RBAC技术在奥运气象服务信息发布系统中的应用

王玉彬[1] 周 勇[2] 周海光[3] 余东昌[1] 苏德斌[1] 梁 丰[1]

(1. 北京市气象局, 100089; 2. 国家气象信息中心;
3. 中国气象科学研究院灾害天气国家重点实验室)

提 要: 结合2008年北京奥运会气象服务信息发布系统的研发,对比分析了目前数据传输业务系统中几种常用的监控方式,提出了针对奥运气象服务信息发布系统运行状态进行安全、有效、便捷监控问题的解决方案,详细论述了应用基于B/S结构的RBAC技术实现分布式监控功能的原理和方法。

关键词: 奥林匹克运动会 气象服务 B/S结构 RBAC 系统监控

Application of RBAC Technique to Beijing Olympic Games Weather Service Information Issuing System

Wang Yubin[1] Zhou Yong[2] Zhou Haiguang[3] Yu Dongchang[1] Su Debin[1] Liang Feng[1]

(1. Beijing Municipal Meteorological Bureau, 100089; 2. National Meteorological Information Centre;
3. State Key Laboratory of Severe Weather, Chinese Academy of Meteorological Sciences)

Abstract: Combined the development of Beijing Olympic Games weather service information issuing system, several often used monitoring means in data transmission operational systems were comparatively analyzed. Regarding the running state of Olympic Games weather service information issuing system, a solution is proposed to exert secure, effective and convenient supervision. RBAC (Role—Based Access Control) technologies based on B/S structure, in implementation of distributed monitoring are also covered in the paper.

Key Words: Olympic Games weather service B/S structure RBAC system monitoring

资助项目: 科技部国家科技攻关计划"北京奥运短时临近预报实时业务系统建设"(编号: 2005BA904B05),国家科技计划项目衔接—科技奥运专项: 北京奥运会国际天气预报示范计划支持技术研究(编号: Z0006279040191)

收稿日期: 2008年5月26日; 修定稿日期: 2009年1月23日

引 言

在北京举办第29届奥林匹克运动会，对于气象服务而言是一次难得的历史机遇，同时也是巨大的挑战。一方面，成功的奥运赛事离不开高效的气象服务保障。比赛组织者需要准确的天气信息以便提前做好安排，运动员需要精细的天气预报以便提高比赛成绩，观众也需要更富有针对性的应用气象服务[1]。与亚特兰大、悉尼奥运会的气象服务信息发布方式[2]相比，2008年北京奥运会在传统的Info系统和Internet网站外，还增加了对奥组委赛事指挥中心(SCC)、主运行中心(MOC)等用户定点、定量的气象服务产品分发。另一方面，信息网络安全问题也愈显突出。早在2005年下半年，奥组委信息网络系统就曾发生过黑客入侵事件[3]。因此，及时、准确地提供奥运气象服务信息，并保障与其相关的信息发布系统安全运行，面临挑战，任务艰巨。

为了满足2008年北京奥运会气象服务产品需求，北京奥运气象服务中心研发了奥运气象服务信息发布系统(OMIS系统)，与短时临近交互预报预警平台(VIPS)、奥运场馆精细预报交互平台(OFIS)以及各奥运协办城市气象局预报服务系统等连接，接收北京及各奥运协办城市的天气实况、预报、警报等数据文件，解码入库，自动生成各类奥运气象服务产品，并与北京奥运大厦、Internet托管服务器提供商等专线连接，向SCC、MOC、奥运气象服务网站、Info2008系统等分发各自所需的气象服务产品，是北京奥运气象服务中心向重点用户、社会公众传递气象信息的枢纽。图1给出了OMIS系统与其它系统及相关服务对象的结构关系图。

在权衡系统使用便利性和安全性的基础上，第29届奥运会气象服务信息发布系统的研发中，采用了基于B/S(Browse/Server，浏览器/服务器)结构的RBAC(Role－Based Access Control，基于角色的访问控制)技术实现了分布式监控功能，为预报员、系统管理员、现场服务人员和其他各类用户提供了安全、有效、便捷的监控平台，在奥运气象服务的实际应用中收到了很好的效果。

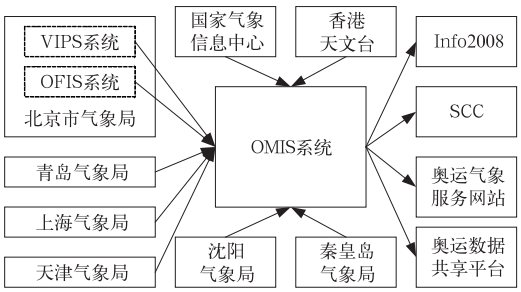

图1 OMIS子系统与奥运气象服务系统及相关服务对象的结构关系图

1 C/S和B/S结构业务系统监控方式比较分析

用于业务系统监控的软件主要基于两种结构：C/S(Client/Server，客户机/服务器)结构和B/S(Browse/Server，浏览器/服务器)结构，分别针对集中式监控和分布式监控两类应用[4]。

基于C/S构架的集中式监控对工作人员的工作地点有所约束，适于有固定工作岗位的运行值班人员使用；而基于B/S构架的分布式监控可以使工作人员在不同场所异地办公，甚至是在家或出国期间，也能及时了解到系统运行状态，快速处理，既适于固定岗位运行值班人员使用，也适用于不参加值班的系统维护、技术支持人员使用。但B/S结构安全隐患多于C/S结构，必须辅以更多、更完备的安全访问和控制策略，才能满足业务应用需要。

早期版本的中国气象局气象卫星综合应

用业务系统(9210 工程)主站通信业务监控平台、PCVSAT 卫星单向广播系统中心站监控软件等基于 C/S 结构;新版国际、国内通信业务系统监控软件、中国气象局向国务院和其它同城用户单位发布决策服务产品的业务系统监控则基于 B/S 结构。

2　基于角色的访问控制(RBAC)结构模型

出于安全方面的考虑,分布式监控需要结合相应的访问控制,才能提供奥运气象服务业务应用。访问控制机制可以限制对关键资源的访问,防止非法用户进入系统或合法用户对系统资源的非法使用。基于角色的访问控制技术(RBAC)以其灵活性、方便性和安全性在许多系统中得到了广泛应用[7]。

RBAC 的基本思想是在用户和访问权限之间引入角色作为中介,通过对角色的授权来控制用户对系统资源的访问[8]。其优势在于:"角色"中间环节的添加极大地简化权限管理复杂度,使系统的组织结构简洁灵活而且易于理解和表达。由于系统中的角色权限的关系相对于用户权限的关系更稳定,只有当业务发生变化或者结构重组时才有必要进行调整,因此提高了权限管理的效率和系统稳定性。2008 年北京奥运会气象服务信息发布系统的监控模块层次结构相对简单,主要基于核心 RBAC 模型设计。

3　奥运气象信息发布系统监控模块的设计与实现

3.1　B/S 结构的选择依据

选择 B/S 架构主要考虑了两方面的因素。首先,2008 年北京奥运会气象服务信息发布系统要提供给诸多用户使用:制作天气预报的预报员、主协办城市负责通信传输的值班人员、通信网络技术人员、OMIS 系统运行值班人员、OMIS 系统技术支持人员、OMIS 系统管理员、网站值班人员、网站维护人员、相关各级单位领导、现场服务人员以及部分重点用户等,用户多、分布广,若采用 C/S 结构设计开发,存在安装和维护困难,工作量大,灵活性差等问题。

其次,由于 OMIS 系统是连接气象局与奥组委赛事指挥中心、奥运主运行中心、奥运气象服务网站、Info2008 系统等的通信枢纽,对奥运气象服务至关重要,因此要求能够及时发现问题并加以处理。通过 B/S 结构设计开发监控系统,可以更方便技术维护人员的使用,保证快速、及时地处理问题。

3.2　用户角色定义

从应用需求和网络安全的角度出发,OMIS 系统不同的用户必须被授予不同的访问权限,而授予的权限还需要根据人员、岗位的调整变化而及时变更。因此,采用科学合理的访问控制机制非常重要。

从 RBAC 的基本思想出发,首先将用户划分为不同的角色,再通过对角色的授权来控制用户对系统资源的访问。根据用户使用性质的不同,把 OMIS 系统用户划分为如下几类,分别归为不同的角色:数据提供者、产品使用者、运行值班者和系统维护者(如表 1)。

3.3　角色权限分配

给不同角色授予不同权限,是 RBAC 的核心思想之一。就 2008 年北京奥运会气象服务信息发布系统而言,不同角色间存在有相关和包含关系,可以 采用公式化表示如下:

角色集 $R=\{r_1,r_2,r_3,r_4\}=\{$"数据提供者"、"产品使用者"、"运行值班者"、"系统维护者"$\}$,分别表示四种角色。权限集 $P=\{p_1,p_2,\cdots\}$。$P(r_i)$表示角色 r_i 的权限子集。

各种角色的权限分配情况如表 2 所示。

表1 OMIS系统用户角色定义

角色	角色对应用户
数据提供者	＞北京市气象局奥运服务团队预报制作岗工作人员、VIPS、OFIS等系统使用者 ＞各协办城市(青岛、上海、天津、沈阳、秦皇岛)气象局预报员、值班员、通信网络技术人员、业务管理人员 ＞国家气象中心、国家气象信息中心等国家级技术支持单位奥运数据传输值班人员
产品使用者	＞北京奥运气象服务中心相关领导 ＞中国气象局及相关职能司部分领导 ＞北京奥运气象服务网站值班人员、网站维护人员 ＞奥运场馆现场服务人员 ＞SCC、Info2008等重点用户 ＞国家气象信息中心数据共享平台维护人员
运行值班者	＞OMIS系统运行值班人员
系统维护者	＞OMIS系统应用软件开发和技术支持人员 ＞OMIS系统服务器系统管理员

表2 OMIS系统角色权限分配

代码	权限	数据提供者	产品使用者	运行值班者	系统维护者
p_1	数据文件上传(FTP send)	√		√	√
p_2	服务产品上传(FTP send)	√		√	√
p_3	数据文件下载(FTP get)		√	√	√
p_4	服务产品浏览(Http方式)		√	√	√
p_5	服务产品下载(Http方式)		√	√	√
p_6	调看历史数据	√	√	√	√
p_7	查询系统日志	√	√	√	√
p_8	查看进程状态	√	√	√	√
p_9	查看磁盘使用率	√	√	√	√
p_{10}	统计到报率、及时率			√	√
p_{11}	修改传输节目表			√	√
p_{12}	修改数据库				√
p_{13}	修改程序				√
p_{14}	修改用户权限				√
p_{15}	增加或删除用户				√
p_{16}	关闭或重启系统				√

3.4 B/S结构RBAC的实现

2008年北京奥运会气象服务信息发布系统基于Suse Linux操作系统平台开发，其B/S结构RBAC功能的实现，结合采用了操作系统自带功能、静态和动态网页开发，以及为提高效率而采用的类似C/S结构的后台进程。

OMIS启动了Linux操作系统的FTP和Http服务，以支持B/S方式的监控。表2中p_1～p_3权限通过操作系统自带FTP Server功能实现，设置参数为开机自动启动并记录详细日志。除有特殊需求的用户外，依据“角色”而不是“用户”，设置用户名和口令。静态和动态网页分别用Html和PHP开发，对p_4～p_{11}权限通过开发PHP函数实现，基本是每种权限对应一个函数，并用Html静态页面链接。p_{12}～p_{16}权限通过PHP结合后台进程间接实现。后台进程采用BShell和C、C++编制，特别注意用户名和密码的认证功能。

监控程序功能包括：网络和系统状态、传输产品节目表、北京及协办城市数据接收状态历史记录查看、服务产品展示、服务产品下载等。监控程序的输入为各种监视和统计信息，输出为静态和动态链接页面，提供对各种统计数据的链接、显示和下载服务。基本固定的信息用HTML静态网页发布，而需要经常更新的内容和链接通过PHP实现。监控程序以Web方式对各种服务产品的文件名、文件格式、产品制作单位、制作日期、文件说明、文件传输状态信息等进行实时显示。

用户可以在奥运气象服务中心内网或中国气象局内部局域网上任意一台授权的主机

远程访问 OMIS 系统,授权结合采用了 IP 地址控制机制,由常规业务网络管理提供最外层的安全保障。用户通过主页面登录,合法用户将在用户名和密码认证后,依据所属的角色授权访问。

4　结语

奥运会气象服务的实际业务应用表明:选择基于 B/S 结构的 RBAC 技术设计和开发的 2008 年北京奥运会气象服务信息发布系统监控程序完全符合安全、有效、便捷的应用需求,收到良好效果,特别是有助于系统管理人员快速地做出响应和处理,为提供优质的奥运气象服务提供了保障。此外,在用户权限的变更管理方面更加便捷,如北京的预报人员,因工作需要,其角色就在奥运服务开始前,从原定的"数据提供者"变更为"运行值班者",以便于其了解自己制作、上传数据的正确性,并协助监视 OMIS 系统运行情况。

该技术也可以应用于其它业务系统,特别是公共气象服务软件的开发中。对于安全性要求不是很高的应用,结合适当的安全控制技术后,可以把目前单位内网授权用户访问扩展到更大范围访问,使其应用更加方便。

参考文献

[1] 章国材,张卫红,王金星. 气象与北京奥运保障工作[J]. 中国科技奖励,2005,(1):66-69.

[2] 梁丰,陈明轩,王玉彬. 近两届奥运会气象服务保障综述[J]. 气象,2002,29,(10):3-8.

[3] 郝文江,杨永川. 北京奥运与网络安全[J]. 北京人民警察学院学报,2007,(5):68-74.

[4] 王玉彬,周海光,苏德斌,等. 天气预警系统技术基础及设计[M]. 北京:气象出版社,2006.

[5] 孙田强. 基于 web 的通用信息管理系统的设计与实现[D]. 复旦大学硕士论文:2007.

[6] 郭晓玉,鲍慧,刘春玉. 基于 B/S 的综合自动化远动信息管理系统研究[J]. 电力系统通信,2006,(1):48-58.

[7] 吴迪,朱森良,陈溪源,等. 分布式环境下基于 RBAC 互操作的安全检测[J]. 浙江大学学报(工学版),2007,(9):1552-1571.

[8] 詹则慧,彭自成. RBAC 学院管理系统安全体系的设计与实现[J]. 华南师范大学学报(自然科学版),2007:(4):59-65.

[9] David Feraiolo, Ricllard Kuhn. Role－based access controls[R]. In Proceedings of 15th NIST－NCSC National Computer Security Conference. Baltimore, MD,October l3-16, 1992: 554-563.