



优炫日志审计系统
CDPS-LAS
产品介绍

北京优炫软件股份有限公司

版权所有 侵权必究

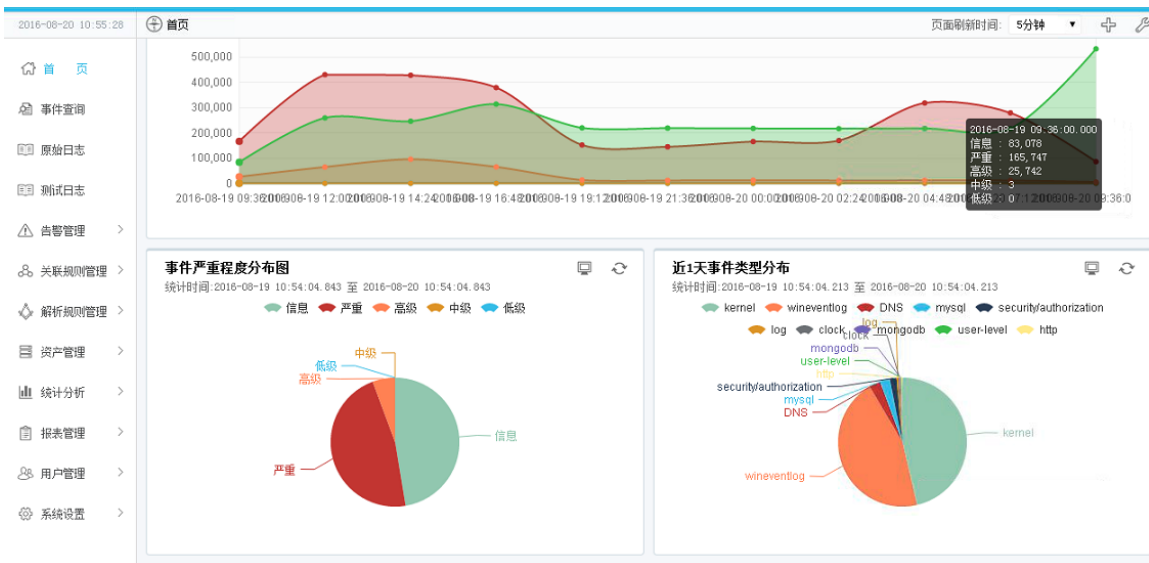
目 录

1	产品概述	1
2	产品特性	2
3	产品架构	3
4	部署方式	4
5	典型应用	5

1 产品概述

优炫日志审计系统（Core Data Protection System Log Audit System，简称 CDPS-LAS）能够实时采集企业和组织中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的日志、事件、报警等信息，并将数据信息汇集到展示平台，进行集中存储、展现、查询和审计。

各种安全产品及设备的日志数据通常杂乱无序，同时也无法体现它们之间的相互关系。CDPS-LAS 为解决这些问题建立起一个信息交换、信息存储、信息处理的平台，通过该平台，可以对各类产品的日志、事件进行统一管理、分析。它适用于对日志管理要求较高的政府机关、运营商、金融机构及一些大中型企业。



2 产品特性

（1）集中化的日志综合审计

CDPS-LAS 提供强大的日志综合审计功能，为不同层级的用户提供了多视角、多层次的审计视图。

（2）全面的智能收集功能

不断的连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控；可配置过滤和聚合功能可以消除无关数据，并且合并重复的设备日志，强大的数据压缩功能可节省昂贵的带宽。

（3）标准化日志

各种安全事件日志（攻击、入侵、异常）、各种行为事件日志（内控、违规）、各种弱点扫描日志（弱点、漏洞）、各种状态监控日志（可用性、性能、状态）、安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类。

（4）创新的日志解析能力

解析规则激活，仅当接收到对应的日志后，规则才会被激活，同时支持未识别日志水印处理，采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理，同时支持多种解析方法（如正则表达式、分隔符、MIB 信息映射配置等）；日志解析性能与接入的日志设备数量无关。

（5）先进关联算法

CDPS-LAS 平台的关联引擎采取了 In-Memory 的设计，全内存运算方式保证了事件分析极高的效率和实时性，这和一般的日志审计产品通过 SQL 查询方式提供关联分析能力有巨大差别，无论在分析速度、分析维度、灵活性、IO 抗压能力方面都完全不可和 CDPS-LAS 的关联分析引擎比拟。

（6）可维护性及可拓展性

系统具有对自身的维护配置功能，如：系统参数设置、系统日志管理等。硬件系统采用模块结构，保证系统内存、CPU 及储存容量的扩展；硬件配置的升级不会引起软件的修改和开发；每个组件都可以横向扩展，通过增加设备满足业务需求。

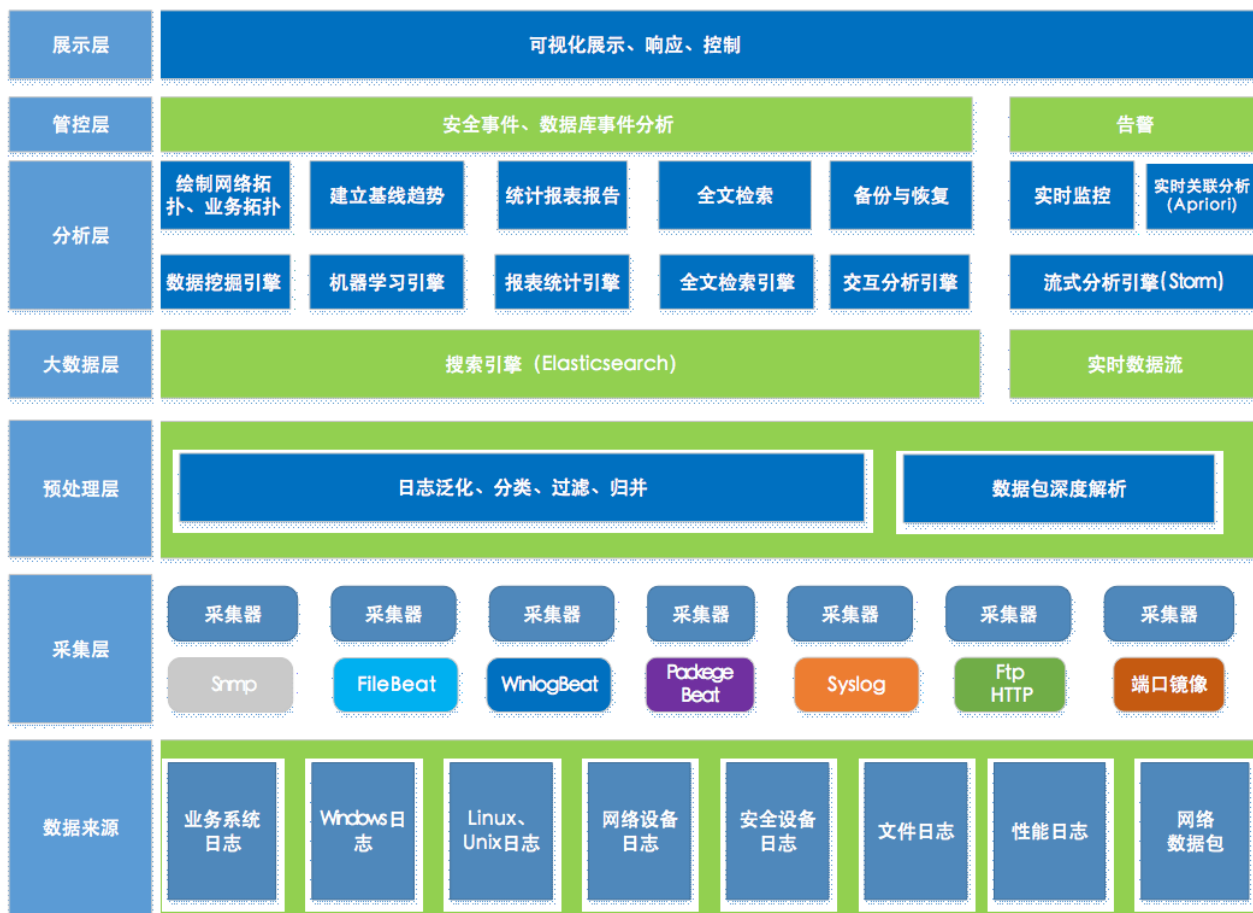
（7）采用通用的安全事件标准

CDPS-LAS 根据多年的网络安全经验，总结出了通用标准的安全事件归一化格式和分类体系结构。

（8）灵活的部署方式

CDPS-LAS 采用旁路方式部署，在不改变网络结构的情况下，实现对信息系统产生的事件进行统一的管理和存储。

3 产品架构



系统架构采用分层协同工作设计，总体上含 Web 展示（展示层）、后台处理（管控层、分析层、大数据层、预处理层）、数据采集（采集层）。

数据采集：系统内置的采集模块对多种数据来源进行收集和识别，再转交给后台处理层进行处理。

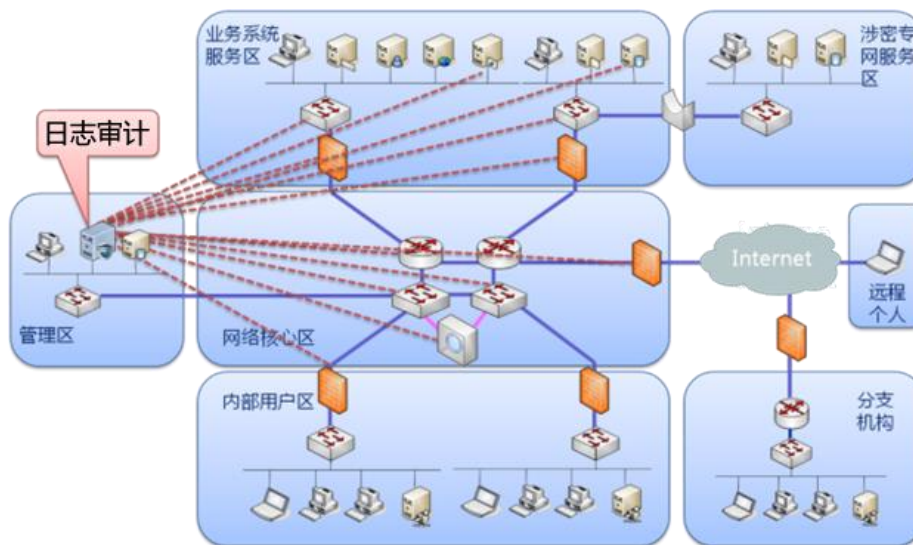
后台处理：采集后的数据先由预处理层进行分类、过滤及解析；再交由大数据层进行实时数据流统计；分析层将大数据层的数据进一步进行数据挖掘、绘制网络及业务拓扑、交互分析等处理，对事件数据进行控制及告警。

Web 展示：对采集数据和分析结果以便捷阅读的方式展示，是管理员与日志审计系统进行人机交互的通道，通过网页的形式为管理员提供数据与分析结果的可视化展示及业务与系统的管理功能。

4 部署方式

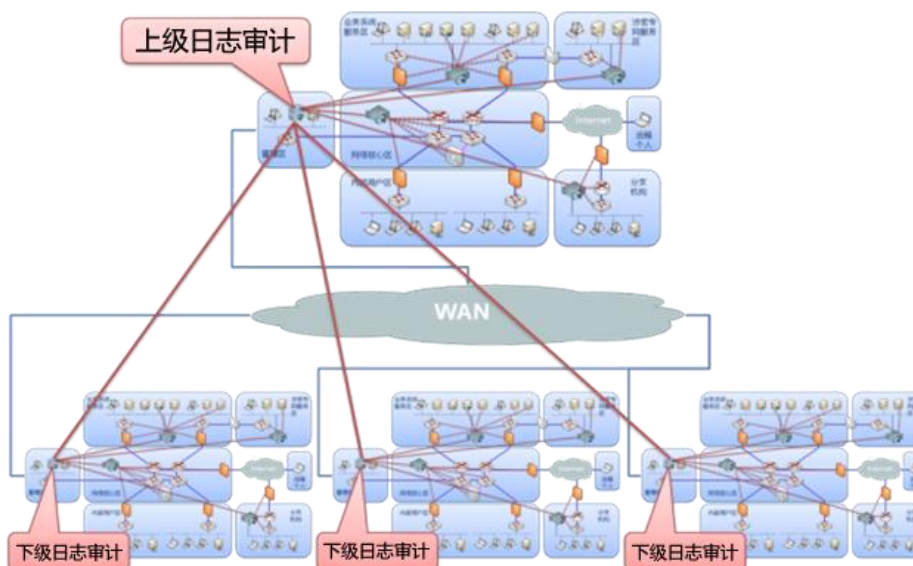
(1) 单一部署

单一的部署环境在不改变原有的网络基础之上，旁路方式接入到网络当中，并且 CDPS-LAS 只需要一个网口接口做管理及采集日志，节省网络交换的端口资源。



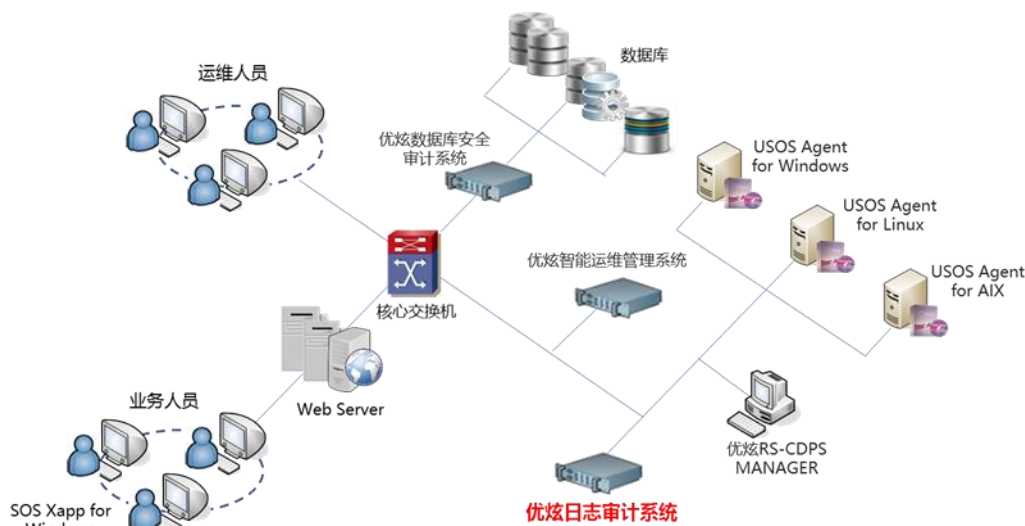
(2) 分布式部署

分布式部署做到各个分支机构的日志汇总到总部统一展示、分析，并且部署方式同样采用旁路方式，不会对网络造成安全风险。



5 典型应用

CDPS-LAS 在某市人力资源和社会保障局的应用



应用拓扑示意图

应用特点：

实现了对主机、服务器、网络设备、安全设备访问的审计和信息过滤等。系统界面友好，操作简便。安装部署可以分步骤推进，不影响用户的网络拓扑和正常业务。

管理员和资源访问人员都通过 **Web** 方式访问日志审计系统。日志审计系统能直观的展现所有资源，可直观的查看到所有目前接入的资产状况以及高危风险事件。

产品达到了对资源使用者访问控制和操作审计的目的，大大提高了市人社局应用系统访问的安全性，有效的控制和记录了可能发生的违规行为。