

DOI:10.16644/j.cnki.cn33-1094/tp.2018.03.025

# 基于大数据机器学习技术的IT运营分析系统建设

陈 俊

(上海浦东发展银行总行信息科技部, 上海 200233)

**摘要:** 数字化时代, 数据分析是原动力, 数据中心每日产生的海量监控数据、日志, 散落于各运维管理工具、服务器中。本项目旨在借助大数据、机器学习和分布式计算等技术建立IT运营分析系统(简称ITOA), 实现PB级运维大数据的准实时处理和探索平台; 创新动态基线算法发现历史规律、预测未来趋势, 在故障诊断、告警决策和性能评估方面智能辅助运维管理, 大大提升监控预警能力、故障处置速度和运维服务质量。

**关键词:** 大数据; 机器学习; ITOA; 动态基线

**中图分类号:** TP391

**文献标志码:** A

**文章编号:** 1006-8228(2018)03-85-04

## Construction of ITOA system based on big data environment and machine learning

Chen Jun

(Shanghai Pudong Development Bank, Shanghai 200233, China)

**Abstract:** In the digital age, data analysis is the driving force. The data center generates a large amount of monitoring data and logs on a daily basis, which are scattered in the operational management tools and servers. This project is designed to establish the IT analysis system (ITOA) by means of big data, machine learning, distributed computing and other emerging technologies, to realize the real-time processing and data exploration platform of the PB level data; the innovative dynamic baseline algorithm discovers the historical law and predicts the trend of the future, and is intelligent assistance operation and management in the aspects of fault diagnosis, alarm decision and performance evaluation, which greatly improves the monitoring and warning capability, the speed of troubleshooting, and the quality of the maintenance service.

**Key words:** big data; machine learning; ITOA; dynamic baseline

## 0 引言

近年来大数据分析和机器学习的概念越来越热门, 与之相关的技术和应用也呈现蓬勃发展的态势, 各行各业都将眼光投向了这一领域, 期望利用大数据分析和机器学习的手段来提升自身的核心竞争力。

作为数据大集中地——数据中心, 运维了成千上万的设备, 每天产生着TB级乃至更大规模的数据, 本项目旨在利用开源大数据技术, 探索机器学习算法, 通过对数据中心运行的各个系统的性能容量监测数据、日志数据进行实时采集加工、分布式计算、贴合应用场景的建模和调参, 改进传统性能数据、日志分析做法, 解决传统运维过程中一直存在难点或痛点问题。

## 1 平台体系架构

IT运营关键在于对运维数据的分析, 业界还没有成熟的产品或解决方案, 本项目的架构设计, 参考了业务大数据及部分大数据日志分析平台的做法, 引入当前主流的大数据组件, 搭建起支持离线批量和实时两种处理模式平台, 一方面支持运维管理中的实时监控、另一方面支持离线批量计算实现特征提取。

系统物理架构如图1系统物理架构图所示。

服务器方面, 由38台X86服务器组成, 20台数据节点和2台管理节点组成CDH hadoop大数据集群, 8台服务器组成ES集群, 其中包括两台管理节点合并部署, 这些服务器每台上配备大容量磁盘。4台服务器用于运行内存数据库、部署应用程序和报表服务。

收稿日期: 2018-01-10

作者简介: 陈俊(1982-), 男, 上海人, 主要研究方向: 大数据, 运维自动化, 系统监控。

2台web集群用于负载均衡和前端页面展示。2台数据库集群保存少量结果数据以及CDH组件的元数据等。网络方面,大数据组件相关节点均部署于万兆网络,

以支持ES<sup>[1]</sup>和hadoop<sup>[2]</sup>的数据副本复制。其他应用服务器、数据库服务器、管理节点等,部署于千兆网络。系统逻辑架构如图2所示。

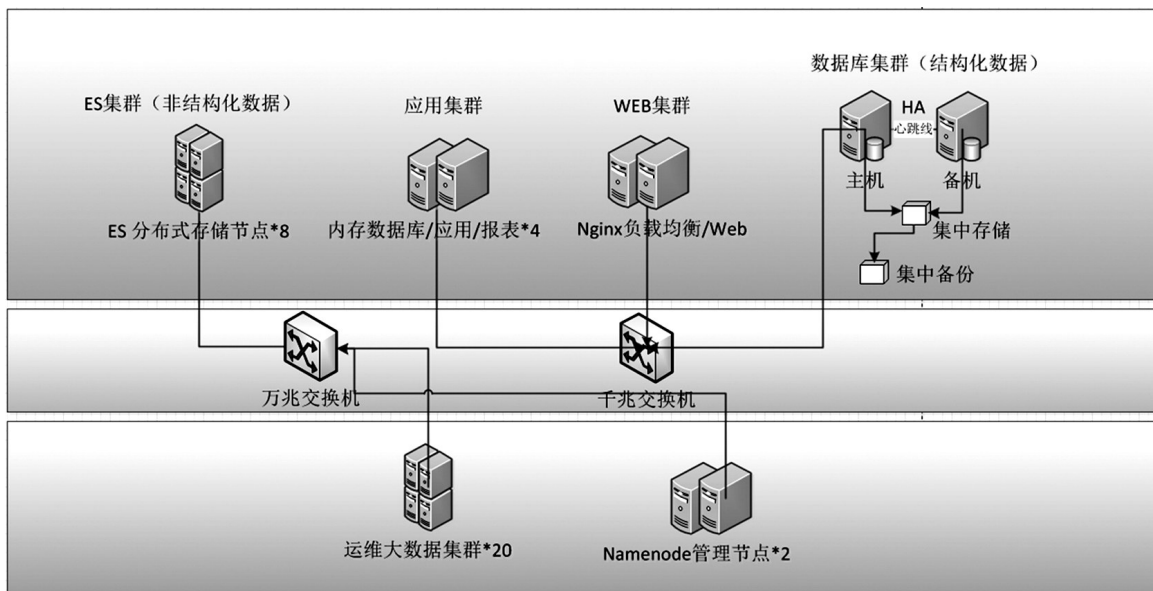


图1 系统物理架构图

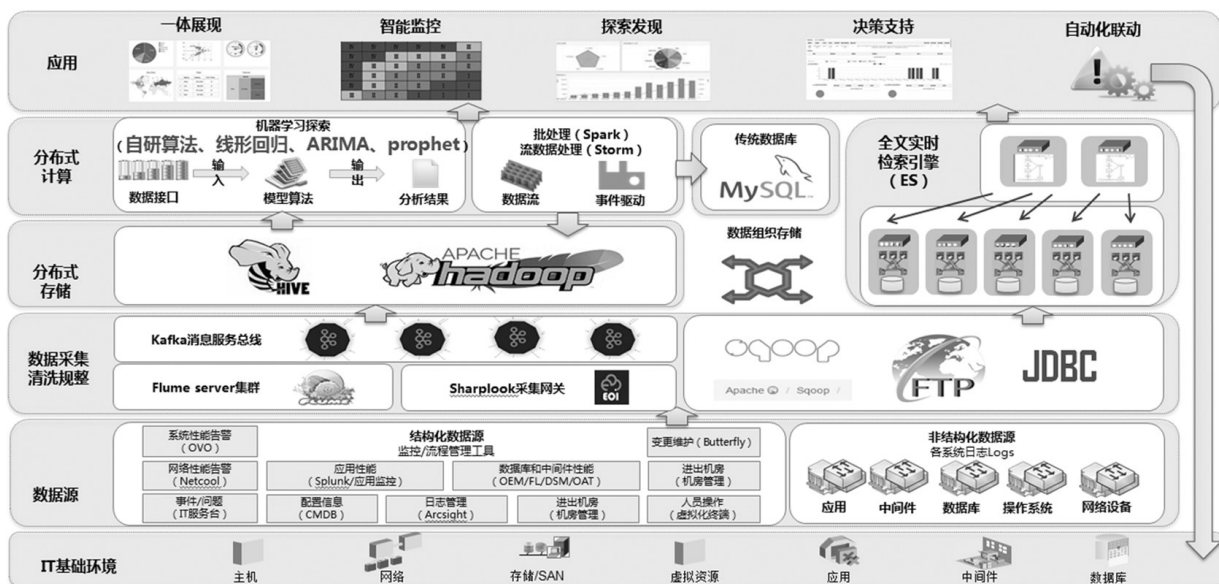


图2 系统逻辑架构图

图中共分为IT基础环境、数据源、数据采集清洗规整、分布式存储及应用共五层。

(1) IT基础环境,为本系统管理的对象,包括主机、系统、网络等各个环节;

(2) 数据源,分为从运维工具中抽取出来的结构化数据、以及这些软件、设备上的非结构化日志数据;

(3) 数据采集清洗规整层,用到了支持实时采集的flume+kafka,以及sqoop\FTP\JDBC等非实时的数据采集方式;

(4) 分布式存储,使用了CDH社区版的组件、非结构化分布式数据库ES,所有节点可通过横向扩展以提升计算处理能力和数据存储量;

(5) 应用,通过利用底层的大数据组件,通过JAVA调用接口,实现各种运维支持服务。

## 2 大数据机器学习助力IT运营分析

基于上述架构搭建而成了实时和离线计算两种数据分析平台,实现三方面功能模块支持IT运营分析。

## 2.1 PB 级运维大数据准实时处理和探索平台

运维数据分为系统运作过程中自动产生的日志,包括性能容量监测数据、系统日志,以及人在运维过程中产生的行为和记录,包括 ITIL 服务管理流程记录、服务器登录日志。

基于开源的运维大数据组件框架,搭建起海量运维数据处理和存储平台,共计从 60 余种数据源中实时抽取每日 300GB 的运维数据,单节点支持数据处理的速度峰值达每秒 10 万条、均值约 3 万条,架构上支持横向扩展,实现数据的长久保存和计算能力的扩充。数据探索功能上,支持使用类 SQL 语法进行即时数据检索,易于上手、检索方式灵活,降低数据探索门槛,数据分析结果可直接转化各种图表,图表可组成各式仪表盘,方便再次调阅和彼此共享。

## 2.2 利用机器学习算法实现异常波动监测

创新自研基于历史基线的动态监测算法,针对 CPU、Memory、SWAP、diskIO 性能类 KPI 指标异常抖动情况的监控。

首先,通过前端界面的人工标注区分异常、熔断、切换三种极大影响基线结果准确度的事件:

(1) 异常:当系统发生异常时,可能出现性能容量陡增,走势不符合日常规律的情况,基线的计算需要排除异常区间的指标值;

(2) 熔断:当系统因为异常或者计划内维护,出现服务器重启的情况,重启后可能导致系统资源释放,从而观测到指标值走势整体下降,基线的计算需要从重启后重新开始计算,历史的值无参考价值;

(3) 切换:当主备高可用模式的双机发生了切换时,原主机因资源包切换至新主机上,导致性能指标值整体下降,新主机资源整体上升,切换后的新主机基线需要以老主机的历史值计算获得,老主机基线需要以新主机的历史值计算获得;

另外,工作日和休息日的系统运行指标值因交易量不同,呈现出截然不同的特征,同样需要有所区分。

综上两种情况,计算出当前时刻对应的一组历史当前时刻指标值,对这些值进行均化获得当前时刻点基线值,如图 3 基线图所示。

基线( $\mu$ )为  $n$  个历史同一时点值的平均值,历史日期为异常、熔断、切换,公式为:

$$\mu = \frac{x_1 + x_2 + x_3 + \cdots + x_n}{n}$$

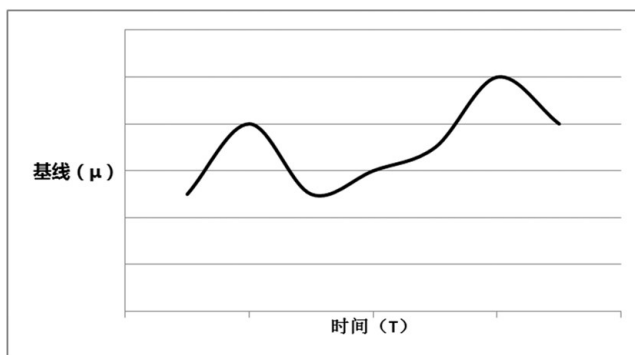


图3 基线图

其次,计算历史当前时刻指标标准差并乘以系数获得符合正态分布规律的波动区间,为了避免凌晨时间标准差非常小导致波动区间狭窄,而引起监控报警过于敏感的情况,额外增加常量系数,波动区间如图 4 所示。

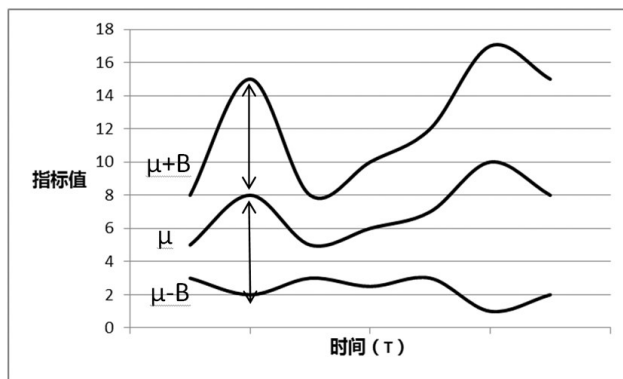


图4 波动区间图

波动区间的计算公式如下:

$$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - \mu)^2}$$

$$B = f(s, t) = 3\sigma + \text{常量} 5\%$$

经过上述计算获得波动区间后,引入大数据实时 storm 流式计算框架,将实时性能数据与波动区间上下限进行对比,当实时性能数据持续偏离波动区域连续超过预设的偏离次数阈值,则联动邮件系统发出监控告警。偏离次数阈值灵活可调,根据每台服务器的特性进行设置。

## 2.3 智能辅助运维决策

智能运维决策共分为三个模块,故障诊断、告警决策、性能评估:

(1) 故障诊断功能可实时分析正在发生或已经发生的事项,包括日志、性能、流程、人员操作等所有进入大数据平台的数据;可编辑预置特征库锁定关注的



相关信息,通过分高、中、低分级设定关键字或类SQL搜索条件,当故障发生时,一键式点击查看故障诊断报告,加快搜索定位过程。

(2) 告警决策功能可根据中英文的日志告警内容采用不同的分析策略,以此提升分词准确性和相似度准确性。利用TF/IDF算法将告警内容量化,对量化后文本矩阵相似度计算。新告警产生后,与知识库匹配判断关键等级进行红色、黄色颜色标识,点开告警后,系统分析出历史上本机和他机器此类告警的出现分布,“此类告警”检索技术是先对告警进行中英文分词,然后利用TF/IDF算法将告警量化并进行文本矩阵相似度计算,把90%相似的告警列出,进一步联动自动化,对此主机发布命令获得进一步信息,整个过程无需登录服务器。

(3) 性能评估功能可自动进行性能容量评估,将预定义的评估指标、评估方式、评估阈值转化至系统中形成评估规则库,系统自动画出性能评估报告,并每日自动产生全辖超过阈值的情况汇总清单,以一个100台主机组成的渠道类系统为例,3人天的评估过程缩短至了10秒内自动完成。

### 3 应用效果分析

经济效益方面,每年约计可节约人力1628人天。

(1) 自动性能容量评估,按350个系统,一个系统一年4次,每次1人天计算,预计共节省1400人天;

(2) 集约化系统监控和告警处理,能减少晚间和双休日值班告警转通知,加速告警处理,按照每天5个告警节省1小时计算,预计共节省228人天。


社会效益方面,大大提升数据中心运维管理质量。

- (1) 排障时间从小时缩短至分钟;
- (2) 查询效率从小时缩短至秒;
- (3) 获取报表时间从天缩短至实时;
- (4) 数据可维护规模从MB提升至TB;
- (5) 数据持久存放时间从月扩充至年;
- (6) 运维管理视角从IT拓展至业务,化被动运维为主动运营。

### 4 总结

综上所述,IT运营分析系统建设项目属于运维大数据新兴领域的深入探索和应用,项目通过搭建PB级运维大数据准实时处理和探索平台,实现运维数据的整合与关联分析,通过创新研究动态基线算法,实现对性能指标异动的提前预警,通过数据分析实践智能辅助人在故障诊断、告警决策、性能容量评估方面决策,大大提升了运维能力。

#### 参考文献(References):

- [1] elastic. Elasticsearch Reference[EB/OL].www.elastic.co/guide.
- [2] Tom, Whit. Hadoop:The Definitive Guide[M]. America: O'reilly,2010.
- [3] Jiawei Han and Micheline Kamber.Data Mining Concepts and Techniques[M].机械工业出版社,2001.
- [4] Fay Chang, Jeffrey Dean, Sanjay Ghemawat, "Bigtable: A distributed storage system for structured data"[M]. Seventh Symposium on Operating System Design and Implementation,2006.
- [5] Fay Chang et al., "Bigtable: A Distributed Storage System for Structured Data"[M], ACM TOCS,2008.26(6):1-4
- [6] L. Breiman. Random forests. Machine learning[M], 2001.45(1):5-32 

(上接第84页)

不断探索和改进的。

#### 参考文献(References):

- [1] 秦训学.自我教育——研究生德育的重要形式[J].学校党建与思想教育,2007.4:58-59
- [2] 柯翠英.德育是研究生教育中的重要内容[J].湖北师范学院学报(哲学社会科学版),2003.23(3):108-111
- [3] 宋文静.美国哈佛大学案例教学及其对我国高校德育教学的

启示[J].当代教育科学,2015.7:58-61

- [4] 王子薪.高等教育国际化背景下的研究生德育工作探析[J].教育探索,2012.8:124-125
- [5] 谢海钧.试论高校专业课教学中的德育渗透问题[J].学校党建与思想教育,2005.5:58-59
- [6] 刘胜利.浅谈在《信息安全》课程中的德育教育[J].科技信息, 2008.27:569-570 