

HeTuo 日志管理综合审计系统

产品型号	HeTuo-LDS5840 HeTuo-LDS5840D (支持双电源)
产品架构	1、 产品架构 : 主机+探针方式的日志审计系统; 无需用户另行提供服务器、操作系统、数据库系统; 2、 操作系统 : 精简Linux系统; 3、 管理方式 : 基于https 的B/S方式; 4、 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。
网络接口	1、 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 1、 支持网络行为日志(HTTP、FTP、TELNET、SMTP、POP\POP3、P2P、即时聊天等) 2、 支持数据操作行为日志(Oracle[8i、9i、10g、11g], SQL-SERVER[2000、2003、2008], MySQL、Informix、SyBase); 3、 支持主流网络设备交换机和路由器[Cisco、H3C、HUAWEI、Juniper]; 4、 支持主流安全产品防火墙[Netscreen、Checkpoint、天融信、东方龙马、东软、H3C等], IPS/IDS[启明星辰、绿盟], 5、 防毒墙[趋势、FortiGate]、UTM[Fortinait、启明星辰]; 6、 支持操作系统Windows、Linux、BSD、Unix等; 7、 WEB应用IIS、Apache等; 中间件Websphere、WebLogic等; 8、 任何文本型应用日志 。
	日志采集方式 1、 网络行为日志及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; 2、 Windows系统日志采用安装Agent方式采集日志; 3、 安全产品、网络设备、及Unix操作系统通过SYSLOG、SNMP、OPSEC LEA等协议采集; 协议日志采集需要通过专用探测器进行采集 4、 文本记录型日志[IIS、APACHE、WEBlogic等]可通过FTP、HTTP等协议进行远程采集; 文本记录型日志需要通过专用探测器进行采集
	日志采集能力: 10000条/秒以上
存储	1、 所供系统设备自带内部存储空间; 2、 为减少维护量和通用软件带来的安全漏洞, 不得使用通用数据库作为后台存储系统, 必须使用审计厂家自主研发的存储系统 3、 物理磁盘空间>=2T; 日志存储量至少10亿条; 4、 硬盘采用RAID5架构以保证数据可靠性, 支持热插拔 5、 支持外部网络存储(IP SAN、NAS、DAS、磁盘阵列等);
	实时审计功能 1、 支持实时监控界面布局自定义; 2、 日志显示可自定义显示日志字段; 3、 支持按日志类型对最新日志进行分类展示;

基本功能	<p>4、支持按日志属性（原始日志、重要日志、告警日志）对日志进行分类展示；</p> <p>5、实时按审计目标设备显示当前日志流量（当前一分钟日志量、最大一分钟日志量、当天总日志量）；</p>
	<p>审计分析报表</p>
	<p>1、系统默认报表数量不少于百种；</p> <p>2、支持通过图形（柱、曲线、饼等）及图表等方式展现统计、明细审计报表；</p> <p>3、支持手工\自动（日报、周报、月报）两种方式生成报表；</p> <p>4、支持自定义审计报表模版创建、修改、删除功能；</p> <p>5、支持报表自动发送至特定邮箱功能，发送目标支持多个邮箱；</p> <p>6、支持报表自定义归类；</p> <p>7、支持html、Excel格式的报表输出；</p>
	<p>查询检索</p>
	<p>1、日志数据全字段检索至少满足500万条<5秒；</p> <p>2、支持任意多条件组合查询；</p> <p>3、查询结果包含多种日志类型时，系统进行分类型显示；</p> <p>4、查询条件支持多种逻辑运算符（或、与、非、包含、不包含、等于、不等于、大于、小于、开始、结束等）；</p> <p>5、支持查询模版创建、修改、删除功能；</p> <p>6、支持历史查询任务列表的查看；</p> <p>7、支持将查询结果数据导出为Excel格式文件；</p>
	<p>分析规则</p>
	<p>1、默认规则库数量至少500条；</p> <p>2、支持管理员自定义创建审计规则；</p> <p>3、规则条件设定支持逻辑运算符与支持正则表达式；</p> <p>4、异常日志支持以屏幕、邮件、短信等方式进行告警；</p> <p>5、审计规则条件支持多条件组合；</p> <p>6、支持对规则启动、停用；</p>
	<p>备份归档</p>
	<p>1、支持按日志属性（原始日志、重要日志、告警日志）、日志类型、存储周期的方式有选择性进行备份；</p> <p>2、支持WEB界面备份及日志恢复导入工作；</p> <p>3、支持自动与手动两种备份归档方式；</p> <p>4、系统支持FTP上传、SFTP等方式将归档文件存储到第三方存储系统中；</p> <p>5、支持各种日志类型磁盘空间比例分配设定；</p>
	<p>系统管理</p>
<p>1、支持审计系统帐号、组管理（添加、修改、删除）；</p> <p>2、支持资产管理，即所有采集日志源管理维护；</p> <p>3、支持实时显示审计主机系统状态（CPU、内存、磁盘空间）；</p>	
	<p>系统自身安全</p>
	<p>1、探针和主机之间数据传输采用内部加密机制进行；</p> <p>2、管理接口支持串口或电口的方式管理</p>

系统安全	3、管理界面与其他功能模块分离；
	系统权限控制
	1、审计员只能查看权限范围内的日志数据； 2、支持按日志类型、IP 范围、系统功能模块设定 IP 审计员权限；
系统升级 二次开发	1、在设备维保期内，提供对系统软件的免费升级服务，保证系统软件为最新版本。 2、根据用户需求定制开发相关内容，包括报表和报表日志的查询等功能。
其他要求	
系统 许可方式	永久许可方式，不限制审计对象数量，后续增加审计对象不用增加授权许可。
产品服务	1、提供原厂一年 7*24 小时的售后服务， 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。