华为DAS1500-V数据库审计系统

产品概述

DAS1500-V是华为针对日益严峻的数据安全形势推出的一款数据库审计产品，旨在保护客户核心数据库安全，防止数据被篡改或泄露。该产品以虚拟机形式支持部署在KVM、VMware、XEN等虚拟化网络环境，可对数据库操作行为和内容进行全面的审计和管理，对数据库操作进行解析、记录、分析，帮助客户监控数据库操作，以达到违规操作可实时发现，发生事故有源可溯，提高管理者对业务系统信息资源的全局把控和调度能力。产品具有性能高、网络环境适应性强、应用简单、功能强大的特点。

产品特点

协议覆盖全

- 支持审计Oracle、MySQL、DB2、Sybase、SQL Server等主流数据库
- 随着国产数据库的盛行，支持审计达梦（DM）、南大（GBASE）、人大金仓（Kingbase）、神通（OSCAR）等
- 大数据技术逐渐发展，许多行业开始使用NoSQL数据库，支持对MongoDB、Redis数据库的审计
- 支持结合HTTP、FTP、Telnet、NFS、RADIUS、网上邻居等网络协议的审计

审计策略完备

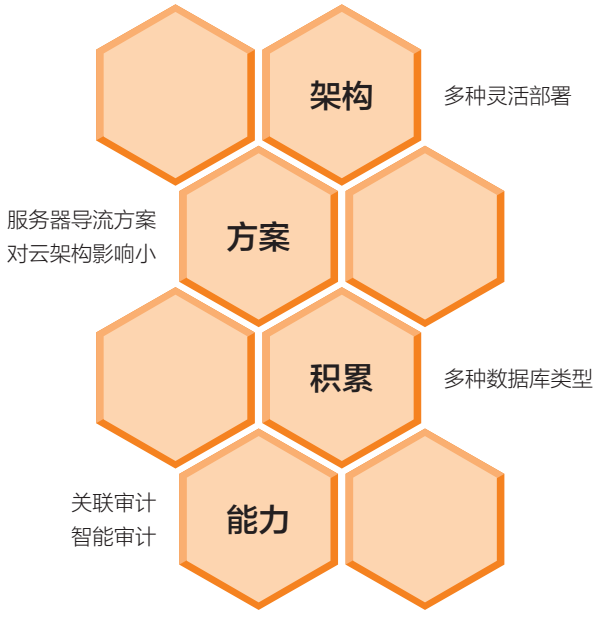
- 审计策略配置因子丰富，支持自定义及精确审计规则，可根据帐号、IP地址、端口操作类型、数据库名、数据库表名、返回行数、响应时间、数据库返回码、操作特征设定审计规则、任何违规操作均可实现告警
- 系统内置200余个缺省审计规则库，可使用自带规则库对访问流量审计，便于配置选择
- 审计策略支持导入、导出、优先级调整、分组配置，便于操作配置
- 具有多种响应方式，一旦发生可疑操作可通过邮件、Syslog、SNMP、短信等多种方式通知管理员，帮助客户实时掌握网络动态

异常智能发现

- 基于特定操作的频次分析，出现数据偏差立即上报告警，通知管理员处理
- 对审计到的历史数据自动学习，智能建模，对数据进行深度挖掘分析，发现隐蔽的异常操作，实时告警

应用简单，报表易读

- 系统提供20余种报表模板，同时支持根据自身业务特点自定义报表
- 支持报表导出为HTML、EXCEL、PDF、Word等，提供从宏观数据到微观事件的决策依据



HUAWEI

华为DAS1500-V数据库审计系统

产品规格

推荐虚拟机资源	低配	中配	高配
CPU	4核（≥2.0Ghz）	8核（≥2.0Ghz）	16核（≥2.0Ghz）
内存	8G	16G	32G
硬盘	系统盘 4G 数据盘 2T（集中式）100G（分布式）	系统盘 4G 数据盘 2T（集中式）100G（分布式）	系统盘 4G 数据盘 4T（集中式）100G（分布式）
功能特性			
部署方式	以虚拟机的形式部署在虚拟化服务器上		
策略管理	支持审计策略中IP地址、时间、协议、帐号的设置 支持自定义审计规则 支持对策略中数据库表、数据库操作命令的设置		
审计全面	支持主流数据库协议审计：Oracle、SQL Server、MySQL、DB2、Sybase等 支持国产数据库审计：人大金仓、达梦、南大通用、神通数据库等 支持NoSQL数据库的审计：MongoDB、Redis等 支持常用网络协议审计：HTTP、FTP、Telnet、NFS、RADIUS等		
日志查询	支持按时间、级别、源\目的IP、源\目的MAC、协议名、源\目的端口等条件查询日志信息		
日志统计	多维度日志统计，可从源IP、帐号、策略、时间等维度统计数据		
SQL注入检测	基于SQL注入和XSS攻击识别，远程命令执行、跨站脚本攻击的识别、对于支持的攻击或高危指令实时告警		
三层关联	可将中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到前端用户，实现三层环境下的审计追溯		
丰富的报表	支持多种报表格式：HTML、Excel、PDF、Word 提供多种缺省的报表模板库 支持自定义报表模板 可视化多维度报表，支持帐号、时间、操作内容、趋势等呈现形式		

* 以上内容适用于中国大陆地区