HeTuo 数据库审计系统

产品型号	HeTuo-DSA5620	
系统要求	1、 **产品结构：**此产品为一个完整的软硬件一体化的日志审计系统;无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁； 2、 **操作系统**：精简嵌入Linux系统，系统大小不超过150M； 3、 **日志生命周期管理：**包括数据库日志采集、审计分析、存储备份功能。 4、 **管理方式：**B/S方式； 5、 **设备部署：**提供旁路接入模式，设备部署不影响原有网络结构。 6、 支持系统维护行为审计 7、 支技分布式部署升级 8、 支持支持外部存储； 9、 支持分中心； 10、 支持RAID5，可用存储量1TB；	
网络接口	审计主机至少提供2个千兆电口，支持1路千兆监听， 可扩展4路监听口（千兆电口或光口）	*
采集	**采集日志范围**	
	★ 支持数据操作行为日志： ★ (Orale[8i、9i、10g、11g]， ★ SQL-SERVER， ★ MYSQL、 ★ Informix、 ★ SyBase； ★ DB2；	
	日志采集方式	
	★ 数据库行为日志采用旁路镜像网络流量，提取筛选日志数据；	
	数据库日志实时采集	
存储	★ 系统设备自带本地存储功能； ★ 存储系统为自主研发文件系统 ★ 日志存储量存储量5亿条；（指标以原厂公开资料为准）	*
基本功能	**实时功能**	
	★ 实时窗口支持自定义布局，多种日志类型分子窗口实时滚动显示； ★ 实时滚动显示的明细日志可自定义显示日志字段； ★ 实时窗口支持图形(饼、柱、曲线图)及明细日志等多种显示方式； ★ 实时显示多种日志属性滚动显示（原始日志、重要日志、告警日志）； ★ 实时显示审计主机系统状态（CPU、内存、磁盘空间）； ★ 实时显示当前日志流量（当前总流量、各日志源流量等多种TOP N显示方式）；	
	审计分析报告	
	★ 系统默认报告数量不少于百种； ★ 以图(柱、曲线、饼等)，统计、明细数据的方式表现； ★ 支持动态\静态（日报、周报、月报）两种系统生成方式； ★ 支持报告模版创建、修改、删除功能； ★ 支持自定义审计报告； ★ 支持多层嵌套报告； ★ 支持报告自定义归类；	

	★ 支持导出html、Excel； ★ 报告名称以树型菜单统一高效管理；	
	查询检索	
	★ 日志数据全字段检索满足500万条<5秒； ★ 支持多条件组合查询方式； ★ 支持多日志类型同时查询，以日志类型分别显示； ★ 支持逻辑运算符(或、与、非)； ★ 支持IP、字符、数字、日期、时间等日志字段； ★ 支持查询模版创建、修改、删除功能； ★ 支持历史查询任务列表的查看； ★ 支持导出html、Excel； ★ 支持日志字段自定义选择显示；	
	分析规则	
	★ 默认规则库数量至少500条； ★ 支持自定义规则； ★ 规则条件支持逻辑运算符运算； ★ 规则条件支持正则表达式方式； ★ 规则告警支持屏幕、邮件、短信方式； ★ 规则条件支持多条件组合方式； ★ 支持告警日志内容自定义等级、接收用户组、描述信息； ★ 支持对规则启动、停用；	
	备份归档	
	★ 支持日志属性(原始日志、重要日志、告警日志)、日志类型、存储周期的方式选择备份； ★ 支持日志恢复导入； ★ 支持自动与手动两种归档策略 ★ 支持本地、FTP上传、SFTP上传等归档方式； ★ 支持各种日志类型磁盘空间比例分配；	
	系统管理	
	支持审计系统帐号、组管理（添加、修改、删除）； 支持资产管理，即所有采集日志源管理维护；	
系统安全	**系统自身安全**	*
	★ 系统内置安全防火墙；支持控制访问审计主机范围； ★ 提供内部通讯检查机制，传输 128 加密； ★ 管理接口支持串口或电口的方式管理 ★ 管理界面与其他功能模块分离；	
	日志数据安全	
	★ 审计日志文件方式存储； ★ 审计日志加密导出审计系统； ★ 支持所有审计管理员操作审计系统的动作进行审计； ★ 支持记录审计系统之间的物理、逻辑状态变化；	
	日志权限	
	★ 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； ★ 支持日志类型权限设置；	

	★ 支持 IP 地址权限设置； ★ 支持页面功能模块权限设置；	
其他要求		
产品服务	1、提供原厂一年 7*24 小时的售后服务承诺， 2、提供一年原厂保修及原厂免费现场服务，产品的安装、培训由原厂工程师完成实施。	