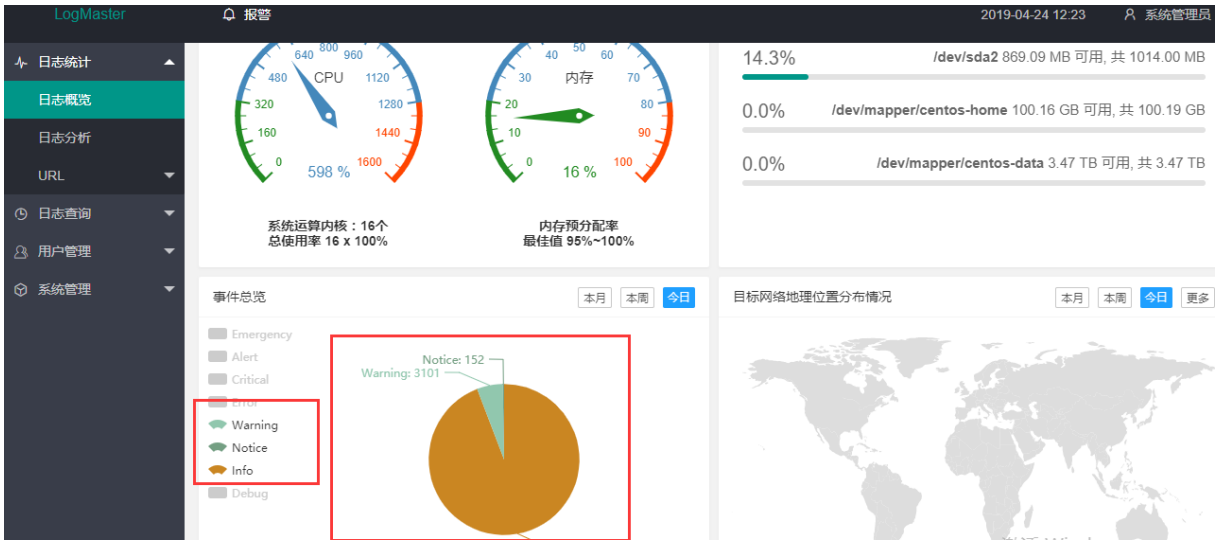
LogMaster 综合日志分析平台

LogMaster是一款基于插件技术研发的综合日志分析平台，产品技术独特、功能强大、性能卓越，可支持接收处理每秒百万级任意来源日志。LogMaster完美支持阿姆瑞特安全网关日志接收分析，并可实时显示系统资源使用情况，如：CPU利用率、内存和硬盘使用率；通过查询分析，可显示并发连接数、防病毒、入侵检测和防御（IDP）拦截等重要系统运行状态数据。

该平台还可以对其它设备生成的日志数据进行收集、存储、创建索引、联合查询、可视化、分析和生成日志分析报告，进而确定和解决通过访问日志定位到“用户”和其它信息安全问题。



功能&技术特点：

➢ 实时统计分析

可对系统资源使用情况、事件分级、目标网络地理位置分布情况、日志处理速度、日志事件（按类型、等级）等进行不同时段的实时统计。可对匹配的规则、IP、接口、应用程序和 IP 名声等进行 Top 排名进行实时统计分析。

➢ URL 分析查询

支持对 URL 访问记录进行实时 50 位排名统计分析。观察域名排名变化，通过查询域名访问记录是追踪这些事件的有效手段。

➢ IP 名声查询

支持对源 IP 名声查询。一些互联网源 IP 进行恶意网络扫描、实施僵尸网络控制等 DOS 攻击，通过 IP 名声查询，可以迅速定位攻击源 IP。

➢ IDP 日志查询

提供对入侵检测和防御（IDP）日志的查询。一些服务器被入侵或正在遭受外网的攻击，网管可能全然不知，通过查询 IDP 日志，可以清晰显示服务器是否被攻击。

➢ 反病毒日志查询

提供对反病毒日志的查询。哪些文件含有病毒，被规则拦截，通过查询可以一目了然。

➢ 综合查询

提供对不同来源日志的综合查询。通过网络出口 NAT 日志来定位到攻击来源自哪台计算机，再根据当时的时间，联合查询上网认证日志定位到人。

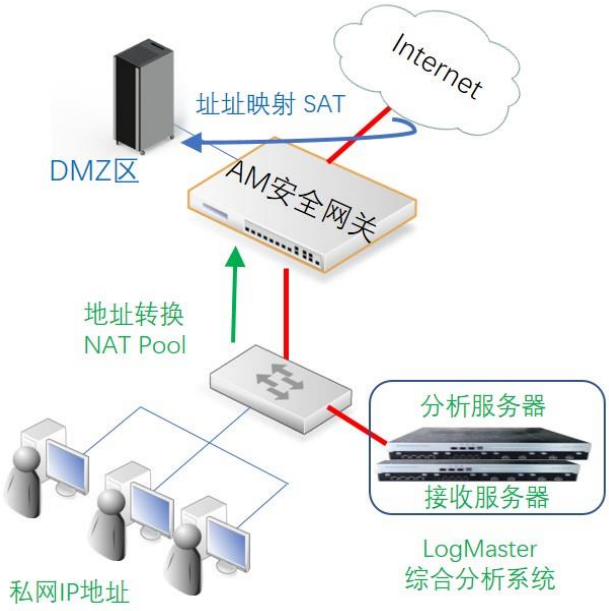
➢ 报警管理

提供按预先设定的日志规则报警功能，目前支持邮件报警和实时报警两种方式。

产品部署：

LogMaster 综合日志分析平台，理论上可以部署在内网任何位置，只要网络可达，但由于 LogMaster 综合日志分析平台是网络的基础服务，重要性极高，因此建议将 LogMaster 综合日志分析平台部署在服务器区域或直连核心交换机以保证其网络畅通性，根据网络规模和日志量可分为两种部署模式。

LogMaster 综合日志分析平台支持单台服务器部署模式和多台服务器部署模式。LogMaster 的日志接收服务器和日志分析服务器可以部署在一台主机上，也可部署在两台或多台主机上。



产品优势：

➢ 高效实时处理

高效接收，实时分析，专用加速芯片，提升日志分析处理速度。

➢ 兼容扩展性强

支持标准的 Syslog 日志格式，同时支持其它来源的日志，及自定义的日志格式。

➢ 功能齐全

通过收集、索引、监控、报告和警报机制来解决日志分析处理所需的一切，得到最终可操作的数据分析报告。

➢ 独特插件功能

当需要接收查询其它设备日志时，只要通过导入设备插件，就可立即接收所需要的日志，支持处理任意来源日志。

➢ 联合查询功能

当接收多个设备日志时，可以对相关日志进行联合查询分析，可查询分析出您想要的日志中任何有价值的信息 ,如 :查询访问某一目标的源地址对应到用户名 ,需要联合查询认证系统日志。

➢ 丰富的报表功能

在不需要第三方报告软件的情况下，可以实现即时查询历史数据并生成日志分析报告。日志分析工具支持丰富的日志数据，可灵活访问相关的数据库，并可灵活自定义报表。

产品参数

产品型号	AS-6000Ltd-LMA	AS-6000Pro-LMA	AS-6000Plus-LMA
设备许可数	5~10 台	10~20 台	20~50 台
日志容量	2T	8T	16T
配置	6核CPU*1 32G内存	6核CPU*2 32G内存	6核CPU*2 64G内存
机架型	2U（冗余电源）	2U（冗余电源）	2U（冗余电源）
电源	AC 100-240V，50-60Hz 最大10A/350W		
平均故障间隔时间	80,000小时		
运行温度	0°-45°C		
相对湿度	8%-90%，冷凝		
海拔高度	-2,000至18,000英尺		

全国分支机构

北京（总部）
地址：北京市朝阳区清河营东路中铁国际城•乐想汇2号楼720室
电话：(010)84476440

西安办事处
地址：西安市经开区迎宾大道138号豪盛花园D2501室
电话：(029)88855367

成都办事处
地址：成都市锦江区锦华路一段8号万达锦华城7单元1201号
电话：(028)84191711

上海办事处
地址：上海市青浦区华徐公路962弄69号复能大厦405室
电话：(021)62676906

南京办事处
地址 :南京市鼓楼区集庆门大街268号苏宁慧谷E2座1613室
电话：(025)85652586

重庆办事处
地址：重庆市九龙坡区万象大道华润中心28栋1708室
电话：(023) 88959717

广州办事处
地址：广州市天河区中山大道中393号天长商贸园B209
电话：(020)87584690

郑州办事处
地址：郑州市惠济区新城路睿谷创新中心3区5号楼401室
电话：(0371)55958385

昆明办事处
地址：昆明市官渡区矣六街道万科魅力之城A1-6-2909
电话：(0871)67202231

北京云安信息技术有限公司
咨询热线：400-8060-389
www.amaranten.cn
www.bjyunan.cn

官方微信　　官方网站