祺石日志数据智能分析系统

产品介绍

2022 年 11 月 17 日

郑州祺石信息技术有限公司

目 录

一、 产品概述 1

二、 产品架构 2

三、 功能特性 3

四、 产品价值 4

4.1 满足政策监管合规要求 4

4.2 多源日志数据统一收集，解决日志数据孤岛 4

4.3 海量日志统一存储，集中检索秒级响应 4

4.4 多业务场景分析，全方位开展业务透视 4

4.5 多模式数据分析，科学提供决策依据 5

4.6 日志事件快速分析，精准定位 5

4.7 日志数据实时分析，异常消息统一推送 5

五、 部署环境 6

一、 产品概述

祺石日志智能分析系统（QS-LMA），是为运维人员量身定做，用以持续采集网络日志、安全日志、操作系统日志、Web 应用日志、中间件日志、硬件日志等的大数据智能分析系统。

系统以日志数据为基础，通过日志数据多维度数据智能分析模型，实现设备、业务运行安全分析；通过日志检索，实现海量数据快速检索与问题溯源；通过场景分析，全面了解业务运行态势；通过运行报告，定时出具设备、业务运行状况报告；通过智能告警配置，实现异常消息多渠道通知。

借助 QS-LMA 可构建统一日志存储与日志分发中心，将分散的日志集中收集并有效留存，解决日志留存孤岛问题，确保单位网络安全满足《网络安全法》与《国家信息安全等级保护制度第三级要求》，同时系统可配合日志审计设备开展安全审计分析，确保安全事件及时发现，从而达到提升运维人员工作效率，降低安全运维人员投入等目的。

二、 产品架构

表现层
PC
Mobile
Pad
监控屏
拼接屏
驾驶舱
Open API
SSO
逻辑层
工作台
应用日志
系统日志
安全日志
日志检索
应用分析
安全分析
告警配置
人员管理
全景分析
日志管理
系统配置
处理层
数据格式化
数据去重/降噪
关键信息提取
数据清洗引擎
告警推送引擎
图形化分析
数据报表分析
对比实时分析
数据分析引擎
任务调度配置
周期数据同步
异常数据监控
任务计划引擎
采集层
数据采集引擎
Windows Event Log
Linux Syslog
Apache Log
Nginx Log
IIS Log
MySQL Log
MS SQL Syslog
Network Log
FW Log
.....
syslog / agent
存储层
采集数据存储
(Elasticsearch Cluster)
业务数据存储
(PostgreSQL)
文件数据存储
(File)
缓存数据存储
(JSON)
支撑层
CentOS
OpenEuler
docker
inspur
Huanghe
HYGON
中科海光
FUSION

三、 功能特性

序号	功能名称	功能说明
1	日志采集	支持 Linux Syslog、Windows Events 等的操作系统事件
		支持 IIS、Nginx、Apache、Syslog 等日志文件
		支持对华为、华三、锐捷、山石、启明星辰、奇安信、天融信、绿盟、安恒、迪普等主流安全厂商的日志采集
		支持对锐捷、中兴、华为、华三等主流路由器、交换机厂商的设备日志采集
		支持自定义方式日志采集
2	日志检索	支持模糊日志查询与精准日志查询
3	日志展示	支持不同来源、不同索引的日志分析数据的聚合展示
		支持面积图、柱状图、饼状图、折线图、地图、数据表、仪表盘、标签云
4	应用分析	支持 HTTP Server、DNS Server 应用日志分析，提供日志趋势分析、日志来源分析、用户行为分析、安全审核分析，提供不低于 80 个数据分析模型
5	系统分析	支持 Linux Syslog、Windows Events 日志分析，提供日志趋势分析、日志来源分析、用户行为分析、安全审核分析，提供不低于 70 个数据分析模型
6	安全分析	支持包过滤、会话、应用控制、用户认证、VPN 等日志分析，提供日志趋势、日志来源、用户行为分析，提供不低于 130 个数据分析模型
7	全景分析	支持 HTTP Server、DNS Server、Windows Event、包过滤、会话、VPN、攻击防护全景分析，提供不低于 200 个全景分析模型
8	告警消息	支持告警规则配置，告警信息查看，支持邮件、短信、企业微信、钉钉等方式通知管理人员
9	运行监控	提供系统运行监控，支持集群状态，索引个数，存储空间，操作系统，JVM，Cluster，Share 运行情况监控
10	系统配置	提供用户权限、日志报告、日志采集、消息通知、主题样式、系统集成等系统配置，支持用户操作审计管理
11	扩展方式	集群化分布式部署，支持扩容节点完成存储扩容

四、 产品价值

4.1 满足政策监管合规要求

《网络安全法》规定："采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；采取数据分类、重要数据备份和加密等措施"。

《国家信息安全等级保护制度第三级要求》安全审计规定：①应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录;②审计记录应包括:事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;③应能够根据记录数据进行分析,并生成审计报表。

产品应用可确保单位网络安全满足《网络安全法》与《国家信息安全等级保护制度第三级要求》，同时系统可配合日志审计设备开展安全审计分析，确保安全事件及时发现。

4.2 多源日志数据统一收集，解决日志数据孤岛

QS-LMA 可构建统一日志存储与日志分发中心，将分散的日志集中收集并有效留存，解决日志留存孤岛问题，产品支持对网络日志、安全日志、操作系统日志、Web 应用日志、中间件日志、硬件日志等信息进行收集，支持 syslog、agent 等通用日志自定义数据采集，支持日志来源较广，可清晰的观察业务运行过程状态。

4.3 海量日志统一存储，集中检索秒级响应

产品支持 TB 级日志数据收集、清洗、处理，并以特定的格式进行日志压缩存储，实现数据分析秒级响应，达到分析结果快速展示的效果，降低页面加载时间，提升用户访问体验与运维工作效率。

4.4 多业务场景分析，全方位开展业务透视

产品支持 HTTP Server、DNS Server、Windows Event、包过滤、会话、VPN、攻击防

护等场景分析，支持面积图、柱状图、饼状图、折线图、地图、数据表格、仪表盘、标签云等多种数据展示方式，根据分析模型指定不同的分析图表，从而可将日志分析结果进行直观呈现。

4.5 多模式数据分析，科学提供决策依据

支持对日志数据进行多维度、多角度的聚合分析、统计分析、抽样分析等，从而直观表现出日志分析结果，让用户直观了解日志分析结果含义，从而为 IT 投资和运维决策提供科学而全面的数据支撑。日志事件快速精准定位

4.6 日志事件快速分析，精准定位

产品可按照时间范围、主机、IP 地址、应用名称、来源等查询日志，也可按照日志自身的解析字段（如源 IP、目的 IP、协议、应用名称）进行查询，协助开展安全事件快速精准定位，确保在单位时间段内对安全事件开展有效分析，解决因运维人员有限，安全事件存在分析滞后且无法精准定位等问题。

4.7 日志数据实时分析，异常消息统一推送

系统支持基于日志数据，利用人工智能与大数据分析技术开展实时日志分析，借助强大的告警检测引擎，将异常日志信息以电子邮件、短信、界面、声音、微信、钉钉等方式将通知管理员，同时支持异常消息与第三方消息平台对接，确保管理员可快速定位及时解决，使故障遏制于萌芽状态、防患于未然。

五、 部署环境

名称	配置	
硬件平台	处理器	≥4 核，64 位处理器
	内存	≥8GB
	硬盘	≥500GB
软件平台	操作系统	CentOS 7.9 openEuler 20.03
	数据库	PostgreSQL 14.4
	容器环境	Docker 20.10.15
	数据存储	Elasticsearch 8.4.3
	数据清洗	Logstash 8.4.3
	ODBC	Microsoft ODBC

专注互联网创新应用 / 提升信息化业务价值

电话：0371-67896990

邮箱：support@yeework.cn

手机：13215998179

地址：郑州市高新技术产业开发区总部企业基地 37 号楼 3 层