GRIDSUM 国双

数据库审计系统白皮书

北京国双科技有限公司

2020年7月

概述

随着计算机技术不断进步带来的企业信息化的飞速发展，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应用软件，如OA、ERP、CRM、FTP、邮件服务器、文件服务器等，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，极大的提高了公办灵活性与办公效率。其中，数据库存储着大量的企业客户信息、财务信息甚至国家涉密信息。然而数据库使用过程中缺乏必要技术防护手段，使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。

针对数据库存在的诸多安全风险以及审计需求，国双科技凭借对数据安全方面的技术积累和沉淀，推出了数据库审计系统（以下简称“DBA”）。通过实时监控、记录网络上的数据库活动，对用户访问数据库行为进行记录、分析和汇报，实现数据库操作行为的全方位、实时、细粒度审计，帮助用户事后生成合规报告、事故追踪溯源，提高数据资产安全。

本文将梳理数据库审计系统的架构和能力，深入理解数据库审计系统的意义和价值，以及系统的特点。

目录

1.产品介绍

1.1 产品概述

国双数据库审计系统是一款专业、实时进行数据库访问监视与审计的数据库安全设备。能够多角度分析数据库活动，并对异常行为进行告警、审计和记录。

国双数据库审计系统系统支持Mysql、Oracle、SQL Server、PostgreSQL、DB2、Mongodb、Cassandra等关系型、非关系型及实时数据库的审计分析，采用高性能流量捕获引擎保证数据流量的完整性，高速审计匹配引擎保证违规操作的及时告警，旁路部署方式在不影响数据库的前提下，达到安全管理的目的。

- 真实准确还原用户操作数据库情况；
- 迅速发现并及时响应相关数据安全威胁；
- 帮助企业单位切实保障核心数据库资产安全。

1.2 产品形态

数据库审计系统产品提供多种授权模式，满足不同业务需求。

1.2.1 软件形式

数据库审计系统产品可以软件授权形式提供安全功能和服务，满足单机部署、云部署等各种场景需要。

1.2.2 软硬一体化

数据库审计系统产品可以软硬一体化形式提供安全功能和服务，软件授权与提供的硬件绑定。

数据库审计系统软硬件一体化服务器

2.产品功能

2.1 系统总体架构图

2.2 丰富的数据库协议支持

国双数据库审计系统支持目前市场上绝大部分主流数据库，如常用的关系型数据库、非关系型数据库、实时数据库等，包括Oracle、Mysql、PostgreSQL、SQLServer、DB2、Sybase、MongoDB、Cassandra等。

2.产品功能

2.3 全方位细粒度协议解析

系统通过对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时审计，而且还可对数据库系统返回结果进行完整的还原和审计，包括数据库命令执行时长、执行的结果集等内容。

2.4 多维度数据库操作审计

DBA 可实时监控数据库各种帐户（如超级管理员、临时帐户等）的数据库操作行为，准确发现各种非法、违规操作，并及时告警响应处理，降低数据库安全风险，保护企业数据库资产安全。

支持基于IP 地址、用户/用户组、数据库类型、数据库操作类型、数据库表名、操作等精细组合数据库审计策略，从而全面监测各种非法违规操作。

支持完整还原数据库操作，实时审计用户对数据库系统所有操作，精细还原 SQL 操作命令包，实现数据库安全事件准确全程跟踪定位。

2.5 实时告警

DBA可以根据配置的策略所产生的事件进行实时推送。以便于管理员及时发现潜在危险，快速处理，保证网络运行的安全。

2.产品功能

2.6 系统管理责权服务分离

DBA提供一套安全的自身系统管理机制，严格按照相关技术标准与管理要求实行系统管理员、日志审计员、系统操作员三权分离管理。

2.7 生成和导出合规的分析报告

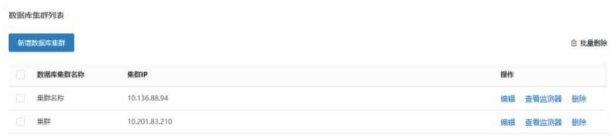
国双数据库审计系统具有自动生成和导出合规的分析报告的能力，包括：

- 支持基本报告生成：通过输入开始时间和结束时间，自动生成合规报告。报告包括数据库列表、账号、客户端访问情况、服务器访问情况等。
- 支持违规风险报告：包括支持向用户展示出审计规则下的操作信息、告警信息等。
- 支持定制化报告：针对不同机构、不同业务逻辑，针对用户的特殊要求进行定制化报告。

3.产品特点

3.1 集群管理及审计

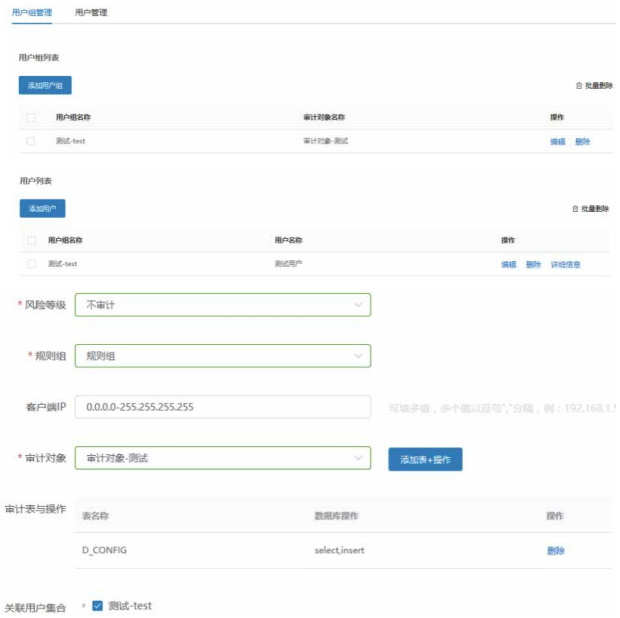
DBA既提供单一IP数据库服务器的审计又提供连续IP、动态IP段的集群式数据库服务器的审计。系统管理员可根据用户的物理或逻辑集群定义进行相应的集群配置、制定审计规则，提供所属集群的展示。



3.2 灵活的审计用户管理

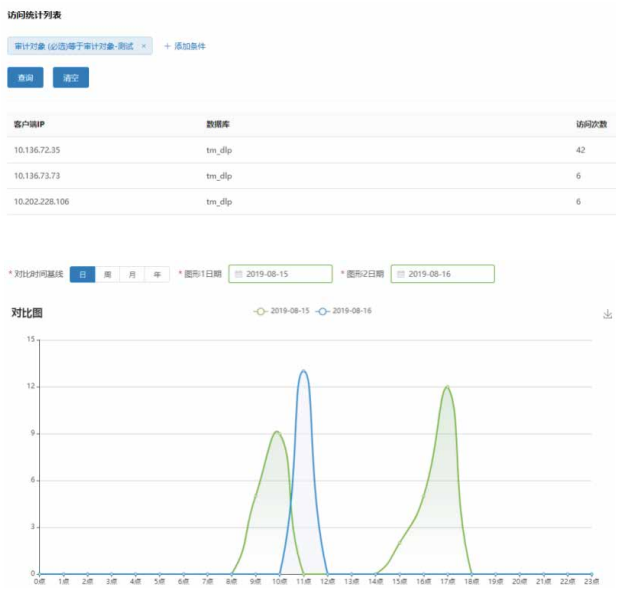
DBA 提供基于审计用户的审计功能，通过建立用户组及用户，以及在制定规则的同时可选择性的添加关联用户集合。管理员可通过数据分析功能查看同一个用户组下用户的操作行为和表集合；也可通过用户的表关联+操作详细信息方便的查看其审计的表对象。为安全事件的准确、快速追踪和定位提供了有力支持。

3.产品特点



3.3 丰富多样的图表展示

国双数据库审计系统为用户提供了丰富多样的数据库统计分析功能，并且以图形或列表的形式进行展示，形象且直观。下图为客户端访问某种类型数据库的统计表和，一段时间内访问流量对比图。



3.4 高速流量捕获引擎

数据库审计系统采用零拷贝技术，可以减少数据拷贝次数和简化协议处理，在应用和网络间可以提供更快的数据通路，增加网络吞吐率，有效降低网络丢包率，保证千兆网络数据的完整性和可用性。

GRIDSUM 国双

关于国双

国双（NASDAQ:GSUM）是中国领先的企业级大数据和人工智能解决方案提供商。基于国双大数据平台独有的分布式数据架构和先进的实时、多维度关联性分析技术，同时利用自然语言处理、知识图谱等人工智能技术，国双的解决方案能够使客户充分洞悉数据间的复杂关系，获得全新的商业洞察，帮助企业和政府客户作出更好的业务决策，有效驱动产业智能化和数字化转型。

服务领域

工业互联网　智慧能源　智慧司法　新零售　航空及旅游　汽车　运营商

合作伙伴

服务客户

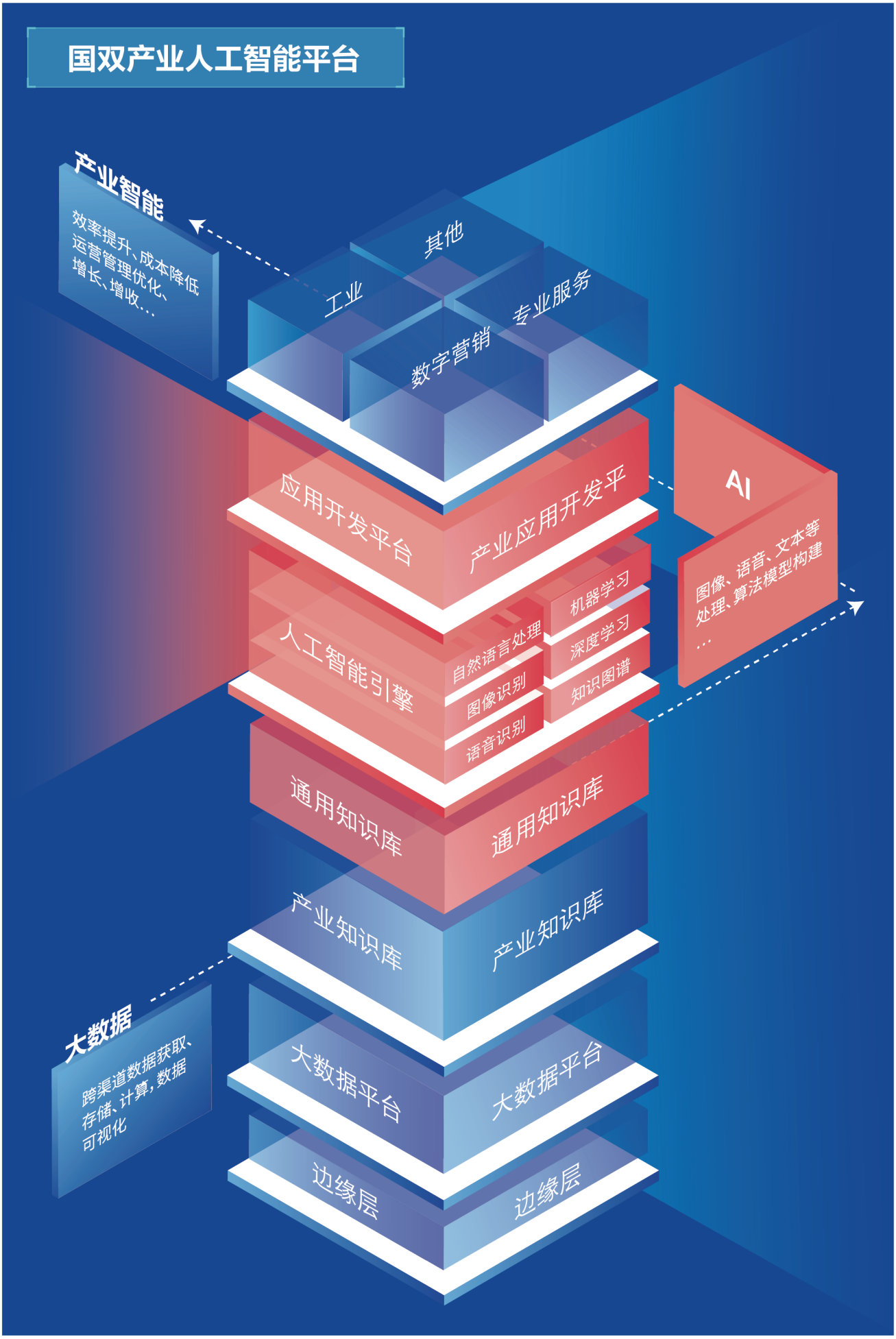
北京总部

地址：北京市海淀区北四环中路229号国双大厦

电话：(86-10) 8261 9988

传真：(86-10) 8261 9993

国双官方微信


国双产业人工智能平台
产业智能
效率提升、成本降低
运营管理优化、
增长、增收...
其他
工业
专业服务
数字营销
应用开发平台
产业应用开发平
AI
图像、语音、文本等
处理、算法模型构建
...
人工智能引擎
机器学习
深度学习
知识图谱
自然语言处理
图像识别
语音识别
通用知识库
通用知识库
产业知识库
产业知识库
大数据
跨渠道数据获取、
存储、计算，数据
可视化
大数据平台
大数据平台
边缘层
边缘层