分布式微服务集成应用系统监控审计技术

赵 侃
南京莱斯信息技术股份有限公司 江苏 南京 210000

【摘 要】分布式集成应用系统监控审计是解决在微服务分布式架构下，对集成应用系统的全流程的系统监控审计的技术。针对目前微服务框架下的分系统繁杂、各系统之间接口调用频繁，生产环境的异常和流程数据出错难以捕捉的问题，同时受到微服务系统的硬件、应用服务和数据库的性能限制，造成系统异常、数据错误的问题。提供一整套、全流程的系统监控审计解决方案。

【关键词】分布式；微服务；集成应用系统；监控；审计

引言：分布式微服务集成应用系统，使用容器技术将应用和服务构建在云平台上。各微服务间松耦合、每个服务之间高度自治并且使用轻量级协议进行通信。并且可进行持续集成部署。每个微服务都是拥有独立功能的程序系统，并通过轻量级设备与 HTTP 型 API 进行沟通。

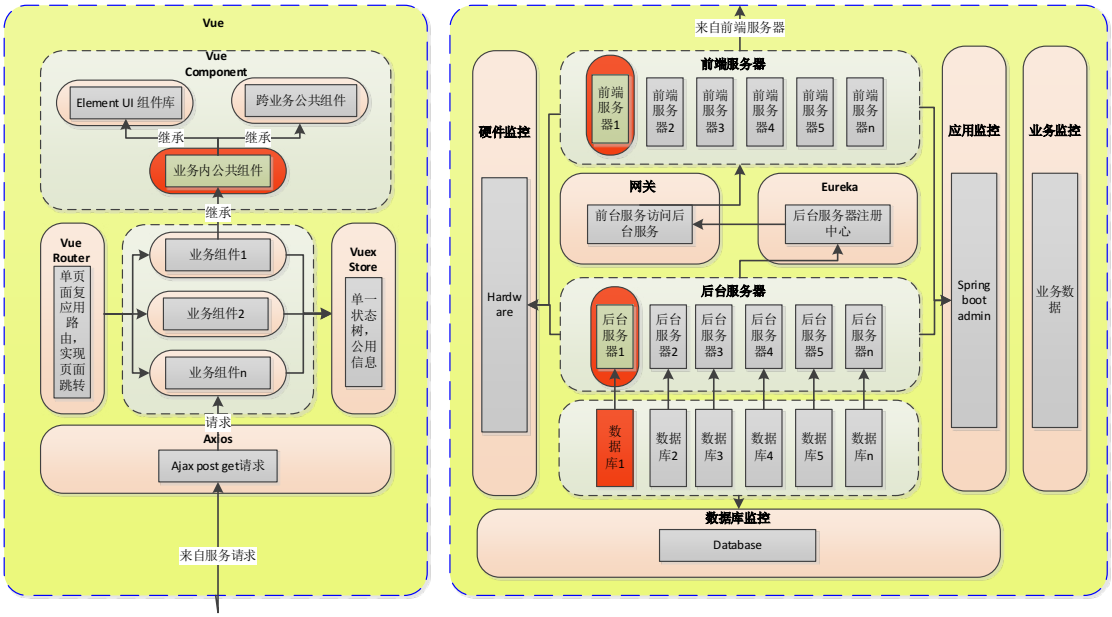

图 1 分布式微服务集成应用系统

分布式微服务集成应用系统前端使用 VUE 的组件化和自定义模块化开发方式。中间层使用 Springcloud、SpringGateway 实现分系统负载均衡和前后台分离。后台使用 SpringBoot 微服务实现分系统信息数据处理、完善、分析、统计等工作。同时应用系统环境以容器为依托分布式部署，并且以分布式的硬件环境、多源的数据库为支撑。

为了更好的保障分布式微服务集成应用系统能稳定的运行，需要一整套、全流程的系统监控审计解决方案。为生产环境中的系统保驾护航、优化更新提供支撑。

分布式微服务集成应用系统的监控审计，通过收集各业务系统、应用服务、数据库服务、硬件环境的各类日志表现，经过系统解析、整合、分析，提供给用户一套审计和监控的手段。其中这些日志表现包括文本型日志、请求型日志、数据库生成日志、系统命令行日志等。监控审计提供对应的手段将以上各类日志表现进行收集。

业务监控审计，为用户和实施人员提供业务场景中调用请求过程、业务操作过程、业务查询过程、数据传递过程、异常捕捉情况的全流程监控审计。协助用户掌握业务全局执行情况，辅助用户优化业务流程、改进业务方向。同时帮助实施人员快速排查异常业务信息，快速定位和整改系统异常。

应用监控审计，通过监控各子系统的应用服务，实时提供服务器应用的运行情况。监控应用服务系统运行状态、异常情况。

数据库监控审计，通过监控数据库连接数、用户操作、空间存储等情况，实时提供数据库运行情况，进行危险操作行为的预警，提供周期性的统计分析报告。

硬件监控审计，通过监控处理器、内存、磁盘、网络等情况指标，实时提供硬件运行情况，并提供周期性的指标统计分析报告，提供硬件调整、扩容的预警提醒。

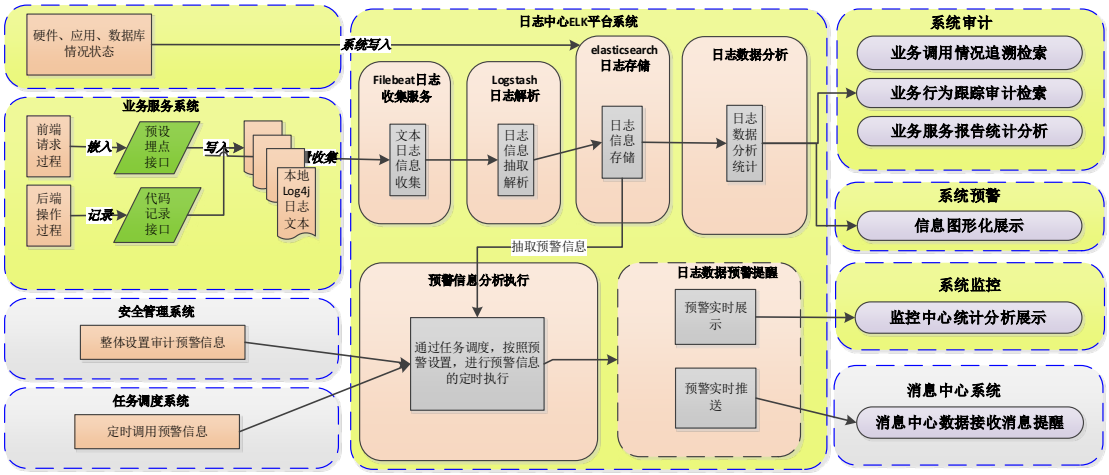

图 2 监控审计架构

1 监控审计的实现概述

1.1 业务监控审计实现方式为在各业务子系统中嵌入文件日志生成接口，产生结构化的、有逻辑关系的业务日志数据。通过日志收集、日志存储、日志整理完善，将经过分析统计信息用于系统审计，将具有时效性的信息用于系统监控。

1.2 应用监控审计实现方式为通过 Spring Boot 提供的应用监控服务方案，实时的收集各应用服务的运作状态，包括应用服务使用 CPU 情况、使用内存情况、当前服务启动状态等。然后通过系统请求，使用状态收集程序收集应用服务运行状态，实时向日志中心后台发送应用监控请求数据。

1.3 数据库监控审计实现方式为通过 ORACLE 数据库提供的 Session 日志，定时的收集各相关数据库的日志信息，包括增删改查等数据库日志。对于 Gbase 等数据库，其日志是通过命令行输出方式获取，系统后台定时收集获取命令行输出日志。

1.4 硬件监控审计实现方式为通过在各台硬件服务器上部署日志状态收集程序，实时的向系统审计后台发送硬件状态信息，这些信息包括 CPU 状态信息、内存使用信息、磁盘使用信息等。然后通过系统请求，使用状态收集程序收集硬件环境运行状态，实时向日志中心后台发送应用监控请求数据。

2 监控审计的实现详情

2.1 日志收集过程

文本日志通过 ELK 工具进行收集，系统将各微服务中的文本型日志通过 FileBeat 进行采集，FileBeat 通过增量获取的方式将日志信息逐一推送给日志分析器 Logstash，在 Logstash 系统中配置特定的正则表达式规则，过滤相应的日志信息推送给日志的存储系统 ElasticSearch。

2.2 日志存储

日志中心将收集到的业务、应用服务、数据库、硬件的各类日志分类、结构化的存储到非关系数据库 ElasticSearch 中，ElasticSearch 按照文本形式进行分类存储，并对相应的字段进行中文分词，方便后续分词查询。

2.3 日志整合完善

日志中心对收集存储的离散的，缺失的日志进行多次日志整合完善，例如原始日志中只能获得用户编号，业务功能类名，通过定时处理，完善数据的部门、角色类型、所属功能菜单等信息。同时根据业务场景，一次业务场景日志分别记录与前台请求、后台各步数据库操作，将这些日志按照顺序进行整合，完整的进行展现。

2.4 日志分析汇总

日志中心按照各种维度过滤，对特定指标进行分组统计，对一定区间内的数据进行分析汇总，方便用户全面的了解业务趋势，环境运行状态。并且日志分析统计提供定制化的报告生成功能。

2.5 监控预警配置

日志中心通过对涉及安全的、异常的日志进行收集，并提供安全预警的类型、周期、阀值的配置，当涉及的日志信息满足了阀值场景，将会产生预警事件。

2.6 监控预警提醒

日志中心通过预警项的配置，定时扫描，达到预警条件产生预警事件，进行事件的持久化，并通过消息中心推送消息给应用监控。

3 监控审计的展示

3.1 系统审计展示

日志中心通过监控审计、监控预警来展示日志信息。监控审计包括审计综合查询、用户操作日志、平台操作日志、系统专项日志。

系统审计是整个系统应用运行情况预警审计。负责对系统的运行情况进行集中预警审计，对系统运行结果进行审计，对应用运行异常进行预警。通过在安全管理中审计预警管理的配置参数项，通过任务调度系统管理定时任务并进行任务发起，最后通对系统审计系统本身收集的日志信息进行分析汇总，按照任务调度系统的调用，生成满足客户要求的报告信息。

审计综合查询包含日志综合查询和审计报告查询。向系统管理员、系统安全员、系统审计员提供全面的日志综合查询和对应的审计报告查询。三员用户通过日志类型（严重错误、错误、重要信息、一般信息等）、业务类型（新增、修改、删除、查询、审核、配置等）、

操作用户、所属系统、用户部门、返回结果（成功、失败）、用户 IP、日志日期、日志信息模糊查询等查询条件对日志进行综合查询。同时提供根据各类日志场景产生的审计报告查询。

3.2 系统预警展示

包括预警综合查询、系统预警日志、安全预警配置等功能。

预警综合查询主要包括：登录异常查询、硬件异常查询、应用异常查询、数据库异常查询等功能。

系统预警日志主要包括：登录异常预警、硬件异常预警、应用异常预警、数据库异常预警等功能。

安全预警配置主要包括：登录异常配置、硬件异常配置、应用异常配置、数据库异常配置等功能。

3.3 系统监控

系统监控是整个系统应用运行情况监控中心。负责对系统的运行情况进行集中监视，对系统运行的潜在风险进行排查与提示，对应用运行故障进行集中告警，并辅助应用问题的快速定位。通过可视化展示方式，提供系统业务运行统一监控功能，实时监控业务运行的整体动态状况，监控内容主要包括：数据采集、数据处理、主题加工、共享交换、应用服务、数据质量、数据资源、业务运行等。系统监控功能主要包括监控数据收集、监控综合展现、监控预警管理。

系统监控主要监控硬件服务、应用服务、数据库服务，实时获取关键监控指标。用户通过监控中心，全面系统的了解管控平台软硬件运行情况。方便用户及时发现服务异常，及时进行异常排除。

（1）硬件监控：硬件监控通过对管控平台涉及到的硬件服务器进行监控，从而获取详细的硬件信息；（2）数据库监控：数据库监控通过对管控平台涉及到的数据库环境进行监控，从而获取详细的数据库信息；（3）应用监控：应用监控通过对管控平台全流程的应用信息进行监控，从而获取详细的应用服务信息。

4 结论

分布式集成应用系统监控审计以日志管理为依托，为应用系统平台提供松耦合的监控审计与预警功能。为解决各微服务系统本身以及接口调用的监控问题，提供了有力的支撑。同时监控审计也提供统一的标准和工具，为第三方接入平台提供监控审计基础。为用户提供统一全面的业务系统运行情况。

【参考文献】

[1] 李宁，张轶昀．一种分布式微服务架构系统缓存解决方案 [J]．电脑知识与技术，2020,16(36):73-74.

[2] 唐爱民．企业员工心理问题及对策研究 [J]．化工管理，2020(29):13-14.

[3] 梁静． 微服务框架下敏感信息的交叉跨域安全通信技术研究 [D]．四川师范大学，2020.