DOI: 10.7544/issn1000-1239.ps20231101
60(11): 2441−2441, 2023

基于不同场景的日志压缩与检索设计

陈　军

（北京优特捷信息技术有限公司　北京　100102）

互联网和云计算的普及，让IT系统每天产生的日志量暴增. 日志是一种带时间戳的时间序列文本数据，由IT系统生成，可能每秒钟产生数百万条，每天达到PB级，具有数据量大、产生速度快的特点，而日志里往往包含重要的系统和应用信息，存储、分析这些日志属于准实时大数据（Fast Big Data）. 如何高效存储、快速分析这些日志，成为业界的挑战.

产业界通常采用准实时搜索引擎来存储、分析日志这种时间序列文本数据，对日志建立倒排索引，方便检索. 日志是非结构化或半结构化文本数据，在对其进行统计分析时，需要抽取其中的字段进行结构化. 产业界通常有两种解决方案：一种是日志存储前抽取字段做结构化，称作写时建模（Schema On Write），抽取字段会导致存储膨胀，花费更多的存储空间，但节省了分析的时间，是以空间换时间；另一种是在日志统计分析时才做结构化，称作读时建模（Schema On Read），由于只存储原始日志及其倒排索引，也被称作Schemaless，分析时根据需求抽取相关字段，更灵活，节省了存储空间，但在分析时需要花更多时间，属于以时间换空间. 存储空间与分析时间的矛盾难以解决，只能根据具体场景做取舍. 这两种方案在存储时都会对索引文件及日志原文进行压缩，但压缩率有限，而且由于日志的产生速度可能非常快，为了不丢日志，需要在很短的时间内把日志处理完并写入永久存储介质（SSD或硬盘），所以对索引构建及压缩的速度都有要求. 这些属于在线日志的处理方式，对检索延迟要求高，需要放松对存储空间的成本要求.

另外还有数据量庞大的日志不需要经常检索分析，属于近线日志或离线日志，它们对检索延迟要求不高，但对存储空间的成本要求较高. 数年前多伦多大学发明了CLP技术，对索引构建和压缩做了优化，日志写入速度快，但压缩率和检索性能相对低.

清华大学张广艳教授团队对近线日志和离线日志做了进一步探索和研究，通过深入研究日志数据常见的两种模式：静态模式和动态模式，及其常用处理算法，提出了对应的解决方案：对离线日志基于静态模式，提出了LogReducer方法，实现了较高的压缩率；对近线日志基于静态模式和动态模式，提出了LogGrep方法，实现了较高的压缩率和较低的检索延迟. 高压缩率与低检索延迟的矛盾焦点在于数据的压缩粒度，张广艳教授团队通过挖掘日志数据模式，找到了数据压缩的最佳粒度. 他们还在某国际著名云厂商的真实生产场景对CLP、LogReducer和LogGrep做了评测.

计算机系统的高吞吐率和低延迟往往互相矛盾，日志处理系统需要同时兼顾高压缩率、高压缩速度、低检索延迟三个互相矛盾的要求，张广艳教授团队在这方面做出了有益的探索，从日志存储分析全生命周期的视角，同时实现了高压缩率和低检索延迟.

现在IT运维监控进入“可观测性”（Observability）时代，需要把日志、指标、链路追踪三个维度的数据进行准实时观测，随时了解IT系统的健康度. 指标数据与日志数据有一定的相似度，如何让系统能够同时存储日志、指标、链路追踪这三种数据，并能够准实时分析海量数据，对学术界和产业界又提出了新的挑战. 另外，基于日志的安全态势感知及用户与实体行为分析，需要从全量日志中找到安全攻击的蛛丝马迹，也要求准实时分析海量日志. 希望能有更多团队在这个领域深入研究，推陈出新.

评述专家

陈军，日志易创始人兼CEO. 主要研究方向为数据中心自动化运维和监控、云计算、搜索、大数据和日志分析等.

亮点论文

魏钧宇，张广艳，陈军超. 数据模式感知的低成本云日志存储系统 [J]. 计算机研究与发展，2023, 60(11): 2442−2452. DOI: 10.7544/issn1000-1239.202330178