UMA数据库审计系统

产品概述

随着计算机技术的飞速发展，数据库的应用也随之广泛深入到各个领域，各种应用系统的数据库中大量数据的安全问题以及敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。

华为数据库审计系统是华为公司自行研制开发的新一代数据库安全审计系统。通过旁路侦听的方式对访问数据库的数据流进行采集、分析和识别。实时监视数据库的运行状态，记录多种访问数据库行为，发现对数据库的异常访问，并对访问数据库的相关行为、发送和接收的相关内容进行存储、分析、排名和查询。

产品特点

完整的数据库版本支持

- 覆盖主流商用数据库，包括：Oracle 8/9/10/11等、Sybase所有版本、SQL Server 2000/2005、Informix所有版本、DB2所有版本。

“细粒度”数据库审计

- 深度解码数据库网络传输协议，完整、细粒度分析并再现用户数据库操作活动过程。

灵活的数据库访问策略

- 提供全方位的策略规则匹配，策略因子包括：数据库操作来源IP地址、数据库服务器IP/端口、数据库类型、数据库名称、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL操作语句(DDL、DML、DCL)、高级权限操作、存储过程、数据库表组(表、字段、值)、数据库SCHEMA、操作执行时间、操作返回条目大小等。

完整的数据库操作回溯

- 记录数据库会话详细细节，当发生数据库安全事件时，用户可根据数据库地址、源客户端地址、事件发生时间、数据库安全事件内容等，快速检索定位操作会话。

直观的统计报表

- 统计报表以饼状图、折线图、柱状图、表格形式输出，统计结果支持HTML、PDF、EXCEL等格式导出。

可靠的实时监控

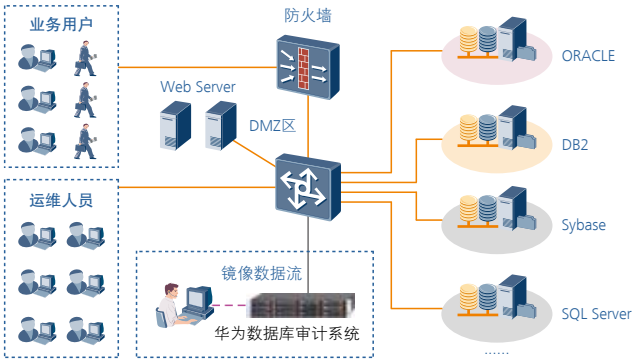
- 实时监控数据库的运行状态、SQL语句数量、数据库流量使用情况、数据库的会话连接数等；不仅提供数据查看，而且提供直观的视图查看。

HUAWEI

UMA数据库审计系统

典型方案

华为数据库审计系统旁路部署在交换机上，通过配置交换机将数据镜像到数据库审计系统的数据采集口，采用旁路侦听的方式对访问数据库的数据流进行采集、分析和识别。部署简单，管理方便，无需改变网络拓扑也不需要安装任何插件或嗅探器。



产品规格

型号	标准版	企业版
硬件特性		
硬件规格	尺寸：高*宽*深=87mm*440mm*685mm CPU：1*英特尔至强四核CPU 内存：8G内存 电源：冗余可热插拔电源，风扇 系统盘：2*300G SAS RAID1 数据盘：4*2T SAS RAID 10 （可选配磁盘容量，最大支持24T存储空间） 网络接口：主板集成6个GE口，支持IOAT	尺寸：高*宽*深=87mm*440mm*685mm CPU：2*英特尔至强四核CPU 内存：16G内存 电源：冗余可热插拔电源，风扇 系统盘：2*300G SAS RAID1 数据盘：4*2T SAS RAID 10 （可选配磁盘容量，最大支持24T存储空间） 网络接口：主板集成6个GE口，支持IOAT
性能和功能		
功能参数	系统管理，数据库策略配置，日志审计，统计报表，实时监控，系统监控。	系统管理，数据库策略配置，日志审计，统计报表，实时监控，系统监控，返回结果捕获，变量绑定解析，原始pcap数据包捕获。
数据库支持	Oracle 8/9/10/11等、Sybase所有版本、SQL Server 2000/2005、Informix所有版本、DB2所有版本	
其他特性		
日志输出	支持对syslog日志服务器的输出；支持FTP/SFTP的审计日志的备份任务；	
告警动作	支持WEB页面的实时告警；支持邮件实时告警。	