UMA-DB数据库审计系统

华为技术有限公司

HUAWEI

产品概述

华为UMA-DB数据库审计系统是华为自行研制开发的新一代数据库安全审计系统。数据库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。系统在网络中实现对数据库的访问行为、内容进行审计、报警、过滤和分析，支持主流的多种数据库的审计，如：oracle、informix、DB2、SQL server、Sybase等。

产品型号与外观

UMA-DB-ST

1*四核CPU，8G内存，2块300G SAS（raid1）为系统盘，4块2T SATA（raid10）为数据盘，安装存储节点控制板管理软件标准版本

UMA-DB-EN

2*四核CPU，16G内存，2块300G SAS（raid1）为系统盘，4块2T SATA（raid10）为数据盘，安装存储节点控制板管理软件企业版本

产品功能简介

华为UMA-DB数据库审计系统的主要功能包括：系统管理、策略管理、日志审计、统计报表、实时监控和系统监测。

- 系统管理是对数据库审计系统本身的配置，以便对系统的访问、授权与管理等功能。其中包括：接口配置、用户管理、输出配置与授权许可。
- 策略管理是对目标数据库服务器资产的添加、授权、策略制定、告警设置等配置功能。其中包括：资产、白名单、对象、策略、动作与管理。
- 日志审计是以数据库服务器资产为审计对象，从而记录运维人员对数据库服务器的操作与访问的行为；便对数据库运行情况的实时查看、故障分析以及告警级别的确定。其中包括：会话审计、策略告警、异常告警与系统事件。
- 实时监控提供数据库实时监控功能，可以对总体或数据库类型或数据库组别进行实时监控，监控其网络流量、数据包、突发链接、并发连接数、SQL语句数。并提供波形图展示，用户能够直观地了解当前数据库运行状态。
- 系统监测是用户通过数据库审计系统的审计数据信息的显示；以便用户全面的、统一的、及时的对数据库服务器的运行情况进行分析与排错。其中包括：最新策略告警、最新违规操作、最新系统事件。

产品特性与优势

保证数据库访问审计的完整性

- 实现对数据库各种操作行为的完整解析并再现用户数据库操作活动会话过程，能深入细化到SQL操作涉及表组、字段、视图、索引、过程等；
- 华为数据库审计系统采用现今最先进的网络数据审计技术——流技术，保存“流生命期”内“上下文”相关环境，进行分析解码，从而实现深度解码数据库网络数据流传输协议，完整、细粒度分析并再现用户数据库操作活动会话过程；
- 会话审计内容从访问的发起、连接、到结束进行完整记录，完整记录用户数据库会话细节，包括用户数据库登录行为、登出行为、SQL操作用户名称、SQL操作源程序名称、SQL操作源终端名称、SQL操作源终端登录用户名称、SQL会话参数设置、SQL操作语句、SQL操作返回状态、SQL操作涉及表组、字段、视图、索引、过程、函数、SQL DML操作影响行数、SQL语句执行时间、原始数据库记录包等；
- 完整解析、记录、关联SQL操作语句参数，可自动回溯重构完整SQL操作语句；
- 华为数据库审计系统最大支持并发4096连接，68000SQL命令/秒的数据库业务环境，完全能满足用户的各种峰值环境。

提供了灵活的策略设置

- 华为数据库审计策略配置灵活，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；

- 提供数据库SQL语句执行时间、数据库操作闲置时间策略报警，提供数据库DML、DDL等操作影响行数策略报警，提供数据库SELECT SQL操作语句返回行数策略报警；
- 根据设定的数据库策略，可选择对关键资源操作行为进行数据包录像、深度分析解析开关。

权限分离

- 实现对管理员、审计员、操作员进行权限划分，规定各角色用户只能在其权限范围内对数据库审计产品进行操作，同时对整个操作进行自身审计；
- 华为审计系统满足各种法案法规中明确提出对工作人员进行职责分离，系统设置权限角色分离。在系统中提供超级管理员、资产管理员和审计管理员权限分离；
- 资产管理员可以添加数据库审计服务器、审计策略制定、审计记录查看等；
- 审计管理员可以查看和审计数据库会话详细信息、统计分析报表、安全操作日志、维护日志。并支持角色按模块灵活授权。

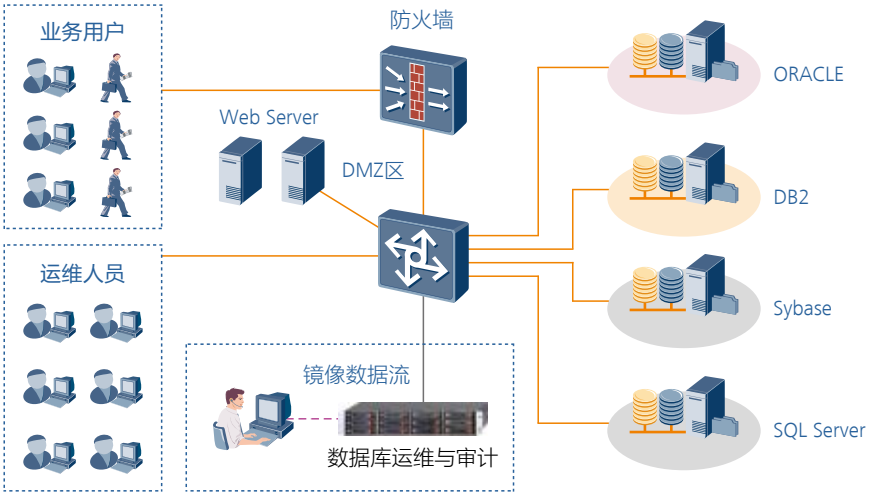
客户价值

通过部署华为数据库安全审计产品，能给用户带来的益处：

- 满足合规性要求，顺利通过IT审计：华为数据库审计系统为用户核心系统提供了独立的审计解决方案，有助于完善组织的IT内控体系，从而满足各种合规性要求，并且使组织能够顺利通过IT审计；
- 有效减少核心信息资产的破坏和泄漏：通过使用华为数据库安全审计产品，能够加强对这些关键系统的审计，从而有效地减少对核心信息资产的破坏和数据泄漏；
- 追踪溯源，便于事后追查原因与界定责任：一个单位里负责运维的部门通常拥有数据库管理系统的最高权限（掌握DBA帐号的口令），因而也承担着很高的风险（误操作或者是个别人员的恶意破坏）。审计系统能够帮助企业进行事后追查原因与界定责任；
- 实现独立审计，完善IT内控机制：华为审计系统实现独立审计，帮助监督人员获得有效的技术手段，从而完善企业IT内控机制。

组网应用

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；无需任何插件或嗅探器；不改变网络拓扑。



产品规格

产品型号	UMA-DB标准版	UMA-DB企业版
设备规格	2U	2U
SQL交易量	峰值：20000条/秒	峰值：30000条/秒
会话并发	2000Sessions	4000Sessions
硬盘	2T*4 (可扩展)	2T*4 (可扩展)
RAID	RAID10	RAID10
内存	8G	16G
CPU	2*四核	2*四核
网口	6个千兆以太网电口	8个千兆以太网电口 (可扩展)
电源风扇	1+1冗余电源、风扇	1+1冗余电源、风扇
兼容性	ORACLE、DB2、SYSBASE、INFORMIX、SQL SEVER等以及其子版本	ORACLE、DB2、SYSBASE、INFORMIX、SQL SEVER等以及其子版本
审计功能	标准审计功能	增加变量绑定、超长SQL语句、会话PCAP记录。
系统管理	对数据库审计系统本身的配置，以便对系统的访问、授权与管理等功能。其中包括：接口配置、用户管理、输出配置与授权许可。	
策略管理	对目标数据库服务器资产的添加、授权、策略制定、告警设置等配置功能。其中包括：资产、白名单、对象、策略、动作与管理。	
日志审计	日志审计是以数据库服务器资产为审计对象，从而记录运维人员对数据库服务器的操作与访问的行为；便对数据库运行情况的实时查看、故障分析以及告警级别的确定。其中包括：会话审计、策略告警、异常告警与系统事件。	
实时监控	实时监控提供数据库实时监控功能，可以对总体或数据库类型或数据库组别进行实时监控，监控其网络流量、数据包、突发链接、并发连接数、SQL语句数。并提供波形图展示，用户能够直观地了解当前数据库运行状态。	
系统监测	系统监测是用户通过数据库审计系统的审计数据信息的显示；以便用户全面的、统一的、及时的对数据库服务器的运行情况进行分析与排错。其中包括：最新策略告警、最新违规操作、最新系统事件。	
变量绑定	无	能够完整、细粒度地解析绑定变量。可以精确定位到操作客体，真正审计到数据发生了什么事情。
超长SQL解析	无	支持对超过1500字节的SQL语句进行完整重组，实现审计和解析，保证审计日志的完整性和可靠性，无遗漏。
会话PCAP记录	无	能够完整记录会话的原始PCAP数据包，并提供下载分析。

华为技术有限公司

深圳市龙岗区坂田华为基地

电话: (0755) 28780808

邮编: 518129

版本号: M3-035027-20121203-C-1.0

www.huawei.com