日志审计与分析系统
Datasheet

恩创致力于将先进的信息技术带入工业控制与工业信息领域。

安通恩创信息技术（北京）有限公司 www.avcomm.cn

电子邮箱: sales@n-tron.com.cn

电话：（010）- 82859971

地址：北京市海淀区马甸东路19号金澳国际公寓3105

日志审计与分析系统

AVCOMM 恩创 INDUSTRIAL IT

产品概述

恩创日志审计与分析系统是工业控制网络中软硬件资产日志信息的统一审计与分析平台,该产品能够实时将工业控制网络中不同厂商的网络设备、安全设备、服务器、操作员站、数据库系统的日志信息，进行统一地收集、处理和关联分析，帮助一线管理人员从海量日志中迅速、精准地识别安全事件，及时对安全事件进行追溯或干预，满足网络安全法对日志保存6个月以上的要求。

产品亮点

高效的日志采集、分析能力

产品可实现高速、海量、异构、分散的日志数据采集，可以灵活配置日志范化、增强、过滤与归并，支持可视化日志范化，具有日志动态建模能力。

基于大数据的日志存储架构

产品采用基于大数据架构实现日志存储，可实现日志结构化存储以及原始日志的非结构化存储与全文索引。

基于机器学习的日志识别

产品基于聚类分析的机器学习算法，可实现海量日志信息的自动范化和精准识别。

高效的数据搜索引擎

产品内置4种交互式安全分析模式，具备强大的即席查询能力和批量分析能力，综合范化字段与大数据全文索引技术构建的交互式数据搜索引擎，为用户提供及时查询的审计支撑。

智能化安全事件关联分析引擎

产品采用分布式关联分析架构，适用于大规模日志关联分析场景，支持实时关联和历史关联，具备逻辑关联、统计关联和情境关联（资产关联、脆弱性关联、威胁情报关联）能力，提供多种类型的安全策略包，内置1000+场景分析策略，提供可视化规则编辑器。

功能规格

采集方式

- 支持 Syslog、WMI文件\文件夹等多种方式完成日志收集功能。

日志范式化

- 实现对异构日志格式的统一化描述，范式化字段可根据审计需要灵活扩展，并可参与关联分析；
- 可自动识别收集的日志并自动选择范化策略，无须人工指定；
- 支持日志进行聚类分析，能够对原始日志模式进行自动识别；

日志传输和存储转发

- 支持日志加密传输、定时传输和断点续传；
- 支持根据转发条件，将采集后的数据转发到其他的目标地址。

日志过滤

- 支持对无用日志的自动过滤，减少垃圾数据数量；

日志交互分析

- 支持对安全事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件；
- 支持自定义事件搜索条件，建立搜索分析策略树；
- 支持时间段内的动态事件移动图。

系统管理

- 对自身运行的CPU、内存和磁盘空间等的使用率进行监测并设置告警阈值；
- 支持对采集的日志源进行监控，一旦日志源发送日志间隔超过阈值，系统将产生告警。

日志统计分析

- 支持自定义统计场景，统计的条件和时间段可自由设定；
- 支持柱状图、饼图、折线图、地图等形式的统计信息可视化展示。

日志查询

- 支持自定义查询场景。

日志关联分析

- 支持基于规则的关联分析，能够提供逻辑关联、统计关联和情境关联三种关联分析能力；
- 支持规则嵌套和引用、单事件关联和多事件关联；
- 支持单事件关联和多事件关联；
- 关联规则触发后能够通过多种方式进行告警，支持发邮件、发送syslog、执行命令和脚本、发送SNMP Trap等方式发送告警。

日志告警

- 告警规则可以自定义，告警可查询，导入导出；
- 提供告警统计策略，通过统计图表，支持柱图、饼图、曲线图等进行展示；
- 支持告警归并，有效抑制重复告警。

日志报表

- 支持按照天、月度、季度、年度等时间周期生成报表。

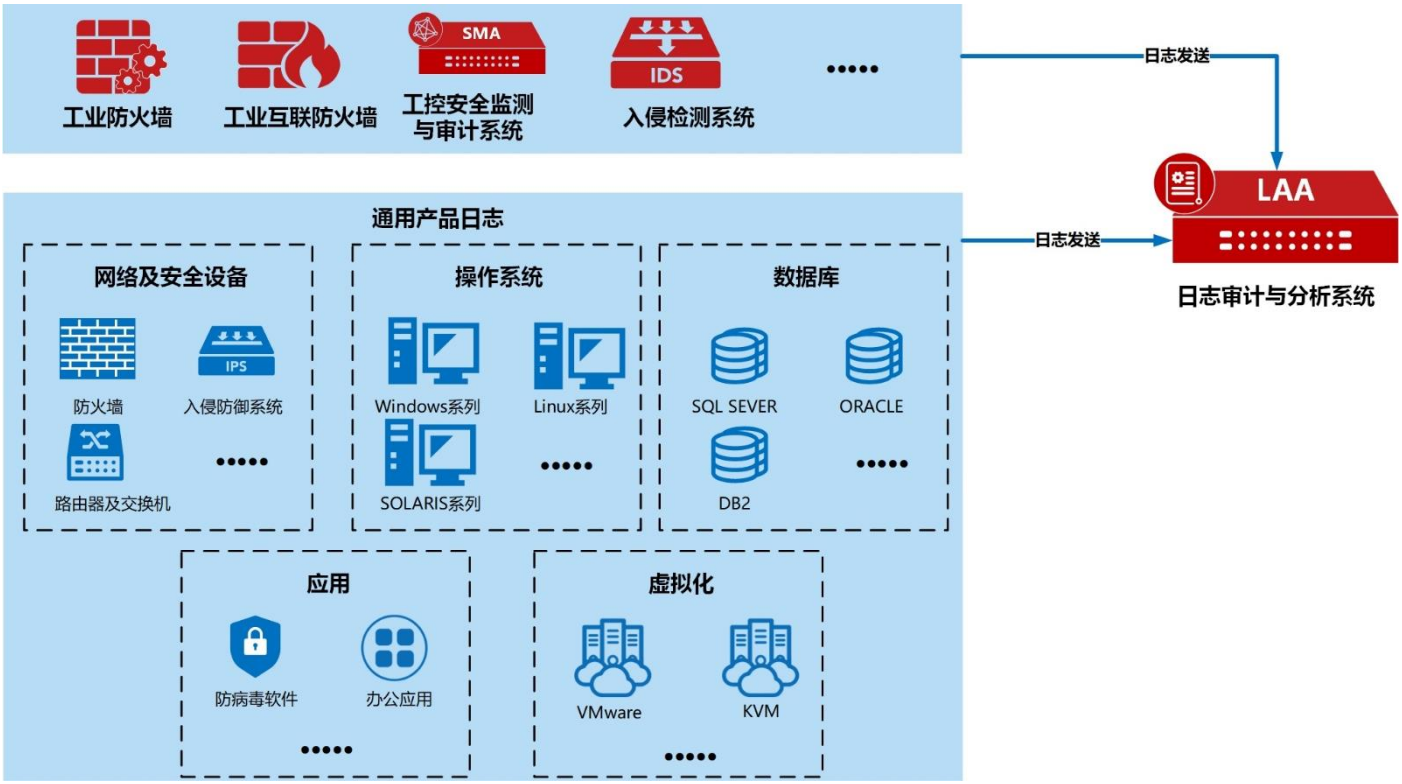
日志存储

- 支持全文索引；
- 支持日志数据的备份恢复功能；
- 支持原始日志和范式化后的日志的同时存储。

硬件指标

产品型号	LA6000	LA6100	LA6002（新）	LA6102（新）
部署类型	2U、机架式部署	2U、机架式部署	2U、机架式部署	2U、机架式部署
硬盘	2TB	3TB*2	2TB	4TB
业务端口	6*RJ45	6*RJ45+2*SFP	2*RJ45可扩展12光或12电	2*RJ45可扩展12光或12电
VGA接口	1*VGA	1*VGA	1*VGA	1*VGA
串行接口	1*Console口	1*Console口	1*Console口	1*Console口
USB接口	2*USB	2*USB	4*USB	4*USB
工作环境	温度：5℃～45℃；湿度：20%～90%（非凝结）	温度：5℃～45℃；湿度：20%～90%（非凝结）	温度：5℃～45℃；湿度：20%～90%（非凝结）	温度：5℃～45℃；湿度：20%～90%（非凝结）
存储环境	温度：-10℃～70℃；湿度：5%～95%（非凝结）	温度：-10℃～70℃；湿度：5%～95%（非凝结）	温度：-10℃～70℃；湿度：5%～95%（非凝结）	温度：-10℃～70℃；湿度：5%～95%（非凝结）
电源	250W（单电源）	300W（双电源）	250W（单电源）	500W冗余白金电源
尺寸（W*D*H）mm	440x550x88	440x550x88	440x440x88	440x440x88
安装方式	机架式安装	机架式安装	机架式安装	机架式安装
入库性能	5000EPS	8000EPS	10000EPS	15000 EPS
关联分析性能	3000EPS	4000EPS	3000-4000 EPS	4500-6000 EPS

应用场景



监管及合规建设

- 满足《网络安全法》对日志审计的要求；
- 及时掌握各类人员的访问行为，针对违规行为进行有效预警和追溯。

运维管理

- 通过对日志数据进行规范化和标准化处理，及时发现隐患、快速定位故障；
- 通过图形或者趋势图，辅助运维人员高效率把控安全态势。