doi:10.3969/j.issn.1000-436x.2014.z1.025

CoolView 中的日志管理子系统的设计和实现

徐凯硕，袁华
（华南理工大学 计算机科学与工程学院，广东 广州 510006）

摘 要：为了实现在视频会议系统中对审计、追踪、报警等任务的规范化管理，采用 AOP 思想搭建日志子系统结构，结合 Syslog 和 Log4j 等技术设计日志模块，利用 SSH 框架实现了系统。上述子系统已经在 CoolView 视频会议系统中实现，为视频会议系统的运维奠定了基础。
关键词：视频会议系统；日志管理；松耦合；SSH 框架
中图分类号：TP311.52　　**文献标识码：**A　　**文章编号：**1000-436X(2014)Z1-0129-05

Development of log management system in CoolView

XU Kai-shuo, YUAN Hua
（School of Computer Science & Engineering, South China University of Technology, Guangzhou 510006, China）

Abstract: In order to realize the normalized management of the tasks such as auditing, tracking and warning in video conference system. A log management subsystem structure was built using AOP. Its log module adopting Syslog and Log4j technology was designed, and using SSH framework was implemented. The above subsystem also has been enbeded in CoolView video conference system, and it provides foundation data for daily operation and maintenance of CoolView.
Key words: video conferencing system; log management; loose coupling; struts spring hibernate frame

1 引言

日志管理已经成为加快系统开发和简化系统维护的关键。但是，很多系统却漠视日志管理，不提供日志管理或者只提供很少的功能。

2012 年的 SANS（全名：SysAdmin，Audit，Network，Security）的日志管理调查报告显示[1]，82%的人认为收集日志的关键原因是“检测/追踪来自内部/外部的可疑行为”，有 58%的人采用 LM 的方式采集日志，只有 46%的每周花费超过一天的时间用于日志分析，同时有 18%的完全不知道日志分析[2]。可见，人们对日志和日志管理的认识仍然是片面性的，日志管理亟待完善和提高。

在视频会议领域存在同样的问题，本文对国内外各大商用视频会议系统进行了调研，如华为、视高、中兴、腾商、视维；国外的 Polycom，Sony，Cisco 等，这些视频会议系统中，仅有华为、视高、Polycom 等少量视频会议系统实现了较为完善的日志管理机制，如：华为视频会议系统在视频会议管理台软件中添加了独立的日志管理模块用于记录系统每天的运行，同时在系统后台维护管理中还添加了定时软硬件监测，日志记录，故障自动诊断等[3]；视高视频会议系统在终端上实现了独立的工作日志管理页面，用于处理用户在线记录、日志管理、群发日志，同时在服务器上也实现了专门的日志服务模块[4]，Polycom 视频会议系统也实现了日志管理模块。可见，各视频会议系统厂商对日志管理的认识不同，研发的日志管理不同，甚至不提供日志管理，这给视频会议系统的日常使用和维护带来了一定的困难。

CoolView 视频会议系统是实验室自行研发的系统，原有的日志管理较简单，只提供用户登录等基本

收稿日期：2014-10-15
基金项目：2012 年广东省大学产学研结合基金资助项目（2012B091100449）
Foundation Item: 2012 University-Industry Cooperation Project of Guangdong Province (2012B091100449)

信息的采集和下载，且和视频会议系统本身联系紧密。本文拟重新设计和实现一个日志管理子系统，相对独立并提供完整的日志信息参加、查询和管理等。

2　系统的结构和构成

日志管理子系统一方面要采集视频会议产生的各种信息，包括大量的实时信息，同时要不影响系统的正常运作。所以，本文的日志管理子系统与 CoolView 视频会议系统是松耦合的，采用面向切面编程的思想，将日志采集点归入了一个切面——日志实时采集器，日志管理子系统的体系结构如图 1 所示。

如图 1 所示，在结合面向切面编程（AOP）的日志管理设计思想的基础上[5,6]，日志管理系统被分割 5 大模块，由左上至右下分别是会议功能执行点、日志页面模块、日志服务模块、日志工具集、日志数据库。

会议服务功能执行点是所有日志采集点的汇总，也是会议功能执行关键点，实现了日志实时采集切面与各会议功能切面的松耦合。

日志页面模块是日志管理子系统的视图层，主要负责实现日志管理界面和发送并响应日志管理的相关请求。日志页面子模块的实现主要包括两大部分，一部分是利用 SSH 框架的 Struts 技术实现的业务逻辑控制器 Action 类，JSP 文件和 Struts 配置文件；另一部分是利用网页制作技术 HTML+CSS+JavaScript+Ajax 和 JQuery，HighChart 等框架实现的日志管理页面。日志管理页面主要包括了实时日志监控界面，日志查询页面，日志实时跟踪页面，日志统计页面。

日志服务子模块是实现日志管理系统的核心，该模块位于视频会议服务器系统的业务逻辑层，实现了日志实时采集、日志实时存取、日志统计和日志列表处理等功能，同时采用了工厂模式，由工厂类 ServiceFactory 通过 JNDI 实现日志服务接口的统一调用。如图 1 所示，该模块包括了 4 个部分：日志实时采集器、日志实时存取器、日志统计器和日志列表处理器。

日志工具集是实现日志管理子系统的基础，它包括日志调度器和日志定义两部分，日志调度器完成日志相关任务的调度，日志定义完成日志类型，日志格式的定义以及日志的格式化和反串化（日志反串化是指日志格式化的逆过程，将格式化的日志解释成多个日志字段）。

日志数据库是日志规范化存储的重要容器，它负责日志数据库的创建和所有日志的规范化管理。

3　日志管理模块的实现

采用了 SSH（Struts+Spring+Hibernate）框架实现上述系统。其主要类图如图 2 所示。

如图 2 所示，展示了实现日志管理系统的主要类的类图，图顶端 7 个 Action 类图表示的是实现日志业务逻辑控制器的关键类，图底部 7 个日志实体类表示是实现日志数据库的关键类，LogMessage 类是实现日志定义的关键类，其他类则是实现日志服务模块的关键类。

3.1　日志的分类和封装

日志的分类和封装是实现日志管理子系统的基础，其合理化程度将决定日志管理难度和日志管

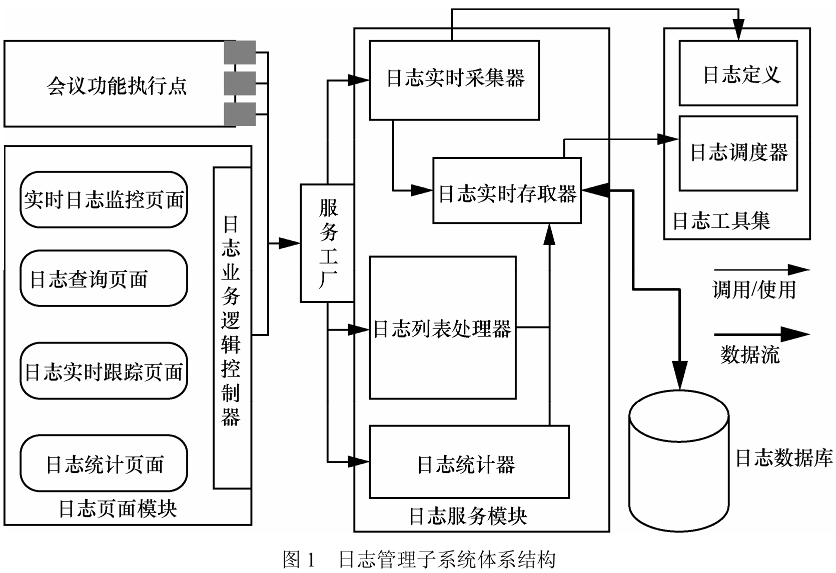


图 1　日志管理子系统体系结构

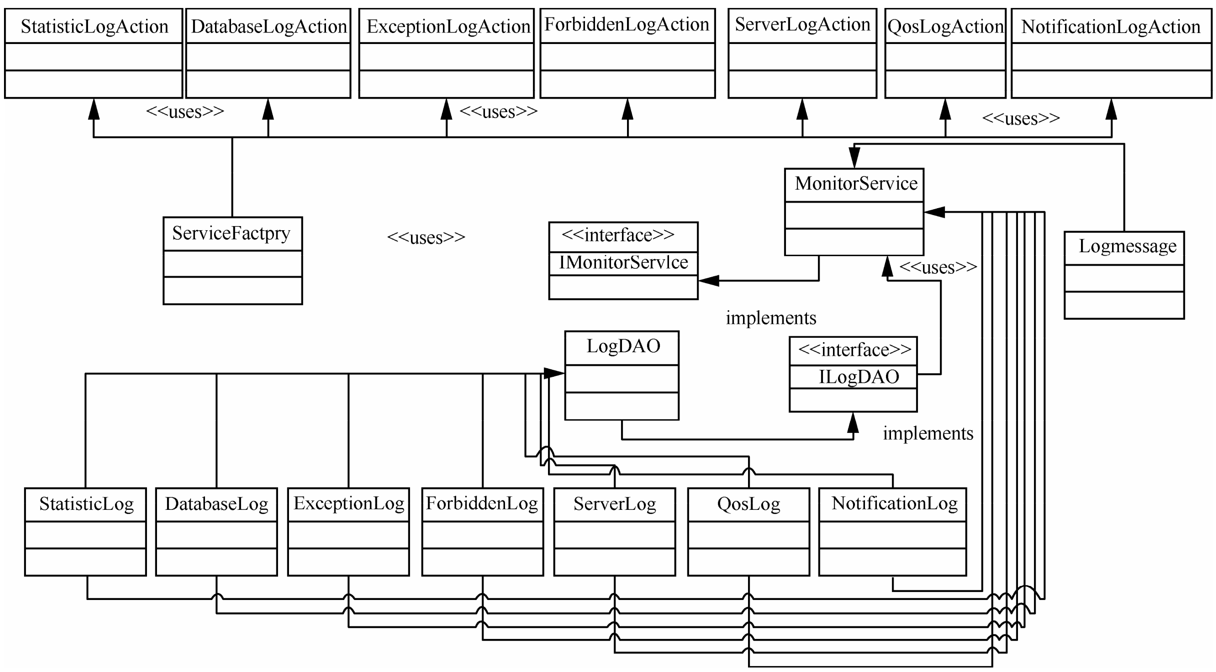


图 2　日志管理系统主要类的类图

理子系统的实现难度。根据日志管理子系统的设计理念，日志的记录应囊括会议操作记录、异常记录、非法操作记录、数据库操作记录、服务器运行记录等，同时，还应满足记录过程不影响系统性能，日志存储筛选方便等性能要求，因此，参照 Log4j[7,8] 和 Syslog[9]，将日志类别划分为 8 大类，分别是统计日志、数据库日志、异常日志、非法操作日志、服务器日志、QoS 日志、通告日志、审计日志[10]。这 8 个大类下又分若干小类，参照文献[7~9]，定义了各小类日志格式，每条日志包括 6 个字段，分别是日志 ID、日志类别、时间戳、日志名称、日志标签、细节信息。构成日志的各个字段之间采用“[”和“]”作为分隔符，每条日志按照“[时间戳][日志类别][日志 ID][日志标签][日志名称][细节信息]”的格式进行组织[11]。

日志由 LogMessage 类完成封装，定义了组常量分别表示日志类型和日志 ID，日志类型常量格式为“LOG_TYPE_日志类型”，如：统计日志类型常量表示为 LOG_TYPE_STATISTIC；日志 ID 常量格式为“ID_日志类型_操作主体_操作名称”，如：终端登录日志 ID 常量表示为 ID_STATISTIC_ TERMINAL_LOGIN，其整数表示：10000。同时，LogMessage 类通过重写 toString 方法实现对日志的格式化处理。LogMessage 类的类图如图 3 所示。

以上类图中，带 5 个参数的 LogMessage 构造方法实现了新日志的创建，带一个参数的 LogMessage 方法实现了日志的反串化，其他 get 方法则各自用于返回不同的日志字段。

3.2　日志服务子模块的实现

日志服务子模块位于视频会议服务器系统的业务逻辑层，是日志管理功能的处理核心，根据是否与数据库直接交互，该层被分为两部分，一部分是与数据库交互的日志存取器，另一部分则是负责日志监控、查询、统计等功能的业务逻辑部分，根据面向切面编程的思想，两部分是松耦合的，因此日志服务子模块采用 SSH 集成框架中的 Spring 框架技术实现了上述要求，Spring DAO 提供了数据访问的抽象，保证了系统性能和数据完整性，它实现了日志实时存取功能；控制反转（IoC）技术则促进了松耦合，建立了负责日志监控、查询、统计等功能的业务逻辑切面。

本文为了实现 CoolView 视频会议服务器业务逻辑的统一管理，同时考虑到利用 Spring 框架 IoC 机制完全代替实现 CoolView 视频会议服务器业务逻辑的传统 EJB 技术的技术成本，本文选择继续沿用传统 EJB 组件实现日志服务模块的业务逻辑部分，将该业务逻辑部分封装成一个 Service，同时在业务逻辑层部分采用了面向接口编程的软件设计思想，为 Service 定义了一个接口，并且利用工厂

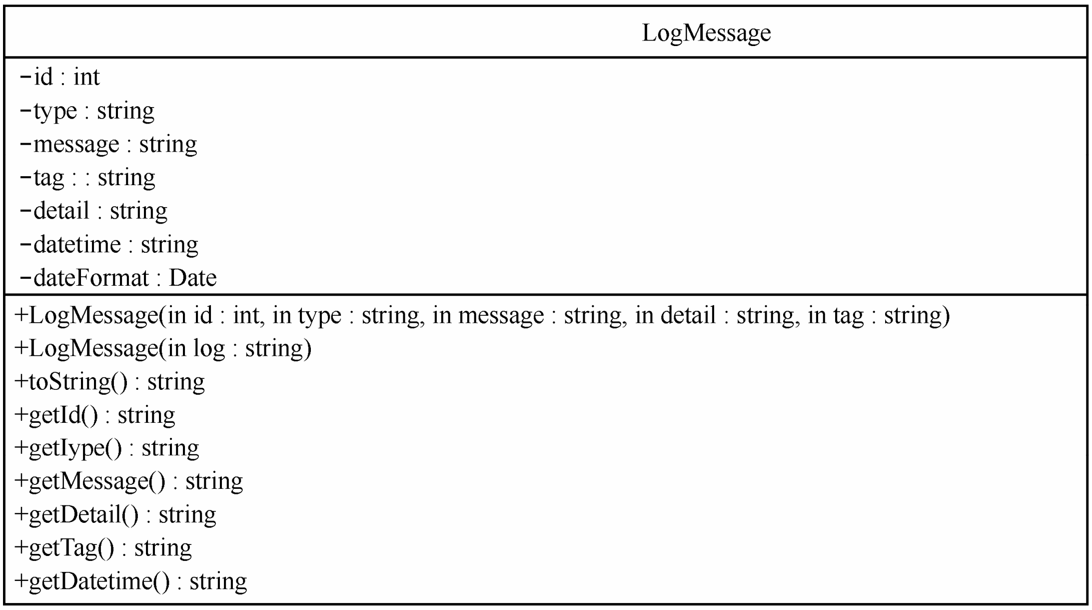


图 3　LogMessage 类的类图

模式，将接口添加至 ServicFactory 工厂类。

根据以上设计，日志服务子模块的实现主要包括两部分，一部分是实现日志服务模块实时日志存取器部分的 ILogDAO 接口和 LogDAO 实现类；另一部分是实现日志服务模块其他功能的 IMonitorService 接口和 MonitorService 实现类。日志服务子模块的类图及关系如图 4 所示。

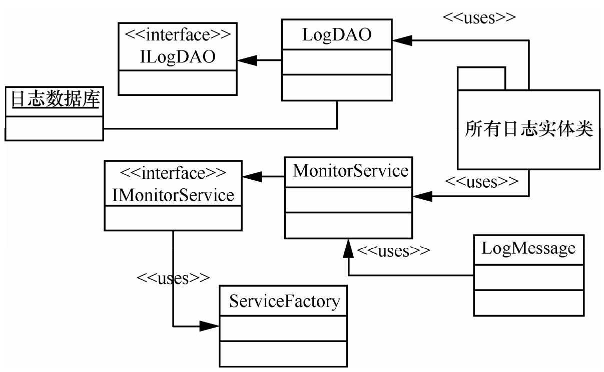


图 4　日志服务子模块的类图及关系

以日志实体类类分组的形式代表所有日志实体类，用一个对象图代表日志关系型数据库。

3.3　日志业务逻辑控制器的建立

日志业务逻辑控制器是日志管理界面与日志服务模块间的纽带，它负责用户请求的响应处理，后台业务逻辑的调用以及返回页面的跳转等。为了实现日志管理子系统表现逻辑和业务逻辑的解耦，提高系统的可维护性和可扩展重用性，同时结合本文对日志类型的定义和用户请求按日志类型的分类，本文采用 SSH 集成框架的 Struts 框架技术，按照日志类型对日志业务逻辑控制器进行分类设计。

按照日志类型不同，设计了 7 个子日志业务逻辑控制器，每个子日志业务逻辑控制器对应一个 Action 类，分别是 StatisticLogAction、DataBaseLogAction、ServerLogAction、ExceptionLogAction、Forbidden LogAction、QosLogAction 和 NotificationLogAction，各 Action 类的类图及关系如图 5 所示。

如图 5 所示，由于各 Action 类的类图相似，本文以 StatisticLogAction 类为例作具体类图展示，Action 控制器负责完成后台逻辑的调用，而用户请求的响应和页面的跳转则由 Struts 框架的 View 层的 JSP 负责完成，Struts 配置文件则实现了 Action 类方法与 JSP 文件的绑定。

4　结束语

日志管理子系统已经基本实现完成，日志统计页面运行如图 6 所示。

日志管理子系统实现了日志的监控、查询、统计和跟踪功能，在 IE9、Chrome、Firefox、Safari、Opera 等浏览器中运行稳定，日志采集全面，数据库运行流畅。

本文设计的日志管理系统具有完备的日志分类，参照 Log4j 和 Syslog 定义了日志格式，采用 SSH 技术实现了各模块，日志分析和挖掘的功能将是下一步的工作重点。

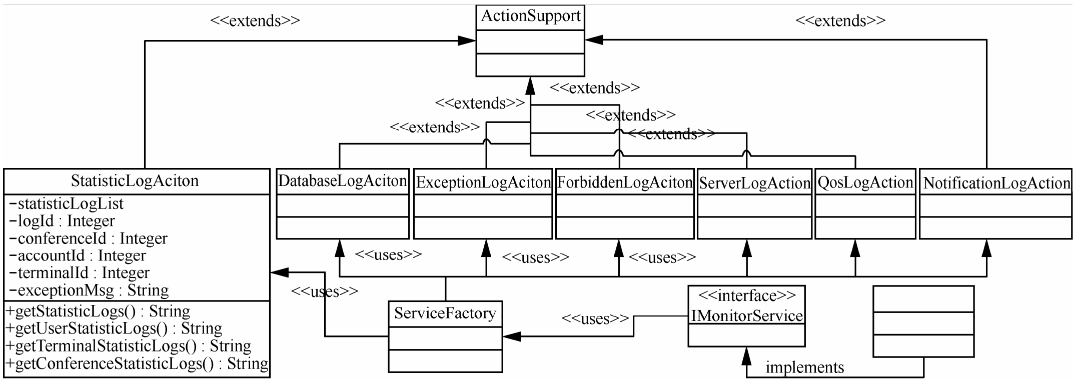


图 5　各 Action 类的类图和关系

日志类别	统计个数
状态日志	187
数据库日志	226
异常日志	1
非法操作日志	0
服务器日志	103
Qos日志	0
通告日志	182

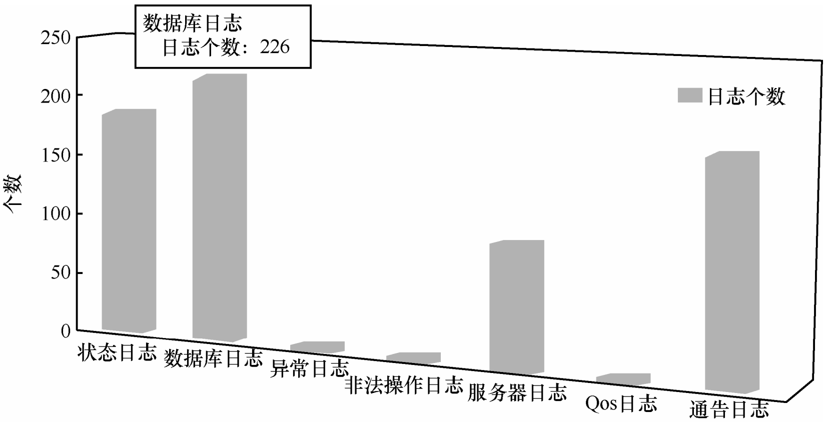


图 6　日志统计运行截图

参考文献：

[1] DAVE S, BARBARA F, JERRY S. SANS Eighth Annual 2012 Log and Event Management Survey Results: Sorting Through the Noise[R]. SANS Institute. 2012.

[2] SANS：2012 年度日志管理调查报告[EB/OL]. http://yepeng.blog.51cto.com/3101105/862473, 2014.
SANS: 2012 log management survey[EB/OL]. http://yepeng.blog.51cto.com/3101105/862473, 2014.

[3] HUAWEI SMC2.0 V100R001 管理员指南[EB/OL]. http://www.huaweri.com/cn/, 2013.
HUAWEI SMC2.0 V100R001 administrator guide[EB/OL]. http://www.huawei.com/cn/, 2013.

[4] 视高全高清视频会议系统产品介绍[EB/OL]. http://www.seegle.com/V4/product_feat.htm, 2014.
The introduction of seegle full HD video conference system[EB/OL]. http://www.seegle.com/V4/product_feat.htm, 2014.

[5] 王永红. 面向方面编程（AOP）在日志管理中的应用[J]. 硅谷，2011,(20): 125-126
WANG Y H. The application of aspect oriented programming(AOP) on log management[J].Silicon Valley,2011,(20):125-126.

[6] 牛永洁. 基于 AOP 的动态日志系统的实现[J]. 计算机技术与发展，2011,21(3):102-104.
NIU Y J. Implementation of dynamic log system based on AOP[J]. Computer Technology and Development, 2011,21(3)：102-104.

[7] Apache Logging Services Log4j[EB/OL]. http://logging.apache.org/log4j/1.2/,2014.

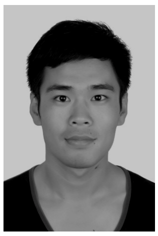
[8] 陈兀,程耕国. 基于 Struts+Spring+log4j 框架的日志管理[J]. 武汉科技大学，2010, 9(5):5.
CHEN W, CHENG G G. The application of spring+log4j+struts in the diary management[J]. Software Guide, 2010,9(5):5.

[9] LONVICK C. The BSD Syslog Protocol(RFC3164)[S]. Cisco Systems, 2001.

[10] SÖDERSTRÖM O, MORADIAN E. Secure audit log management[J]. Procedia Computer Science, 2013, (9): 10.

[11] 罗仲君. 视频会议服务器监控管理系统的设计与实现[D]. 广州: 华南理工大学, 2013.
LUO Z J. Design and Implementaion of Monitoring and Management in Video Conferencing System[D]. Guangzhou: South China University of Technology, 2013.

作者简介:



徐凯硕（1991-），男，山东青岛人，华南理工大学硕士生，主要研究方向为计算机网络应用。

袁华（1969-），女，四川成都人，博士，华南理工大学副教授，主要研究方向为计算机网络应用、图形处理、视频通信。