JUMING 聚铭

聚铭数据库安全审计系统
产品技术白皮书

南京聚铭网络科技有限公司

目 录

声明

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

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。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

第一章　概述

随着政府部门、金融机构、企事业单位、商业组织等对重要数据库业务系统依赖程度的日益增强，数据库安全及数据安全的问题越来越受到广泛关注。随着信息化建设、业务增长、系统上云等趋势的变化，各系统中的数据库服务器在不断增加，对数据库的管理的方式和通道也日趋复杂多样。在如此繁杂的情况下，引发了如滥用特权账号、滥用合法权限、身份验证不规范、备份数据暴露、审计记录不足等各类安全问题，并加大了 IT 内控审计的难度。与此同时，数据安全问题日益突出，如系统和数据库的通信协议存在漏洞、SQL 注入攻击、拒绝服务攻击、权限和账号被盗、弱口令等，给攻击者留下了可趁之机，也给管理者带来了管理层面的麻烦与困难。

另外，目前国内、国际的很多标准、法案法规都要求相关组织单位建设安全的审计系统，并确保审计信息是安全、完整、可查及唯一的。如：

- 《网络安全法》
- 《信息安全技术信息系统安全等级保护基本要求》（等保）
- 《涉及国家秘密的信息系统分级保护技术要求》（分保）
- 《通用数据保护条例》（欧盟 GDPR）
- 《商业银行内部控制指引》-计算机信息系统的内部控制

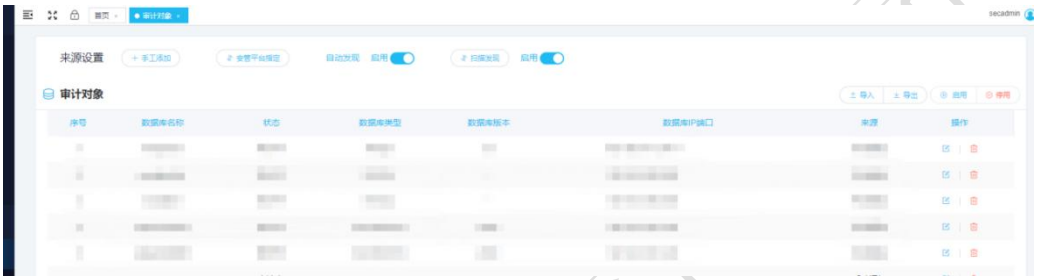
在普遍认知中，数据库审计系统是数据安全领域的入门级产品，产品历经近 20 年的发展，其技术路线和产品定位不断革新和演变，如今已经逐渐发展为新一代智能化产品。从产品演进看，第一代数据库审计系统解决了有无问题；第二代产品通过语法解析技术实现精准审计和告警；第三代产品凭借全文检索、多进程并发等技术，完成了性能瓶颈的突破，真正开始审计大型业务系统上的应用；而第四代审计产品主攻“智能发现”、“主动推送”等智能技术方向，通过机器自学，聚类访问来源、操作行为特征、资产信息，全面掌握每个数据库被访问的基础情况，有效建立基线，形成高密度可信边界，当访问来源及其操作行为发生变化时，自动伸缩基线，同时辅以通用型的轻量级策略，轻松建立防护圈，极大降低人工参与，快速落地安全策略，此时审计将不再是独立系统，不再独立工作，而是为平台提供数据的输入。这样更能与 KAFKA、FLUME、ELK 等先进的大数据分析和流式处理等分析技术结合，真正解决超大数据规模日志的利用问题，这也是未来数据安全的发展方向之一。

聚铭数据库审计系统（以下简称“系统”），本产品采用数据库动态基线检测技术、访问与反馈结果的双向审计技术、主流国际数据库与国产数据库的专用协议解析分析技术、中间件关联审计技术等，集传统的细粒度审计、精准化行为回溯、新型的用户行为风险分析、全方位风险告警能力于一体。

第二章　产品主要功能

2.1 数据库资产自动梳理

基于数据库协议嗅探技术（端口扫描），自动梳理数据库资产，快速添加规则进行审计。自动梳理数据库的基本信息包括：端口号、数据库类型、数据库版本、数据库实例名、数据库服务器 IP 地址等。



2.2 精确审计

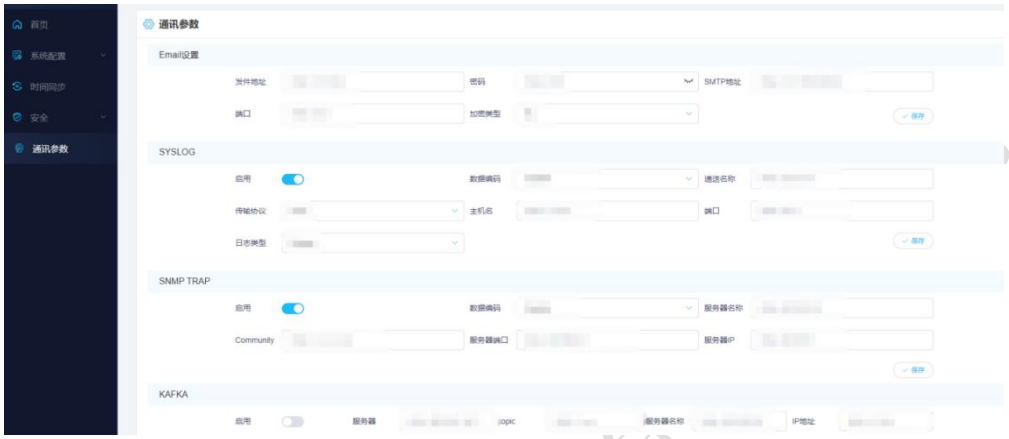
能对 SQL 语句的执行结果（成功或失败）、执行时长、返回行数、绑定变量值进行深度解析，帮助客户有效地提升审计内容的精确性。

2.3 安全策略

提供了黑白名单、自定义告警规则、审计例外等安全配置策略，帮助客户及时发现威胁，并告警。

2.4 多样的告警方式

当系统检测到数据库攻击、异常、违规等行为时，会自动触发系统预置访问规则进行实时告警，告警方式包括：邮件、Syslog、Snmp、Kafka，提升了运维人员在数据库访问异常情况下的处理效率。



2.5 丰富的报表模板

提供丰富的审计合规性报表、综合性报表、专项报表等报表模板，满足用户各种报表要求，同时可以实现定制化报表扩展，根据用户的实际需求输出符合企业自身业务的定制化报表。

2.6 实时用户行为监控

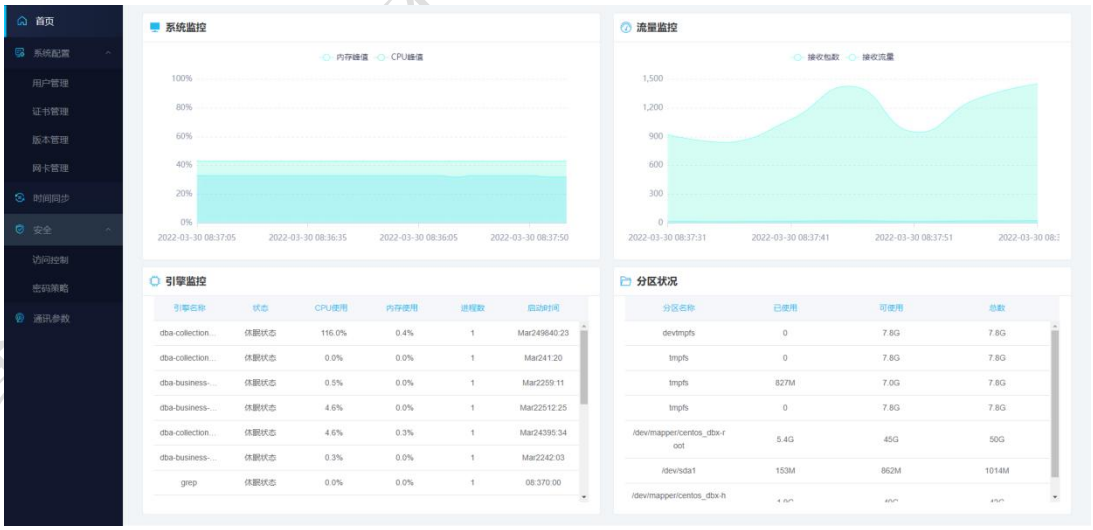
对网络的入侵行为、用户的异常行为和违规行为进行监控。

2.7 实时监控

对数据库的实时流量进行实时监控，帮助用户更好地了解数据库审计流量状态。

2.8 系统管理

提供了系统升级维护、系统运行状态监测、网络接口配置、数据存储空间大小设置等管理功能。



2.9 三权分立

实现三个管理员（系统管理员、安全管理员、审计管理员），分管系统的不同功能模块，满足三权分立要求。

第三章　产品价值

3.1 降低数据资产管理成本

通过自动发现能力定位数据库基本信息，如：数据库类型、数据库实例名、数据库服务器 IP 等，帮助用户梳理数据库底账，摸排僵尸库、临时库等，有效地提高了企业对于资产安全状况摸底及资产管理效率，降低了数据库资产管理成本。

3.2 全面摸查数据资产风险

分析数据库可能存在的安全缺陷，进行系统化的安全漏洞检查，安全配置核查，及时暴露当前 DBMS 系统的安全问题，帮助用户完成数据资产风险全面、自动化摸查。

3.3 帮助用户快速溯源追责

全面、精准地记录并展示数据库访问过程及操作结果， 通过应用关联审计功能，将安全事件进行精准定位、追责到人，发现问题爆发点，以便快速解决问题。

3.4 满足相关法律法规要求

全面满足《网络安全法》、《等级保护 2.0》、《分级保护》等国家法律法规要求，同时满足《行业/企业内控相关要求》，如政府、金融、电信、互联网企业等行业安全相关规范。

第四章　核心优势

4.1 高效处理（快）

结合归一化、模板化、列存化以及深入优化技术实现审计系统的极致性能，提升了数据入库的处理性能和数据出库的检索性能，同时优化了数据及结果集的存储性能。实现海量数据免压缩，百亿级日志规模下查询秒级返回的效果。

4.2 精准识别（准）

采用双向审计、SQL 词法分析、嵌套语句/长语句深度解析、数据包重组、绑定变量交叉关联、应用关联等技术，实现数据库协议与复杂语句的 100%精准识别和解析，彻底避免 “误审”、“漏审”等问题发生。

4.3 自动发现（智）

能够自动识别数据库结构变化，与安全审计策略形成联动调整，一旦防护目标出现结构变化，策略会跟随变化，确保审计针对性及防护效果始终处于正确基线。

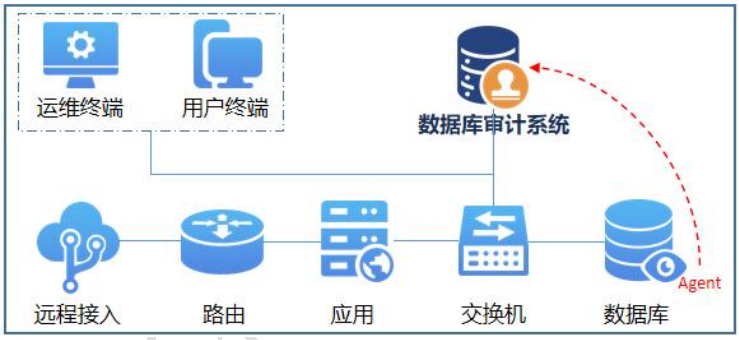
4.4 语句回放（录）

在传统的 SQL 语句内容审计基础之上，采用 SQL 操作语句回放技术，完整地还原整体操作过程，身临其境般展现“作案过程”和“作案现场”，实现数据库安全问题的有效分析和快速追踪。

第五章　部署方案

系统以旁路部署方式部署在网络之中，通过流量镜像、 agent 或者流量镜像与 agent 混合的方式获取数据库访问流量，对目标数据库进行审计与分析。

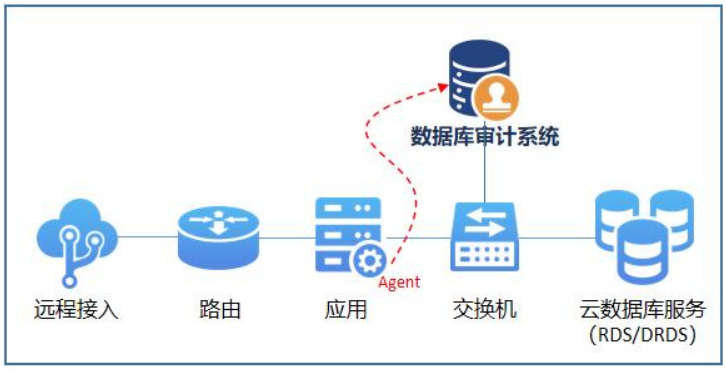
镜像流量部署模式



Agent 部署模式

当数据库部署在云环境上且为自建库时，系统可以通过在数据库主机上安装软件探针的方式获取数据库的通信流量，对数据库进行审计。

如果使用的是 RDS 或者 DRDS，可以通过将软件探针安装在应用主机上，获取数据库的通信流量，对数据库进行审计。



云数据库服务审计模式