产品说明文档

|  |  |  |  |
| --- | --- | --- | --- |
| 个人信息PROFILE | | | |
| 姓名 | Minminmsn | 职位 | OP |
| 工具信息 INFORMATION | | | |
| 工具名称 | 访问日志分析报警系统 | 版权所有 | √原创 第三方 |
| 开发语言 | Python、JavaScript | 应用环境 | Linux |
| 前置依赖 | ElasticStack、Elasticsearch Python Api、Grafana、ElastAlert、Nginx | | |
| 下载地址 | https://github.com/minminmsn/accesslog-analysis-alarm | | |
| 开发背景BACKGROUND | | | |
| 公司网站架构是CDN回源到Nginx反向代理前端，再回源到Iis、Tomcat、Java等各种源站，其中Nginx反向代理前端就有几十个节点，每天访问量有几十亿PV，并产生海量日志。要求访问日志至少保留一周时间，一周时间内能够随时分析，且发现错误日志、异常访问、流量突增等情况能够及时给相关负责人发送报警。  针对访问日志分析需求统计了下每天Nginx反向代理前端日志量1TB左右。访问日志需要分析的指标有：客户端IP、发送字节、请求Url、Http状态码、Reffer、客户端Agent、响应时间、地区分布等。根据实际情况最终经过选型确定了ELKB架构，既是Nginx服务器安装Filebeat客户端推送日志到Kafka消息队列、然后使用Logstash消费过滤消息到Elasticsearch分布式集群，最后使用Kibana展示分析结果，制作各种指标视图，组成仪表盘，导出分析结果报表。  针对错误日志异常情况及时报警需求，对比了几种方案最终确定在现有架构的基础主要使用ElastAlert制作各种报警规则，触发规则后发送邮件与微信报警给相关责任人。另外使用Logstash-Output-Zabbix插件传送报警信息给Zabbix服务器长期保留、且能够及时通知多方监控人员处理故障。 | | | |
| 操作说明OPERATION | | | |
| 1，该工具报警架构图如下需要提前部署好Elastic Stack实时收集前端日志，架构图如下所示：    实现的过程中主要注意以下几点：  Nginx日志格式设计  Filebeat客户端部署  Kafka消息队列集群部署及优化  Logstash分Topic消费日志  Elasticsearch分布式集群部署及优化  Kibana设计视图仪表盘  使用DSL语言实时分析前端日志  2，然后制定报警规则，触发规则报警  报警流程：查询--匹配—报警--归档记录（该流程可以开debug模式记录）  报警规则：频率、百分比、波峰波谷、聚合运算  报警方式：邮件报警、微信报警、结合Zabbix报警  3，最后查看效果需要登录平台或者查收邮件  Grafana入口： 略  Kibana入口： 略 | | | |
| 效果说明EFFECT | | | |
| 1，日志分析效果    2，错误报警效果    3，报表统计效果    4，自动防护效果 | | | |