

江苏电力统一日志管理平台

田 然，滕爱国

(江苏省电力公司，江苏 南京 210024)

摘 要：日志管理是信息安全管理的一个重要组成部分，同时也是信息系统审计的重要依据。江苏省电力基于云计算技术建立了统一的日志管理平台，该系统具有高性能、数据安全和可靠、即插即用、低成本、易扩展等特点。

关键词：云计算；统一；日志管理

0 引言

日志管理系统是企业信息化系统一个非常重要的组成部分。它负责记录企业中各业务系统在日常运行过程所产生的各种操作行为和运行状态。是保障信息系统安全、可控地运行的重要手段和基础，同时也是系统的跟踪、监控、优化甚至灾难恢复、以及后续审计的重要数据依据。

江苏省电力公司按照国网公司信息化建设的统一要求，构建信息基础平台，建设完善业务应用，并在深化完善“SG186”工程的基础上，按照 SG-ERP 总体建设方案要求，开展一体化企业级信息系统的建设工作，其中，基于云计算核心构件搭建了统一日志管理平台，将分布在多台服务器上主要应用系统的各类日志纳入统一管理，进行统一处理和审计。

统一日志管理平台的建成，使得用户能够通过集中化的管理模式对系统各种资源以及业务系统中各种行为、状态进行全面的实时监督和风险控制，从而降低 IT 系统运营故障维护的风险和成本。

1 江苏电力日志管理历史情况

十一五期间，江苏省电力公司积极贯彻国网信息化建设方针，信息基础设施及信息系统建设取得了长足的发展，所有主要业务系统均已集中到省公司集中运行维护，为日常管理和业务操作发挥了积极作用。从以往的运维经验来看，作为重要安全和审计依据的日志分散在各个业务系统上，日志管理呈现以下特点：

1) 业务系统多，审计和日志子系统多，日志数据输出量大；涉及的日志包括设备日志、操作系统日志、DBMS 日志、应用中间件日志、业务操作日志等等，数量和种类众多。

2) 各个系统相对独立，输出的日志类型、格式、重要程度各不相同；由于采用不同厂家的不同产品，而日志本身缺乏统一的标准，而协同、有效的利用日志进行分析的前提是日志格式的统一。

3) 系统分布较为分散，日志的存储和处理相对孤立；除数据库管理系统的日志有单独存储外，其他日志基本上在本地存储，日志的收集和集中存储是个难题。

4) 当前系统长期运行，需要尽可能保持稳定；一方面我们需要对日志进行统一管理，而另一方面，我们又不希望实施方案对原来应用系统的运行影响太大。

5) 越来越多的系统业务量，导致对日志文件的日常访问、修改和管理等操作急剧增长，现有日志文件管理的规模不断扩大，最终形成一个拥有越来越多日志文件的庞大的日志文件服务环境。

因此，建立统一日志的存储和管理平台，进行统一的日志处理和审计，可以更好地进行故障的提前预测、事后分析、辅助决策支持应用系统运行的结构优化和系统运行效率的分析。同时，整个系统的设计能够针对未来业务审计的具体需求和其他可能的变化进行灵活定制和扩展。

2 基于云计算技术的统一日志管理平台

综上所述，建立更好得统一日志的存储和管理，可以更好地进行管理、审计和决策支持。然而，如何有效地对这些海量的异构日志进行集中式存储、管理及监控是一个难题，也是几年来在国内推广信息系统审计工作的一个重点和难点。有效地组织管理渐已成熟的企业 IT 系统各个环节产生的海量日志，从中找到有效信息，及时监控系统运行中的重要事件，并对这些日志进行数据挖掘、支持领导决

策,早已成为公司IT系统建设的迫切需要。

为了满足上述需要,江苏电力采用基于云计算技术构建统一日志平台。

2.1 云计算技术概述

云计算技术不仅用于公共云和内部云的建构,还可以广泛应用于各种IT系统,解决现有系统中关于后台数据进行处理、系统监控、系统备份、数据管理等方面的问题。由于云计算技术在大规模数据处理和分布式系统的管理方面具有先天的优势,充分利用它就可以更快速更高效地开发适合客户新业务需要的IT系统,同时降低系统使用维护成本。另外,现有系统也可以通过云计算的相关技术进行改造和优化,以最小代价改善现有系统的性能或提供便利的管理工具。

2.2 建设方案

江苏电力采用数流平台(Bitsflow)、分布式数据库(DataCell DB)和分布式资源管理调度系统(NetVM),构建了一套分布式的统一日志管理系统,对主要业务系统和底层的第三方中间件基础设施的日志进行统一管理和数据分析。在此基础上,可以根据实际业务需求,灵活、快速地开发和部署各种审计系统,对日志进行实时、高效、便捷的处理以及对历史日志进行数据挖掘和统计分析。主要功能模块包括:

(1) 数流平台

数流平台是高性能消息总线平台,是用C语言实现的跨平台的守护进程,安装在每台需要信息交换的服务器上,主要用于实现整个系统中各个组件及节点的信息交换,并保证信息的可靠性、实时性和一致性。数流平台支持队列、发布/订阅、群组通讯等模式,允许开发人员搭建高效、可靠、松耦合的分布式系统。它支撑了各服务器、存储器节点以及服务器端和客户端之间高容错、高性能的数据传输,是整个系统进行数据交换的基础架构。数流平台的性能对整个分布式日志系统的性能有重要影响。

(2) 数据接口层

基于原有日志子系统构建的统一数据接口,可以将所有的日志信息通过数流平台异步发送给日志存储子系统。应用接口层提供支持业界标准的log4j、commons-logging、J2SE logging等框架的插件,从而无须更改原有程序。

1) 日志获取

通过对原有业务系统采用的日志系统进行分析和改造,构建统一的数据接口,可以将所有业务系统和底层第三方中间件基础设施产生的日志全部通过数据总线输出到日志存储子系统中。

日志的处理和传输全部采用异步形式,高效、可靠的数流平台,可以最大程度得减少日志系统对整个系统的性能损耗,同时保障数据的可靠性和一致性。

2) 预处理接口

将所有的日志数据统一发布到数据总线中,可以支持对数据的格式化和统一处理。

对于多个系统发出的日志,需要在存入存储子系统之前对日志数据进行预处理,其中包括过滤、格式化、优化、事件触发等操作。

数据接口层内置工作流引擎,在开发审计系统时,通过该引擎可以灵活提交各种预处理逻辑,当有日志发出时,工作流引擎会自动调用相应的逻辑对日志数据进行处理。

(3) 日志存储子系统

1) 日志存储

日志存储子系统采用分布式数据库来搭建。分布式数据库是非关系型数据库,这种数据库的特点是高性能、高存储、高可靠,而且可以根据需要动态扩展。另外分布式数据库具有灵活的数据结构,可以支持自定义的各种日志数据格式。

分布式数据库包含多个子节点,各个节点的存储资源(内存和磁盘)统一组织成分布式数据库系统。其中内存部分组成高速缓存系统,磁盘组成持久化数据库系统。系统中保存的数据是应用系统接口通过数据总线,根据预先设定的规则发送过来的。其中高速缓存系统存储最近的日志信息,持久化数据库系统保存历史日志信息,可以对日志数据进行分析、统计和高效地查询。日志存储子系统可以通过管理界面实现方便的配制,具有高度的可扩展性。

分布式数据库系统是一个去中心化的系统,所有的数据都有多份拷贝,确保没有单点失效和服务器故障导致的数据损失,具有高可用、高可靠的特点。另外,相比以文件形式存储的日志,分布式数据库存储的数据不易窃取和篡改,更加安全可靠。

另外,分布式数据库系统支持snapshot、异步备份等功能,可以方便得进行备份和恢复。用户可以根据业务需求,定制分布式数据库的运行策略,进一步满足性能和灵活性的要求。

2) 日志查询

对庞大的历史日志进行查询,需要高效、强大、灵活的日志查询功能。日志查询不但需要根据管理人员的请求,高效地定位和获取相应的数据,更重要的是它对数据挖掘和统计分析报表等功能模块提供功能支持。分布式数据库系统提供灵活的数据查询接口,支持多进程、多线程、分布式的数据访问,为实现数据挖掘功能提供高效、灵活的支持。

(4) 日志管理子系统

1) 日志预处理

由于日志数据来自于多个不同的、分布的业务系统和其他系统,日志的格式也各有不同,这些日志在进入统一存储和处理阶段之前,需要进行格式化,以方便得进行统一规则匹配、查询等操作。

系统在出现故障等某些特定情况下,可能会有多个系统大量重复的日志同时发出,造成所谓的“日志风暴”,这些日志在预处理阶段就可以进行合并和优化,避免不必要的网络负载和存储压力。

根据管理人员定制的策略,不同应用程序、不同类型、不同重要级别的日志可以在这个阶段进行归类,以方便系统其他部分进行处理。

另外,在预处理阶段还可以进行数据实时统计、实时监控、实时告警等操作。

2) 事件和响应

除了事后审计,实时审计对于审计系统也有着重要意义。要做到实时审计,系统分析的速度和效率至关重要,日志经过预处理阶段之后,对于需要实时告警的日志,将进行标记后传入数流平台。开发人员可以利用数流平台的发布/订阅机制,在系统中部署告警处理模块,实时捕获需要监控的日志,及时通知相关管理人员。

3) 数据挖掘

对于庞大的历史日志数据,通过数据挖掘进行统计和审计需要很大的计算和数据访问。日志管理系统利用分布式计算平台,可以对数据进行分布式并行计算,极大的缩短数据分析需要的时间。

(5) 分布式计算平台

分布式计算平台依托数流平台高效、高可靠的信息交换技术,实现了利用计算机集群进行大规模并行计算的运行管理机制。用户只需通过简单而强大的编程框架提交需要完成的计算任务以及相关的数据,就可以自动安排和处理支撑分布式计算所需的复杂工作。如输入数据的分割、中间数据的

传输分布和输出数据的聚合;多机环境下的程序执行和调度;各种软硬件故障的自动处理;计算机集群的负载均衡;以及众多功能模块间的通讯管理等。

分布式计算平台直接部署在日志存储节点上,可以充分利用各个节点的计算资源,实现分布式计算,另外,高效的调度算法可以支持各个节点充分利用本地数据进行计算,提高效率并减少数据迁移带来的资源占用。

分布式计算平台主要有两种工作机制:一是支持利用其 API 开发并行处理程序,在程序内部对需要并行处理的部分,通过调用 API 来实现;二是支持 Java 或其他二进制可执行文件的自动分发和并行执行,由平台本身来完成任务的封装和调度工作。

开发人员可以利用分布式计算平台两种工作机制,开发审计相关的业务逻辑,通过前端用户界面调用相应计算任务,再将审计结果返回给前端。

分布式计算平台充分得利用了分布式计算的优势,极大提高了并行度,从而提高吞吐量,降低计算时间,以满足对海量数据的处理需求和审计系统的实时性要求。

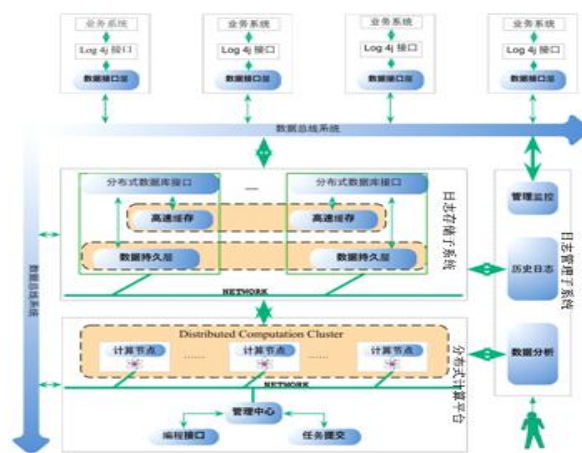


图1 统一日志管理平台逻辑架构图

统一日志管理平台逻辑架构见图1。统一日志管理平台在保证原有业务系统的完整性和稳定性的前提下,通过定制化开发的方式整合企业特有业务系统日志处理过程。同时,构建一个应用接口层,通过改造原有日志模块的底层接口实现来实现日志的集中收集、监控,并保留原有系统的应用层日志访问接口代码不变,从而实现与原有各应用系统的“无缝”接合。

3 系统特点

统一日志管理平台采用云计算技术这种全新的

机制来支持对于海量日志的存储和处理,解决海量数据的处理带来的性能瓶颈,满足高吞吐量的要求,实现相关的实时性功能。基于云计算的统一日志管理平台还可以做到实时的数据备份和系统的热灾备,彻底解决系统的单点失效问题,从而保证整个系统的高可用性和数据的高可靠性。同时现有系统利用标准日志系统接口,无缝对接,无需修改现有业务系统。即能够保证系统的高度可扩展性,又可以实现按需扩容。前期投入少,后期可以不断扩展审计模型。存储和计算能力可按需动态平滑扩展,保证系统正常运行。

(1) 即插即用

1) 不修改现有业务系统:现有系统利用标准日志系统接口,无缝对接,完全不需要修改现有业务系统;

2) 易扩展:高度可定制化,满足业务的功能需求;

3) 跨平台:适合多种操作系统和业务系统平台。

(2) 高性能

1) 满足超大规模数据分析的要求:多个繁忙的业务系统其日志数据会出现 TB 为单位的数据量,面对海量数据处理必须能支持快速的处理能力;

2) 高效数据总线系统,系统日志异步传输和处理,最大程度降低对现有系统的影响;

3) 分布式数据存储:支持无限数据存储,可动态扩容;

4) 分布式计算平台:分布式并发访问,提高高吞吐量,利用集群进行数据处理,成倍提高数据处理速度。

(3) 数据安全和可靠性

1) 数据分布式存储,日志和业务系统的访问各自独立,分离的访问权限控制,防止盗窃和篡改,数据更加安全;

2) 去中心化设计,没有单点失效,确保高可用;

3) 可控的数据多拷贝和异地灾备机制,单机故障不会导致数据损失,数据更加可靠;

4) 高容错连续服务能力:服务器硬件出现故障结点数不超过总节点数的 30% 时,系统功能不受影响;及时更换硬件无需数据恢复及可恢复服务性能。

(4) 低成本

1) 按需扩容:根据使用情况可以灵活扩充;

2) 维护成本低:高容错机制降低维护成本,只需要对硬件进行日常维护,无需特殊人工干预;

3) 升级成本低:存储和计算能力可按需动态平滑扩展,保证系统不中断正常运行;

4) 可以充分利用现有设备和闲置设备,降低系统硬件资源的投入。

(5) 扩展性

多任务并行处理:多个审计任务可以并行执行;审计任务可扩展:根据任务要求,可以在后期不断扩展审计模型;采用统一开发接口,易于扩展。存储和计算能力可按需动态平滑扩展,保证系统正常运行。

(6) 助力管理

通过统一平台的建设,大大地减轻了管理人员的工作量,使日志文件管理科学化、规范化,提高了日志文件管理的高效性和安全性,对日志文件进行分类存储和管理,积累故障经验,避免日志流失,促进故障处理的学习、共享、培训、再利用和创新。

4 结论

统一日志管理平台使得 IT 运维和 IT 审计人员能以一个整体、全面的视角审视 IT 系统运行情况,有助于 IT 运维人员建立事前规划预防、事中实时监控、事后合规报告、事故追踪回放的先进运维管理模式。并且能够更好的遵循 ISO27001、SOX、COBIT、计算机信息系统安全保护等级条例等法律法规合规性要求。

江苏省电力公司在平台建设中创新性的应用了云计算技术,在确保了原有系统地稳定运行的基础上,实现统一日志管理系统的高可靠性和高性能,充分利用原有资源,实现了系统按需弹性扩展,集中化的统一运维,大大减少了日志监控和问题分散处理的人工成本;使日志文件管理科学化、规范化,提高了日志文件管理的高效性和安全性;强化了信息运行管控能力,提升了业务支撑水平,满足了国网公司对各类信息资源的统一调度、信息安全一体化联合防御和集团化应急处置的要求;同时积极响应了国网公司整体战略发展的需要,全面支撑公司统一坚强智能电网的建设,不断推进信息化工作在人财物集约化管理上向纵深发展。

参考文献:

- [1] 李晶,李星.基于 Oracle 存储过程与触发器的三维空间数据日志管理方法[J].计算机与现代化,2010(7).
- [2] 顾飞飞,唐陇军,孙勇,等.面向事件的智能化电网调度运

行日志管理系统[J]. 电力系统自动化, 2010(4).

力信息化工作;

滕爱国 (1974—), 男, 江苏淮安人, 高级工程师, 从事电力信息化工作。

作者简介:

田 然 (1985—), 男, 江苏南京人, 助理工程师, 从事电