基于 BPC 的网站全流程监控①

张 华

(中国移动(深圳)有限公司, 深圳 518000)

摘 要: 随着电信行业竞争的加剧, 服务满意度成为客户选择运营商的重要标准之一. 为提供给客户最佳服务, 运营商越来越重视门户网站与用户交互时的表现, 但怎样才能准确掌握交互期间系统各环节响应情况是一个难题. 探讨了建设网站全流程实时监控系统的必要性, 介绍了相关技术, 给出了具体的建设方案. 实践证明, 使用该方案建设的全流程监控系统, 可以从业务角度准确掌握任意时刻系统支撑用户访问时各环节的实时响应情况, 实现全方位、全流程关联监控, 及时发现异常及时告警, 提升用户感知.

关键词: BPC; 流量监测; J2EE; 门户网站; 全流程监控

Website Whole Process Monitoring Based on BPC

ZHANG Hua

(China Mobile (Shenzhen) Co.Ltd, Shenzhen 518000, China)

Abstract: With the increasing competition in the telecommunication industries, the degree of service satisfaction has become an important criterion for customers to choose operators. To provide the best service, the operators are more and more focusing on the performance of the interaction between portal websites and users, but how to monitor various aspects of the response of the system during the interaction is a new challenge. The necessity of the constructing website whole process real-time monitoring system is discussed in this paper and some related technologies are introduced and concrete construction program is presented. Practice has proved that the whole process real-time monitoring system constructed by this program can accurately grasp the real-time response at any time to support all aspects of the system when the user accesses the situation from a business perspective and achieve all-round and whole process associated monitoring to detect abnormal problems in a timely alarm and enhance the user perception.

Key words: BPC; traffic monitoring; J2EE; portal website; whole process monitoring

随着用户量趋于饱和, 电信行业开始从争取用户向维系用户转变, 通过深挖自身系统能力, 力争提供给客户最优的访问体验. 但现有的主机、数据库、网络等资源层面的监控和预警手段[1-7], 均为“竖井式”监控, 缺乏全局关联性, 难以从业务角度去反映门户网站的可用性与感知情况. 当客户抱怨系统响应慢或者不可用的情况下, 往往现有监控手段并未发现问题, 运维人员也没有办法快速定位. 怎样从业务角度出发, 全流程展现运营商提供服务的质量, 及时发现异常并快速准确定位, 是面向客户化运营的首要难题.

本文基于某公司(以下简称 X 公司)流量监测技术以及J2EE技术, 设计和实现了针对门户网站的全流程实时监控系统, 该系统使用 X 公司流量监测产品 BPC 作为业务数据采集工具, 针对门户网站后端应用的关键业务环节进行实时监控, 并把采集到的数据在监控系统中进行实时展示, 方便网站运维人员直观了解系统运营情况以及支撑用户访问情况, 及时发现问题及时解决.

1 全流程监控原理

1.1 流量监测技术介绍

在目前规划的网络架构中, 一个大型生产系统通

① 收稿时间:2014-07-23;收到修改稿时间:2014-09-11

常由防火墙、交换机、WEB 服务器等一系列组件构成. 当一个用户访问系统时, 用户请求经由防火墙进入到 WEB 服务器中, 然后系统调用应用服务器以及数据库资源完成用户请求的内容, 各组件之间数据的交互均经由交换机完成. 通过对交换机镜像端口进行旁路监听, 获得真实用户和系统交互时系统各环节处理用户请求时的流量数据, 然后解析获取系统 WEB 服务器、中间件服务器等环节在处理用户请求时的响应情况, 例如某环节处理业务笔数、成功率、耗时等. 在监测模式上, 流量监测技术所采用的监测模式为非干扰式(Non Intrusive), 只需要在网络交换机上设定网络端口流量镜像(Port Mirror), 将被监测的系统网络流量复制一份到另外一个交换机物理端口, 无须在业务应用服务器上安装任何的代理程序, 即可分析得到最终用户的操作和系统响应情况. 这种技术具备不干扰系统生产环境、不影响系统性能、不依赖系统实现、也无需人工介入的特点. 原理如图 1 所示.

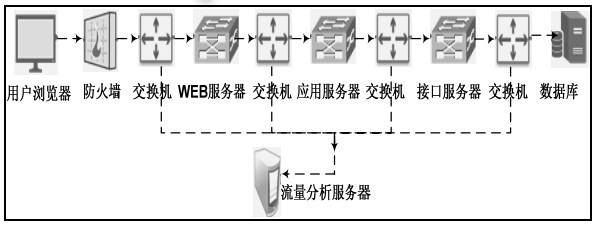

图 1　流量监测数据采集原理图

数据采集流程描述如下:

① 通过旁路方式(交换机镜像、分光器等)获取系统各环节业务原始流量数据包(WAS、XML、Tuxedo、私有协议等), 并导入流量分析服务器 .

② 使用软件解码引擎对业务数据包进行解码, 获得可以阅读和分析的业务信息.

③ 通过 IP、业务编码等方式进行非关键数据的过滤, 非需要数据直接丢弃.

④ 将关键信息存入流量分析服务器, 供后续汇总、分析使用.

1.2 BPC 简介

BPC 产品全称为 Business Performance Center(业务性能中心), 是 X 公司的产品, 实现采用了流量监测技术, 其产品主要针对中间件、接口等系统后端进行监测, 获取业务在各应用环节响应情况. 通过强大的协议解码引擎, 将网站各种协议进行解码. 在指标上, 以业务为中心, 提供交易量、成功率、响应时间三大关键指标, 并区分交易类型、子交易类型、交易渠道等多个维度. 在监视范围上, 覆盖端到端的应用服务组件, 实现了应用性能和可用性的多维度可视化, 实现业务性能监控、多维指标统计、应用交易追踪分析、实时故障定位和告警.

BPC 为一体化纯软件产品, 采用清晰的层次化设计, 架构如图 2 所示, 主要分成三层:

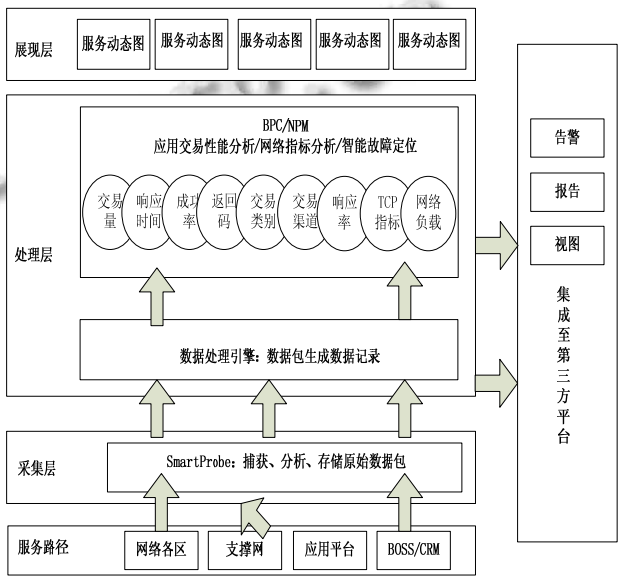

图 2　BPC 架构图

① 采集层: 负责采集网络原始报文, 通过在各个网络区域的关键位置部署分光器或交换机端口镜像来获取流量, 并对流量进行分析、传递和存储.

② 处理层: 负责分析原始数据报文并进行统计和汇总, 生成各种应用层和网络层指标, 以不同维度进行存储.

③ 呈现层: 用户通过 Web 浏览器登录软件界面, 实时查看业务应用的各项关键性能指标和业务状态, 并监控告警和提供故障定位等信息.

2　全流程监控系统说明

2.1 系统方案

全流程监控系统拓扑如图 3 所示, 监测的实施和运行方案概述如下:

(1) 整理门户网络拓扑图. 业务访问信息经由流量解析得到, 为快速过滤冗余数据, 减少解析工作量, 需要明确 WEB 服务器、应用服务器、接口服务器等

关键组件的 IP 和使用端口情况.

(2) 选择采集业务的关键路径交换机. 流量采集通过交换机镜像端口完成, 交换机选取原则为业务访问过程中各环节处理业务时请求流经关键路径上的交换机. 每个业务环节选择一台即可, 如果某环节有多台交换机进行负载均衡或主备, 所有交换机均认定为关键路径交换机.

(3) 选择 BPC 流量采集点. 本监控系统中, BPC 产品用于获取应用层各环节的处理性能情况, 例如接口成功率和处理时长等情况. 选取原则为每个应用环节选择一个.

(4) 数据分析和展示. 当用户访问时, 本监控系统通过 BPC 获取到各个环节的处理情况, 并将结果汇总到分析展示服务器, 各应用环节之间的关联以“手机号码加时间“方式进行关联, 将最终结果展示给日常运维人员使用.

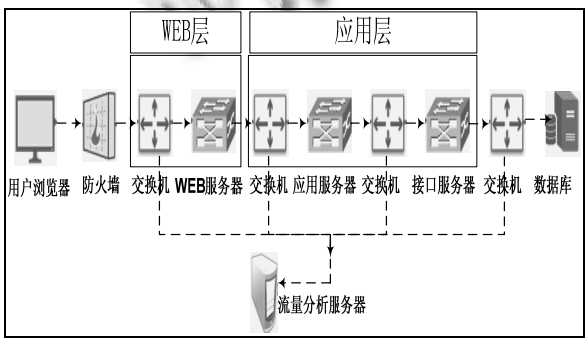

图 3 全流程监控系统拓扑示意图

2.2 监控系统架构

软件架构如图 4 所示, 参照 IT 行业内软件架构设计的成熟经验[8-10], 共分为四层, 从上到下分别是展示层、数据层、控制层以及采集层.

2.2.1 展示层

展现层主要是将告警信息以及数据汇总结果以拓扑视图、图表以及声光电等方式展现给用户, 并为用户提供各种管理功能界面. 不同的应用人员通过登录可以实现相关系统应用和资源的浏览查询操作. 依据运维人员要求可以分为多个维度展示, 例如: 实时告警展示、网站各环节性能展示等.

2.2.2 数据层

对结构化数据和非结构化数据进行调度和存储. 采集完成的数据将依据运维人员需求以及管理需求进行过滤、清洗、分析、汇总, 以方便展示层快速展现.

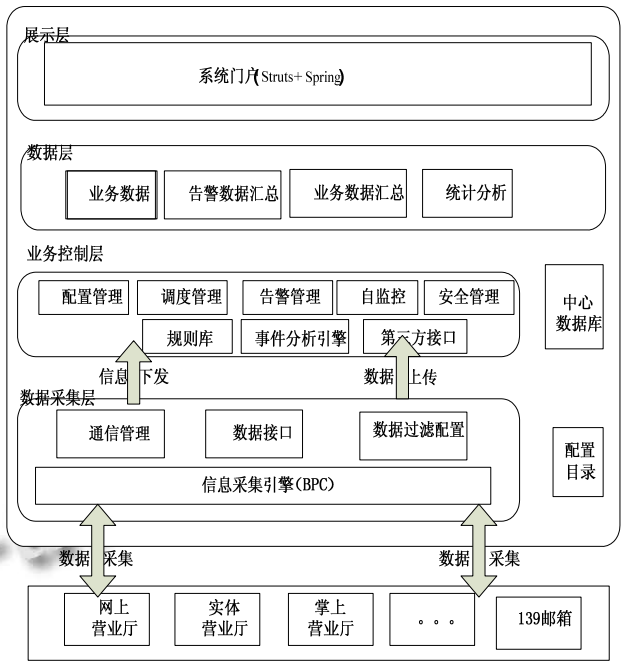

图 4 全流程监控系统架构图

2.2.3 业务控制层

用于控制整个系统的业务逻辑. 主要功能有三方面: 一是控制 BPC 软件采集的业务、频率, 以及软件过滤数据的规则; 二是管理业务配置信息, 提供增删改查功能, 并将业务规则同步到采集层使用; 三是告警规则的配置和管理, 当网站信息变更、性能下降等情况出现时, 及时告警提示.

2.2.4 数据采集层

用于从网站交换机镜像端口采集用户和网站交互的实时数据, 采集规则和业务依赖于控制层的配置. 数据采集后依据控制层的过滤规则剔除冗余数据后, 交由数据层数据汇总模块进行汇总处理.

2.3 关键监控指标设计

本监控系统的目的一是实施掌握系统运行情况; 二是快速发现用户访问的异常以及异常所在系统应用环节. 从目的出发, 我们在监控维度和监控指标方面进行了如下设计.

2.3.1 监控维度

① 用户访问角度. 一个异常的出现通常会影响到一批用户. 例如某地市网络异常会造成一个地市的用户无法访问, 某业务异常会造成所有用户访问异常. 经过评估, 我们选择了地市和业务作为用户访问异常发现指标的关键两个维度.

② 应用环节角度. 基于系统物理组网情况, 我们

将其按照交换机拆分为了负载均衡、中间件、接口三层, 并在三层中基于物理主机进行了再次拆分, 确保异常时立即发现异常所在环节以及所在主机.

2.3.2 监控指标

监控指标的选取是系统设计的重点, 指标的好坏直接影响了我们发现问题的及时程度. 从项目目的出发, 我们选择了 4 个关键指标, 分别是时长、成功率、业务量以及告警数量, 通过这四个指标对每个环节进行快速评估.

① 时长, 标示用户访问请求从当前环节经过, 到系统响应结果信息回到本环节的时间. 本指标通常和业务量指标联合使用.

② 成功率, 标示流经该环节的用户请求成功百分比. 通过本指标的变化, 可以看出当前环节是否出现异常或者是否受到了后端环节异常的影响.

③ 业务量, 标示流经该环节的用户请求的数量. 通过本指标的变化, 可以看出系统当前的繁忙程度, 结合时长指标即可评估系统运行是否有变坏的趋势.

④ 告警量, 标示当前环节的告警情况. 针对时长、成功率、业务量定义了多种类型的阀值, 例如成功率低于阀值 99%, 就会产生一条告警.

3 全流程监控系统实现

3.1 数据采集实现

本系统的数据采集由 BPC 产品实现, 虽然 BPC 提供了强大的、全面的监控功能, 但并不能完全满足运营监控的实际需要, 故本系统中使用 BPC 软件获取门户网站内部各个应用环节的业务处理信息, 主要处理应用服务器的协议以及门户网站内部的私有协议, 协议如 WAS、XML 等. 当从交换机镜像端口获取到数据流量后, 经过协议解析, 转换为标准格式的业务和流程数据.

3.2 系统功能实现

从模块化、可扩展性、快速实现、易部署、易维护等多个角度考虑, 整个系统采用了 J2EE 体系架构、B/S 模式, 采用基于 MVC 模式的 Struts 框架实现[11-13].

数据处理是整个系统的核心, 针对采集数据量大的特点, 采用专门的 ETL 工具进行数据的过滤、清洗、汇总. 该模块主要包含运营数据处理流程、告警数据处理流程以及事件数据处理流程等内容.

3.2.1 明细数据处理流程

主要实现对采集的各环节明细数据分多个维度进行处理和聚合, 得到运维人员关注的各种指标. 维度一般可分为渠道(网上营业厅、掌上营业厅等)、来访地市(用户在那个地市登陆了门户)、归属地市(用户是那个城市的, 通常由手机号码关联得到)、访问时间、业务类型、业务名称、应用环节等, 指标有成功率、时长、业务量、用户数等.

3.2.2 告警数据处理流程

主要对告警单进行生成、处理、升级、关闭等操作. 依据规则库中定义的各种告警指标, 通过分析引擎处理, 快速生成告警单. 通过监控界面和邮件、短信等方式将告警情况知会给监控系统运维人员处理. 当告警处理完成后, 可以直接关闭告警. 若告警持续达到一定时间或严重程度达到一定级别, 按预设的规则直接将告警单升级为事件单.

3.2.3 事件数据处理流程

主要对事件单进行生成、下发、升级、关闭等操作. 当事件单生成后, 按照规则库中事件规则对事件进行分类和分级处理, 并按照各种事件的关联性进行事件合并, 然后通过历史和相关性分析, 定位事件发生根源, 提高告警信息准确性, 然后下发给网站开发商处理, 告警清除后该事件可以进行关闭. 如果告警严重程度进一步升级, 也可将事件单进行升级, 催促网站开发商尽快处理解决.

4 系统应用效果举例

某电信运营商采用所述方案建立了全流程监控系统, 将整个大型支撑系统按照用户接入渠道分为了网上营业厅等多个渠道进行展示, 将支撑系统架构横向切割为接入渠道、负载均衡、中间件、以及接口多个环节进行展示, 实时分析展示各渠道、各应用环节运行情况. 业务方面, 展示维度选择了业务名称以及用户归属地市, 应用环节的指标选取了交易量、成功率、时长以及告警的笔数.

4.1 系统整体应用效果举例

如图 5 所示, 为 2013 年 12 月 05 日某一个时间点某省份支撑系统的实际运行情况. 当出现故障时, 以红色标示信息描述了整个故障的影响情况. 业务方面, 从业务维度明显可以看出网上营业厅和实体厅营业厅强制停机和强制复机两个业务受到了影响, 而从地市维度没有什么发现; 应用环节方面, 负载均衡、中间件

以及接口层均有主机进行了业务告警. 从图上信息可以直观分析出, 服务开通接口中停开机业务接口出现异常, 造成了此次故障的发生. 点击出现故障的接口机图标进行下钻, 发现“停开机”业务类型中有大量返回码为“8888”, 再下钻钻取至业务追踪界面, 查看“返回信息”字段, 发现大量失败原因为“用户在保留期内, 不允许办理此业务”. 至此, 整个故障的原因分析结束.

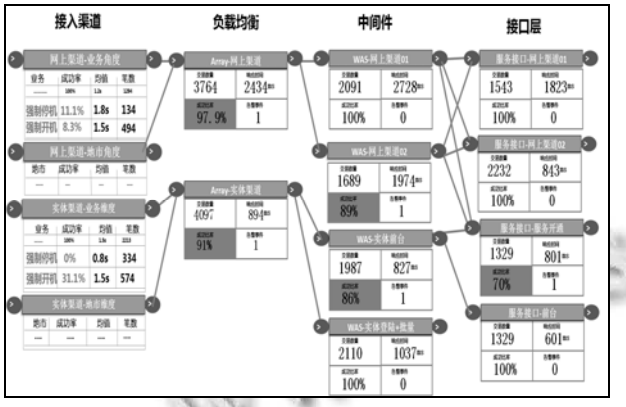

图 6 系统监控界面展示图

4.2 应用环节监控效果举例

2013 年 08 月 01 日, 当从图 06 整体监控页面上发现详单查询业务整体响应缓慢时, 通过点击详单业务下钻到应用环节耗时的监控分析页面进行快速定位. 从图 6 可以看出, 对于详单查询业务的调用, 共经历了四个应用环节, 各环节耗时分别是: 从接入渠道到负载均衡耗时 0.74 秒, 从负载均衡到中间件耗时 0.34 秒、从中间件到接口层耗时 0.28 秒, 从接口层收到请求到结果返回耗时 1.20 秒. 故此可以直观看出, 详单业务查询响应缓慢的主要原因是系统处理请求时间较长, 造成接口返回结果耗时较多. 经分析原因为月初出账期间整个系统资源消耗较多, 详单查询业务查询需要消耗大量资源, 故此该情况判定为正常, 提升方法可以为增加资源或进行功能模块分拆.

5 结语

本文给出了基于X公司BPC产品的网站全流程监控系统的设计和实现方法. 该系统从业务角度出发, 充分利用可靠的网络数据源实现敏捷的服务性能管理, 帮助企业 IT 部门了解、把握业务应用系统的运行状态, 一旦发现异常波动, 可以在预防阶段捕捉并解决, 避免因业务性能下降或中断范围扩大而导致经营损失, 实现了以”设备为中心“向以”服务为中心”的转变, 提高客户满意度. 在上线该系统前, 由于支撑系统复杂多样, 一旦出现问题, 基础架构、中间件、数据库和应用等多方人员分头定位, 但相互孤立, 难以关联分析整个过程, 导致问题定位困难. 系统上线后, 利用该系统进行全方位、全流程快速关联定位, 成功将故障定位时间从原来的 30 分钟缩减到 5 分钟以内, 为整个支撑系统的稳定运营做出巨大贡献.

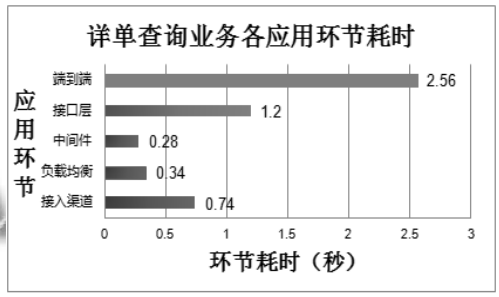

图 7 详单查询时长各环节分时图

参考文献

1 开洁.基于 IBM Tivoli 对工商行开放平台监控系统的设计与实现[学位论文].北京:北京邮电大学,2010.
2 王娜,宿红毅,白琳,王鑫,郝子昭.数据库性能监控分析系统的设计与实现.计算机工程,2005,12(31):105–107.
3 谭鑫.IT 业务系统监控及其关键技术研究[学位论文].长沙:中南大学,2012.
4 赵勇.电信运营支撑系统的现状与发展趋势.通信世界,2009,1:10–11.
5 江波.基于 B/S 模式的服务器性能监控系统.重庆师范大学学报(自然科学版),2010,5(27):1–4.
6 张黎,潘劲.一种新的服务器性能监控软件研究.计算机安全,2009,7:33–36.
7 王佳.基于 SNMP 的网络流量监控系统的设计与实现[学位论文].武汉:武汉理工大学,2012.
8 温昱.软件架构设计.北京:电子工业出版社,2007.
9 郭建华,谢燕瑜.下一代电信网络性能监控系统设计.计算机应用,2010,30(11):3080–3083.
10 金晓蓉,石冰心.基于 Web 的互联网络性能监控系统的设计与实现.电信科学,2001,10:55–57.
11 鲍胜利,钟勇.基于 Struts 框架和 Procedure 的 Web 开发模式.计算机工程,2008,9:67–69.
12 孙卫琴.精通 Struts:基于 MVC 的 Java Web 设计与开发.北京:电子工业出版社,2004.
13 顾艳红,杨志浩.COGNOS 及其在电信计费领域中的应用.计算机应用,2004,24:113–118.