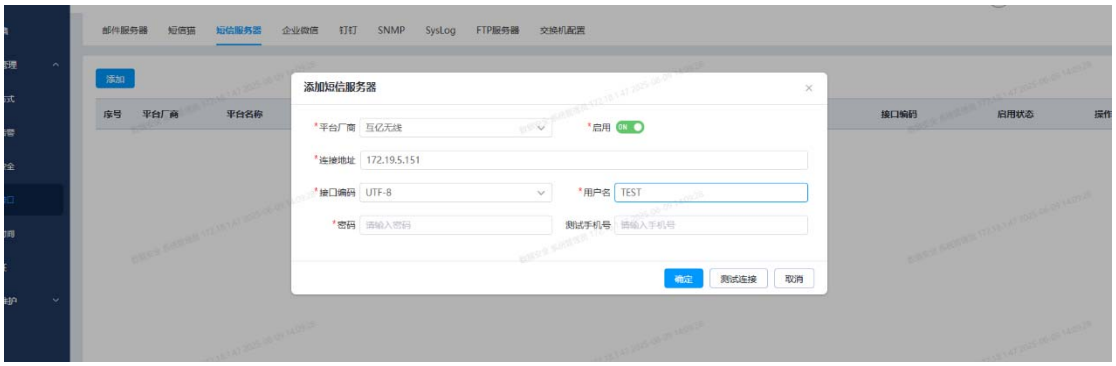
4.2.4.2. 短信猫

配置发送短信的短信猫信息。当告警方式选择短信，或开启多因子认证时，可以使用短信猫发送短信。

短信猫接入的注意事项：将短信猫的天线接入，确保天线方向垂直向上；确保短信猫和目标计算机或设备的硬件规格兼容；确保 SIM 卡无欠费，能正常通信和收发短消息。

4.2.4.3. 短信服务器

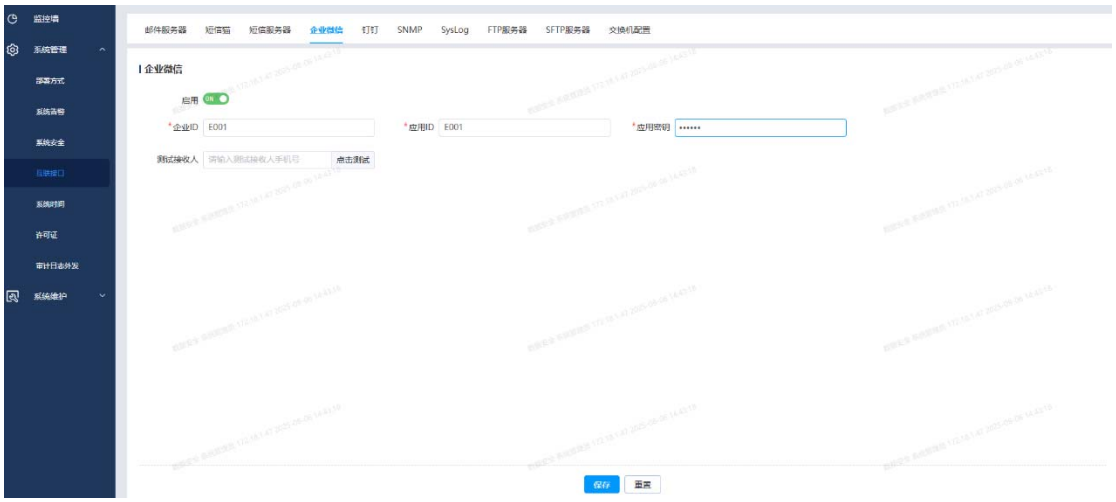
配置发送短信的短信平台信息。支持的平台厂商包括互亿无线、梦网平台及通过自定义方式添加的平台厂商。点击页面左上角添加，添加短信服务器信息。当告警方式选择短信，或开启多因子认证时，可以使用短信服务器发送短信。点击添加按钮，进入添加页面，如下图：



注意：短信猫和短信服务器只能同时开启其中一个。

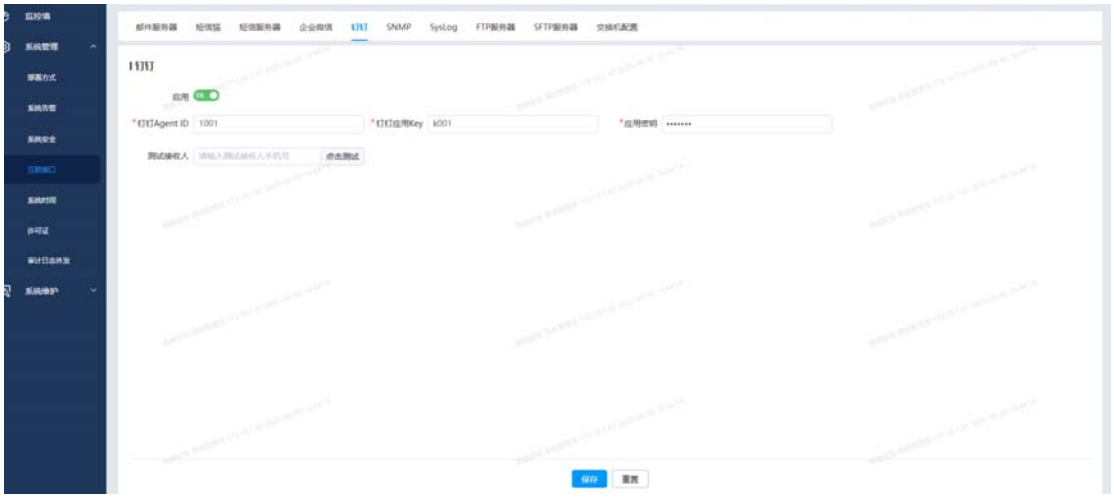
4.2.4.4. 企业微信

配置企业微信接收方信息。当告警方式选择企业微信时，会将告警信息发给配置的企业微信。详细对接流程请参见【附录-企业微信对接流程】。



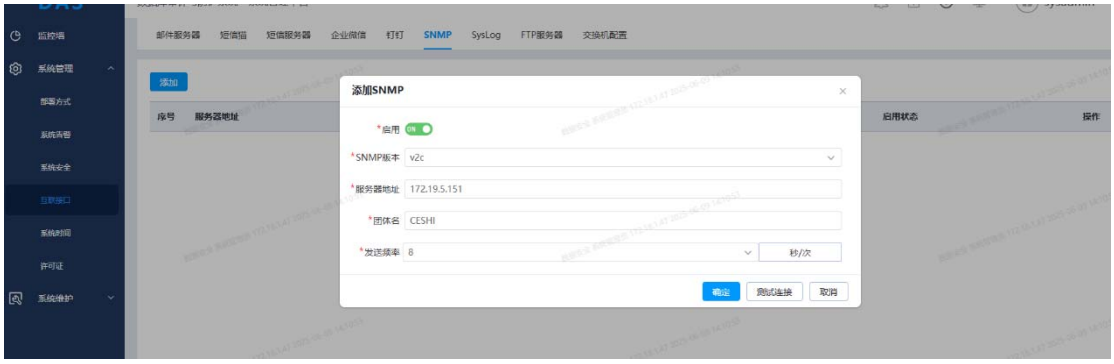
4.2.4.5. 钉钉

配置钉钉接收方信息。当告警方式选择钉钉时，会将告警信息发给配置的钉钉服务器。详细对接流程请参见【附录-钉钉流程对接】。



4.2.4.6. SNMP

配置 SNMP 接收方信息。当告警方式选择 SNMP 时，会将告警信息发给配置的 SNMP 服务器。点击添加按钮，进入添加页面，如下图：



注意：需保证接收方的 SNMP 端口为 161。

4.2.4.7. SYSLOG

配置 SYSLOG 信息。当告警方式选择 SYSLOG 时，会将告警内容发送到配置的 syslog 服务器。

可自定义端口号，需要保证与接收端 SYSLOG 端口号一致，默认 514。填写完后，保证接收方的 SYSLOG 服务是打开的，点击测试确认 SYSLOG 服务器的连通性。

注意：消息等级是向上兼容的，如选择中风险，则支持中、高风险告警。

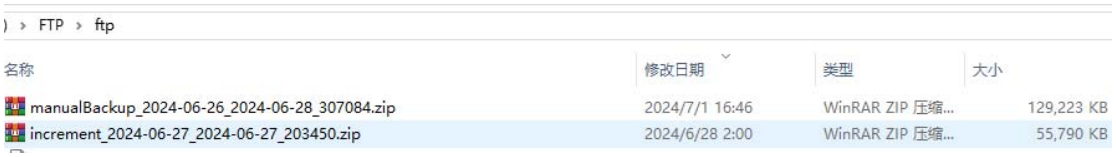
4.2.4.8. FTP 服务器

配置接收备份文件的 FTP 服务器。数据备份时选择对应的 FTP 服务器后，文件将会自动上传至配置的 FTP 服务器，

添加完成后点击“测试链接”确认 FTP 服务器的连通性，示例如下：

FTP 服务器主要用于数据维护-数据备份，以手动备份为例，手动备份审计日志、配置信息，上传方式选择 FTP。

备份完成后查看 ftptest 的存放路径将能看到备份的文件。



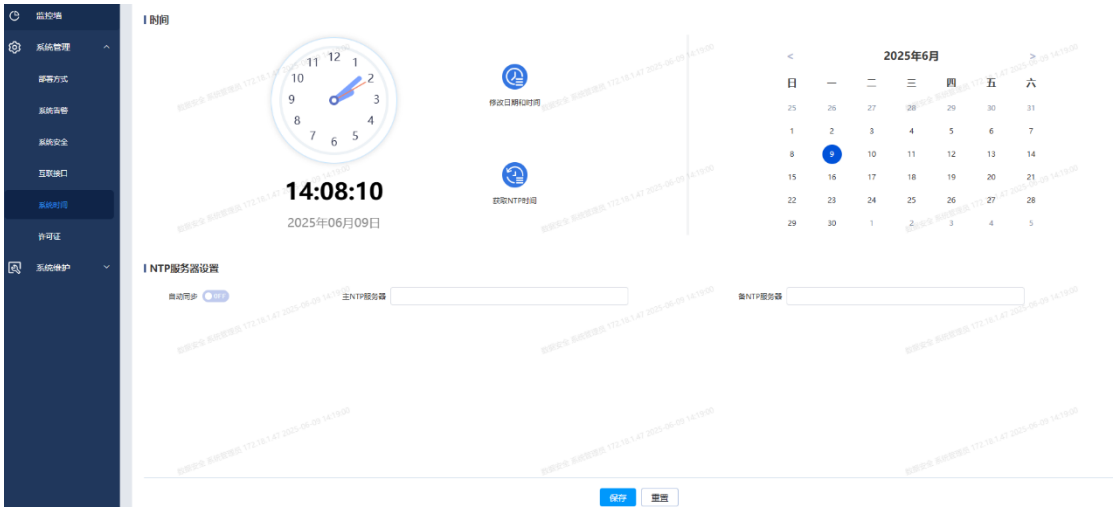
4.2.4.9. 交换机配置

PC 端到数据库的数据经过交换机时，设备获取到的 MAC 不是真实的 MAC，导致审计日志记录的客户端 MAC 地址不正确。可以通过交换机的配置，使审计记录获取交换机路由表中存放的实际客户端 MAC 地址。交换机相关信息可以网络管理员获取。

注意：需要保证所填写的交换机开启了 SNMP 协议，OID 默认为 1.3.6.1.2.1.4.22.1.2。

4.2.5. 系统时间

页面展示系统当前时间及 NTP 服务器设置，可手动修改或获取 NTP 时间。当设备因为因设备长时间断电等原因导致系统时间与正常时间不一致，会导致审计日志以及各种日志记录的时间不准确，需要及时调整系统时间。



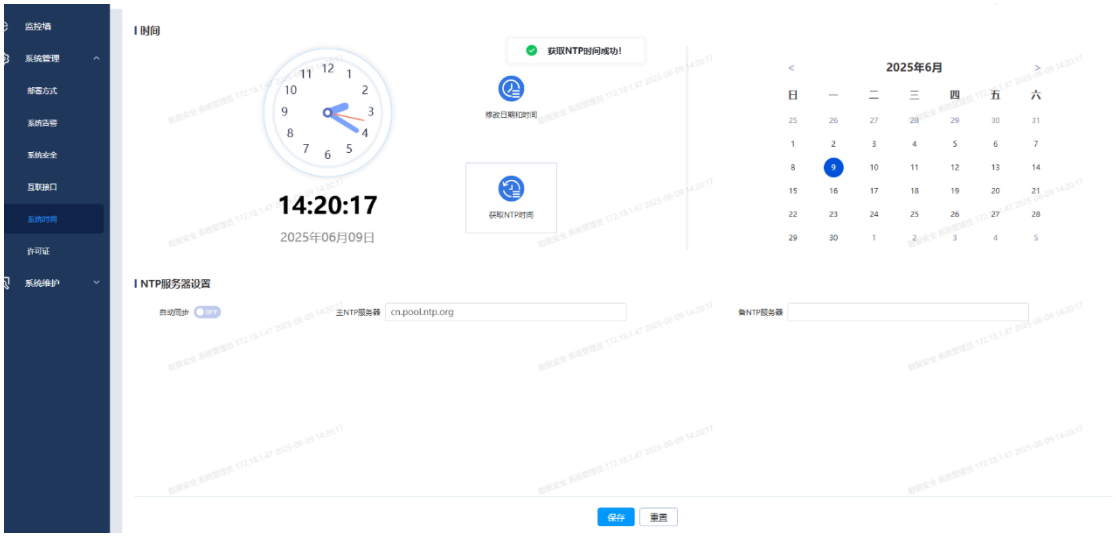
1、手动修改

点击界面上修改日期和时间，输入当前正确的日期和时间，点击修改。

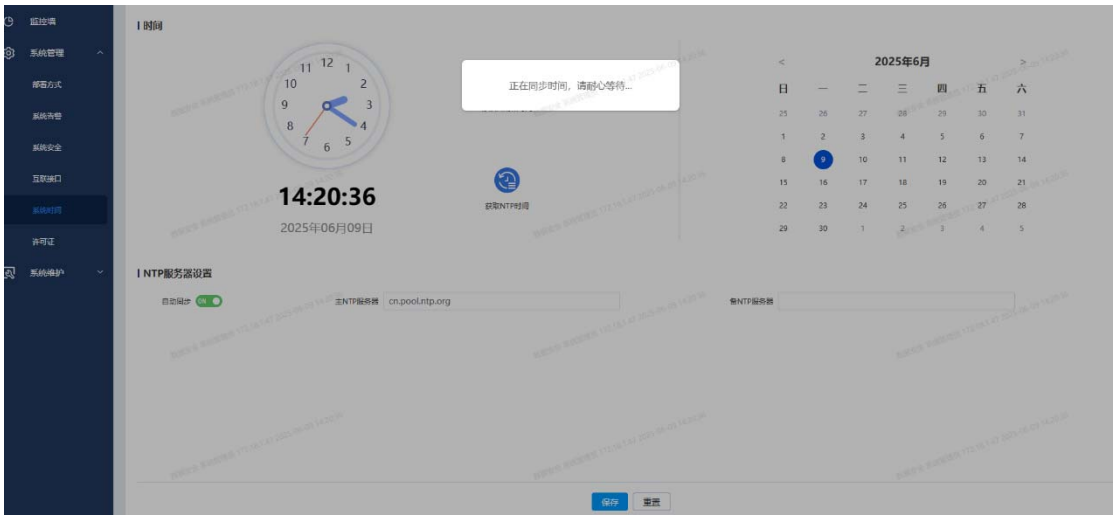
2、获取 NTP 时间

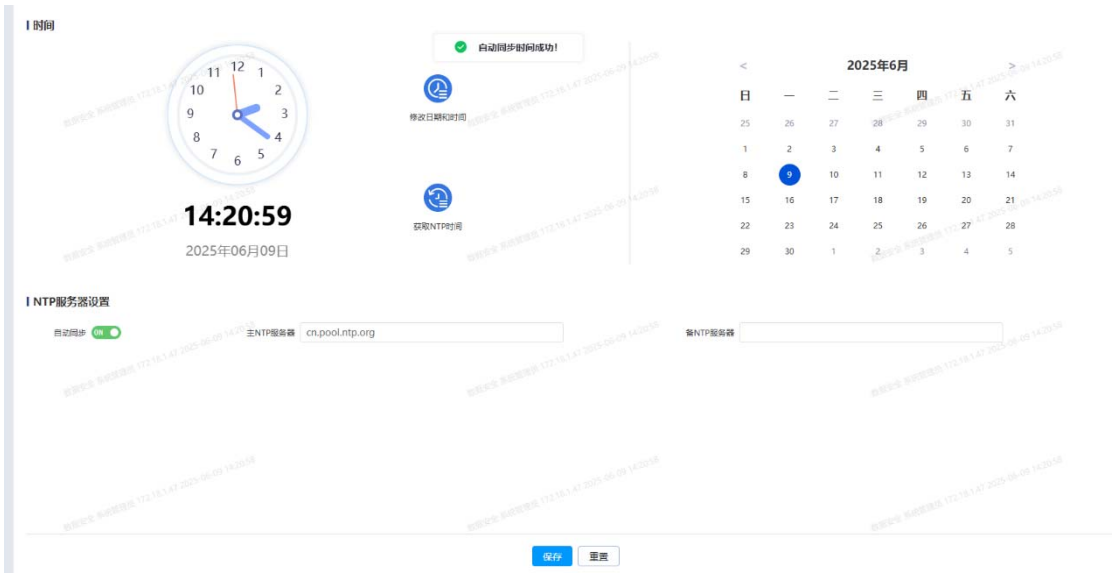
配置 NTP 服务器，支持主备 NTP 服务器配置。如填写主 NTP 服务器：cn.pool.ntp.org，点击保存按钮保存可用的 NTP 服务器信息。填写的 NTP 服务器信息需要保证审计设备可以正常连接，无法连接成功的 NTP 服务器将不能保存。

配置成功后，可直接点击获取 NTP 时间更新时间。



打开自动同步开关，系统会自动同步时间。





4.2.6. 许可证

可以下载授权机器码，在生成证书后上传授权文件。上传授权文件后，检查【监控墙】引擎模块及其他功能是否都正常。

支持证书有效期及维保信息有效期展示，过期前 30 天开始每天会有过期提醒。

注意检查返回的证书文件编码是否与发送的一致，例如：

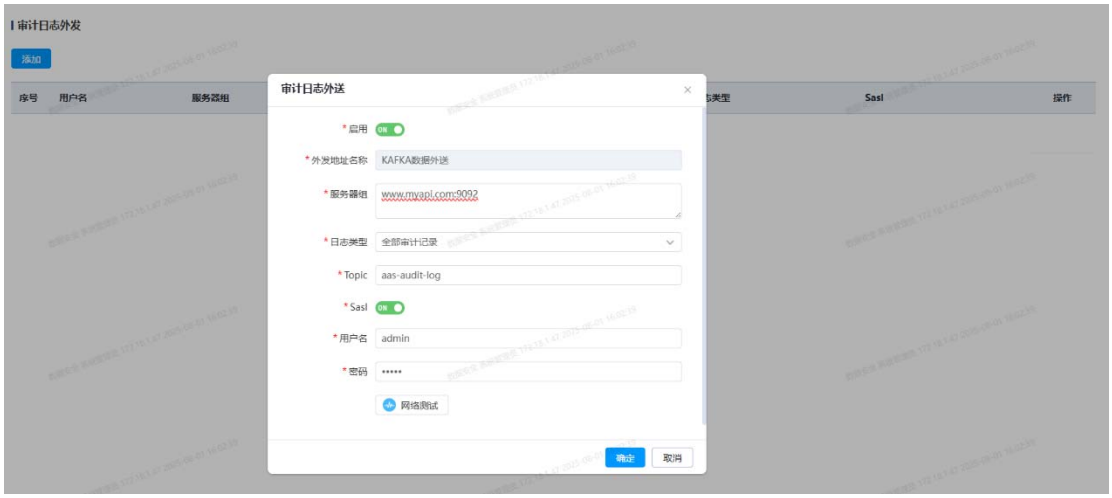
下载的机器码：clientInfoFileB7E84C4396832168.info

返回的证书文件：B7E84C4396832168_audit.lic

注意：上传证书时先确保系统时间正确，系统时间不正确时上传证书会导致证书校验不通过。

4.2.7. 审计日志外发

审计日志外发，这里可以推送全部审计记录、非风险审计记录、风险审计记录。服务器组支持域名或 IP，多个地址逗号隔开，点击确认前进行网络测试，保证连通性。



注意：服务器组为域名时，需先在【部署方式-hosts 配置】页面配置映射关系。

4.3 系统维护

4.3.1. 系统维护

4.3.1.1. 设备管理

支持在设备管理中直接对设备进行操作，包括重启系统、关闭系统、恢复出厂设置、清除业务数据、ssh 协议开关控制等操作，同时提供审计引擎的重启及关闭功能。

重启系统、关闭系统、恢复出厂设置、清除业务数据操作需要输入登录密码，该部分功能会影响审计业务的运行，需要谨慎操作。

注意：恢复出厂设置以及清理业务数据需保证所有引擎正常的情况才能操作成功。

4.3.1.2. SSL 证书管理

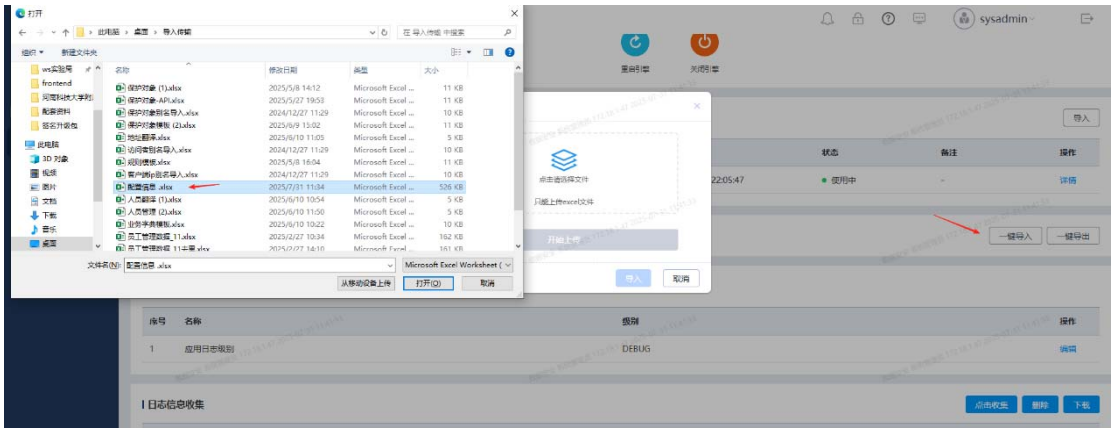
提供便捷的 JKS 证书导入功能，系统自动完成证书有效期校验，并实时显示颁发时间与截止时间。证书状态“使用中”清晰标识，便于运维人员及时监控证书生命周期，确保服务安全不间断运行态。

4.3.1.3. 配置信息管理

此功能支持一键导入和导出配置信息。

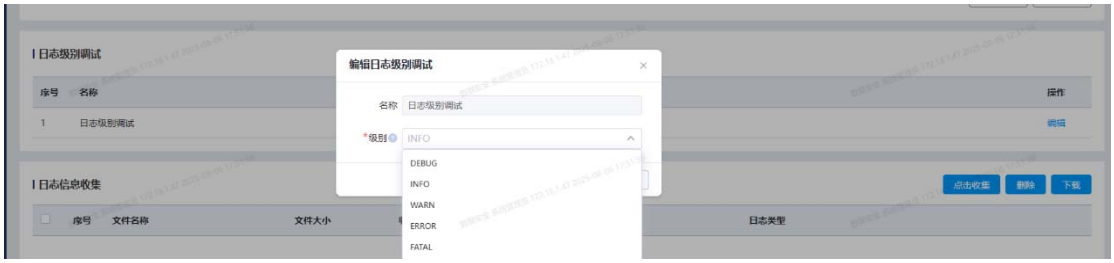
一键导出将收集配置信息并通过 Excel 文件导出，导出的配置信息包括：保护对象、策略管理、对象管理以及各个配置之间的引用关系。

一键导入功能支持用户对 Excel 文件中的配置信息进行导入。



4.3.1.4. 日志级别调试

系统提供动态日志级别配置功能，支持 DEBUG、INFO、WARN、ERROR、FATAL 等级别设置。用户可通过点击“编辑”按钮进行调整，配置保存后立即生效，无需服务重启，显著提升运维效率和问题排查速度。



4.3.1.5. 日志信息收集

通过点击“点击收集”按钮，统计目前关于各个日志的大小情况。

注意：前台界面不支持超过 5GB 的日志收集，如超过则需要联系相关的技术人员进行日志的获取。

勾选需要的日志，点击“确定。

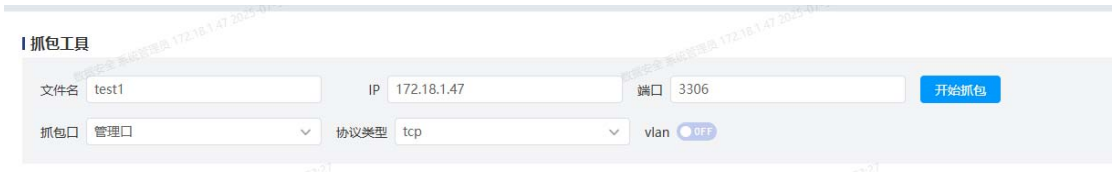
收集成功后可在列表中查看收集的文件，列表展示文件名称、文件大小、收集时间、日志类型。勾选文件，通过右上方的“删除”“下载”按钮对文件进行操作，支持批量下载和删除。

注意：由于收集的文件是压缩文件，所以文件大小与实际收集不一致。具体大小可通过解压后查看，且收集过程中还会产生新的日志，最终生成的日志文件大小可能大于收集时选择的文件大小。

4.3.1.6. 抓包工具

当系统功能出现问题时，用户可以通过抓包工具获取网络上传输的数据，将其提供给相关技术人员进行分析。

例如抓取 IP 是 172.18.1.129，端口是 3306 且经过管理口的 tcp 协议数据，配置如下：



配置完成后，点击开始抓包，一段时间后点击结束抓包，抓包文件如下：

选中抓包文件，点击下载，可以将抓包文件下载到本地。

4.3.2. 系统升级

支持用户在前台界面进行版本、补丁、漏洞补丁等多种类型的升级及回退，升级记录列表可以查看所有的升级记录。升级出现异常时，可以在页面下载升级日志文件，将日志发送给相关的技术人员查看失败原因。

大版本之间升级选择系统版本升级，同一版本内的更新迭代选择补丁版本升级，组件漏洞选择漏洞补丁版本升级。

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。

4.3.3. 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，页面支持查看的日志类型包括系统日志、异常日志、通信日志、设备日志、版本更新日志、其他日志。

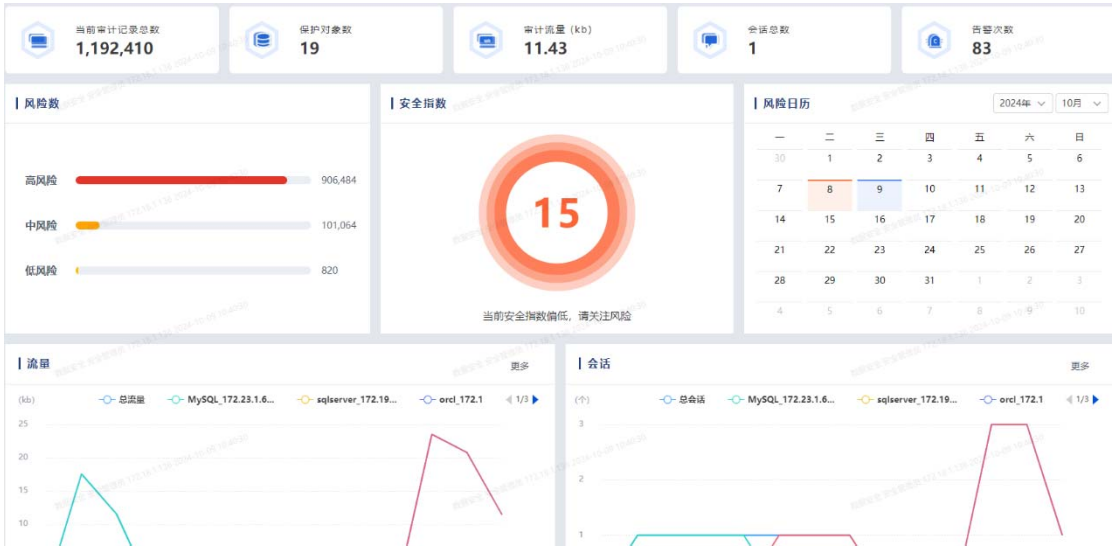
支持对指定条件的系统日志进行查询，支持对系统日志的导出。

DAS
数据库审计与防护系统 - 系统管理平台
sysadmin
监控端
系统管理
系统维护
系统维护
系统升级
系统日志
日志事件等级
42
事件总数
致命告警 14 33.33%
一般告警 16 38.10%
一般事件 12 28.57%
日志统计
数量（个）
18
15
12
9
6
3
0
2
3
10
9
版本更新日志
异常日志
系统日志
设备日志
通信日志
日志信息收集
日志类型
事件等级
时间范围
2025-06-06 14:33 ~ 2025-06-09 14:33
查询
重置
导出
时间
日志类型
事件等级
结果
描述
2025-06-09 14:28:07
异常日志
致命告警
成功
重启引擎成功, 重启时间:2025-06-09 14:28:07
2025-06-09 14:27:07
异常日志
致命告警
成功
重启引擎成功, 重启时间:2025-06-09 14:27:07

5 安全管理平台

5.1 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情况，及时把控风险的数量。



a、当前审计记录总数，展示当前设备审计到的所有记录。

b、当前保护对象个数，展示保护对象页面状态为开启的保护对象个数。

c、审计流量，展示当前所有保护对象流量的总和，包括通过旁路镜像和 agent 部署方式发到审计设备的流量，5 秒更新一次。

d、会话总数，展示所有保护对象的实时会话总和，包括通过旁路镜像和 agent 部署方式进来的会话。不同的客户端 IP 或客户端端口统计为一个会话，以此累加计算实时会话总数。

e、告警次数，展示当前设备已发送的告警总数。配置告警策略并关联到保护对象中，达到告警条件时将发送告警，告警次数增加一次。

f、风险数，展示当前设备审计风险总数及高中低风险数量。

g、安全指数，是通过各类风险数据的数量计算的值，初始状态默认为 100，根据风险情况进行计算得出。计算公式如下：

安全指数 = 100 - 风险指数。计算后去除小数部分取整即为最后的安全指数。

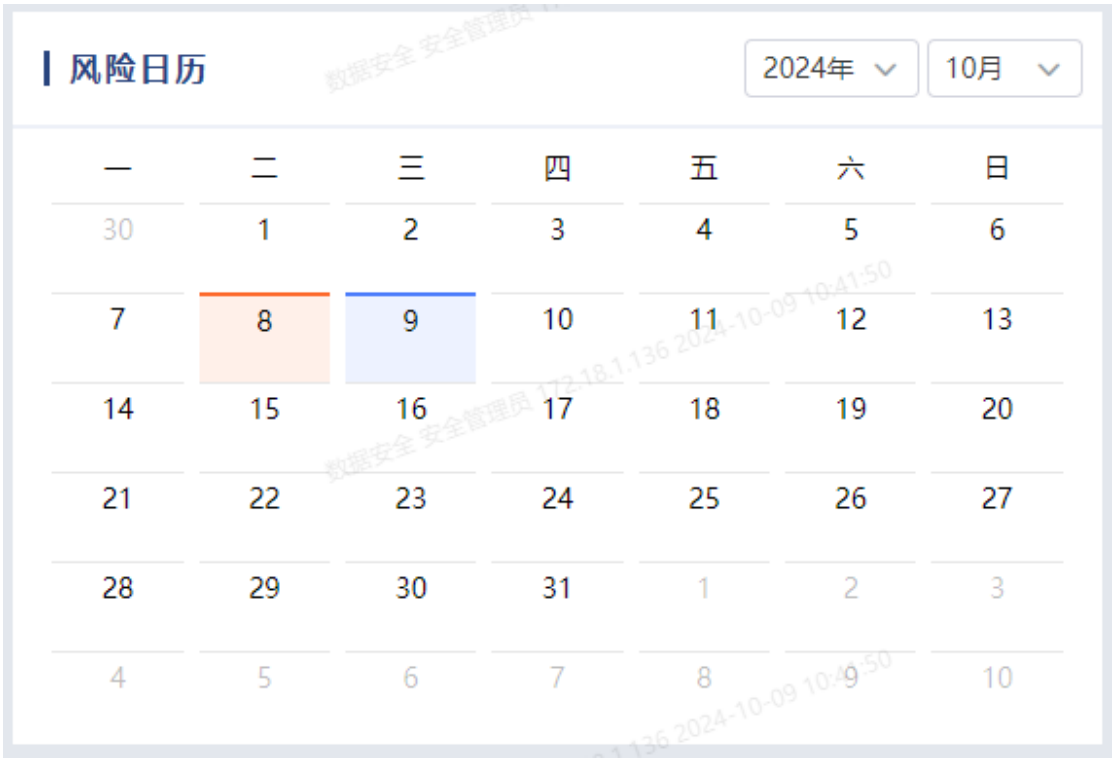
风险指数 = 高风险指数 + 中风险指数 + 低风险指数。

高风险指数=(高风险数 / 记录总数) * 100 * 1。取值范围为 10-100，计算值大于 0 且小于 10 时取值 10，大于 10 时取计算值。

中风险指数:(中风险数 / 记录总数) * 100 * 0.5。取值范围为 5-100，计算值大于 0 且小于 5 时取值为 5，大于 5 时取计算值。

低风险指数:(低风险数 / 记录总数) * 100 * 0.2。取值范围为 3-100，计算值大于 0 且小于 3 时取值为 3，大于 3 时取计算值。

h、风险日历，根据日历展示每天的风险情况。当某一天存在高风险时显示为红色背景，中风险显示橙色背景，低风险显示黄色背景，系统当天没有风险事件时背景显示蓝色背景。用户可通过该日历查看每一天的风险情况。

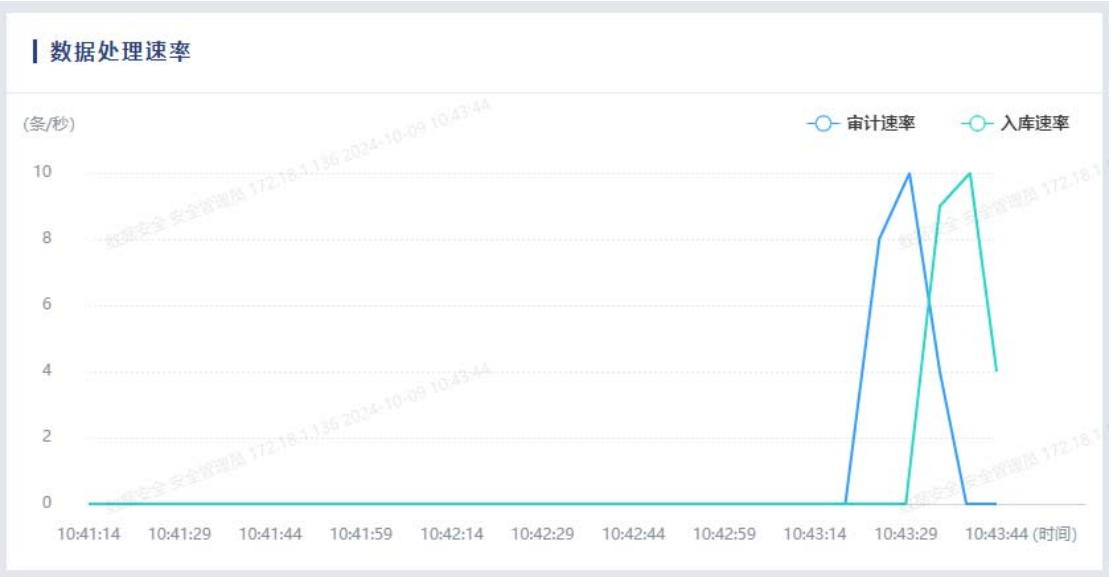


i、流量图展示最近各保护对象流量情况，保护对象较多时可使用右上角全屏按钮放大

展示。

j、会话图展示最近各保护对象会话情况，保护对象较多时可使用右上角全屏按钮放大展示。

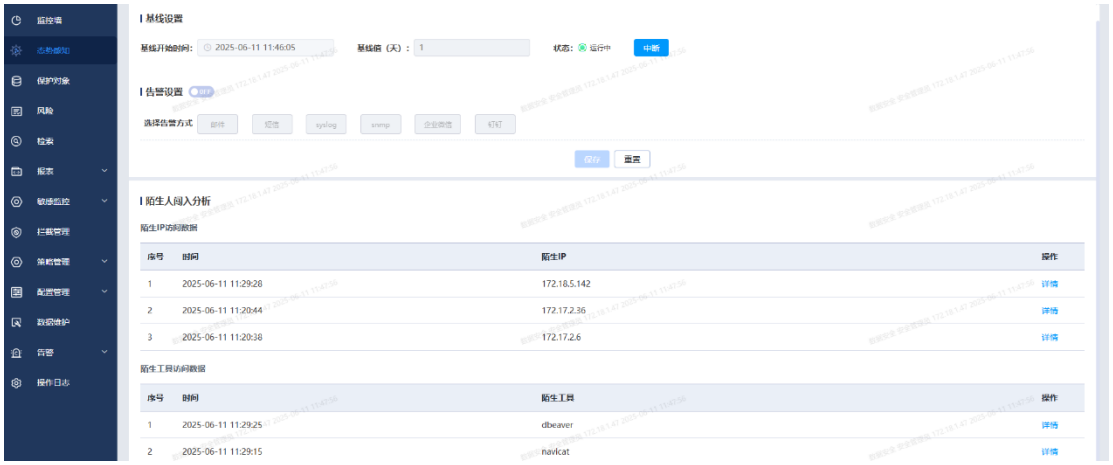
k、数据处理速率，展示最近的审计速率以及入库速率情况。



1、显示触发的规则名称及触发的记录数。

5.2 态势感知

对访问数据库的客户端 IP 以及访问工具进行识别，针对在设置时间范围内的 ip 以及客户端访问工具进行学习，对设置时间范围外的范围的陌生 ip 以及客户端访问工具进行记录及展示。



1、基线设置

配置基线设置，用于学习配置时间范围内的客户端 ip 以及数据库访问工具，学习时间内的访问不会生成陌生人记录。

字段填写说明：

基线开始时间	开始学习时间，基线开始时间不能小于当前时间，系统时间到达设置的开始时间时，自动开始学习
基线值	学习的时长，以天为单位，取值范围：1-266 的正整数
状态	包含三种状态：未运行、运行中、已完成
开始/中断按钮	开始任务、中断任务

2、告警设置

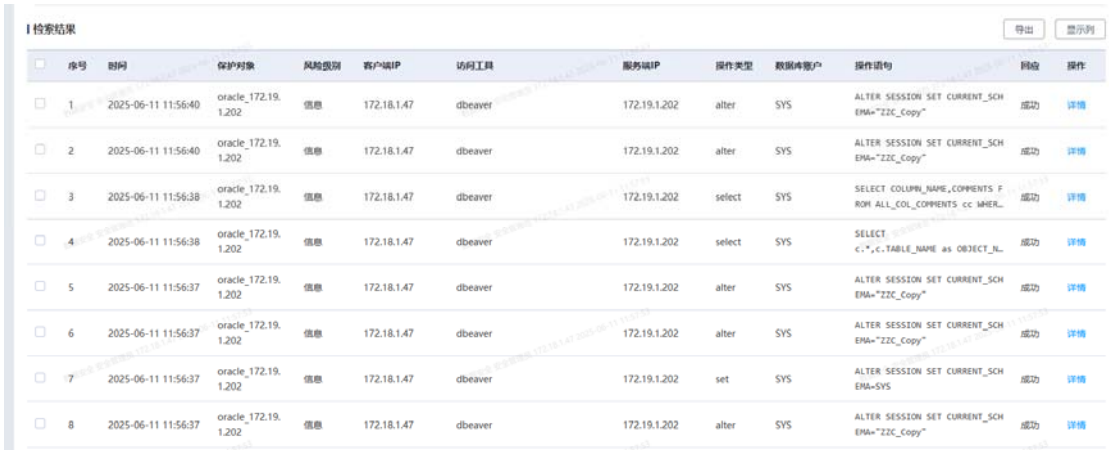
字段填写说明：

状态	启用告警：ON，关闭告警：OFF
告警方式	邮件、短信、syslog、snmp、企业微信、钉钉六种方式的组合，需要提取在【互联接口】中配置服务器信息
告警接收人	任意选择系统用户中的一个或多个

3、陌生人闯入分析

陌生 IP 访问数据：基线学习时间结束后访问保护对象的陌生 IP，点击“详情”按钮，可以查看该 IP 的所有审计记录。

陌生工具访问数据：基线学习时间结束后访问保护对象的陌生工具，点击“详情”按钮，可以查看该工具的所有审计记录。



5.3 保护对象

配置需要保护的数据库信息，支持配置 MySQL、Oracle、sqlserver、PostgreSQL、Caché、hive、hbase、MongoDB、http、达梦、人大金仓、阿里云_MySQL 等数据库类型。

5.3.1. 保护对象配置

5.3.1.1. 添加

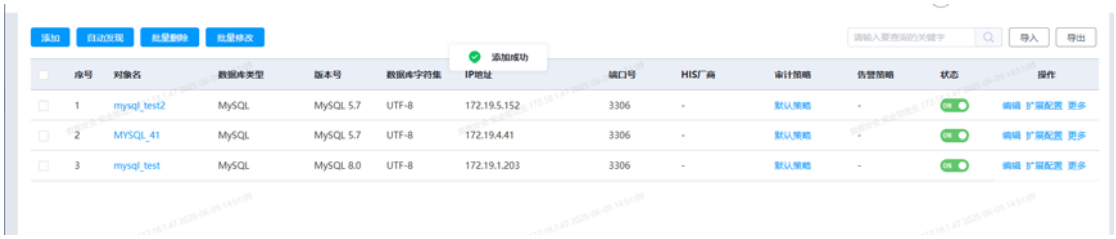
点击“添加”按钮，输入保护对象信息，点击保存按钮完成保护对象的添加。

字段填写说明：

对象名	输入保护对象名称，50 个字符以内，不包含< > ^ ″ 空格。
状态	默认为 ON，开启保护对象审计。状态设置为 OFF 后，保护对象不再进行审计。
敏感防护	默认为 OFF，不开启敏感防护。状态设置为 ON 后，操作保护对象的敏感数据会匹配敏感规则。
数据库类型	选择要添加的数据库类型，如 Oracle。
版本号	选择数据库版本号，如 Oracle 11g。

IP 地址	输入需要审计的数据库 IP 地址，支持配置单个 IP 地址或 IP 地址段。其中单个 IP 支持配置 IPV4 或 IPV6，IP 地址段只支持 IPV4，如 172.23.1.23-172.23.1.29，不支持 IPV6 地址段。
端口号	输入需要审计的数据库端口。支持输入单个或多个端口，输入多个端口需要使用‘|’符号隔开,如 3300|3301|3306。
数据库字符集	选择需要审计的数据库的编码字符集。
HIS 产商	对保护对象按照不同的 HIS 厂商进行审计，HIS 厂商版本号可以根据实际版本号输入，或在已有版本号中选择。
审计策略	输入需要审计的数据库端口。支持输入单个或多个端口，输入多个端口需要使用‘|’符号隔开,如 3300|3301|3306。
告警状态	默认为 OFF。设置为 ON 后，必须选择告警策略才能保存配置。当访问该保护对象的操作触发了审计策略中的规则，且触发的规则风险级别与告警策略配置的级别一致时，将会通过配置的告警策略发送告警信息。
告警策略	按需配置，详见【告警策略】。

点击保存，添加成功，界面出现添加的保护对象。



5.3.1.2. 编辑

1、单个保护对象编辑

选择需要修改的保护对象，点击“操作”栏的 “编辑”按钮，弹出编辑保护对象的对话框，修改信息后点击“确定”按钮。

2、多个保护对象批量编辑

勾选多个保护对象后，点击批量修改。

弹出批量修改保护对象的对话框。仅支持对保护对象的状态和审计策略进行修改。

勾选需要更改的保护对象的状态或者审计策略，对状态和策略做统一的更改，如图。

点击单个保护对象的状态或者审计策略，下拉展示可选择的配置信息，可更改单个配置。

更改后点击“确定”按钮，保存修改的配置信息。

5.3.1.3. 复制

使用复制功能可以实现快速“添加”保护对象。已添加的保护对象与将要添加的保护对象配置相似时，可以点击已添加保护对象“操作”栏“更多”中的复制按钮，在打开的复制保护对象对话框中修改保护对象信息并保存。

5.3.1.4. 删除

勾选一个或多个要删除的保护对象，点击“批量删除”按钮。

5.3.1.5. 其他操作

修改保护对象状态。点击保护对象的 ON 按钮可以开启或关闭保护对象。

查询保护对象。在输入框中输入保护对象名称，点击查询按钮，筛选符合条件的保护对象。

导出保护对象。点击“导出”按钮可将保护对象导出到 Excel 文件中。支持通过勾选一个或多个保护对象，选择要导出的保护对象信息；未勾选保护对象，则导出列表中所有保护对象；

导入保护对象。点击“导入”按钮可下载模板，完成模板填写后可将模板中的保护对象信息导入到保护对象列表中。

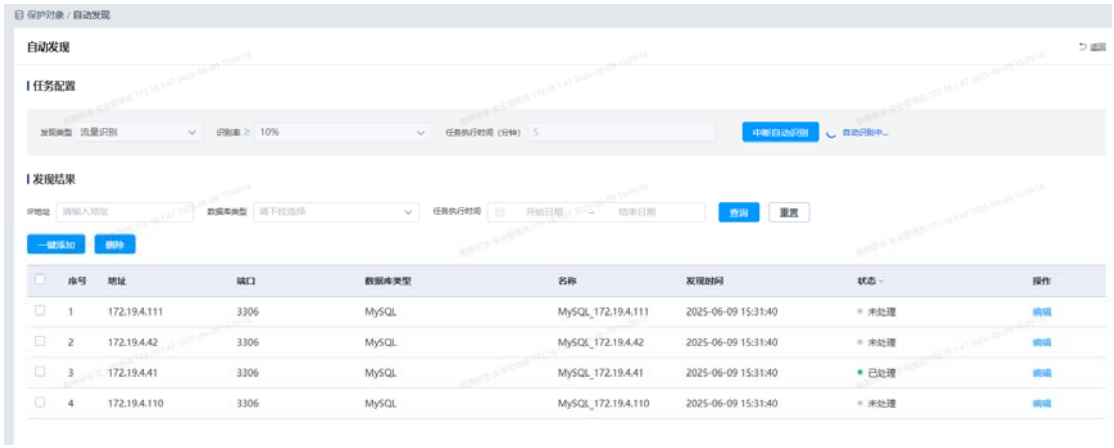
支持配置保护对象的扩展信息，可用于获取保护对象的存储过程、触发器及表对象信息。

5.3.1.6. 自动发现

点击“自动发现”按钮，进入自动发现页面。自动发现分为流量识别和端口扫描两种方式。

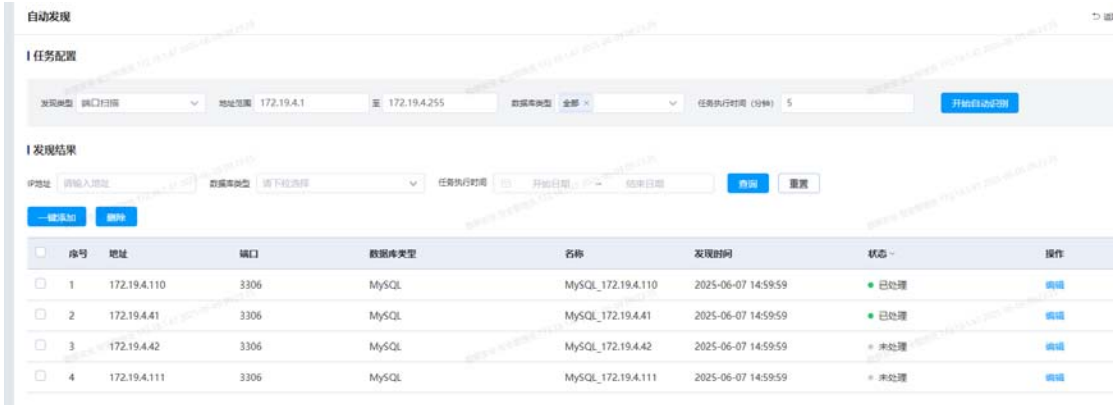
1、流量识别

发现类型选择“流量识别”时，需要选择识别率及任务执行时间。识别率表示任务执行时间内流量匹配占比率，可以根据实际情况进行填写，填写完成后点击“开始自动识别”按钮进行识别。

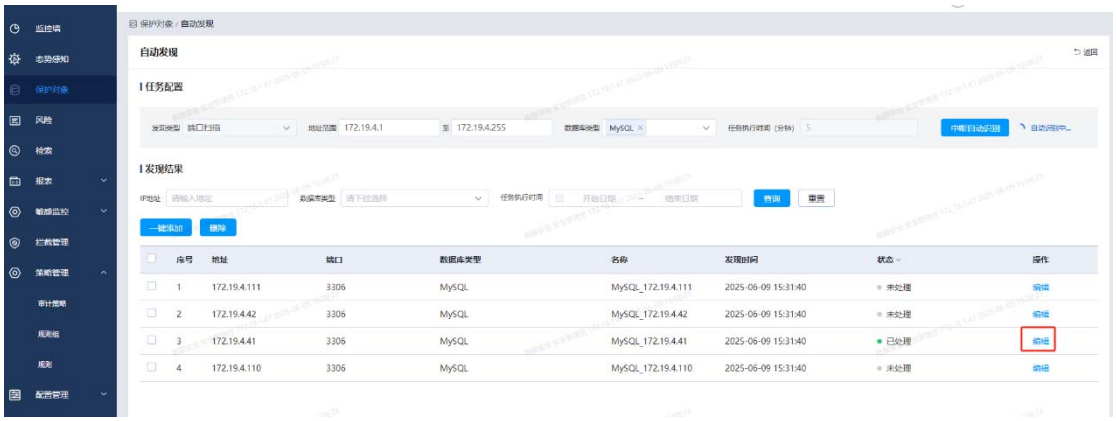


2、端口扫描

发现类型选择“端口扫描”时，需要输入地址范围、数据库类型和任务执行时间，可以根据实际情况进行填写，填写完成后点击“开始自动识别”按钮进行识别。



扫描完成后可以点击“一键添加”按钮，完成保护对象的批量添加，或者点击“编辑”按钮，进行单个数据库的添加。



5.3.1.7. Agent 部署

点击 Agent 部署按钮，进入 Agent 部署页面。可以根据添加的保护对象进行 Agent 远程部署，SSH 账户需拥有 root 权限，默认安装路径为:/opt/linux_agent，支持 IPv4、IPv4 段或 IPv6 地址。

1.远程安装

点击远程安装按钮，阅读安装说明，输入 SSH 相关信息，点击确认进行远程安装。

字段填写说明：

客户端 IP	输入保护对象客户端 IP 地址，支持配置单个 IP 地址或 IP 地址段。其中单个 IP 支持配置 IPV4 或 IPV6，IP 地址段只支持 IPV4，如 172.23.1.23-172.23.1.29，不支持 IPV6 地址段。
SSH 账户	SSH 账户，需要拥有 root 权限
SSH 密码	SSH 密码
SSH 端口	SSH 端口
标签	一条数据最多可以添加五个标签
全局	表格中的配置优先于全局的配置
服务端 IP	Agent 流量转发地址

可以一次添加多个客户端 IP 或者 IP 段，如果是 IP 段，会生成多条安装记录。

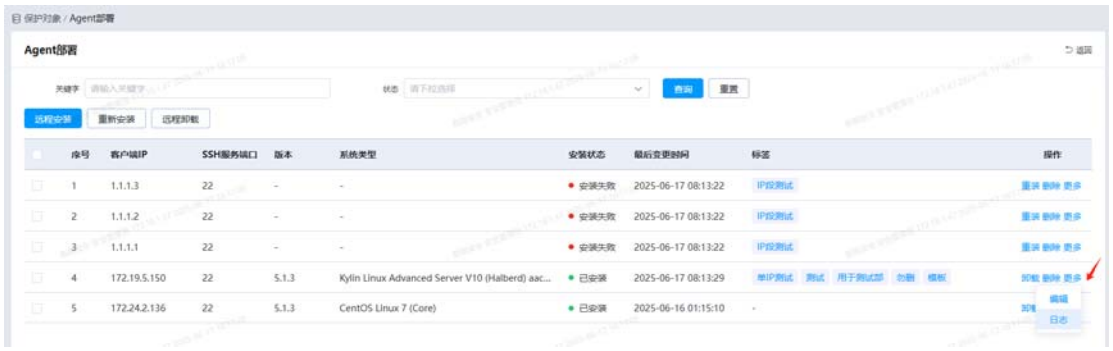
Agent远程安装
安装说明：
1、支持IPv4、IPv4段或IPv6地址。
2、SSH账户需拥有root权限。
3、默认安装路径为:/opt/linux_agent。
展开更多
*安装客户端列表 表单填写 文本输入
序号 客户端IP SSH账户 SSH密码 SSH端口 标签 操作
1 172.19.5.190 root 22 请输入 +1 删除 添加
全局
SSH账户 root SSH密码 请输入SSH密码
SSH端口 22 服务端IP 172.19.4.165
密码策略 不保存 保存
确定 取消

Agent远程安装
安装说明：
1、支持IPv4、IPv4段或IPv6地址。
2、SSH账户需拥有root权限。
3、默认安装路径为:/opt/linux_agent。
展开更多
*安装客户端列表 表单填写 文本输入
序号 客户端IP SSH账户 SSH密码 SSH端口 标签 操作
1 172.19.5.150 root 22 请输入 +5 删除 添加
2 1.1.1.1-1.1.1.3 root 22 请输入 +1 删除 添加
全局
SSH账户 root SSH密码 请输入SSH密码
SSH端口 22 服务端IP 请选择服务端IP
密码策略 不保存 保存
确定 取消

Agent部署
操作成功 已添加到安装列表,请稍后在列表查询安装结果
查询 重置
远程安装 重新安装 远程卸载
序号 客户端IP SSH服务端口 版本 系统类型 安装状态 最后变更时间 标签 操作
1 1.1.1.3 22 安装中 2025-06-17 08:13:19
2 1.1.1.2 22 安装中 2025-06-17 08:13:19
3 1.1.1.1 22 安装中 2025-06-17 08:13:19
4 172.19.5.150 22 安装中 2025-06-17 08:13:19
5 172.24.2.136 22 5.1.3 CentOS Linux 7 (Core) 已安装 2025-06-16 01:15:10

2. 查看日志

远程安装完成之后，可以在列表操作项中更多-日志按钮查看成功或者失败日志，并且日志支持导出。

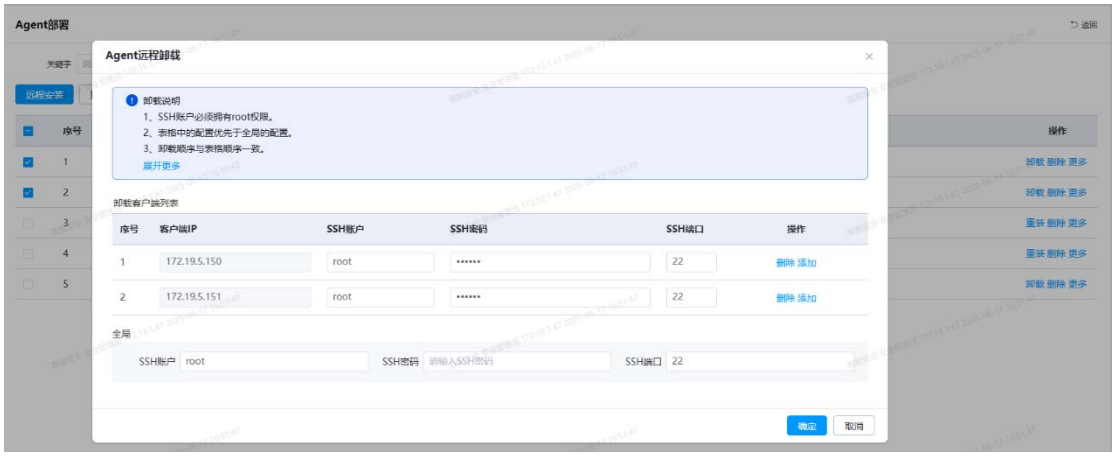


3. 删除

操作项点击删除按钮，删除该条安装记录。

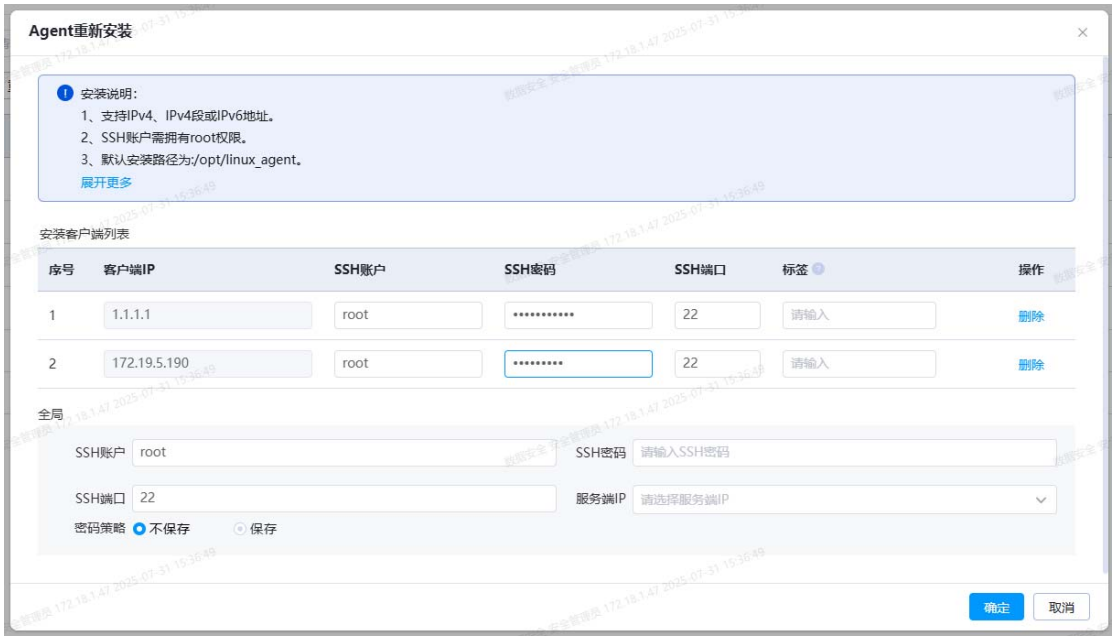
4. 卸载

操作项点击卸载按钮，或者勾选多个点击远程卸载，进行批量卸载。



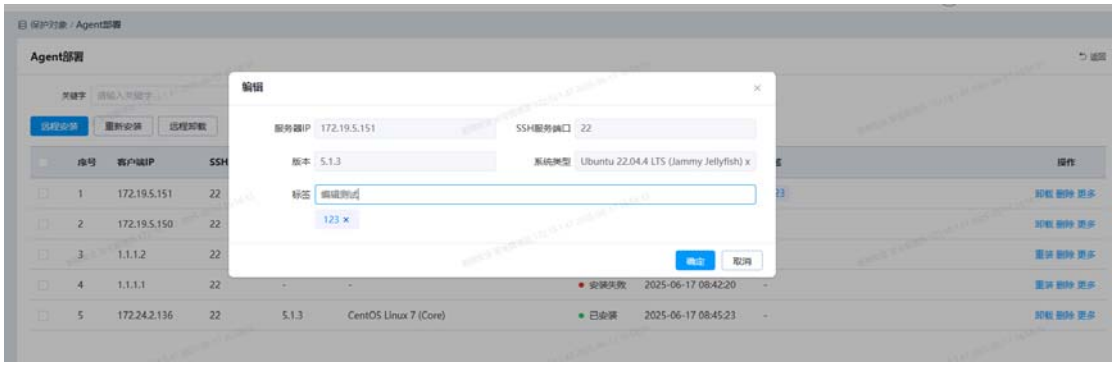
5. 重新安装

操作项点击重装按钮，或者勾选多个点击重新安装，进行批量重新安装。



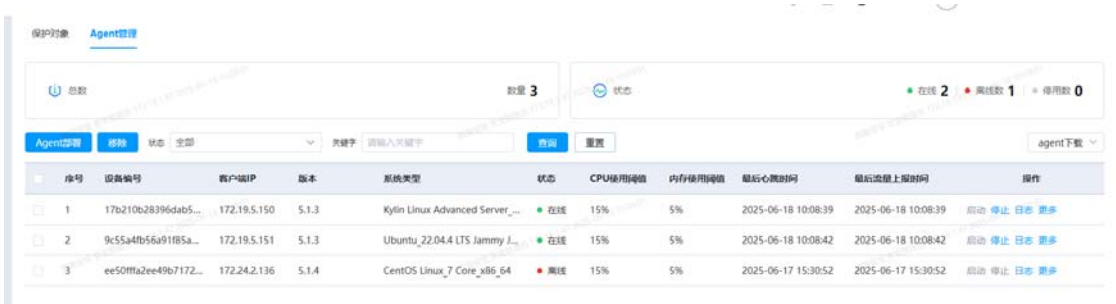
6. 编辑

操作项中更多-编按钮，进行标签修改。

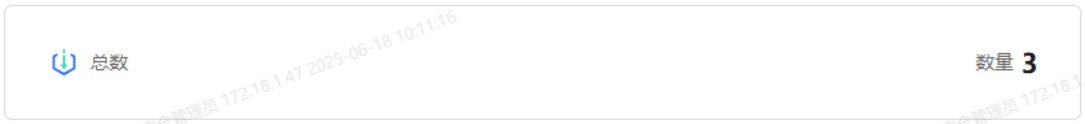


5.3.2. Agent 管理

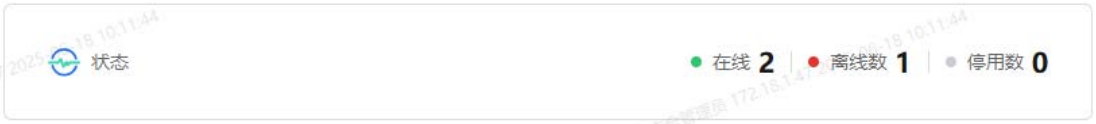
该界面主要是集中管理监控设备，允许用户查看设备状态、部署新的 Agent、监控设备性能以及配置下发等。



1.连接总数



2.状态统计



3. 根据设备状态和关键字搜索相关数据

5.3.2.1. Agent 部署

点击 Agent 部署按钮进入 Agent 部署页面，详情请参见【5.3.1.7】

5.3.2.2. 移除

对于长久离线或废弃的 Agent 可以进行移除操作，只有离线状态的才能进行移除操作。

5.3.2.3. 自动发现

点击右侧操作项中更多-自动发现，填写任务执行时间可以自动扫描该设备上的数

据库，扫描结果在可在保护对象页面自动发现按钮查看。

5.3.2.4. 下发配置

点击右侧操作项中更多-配置下发，远程修改 Agent 配置。

字段填写说明：

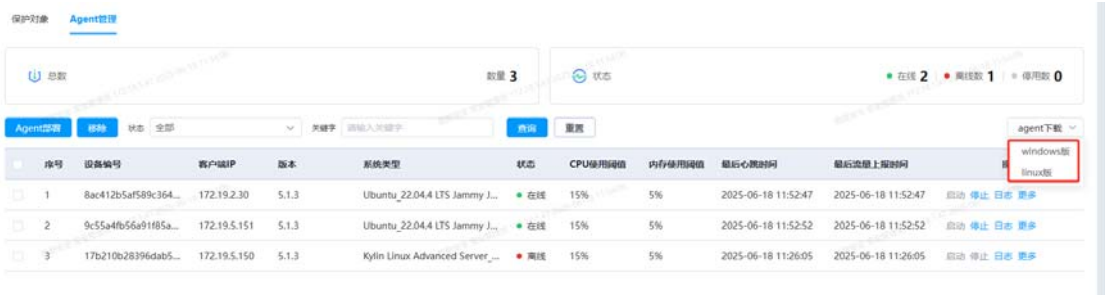
客户端 IP	Agent 客户端 IP
服务端 IP	Agent 流量转发地址
管理 IP	Agent 客户端与审计端通讯使用,如 agent 状态管理、配置下发等
管理端口	Agent 客户端与审计端通讯默认端口 443
抓包过滤串	配置方式如下: 1.审计不同的端口 单个端口示例: tcp port 3306 多个端口示例: tcp port 3306 or port 1521 该配置支持同时审计端口为 3306 和 1521 的流量 2.审计不同的 IP 单个 IP 示例: host 172.18.1.2 多个 IP 示例: host 172.18.1.2 or host 172.18.1.136 该配置支持同时审计 172.18.1.2 和 172.18.1.136 的流量 3.审计不同协议的端口 示例: (tcp port 80) or (udp port 53)

	该配置支持同时审计 80 和 53 端口 4.审计指定 IP 对 示例：host 172.18.1.136 and host 172.18.1.26 该配置支持审计 172.18.1.136 访问 172.18.1.26 的所有流量 5.审计指定端口并排除单个 IP 示例：tcp port 3306 and not host 172.18.1.136 该配置支持审计 IP 除 172.18.1.136 以外的所有访问 3306 端口的流量 6.审计指定端口并排除多个 IP 示例：tcp port 3306 and not host 172.18.1.136 and not host 172.24.2.113 该配置支持审计除 172.18.1.136 和 172.24.2.113 外的所有访问 3306 端口的流量 7.审计指定 IP 加指定端口的流量 示例：tcp port 3306 and host 172.18.1.136 该配置支持审计 IP 为 172.18.1.136 且端口为 3306 的流量 8.审计指定端口段 示例：portrange 2000-5000 该配置支持审计端口为 2000-5000 的所有流量
抓包端口	抓包端口
抓包网口名称	抓包网口名称
服务端 IP	数据库审计与防护系统平台 IP
发包网口名称	发包网口名称
内存阈值	内存超过设置的阈值，将停止审计
CPU 阈值	CPU 超过设置的阈值，将停止审计
CPU 核数开关	CPU 核数开关；开启状态，CPU 阈值和内存阈值会按照总核数来计算

5.3.2.5. 其他操作

1. Agent 下载

提供 windows 版和 linux 版本

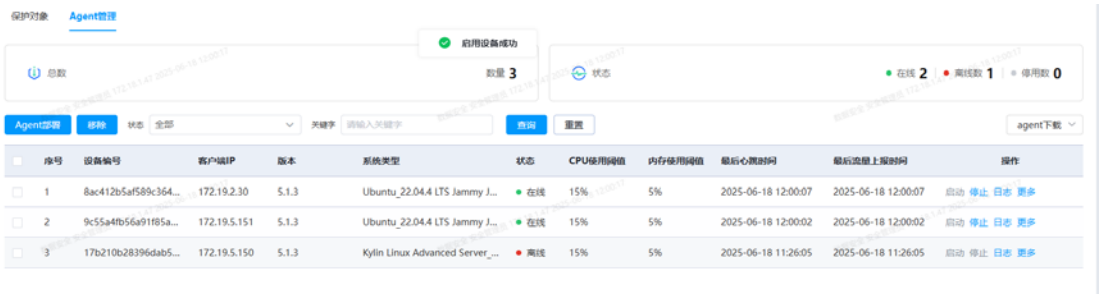


2. 停止

对 Agent 设置进行停止操作，停止后该设备将暂停审计。

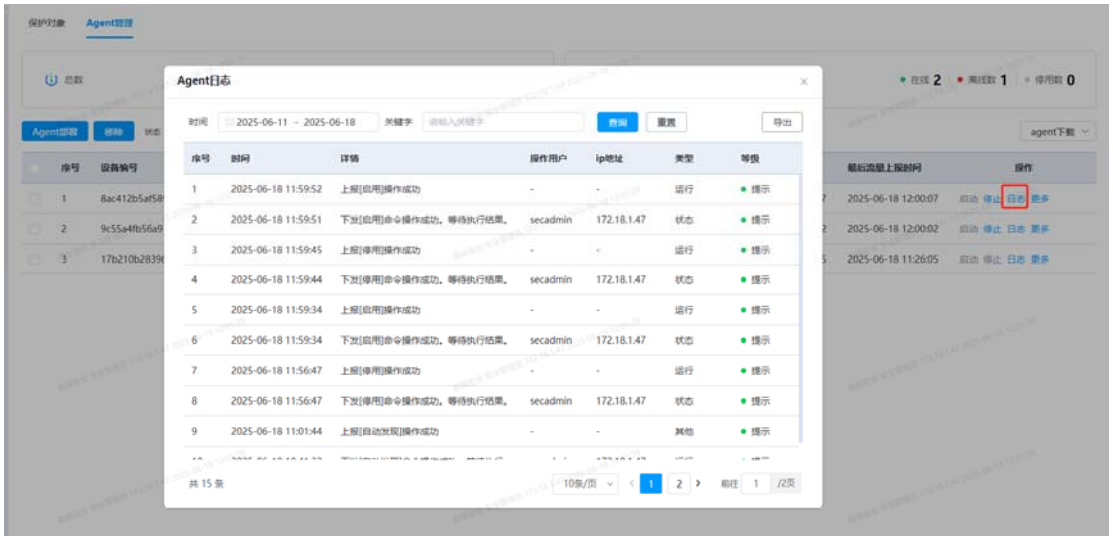
3. 启动

对 Agent 设置进行启动操作，开启审计功能。



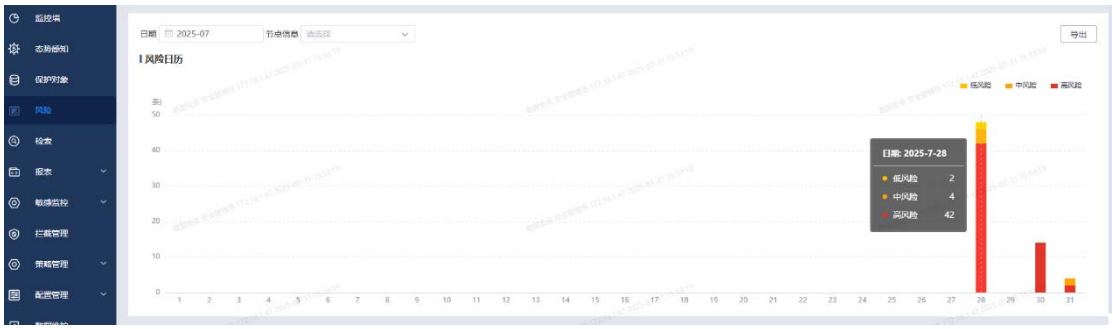
4. 日志

查看 Agent 的操作记录并支持导出。

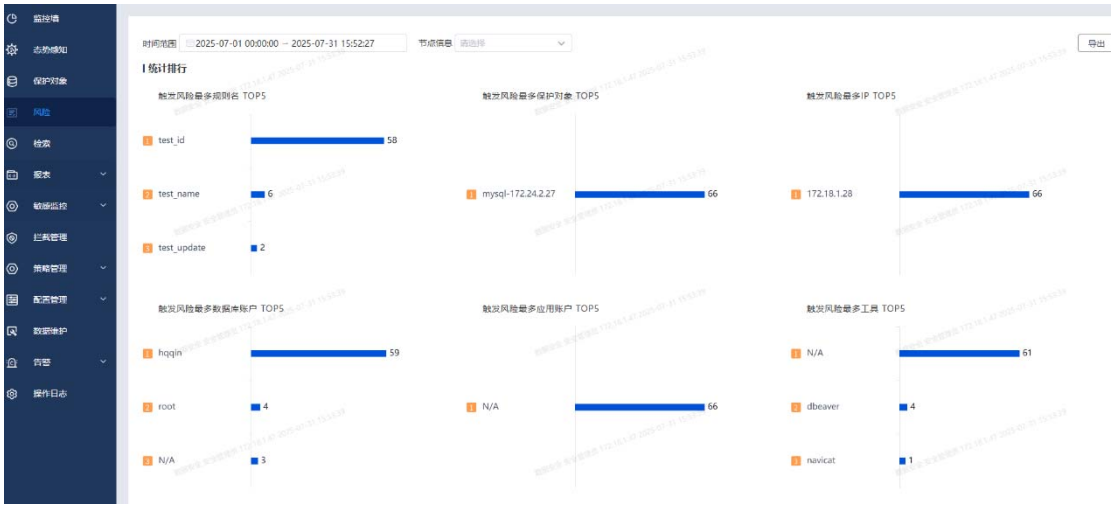


5.4 风险

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。



第二部分为统计排行，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。



5.5 检索

检索页面支持对所有审计记录进行查询，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、检索结果两个模块。

1、检索条件

检索页面支持包括筛选时间、风险级别、关键字过滤 3 个默认条件，点击“更多筛选”按钮可以展开隐藏的查询条件，点击 + 按钮可以按照需要添加更多的高级检索条件。输入不同的查询条件点击查询按钮可以筛选数据，点击重置按钮可以清除查询条件。

2.设为模版

选好了常用条件点击设为模版，输入名称、筛选时间可以选择保留或者不保留，点击确认就可以保存模版，下次进入检索页面可以选择设置好的模版，直接查询。模版最多保存 8 个，不用的模版可以点击模版名称右上角的 进行删除。

3、检索结果

列表默认展示序号、时间、风险级别、客户端 IP、服务端 IP、操作类型、数据库账户、操作语句、回应、处置状态等信息，可以点击列表右上角“显示列”按钮，根据需要选择不同的展示列。

4、导出

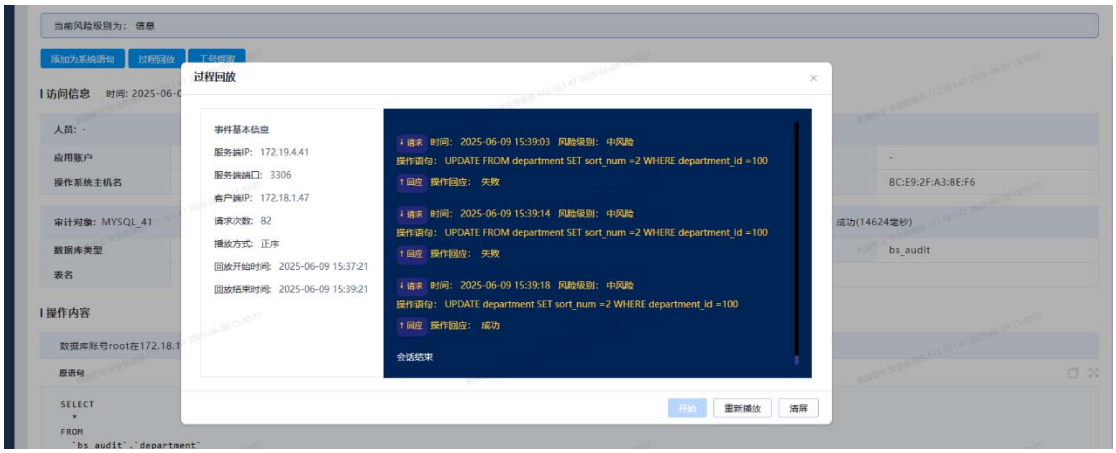
点击“导出”按钮可将审计导出到文件中，支持导出的文件格式包括 Excel、Word、PDF。支持通过勾选一条或多条审计记录，导出指定的审计记录；未勾选审计记录时，则导出列表中所有审计记录。

5、详情

选择一条审计记录，点击“操作”栏下“详情”按钮，可以进入审计记录详情页面。

在详情页面，点击“添加为系统语句”按钮，可以把当前的语句添加到系统语句中。

在详情页面，点击“过程回放”按钮，可以按照选择的时间和播放方式进行前后数据的播放。



在详情页面，点击“工号提取”按钮，可以按照当前语句添加工号提取配置，添加成功后配置将展示到【工号提取】页面，对后续执行的语句进行工号的提取。

5.6 报表

5.6.1. 分析报表

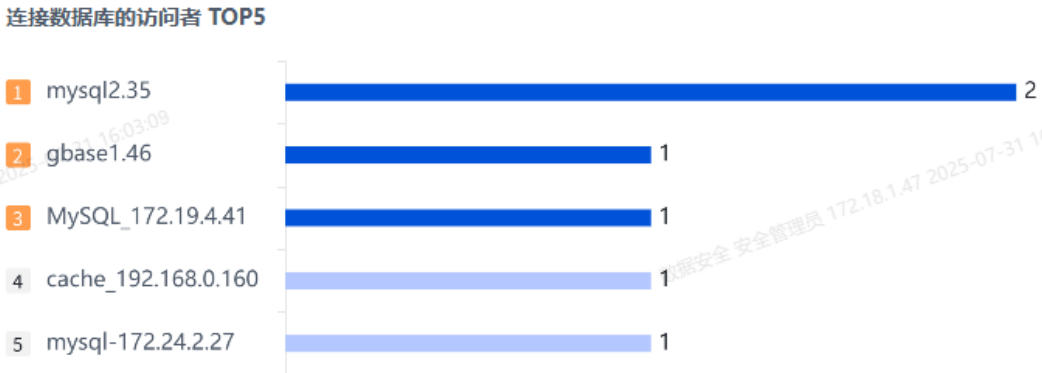
5.6.1.1. 服务器分析

1、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。

账户数最多的数据库 TOP5：这部分报表记录了审计对象中账户数最多的 top5，用户可以了解对应的审计对象使用了多少用户进行访问。

连接数据库的访问者 TOP5：这部分报表记录了审计对象中 ip 连接数量最多的 TOP5，用户可以了解到哪个审计对象连接的 ip 最多。



操作和登录次数最多的数据库信息列表：这部分报表记录了审计对象中登录次数和操作次数最多的 TOP5，用户通过这些可以了解到哪个审计对象的活跃度最高。

操作和登录次数最多的数据库信息列表

序号	保护对象名	登录数量	操作次数
1	mysql2.35	0	9155753
2	MYSQL_199	122	6911
3	mysql-172.24.2.27	17	711
4	MySQL_172.19.4.41	6	181
5	pop1.28	0	39
6	cache_192.168.0.160	1	30
7	pop18.21	0	10
8	smtp1.28	3	6
9	mysql-172.18.1.199	1	6
10	gbase1.46	0	5

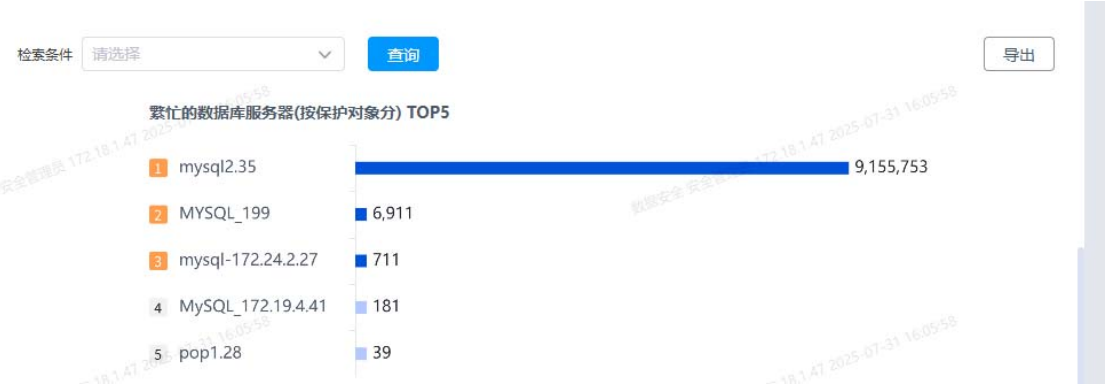
共 11 条 10条/页 1 2 前往 1 /2页

2、数据库服务性能

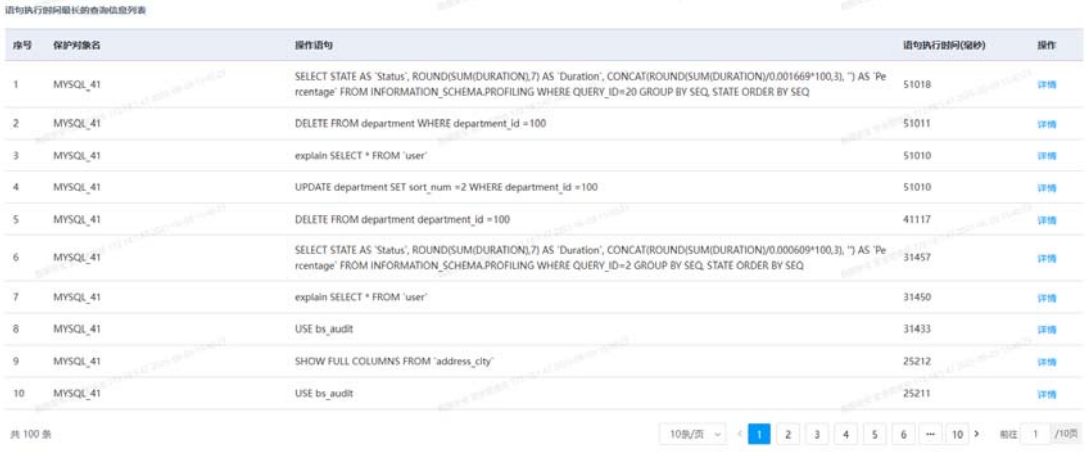
该部分数据主要是针对数据库本身的查询参数进行统计，旨在给客户提供其数据库查询性能的相关参数。

查询语句执行时间分布 TOP5：这部分报表主要罗列了查询语句在不同时间区段的分布，通过这些可以了解到语句执行的快慢情况。

繁忙的数据库服务器 TOP5：这部分报表主要展示了审计对象操作次数最多的TOP5，通过这些用户可以了解到每个审计对象的活跃程度。



语句执行时间最长的查询信息列表：这部分报表会根据每个审计对象语句的执行时间，按降序的顺序进行排列，通过这些用户可以了解到哪些语句的耗时较长，耗时长的语句操作代表返回的数据量比较多，评估是否是查询大数量的操作。



语句执行时间最长的查询信息列表

序号	保护对象名	操作语句	语句执行时间(毫秒)	操作
1	MYSQL_41	SELECT STATE AS `Status`, ROUND(SUM(DURATION),7) AS `Duration`, CONCAT(ROUND(SUM(DURATION)/0.001669*100,3), '') AS `Percentage` FROM INFORMATION_SCHEMA.PROFILING WHERE QUERY_ID=20 GROUP BY SEQ, STATE ORDER BY SEQ	51018	详情
2	MYSQL_41	DELETE FROM department WHERE department_id =100	51011	详情
3	MYSQL_41	explain SELECT * FROM `user`	51010	详情
4	MYSQL_41	UPDATE department SET sort_num =2 WHERE department_id =100	51010	详情
5	MYSQL_41	DELETE FROM department department_id =100	41117	详情
6	MYSQL_41	SELECT STATE AS `Status`, ROUND(SUM(DURATION),7) AS `Duration`, CONCAT(ROUND(SUM(DURATION)/0.000609*100,3), '') AS `Percentage` FROM INFORMATION_SCHEMA.PROFILING WHERE QUERY_ID=2 GROUP BY SEQ, STATE ORDER BY SEQ	31457	详情
7	MYSQL_41	explain SELECT * FROM `user`	31450	详情
8	MYSQL_41	USE bs_audit	31433	详情
9	MYSQL_41	SHOW FULL COLUMNS FROM `address_city`	25212	详情
10	MYSQL_41	USE bs_audit	25211	详情

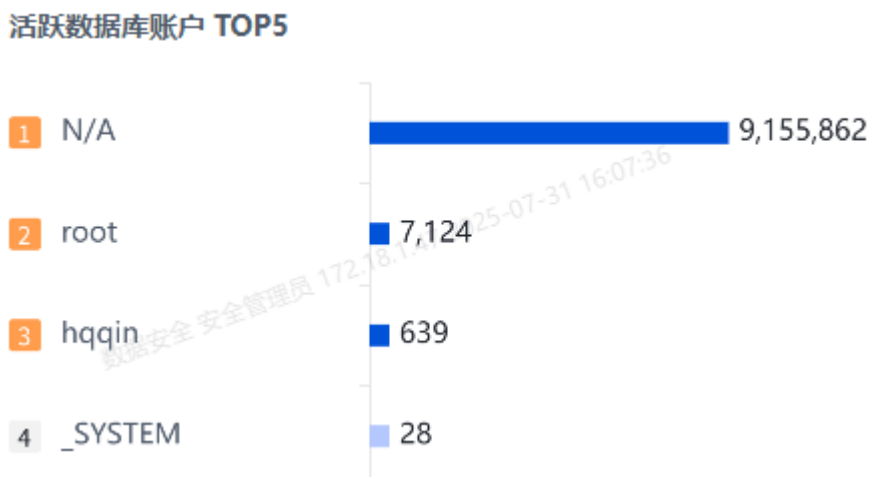
共 100 条　10条/页　1 2 3 4 5 6 ··· 10　前往 1 /10页

5.6.1.2. 源分析

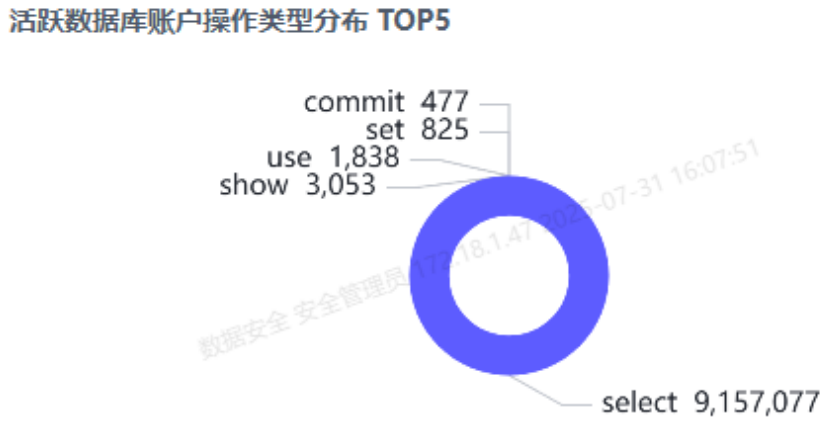
源分析报表主要是对客户端进行分析，通过“数据库账户”，“客户端”，“访问者IP”三者的结合，让用户更好的了解审计对象被访问的情况。

1、数据库账户

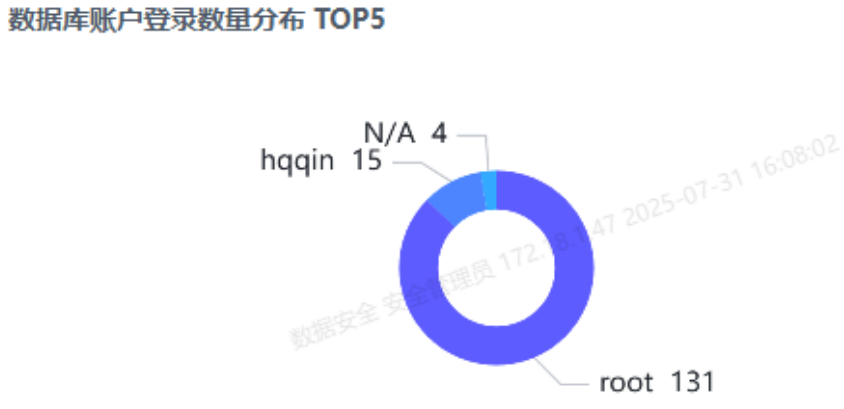
活跃数据库账户 TOP5：报表记录了审计对象使用账户最多的 TOP5，通过这些用户可以判断是否存在异常账户。



活跃数据库账户操作类型分布 TOP5：报表记录了审计对象操作类型次数最多 TOP5，通过这些用户可以判断有哪些常用操作以及是否存在异常操作。



数据库账户登录数量分布 TOP5：报表记录了登录数量最多账户的 TOP5，通过这些用户可以了解到对应审计对象账户的活跃程度。



数据库账户登录和操作信息列表：报表记录所有保护对象对应的“访问者 IP”，“数据库账户”，“操作次数”，“登录数量”，用户可以从中了解所有保护对象的操作信息。

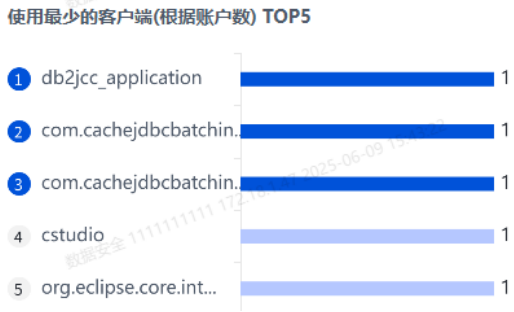
数据库账户登录和操作信息列表

序号	保护对象名	访问者IP	数据库账户	操作次数	登录数量
1	172.19.1.237_62005	172.19.6.18	N/A	984206	0
2	oracle	172.19.3.199	SCOTT	61776	11321
3	oracle	172.19.6.32	SCOTT	35658	11505
4	172.19.1.233_5432	172.24.3.189	postgres	30950	3927
5	mongodb172.19.1.233	172.19.5.3	N/A	21429	0
6	MongoDB_172.19.1.222_27017	172.19.6.18	N/A	21405	0
7	sqlserver2016-237	172.19.6.19	N/A	11913	4079
8	sqlserver2016-237	172.19.3.199	N/A	10720	10720
9	MyS203	172.19.6.19	N/A	2335	0
10	mysql_172.19.4.41	172.18.1.39	root	1352	35

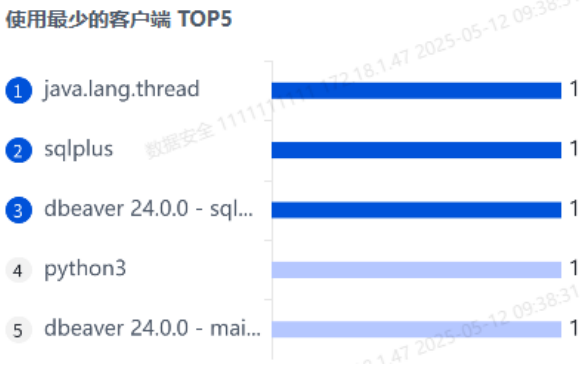
共 90 条数据　10条/页　1 2 3 4 5 6 … 9　前往 1 /9页

2、客户端

使用最少的客户端（根据账户数）TOP5：报表记录了每个账号使用的客户端数量，通过这些用户了解是否存在不常用的客户端。

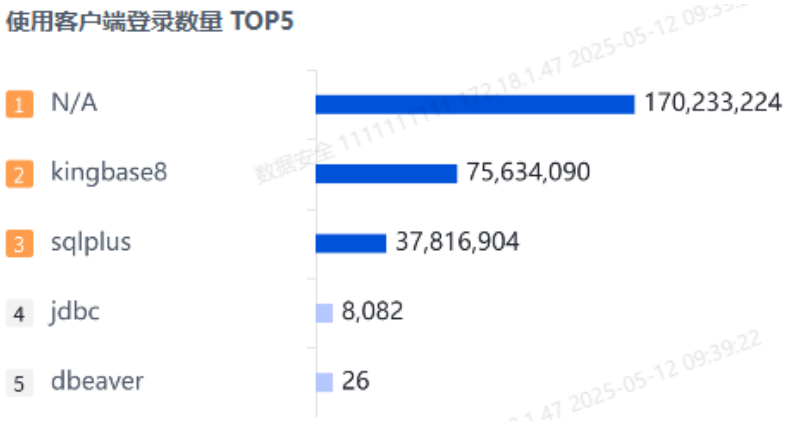


使用最少的客户端 TOP5：报表记录了每个 ip 使用的客户端数量，通过这些用户可以了解每个 ip 使用客户端的频次，以及是否存在异常客户端。



使用客户端登录数量 TOP5：报表记录了登录次数最多的客户端 TOP5，通过这些

用户可以了解每种客户端的活跃程度，以及是否存在异常客户端。



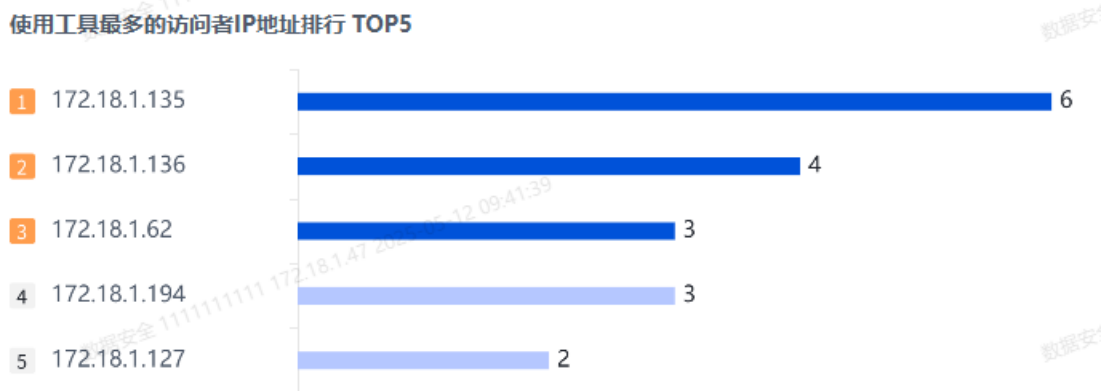
客户端会话信息列表：报表记录所有保护对象对应的“客户端”，“访问者 IP”，“数据库账户”，“登录数量”，用户可以从中了解所有审计对象客户端的访问情况。

客户端会话信息列表

序号	保护对象名	客户端	访问者IP	数据库账户	登录数量
1	mysql_172.19.1.26	N/A	172.18.1.136	root	8
2	mysql_172.19.2.150	N/A	172.18.1.136	root	6
3	orcl_172.19.1.14	navicat	172.18.1.136	sys	4
4	orcl_172.19.1.14	dbeaver	172.18.1.136	SYS	3
5	mysql_172.19.1.26	navicat	172.18.1.136	root	1
6	mysql_172.19.2.150	navicat	172.18.1.136	root	0

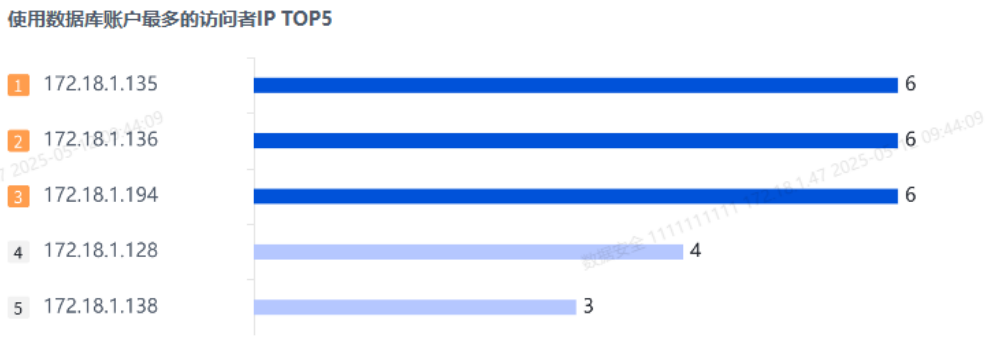
3、访问者 IP

使用工具最多的访问者 IP 地址排行 TOP5：报表记录了每个 ip 使用工具的数量最多的 TOP5，通过这些，用户可以了解到每个 ip 的访问习惯以及是否存在异常的访问工具。



使用数据库账户数最多的访问者 IP TOP5：报表记录了每个 ip 使用数据库账户最

多的 TOP5，通过这些，用户可以了解到对应审计对象常用的用户以及是否存在非法用户。



基于访问者 IP 的操作信息列表：报表记录所有保护对象对应的“访问者 IP”，“数据库账户”，“客户端”，“操作次数”，用户可以从中了解所有基于访问者 ip 的操作情况。

基于访问者IP的操作信息列表

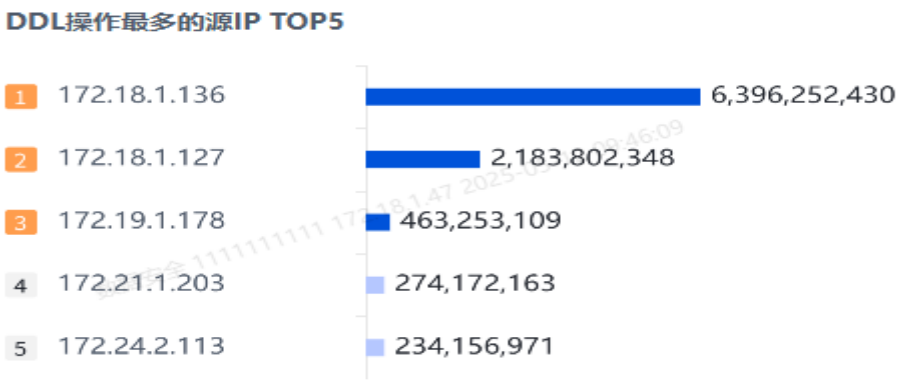
序号	保护对象名	访问者IP	数据库账户	客户端	操作次数
1	orcl_172.19.1.14	172.18.1.136	sys	navicat	62
2	mysql_172.19.2.150	172.18.1.136	root	N/A	49
3	mysql_172.19.2.150	172.18.1.136	root	navicat	39
4	orcl_172.19.1.14	172.18.1.136	SYS	dbeaver	30
5	mysql_172.19.1.26	172.18.1.136	root	N/A	13
6	mysql_172.19.1.26	172.18.1.136	root	navicat	12

5.6.1.3. 行为分析

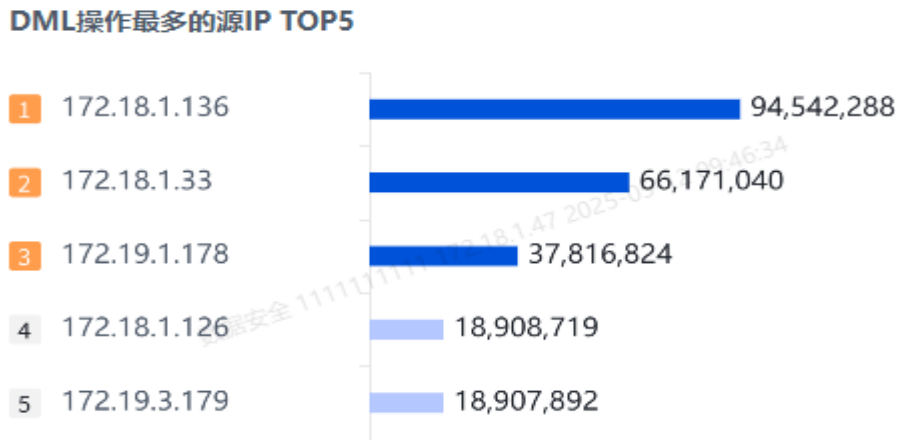
行为分析报表主要是对保护对象操作类型进行分析，通过“操作分析”，“权限分析”，“认证管理分析”三者的结合，让用户更好的了解审计对象行为的情况。

1、操作分析

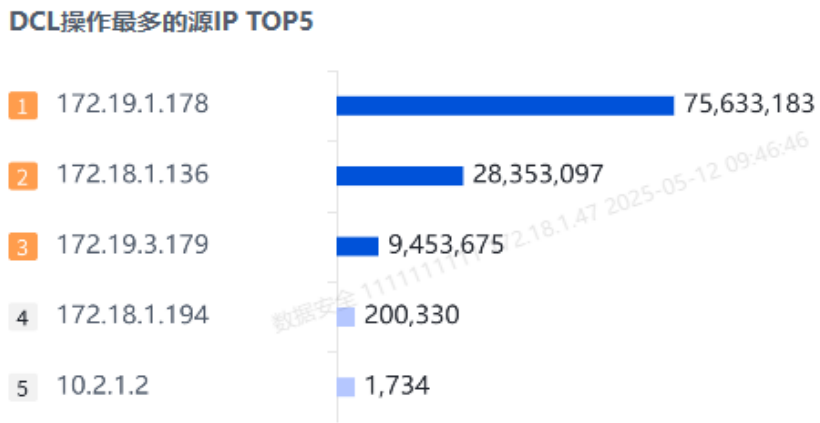
DDL 操作最多的源 IP TOP5：报表记录了操作保护对象执行 DDL 操作最多的 TOP5，通过这些可以了解到源 IP 的操作习惯以及是否存在异常操作。



DML 操作最多的源 IP TOP5：报表记录了操作保护对象执行 DML 操作最多的 TOP5，通过这些可以了解到源 IP 的操作习惯以及是否存在异常操作。



DCL 操作最多的源 IP TOP5：报表记录了操作保护对象执行 DCL 操作最多的 TOP5，通过这些可以了解到源 IP 的操作习惯以及是否存在异常操作。



2、权限分析

授权最多的账号 TOP5：报表记录了操作保护对象执行授权操作最多的账号 TOP5，通过这些可以了解到主要进行授权操作的具体账号以及是否存在异常账号授权。

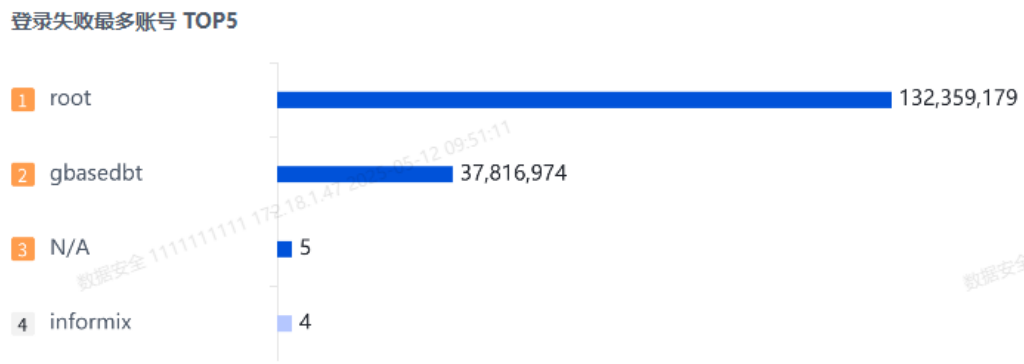
授权最多的 IP TOP5：报表记录了操作保护对象执行授权操作最多的 IP TOP5，通过这些可以了解到主要进行授权操作的具体 IP 以及是否存在异常 IP 授权。

权限回收最多的账号 TOP5：报表记录了操作保护对象执行权限回收操作最多的账号 TOP5，通过这些可以了解到主要进行权限回收操作的具体账号以及是否存在异常账号权限回收。

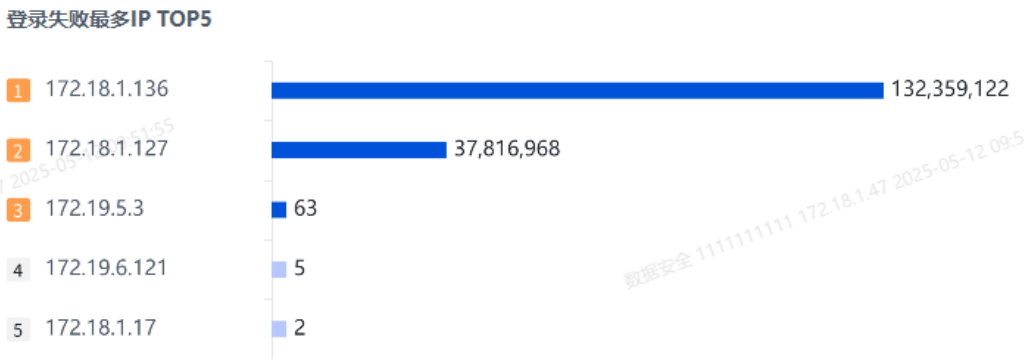
权限回收最多的 IP TOP5：报表记录了操作保护对象执行权限回收操作最多的 IP TOP5，通过这些可以了解到主要进行权限回收操作的具体 IP。

3、认证管理分析

登录失败最多账号 TOP5：报表记录了登录保护对象失败最多的账号 TOP5，通过这些可以了解到具体的登录失败 TOP5 账号。



登录失败最多 IP TOP5：报表记录了登录保护对象失败最多的 IP TOP5，通过这些可以了解到具体的登录失败 TOP5 IP。

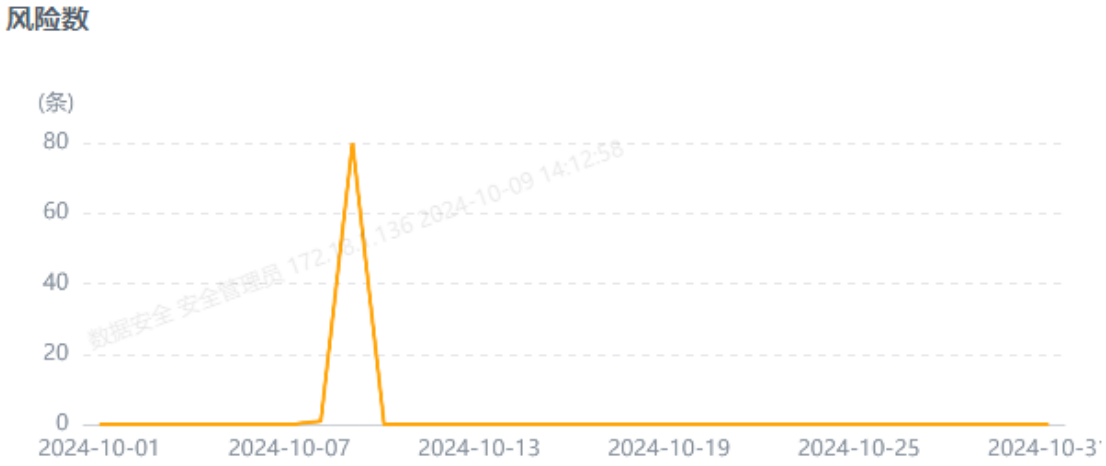


5.6.1.4. 趋势分析

趋势分析报表主要是对进行分析，通过“操作分析”，“权限分析”，“认证管理分析”三者的结合，让用户更好的了解审计对象行为的情况。

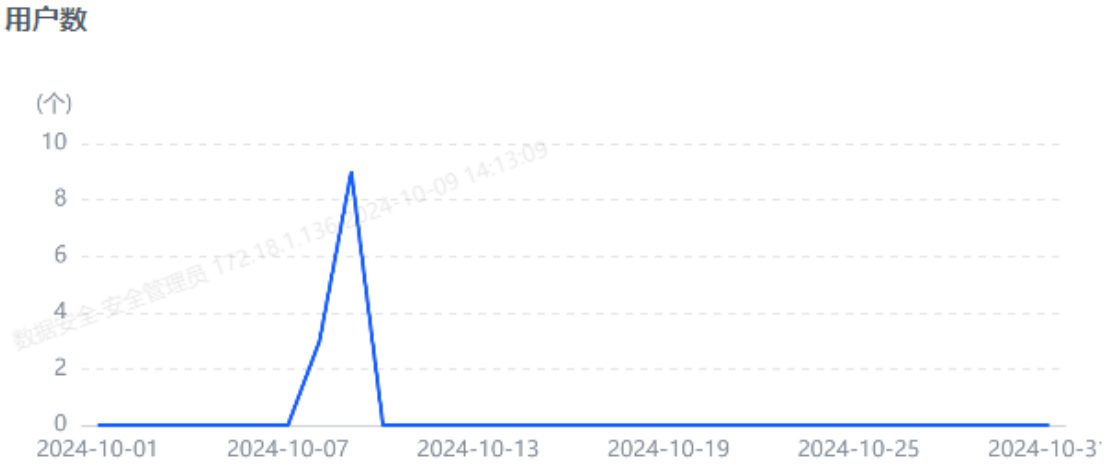
1、风险数

报表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。



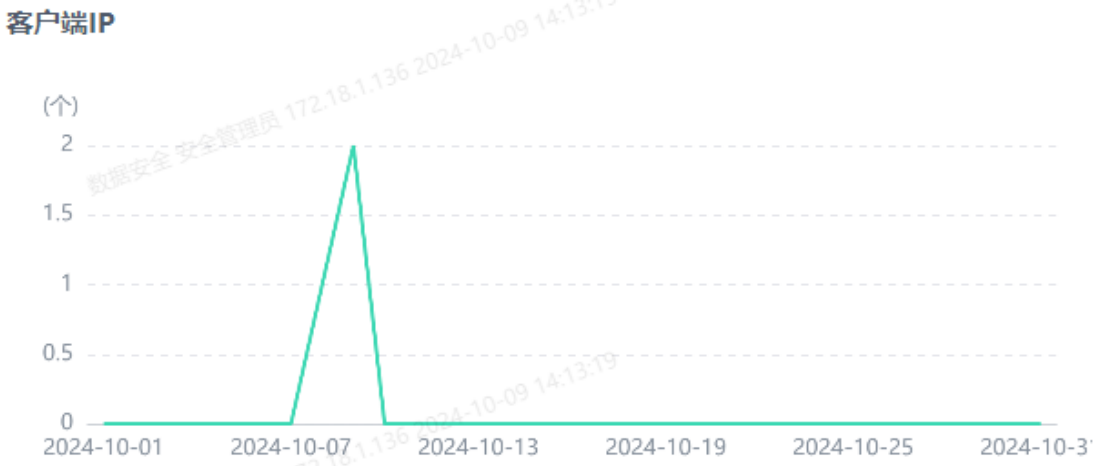
2、用户数

报表展示一个月每一天，保护对象用户数的情况，直观看见每天用户数的趋势图。



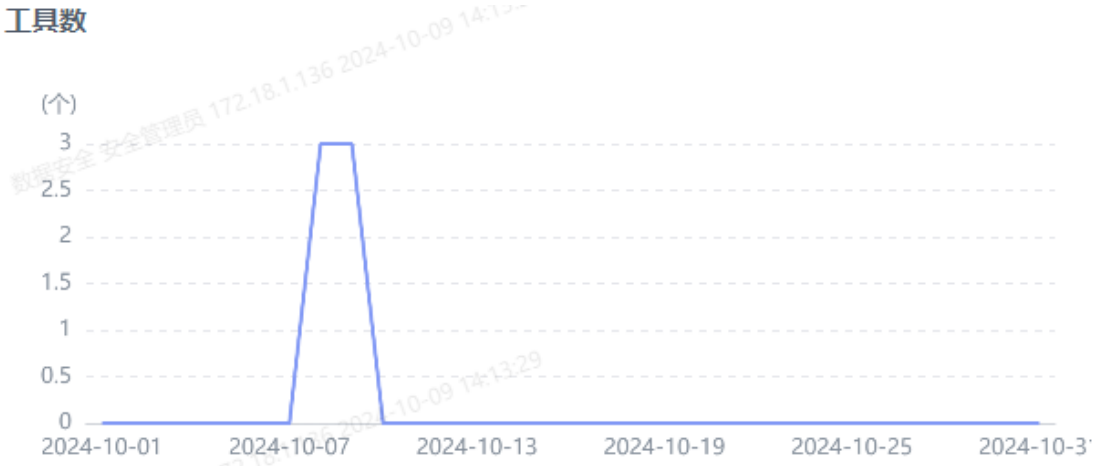
1、客户端 IP

报表展示一个月每一天，访问保护对象客户端 IP 的情况，直观看见每天客户端 IP 数量的趋势图。



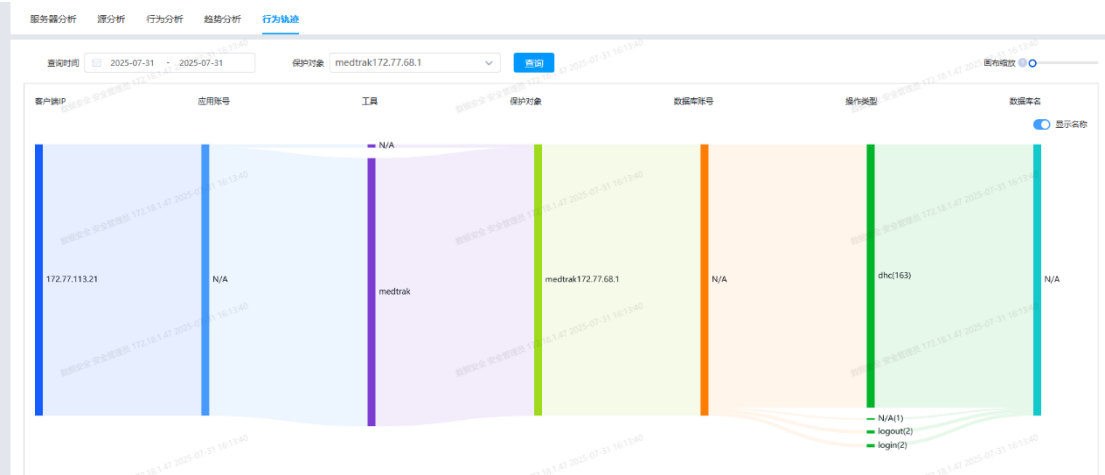
2、工具数

报表展示一个月每一天，访问保护对象客户端 IP 的工具使用情况，直观看见每天连接工具数的趋势图。



5.6.1.5. 行为轨迹

行为轨迹展示基于客户端 IP、应用账号、工具、保护对象、数据库账号、操作类型、数据库的审计数据统计情况，可以调整查看不同时间及不同保护对象的统计数据。



5.6.1.6. 合规报表

5.6.1.7. 等保报告

本报表参考《中国国家信息安全保护检验标准》，根据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

1、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”。

2、客户端访问分析

使用最少的客户端 TOP5：报表记录了每个 ip 使用的客户端数量，通过这些用户可以了解每个 ip 使用客户端的频次，以及是否存在异常客户端。

客户端访问列表：报表主要展示了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”。

客户端访问列表

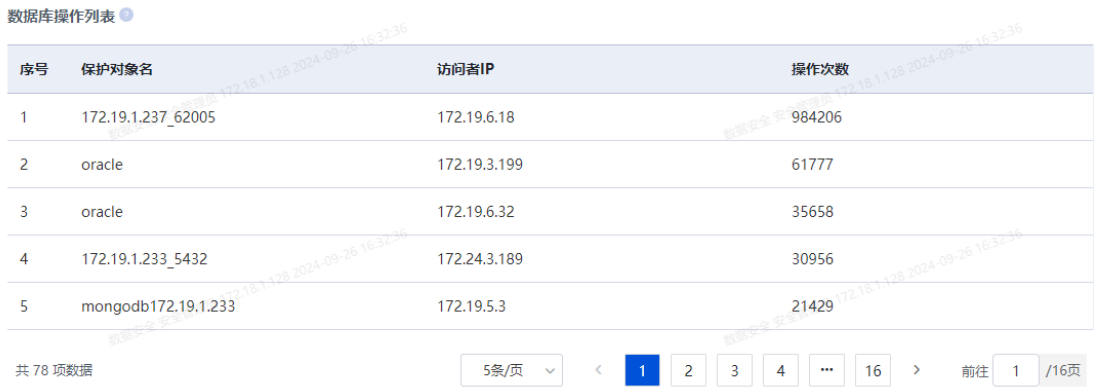
序号	保护对象名	访问者工具	访问者IP	数据库账户	登录数量
1	oracle	jdbc	172.19.6.32	SCOTT	11505
2	oracle	jdbc	172.19.3.199	SCOTT	11321
3	sqlserver2016-237	N/A	172.19.3.199	N/A	10720
4	sqlserver2016-237	N/A	172.19.6.19	N/A	4079
5	172.19.1.233_5432	N/A	172.24.3.189	postgres	3927

共 100 项数据 5条/页 1 2 3 4 ··· 20 前往 1 /20页

3、审计日志统计分析

被审计数据库的审计记录数 TOP5：该报表根据当前所有审计对象的审计日志数量，按从高到低进行排序，用户可以根据当前审计日志的数量，判断哪个审计对象风险较高。

数据库操作列表：该报表展示了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。

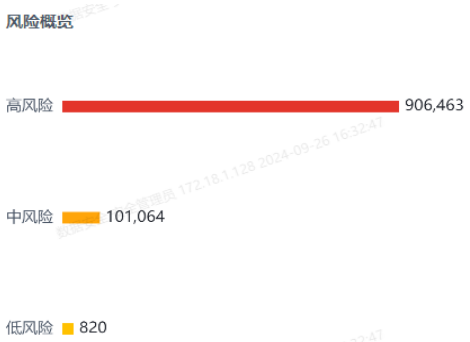


5.6.1.8. SOX 萨班斯报告

本报告参考《萨班斯—奥克斯利法案》（Sarbanes-Oxley Act，简称 SOX）， 针对企业内部控制体系有效性评估关注 的 IT 系统使用状况数据统计梳理。旨在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。

1、概述

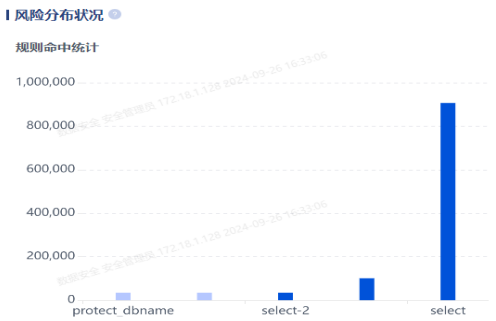
风险概览：该报表主要是展示统计时间内，风险总数以及高、中、低风险占的总比例。



最近的会话信息：统计时间内，不同的数据库用户使用各个客户端，访问保护对象的最后一次信息记录。

2、风险分布状况

规则命中统计：报表记录了统计时间内，被审计数据库的命中规则名称以及各命中数量，帮助用户了解当前数据库的风险状态。



风险 IP：报表记录了统计时间内，每个客户端 IP 命中风险级别的数量，通过报表可以了解到是否存在异常客户端 IP。

风险IP

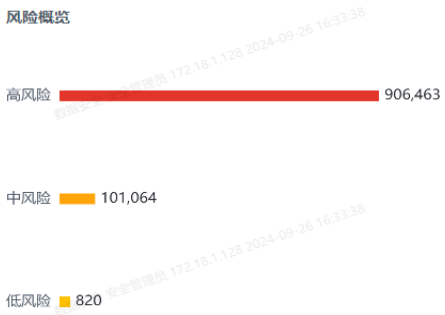
序号	客户端ip	高风险数	中风险数	低风险数
1	172.19.6.18	849,951	94,439	0
2	172.19.3.199	34,576	3,838	0
3	172.19.6.32	11,560	1,286	0
4	172.24.3.189	6,021	669	0
5	172.19.6.19	2,723	301	59

5.6.1.9. PCI 报告

本报告参考《支付卡行业数据安全标准》（Payment Card Industry (PCI) Data Security Standard， 简称 PCI DSS），针对规范重点关注的持卡人敏感数据安全性、跟踪敏感数据使用、以及数据管理员安全活动行为进行统计分析。旨在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即时发现，快速定位分析，为整体信息安全管理提供决策依据。

1、概述

风险等级：该报表主要是展示统计时间内，风险总数以及高、中、低风险占的总比例。



最近的会话信息：统计时间内，不同的数据库用户使用各个客户端，访问保护对象的最后一次信息记录。

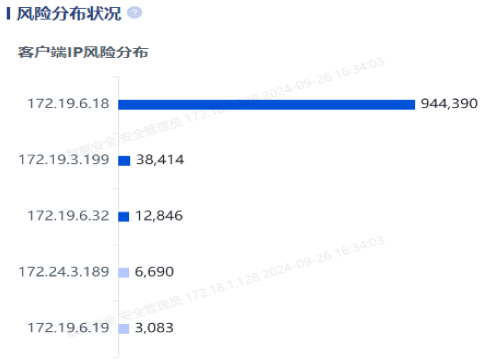
最近的会话信息

序号	客户端IP	数据账户	访问工具	发生时间
1	172.18.1.136	root	N/A	2024-09-25
2	172.18.1.136	root	navicat	2024-09-24
3	172.18.1.16	my_sql	N/A	2024-09-20
4	172.18.1.16	my_sql	navicat	2024-09-20
5	172.18.1.16	root	N/A	2024-09-20

共 57 项数据　5条/页　‹ 1 2 3 4 ··· 12 ›　前往 1 /12页

2、风险分布状况

客户端风险分布：报表记录了统计时间内，客户端触发高、中、低风险数量统计，帮助用户关注可能存在风险的客户端。

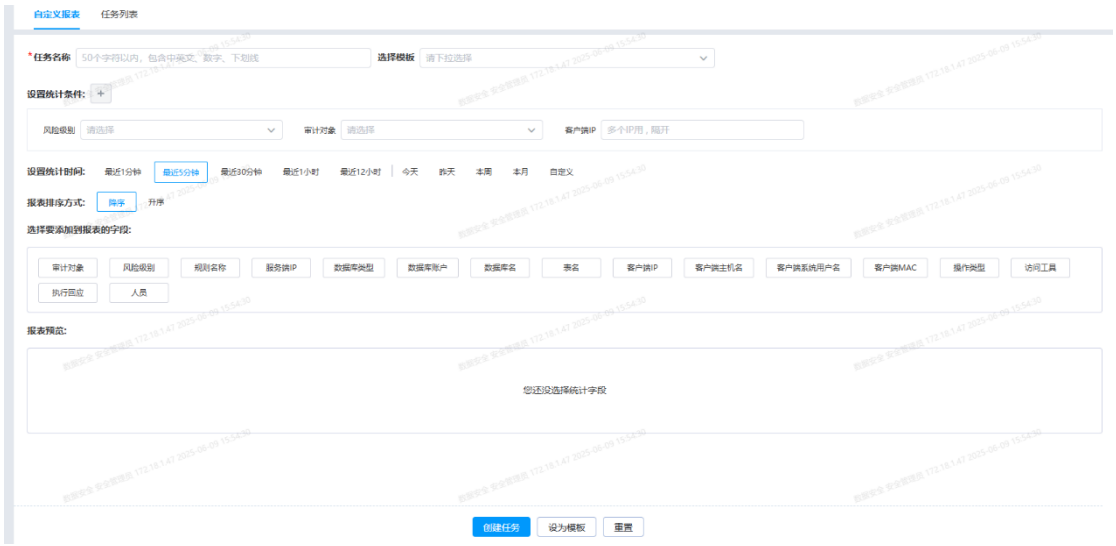


风险IP

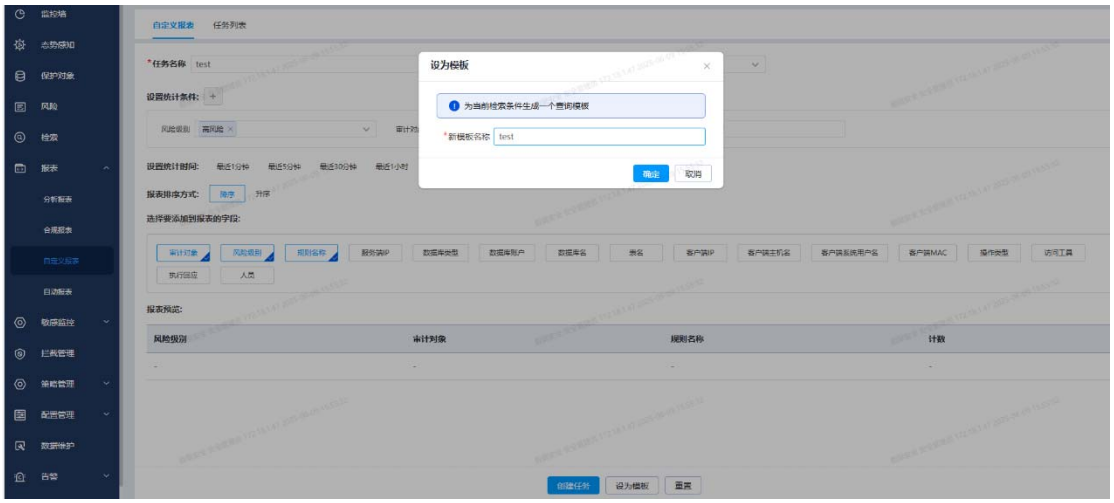
序号	客户端ip	高风险数	中风险数	低风险数
1	172.19.6.18	849951	94439	0
2	172.19.3.199	34576	3838	0
3	172.19.6.32	11560	1286	0
4	172.24.3.189	6021	669	0
5	172.19.6.19	2723	301	59

5.6.2. 自定义报表

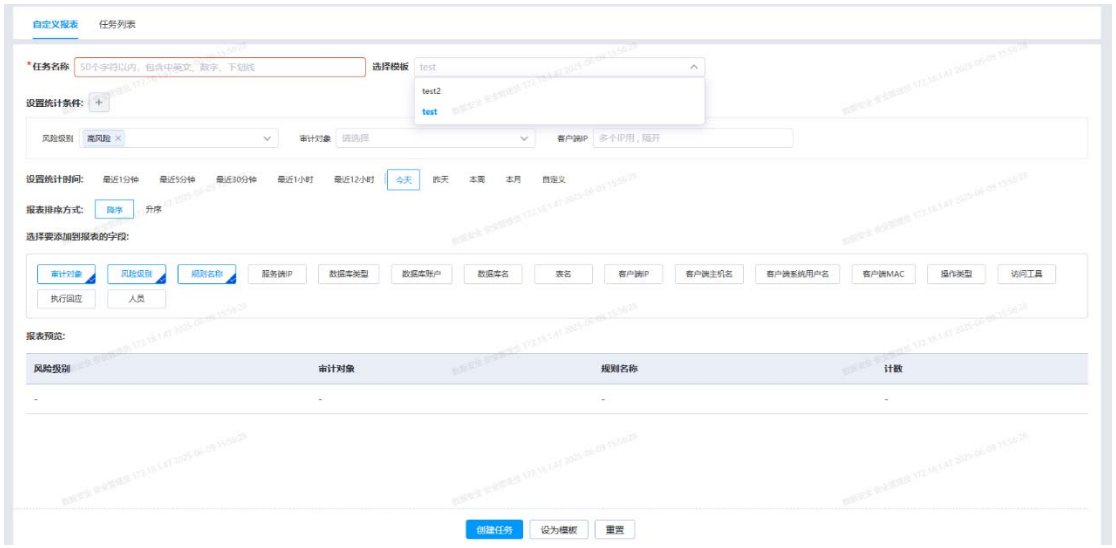
自定义报表可以自定义选择报表内容，包括统计条件、统计时间、排序方式、要添加到报表中的字段、报表预览。



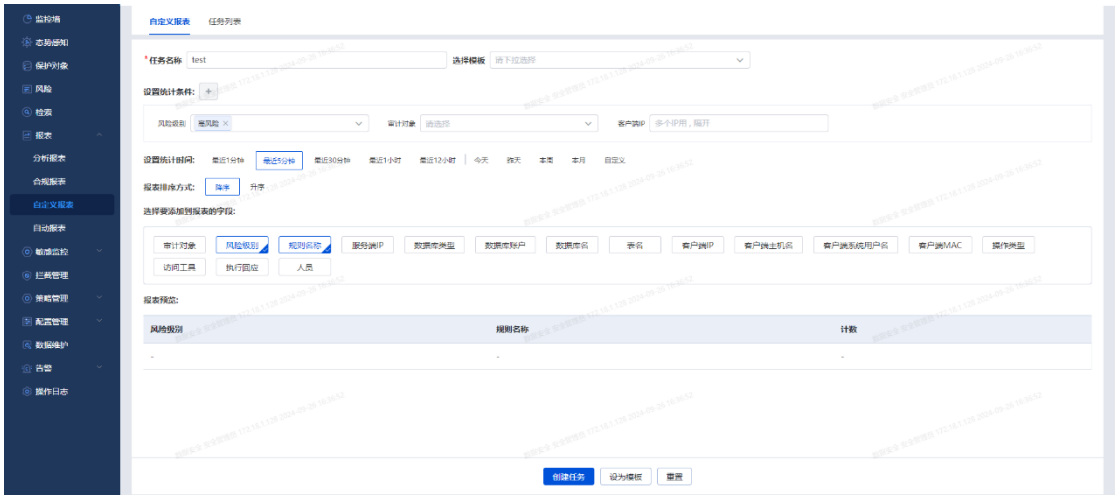
支持将所有条件设置为模板，后续生成报表时可以直接选用模板，使报表统计更加便捷。



使用模板创建自定义报表任务时，可以直接在“选择模板”字段的下拉列表中选择，选择模板后任务条件将自动加载模板中的字段。



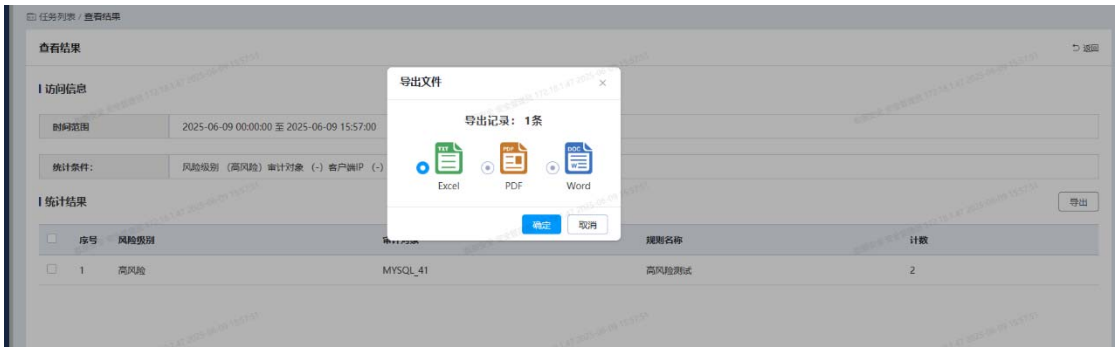
创建报表任务通过选择选择模板或者直接配置进行创建，选择完任务参数后,点击“创建任务”即可完成报表任务的创建。



注意：选择已有的模板后依然可以自行修改对应的维度参数

报表任务创建完成后，可以在任务列表中点击“查看结果”按钮查看任务直接结果

自定义报告页面支持点击“导出”按钮将报表内容导出到 Excel、PDF、Word 文件中。支持勾选部分数据后导出，不勾选数据则导出所有数据。



5.6.3. 自动报表

自动报表可以通过邮件自动发送报表。支持配置报表接收人、报表发送方式、报表格式及发送周期等内容,一次最多可以选中五个报表进行发送。

作业名称	自动报表任务名称。
接收人	只支持邮件方式，邮件需要在邮件服务器进行配置，详见 4.4.6.1 邮件服务器。
发送报表	支持选择自定义报表模板和固定报表模板。
报表格式	支持 PDF、Word 方式。
作业状态	启用：报表任务启用，禁用：报表任务关闭

发送周期	支持按周、按月、立即发送，按周，每周星期一的凌晨一点执行任务；周月，每月 1 号的凌晨一点执行任务；立即发送，配置完成后立即发送。
描述	对任务的信息描述，非必填，根据用户实际情况选择性填写。

5.7 敏感监控

5.7.1. 敏感数据

敏感数据是敏感监控的具体对象，可以通过手动添加、导入以及敏感发现的方式定义需要监控的敏感数据。敏感规则通过配置已经定义的敏感数据进行规则审计以及敏感监控。

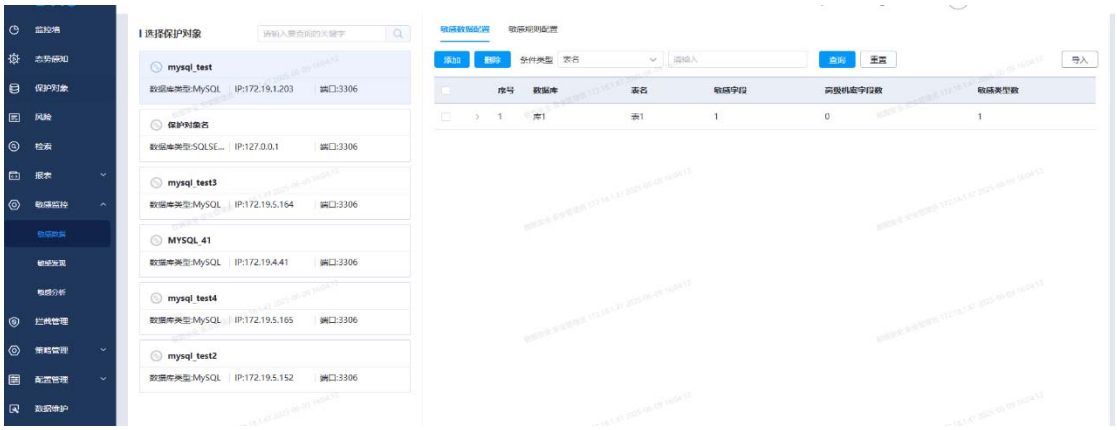
5.7.1.1. 敏感数据配置

敏感数据配置有三种方式，第一种：页面手动添加配置，第二种：导入敏感数据，第三种：通过敏感发现扫描的敏感数据。

1、页面手动添加配置：

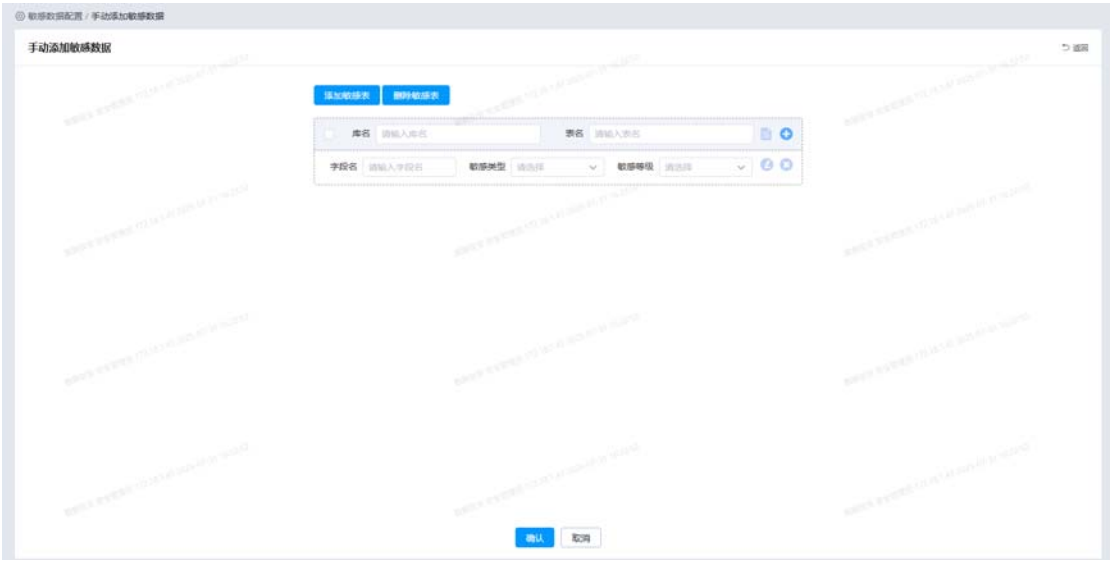
选择保护对象：

点击“选择保护对象”，选择一个需要配置的保护对象，点击确定



添加敏感数据配置：

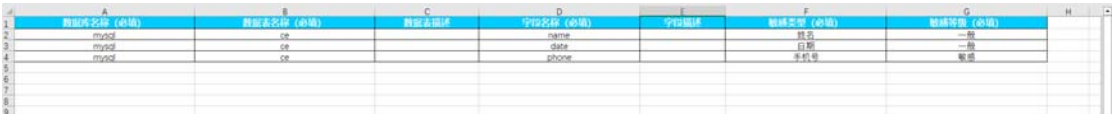
点击页面“添加”按钮，跳转到“手动添加敏感数据”页面，点击“添加敏感表”，配置敏感任务。



库名	敏感数据对应的数据库名
表名	敏感数据对应的表名
字段名	敏感数据对应的字段名
敏感类型	敏感数据对应的敏感类型。支持选择内置和自定义的敏感类型。
敏感等级	敏感数据对应的敏感级别。可选范围包括一般、敏感、机密、绝密

2、导入敏感数据：

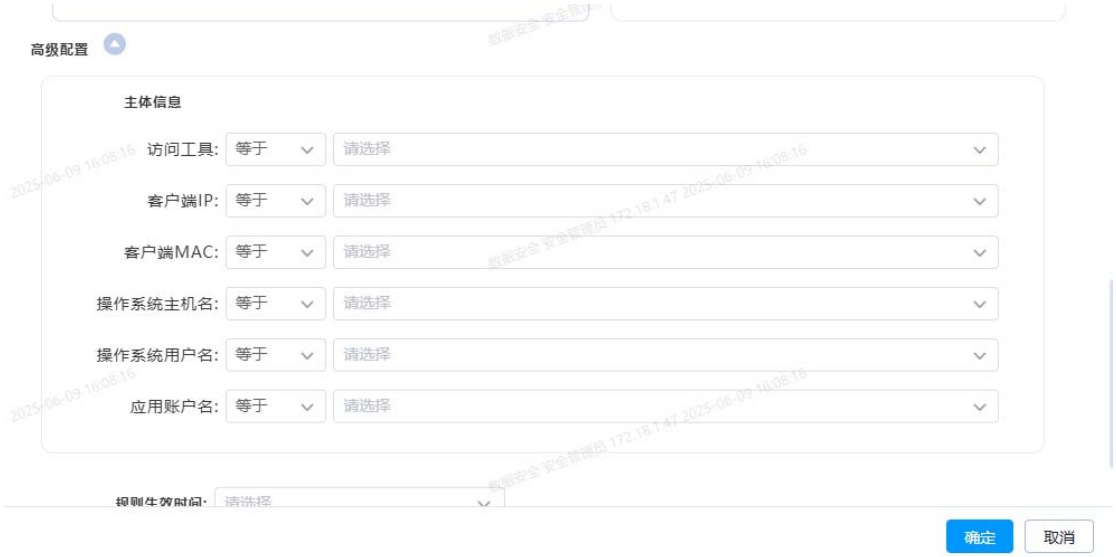
点击 模板下载 按钮，确定并下载完成后，删除模板文件中的示例内容，根据实际情况填写敏感数据相关信息后保存文件。



点击 导入敏感数据 按钮，上传模板文件并导入成功后，页面实时展示导入的数据。

5.7.1.2. 敏感规则配置

支持对敏感数据配置审计规则。点击添加，弹出新增敏感规则对话框，对话框内容如下：

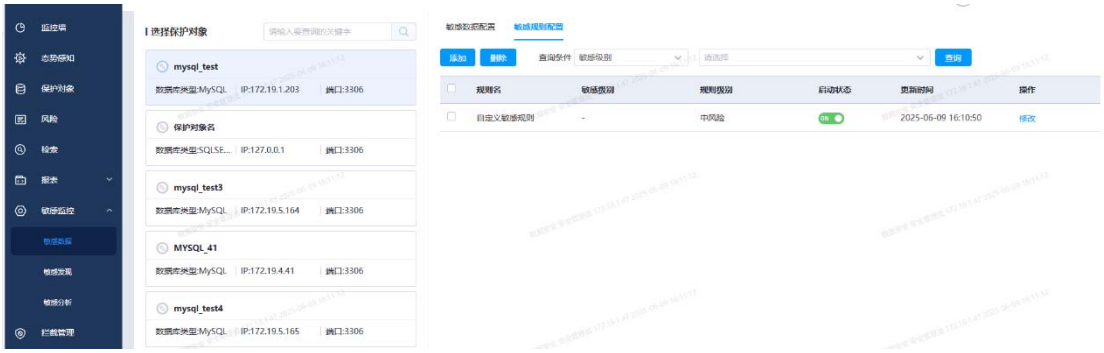


规则名	对敏感规则取名字
风险级别	风险级别包含高风险，中风险，低风险，关注行为，一般行为。
状态	默认为“ON”状态，可以手动修改为“OFF”。
操作类型	操作类型包含了几十种常见的数据库操作，例如 select，insert，update，delete 等。
动作	动作包含审计，严格阻断，宽松阻断。
敏感类型	选择敏感类型库中的敏感类型进行筛选敏感配置中的敏感数据
敏感级别	根据敏感级别筛选敏感配置中的敏感数据
敏感配置	根据库名、表名、字段名进行选择敏感配置，敏感规则通过敏感表及字段进行审计匹配
访问工具	通过访问工具的匹配来完成审计，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素

客户端 ip	通过客户端 ip 的匹配来完成审计，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素
客户端 mac	通过客户端 mac 的匹配来完成审计，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素
操作系统主机名	通过操作系统主机名的匹配来完成审计，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素
操作系统用户名	通过操作系统用户名的匹配来完成审计，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素
应用帐户名	通过应用账户的匹配来完成审计，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素
规则生效时间	可以让规则在指定时间段内生效，可以手动输入进行模糊匹配选择集合配置中配置的集合或者基础元素

添加敏感数据：

添加敏感规则：



开启保护对象的敏感防护开关。

访问敏感规则中涉及的敏感数据，就会触发敏感规则。

5.7.2. 敏感发现

5.7.2.1. 敏感发现任务配置

1、敏感发现任务 – 添加

点击“添加”，跳转到“创建敏感识别”页面

任务名称	用于敏感任务名称
保护对象	需要敏感发现的保护对象，目前支持 Mysql、Oracle、SQLserver、DB2 四种数据库类型
SID/数据库名	保护对象中需要敏感发现的数据库的名称，SQLserver、DB2 这两种数据库类型则填写模式名

用户名	用户填写数据库登录账号，Oracle 不支持 SID 登录
密码	数据库登录密码
测试按钮	填写任务名称、保护对象、数据库名、用户名、密码之后，点击 测试 按钮获取敏感发现目标保护对象中的表及字段
更新	修改敏感发现任务时，需要重新获取表及字段信息点击 更新 按钮
表/字段	选择已获取的表及字段作为需要敏感发现敏感数据的目标对象
样本数	敏感发现任务根据样本数对数据进行扫描判断字段的数据条数
匹配率	根据扫描的样本数，与敏感类型进行匹配对比的比率
扫描方式	可以根据手动执行、定时执行、周期执行方式进行任务扫描

配置数据库连接信息后点击测试按钮，列表会自动加载填写的数据库对应的表名和字段名信息，选择需要进行敏感扫描的表和字段后，配置样本数、匹配率、扫描方式，点击确定按钮。

2、敏感类型敏感发现-任务执行：

手动执行：点点击列表中的开始按钮，任务进度从 0%到 100%变化，任务状态为‘已完成’后，任务执行成功。

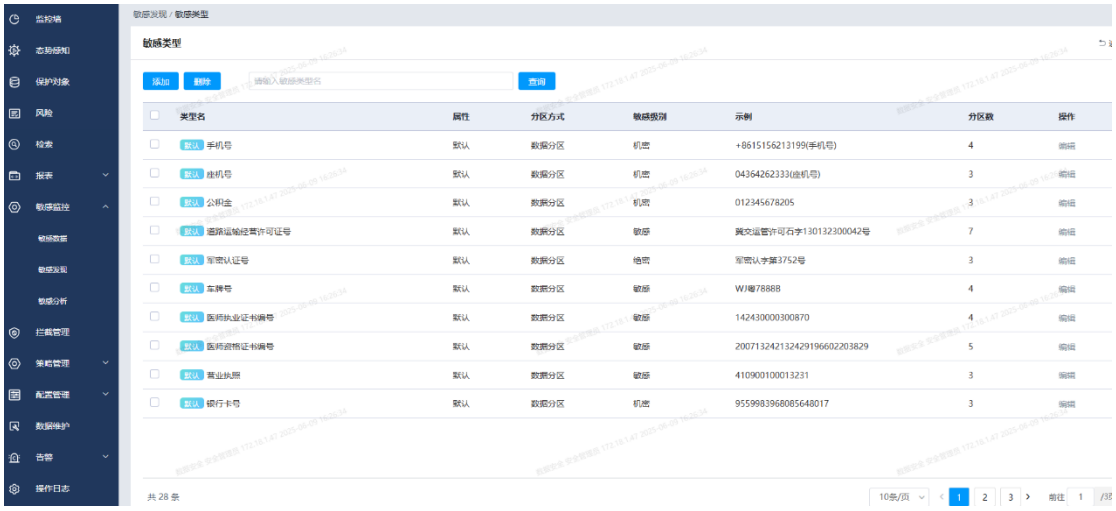
定时执行/周期执行：执行方式选择定时执行/周期执行时，时间到达设置的时间

点，则任务会自动执行。

3、敏感类型敏感发现-敏感任务发现结果：任务执行成功后，可以点击任务列表中的查看结果按钮，跳转到敏感任务发现结果页面，查看资产中的敏感数据。可输入表名或者字段名进行搜索查看。点击确认，将敏感发现的数据更新至敏感数据里。

5.7.2.2. 敏感类型

进入敏感发现页面，点击列表右上角的 按钮，进入敏感类型模块，查看敏感类型信息。系统有内置敏感类型，内置敏感类型不支持删除和修改。支持根据实际需要手动添加未内置到系统中的敏感类型。

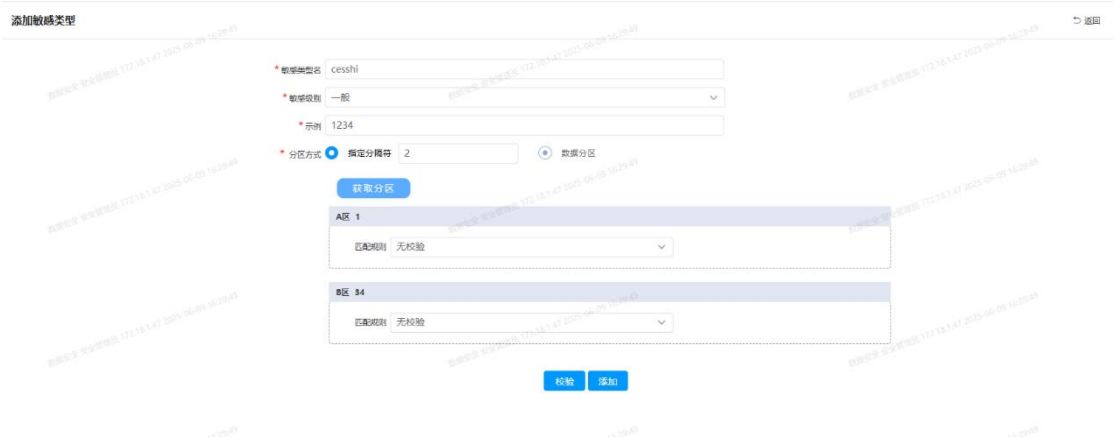


1、敏感类型-添加：

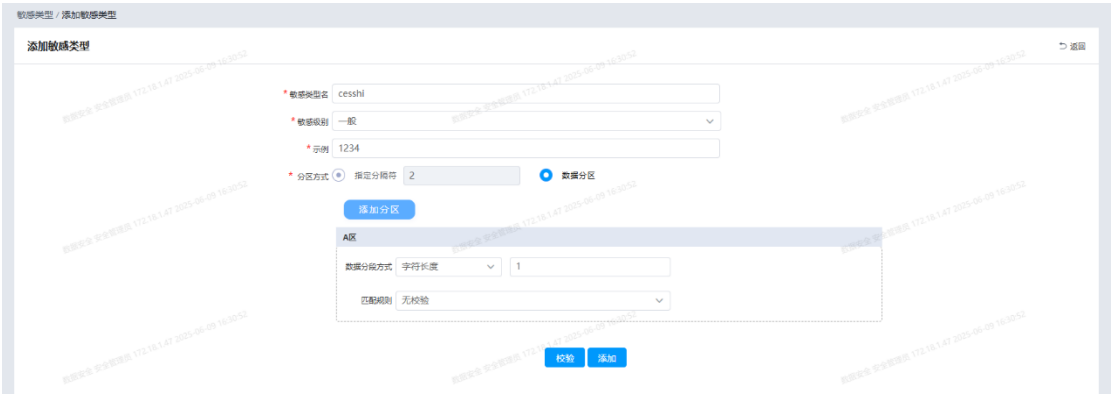
点击添加，跳转到“添加敏感类型页面”；首先填写敏感类型名、敏感级别、示

例，选择分区方式，点击添加，添加敏感类型。分区方式有两种

a、分区方式 - 指定分隔符：选择指定分隔符分区方式，并输入分隔符后，点击获取分区按钮 获取分区 ，获取分区信息。



b、分区方式-数据分区：选择数据分区方式，出现分区设置。点击添加分区按钮 添加分区 。



2、敏感类型-添加校验：输入敏感类型信息，并设置各分区的校验规则后，点击 校验 按钮，可以对各区间数据进行匹配，并弹出校验结果。

3、敏感类型 - 删除：勾选一条或多条自定义敏感类型，点击列表左上角的删除按钮 进行删除。

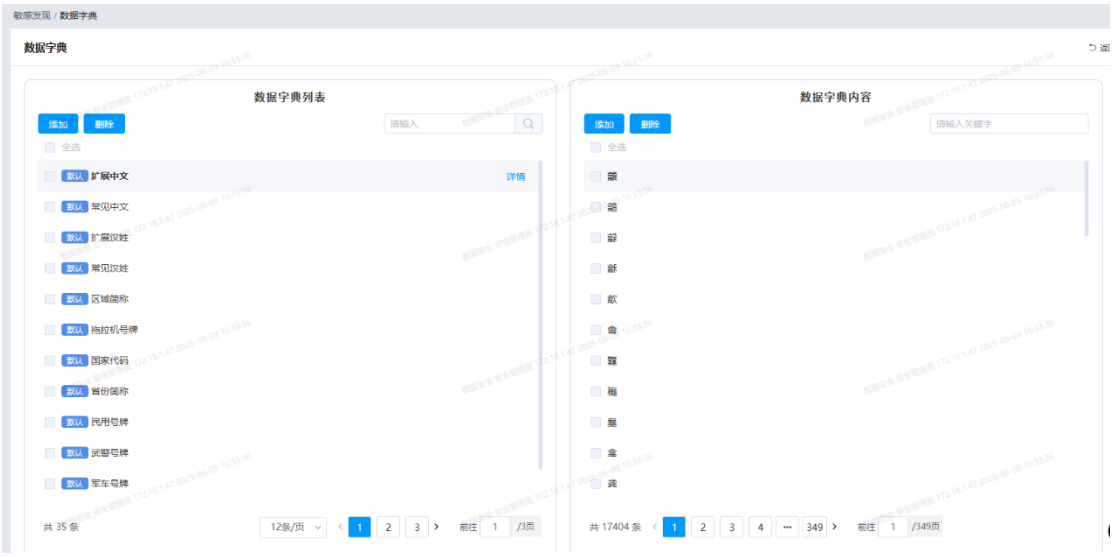
4、敏感类型-修改：点击列表右侧的编辑按钮，进入编辑页面，可进行相关信息的修改。内置敏感类型不可修改。

5.7.2.3. 数据字典

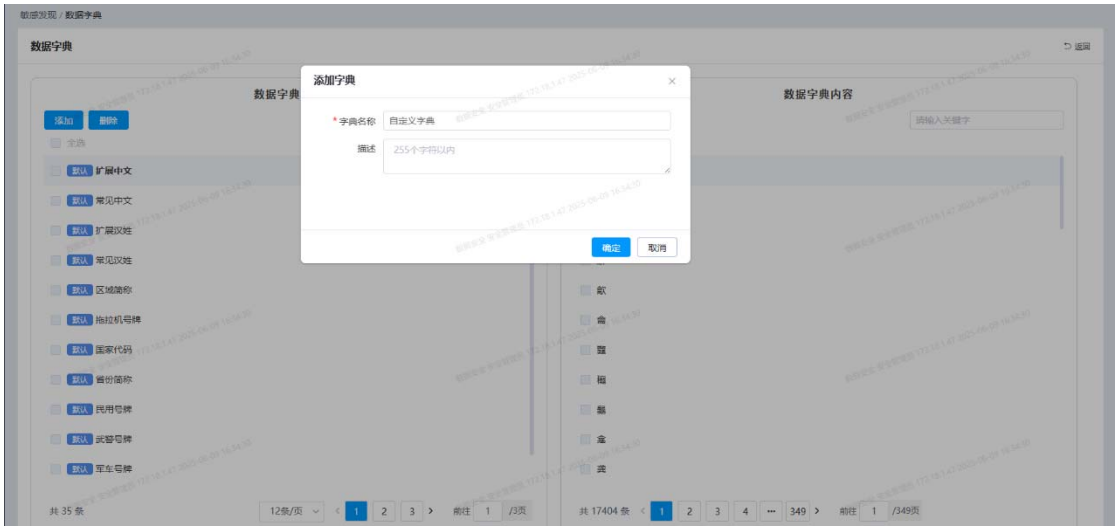
进入敏感发现页面，点击右上角

按钮，进入数据字典管理页面。

数据字典用于添加自定义敏感类型校验，匹配规则方式选择数据字典时使用，系统有内置数据字典，内置的数据字典不能删除与修改，支持根据需要自定义数据字典。



1、数据字典-添加：点击数据字典列表左上角的添加按钮，打开添加弹窗，输入正确的字典名称与描述，然后点击确定按钮进行添加。

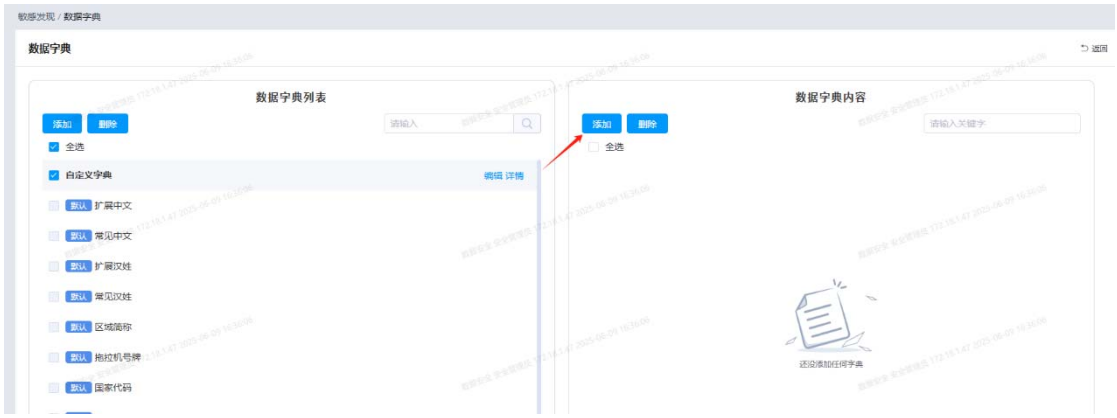


2、数据字典-删除：选择自定义的数据字典，点击列表右上角的删除按钮后，进行删除。内置的数据字典不可删除。

3、数据字典-修改：点击列表右侧的编辑按钮，打开修改弹窗，进行数据字典名称与描述的修改。内置的数据字典不可修改。

4、数据字典-详情：点击详情按钮，查看详情信息。

5、数据字典内容-添加内容：点击数据字典内容列表右上角的添加内容按钮，打开添加弹窗。

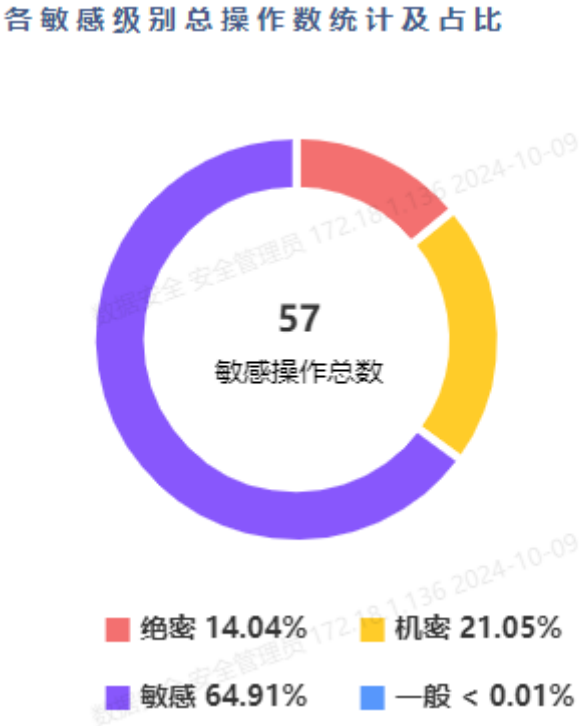


5.7.3. 敏感分析

敏感分析包含对敏感数据被访问的多维度分析报表，可根据时间、保护对象、源 IP 方式进行统计分析

1、敏感数据统计

各敏感级别总操作数统计及占比：这部分报表记录了操作敏感级别数据的总次数，以及各敏感级别的操作次数，可让用户直观的判断是否存在数据泄露风险。



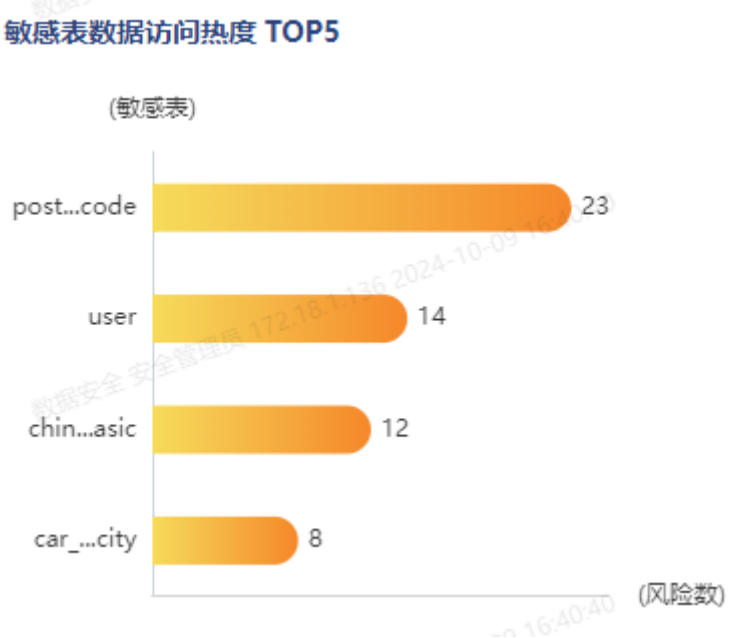
分类统计结果：这部分报表记录了操作保护对象敏感级别数据的总次数，以及各敏感级别的操作次数，让用户了解到具体保护对象是否存在数据泄露风险。

分类统计结果

保护对象	总操作数	绝密数据访问总数	机密数据访问总数	敏感数据访问总数
mysql_172.19.2.150	51	7	11	33
mysql_172.19.1.26	6	1	1	4

3、敏感数据访问热度统计及分析

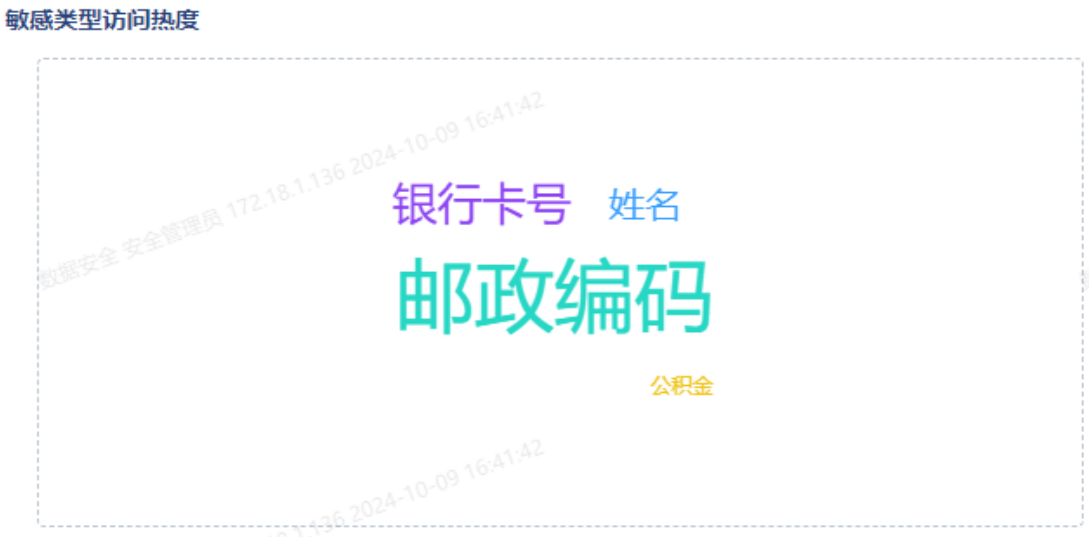
敏感表数据访问热度 TOP5：这部分报表记录了操作的具体敏感表，以及 TOP5 敏感表的操作次数，让用户了解到具体的数据表是否存在数据泄露风险。



敏感数据访问热 IP TOP5：这部分报表记录了操作敏感级别数据的具体 IP，以及各 IP 的操作次数，让用户了解到具体的 IP 是否存在数据泄露风险。

敏感数据访问热账号 TOP5：这部分报表记录了操作保护对象敏感级别数据的具体账号，以及账号对应的操作次数，让用户了解到具体的账号是否存在数据泄露风险。

敏感类型访问热度：这部分报表记录了触发的敏感类型名称，鼠标轻触展示敏感类型访问的次数。

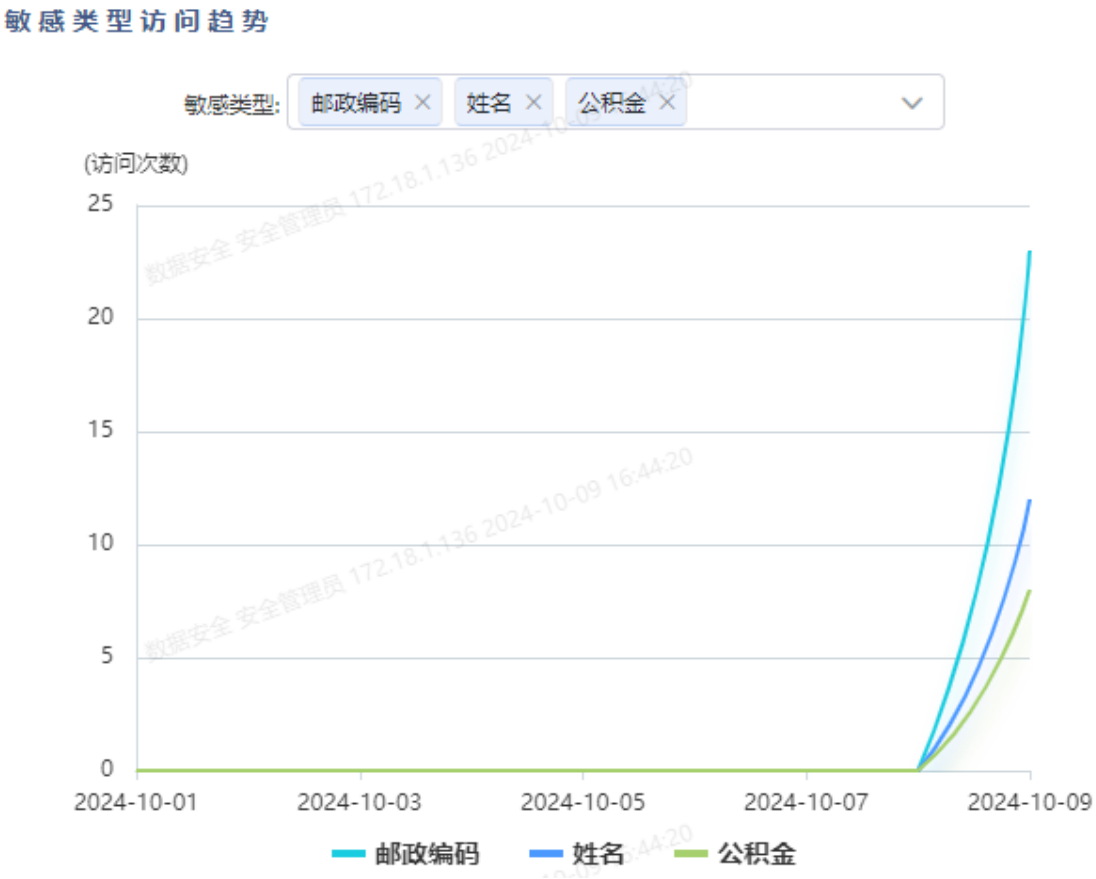


敏感级别访问热度：这部分报表记录了各敏感级别访问排行，以及各敏感级别的

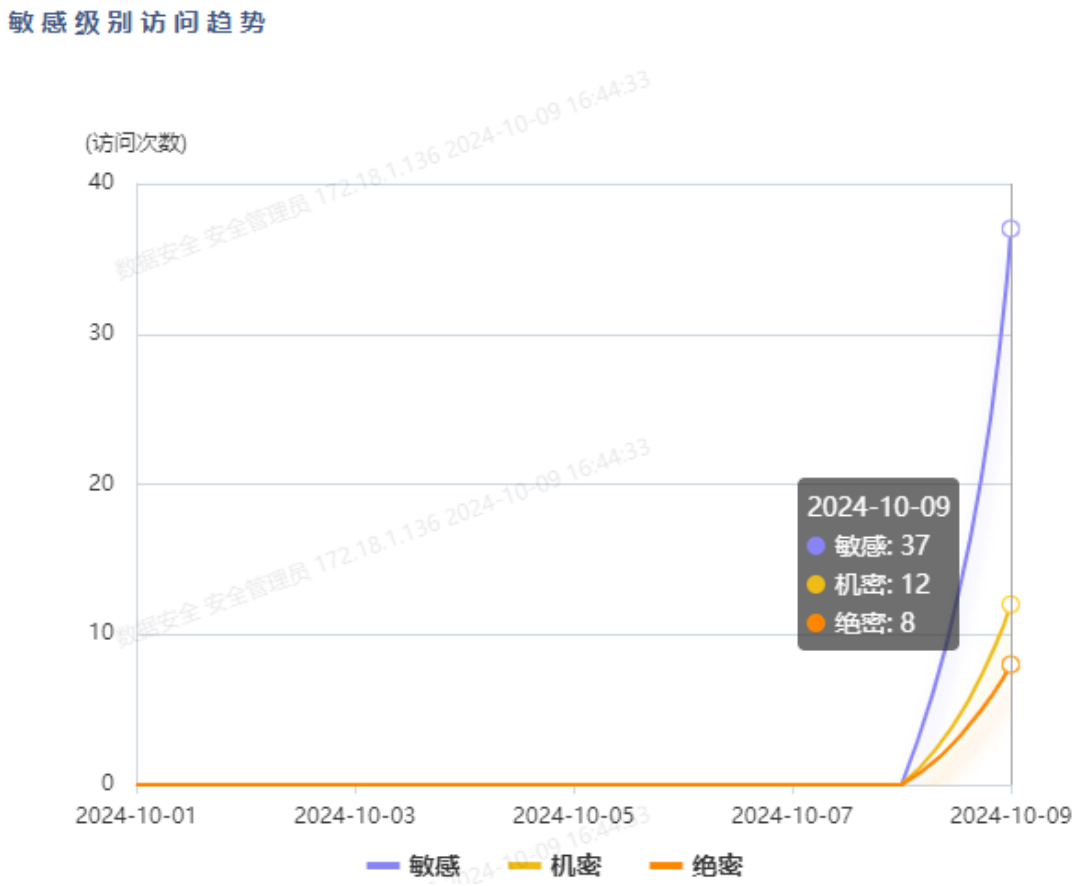
访问次数，让用户了解到是否存在数据泄露风险。

3、敏感数据访问趋势及分析

敏感类型访问趋势：这部分报表记录一个月每一天触发敏感类型的情况，以及各敏感类型的次数，直观看见触发敏感类型趋势图。



敏感级别访问趋势：这部分报表记录一个月每一天触发敏感级别的情况，以及各敏感级别的次数，直观看见触发敏感级别趋势图。



5.8 拦截管理

拦截管理中展示所有通过配置阻断规则和审计策略后被拦截的会话信息。

需要对客户端进行拦截时，可以按照如下步骤进行配置：

a. 添加动作为严格阻断的规则。

b. 将规则添加到保护对象关联的审计策略中，并在审计策略中开启阻断开关。

c. 当客户端执行了符合阻断规则的操作时，该客户端信息将被加入到阻断列表中。支持释放已被阻断的连接，在手动释放前，被拦截的客户端将不能继续操作数据库。

1、 查询

支持的查询条件包括“时间范围”， “审计对象”，“客户端 IP”，“服务端 IP”。

输入关键字后点击查询按钮可筛选出符合条件的数据。

2、 重置

支持使用重置按钮清除已选择的查询信息。

3、释放

支持勾选一个或多个被拦截的记录，点击释放按钮释放被阻断的客户端 ip。释放后该客户端 ip 可以继续操作数据库，但如果继续触发了阻断的规则，将会再次被阻断。

5.9 策略管理

5.9.1. 审计策略

审计策略是审计方式、规则、规则组的集合。所有的规则组、规则都需要添加到审计策略中，再将审计策略关联到保护对象后才能生效。保护对象通过应用不同的审计策略，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。

1、添加策略

点击添加按钮，输入策略名称和策略描述，选择审计方式，通过 < 和 > 按钮对规则组和规则进行删除和增加，点击“确定”按钮完成审计策略的添加。

字段填写说明：

策略名称	用于策略命名。
策略描述	用于对策略进行简要说明。
审计方式	全审计：表示审计所有操作，不能匹配规则的操作风险等级记为信息。 按规则审计：表示只记录匹配审计规则的操作，其余均不记录。
单向审计	表示只审计操作的请求信息，不审计返回结果，增加审计效率。
阻断	可以阻断触发规则的操作，需要配合规则动作中的宽松阻断或严格阻断使用。
规则	展示已选择的规则和可选择的规则列表。鼠标悬停在规则名

	称上，可点击编辑按钮跳转至规则页面，修改规则信息。
规则组	展示已选择的规则和可选择的规则组列表。鼠标悬停在规则组名称上，可点击编辑按钮跳转至规则组页面，修改规则组信息。

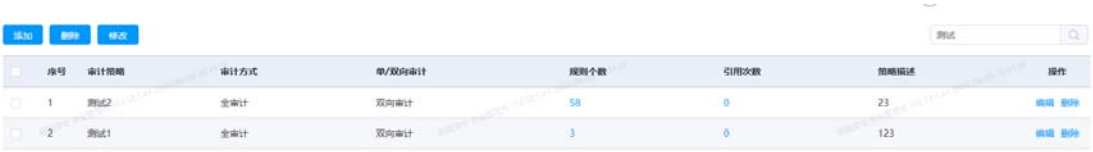
2、批量操作

审计策略支持删除和修改的批量操作。点击策略左上角的复选框选择需要进行批量操作的策略，或者点击全选选中所有策略；点击批量删除按钮可以删除所有选中的策略，点击批量修改按钮可以批量修改审计方式和单向审计。

注意：默认策略无法被删除，但可以被修改

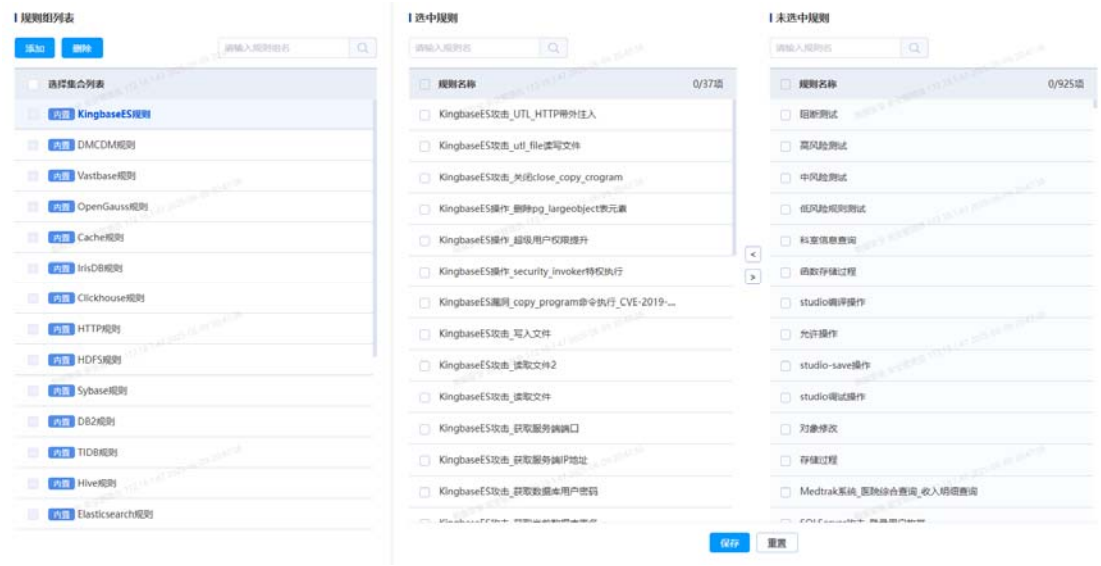
3、查询

在输入框输入审计策略名称可以筛选符合条件的审计策略。



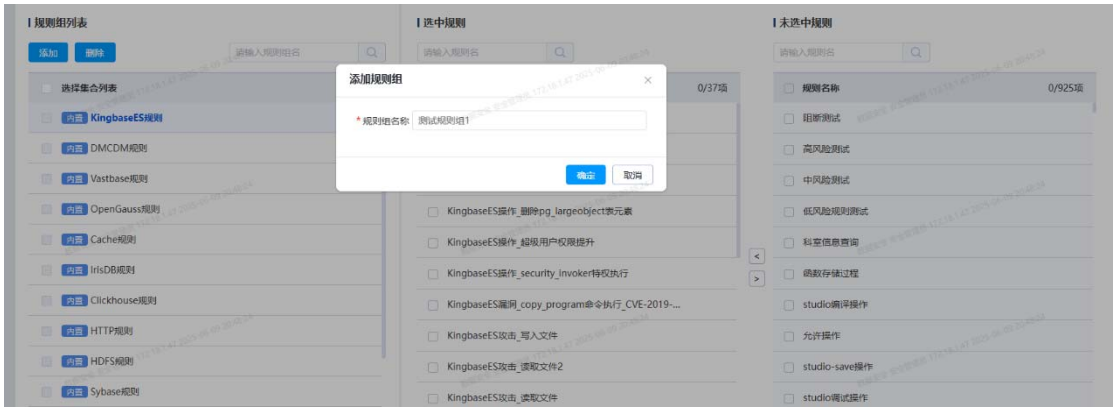
5.9.2. 规则组

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。



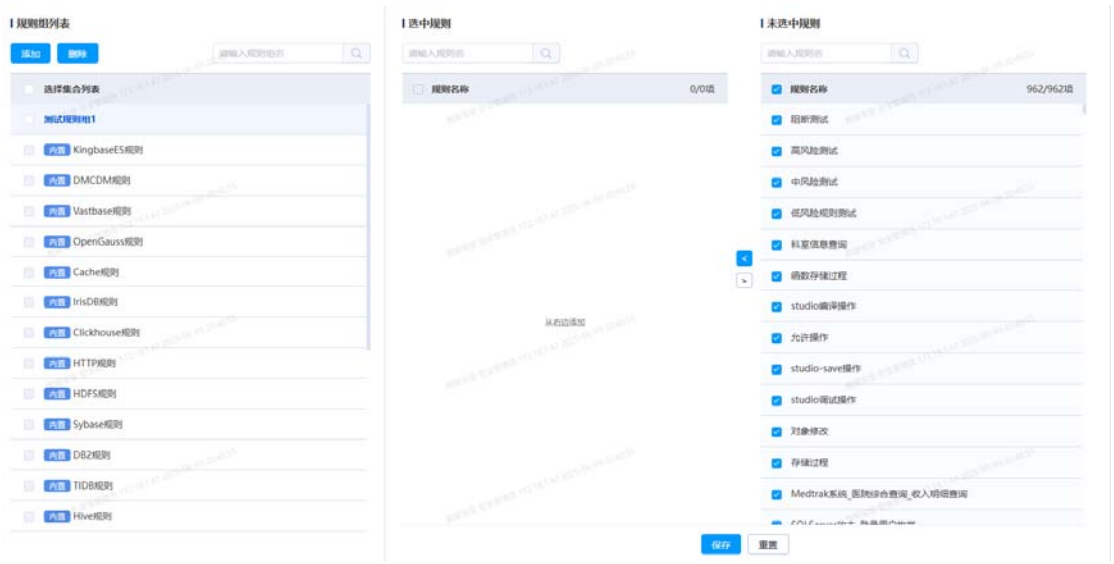
1、添加规则组

点击“添加”按钮，输入规则名，点击“确定”即可完成一个规则组的添加。



2、规则组中添加规则

选择规则组，在右侧“未选中规则”列表勾选需要的规则，点击 < 按钮将规则添加到“选中规则”，在“选中规则”中勾选后点击 > 按钮移除规则，点击“保存”按钮完成规则组的添加。



3、删除操作

在规则组列表中勾选一个或多个非内置的规则组，点击删除并确定即可删除选中的规则组。

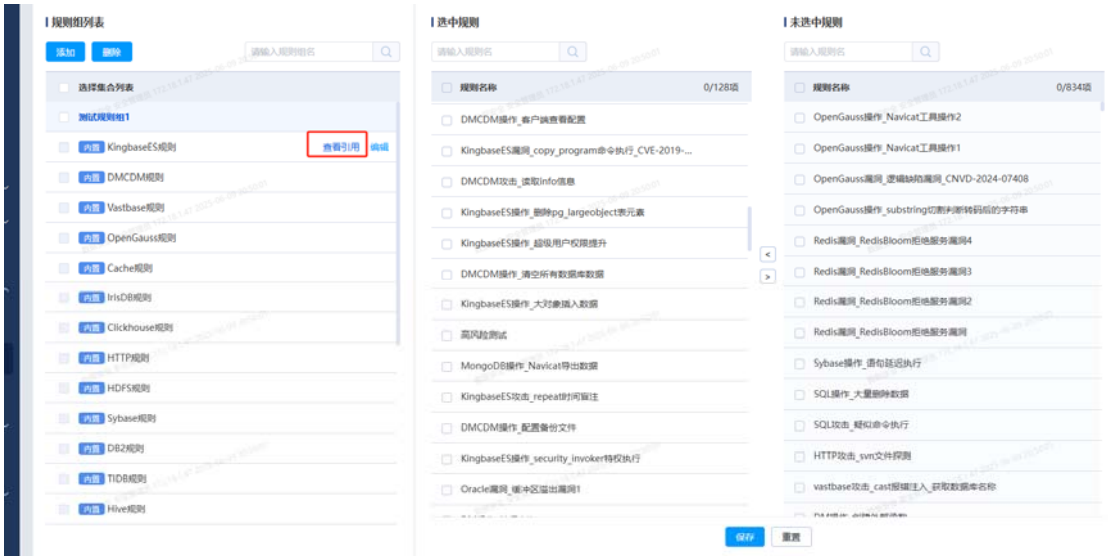
注意：内置规则组无法被删除和修改。

4、查询

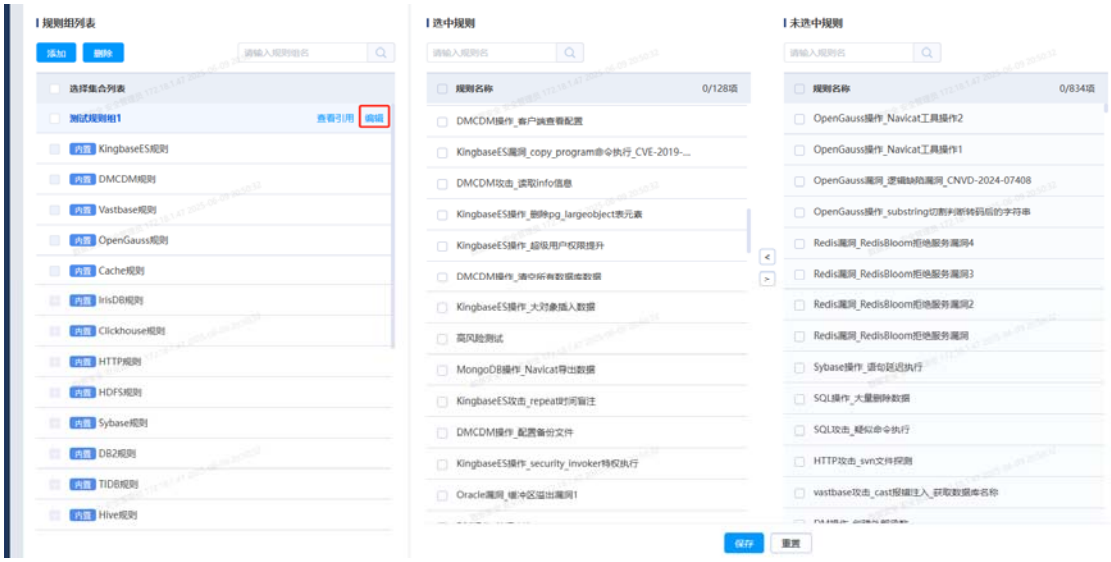
在各列表中输入关键字可对列表数据进行查询。

5、其他操作

查看引用：鼠标悬停在规则组名称上，点击“查看引用”可以查看所有引用该规则组的审计策略名称。



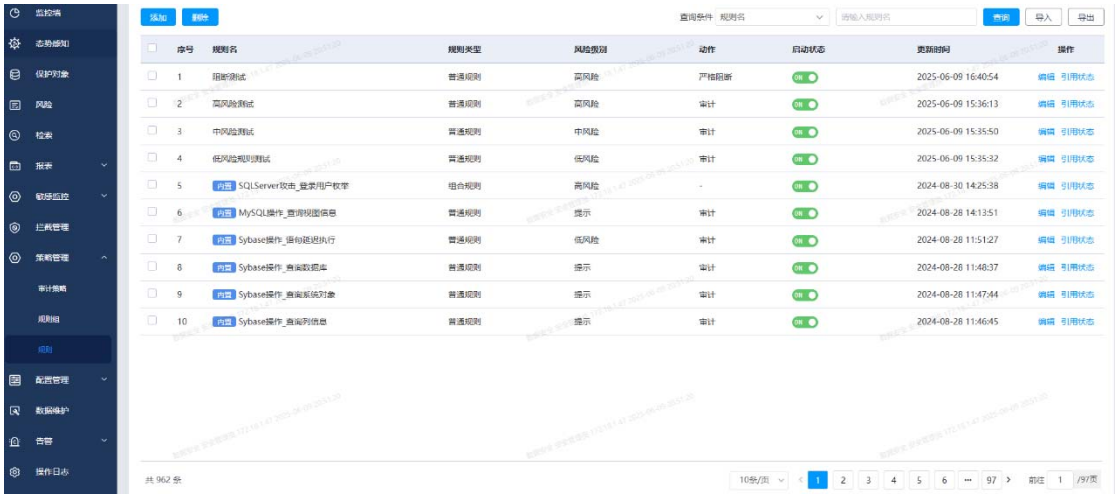
编辑：鼠标悬停在规则组名称上，点击“编辑”可以修改对应的规则组名或者规则的属性。



重置：点击重置按钮可以清除所有未保存的修改操作。

5.9.3. 规则

规则是审计策略的最小单位，所有操作的审计都可以通过配置对应的规则来完成风险匹配，灵活运用规则可以大大提高审计的效率和准确性。



1、添加规则

点击添加按钮，选择规则信息，点击“确定”按钮完成规则的添加。添加规则支持手动添加和导入两种方式。

a、手动添加

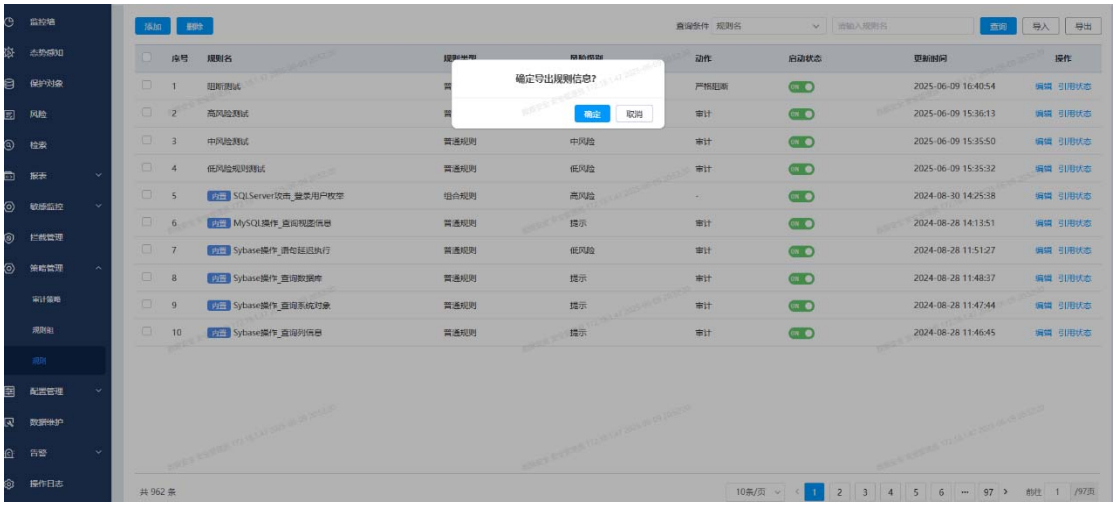
字段填写说明：

规则名	用于规则命名。
状态	默认为“ON”状态。可以手动修改为“OFF”，修改为“OFF”后审计操作不再匹配该规则。
规则类型	规则类型包含普通规则和组合规则。普通规则为基础规则，组合规则分为触发类型为“组合”和“统计”的规则。触发类型为“组合”的组合规则需要设置时间范围并任意选择至少 2 个普通规则，当审计数据在设置的时间范围内同时触发选择的所有普通规则时，会再生成一条触发组合规则的记录，记录的规则为组合规则名。触发类型为“统计”的组合规则需要设置时间范围、统计次数和任意一个普通规则，当审计数据在设置的时间范围内触发选择的普通规则次数达到设置值时，会再生成一条触发组合规则的记录，记录的规则为组合规则名。
风险级别	风险级别包含高风险，中风险，低风险，提示，信息。普通规则和组合规则均可以任意选择。
操作类型	操作类型列表展示【操作类型】页面配置的所有操作，例如 select，insert，update，delete 等
动作	动作表示匹配规则后需要执行的操作，包含审计，不审计，严格阻断，宽松阻断
关键字审计	根据设置的关键字在审计的操作内容中进行匹配，例如表名，数据库名，用户名等
备注	可以设置规则的备注信息
访问工具	通过访问工具进行规则匹配。支持选择配置管理中配置的访问工具集合或基础元素
客户端	通过访问的客户端 IP 进行规则匹配。支持选择配置管理中配置的客户端 IP 集

IP	合或基础元素
客户端 MAC	通过访问的客户端 MAC 进行规则匹配。支持选择配置管理中配置的客户端 IP 集合或基础元素
操作系统主机名	通过访问的操作系统主机名进行规则匹配。支持选择配置管理中配置的操作系统主机名集合或基础元素
操作系统用户名	通过访问的操作系统用户名进行规则匹配。支持选择配置管理中配置的操作系统用户名集合或基础元素
应用账户名	通过访问的应用账户名进行规则匹配。支持选择配置管理中配置的应用账户名集合或基础元素
数据库对象	通过访问的数据库对象进行规则匹配。支持选择配置管理中配置的数据库对象集合或基础元素
最大操作语句长度	通过操作的语句长度进行规则匹配。可以选择大于等于或小于，并输入 0-99999999 的数字
正则表达式	通过正则表达式进行规则匹配。支持输入长度为 500 以内的字符
正则测试	可以输入执行语句，点击测试按钮检查语句和正则表达式是否匹配
统方时间	通过语句中的时间范围进行规则匹配。支持按照大于等于、小于等于、时间段、本日、本周、七日内、本月进行选择
开始时间字段	通过语句中时间开始字段进行规则匹配。用于计算执行语句中查询的时间开始范围
结束时间字段	通过语句中时间结束字段进行规则匹配。用于计算执行语句中查询的时间结束范围
Sql 语句执行回应	通过 sql 语句的执行结果进行匹配。可以按照等于或不等于匹配成功或失败
语句执行时间	通过 sql 语句执行的时长进行匹配。单位为毫秒。可以选择大于等于或小于，并输入 0-99999999 的数字
返回行数阈值	通过 sql 语句执行后的返回行数进行匹配。可以选择大于等于或小于，并输入 0-9999 的数字
返回内容	通过 sql 语句执行后的返回内容进行匹配。可以输入 255 范围内的字符
规则生效时间	通过访问的时间进行规则匹配。支持选择配置管理中配置的规则生效时间集合或基础元素

b、文件导出、导入

点击“导出”按钮可将规则导出到 Excel 文件中。支持通过勾选一个或多个规则，选择要导出的规则信息；未勾选规则，则导出列表中所有规则；



支持规则的导入，根据模板填写规则名称、操作类型、风险级别等信息。

	基础规则						
规则名称(必填)	操作类型	风险级别(必填)	规则状态	规则动作	匹配规则	关键字审计	正则表达式
delete	delete	高	开启	审计			

点击“导入”按钮可以将 Excel 中的规则信息导入到规则列表。导入的文件类型只支持 xlsx 格式的 Excel 文件。

注意：只支持普通规则的导入导出，不支持组合规则的导入导出。

2、删除规则

在规则列表中勾选一个或多个自定义的规则，点击删除按钮并确定即可删除选中的规则。

注意：默认规则无法被删除和修改。

3、查询

规则的查询条件包含“规则类型”，“启用状态”，“规则级别”，“规则名”，输入关键字后点击查询按钮可筛选出符合条件的数据。

4、其他操作

启动状态：点击 ON 按钮可以修改规则的状态。

修改：点击“编辑”按钮可以对规则内容进行修改。

引用：点击“引用状态”按钮可以展示所有引用该规则的审计策略、规则组和组合规则。

5.10 配置管理

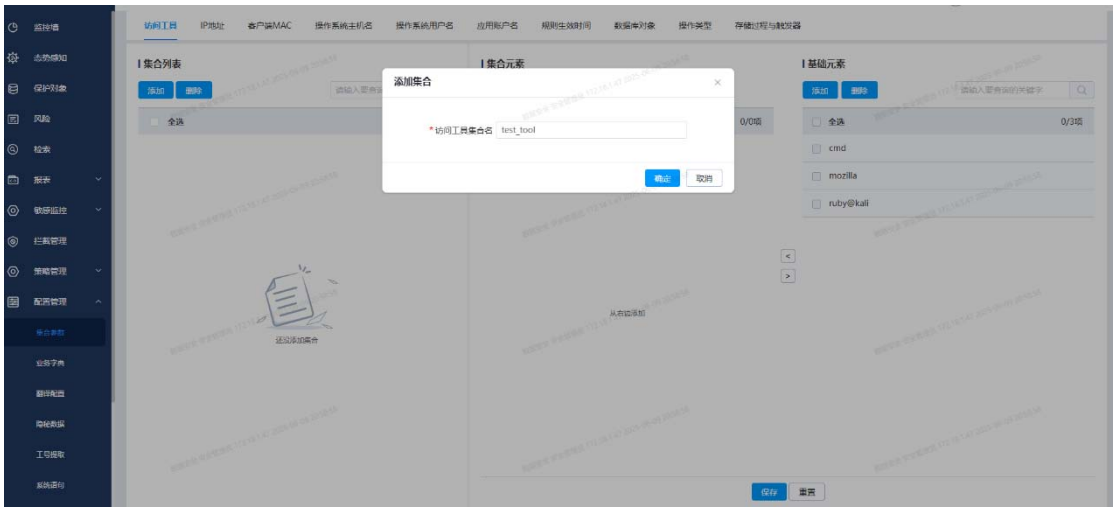
5.10.1. 集合参数

集合配置中可以配置访问工具、IP 地址、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名等操作主体信息及规则生效时间、数据库对象、操作类型、存储过程与触发器的集合和基础元素，方便在检索中作为搜索条件过滤审计结果，也可以应用到【规则】中作为规则的高级配置项。

5.10.1.1. 主体信息

主体信息包括访问工具、IP 地址、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名等信息，可以分别添加集合和基础元素，并将基础元素可以添加到集合中。

以访问工具为例，在访问工具中添加一个名为 navicat 的集合，并将基础元素 navicat 关联到集合中。



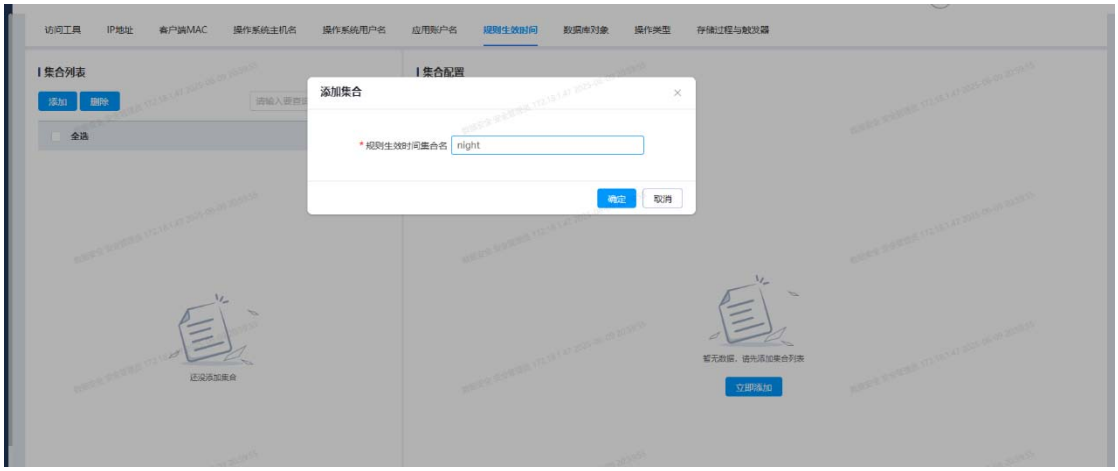
添加完成后，在规则的高级配置访问工具字段，可以选择名称为 navicat 的集合或基础元素。

将规则关联到保护对象的审计策略后，使用 navicat 客户端，对保护对象进行操作将被审计为匹配规则，使用其他工具的访问信息将不会审计为匹配规则。

注意：审计记录中的规则信息将会自动添加到基础元素中，如果已经添加，则不再重复添加。

5.10.1.2. 规则生效时间

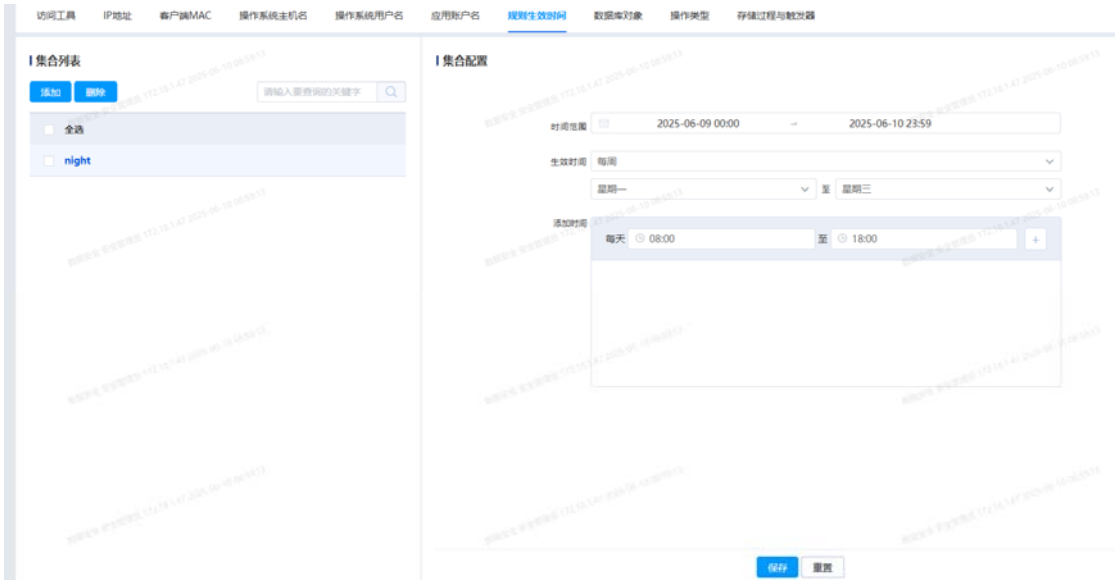
通过设置生效时间，控制规则在时间段内生效或不生效。



对新添加的规则生效时间集合进行配置，字段填写说明：

时间范围	支持选择任意时间段
生效时间	每周和每月的配置
添加时间	支持任意添加多个时间段

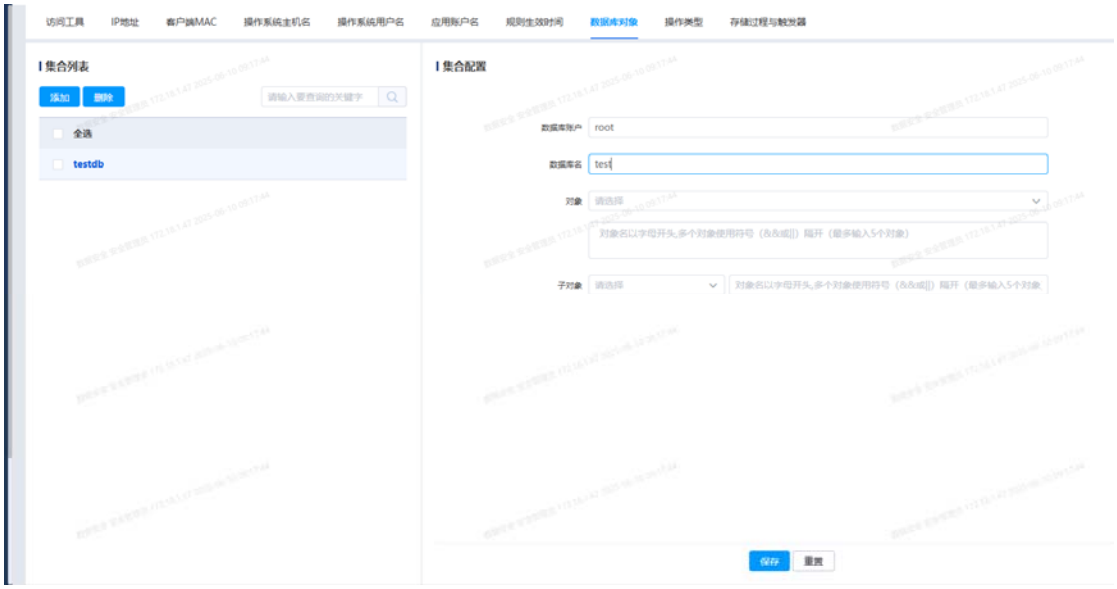
配置示例如下:



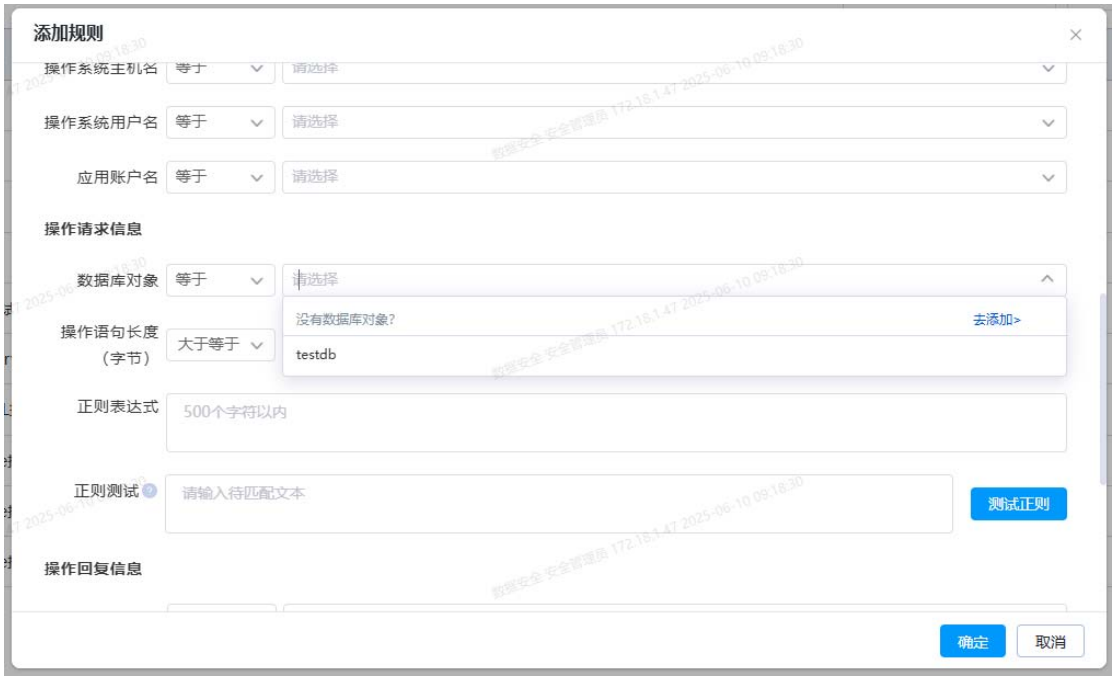
添加完成后，在【规则】的高级配置中选择规则生效时间集合，保存后对保护对象的操作只有在 2025-06-09 08:00 到 2025-06-10 18:00，每周一到周三的 8 点到 18 点才能触发规则。

5.10.1.3. 数据库对象

提供精确到数据库账户、数据库名、对象（表）、子对象（字段）的规则配置。如用户想让数据库账户 testuser 对数据库 testdb 执行关于 test 表的操作时触发风险，可以在数据库对象中点击“添加”按钮添加集合，配置以下信息：



点击保存后，配置生效。添加规则时，在高级配置中可以引用数据库对象集合配置，选择等于，则所有的操作需要先满足配置的数据库对象才能触发规则，选择不等于，则所有操作需要先不满足配置的数据库对象才能触发规则。



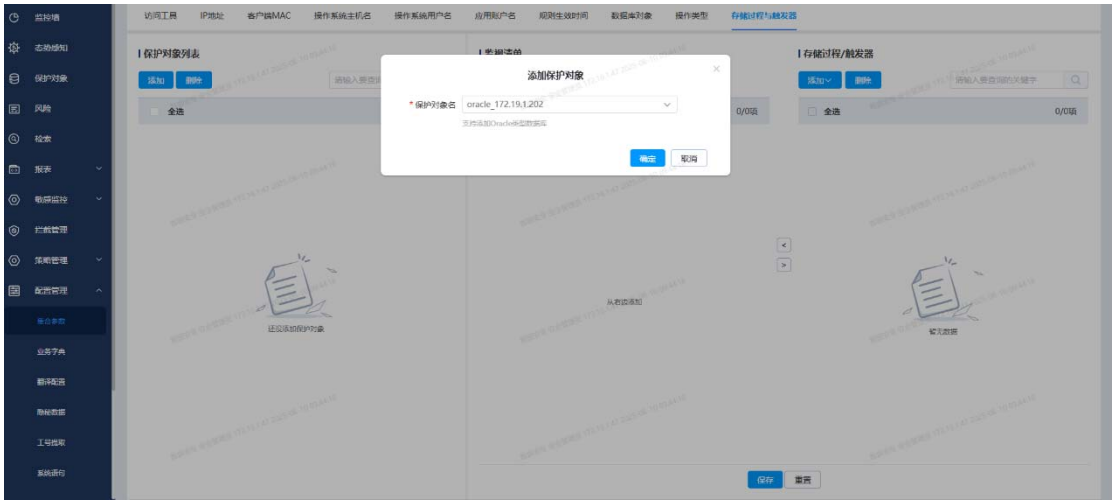
5.10.1.4. 操作类型

系统内置了常见的 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，也可以根据需要添加未内置的操作类型，内置和自定义的操作类型都可以在规则中引用。

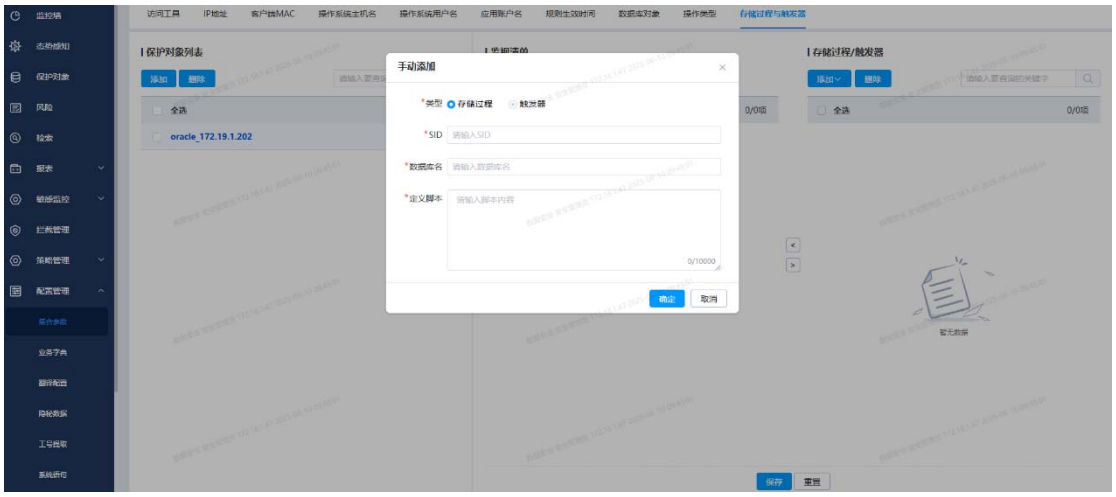
5.10.1.5. 存储过程与触发器

用于配置保护对象的存储过程与触发器信息。支持选择保护对象，并添加、删除、修改、查询保护对象的存储过程与触发器。

点击添加按钮可以添加保护对象集合。保护对象列表展示保护对象页面已添加的所有 Oracle 数据库。

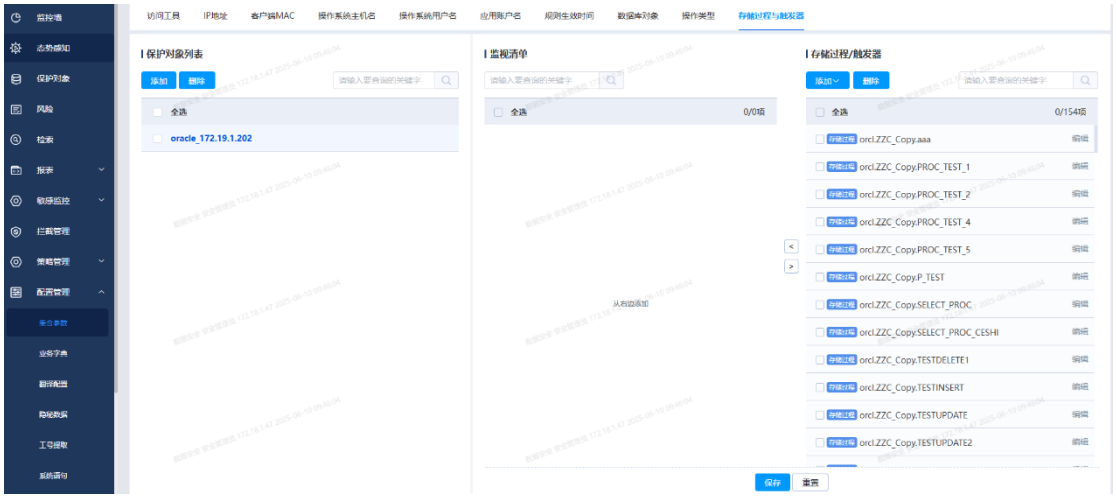


手动添加存储过程或触发器:选中添加的保护对象，点击添加按钮选择手动添加存储过程和触发器信息。

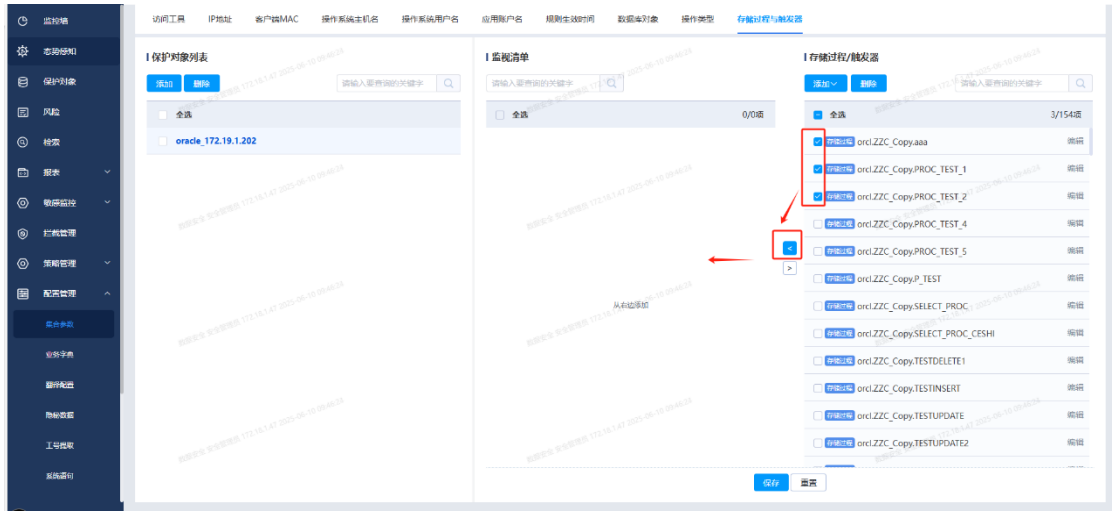


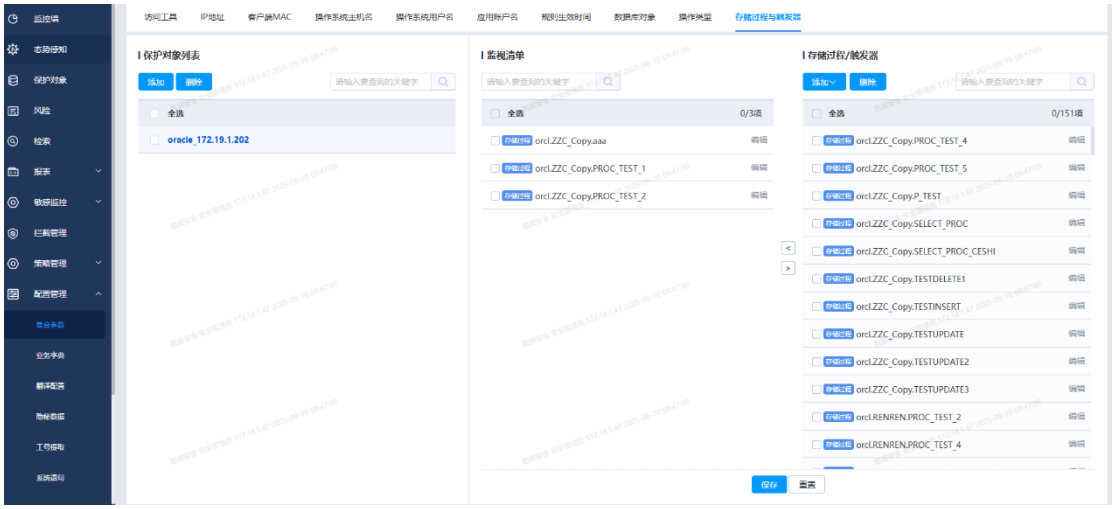
自动获取存储过程或触发器：选中添加的保护对象，点击添加按钮选择自动获取数据库中的存储过程和触发器信息。获取操作需要使用数据库连接信息，根据【保护对象其他操作】配置保护对象扩展配置后才能进行自动获取。

自动获取添加成功后，列表自动展示数据库中的存储过程和触发器信息。

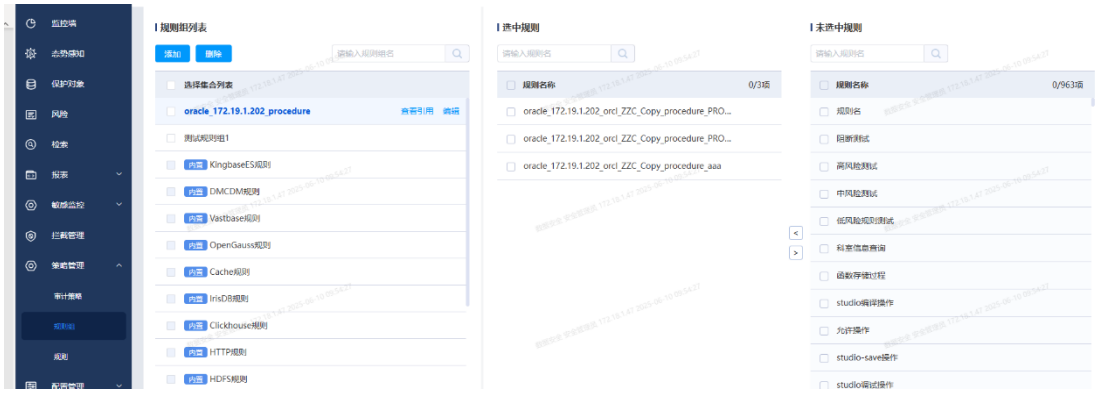


选中一个或多个存储过程和触发器，点击 < 按钮将存储过程和触发器添加到监视清单中，点击保存。



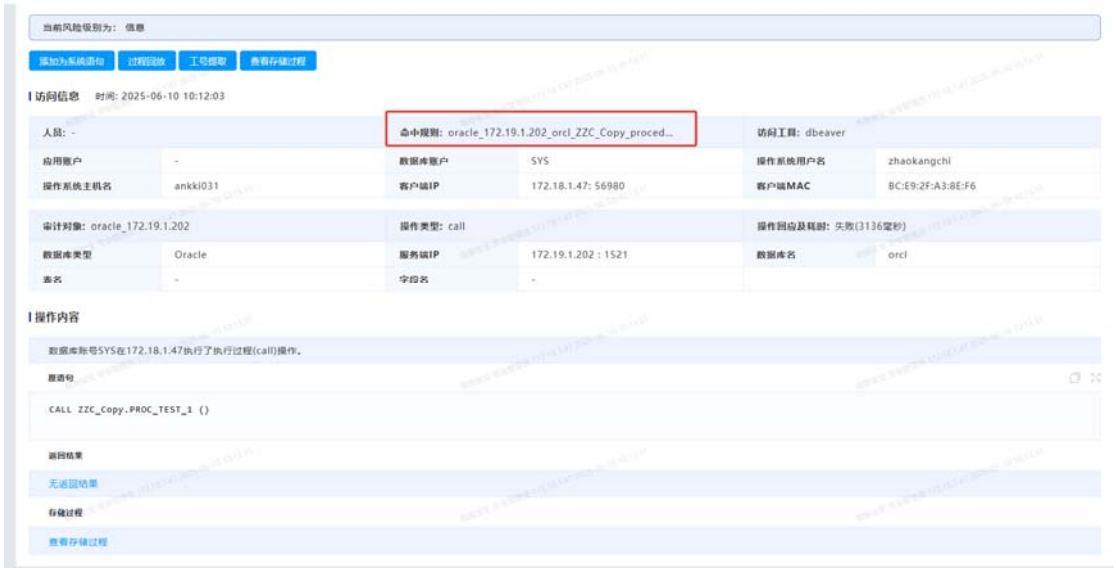


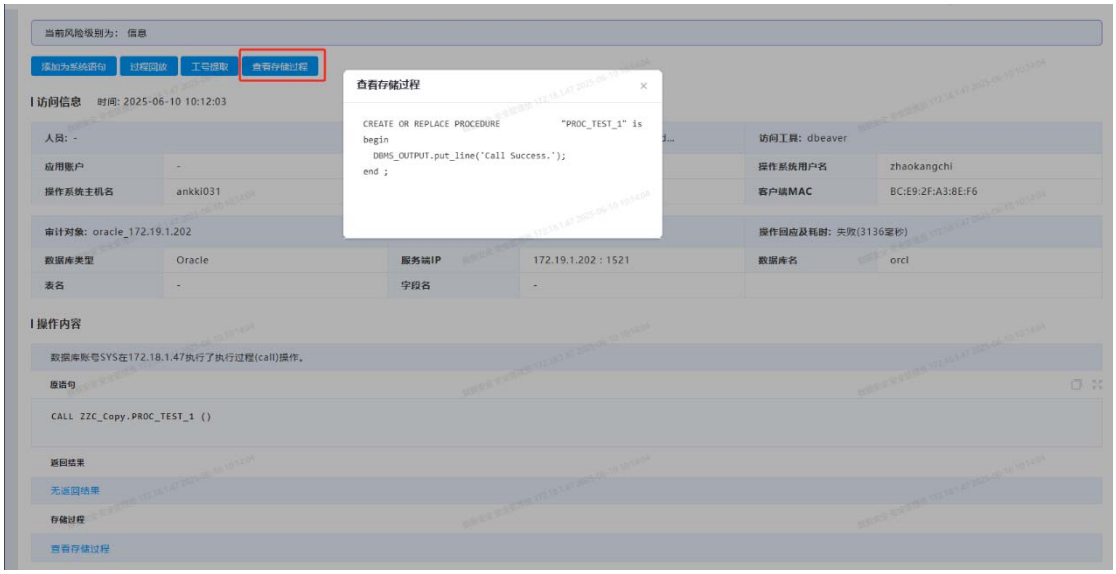
保存后每个存储过程或触发器均会生成单独的规则，且按照存储过程或触发器对应的保护对象自动生成规则组，并将规则自动加入到规则组中。



将规则或规则组添加到保护对象关联的审计策略中，操作存储过程或触发器时可以生成审计记录并匹配规则。

操作数据库执行存储过程或触发器时，审计记录能匹配到对应的规则并记录触发器信息。



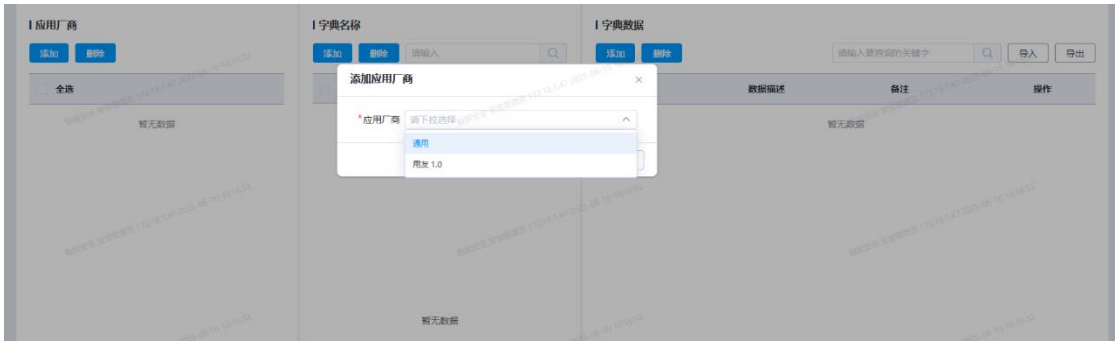


5.10.2. 业务字典

业务字典中是对不同业务厂商的字典数据的翻译集合，用于实现保护对象内部表字段与业务字段之间的映射与翻译。

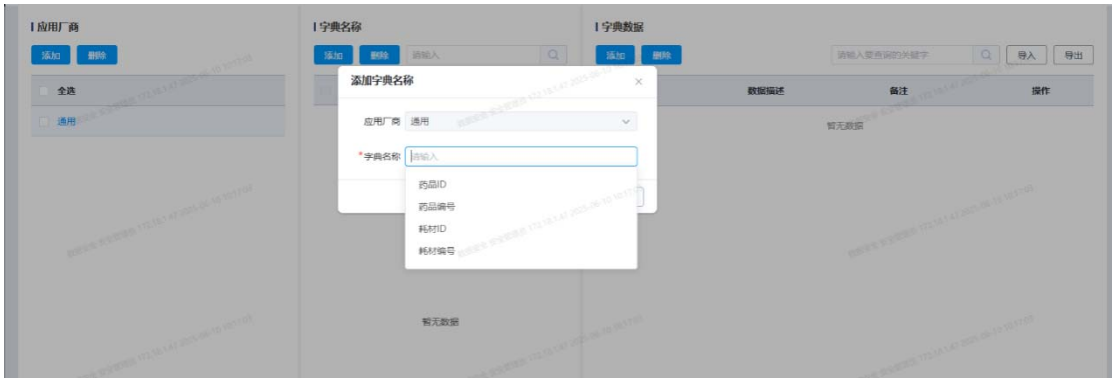
1、添加应用厂商

点击“添加”按钮，选择应用厂商，点击“确定”按钮。应用厂商列表展示通用和其他被保护对象关联的 HIS 厂商。



2、添加字典名称

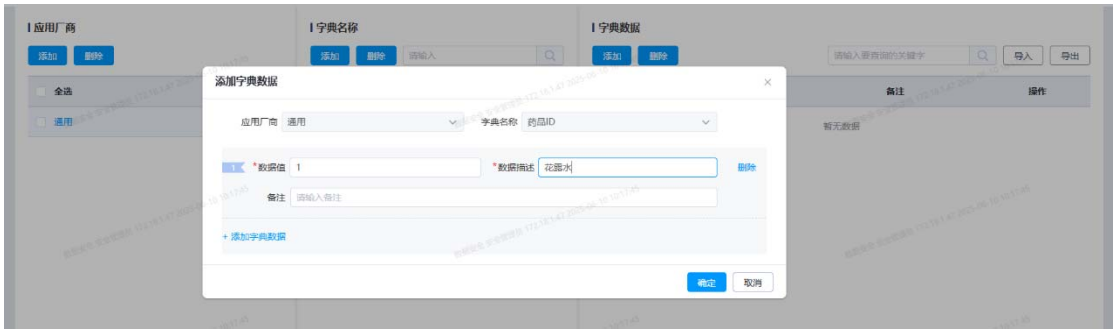
选中已添加的应用厂商，在“字典名称”列表点击“添加”按钮，在列表中选择字典名称。字典名称目前仅支持选择“药品 ID”、“药品编号”、“耗材 ID”、“耗材编号”。



3、添加字典数据

选中已添加的字典名称，在“字典数据”列表点击“添加”按钮，输入药品编

号、药品名称、药品厂商后保存。



4、编辑字典数据

选中字典数据，点击“编辑”按钮，可以修改字典数据信息。

5、删除数据

在应用厂商、字典名称、字典数据列表中勾选一个或多个数据后，均可以点击删除按钮进行数据删除。

6、查询

选中应用厂商和字典名称后，在字典数据列表输入框中输入关键字，可以查询字典数据。

7、导入和导出

导出业务字典。点击“导出”按钮可将业务字典信息导出到 Excel 文件中。支持通过应用厂商、字典名称、字典数据进行数据勾选，并导出选中的数据；未勾选任何数据时，则导出列表中所有业务字典；

导入业务字典。点击“导入”按钮可下载模板，完成模板填写后可将模板中的业务字典信息导入到列表中。

5.10.3. 翻译配置

5.10.3.1. 表对象翻译

表对象翻译会将检索结果中对应的表名、字段名、关键字进行翻译，方便识别和查看。表对象别名添加分为手动添加和自动获取两种方式。

1、手动添加

点击“添加”按钮，选择需要翻译的保护对象，配置数据库名、表名、字段名等翻译信息，保存后将立即对检索页面的表对象信息进行翻译。

例如要把保护对象的数据库 test 的 products 表设置为关键表，且翻译为“商品表”，字段 id 翻译为“产品编号”，配置如下：

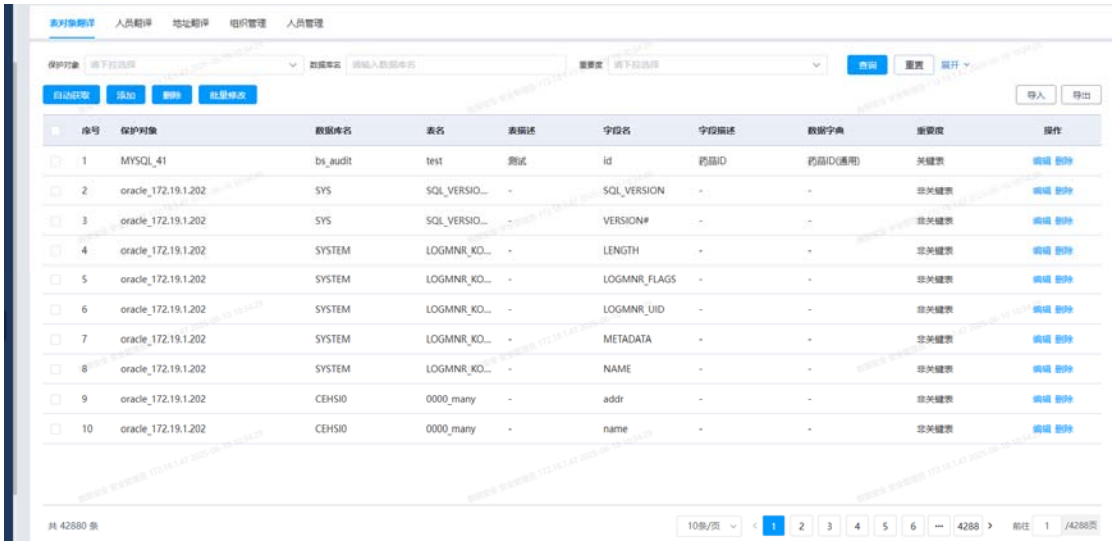
字段填写说明：

保护对象	选择范围为保护对象列表中未关联 his 厂商的保护对象名称，和已关联 his 厂商的 his 厂商名称，显示格式为 his 厂商名称（保护对象名称 1，保护对象名称 2）。
数据库名	需要翻译的表和字段对应的数据库名
表名	需要翻译的表名
重要度	选择范围为关键表和非关键表。检索记录中仅对关键表进行翻译
表描述	表名翻译后的内容
字段名	需要翻译的字段名
字段描述	字段翻译后的内容。支持选择预制的字段描述，或手动输入其他描述信息

添加完成后，查询保护对象 test 库的 products 表的 id 字段，在检索中查看翻译结果。

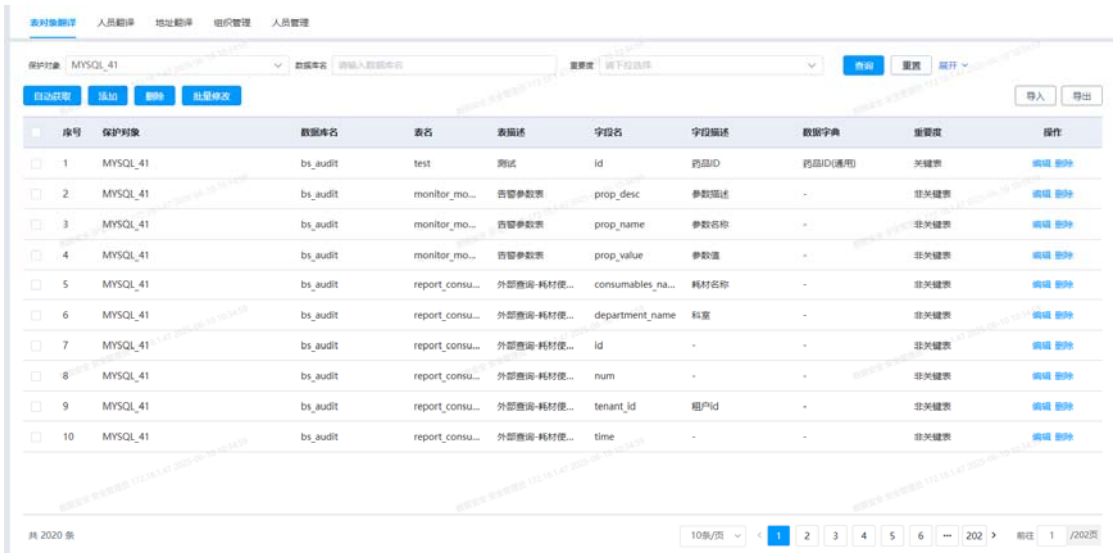
2、自动获取

点击“自动获取”按钮选择自动获取数据库中的表对象信息。获取操作需要使用数据库连接信息，根据【保护对象其他操作】配置保护对象扩展配置后才能进行自动获取



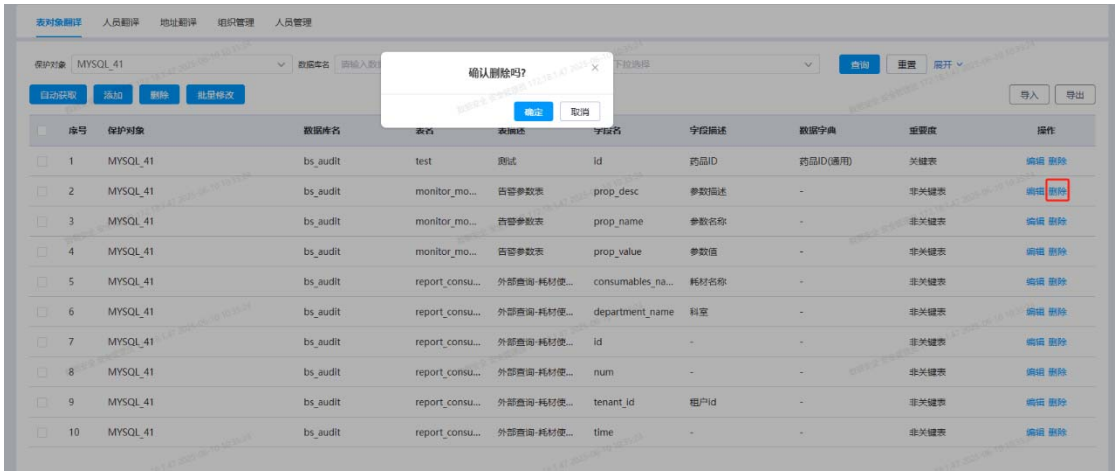
3、查询

输入查询关键字可以查询表对象信息。输入表对象信息后点击“重置”按钮可以清除输入的查询信息。

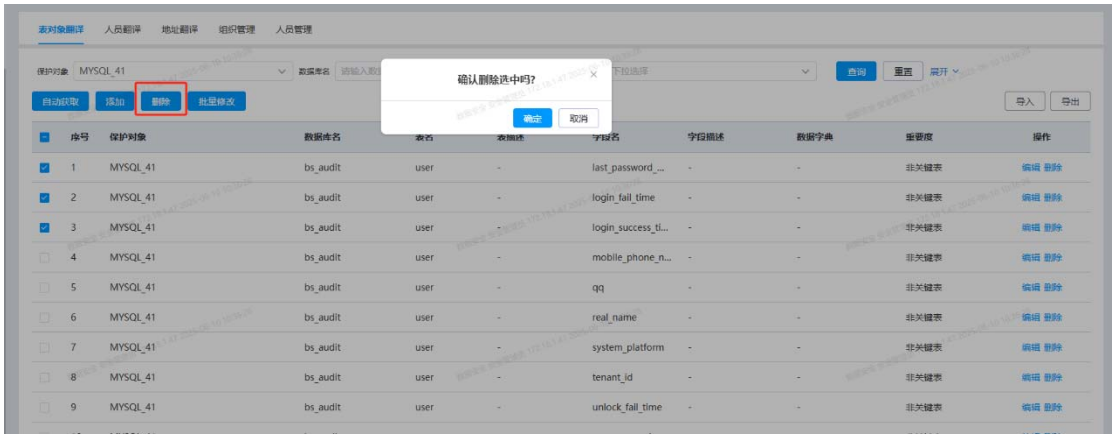


4、删除

支持选中一条数据后，点击“操作”栏的“删除”按钮，删除单条翻译数据。

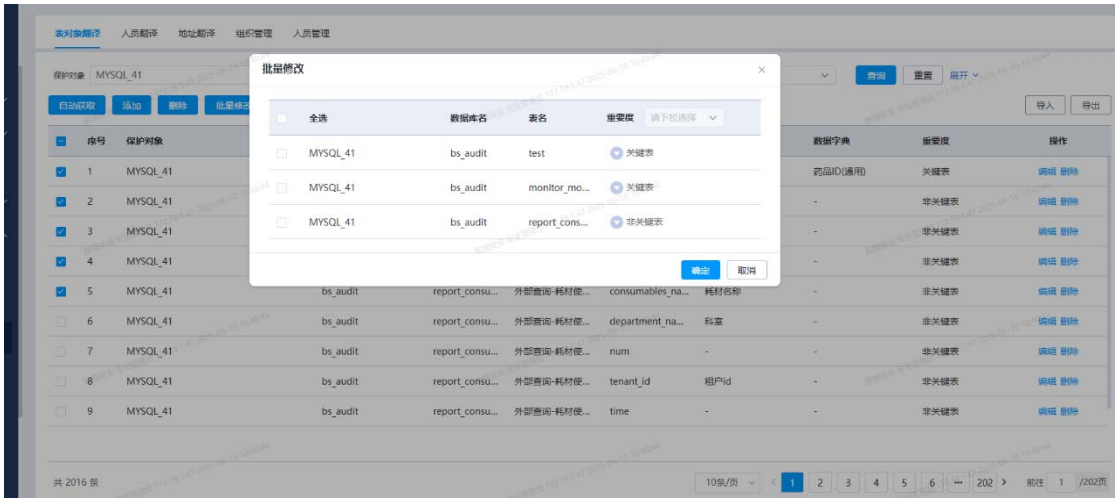


选中一条或多条表对象翻译数据，点击“删除”按钮批量删除选中的数据。



5、批量修改

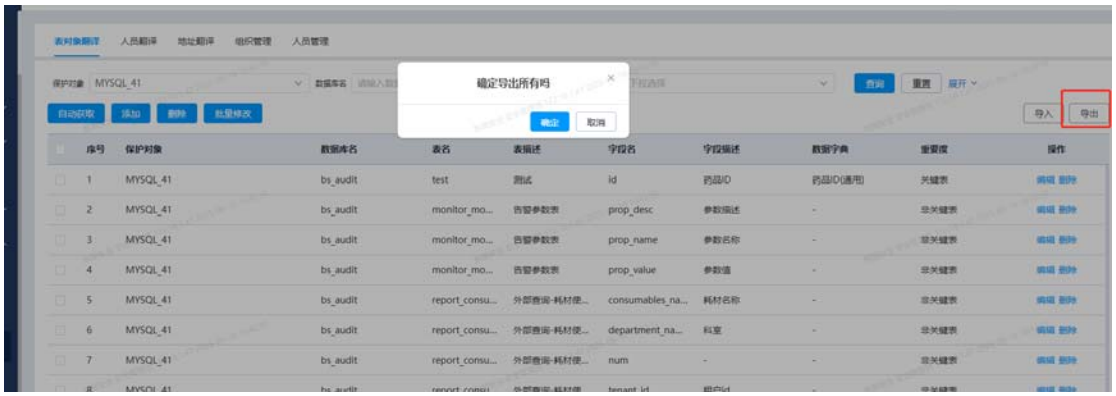
选中一条或多条表对象翻译数据，点击“批量修改”按钮可以批量修改翻译信息。



批量修改页面仅支持对重要度的修改。可以勾选数据后批量修改重要度，也可以依次修改单条数据的重要度。

6、导入和导出

支持表对象信息的导出。点击“导出”按钮可将表对象翻译数据导出到 Excel 文件中。支持勾选一条或多条数据，并导出选中的数据；未勾选任何数据时，则导出列表中所有数据；



支持表对象信息的导入。点击“导入”按钮可下载模板，完成模板填写后可将模板中的表对象信息导入到列表中。

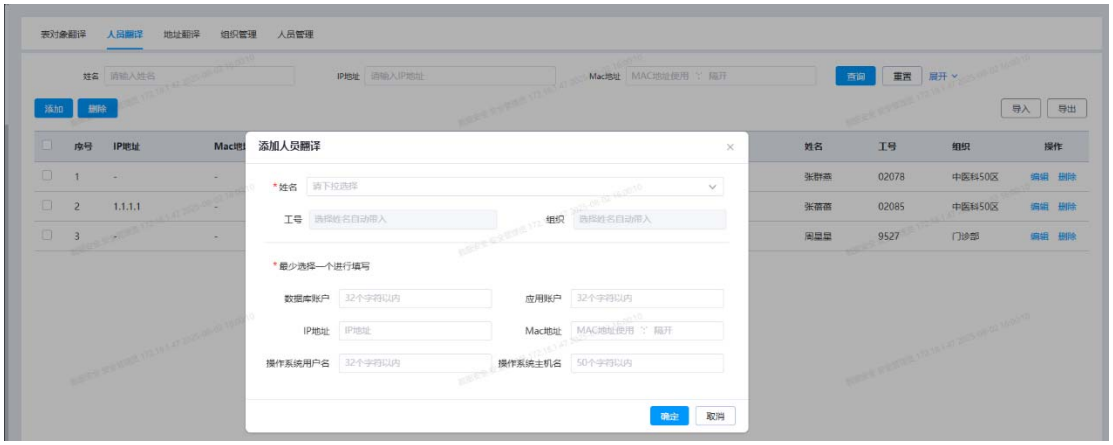
5.10.3.2. 人员翻译

人员翻译会将检索结果中的主体信息进行翻译，可以根据翻译信息快速区分语句的操作人员。

1、添加

点击“添加”按钮，选择需要翻译的姓名和主体信息，保存后检索页面将立即进行人员信息的翻译。其中姓名需要在【人员管理】中配置后关联选择，选择姓名后自动带出工号和组织信息，主体信息可以根据实际情况选择一个或多个字段进行配置。

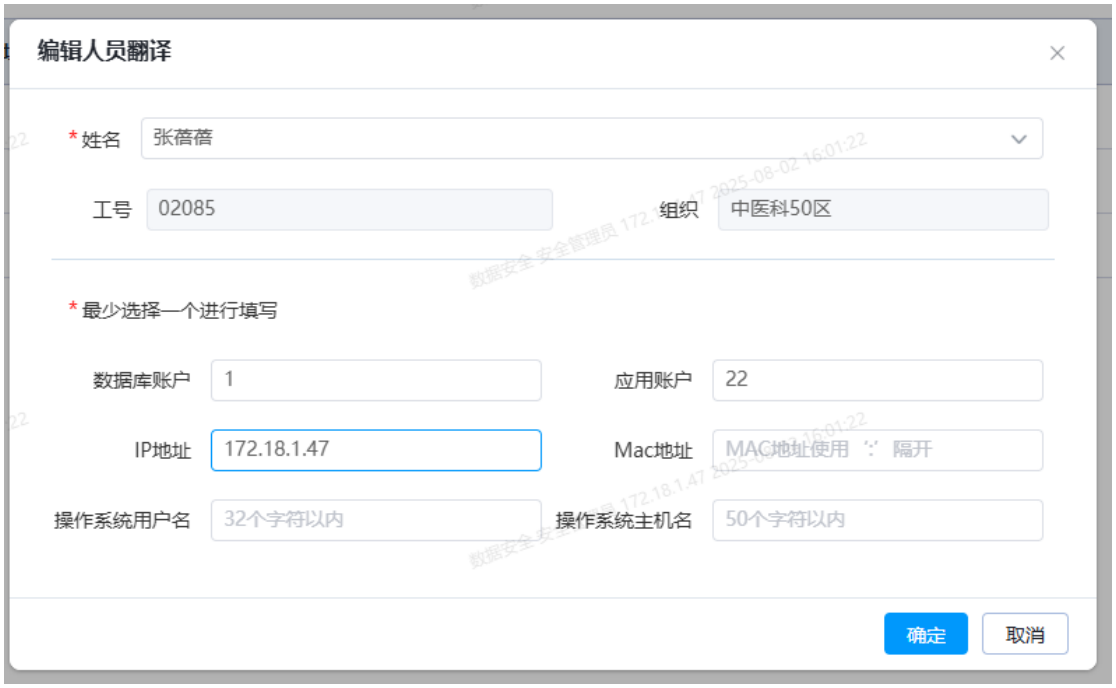
将 IP 地址为 172.18.1.136 翻译为张三，添加示例如下：



添加完成后，通过 172.18.1.136 对保护对象进行操作，在检索中可以看到人员和科室信息。

2、编辑

选中一条翻译数据，点击“编辑”按钮可以修改翻译信息。

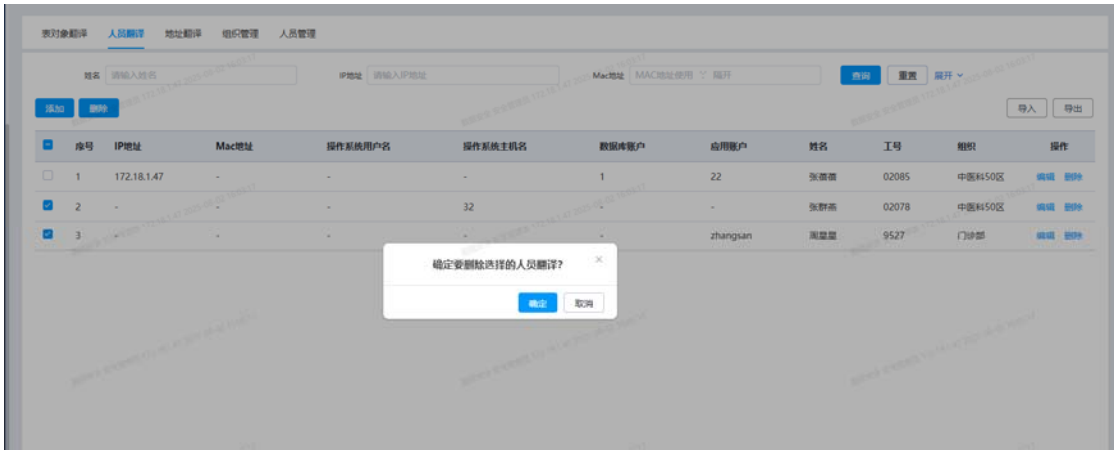


3、查询

输入查询关键字可以查询人员翻译信息。输入查询关键字后点击“重置”按钮可以清除输入的数据。

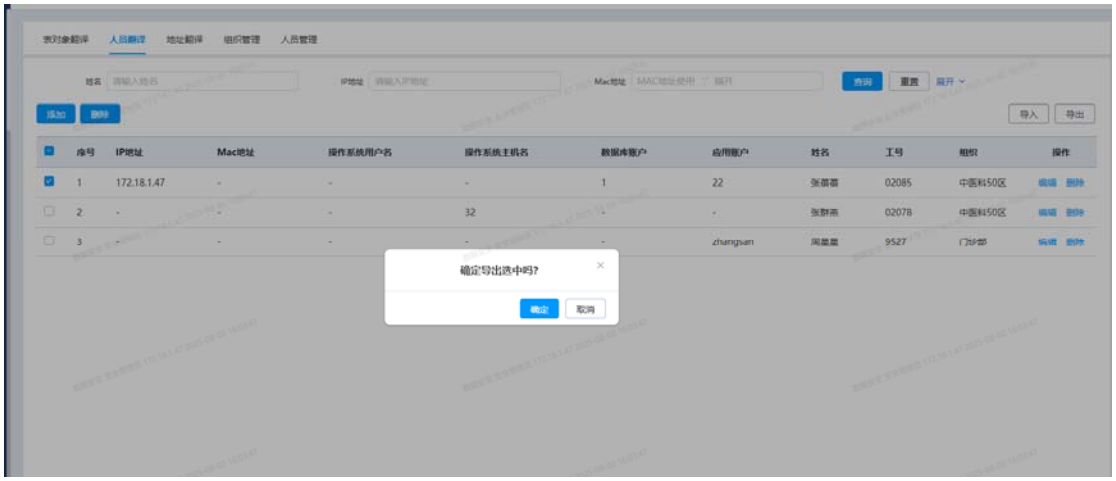
4、删除

支持选中一条数据后，点击“操作”栏的“删除”按钮，删除单条翻译数据。选中一条或多条翻译数据，点击“删除”按钮批量删除选中的数据。



5、导入和导出

支持人员翻译信息的导出。点击“导出”按钮可将人员翻译数据导出到 Excel 文件中。支持勾选一条或多条数据后导出选中的数据；未勾选任何数据时，则导出列表中所有数据；



支持人员翻译信息的导入。点击“导入”按钮可下载模板，完成模板填写后可将模板中的人员翻译信息导入到列表中。

注意：

1、单个人员翻译配置中填写了多个人员条件时，需要同时满足这些条件才会进行翻译。

2、翻译成同一个人员的多条配置，优先匹配翻译字段多的，字段个数相同的优先显示第一个配置的别名。

5.10.3.3. 地址翻译

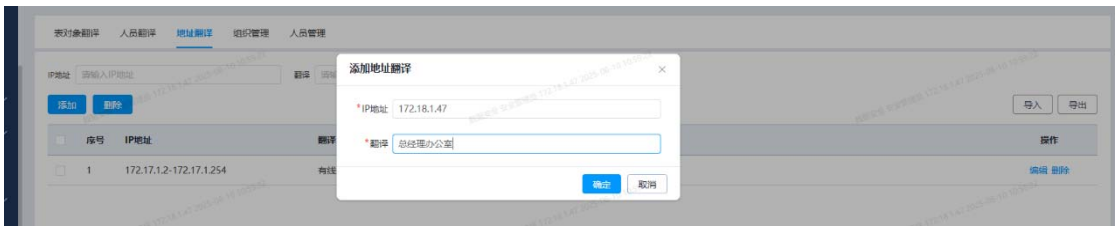
地址翻译会将检索结果中的客户端 IP 地址进行翻译，可以根据翻译信息快速区分操作的客户端地址。

1、添加

点击“添加”按钮，输入需要翻译的 IP 地址和翻译信息，保存后检索页面将立即进行客户端 IP 地址的翻译。

IP 地址可以输入单个 IPV4 地址或 IPV4 地址段，不能重复添加相同的单个 IP，也不能添加有交集的 IP 地址段。

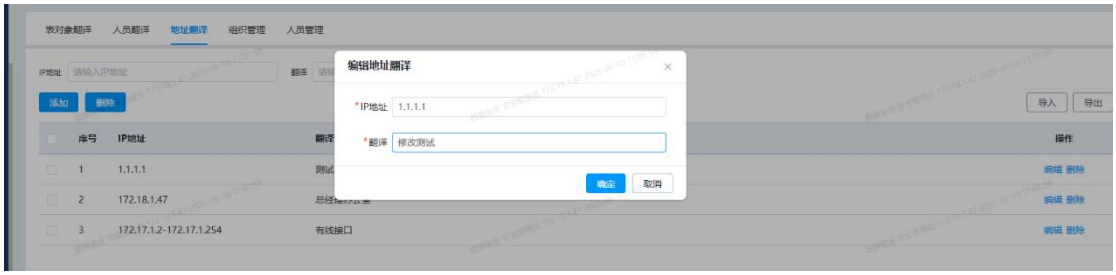
将 172.18.1.136 翻译为总经理办公室，添加示例如下：



添加完成后，通过 172.18.1.136 对保护对象进行操作，在检索中可以看到地址信息。

2、编辑

选中一条翻译数据，点击“编辑”按钮可以修改翻译信息。



3、查询

输入查询关键字可以查询翻译信息。输入查询关键字后点击“重置”按钮可以清除输入的信息。

4、删除

选中一条或多条翻译数据，点击“删除”按钮批量删除选中的数据。

5、导入和导出

支持地址翻译信息的导出。点击“导出”按钮可将地址翻译数据导出到 Excel 文件中。支持勾选一条或多条数据后导出选中的数据；未勾选任何数据时，则导出列表中所有数据；

支持人员翻译信息的导入。点击“导入”按钮可下载模板，完成模板填写后可将模板中的人员翻译信息导入到列表中。

注意：同一个 IP 地址配置了单个 IP 的翻译及 IP 地址段的翻译时，会优先翻译成单个 IP 的翻译值。

5.10.3.4. 组织管理

组织管理中可以添加组织和上级组织信息，可以快速查看组织关系。

1、添加组织

点击“添加”按钮，依次输入组织名称、上级组织等信息，点击“确定”按钮完成添加。每个新组织的添加必须选择对应的上级组织，系统内置“根组织”，可以修改根组织名称。

2、编辑

任意选择一个组织，点击“编辑”按钮可以修改组织信息。

3、查询

在组织树形图和列表中均可以输入关键字后查询组织信息。

4、删除

选中一条或多条数据，点击“删除”按钮批量删除选中的数据。

5、导入和导出

支持导出组织信息。点击“导出”按钮可将组织信息导出到 Excel 文件中。支持勾选部分组织后导出选中的组织；未勾选任何数据时，则导出所有的组织信息；

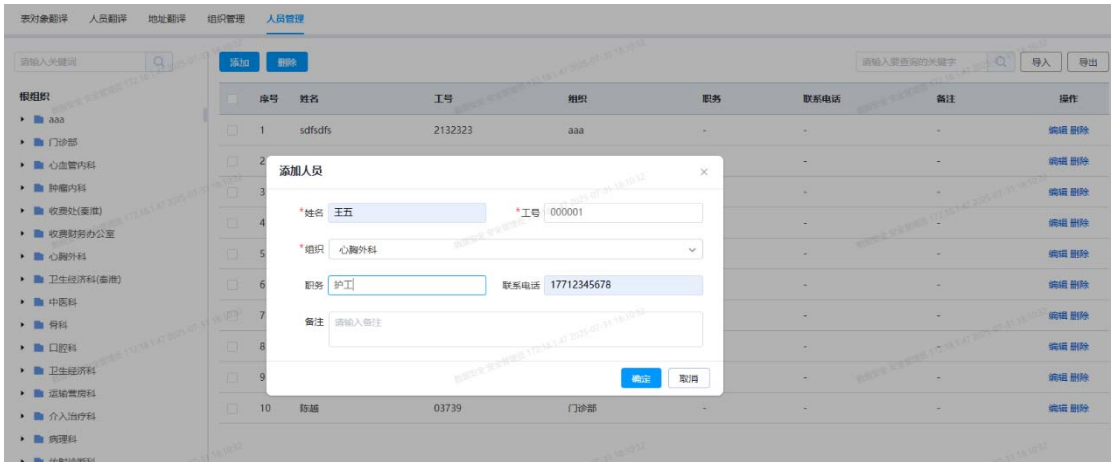
支持导入组织信息。点击“导入”按钮可下载模板，完成模板填写后可将模板中的组织信息导入到列表中。

5.10.3.5. 人员管理

人员管理中可以添加人员的姓名和工号信息，并绑定【组织管理】中已存在的组织信息，方便在人员翻译等功能中快速区分执行人。

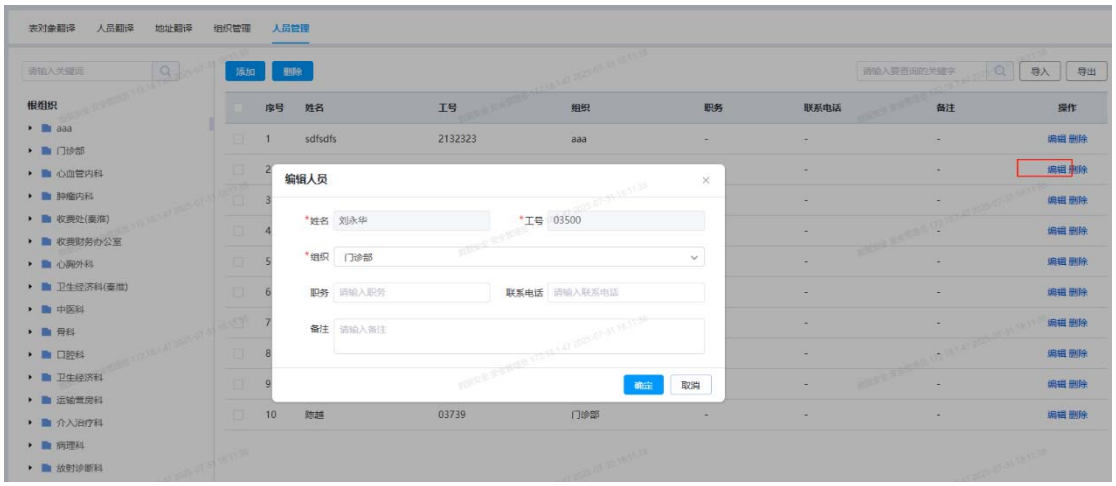
1、添加人员

点击“添加”按钮，依次输入姓名、工号，选择【组织管理】中已存在的组织信息，点击“确定”按钮完成添加。



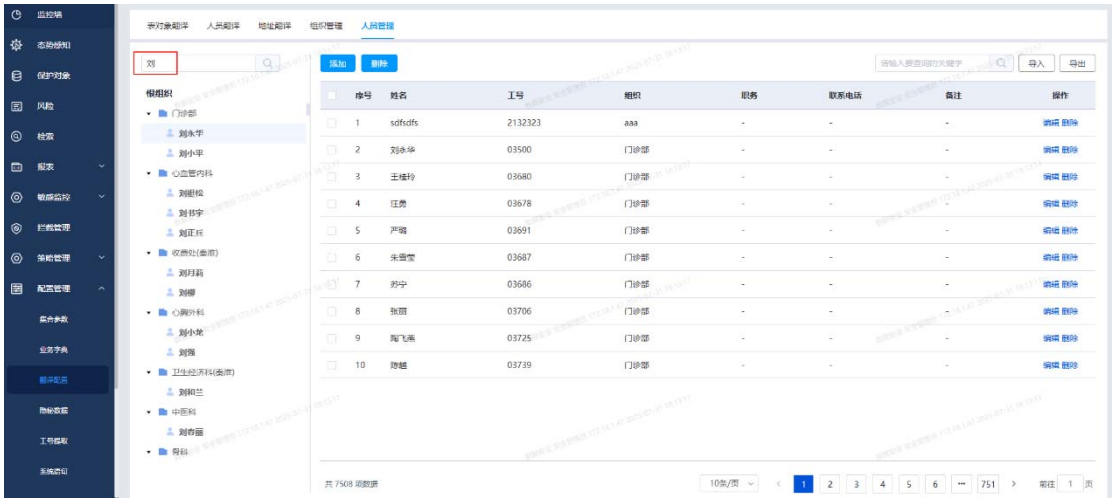
2、编辑人员

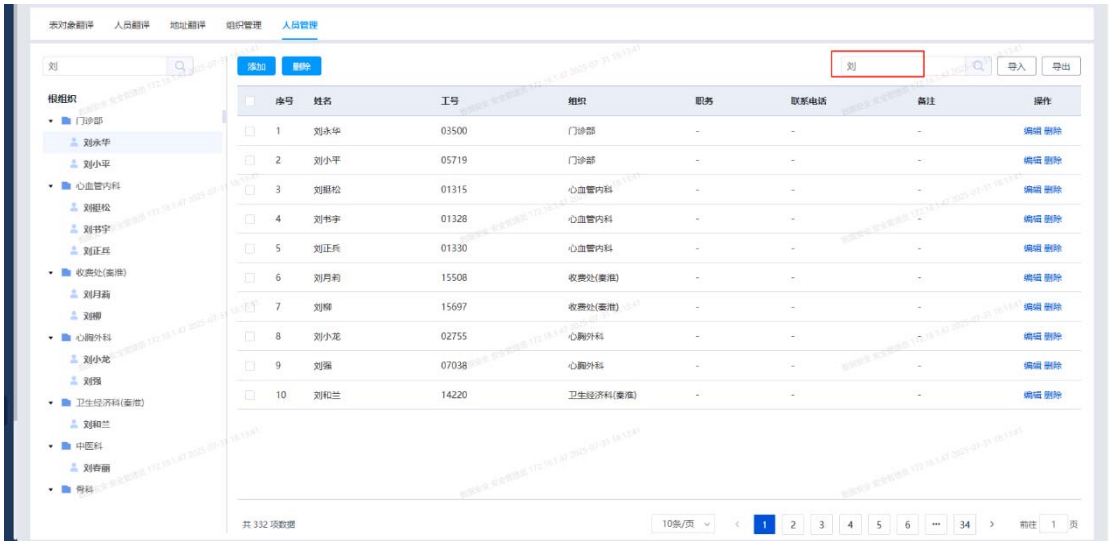
任意选择一个用户，点击“编辑”按钮可以修改人员信息。



3、查询

在人员树形图和列表中均可以输入关键字后查询人员信息。





4、删除

选择一条数据，点击“操作”栏的“删除”按钮，可以删除单条记录，选中一条或多条数据，点击“删除”按钮批量删除选中的数据。

5、导入和导出

支持导出人员信息。点击“导出”按钮可将人员信息导出到 Excel 文件中。支持勾选部分人员后导出选中的人员；未勾选任何数据时，则导出所有的人员信息；

支持导入人员信息。点击“导入”按钮可下载模板，完成模板填写后可将模板中的人员信息导入到列表中。

5.10.4. 隐秘数据

隐秘数据会将符合配置条件的操作语句的审计结果做隐秘处理，防止泄漏。

配置示例如下：

添加完成后，查询保护对象的 user 表的 user_name 字段，在检索页面中查看返回结果，username 字段的数据已被隐藏。

5.10.5. 工号提取

工号提取支持通过配置将审计语句中的信息提取成工号，并显示到检索页面的应用账户字段中。

工号提取规则的添加可选择全局和保护对象中已关联的 HIS 厂商。全局针对所有保护对象生效，HIS 厂商只针对关联的保护对象生效。

提取方式支持关键字、对照提取、分隔符划分、SQL 绑定变量。返回结果提取支持应用范围为 HIS 厂商、保护对象类型为 HTTP 且提取方法不是 SQL 绑定变量的场景。

为了保证提取的准确性，建议将配置中涉及的样例、数据模板、SQL 语句等内容与实际执行的语句保持完全一致。

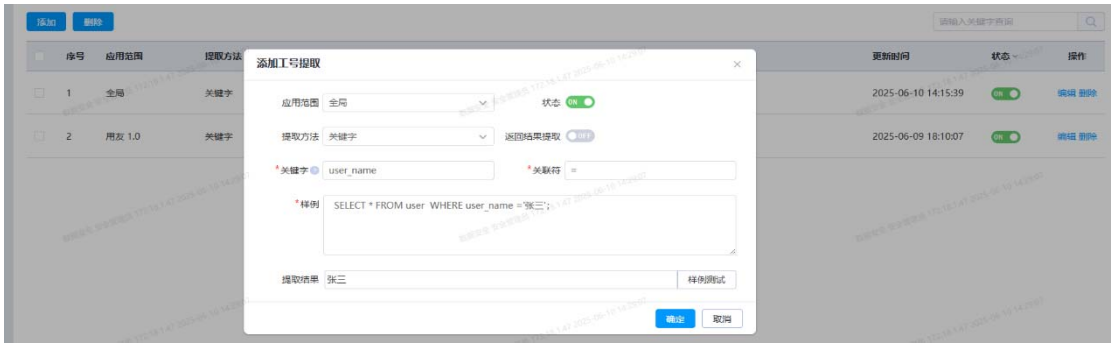
5.10.5.1. 关键字

提取方法选择为“关键字”适用于语句中关键字及关联符都明确的场景，如语句中包含 id=1 或 id：1 等格式，可使用关键字进行提取。

无论是否开启返回结果，都支持填写一个或多个用&隔开的关键字。有多个关键字时，最后一个关键字将作为提取条件，其余关键字作为语句过滤条件，只有一个关键字时，将从“样例”的语句中提取关键信息作为语句过滤条件，以填写的关键字作为提取关键字。

对语句 SELECT * FROM user WHERE user_name =’张三’；进行多个关键字的配置，示例如下：

对语句 SELECT * FROM user WHERE user_name ='张三'；进行单个关键字的配置，示例如下：



添加以上任意一个提取配置，在数据库中执行语句，查看审计检索结果，都能看到“应用账户”字段显示提取到的工号信息为“张三”。

开启返回结果提取，适用于请求中无法获得工号信息的场景。配置时，需要在样例中填写请求信息、返回头信息以及返回结果。如下图，请求信息中的 username 字段为加密状态，返回结果里是明文，则可以使用返回结果进行工号的提取。

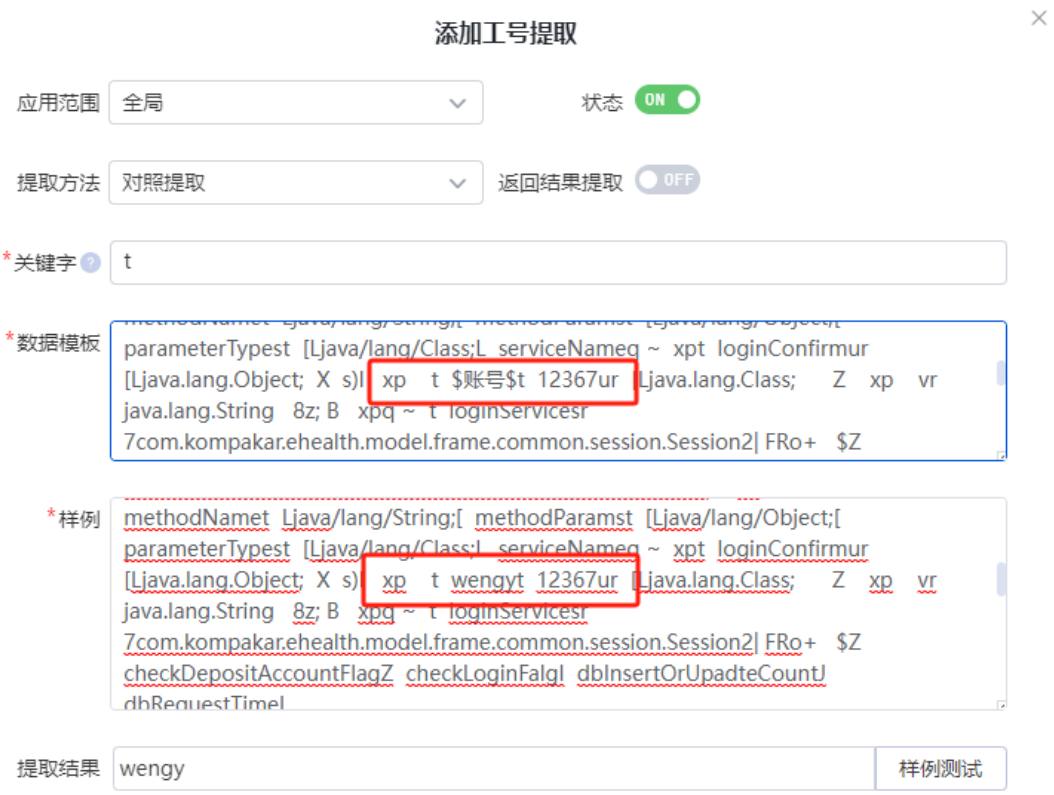
配置完成后，能正确从返回结果中提取到工号信息。

5.10.5.2. 对照提取

对照提取适用于工号信息内容前后字符固定的场景。配置时需要将原始语句粘贴到数据模板中，并将语句中的工号内容用$账号$代替，填写时确保$账号$前后的信息与样例及实际执行语句保持一致。

不开启返回结果时，无论填写一个还是多个关键字，都只作为语句是否提取的过滤条件。开启返回结果时，单个关键字作为返回结果的过滤条件，多个关键字中的最后一个关键字作为返回结果的过滤条件，其他关键字作为语句的过滤条件。

不开启返回结果时，要从操作语句中的 wengyt 中提取 wengy 作为工号，配置示例如下：



执行语句，查看审计检索结果，“应用账户”字段显示提取到的工号信息。

开启返回结果时，适用于请求中无法获得工号信息的场景。配置时，需要在样例中填写请求信息、返回头信息以及返回结果。如下图，请求信息中的 username 字段为加密状态，返回结果里是明文，则可以使用返回结果进行工号的提取。

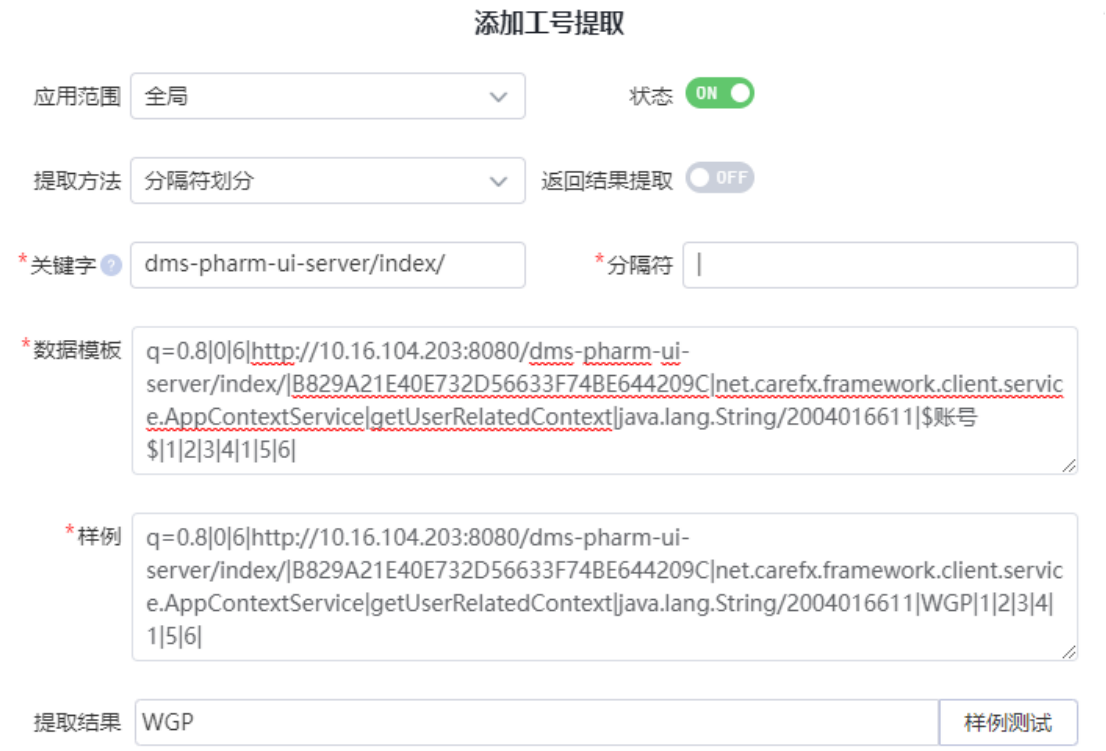
配置完成后，能正确从返回结果中提取到工号信息。

5.10.5.3. 分隔符划分

分隔符划分适用于工号信息前后有固定分隔符，但分隔符前后的内容不固定的场景。配置时需要将原始语句粘贴到数据模板中，并在关联符字段中填写语句中的分隔符，且将语句中的工号内容用$账号$代替。填写时确保$账号$前后的信息与样例及实际执行语句保持一致，且必须替换两个分隔符中间的整段内容。

不开启返回结果时，无论填写一个还是多个关键字，都只作为语句是否提取的过滤条件。开启返回结果时，单个关键字作为返回结果的过滤条件，多个关键字中的最后一个关键字作为返回结果的过滤条件，其他关键字作为语句的过滤条件。

不开启返回结果时，对语句进行配置，示例如下：



执行语句，查看审计检索结果，“应用账户”字段显示提取到的工号信息。

5.10.5.4. SQL 绑定变量

SQL 绑定变量适用于工号信息在绑定变量内容中的场景。配置时需要在 SQL 语句字段中配置原始的执行语句，并在变量序号中配置需要提取的变量序号。SQL 绑定变量不支持在返回结果中进行提取。

语句配置示例如下：

执行语句，查看审计检索结果，“应用账户”字段显示提取到的工号信息。

注意：涉及绑定变量 insert、update、delete、select 语句都对变量值进行了回填，配置工号提取时可以在详情页左上角点击“工号提取”按钮，弹出的配置页面会自动填充未回填的原始语句，需要手动删除变量值后保存。删除语句末尾分号开始的所有内容，分号前的内容需要全部保留，包括空格、换行等内容。如果语句末尾有多个分号，只删除最后一个及后面的内容。

注意：

1、配置了 HIS 厂商的保护对象会优先匹配对应 HIS 厂商的提取规则，没有配置对应的 HIS 规则或对应的规则提取不到工号时，会使用全局规则进行提取。

2、对照提取配置的模板中只能有一个完整的提取占位符：$账号$。如模板中允许配置为 aaa$账号$格式，但不允许配置为 aaa$账号$ aaa$账号$。

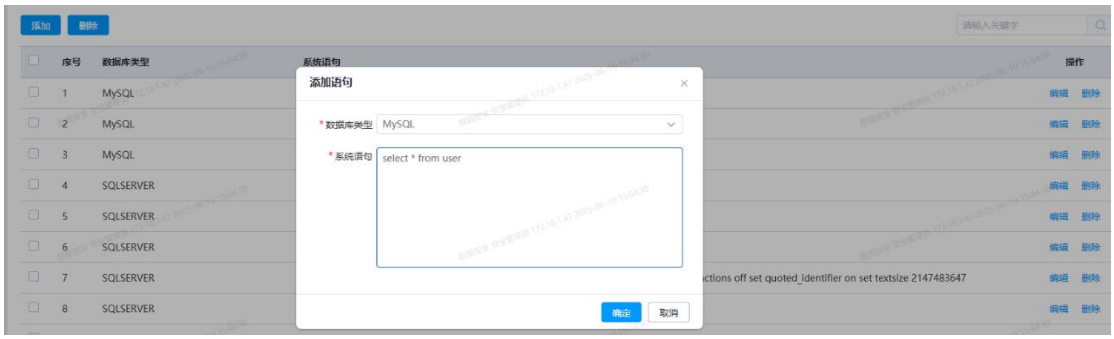
3、对照提取提取规则会针对模板中占位符的位置进行提取，为保证提取的准确性，请确保模板与样例、实际执行的语句一致。

4、HTTP 类型默认不审计返回结果，如果需要从返回结果中提取工号信息，需要提前打开审计 http 返回结果的开关。

5.10.6. 系统语句

添加到系统语中的语句将不再进行审计。

添加配置示例如下：



添加完成后，对已有的 mysql 类型的保护对象执行上述语句，在检索页面将查不到该条语句的执行记录。

5.10.7. 驱动级 IP 过滤

通过添加配置，可以对源 IP 地址到目的 IP 地址的流量进行审计或不审计的过

滤。

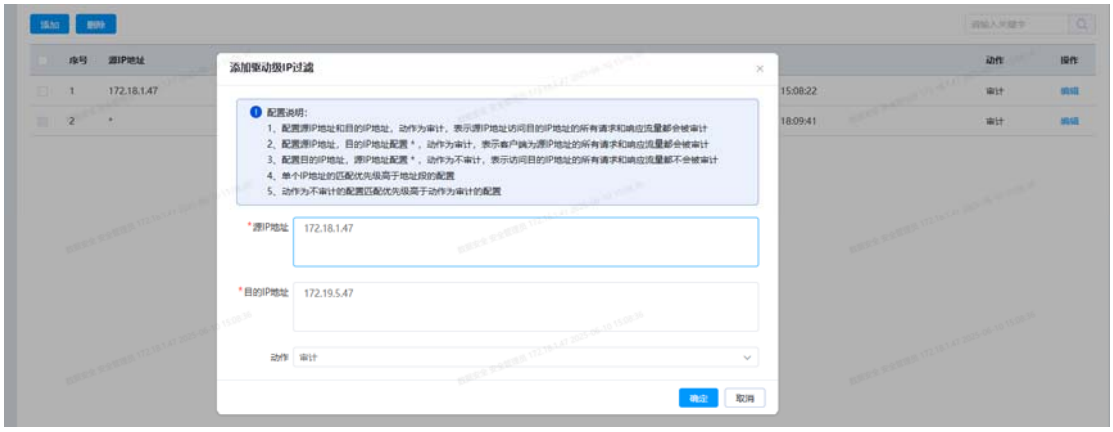
1、默认配置

系统内置*到*，动作为审计的配置，代表所有访问保护对象的流量都将被审计。将动作改为不审计，则表示所有访问保护对象的流量都将不会被审计，可以添加其他审计动作的配置，实现对指定范围的流量进行审计。

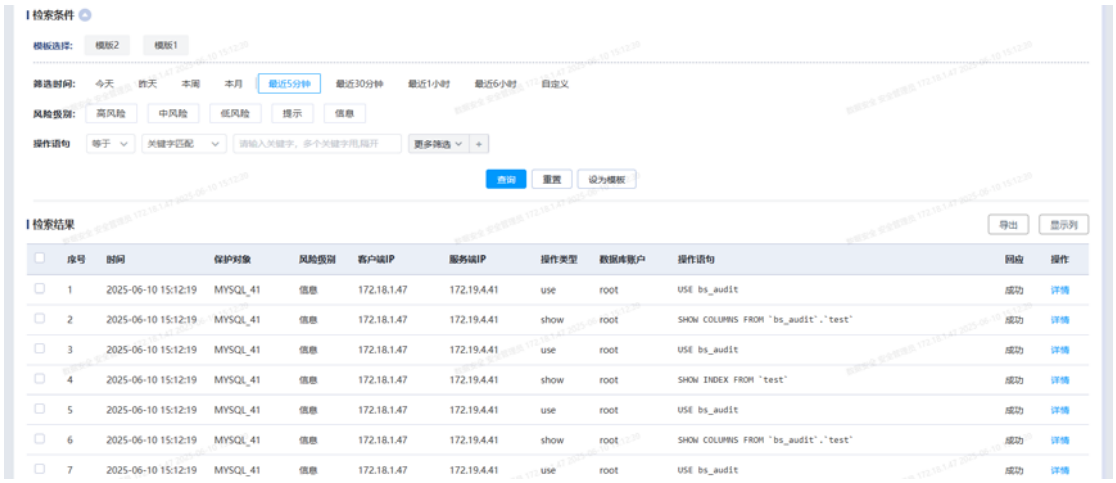
2、添加

点击“添加”按钮，输入源 IP 地址和目的 IP 地址，选择动作后，点击“确定”按钮。

以审计 172.18.1.136 访问 172.19.1.14 为例，配置如下：

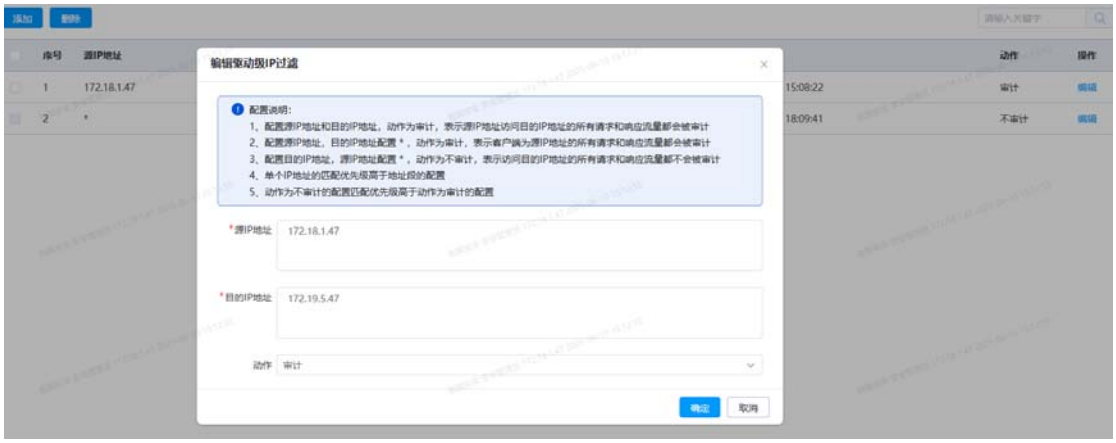


保存后将会审计 172.18.1.136 访问 172.19.1.14 的流量，如果此时将*到*设置为不审计，将只审计 172.18.1.136 访问 172.19.1.14 的流量。



2、编辑

任意选择一条数据，点击“编辑”按钮可以修改配置。



3、查询

输入查询关键字可以查询配置。

4、删除

选中一条或多条非内置的数据，点击“删除”按钮批量删除选中的数据。

注意：

1、IP 地址支持输入单个 IPV4 地址、IPV4 地址段、IPV4 网段。

2、同一个 IP 同时在不同配置中添加了审计和不审计动作时，优先匹配配置 IP 数少的规则（如配置了 172.18.1.136 到 172.19.1.14 为审计，配置了 172.18.1.*到 172.19.1.*为不审计，则 172.18.1.136 访问 172.19.1.14 时会被审计）。

3、同一个 IP 同时在不同配置中添加了审计和不审计动作时，且规则中配置的 IP 数相同，优先匹配不审计规则（如配置了 172.18.1.135-136 到 172.19.1.14 为审计，配置了 172.18.1.136-137 到 172.19.1.14 为不审计，则 172.18.1.136 访问 172.19.1.14 时不会被审计）。

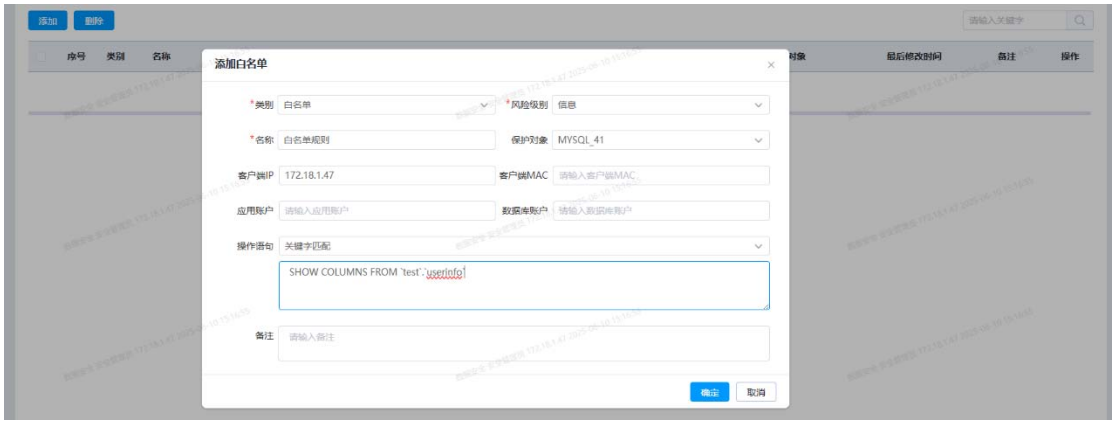
5.10.8. 白名单管理

添加白名单后，符合白名单的操作会优先匹配白名单，不匹配白名单的操作才会匹配规则。

1、添加

点击“添加”按钮，输入白名单名称，选择保护对象，输入需要配置为白名单的一个或多个条件，保存后白名单配置生效，后续符合配置条件的审计记录将不再触发风险。选择多个条件后，需要同时匹配添加的所有条件才会认为符合白名单的设置。

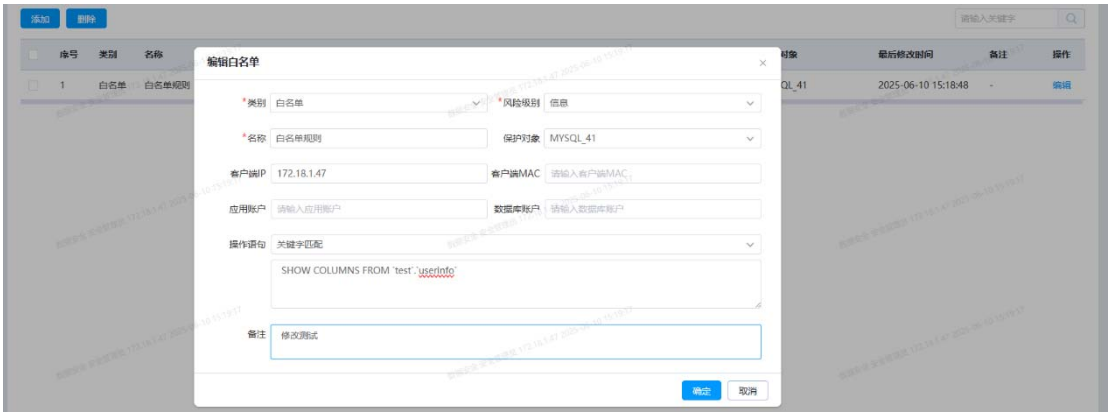
以将 172.18.1.136 访问 mysql172.19.1.26 数据库执行语句 SHOW COLUMNS FROM `test`.`userinfo`为添加示例，配置如下：



执行语句，查看审计检索结果，配置白名单后的语句将不再触发风险。

2、编辑

任意选择一条数据，点击“编辑”按钮可以修改配置。

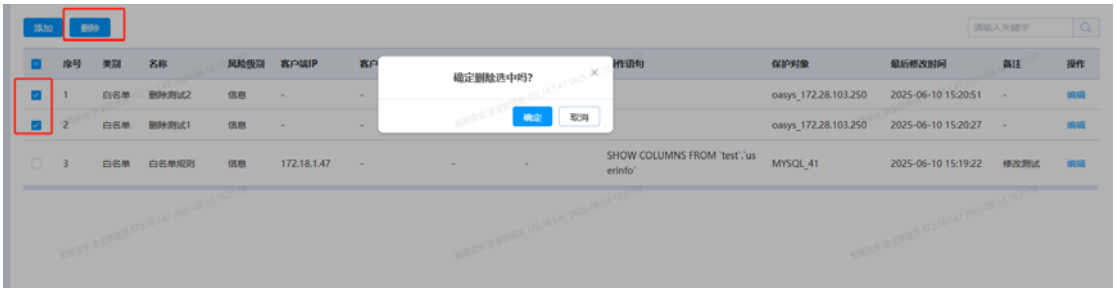


3、查询

输入查询关键字可以查询配置。

4、删除

选中一条或多条白名单，点击“删除”按钮批量删除选中的数据。



5.11 数据维护

数据维护针对审计记录进行维护，主要的操作包括添加外置存储、数据备份、数据清理、数据恢复。

5.11.1. 外置存储

Linux 挂载 Windows 共享文件夹后，在外置存储中可以选择存储的文件路径并保存。数据备份时可以选择将备份数据上传到 Windows 共享路径中。

以 X86 架构的 cifs 文件系统为例：

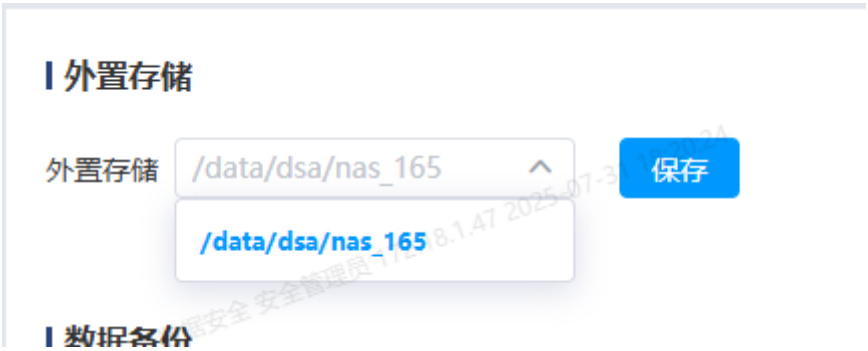
1.准备共享文件夹路径：//172.23.1.15/zhengwx

2.在系统服务器后台创建 cifs 文件系统：yum install -y cifs-utils .x86_64

3.在系统服务器后台创建目录文件：mkdir /data/cccc

4.在系统服务器后台执行挂载命令：sudo mount.cifs //172.23.1.15/zhengwx /data/cccc -o user=zhengwenxiang,pass=******,rw,file_mode=0777,dir_mode=0777

5.在“数据维护”页面“外置存储”中选择文件路径并保存。



注意：

1、在系统服务器后台执行取消挂载命令：umount /data/dsa/nas_165 后，在外置存储选项中将不显示此文件路径。

2、只支持配置单个外置存储。

5.11.2. 数据备份

支持根据指定的条件对数据进行备份，分为自动备份和手动备份两种方式。

5.11.2.1. 自动备份

系统内置一个自动备份任务，每天凌晨 2 点自动进行备份。

1、修改自动备份任务

点击“编辑”按钮可以修改自动备份任务内容。

存储方式：本地和远程两种。选择本地备份后，备份的文件可以在备份记录页面直接下载。选择远程，备份的文件可以上传到 FTP 服务器或外置存储上，远程上传后的文件不可在备份记录页面下载。

上传方式：存储方式选择本地时，上传方式不可选。存储方式选择远程时，支持选择 FTP 和外置存储。FTP 选项需要在 FTP 服务器进行配置，详见【FTP 服务器】。外置存储选项需要在外置存储中进行配置，详见【外置存储】。

数据类型：支持选择审计记录、配置信息、返回结果。其中“审计记录”包括所有的审计数据，“配置信息”包括保护对象、策略管理、配置管理页面的数据，“返回结果”包括 http 类型和 portal 类型的保护对象审计记录的返回结果。

注意：1、不支持修改自动备份任务的执行时间

2、不支持新增、删除自动备份任务

3、修改备份任务后不影响正在备份中的任务运行，修改后的配置在下一次自动备份时生效。

2、备份任务详情

在自动备份任务“操作”栏点击“详情”按钮，可以查看自动备份任务的执行记录。

在“备份记录”页面，点击“操作”栏的“上传”按钮，可将未上传的备份文件远程上传至指定的 ftp 服务器或外置存储上：

在“备份记录”页面，点击“操作”栏的“下载”按钮，可以将存储方式选择本地的备份文件下载至客户端本地：

5.11.2.2. 手动备份

点击“手动备份”按钮，可以手动添加备份任务。

数据时间范围：支持全部时间备份和自定义时间备份。自定义时间可选择对时间范围内的审计记录、配置信息、返回结果数据进行备份。全时间备份只能选择外置存

储方式上传所有数据的备份文件。

存储方式：本地和远程两种。选择本地备份后，备份的文件可以在备份记录页面直接下载。选择远程，备份的文件可以上传到 FTP 服务器或外置存储上，远程上传后的文件不可在备份记录页面下载。

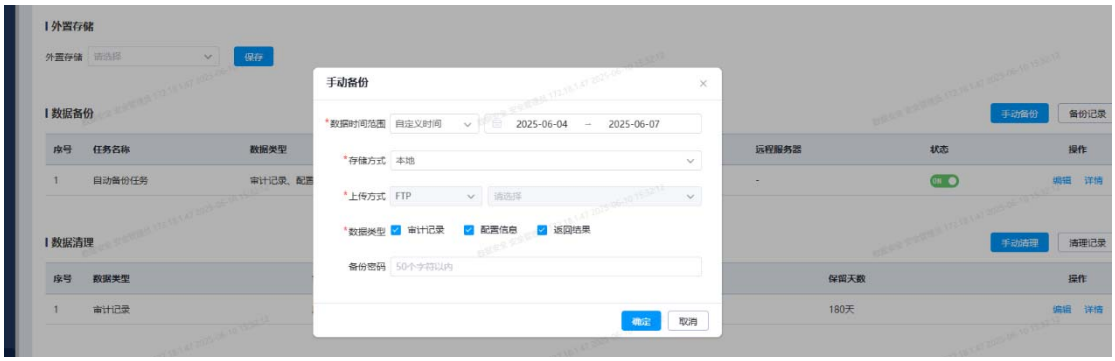
上传方式：存储方式选择本地时，上传方式不可选。存储方式选择远程时，支持选择 FTP 和外置存储。FTP 选项需要在 FTP 服务器进行配置，详见【FTP 服务器】。外置存储选项需要在外置存储中进行配置，详见【外置存储】。

数据类型：支持选择审计记录、配置信息、返回结果。其中“审计记录”包括所有的审计数据，“配置信息”包括保护对象、策略管理、配置管理页面的数据，“返回结果”包括 http 类型和 portal 类型的保护对象审计记录的返回结果。

备份密码：输入备份密码后，备份的文件需要打开或进行数据恢复时都需要输入密码。

1、添加手动备份

点击“手动备份”按钮，添加备份任务。



注意：手动备份为一次性任务，添加完成后立即启动执行，不可修改。

2、备份记录

点击“备份记录”按钮，可以查看备份任务的执行记录。

5.11.3. 数据清理

支持根据指定的条件对数据进行清理删除，分为自动清理和手动清理两种方式。系统内置自动清理任务，不可新增和删除，可以修改任务内容。手动清理只能有一个任务进行清理，且下一个任务必须在上一个任务完成后才能添加。

5.11.3.1. 自动清理

系统内置一条自动清理任务，从最早时间按天清理。清理时优先清理所选条件的最早历史数据，若按天清理一次数据后，清理阈值降至设置值之下，则停止清理，若一直未下降至设置值，再清理至距离系统时间 180 天停止清理风险数据，只清除非风险数据，直到非风险数据只剩 2 天或下降到设置值时停止清理。若按天清理之前数据转存动作失败，则终止清理任务，已清理的数据不可恢复。若风险数据低于 180 天，则只清除非风险数据。自动清理每日 3：33-23：33 期间执行，每小时检测一次清理条件，达到清理条件则启动清理，反之不进行清理。

不支持新增、删除自动清理任务，点击“编辑”按钮可以修改任务配置。

磁盘使用率：默认 90%，可手动配置范围为 50%-90%。当磁盘使用率达到该数值时清理任务开始执行。

清理比例：程序自动清理至 180 天以内数据时，将按照设置的清理比例进行清理

数据类型：支持审计记录、http 返回结果二选一。“审计记录”类型包含审计记录、http 返回结果、本地备份包。其中“审计记录”是指全部保护对象的风险和非风险数据；“http 返回结果”是指 http 类型和 portal 类型保护对象审计的语句执行返回结果；“本地备份包”是指自动备份的压缩文件。

1、修改自动清理任务

选中自动清理任务，点击“编辑”按钮，进入任务修改页面。

注意：正在清理的配置修改后对当前清理任务不影响，修改后的配置在下一次自动清理生效。

2、任务详情

选中自动清理任务，点击“详情”按钮，进入任务详情页面。

5.11.3.2. 手动清理

点击“手动清理”按钮，可以自定义添加手动清理任务。

数据类型：支持审计记录、http 返回结果二选一。“审计记录”类型包含审计记录、http 返回结果、本地备份包。其中“审计记录”是指全部保护对象的风险和非风险数据；“http 返回结果”是指 http 类型和 portal 类型保护对象审计的语句执行返回结果；“本地备份包”是指自动备份的压缩文件。

审计记录类型：“数据类型”勾选了“审计记录”时，需要选择“审计记录类型”。支持选择为高风险、中风险、低风险、提示、信息，可以根据需要选择其中的一个或多个。

保护对象：选“数据类型”勾选了“审计记录”时，可以选择“保护对象”。支持手动选择 5 个以内的保护对象，不选择时默认清理范围为所有保护对象。

数据时间范围：手动选择需要清理的时间范围。

1、添加手动清理

添加一条手动清理份任务时，点击页面“手动清理”按钮，弹出对话框，在对话框中依次输入新增自动清理信息：

注意：手动清理为一次性任务，添加完成后立即启动执行，不可修改。

2、清理记录

点击“清理记录”按钮，可以查看清理任务的执行记录。

5.11.4. 数据恢复

手动备份和自动备份任务生成的备份文件，都可以进行数据恢复。

1、导入文件

点击“导入”按钮，可以上传备份的文件。

注意：不支持全量恢复、自动备份恢复，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，不可存在中文和除去【. - _】之外的特殊字符，建议不要重命名备份文件。

2、恢复数据

点击“恢复”按钮时，没有密码的备份文件立即进行恢复，有密码的备份文件在输入正确的密码后立即进行恢复。

5.12 告警

5.12.1. 告警策略

告警策略支持对触发风险规则的审计记录进行实时告警的发送配置。通过配置策略名、告警事件、通知方式、接收者添加告警策略，并将告警策略应用到保护对象中，当有符合告警策略的审计记录产生，就会实时根据配置的告警策略发送告警。

添加告警策略填写说明：

a. 策略名：150 个字符以内，不包含< > ^ 空格，名称设置后不可修改。

b. 告警事件：高危事件、中危事件、低危事件、关注事件分别对应审计记录的风险等级高风险、中风险、低风险、提示，可以选择一个或多个告警事件。

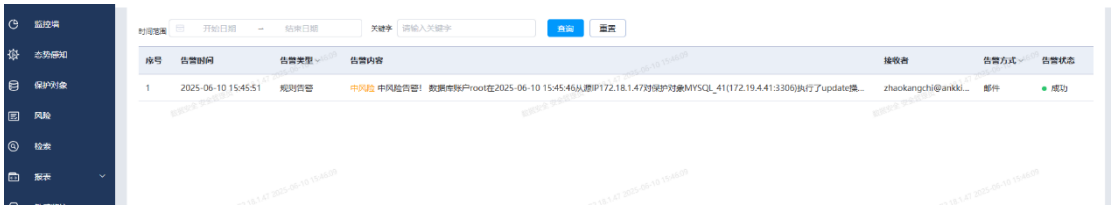
c. 通知方式：可选邮件、syslog、SNMP、短信、企业微信、钉钉，六项配置都需要在系统管理平台-互联接口中预置对应的服务器配置（若使用的是短信猫，请先在设备上插好短信猫并插入 SIM 卡），短信和邮件还需先到个人信息或用户管理中填写邮箱和手机号码，支持选择一个或多个通知方式。

d. 接收者：可选三大平台默认的管理员用户和管理员在用户管理中添加的子用户。

添加完成后，需要到保护对象中启用告警开关，再选择添加的告警策略。对保护对象进行操作，触发相应风险级别的规则后，会按照告警策略发送告警信息给接收者。

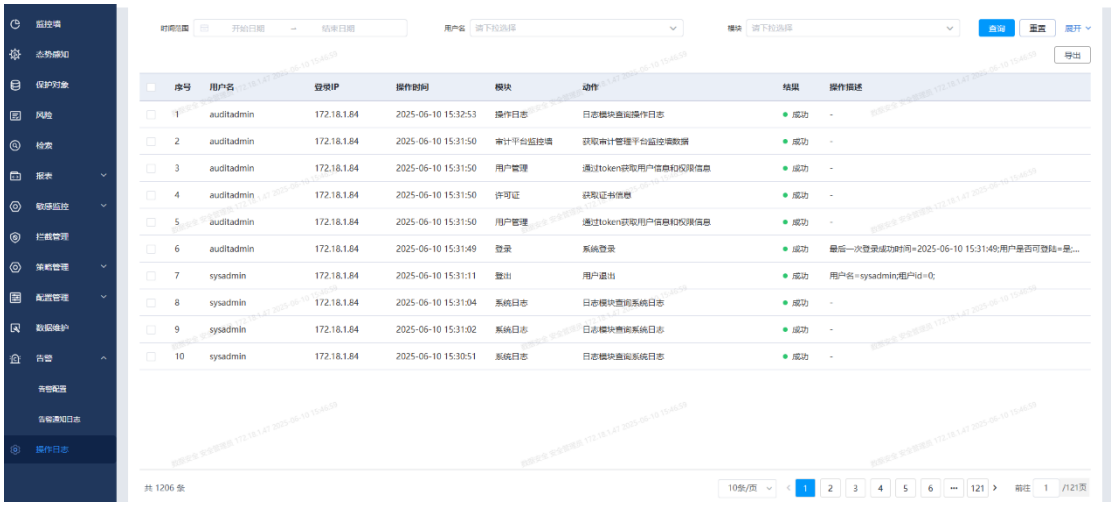
5.12.2. 告警通知日志

告警日志中记录已经触发的告警信息，展示告警时间、告警类型、告警内容、接收者、告警状态等信息。



5.13 操作日志

操作日志展示用户在系统管理平台和审计管理平台的操作记录。


监控墙
态势感知
保护对象
风险
检索
报表
敏感监控
拦截管理
策略管理
配置管理
数据维护
告警
告警配置
告警通知日志
操作日志
时间范围
开始日期
结束日期
用户名
请下拉选择
模块
请下拉选择
查询
重置
展开
导出
序号 用户名 登录IP 操作时间 模块 动作 结果 操作描述
1 auditadmin 172.18.1.84 2025-06-10 15:32:53 操作日志 日志模块查阅操作日志 成功 -
2 auditadmin 172.18.1.84 2025-06-10 15:31:50 审计平台监控墙 获取审计管理平台监控墙数据 成功 -
3 auditadmin 172.18.1.84 2025-06-10 15:31:50 用户管理 通过token获取用户信息和权限信息 成功 -
4 auditadmin 172.18.1.84 2025-06-10 15:31:50 许可证 获取证书信息 成功 -
5 auditadmin 172.18.1.84 2025-06-10 15:31:50 用户管理 通过token获取用户信息和权限信息 成功 -
6 auditadmin 172.18.1.84 2025-06-10 15:31:49 登录 系统登录 成功 最后一次登录成功时间=2025-06-10 15:31:49;用户是否可登陆=是;...
7 sysadmin 172.18.1.84 2025-06-10 15:31:11 登出 用户退出 成功 用户名=sysadmin;用户id=0;
8 sysadmin 172.18.1.84 2025-06-10 15:31:04 系统日志 日志模块查阅系统日志 成功 -
9 sysadmin 172.18.1.84 2025-06-10 15:31:02 系统日志 日志模块查阅系统日志 成功 -
10 sysadmin 172.18.1.84 2025-06-10 15:30:51 系统日志 日志模块查阅系统日志 成功 -
共 1206 条
10条/页
1 2 3 4 5 6 ... 121
前往 1 /121页

6 审计管理平台

6.1 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。

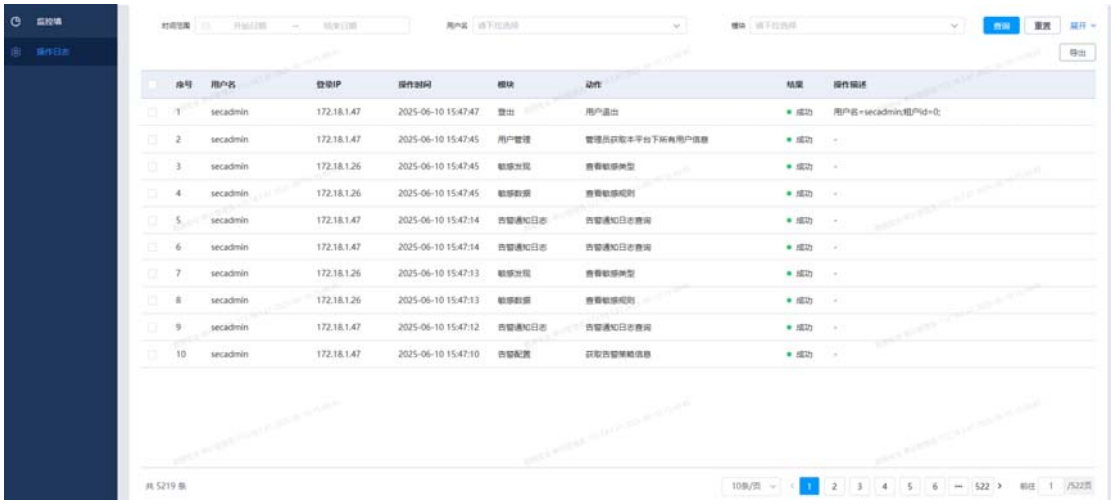
b. 登录失败最多的 IP TOP5：显示搜索时间范围内，登录设备失败次数最多的前五名的 IP 地址，含详细次数和所占百分比，点击饼状图中的任意 IP，可以跳转到操作日志来查看对应 IP 登录失败的时间、用户名等详细信息。

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。

d. 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。

6.2 操作日志

操作日志展示了除自己以外的其他用户的操作情况，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。

操作日志能通过 导出 按钮导出，可以导出选中或所有日志到 Excel 或 PDF 文件中。

7 FAQ

1、恢复出厂设置为什么失败？

恢复出厂设置功能依赖于证书。先检查是否有上传证书、证书是否在有效期。然后再看系统平台监控墙的规则引擎、解析引擎以及通信引擎是否为绿色，正常运行状态，只有满足以上情况，恢复出厂设置功能才可用。

2、 搜索审计记录时，关键字检索一串词检索不出来，如：数据库审计与防护系统。

关键字检索需要有效的词语，这种词语能够通过字典查询出来，且不支持特殊符号检索。

3、 规则配置中，操作返回内容配置里，可以支持多个关键字条件吗？支持正则吗？

返回内容暂不支持多个关键字以及正则。

4、备份下来的文件更改名字后再去恢复，恢复失败。

不支持全量恢复,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，不可存在中文和除去【. - _】之外的特殊字符，建议不要重命名备份的文件。

5、磁盘达到告警阈值之后如何处理？

可在数据维护模块中对之前需要的数据进行备份，备份后将对应日期的数据使用手动清理功能清理掉，如果需要备份非风险数据，需要使用自动备份功能对非风险进行备份。

6、发现已经废弃的子用户是在线状态，如何制止。

可以对在线用户进行修改、重置密码、删除和锁定操作。修改、重置密码、删除会在子用户进行下一步操作时自动返回登录页面，锁定会在下一次登录生效。

7、人员翻译是否有优先级，如果设置了指向同一个访问者的配置如何显示。

对于设置了多个附加条件的，需要同时满足这些条件才会显示别名。对于指向同一个访问者的配置，优先显示条件个数多的，条件个数相同的优先显示第一个配置的别名。

8、手动添加大量的人员翻译配置太耗时了，是否有其他便捷方法。

除了人员翻译，其他配置也可以使用该方法：在系统平台-系统维护中，一键导出所有配置信息，根据导出的内容填写需要添加的配置，所有配置的 UUID 必填。以访问者别名为例，可在前台配置一条查看基本格式，对于本身的 UUID（访问者别名 UUID）可填写序号 1、2、3...部门 UUID 为默认配置 1 不变，按需填写访问者别名，不用填写时间。填写完后保存，一键导入即可生效使用。

9、为什么数据清理后，监控墙展示的当前审计记录总数与实际检索到的日志数量不一致？

因为数据清理不会清理监控墙展示的审计记录总数，所以数据清理后，监控墙展示的审计记录总数一定大于等于检索到的审计日志数量。

10、为什么选择了 Agent 引流方式但是没有审计记录？

首先确认部署方式中的 Agent 引流已经开启成功（已成功勾选上，默认部署方式只有旁路镜像），开启成功后在已连接客户端中会显示对应的 IP 地址；

再查看 Agent 监听端口是否为 9999，此处默认为数据库审计与防护系统端口并非数据库端口。

最后检查 Windows agent 和 Linux agent 配置信息是否正确，具体配置可以根据【Agent 引流】章节下载安装包并查看《agent 使用手册》。

11、为什么没有流量进入数据库审计与防护系统？

检查保护对象页面配置的数据库类型、IP 和端口是否正确。

比如现场环境做了 NAT，根据现场实际环境确认要选择配置数据库的原始 IP，还是映射后的公网 IP；如果是 oracle RAC 集群，审计对象需要将 RAC 集群的所有 IP（物理地址、虚拟地址、SCANIP）都加上，心跳 IP 除外。在数据库服务器上抓业务口的报文，然后操作数据库，分析源 IP 和目标 IP，确认是否跟实际操作的 IP 一致。

端口要确认数据库是否使用了默认的端口，比如 oracle 的端口是 1521，mysql 的端口是 3306。如果数据库的端口做了修改，数据库审计与防护系统要在保护对象配置修改后的端口。

12、如何设置只审计某一个 IP 或某一个 IP 段？

登录安全规则平台，在“驱动级 IP 过滤”模板中，将默认的*到*的配置动作改为不审计，新增一条配置，在源 IP 地址和目的 IP 地址中填写需要审计的 IP 地址或地址段，动作设置为审计，保存后将只审计新增配置中的 IP 地址和地址段。

13、为什么添加了表名描述，但检索记录里没有对表名进行翻译？

当前只支持对勾选为“关键表”的表名进行翻译，需要检查表是否已设置为关键表。

14、为什么驱动级 IP 过滤配置后没有生效？

驱动级 IP 过滤只对部署方式为镜像引流的流量生效。

15、Agent 管理中新增一台设备时，服务显示正常，为什么设备状态为“离线”？

当部署方式仅为"旁路镜像"时，此时 agent 客户端服务无法直接与服务端进行通讯，从而审计系统无法识别其真实的状态，故而设备状态显示为"离线"，而审计服务正常运行。

8 注释

8.1 缩略语

表 8-1 缩略语表

缩略语	英文全称	中文全称
DML	Data Manipulation Language	数据操作语言
DDL	Data Definition Language	数据定义语言
DCL	Data Control Language	数据控制语言
SNMP	Simple Network Management Protocol	简单网络管理协议
SYSLOG	System Logging	系统日志协议
FTP	File Transfer Protocol	文件传输协议
SFTP	SSH File Transfer Protocol	SSH 文件传输协议
CPU	Central Processing Unit	中央处理器

8.2 术语

表 8-2 术语表

术语	英文全称	说明
His 厂商	Hospital Information System	His 厂商是指专门研发、销售、实施医院信息系统的软件公司或解决方案提供商。
集合	Set	集合由确定且互不相同的对象构成的整体。集合中的元素无序、不重复，且每个元素只能出现一次。
集合元素	Element	集合元素是构成集合的每一个独立对象，可以是数字、字符、字符串、甚至其他集合。
存储过程	Stored Procedure	存储过程是数据库系统中的一种可编程对象，用于封装一组 SQL 语句和逻辑控制，以便在数据库服务器端进行执行。
触发器	Trigger	触发器是数据库中一种特殊的存储过程，它在特定事件发生时自动执行，而无需显式调用。
工号	Employee ID	工号是企业或组织为每位员工分配的唯一身份标识号码。在审计系统中，可以绑定数据库账户、应用账户、IP 地址、Mac 地址、操作系统用户名、操作系统主机名。
交换机配置	Switch Configuration	交换机是局域网（LAN）中连接多个设备的核心设备，通过配置交换机，可以实现设备之间的高效通信、VLAN 划分、端口管理、安全控制等。
内存	Random Access Memory	内存是指当前系统中正在使用的内存资源的总量，通常以 MB（兆字节）或 GB（千兆字节）为单位进行衡量。它反映了系统中运行的程序、服务和进程对内存资源的使用情

		况。
审计速率	Audit Throughput	审计速率是指审计系统每秒能够处理的审计事件数量。该指标用于衡量审计系统在高并发、大数据量场景下的处理能力与性能上限，是评估系统性能、容量规划和扩展能力的重要参考依据。
入库速率	Ingestion Rate	入库速率是指每秒系统能够解析并写入数据库的数量。该指标用于衡量系统在高并发、大数据量场景下的数据写入能力，是评估系统性能、稳定性与扩展能力的重要参考依据。
告警	Alarm	告警指系统对关键运行参数、指标或阈值进行实时监控；当被监测值超出预设安全或允许范围时，能够立即生成并推送告警信息，以便运维或管理人员及时采取纠正措施的综合能力。

9 附录

9.1 企业微信对接流程

1.准备工作

请确保已经注册成为了企业微信服务商企业；如果还没有，请参考企业微信应用接入指引的 成为企业微信的服务商 部分。

2.登录服务商后台

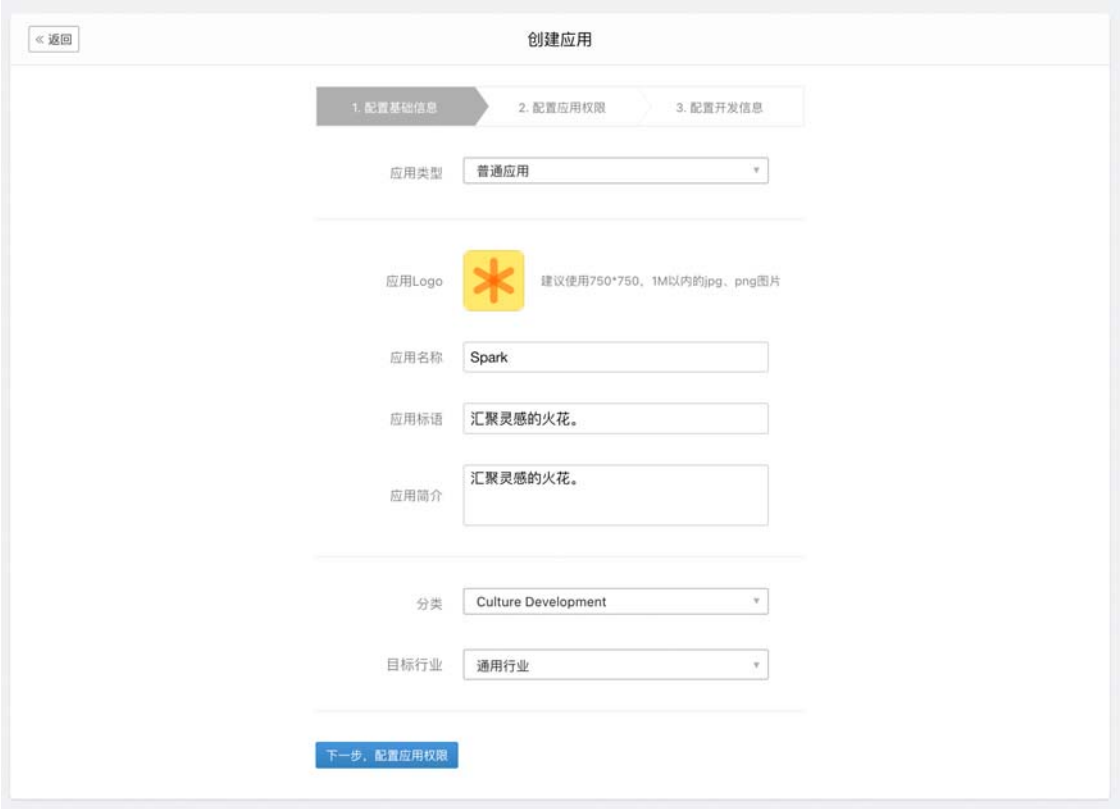
登录 服务商后台，进入【应用管理】-【标准应用开发】-【网页应用】，点击【创建应用】。

3.配置基础信息

应用基础信息主要是在企业微信应用市场的分类展示，以及企业客户安装以后工作台的展示。

请根据实际需要选择应用的基本类型，填写 Logo、名称、简介等基本信息，选择应用所对应的分类以及目标行业。

关于应用基本信息填写的标准，请参考企业微信应用接入指引的 基本信息填写 部分。



4.配置应用权限

根据应用实际使用的需要，选择是否需要企业授权相应的企业应用权限。当启用某一项权限后，企业管理员在授权安装应用时，将看到该权限的授权说明，请根据实际需要进行选择和填写。

关于应用权限信息填写的标准，请参考企业微信应用接入指引的　基本信息填写　部分。

5.配置开发信息

配置完应用权限信息后，需要配置应用开发的详细信息。

应用主页用于成员从工作台点击应用时打开的 URL；为了使支持应用内 Oauth 认证登录或者使用 JSSDK，须要配置对应的可信域名。

指令回调地址，是该第三方应用用来接收企业微信应用授权变更事件（应用添加、删除、修改）的唯一地址。

数据回调地址，是该第三方应用用来接收托管企业微信应用的用户消息、进入应用事件、通讯录变更事件的唯一地址。

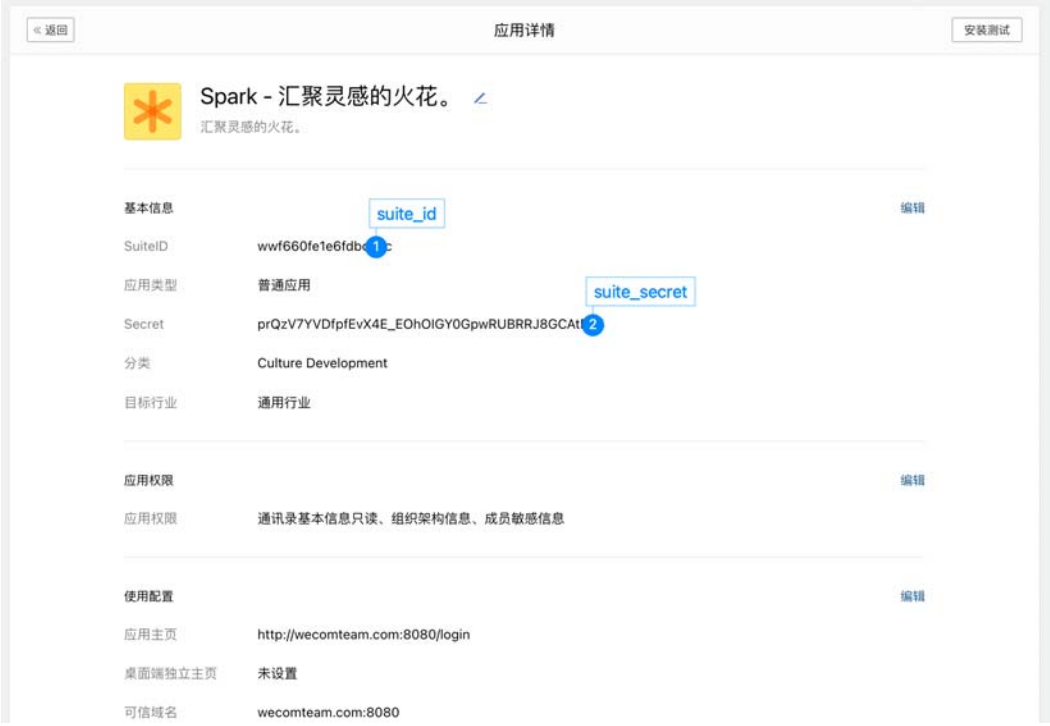
Token、EncodingAESKey 点击随机获取即可。

关于指令回调地址、数据回调地址的验证和配置，在下节课程中会详细介绍，在本教程中可以先暂时根据习惯填写保存即可，后续可以再次编辑和修改。

关于应用配置信息填写的标准，请参考企业微信应用接入指引的 使用配置填写 部分。

6.获取 suite_id / suite_secret

填写完应用的基础信息、应用权限、开发信息后，这个应用便创建成功了，随后页面将跳转到对应的应用详情页面。



在应用的【基本信息】这一栏，可以看到当前应用的 suite_id 和 suite_secret 信息，这两个数据在后续的流程中会多次用到，请妥善保管。

但是在应用的【回调配置】这一栏，页面提示 数据回调 URL 和 指令回调 URL “服务商未响应请求，将无法获取用户事件回调”。

详见：https://developer.work.weixin.qq.com/tutorial/detail/37

9.2 钉钉对接流程

1.登录钉钉开发者后台。

说明

只有管理员和子管理员可登录开发者后台。

2.在**应用开发**页面，选择**企业内部开发**，然后单击**创建应用**。

3.填写应用的基本信息，然后单击**确定创建**。

重要

请谨慎选择应用类型和开发方式，应用创建后无法修改。

4.应用创建后，在**应用信息**页面可获取 AppKey 和 AppSecret。

详见：https://open.dingtalk.com/document/org/create-orgapp