杭州融至兴科技有限公司

# 数据库运维管理

# 白皮书

2023 年 7 月

杭州融至兴科技有限公司

## 【公司介绍】

杭州融至兴科技有限公司，是一家专业的软件开发公司，致力于为客户提供高质量的定制化软件解决方案。本部位于杭州市西湖区，2014 年起成立南京、宁波、台州、嘉兴、金华、衢州等分公司。公司经营范围包括: 软件产品研发，系统设计服务、定制化开发、技术服务、网络安全服务、网络系统，计算机软硬件，通讯设备，计算机系统集成的设计、安装等；获得了华为、H3C、深信服、安恒、DELL EMC、IBM、宏杉、海康威视、大华、洲明、科达、华平等国内外著名厂家的鼎力支持和全力合作。

公司自成立以来，秉承开拓、进取、创新的创业精神，在完善已有成绩的同时，不断拓宽自己的市场，发展成集计算机网络技术研发、专业化系统集成服务、网络产品销售于一体，在国内计算机网络行业具有重要地位的公司。

### 企业资质

### 合作伙伴

# 目录

1 产品发展背景 ..... 1
2 产品介绍 ..... 1
2.1 市场定位 ..... 1
2.2 痛点分析 ..... 2
3 产品属性 ..... 3
3.1 产品迭代 ..... 3
4 产品体系架构 ..... 3
4.1 系统架构图 ..... 3
5 产品功能 ..... 4
5.1 库资源治理 ..... 4
5.2 身份管理 ..... 4
5.2.1 系统用户访问权限 ..... 4
5.2.2 库用户访问权限 ..... 5
5.3 访问控制 ..... 5
5.4 数据匿名化 ..... 5
5.5 连接验证 ..... 6
5.6 连接故障分析 ..... 7
5.7 权限请求 ..... 7
5.8 活动跟踪 ..... 7
5.9 洞察报告分析 ..... 7
6 产品后台 ..... 8
6.1 运行环境 ..... 8
6.2 部署方式 ..... 8
6.3 产品界面 ..... 9
7 产品价值 ..... 12

# 1 产品发展背景

在大数据使用愈发普及的市场背景下，为了更好的服务于业务，大数据形态不断扩展和业务逐渐成熟，大数据审计成为刚需；大量的审计数据结果需要更大的存储空间和更庞大的后续统计分析，而这正是大数据擅长的地方，所以演变成了“用一个大数据应用来审计业务系统的大数据”。在我国《中华人民共和国数据安全法(草案)》、《个人信息保护法(草案)》对数据的分级分类管理数据风险评估和安全保护个人信息处理原则和要求等做出了明确规定，极大的规范了数据安全管理制度。综合来看，随着未来数字经济的深入发展以及安全态势的不断变化，预计会有更多针对数据信息保护的法规制度出台，数据安全已经成为未来 5 年内我国网络安全市场中最重要、最有潜力的子市场之一。

# 2 产品介绍

## 2.1 市场定位

### 1） 市场规模分析

数据库安全方向在我国属于合规型刚需市场，相关的政策要求和技术标准较为清晰，目前已达到十亿级以上的市场规模，竞争强度不断加大，其他三类市场（数据防泄漏方向、数据加密方向、数据合规与治理方向）由于相关政策尚未出台，当前市场规模还偏小，市场增量尚未有效释放。

### 2） 等保 2.0 要求

技术要求（安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心）；管理要求（安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理）；云计算、物联网、移动互联、工控、大数据扩展标准以及行业标准。

## 2.2 痛点分析

### 1） 操作行为风险

数据库内部操作不明，外部的安全系统无法阻止内部工程师的恶意操作、滥用资源和泄露机密信息等行为，由此可见，以“防外”为主的传统网络安全解决方案失去了用武之地。

### 2） 第三方运维风险

数据库运维服务通常由第三方提供或由第三方人员实施运维，缺乏对维护人员操作过程的细腻度监控。无法对数据库维护全过程进行监管，一旦数据安全事件发生，无法追溯并定位真实的违规操作者。

### 3） 账号公用风险

高权限账号往往掌握着数据库和业务系统的命脉，高权限账号任何一个操作都可能导致数据被修改和泄露。最高权限的滥用，让数据安全变得更加脆弱，也让责任划分和威胁追踪变得更加困难。

### 4） 审计功能欠缺

采用数据库自带的审计模块，影响性能。一旦数据库系统出现问题，日志存在丢失风险。操作系统和数据库系统日志繁杂，无法进行风险分析和告警，技术人员使用效率不高。

# 3 产品属性

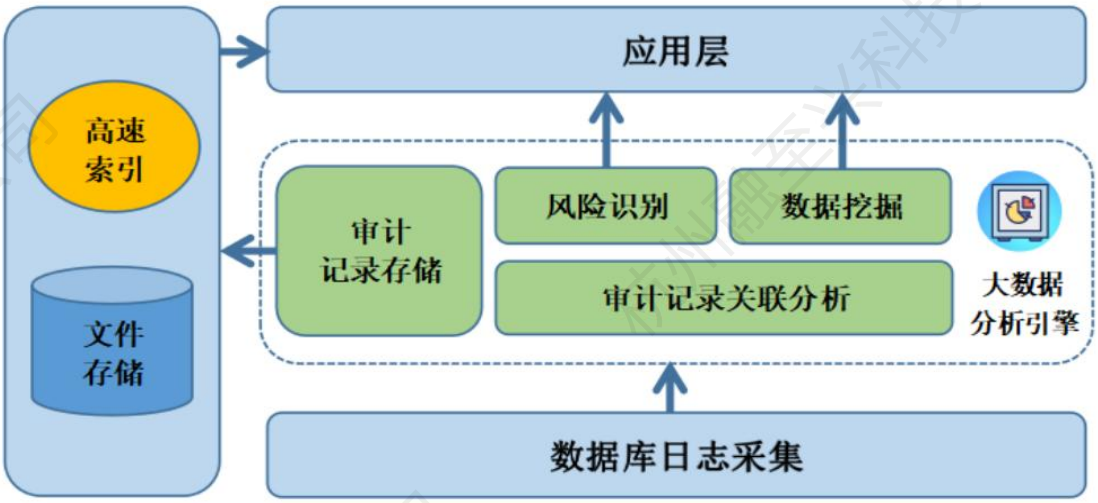
数据库运维管理系统是一款专门针对数据库的操作运维审计系统，以安全事件为中心，以全面审计和精确审计为基础，在不改变数据库系统的任何设置的前提下，对数据库的操作实现跟踪记录、定位，实现数据库的在线监控；不影响数据库系统自身性能的情况下，实现对数据库的在线监控和保护，及时地发现用户针对数据库的违规操作行为并进行记录，有效地弥补现有应用业务系统在数据库安全使用上的不足，为数据库系统的安全运行提供了有力保障。

## 3.1 产品迭代

| 迭代版本 | 版本说明 |
| --- | --- |
| 迭代 1.0 | 对数据库访问行为进行完整的记录和监控； |
| 迭代 2.0（目前） | 记录下数据库的所有访问和操作行为； |
| 迭代 3.0 | 对异常操作定位进行分析和预警；主动发现潜在的漏洞问题； |

# 4 产品体系架构

## 4.1 系统架构图



# 5 产品功能

## 5.1 库资源治理

针对企业内部的所有数据库表单进行框架结构设计，确定所需展示的数据类型、定义表和字段、设置关系等，确保数据的完整性和一致性。本系统支持几乎所有类型数据库，包括 ORACLE、MYSQL、MSSQL、SYBASE、DB2、达梦、人大金仓、神州通用、INFORMIX、PostgreSQL、Gbase、MongoDB、Redis、TeleData、Cache、HANA 等国内外主流数据库。

1) 具有海量的日志存储能力和高效的日志检索能力；
2) 对亿级规模的日志查询响应时间小于 1 分钟；
3) 数据库模型创建、数据加载；
4) 数据库完整性控制和安全性控制；
5) 数据库系统日常维护活动；

## 5.2 身份管理

对用户身份信息进行管理和控制的过程，以确保合法、安全和有效的访问权限。在身份管理中，包括用户认证、用户授权、用户角色分配、密码管理等方面的活动，确保身份安全和合规性的重要性。

### 5.2.1 系统用户访问权限

对登陆本系统的用户身份进行管理和控制，包括用户的创建修改、删除、改密等操作。帮助企业实现对用户的精细化控制和管理，确保企业信息的安全性；有效地避免用户权限的滥用和误操作，保障企业信息的可靠性；提高企业信息化建设的效率和水平，促进企业的发展和壮大。

1) 用户创建：用户管理可以通过管理员的操作，创建新用户并为新用户分配相应的权限和角色，以满足不同用户的需求。

2) 用户修改：用户管理可以修改已有用户的权限和角色，以适应不同用户在不同阶段的需求。
3) 用户删除：用户管理可以删除已有用户，以及清理无用的用户信息，保证系统的安全性。
4) 用户权限的设置：不同用户所拥有的权限和角色应该根据其工作职责和需求进行精细化设置，以保证系统的安全性和可靠性。
5) 用户密码的保护：用户的密码应该设置为强码，并定期修改以避免密码泄露和被破解。

### 5.2.2 库用户访问权限

对登陆数据库的用户身份进行管理和控制，通过有效的数据库登录用户管理，可以确保只有经过授权的用户能够访问数据库，并且可以限制用户对数据库的访问权限，有助于提高数据库的安全性和数据的保护程度。

1) 登录帐户管理：登录系统时需要提供的登录帐户名称和口令；
2) 数据库用户帐户管理：登录帐户在数据库中的映射；
3) 各种角色管理：对登录帐户或用户帐户的集合管理；

## 5.3 访问控制

对系统资源和数据的访问权限进行管理和控制的过程。在访问控制中，包括用户认证、授权策略、权限分配、审计跟踪等方面的活动。此功能对用户访问权限的控制和管理，并强调了保护系统资源和数据不受未经授权访问的重要性。当管理员创建一个新的数据库用户，可以为用户分配适当的权限。权限可以控制用户对数据库对象（如表、视图、存储过程、触发器等）的访问和操作。系统可设定的权限包括查询、增加、删除、修改、自定义。

## 5.4 数据匿名化

数据脱敏的主要目标是保护数据，同时保持数据的实用性，是一种保护敏感数据隐私的方法。为了防止企业身份或敏感信息被识别或暴露，可以通过对敏感

数据进行替换、删除或修改等操作，将原始数据转化为无法直接识别个人身份或敏感信息的形式，将敏感字段的真实值替换为虚化内容，这样可以减少数据泄露的风险，保护用户的隐私。

通过脱敏敏感数据，即使在数据泄露的情况下，攻击者也无法获取有价值的敏感信息。这可以降低数据泄露对组织的影响，减少潜在的金融、法律和声誉风险，本系统能够根据法律法规的要求，遵守合理的信息安全和隐私保护措施。

1) 支持灵活的规则策略配置；

2) 支持提供多种安全策略模版帮助用户快速建立安全策略；

3) 系统具有自定义脱敏规则的策略模版；

## 5.5 连接验证

当用户访问数据库系统时，系统对该用户和口令的确认过程，认证的内容包括确认用户帐户是否有效、是否能访问系统及能访问系统中的那些数据等。通过个人身份信息与数据库进行连接测试，可以保证数据库连接的稳定性和安全性，从而为我们的应用程序提供更可靠的后台支持。

1) 连接验证

验证“个人身份信息—数据库服务器—客户端”是否可以建立有效的连接。检查连接参数（例如主机名、端口号、用户名、密码等）是否正确，并尝试与数据库建立连接。

2) 连接状态检查

检查数据库连接的当前状态，验证连接是否处于打开状态，以确保连接正常运行，并且没有发生异常或错误。

3) 并发连接测试

对于多用户场景，连接测试可以测试数据库服务器在同时处理多个连接时的性能表现。通过模拟多个并发连接，并观察数据库服务器的响应时间和资源利用情况，可以评估其并发处理能力。

## 5.6 连接故障分析

验证数据库服务器对连接错误的处理能力。例如，当连接超时、认证失败或遇到其他连接问题时，它可以检测到并报告相应的错误信息，能够在提醒框内告知用户修改和调整方向。

## 5.7 权限请求

用户能够向系统管理员或授权管理者提交权限获取的申请的过程。在权限请求中，用户描述其所需的权限级别和理由（包括对特定表、视图、存储过程或其他数据库对象的读取、写入、修改或删除等操作），并等待管理员的审批和授权。提供管理员账号对用户的申请进行处理，支持“搁置、拒绝和原因、同意”三种处置方式。

## 5.8 活动跟踪

实时记录用户在数据库内的任意操作行为活动，对数据库操作进行细粒度审计的合规性管理，系统不仅对数据库操作请求进行实时审计，而且还可对数据库返回结果进行完整的还原和审计。通过对用户访问数据库行为的记录、分析、汇报，来帮助用户事后生成合规报告、事故追根溯源，同时通过大数据搜索技术提供高效查询审计报告，定位事件原因，以便日后查询、分析、过滤，实现加强内外部数据库网络行为的监控与审计，提高数据资产安全。

## 5.9 洞察报告分析

提供了对数据库操作的全面记录和追溯，实现数据库审计分析报告的产出，支持自定义时间段内的审计日志形成分析报表，可以帮助组织验证其数据库操作是否符合相关法规、标准和合规性要求。通过审计报告，可以查看数据库的活动记录、访问权限和安全事件，以确保组织遵守法规，并及时采取纠正措施。

# 6 产品后台

## 6.1 运行环境

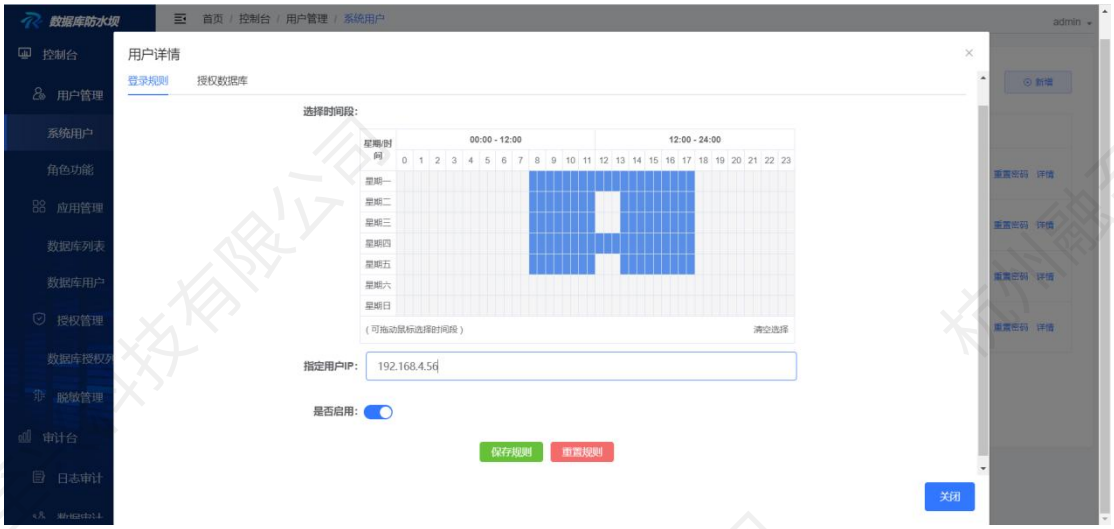
| 序号 | 设施 | 环境参数 |
| --- | --- | --- |
| 1 | 测试虚拟机 | Linux 操作系统；主流国产系统；应用程序版本 JDK1.8；<br>CPU：2/4 核；内存：4G 或以上；存储：50G 以上； |
| 2 | 服务器 | Linux 操作系统；主流国产系统；应用程序版本 JDK1.8；<br>CPU：8 核或以上；内存：8G 或以上；存储：2T； |

## 6.2 部署方式

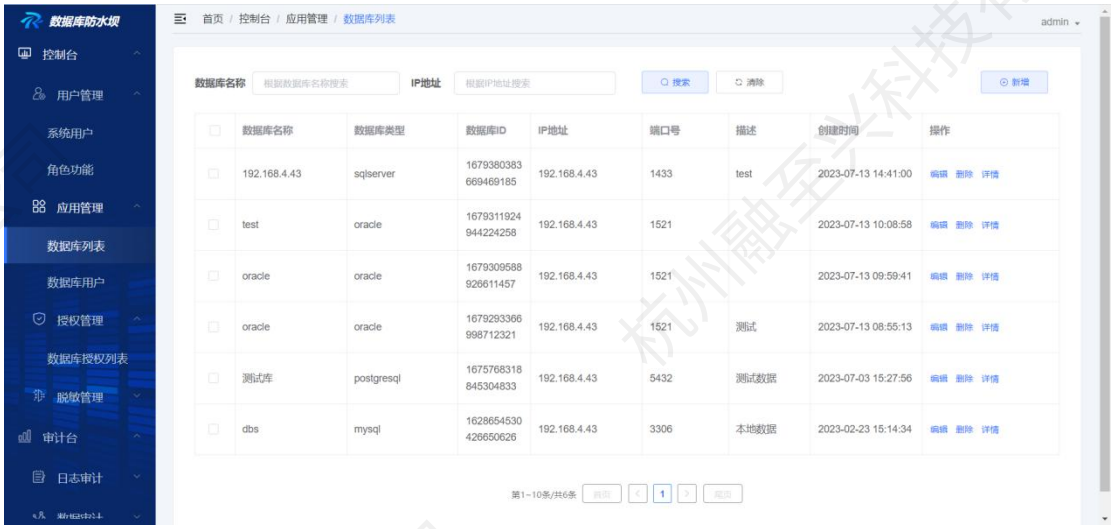
杭州融至兴科技有限公司

# 6.3 产品界面

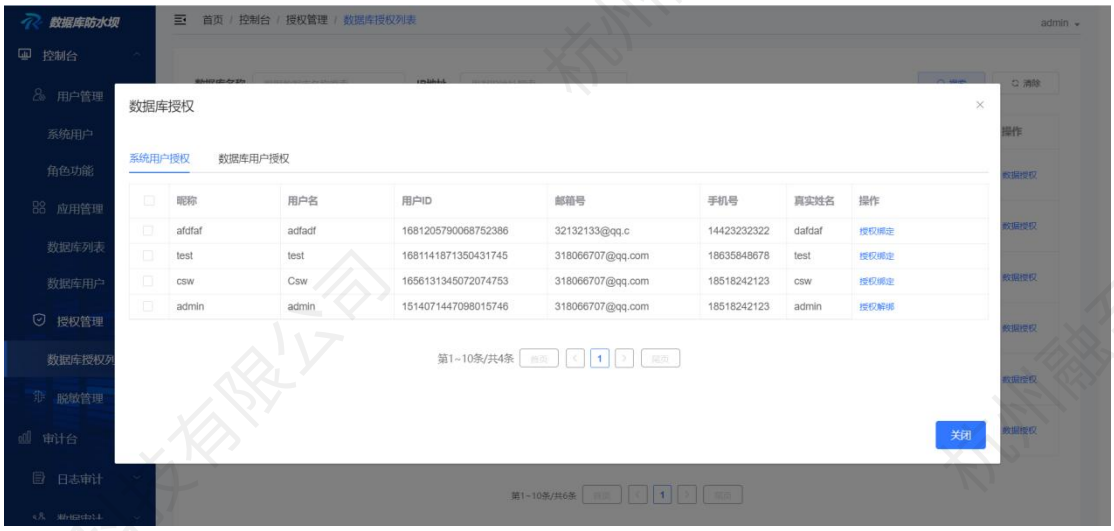
1) 系统用户权限设定

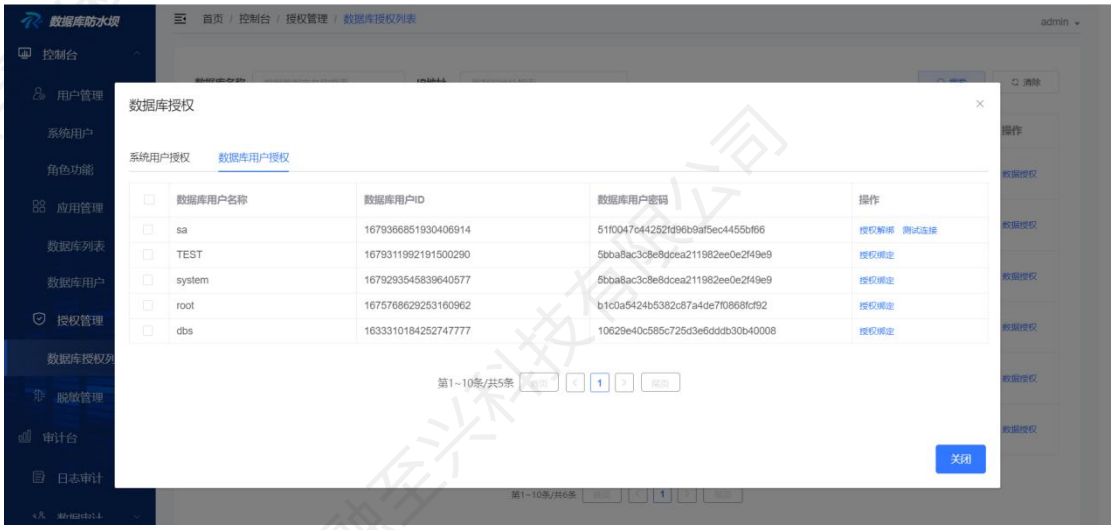


2) 数据库资源管理

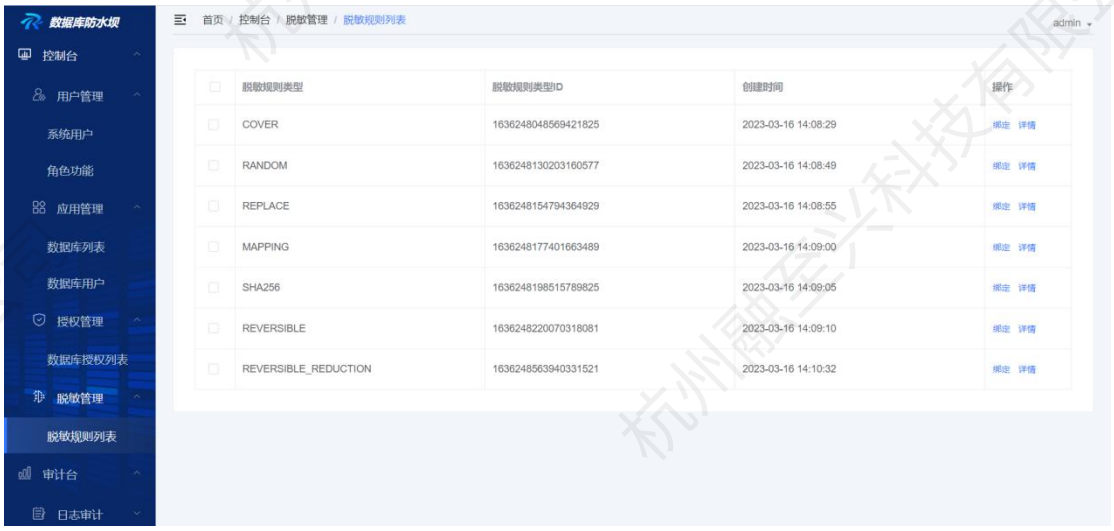


### 3) 数据库用户权限管理



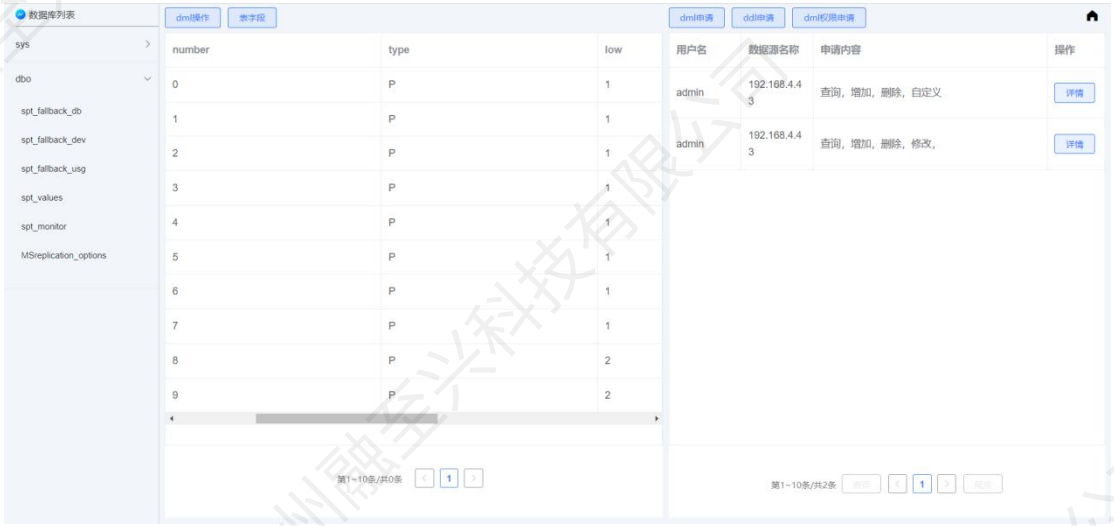




### 4) 脱敏规则制定表



5) 权限申请处置

6) 控制台




7) 数据库执行操作

# 7 产品价值

### 1） 实时监控

数据库行为审计系统可以实时监控数据库的操作活动，可以立即检测到异常行为和潜在的风险，提供实时的安全监控和响应能力。

### 2） 高效分析

具备强大的数据分析功能，可以对大量的审计日志进行快速处理和分析。它能够识别所有访问行为和潜在风险趋势，帮助组织及早发现数据库安全威胁，并采取相应的防护措施。

### 3） 准确溯源

详细记录数据库操作的日志信息，包括用户身份、时间戳、执行语句等，提供全面的操作审计和追踪功能。这些日志记录可以作为重要的凭证和证据，用于安全审计、合规性验证和事件调查等。

### 4） 报表简单

生成合规报表，显示了用户对数据库的操作活动、用户对不同数据库或表的访问权限、审计日志的汇总和统计信息等。这些报表都被设计为简单易懂的形式，提供了必要的信息以便管理员能够快速了解数据库的活动情况、安全状况和合规性情况。

### 5） 产品易用

提供综合的管理平台，集成了审计日志的收集、存储、分析和可视化等功能。管理员可以通过统一的界面进行配置、监控和管理，简化了操作流程，并提高了管理效率。