聚铭数据库安全审计系统

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明

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和北京聚铭信安科技有限公司。

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

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

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。

1 概述

随着信息化的发展，人们的日常工作方式产生了巨大变化。基于计算机与网络的如 OA、ERP、CRM、FTP、邮件服务器、文件服务器应用系统在政府、军工以及其他各行业中得到了大量的部署与应用，实现了日常办公无纸化、网络化，极大的提高了办公灵活性与办公效率。绝大部分应用系统都是基于浏览器、Web 服务器、数据库典型的三层部署架构。其中，数据库中存储着大量的企业客户信息、财务信息甚至国家涉密信息。数据库成为客户核心数据的存储载体，数据库可以类比为所有业务系统的心脏，心脏的安全与稳定直接关系着前台业务的安全与稳定，数据库的安全直接关系着企业的命脉，其遭受的各种攻击，直接会导致用户敏感数据泄露，间接可能导致用户的破产然而数据库在使用过程中缺乏必要技术防护手段，使得存储在数据库里的大量敏感信息的安全性无法得到有效的保障，主要体现在以下几方面：

- 内部用户可以很方便的利用内部网络通过各种通讯协议进行刺探，获取、删除或者篡改重要的数据和信息；
- 内部授权用户对于系统不熟悉而导致误操作也时常给业务系统造成难以恢复的损失；
- 外部非授权人员（如黑客）多数据库进行恶意入侵，获取或者删除数据库里的数据；
- 所有针对数据库的安全事件发生后，无法进行有效的追溯和审计。

对于承载数据的容器—数据库，已然成为安全威胁的重点。信息安全建设的中心已由网络防护向数据防护转移，数据库安全控制已经受到了广泛的关注，与网络安全、系统安全以及协议安全一起构成了信息系统安全的四个主要研究领域。

同时，公安部等级保护、国家保密局 BMB17-2006 号文件中要求政府、涉密单位必须对与涉密敏感信息、业务系统相关的网络行为进行安全审计。在美国上市的公司，必须遵循的萨班斯(SOX)法案，要求对企业内部网络信息系统进行

评估，其中涉及对业务系统操作、数据库访问等业务行为的审计。

因此，为了解决数据库信息安全领域 的深层次、应用及业务逻辑层面的安全问题及审计需求，我司推出了聚铭数据库安全审计系统， 是一款专业的数据库安全审计产品，适用于等级保护、分级保护、企业内控、SOX、PCI、企业内控等信息安全规范，全面保障数据库的完整性、保密性和可用性。

聚铭数据库安全审计系统产品广泛适用于“政府、公安、财政、教育、能源、工商、社保、医疗、国土、金融、运营商、企业”等所有涉及数据库应用的各个行业。部署聚铭数据库安全审计系统，可以帮助用户解决目前所面临的各种数据库安全审计问题，避免数据被内部人员及外部黑客恶意窃取泄露，极大的保护了客户的核心敏感数据的安全！

随着越来越多的用户将传统的业务系统迁移至云环境中，云平台存在系统多、环境复杂的问题，安全问题尤其在云平台中更加突出，数据的泄露及篡改风险变的越发严峻，针对数据安全的防护以及事后审计追溯也变得越来越困难。对此，我司提供了基于虚拟化的云数据库审计解决方案。

2 产品价值

数据库审计系统提供七大产品核心价值，包括满足合规要求、提高监管能力、加快响应速度、快速定位故障问题、解决追责难题等。

监控高风险操作

风险：系统维护人员、外包人员、开发人员等，拥有直接访问数据库的权限，有意无意的高危操作对数据造成破坏。

防护： 完整记录数据库访问行为，识别越权、高危操作等违规行为，数据全记录，完整审计业务信息，重溯高危操作，准确定责。

监控敏感数据泄漏

风险：黑客、开发人员可以通过应用程序或工具批量下载敏感数据，内部运

维人员批量导出敏感数据。

防护：监控敏感数据流向，对操作的用户、时间及地点等进行监控和实时告警。

监控外部黑客攻击

风险：黑客利用 WEB 应用漏洞，进行 SQL 注入；或以 WEB 应用服务器为跳板，利用数据库自身漏洞攻击和侵入。

防护：通过入侵检测技术捕获和分析入侵攻击行为，监控 SQL 注入行为。

多样的预警方式

风险：外部发起的数据库漏洞攻击、SQL 注入攻击，内部违规的业务登录、高危操作等行为等等。

防护：系统提供基于灵活的策略配置、风险规则，实时高效告警，对风险行为进行 syslog 告警、snmp 告警、windows 报警、发送邮件、网关联动、短信等方式告警，提供事后追踪分析工具。

性能优化、辅助决策

为数据库安全管理与业务系统性能优化提供决策依据，掌控业务运行情况，直观评估运行性能，辅助决策。

高效运维、提高内控

三权分立独立审计，高效运维，提高内控

合规审计

提供符合法律法规的报告，满足等级保护、企业内控、网络安全法等合规性要求。

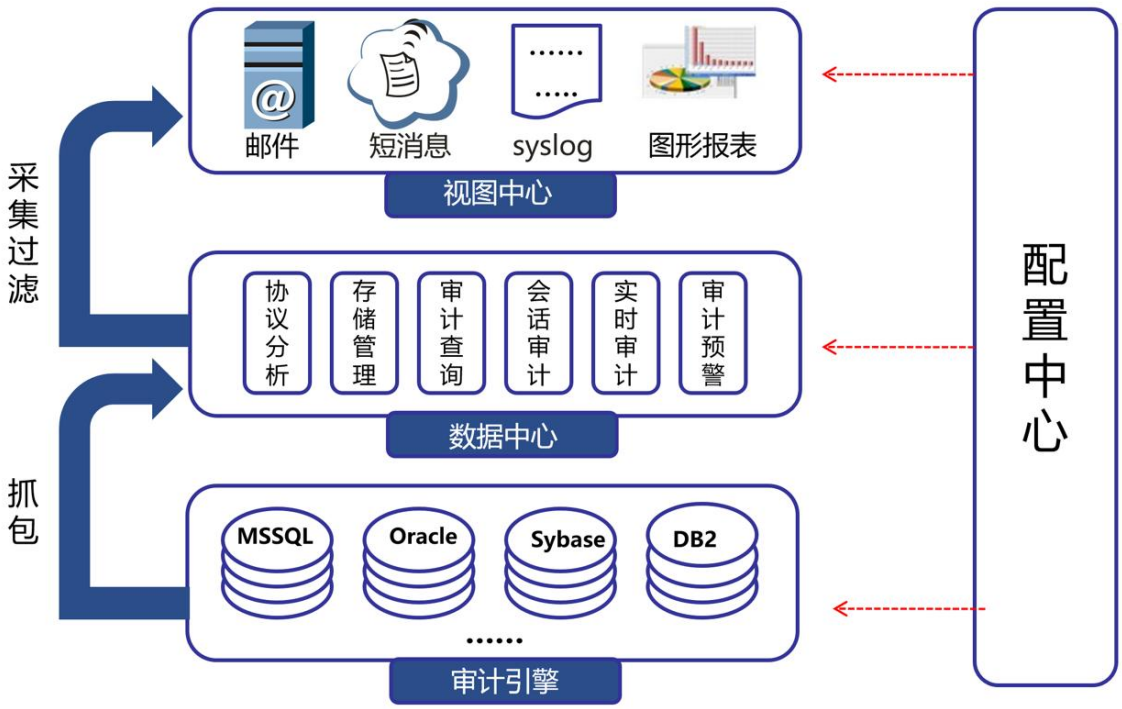
3 主要功能

3.1 一体化高性能处理平台

聚铭数据库安全审计系统采用一体机架构，组件化的逻辑体系，实现对数据捕获、数据分析、数据展示以及系统配置的分布式协同处理，逻辑上主要分为四大组件：

- 审计引擎 SAE（Security Audit Engine）
- 数据中心 SDC（Security Data Center）
- 审计视图中心 SVC（Security View Center）
- 系统配置中心 SCC（System Configure Center）

以旁路监听的方式接入网络，通过在交换机上将访问数据库的流量镜像或采用 TAP 分流监听等方式，使数据库审计系统能够监听到用户通过交换机与数据库进行通讯的所有操作。



3.2 高适用的数据库审计

除全面支持 Oracle，Microsoft SQL Server，DB2，Sybase, Informix、MySQL、Caché、Teradata、MongoDB、Postgressql、Redis 等数据库协议外，聚铭数据库安全审计系统还支持目前主流的国产数据库，包括达梦、人大金仓、南大通用、神舟通用等国产数据库协议，可准确分析出这些数据库的协议，支持对多种不同类型和不同版本的数据库的同时审计。

支持将多个数据库 IP 绑定为一个业务系统，后期的数据分析如流量、用户数和操作行为等，均以业务视角的方式分析展示。

3.3 云化环境，灵活部署

聚铭数据库安全审计系统适用虚拟云化环境，支持 SDN 引流审计、流量探针等多种灵活的部署方式，适用于公有云、私有云、混合云等多种类型云平台的数据库访问流量的审计，实现多种云架构下自建数据库、云数据库的全面审计，对数据库“零”影响。

3.4 授权池化，动态管理

聚铭数据库安全审计系统的授权采用授权资源池化的方式，提供虚拟化数据库审计模板和实例数的授权管理，可动态分配与回收模板授权、实例授权。

3.5 全面支持IPV6环境

聚铭数据库安全审计系统全面支持 IPV6 协议，不仅支持在 IPV6 环境下部署和管理，且支持在纯 IPV4 环境、纯 IPV6 环境及 IPV4 与 IPV6 混杂环境下对数

据库进行审计。

3.6 全面审计，高效分析

聚铭数据库安全审计系统完整记录对数据库的所有操作，以达到全审计的目的。以便用户在未知的风险事件发生后，定位问题的发生过程。

系统可实现在以亿为单位的数据中，多条件查询数据，在数秒内返回结果，同时对海量数据实现压缩比 90%以上的高性能存储。

3.7 实时运行监控

不仅对自身性能（CPU 使用率、内存使用率和硬盘使用率）进行状态监控，还对信息系统数据库产生的安全事件进行 24 小时监控，并以统计图表的形式展示，让管理员一目了然。防止受到特权滥用、入侵攻击、人为失误等等的侵害。通过安全态势提供实时监控页面，显示不同风险级别的事件统计值、审计数据统计图、威胁事件数图、新增因子表、在线用户数图来展示状态。当用户与数据库进行交互时，系统会自动根据预设置的风险控制策略，结合对数据库活动的实时监控信息，进行特征检测及审计规则检测，任何尝试的攻击或违反审计规则的操作都会被检测到并实时告警。

3.8 数据库操作审计

数据库操作审计主要包括语句的解析、操作类型、操作字段和操作表名等的分析。

- 支持语句操作响应时间的审计，支持语句操作返回行数的审计，支持数据库操作成功、失败的审计；
- 支持数据库绑定变量审计，支持访问数据库的源主机名、源主机用户的审计；
- 可审计操作的客户端名称；
- 可进行语句进行语法解析，分析语句的操作类型，操作对象等信息。

- 支持数据采集规则定义，对于不关心的数据可以不采集，有效保证系统审计的稳定性与针对性。

3.9 细粒度审计

聚铭数据库安全审计系统完整记录对数据库的所有操作，通过实时监测并智能地分析、还原各种数据库操作，解析数据库操作，还原 SQL 操作语句；跟踪数据库访问过程中的所有细节，提供数据库操作行为、应用服务器行为、终端录像，为追踪、惩罚犯罪份子提供强有力的证据。

- 全方位的数据库活动审计：实时监控来自各个层面的所有数据库活动以及活动的内容。如：来自应用程序发起的数据库操作请求、来自数据库客户端工具的操作请求、来自数据库管理人员远程登录数据库服务器产生的操作请求、操作返回的结果等。
- 潜在危险活动重要审计：提供对 DDL 类操作、DML 类操作的重要审计功能，重要审计规则的审计要素可以包括：用户、源 IP 地址、操作时间、使用的 SQL 操作类型。当某个数据库活动匹配了事先定义的重要审计规则时，一条告警将被记录以进行审计。
- 支持对数据库 SQL 操作语句的细粒度审计，可完整解析协议的所有 17 个字段；
- 支持正常请求信息的解析，同时支持对返回值行列结果全解析和全记录；
- 支持多元素符合逻辑的事件定义，包括操作时间域、操作方式、数据库用户名、数据库名、表名、应用程序名、执行时长、操作成功/失败、操作内容等；
- 会话分析与查看：单个离散的操作（SQL 操作、FTP 命令、TELNET）还不足于了解用户的真实意图，一连串的操作所组成的一个完整会话展现，可以更加清晰地判断用户的意图（违规的、粗心的、恶意的）。
- 敏感信息细粒度审计：对业务系统的重要信息，提供精确到字段及记录

内容的细粒度审计功能。自定义的审计要素包括登录用户、源 IP 地址、数据库对象（分为数据库用户、表、字段）、操作时间段、使用的 SQL 操作类型、记录内容。

- 支持超长 SQL 语句、注释内容、多嵌套语句、绑定变量、RPC 的审计。

3.10 SQL模版管理与敏感数据

数据库审计系统通过 SQL 语法分析，自动识别并抽取数据库句式语意相同但参数不同的语句，实现了 SQL 语句的归类及合并，构建 SQL 模版。对于一个每天都重复着同样的操作的被审计监控的业务系统，被原始 SQL 语句占据的空间就大大减少，节省了大量的存储空间。同时，数据查询效率大幅度提升。

通过 SQL 模版管理，可协助管理员对审计数据进行处理，将大量的、常见的语句设置为安全规则或过滤规则，大大增加了规则的准确度，优化系统识别事件规则库，形成安全语句和敏感语句管理，对信任语句正常执行，对敏感语句进行及时告警。

3.11 多达27类的查询条件精准检索

对用户而言，一旦发生安全事件，需通过查询事件的前后过程数据，以便获取有效的信息来协助管理人员找到相应的操作过程。系统支持以地址、性能消耗、语句数量等 27 类条件在 TB 级海量数据中快速检索，且能实时以图形化方式统计、展示查询结果。

3.12 基于业务的审计

聚铭数据库安全审计系统与用户实际业务结合，关注关键操作流程和敏感数据表，通过 SQL 行为和业务用户的准确关联分析，使数据库的访问行为有效定位到业务工作人员、基于风险、语句、会话、客户端、应用端、执行时长、返回结果等形成数据库的全量行为记录，进行有效的追溯和定责。例如，是否存在资金归集、漏费、消单等等，一旦发现异常，立即将审计结果以用户业务视角加以展示告警。

3.13 运维审计、辅助决策

聚铭数据库安全审计系统提供实时的数据库运行状态监控，针对数据库访问流量、语句数量、SQL 模板量、语句耗时等进行专项的界面分析；可针对执行量最多、访问最慢的语句进行梳理和呈现，提供专业的性能诊断分析，帮助用户优化数据库性能。

- 每日&每周的业务繁忙高峰，并提供具体峰值；
- 提供对业务性能消耗最大的操作内容，并提供日触发次数；
- 以力导向布局图和明细数据的方式实时监测当前连接会话，以便问题发生时定位故障点和责任人。

3.14 提供丰富报表展示

报表功能是审计日志大数据系统化、可视化分析的具体表现。聚铭数据库安全审计系统可提供根据安全经验和行业需求预定义的报表模板和审计报告，如审计设备自身健康状态分析报告、特权账号与异常时段分析报告、业务流量分析报告、塞班斯（SOX）法案数据库安全审计符合性报告等等。同时，为了提升报表的易用性，系统采用友好人性化的报表查看界面，包含报表缩略图展示、数据有效性的视觉展示以及报表内容支持自动建立快速访问。报表功能中的审计报告、周期报送功能，直观体现了审计日志和风险分析中数据库安全趋势，帮助安全管理人员更加便捷、深入的剖析数据库运行风险。

除了提供根据安全经验和行业需求预定义的报表模板和审计报告外，用户还可利用自定义报表功能定制报表。支持将生成的报表发送到指定邮箱，方便查阅。此外，报表支持导出以及打印功能。

3.15 安全事件回查追溯

当发生安全事件时，安全管理员可对过去某一时段的事件进行回查追溯，真实展现当时的完整操作过程，便于分析和追溯安全事件。很多安全事件或者与之关联的事件在发生一段时间后才引发相应的人工处理，这时，作为独立审计的数

据审计系统就发挥作用，由于有全审计功能，数据都保存在后台（包括相关的告警），可快速定位相关事件，缩小范围，使得追溯变得容易。同时，由于独立监控审计模式，使得相关的证据更具有公证性。

3.16 多样的预警机制

系统将审计事件划分为高风险、中风险、低风险三个级别。对告警信息，系统提供了多形式的预警（丰富的外部、内部接口），包括通过 SYSLOG 告警、SNMP 告警、WINDOWS 报警、发送邮件、网关联动、短信猫等方式。

3.17 精细化的配置管理

在用户环境中配置数据的重要性不言而喻，为防止系统出现操作失误或系统故障导致数据丢失等问题，因此，需精细化的配置管理，能将全部或部分配置数据集合恢复到设备。聚铭数据库安全审计系统支持对审计配置全集和分量（模块）的配置，执行备份与还原。当用户发生设备损坏，更换备机等情况时，能快速进行审计系统配置还原，实现无损更换使用。方便运维人员对审计系统维护，快速还原某个模块的某个配置，实现精细化的配置管理。

3.18 高性能海量数据挖掘及数据建模分析

聚铭数据库安全审计系统完整记录对数据库的所有操作，以便用户在未知的风险事件发生后，定位问题的发生过程。系统可实现在以亿为单位的数据中，多条件查询数据，在数秒内返回结果，同时对海量数据实现压缩比 90%以上的高性能存储。

系统提供多维度海量审计数据对比分析工具，从不同的空间、时间对各个维度进行同比和环比分析；

4 产品优势

4.1 布

旁路部署，不改变现有网络架构，不对数据库性能和网络吞吐产生任何影响。

无需配置数据库用户名和口令。

4.2 云

支持虚拟化云环境，支持 SDN 引流审计、流量探针等多种灵活的部署方式，适用于公有云、私有云、混合云等多种类型云平台的数据库访问流量的审计。

4.3 审

支持国内外标准与非标准近 20 种数据库的协议解析，实现从语句到会话到执行时长，再到语句数量的全方位审计。同时对非数据库的通讯流量加以记录。

4.4 查

支持以地址、性能消耗、语句数量等 27 类条件在 TB 级海量数据中快速检索，且能实时以图形化方式统计、展示查询结果。

4.5 钻

支持对查询结果的深度钻取，进行多角度的结果过滤，且不限制钻取次数。支持多层深度钻取解析数据包，分层次分角度解析会话信息。

4.6 警

提供丰富的外部、内部接口，可采取 SYSLOG、WINDOWS、邮件、SNMP、短信等方式实时通知管理员。

4.7 示

系统拥有多达 26 个交互式图表，每日超过 90%以上的工作内容，通过图表均能一目了然，了解当前的安全态势。

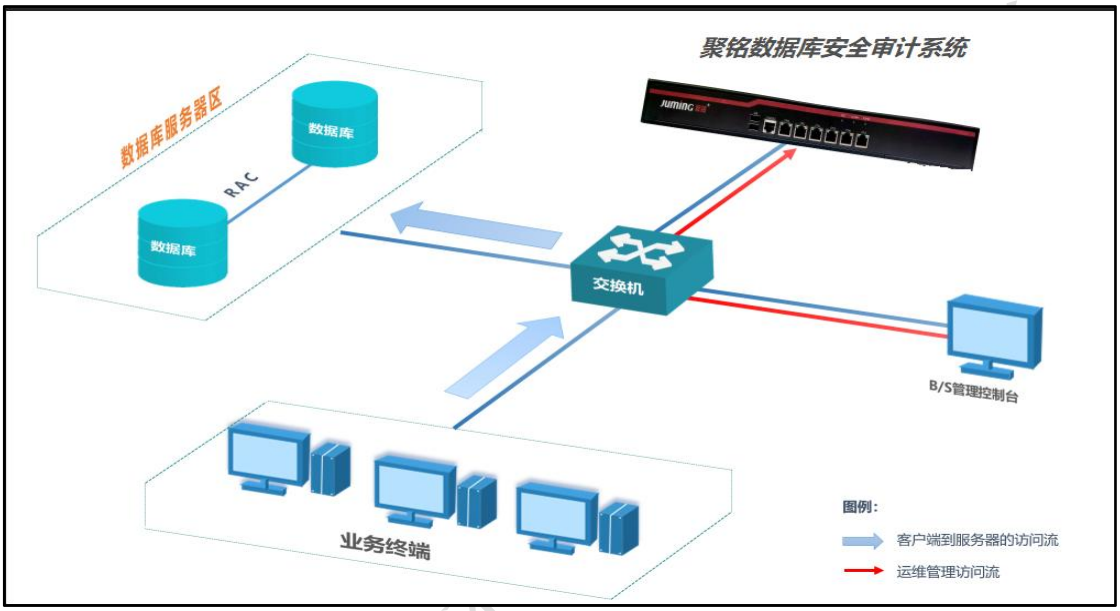
4.8 存

单设备提供本地最大 4T 存储空间，同时对海量数据实现压缩比 90%以上的高性能存储。可设置数据归档外传，实现数据存储的无限扩展。

5 典型应用

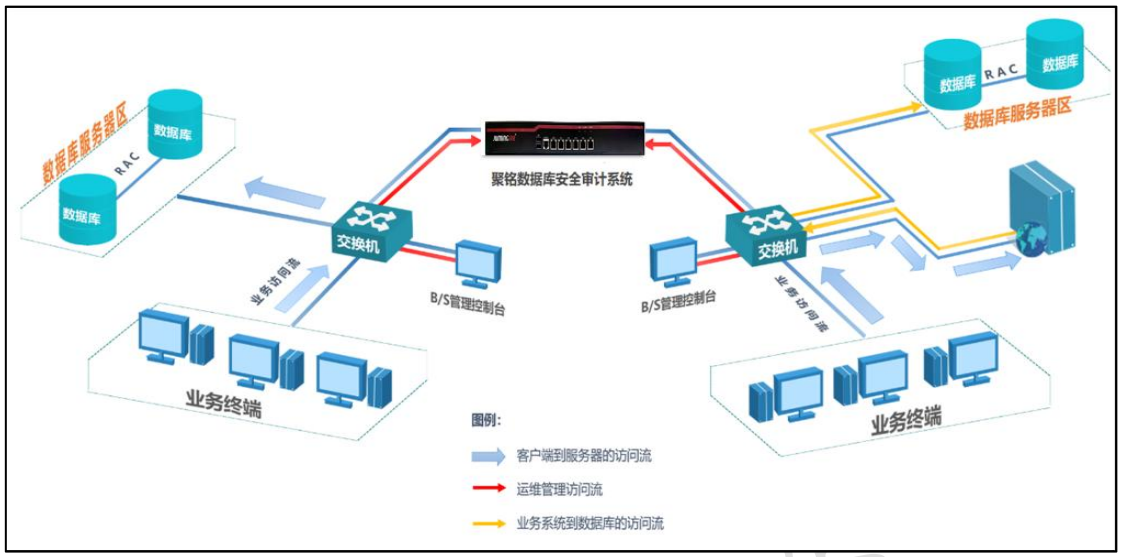
5.1 典型部署

业务系统客户端与数据库客户端一对一对应，直接对数据库服务器进行访问，一台审计系统部署在连接数据库的交换机上，监控所有对数据库的访问记录，并对审计记录进行管理与分析。



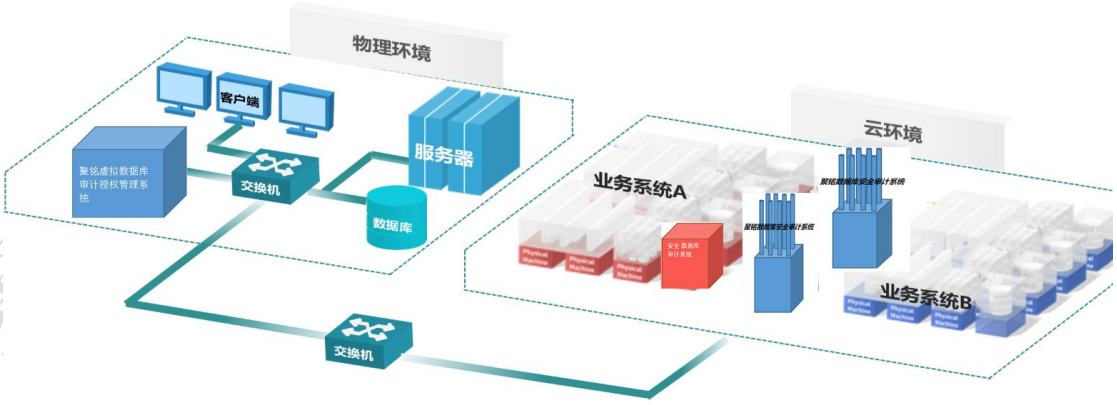
5.2 多路部署

业务数据库环境规模较大，或者必须有多个审计数据采集点的情况，一台审计系统多个监听口分别数路采集不同采集点的流量，集中分析处理，并对审计数据进行集中分析管理。



5.3 虚拟化部署

聚铭虚拟数据库安全审计系统以旁路监听的方式接入云网络，可通过 SDN 引流或流量探针等方式，将访问数据库的流量引至虚拟数据库审计系统，使数据库审计系统能够监听到用户与数据库进行通讯的所有操作。同时，虚拟数据库审计授权管理系统部署在一台物理机上，为多台虚拟数据库审计系统提供授权服务。



6 结论

聚铭数据库安全审计系统是能够实时监视、记录网络上的数据库活动，对数

据库操作进行细粒度审计的合规性管理系统。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部网络行为记录，提高数据资产安全。