WebSphere与 Domino在多目录环境下单点登录的实现

袁桂霞, 杨季文

(苏州大学 计算机科学与技术学院, 江苏 苏州 215006)

[摘要] 实现 WebSphere与 Domino的单点登录, 可以有效地简化用户的使用难度和管理的复杂程度. 简要介绍了在单目录条件下实现 WebSphere与 Domino单点登录的基本原理, 讨论了企业多目录和多用户身份的实际情况, 分析了由此产生的单点登录问题, 探讨了 WebSphere与 Domino分别采用第三方 LDAP的可能性与解决多目录问题的方法. 并结合实例分析了多用户身份情况下单点登录失败的主要原因, 利用"名称映射"方法解决了多用户身份情况单点登录的难题. 在某企业的实际应用表明该方法具有可行性.

[关键词] 单点登录, 多目录环境, WebSphere, Lotus Domino

[中图分类号] TP393 [文献标识码] B [文章编号] 1672-1292(2006) 04-0075-04

Implementation of SSO Between WebSphere and Domino in Multi-Directory Environment

YUAN Guixia, YANG Jiwen

(School of Computer Science and Technology, Soochow University, Suzhou 215006, China)

Abstract Single Sign-on between WebSphere and Domino can lessen difficulty for users and complexity for management. This paper introduces the principle of Single Sign-on between WebSphere and Domino in a single directory, analyses the major problem of Single Sign-on which is caused by multi-directory and multi-identity in the enterprise, studyies the possibility of WebSphere and Domino using the third party LDAP and studies how to settle the problem of multi-directory. It analyses the real reason of the failure of Single Sign-on based on examples and settles the problem of Single Sign-on by 'name mapping' in the case of multi-identity. The possibility of the method has been validated by the actual application in an enterprise.

Key words Single Sign-on, multi-directory, webSphere, lotus domino

0 引言

WebSphere是 IBM公司优秀的企业级软件平台, 提供了包括应用服务器、企业门户、无线应用、业务整合等多个方面的产品, 是 J2EE技术路线中优秀的企业应用平台. WebSphere Application Server是核心 Web服务和 J2EE认证的应用程序服务器, 它启用了业界领先的服务质量和一系列灵活的部署配置来满足单机的、多服务器分布式的和高度动态的非集中分布式企业环境的需要[1].

Lotus Domino是一套得到广泛应用的群件系统, 它集成了多项高尖端技术, 包括通讯(Communication)、群件合作(Collaboration)和对等协调(Coordination)这 3大支柱功能[2]. Louts Domino可以作为优秀的基础通信平台, 提供企业级邮件、目录服务, 可以作为基础工作流引擎, 与 Lotus QuickPlace, Domino Workflow等系统协同工作, 高效灵活地制定工作流.

WebSphere是一个建立、管理并配置 Web应用的大型软件产品, 可以配置和管理从简单 Web站点直至基于 Web复杂的企业业务和电子商务系统. 它侧重于对结构化数据的管理和电子商务的业务处理. 而

收稿日期: 2006-07-20

作者简介: 袁桂霞(1978-), 女, 硕士研究生, 助教, 主要从事中文信息处理、远程教育等方面的教学与研究. E-mail: yuangx@jstvu.edu.cn

通讯联系人: 杨季文(1963-), 教授, 主要从事中文信息处理等方面的教学与研究. E-mail: jwyang@suda.edu.cn

Lotus Domino作为企业级通讯和 Web开发平台,具有强大的集成、协作、消息传递和工作流等功能,它侧重于通过文档型数据库获取半结构化和非结构化数据,在电子政务、办公自动化等领域应用广泛.企业常常通过集成这两者的优势功能,把 WebSphere强劲的事务处理能力与 Domino领先的协作功能紧密集成,为企业提供强大、稳定而全面的信息平台.

1　问题的提出与初步解决

由于 WebSphere和 Domino的强大功能,企业中存在众多基于此的应用系统.如基于 Domino开发的邮件系统、OA系统,基于 WebSphere开发的电子商务系统、企业门户系统等.在这种情况下,一般每个应用系统都有安全认证系统,常采用独立的用户认证模块,在各自的数据库中进行用户认证.但这种用户认证模式特别是较多系统同时使用时存在诸多不足之处[3]:用户需要记忆多个系统用户名和密码;各系统均需要存储用户信息,造成大量数据冗余;每个系统均需开发用户认证模块,重复开发且重用率低.在这种情况下,使用单点登录(Single Sign-on, SSO)技术便可解决上述问题.所谓单点登录,意味着当用户从一个应用程序切换到另一个应用程序时,不再被提示要求输入用户名和密码(或证书),而这些应用程序可以放置在一个或者多个服务器上[4].简言之,用户只需要在某个网络域中进行一次身份认证,随后该用户便可访问该域中被授权的所有网络资源,而不需要再次主动或被动地参与身份认证的过程.相对于传统的用户登录方式,单点登录的益处是显而易见的:用户仅需记忆一个用户名密码,一次登录全网漫游;减轻了系统数据冗余和管理员管理工作量;多个系统可重复使用登录模块,既减轻开发工作量又切实提高了系统的安全性.

WebSphere和 Lotus Domino之间的单点登录是通过一种称为轻量级第三方认证(Lightweight Third Party Authentication, LTPA)的机制来实现的.LTPA是一种应用在 WebSphere和 Lotus Domino以及其他 IBM系列产品的认证技术[5],一般 LTPA在 LDAP(Lightweight Directory Access Protocol轻量级目录访问协议)支持下,采用 Domain cookie方式实现.当用户第一次访问 WebSphere或者 Domino的受限资源时,服务器要求用户输入用户名和密码.系统在 LDAP服务器中进行搜索,若验证成功,则服务器返回一个 cookie,该 cookie中除了含有一般 cookie都包含的名称、到期时间、所属域、传输加密协议外,在 cookie值部分存储了加密的 LTPA标记.LTPA标记中包含了唯一标识用户 ID信息、强制的 LTPA过期时间和用于确认标记的数字签名,结构如图 1所示.

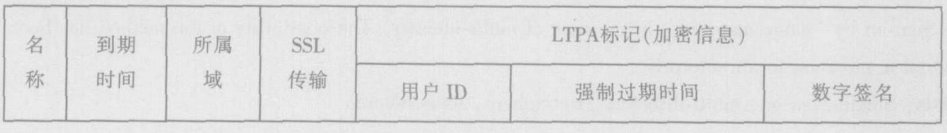

图 1　含有 LTPA 加密信息的 cookie

当再次访问同一域中的其它服务器的受限制信息时,浏览器将向服务器发送含有加密 LTPA标记的 cookie服务器对加密的 LTPA标记进行解密,若 LTPA标记中表明用户已经通过认证,则省略验证过程,从而实现在 WebSphere, Lotus Domino或其它 IBM产品之间的单点登录.

2　多目录环境下的单点登录实现

利用上面介绍的单点登录方式,可以在理想的单目录环境下(即利用 Domino提供 LDAP服务)对两者设置单点登录.基本步骤是在 WebSphere App Server设置 LDAP和 LTPA,并启用全局安全性,导出 LTAP密钥.在 Domino中设置服务器文档,确定单点登录域,并导入 LTPA密钥[5].利用 Domino提供 LDAP服务的原理如图 2所示.

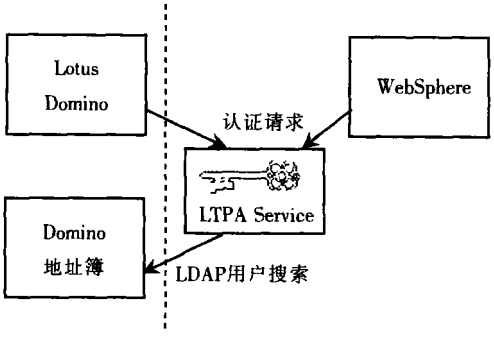

图 2　单目录环境下的单点登录实现机制

尽管企业的最终目标是建立一个统一的包含所有企业用户以及相关资源的单一目录,但在实际情况下,企业可能会拥有至少两个甚至更多的目录.造成这种情况最主要的

原因是, 企业的不同应用系统有不同的目录要求. 如 IBM 产品常默认集成 IBM Directory Server, 而微软公司则在微软产品支持的系统和企业域管理中应用 Active Directory. 而在大中型企业中, Lotus Domino常常是企业级别邮件系统的首选工具, 在院校科研机构还经常使用开源的目录产品如 OpenLDAP等. 在多目录并存的情况下, Domino一般仅处于邮件服务器或 Web服务器的角色, 企业的基础目录服务器由非 Domino的其它 LDAP服务器承担. 相比于理想的单目录情况, 多目录情况下对 WebSphere和 Domino单点登录的难度更大, 同时也更加具有实用意义. 多目录环境下, 一般会将 WebSphere与 Domino设置成共同使用第三方 LDAP实现单点登录, 其原理如图 3所示.

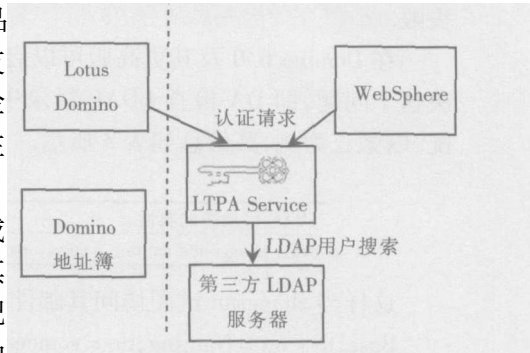

图 3 多目录环境下的单点登录实现机制

(1) WebSphere对非 Domino目录服务器的支持. WebSphere对于目录服务的支持程度较高, 符合 LDAP标准的目录服务器均可直接配置, 如 IBM 的 IBM Directory Server, Microsoft的 Active Directory等, 配置界面如图 4所示.

(2) Domino对第三方 LDAP目录服务的支持. Domino除自身可提供 LDAP服务, 同时也可通过建立并配置 Directory Assistance数据库, 利用第三方的 LDAP进行用户身份认证, 基本步骤为:

①建立一个以 da50. ntf为模板的数据库, 如 da. nsf

②在 da. nsf数据库中增加一个 Directory Assistance条目并进行相关配置, 如图 5所示.

③在 names. nsf的用户目录中加上 da. nsf数据库, 并进行配置.

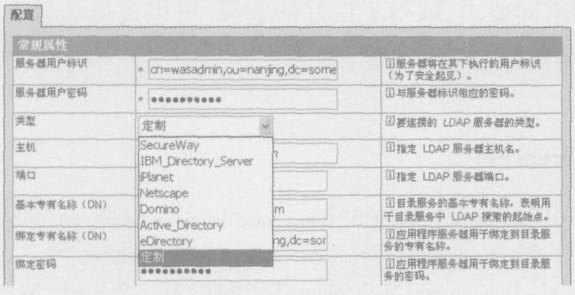

图 4 WebSphere 中设置第三方 LDAP 认证

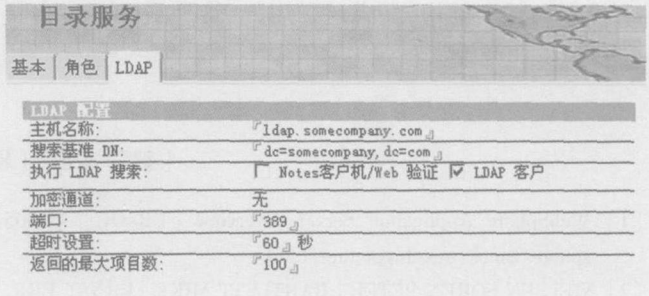

图 5 Domino 中设置第三方 LDAP 认证

在 WebSphere和 Domino同时设置了第三方 LDAP, 并进行 LTPA的导入后, 重启服务器, 即可完成两者基于第三方 LDAP的单点登录.

3 多用户身份的问题讨论

多目录环境下可以通过启用 Domino的 Directory Assistance(简称 DA), 利用第三方 LDAP服务器为 WebSphere和 Domino进行单点登录认证, 但随之而来会带来一个多用户身份的问题. 如用户张三, 在微软 Active Directory中, 其身份信息如表 1如示.

表 1 AD的身份信息

字段	值
dn	cn= zhangsan, ou= Nanjing, dc= somecompany, dc= com
cn	zhangsan

表 2 Domino中的用户信息

User Name	zhangsan/Nanjing/somecompany
Short Name	zhangsan

但在 Domino服务器中, 对应的标识如表 2所示.

当用户 zhangsan首先登录基于 WebSphere应用时, WebSphere会从 LDAP中获取到他完整的 DN, 并建立 LTPA cookie. 当 zhangsan试图使用 Domino服务器上的 Web应用时, 由于 Domino已经配置了 Directory Assistance, 因此可以在 Active Directory中检索到 zhangsan的信息, 允许其访问 Domino应用. 但当 zhangsan访问其在 Domino服务器上的邮件文件时, 问题出现了. 由于邮件文件的 ACL中所列出的标识是 zhangsan/Nanjing/somecompany. 对于 Domino而言, 无从了解 cn= zhangsan, ou= Nanjing, dc= somecompany, dc= com与 zhangsan/Nanjing/somecompany是同一个用户, 因此 Domino拒绝其对邮件文件的访问, 单点登录

失败.

在 Domino 6.0及其更高版可以启用名称映射的方式,检查两个目录中的 Internet地址是否匹配来解决这个问题,即 DA检查 LDAP目录中的 mail信息与 Domino Directory中的 Internet Address属性是否匹配.以张三为例,其信息如表 3所示.

表 3 用户信息对比

LDAP目录中的属性	Domino Directory中的属性
mail zhangsan@nanjing somecompany.com	Internet Address: zhangsan@nanjing somecompany.com

这样当 zhangsan试图访问其邮件文件时,DA会向 LDAP服务器发送搜索请求:

BaseDN: ou=Nanjing, dc=somecompany, dc=com

Filter: cn=zhangsan

attrs to return: "mail"

LDAP服务器返回搜索结果: mail=zhangsan@nanjing somecompany.com,这是 Domino与 zhangsan邮件文件对应的 zhangsan/Nanjing/somecompany的个人文档中的 InternetAddress属性值进行对比,两者匹配.这样就成功地进行了从 LDAP名称到 Domino名称的映射,Domino允许 zhangsan访问其邮件文件,单点登录成功.

4 小结

利用上述方法,在一个同时使用微软 Active Directory和 Lotus Domino目录的企业中,可以实现基于 WebSphere应用服务器的知识管理系统和基于 Domino的邮件系统的单点登录问题,既保护了企业前期的 IT投资和基本架构,又满足了用户、管理员和开发人员的不同要求,取得了良好的效果.可供类似场景下的管理员和开发人员借鉴使用.

[参考文献] (References)

[1] WebSphere Application Server Overview [EB/OL]. [2005-02-01]. http://www-128.ibm.com/developerworks/cn/websphere/zones/was/bigpicture.html

[2] NIELSEN SOREN PETER, BARTLETT MIKE, ERNST ERIC, et al. Domino and WebSphere Together [M]. 2nd ed. New York: IBM Press, 2001: 109.

[3] 张颖江,郑秋华,李腊元,等. 单次登录技术分析及集中身份认证平台设计 [J]. 武汉理工大学学报: 交通科学与工程版, 2004, 28(2): 241-243.
ZHANG Yingjiang, ZHENG Qiuhua, LI Layuan. Analysis of single sign-on technique and design of central authentication platform [J]. Journal of Wuhan University of Technology: Transportation Science and Engineering, 2004, 28(2): 241-243. (in Chinese)

[4] 靳芬,秦肖臻,王卓,等. 用 JSP创建基于 WebSphere的 Domino Web应用 [J]. 微机发展, 2004, 14(10): 17-20.
JIN Fen, QIN Xiaozhen, WANG Zhuo, et al. Design domino web application using JSP based on websphere [J]. Microcomputer Development, 2004, 14(10): 17-20. (in Chinese)

[5] 吴洁明,杨轶鑫,等. 基于 Portal的统一身份认证系统研究与开发 [J]. 航空计算技术, 2004, 34(4): 88-91.
WU Jieming, YANG Yixin. Research and development of unified identity authentication system based on portal [J]. Aeronautical Computer Technique, 2004, 34(4): 88-91. (in Chinese)

[责任编辑: 刘 健]