

基于 LDAP 的框架及其实现

孟凡滋, 谢 琦

(郑州大学 信息工程学院, 河南 郑州 450001)

摘 要:目录服务以其支持分布式环境、安全可靠、灵活方便等优势正从提供用户信息查找、黄页服务等走向网络管理的舞台,并逐渐成为下一代智能化网络管理的核心部分。轻型目录访问协议(LDAP)能够使用一种类似于 X.500 协议中数据的组织方式来访问目录中的信息,并且它得到了 IBM, Tivoli, Novell, Sun, Microsoft 等许多厂商的支持。由于 LDAP 在已有系统中其适应性和兼容性等方面的优势,使得它越来越受到人们的关注。

关键词:轻型目录访问协议;目录服务标记语言;可扩展标记语言

中图分类号:TP393.07

文献标识码:A

文章编号:1673-629X(2006)10-0042-03

LDAP's Framework and Its Practices

MENG Fan-zi, XIE Qi

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: The directory service which supports distributed environment is rather secure, flexible and convenient. Now, with those merits, from just providing the customer information searching and yellow page service, the directory service becomes the stage of the network management and gradually turns into the core part of the next generation intelligent network management. The lightweight directory access protocol provides access to directory information using a data structure similar to that of the X.500 protocol, and it wins the support from IBM, Tivoli, Novell, Sun, Microsoft, and many other vendors. Now due to its flexibility and its compatibility with existing applications, LDAP is more and more popular.

Key words: LDAP; directory service markup language; XML

0 引言

在网络发展日益复杂的今天,如何对网络进行高效智能化管理是当前的一个研究和开发热点。目录服务以其支持分布式环境、安全可靠、灵活方便等优势正从提供用户信息查找、黄页服务等走向网络管理的舞台,并逐渐成为下一代智能化网络管理的核心部分。采用目录服务进行网络管理已成为网络发展的一种必然趋势。

在各种不同的框架及应用中,使用目录服务可以非常方便地访问其组织内的各种信息。轻型目录访问协议(Lightweight Directory Access Protocol, LDAP)^[1]能够使用一种类似于 X.500 协议中数据的组织方式来访问目录中的信息。通常 LDAP 作为一个集中的地址簿使用,提供快速的查询服务。简单地说,LDAP 是一种只需较少资源即可实现目录信息存取的方式,它能够实现安全高速的大用户身份认证。

由于 LDAP 有着很强的适应性以及它把日益增长的数据检索和应用程序的管理两项功能结合到了一块等方面的优势,使得它得到了 IBM, Tivoli, Novell, Sun, Oracle,

Microsoft 等软件厂商的支持,并且都设计并开发了相关的产品。下文将对它们的特性做一简单比较。

1 LDAP 概述

目前,市场上有大量基于 LDAP 的服务器存在,范围从巨型公共服务器比如 BigFoot 和 Infospace 到基于工作组的小型 LDAP 服务器不等。这两种服务器也已被许多大学和企业所采用,用来为他们的研究机构、员工以及学生提供邮件服务、认证服务和资源的访问控制等等。

表 1 展现了一些使用 LDAP 的最为常用的 Web 服务,把 LDAP 集成到已存在的关系数据应用中并总结出其得到的功能,比如:Web 服务、文件传输、视频会议等。

表 1 集成 LDAP 到基于 Web 的服务

基于 Web 服务	集成了 LDAP 的协议及 APIs	LDAP 所提供的功能
Web 服务	安全套接字层, Apache mod plug-ins	提供用户鉴别机制;定义约束机制和访问控制列表
视频会议	H.323, H.320, 会议初始化协议	为用户声音、视频以及其他多媒体信息提供中央存储
Web 数据库	MySQL, PostgreSQL, Oracle 9i, IBM DB2 等等	提供对各种数据库管理系统的访问
文件传输	FTP, WebDAV	定义用户分配的最大空间以及文件的所有性问题;为储存文件定义主目录及服务器提供用户认证服务
应用环境	Java, XML, C/C++, ASP, Perl, Python, PHP, 公共网管接口	支持多种编程语言

收稿日期:2006-01-04

作者简介:孟凡滋(1981-),男,河南郑州人,硕士研究生,主要研究方向为计算机网络应用技术;谢 琦,副教授,从事分布式信息系统、高效率配电网地理信息平台的研究。

2 LDAP 目录服务的框架

LDAP 是基于客户机/服务器模式的运行于 TCP/IP 上的应用层协议,一个或多个 LDAP 服务器组成了 LDAP 目录树^[2,3]。LDAP 客户机与一个 LDAP 服务器连接,并向它发出操作请求,负责在目录上执行必要的操作。一旦服务器完成了这些操作,便向发出请求的客户机返回结果或错误应答,或通过引用 Referral(一种重定向机制,允许将目录服务扩展到最大范围)指向另一个 LDAP 服务器使客户得到服务。不论客户与哪一个 LDAP 服务器连接,它看到的目录视图是一样的。

LDAP 客户端或者直接被 LDAP 服务器所控制,或者被集成了 LDAP 的应用程序所管理。图 1 展现了 LDAP 总的框架,并且显示了各类设备和服务器如何访问存储在给定 LDAP 服务目录中的数据。

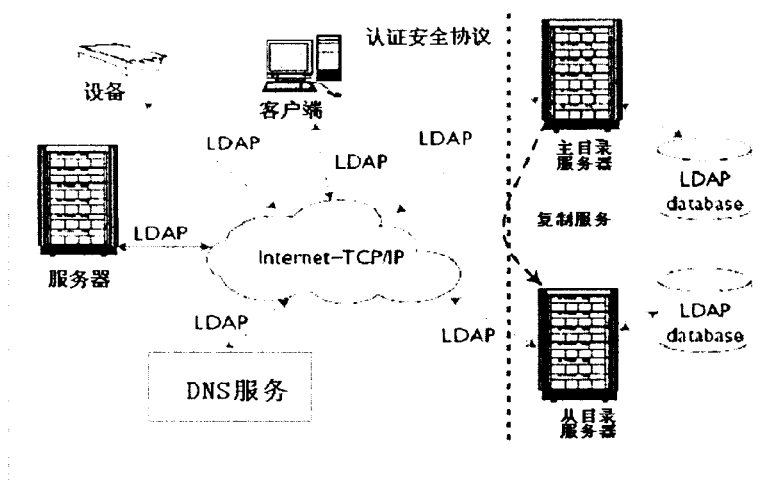


图 1 LDAP 框架

通过使用 LDAP 协议相关设备和服务器可访问存储在 LDAP 目录服务中的数据,在 LDAP 框架中,目录(提供数据存储的地方,也即数据库)和基于 XML 的数据表示是两个至关重要的组件。

2.1 LDAP 目录

LDAP 目录^[4]中的信息按照树型结构进行组织,目录由条目组成,条目是具有区别名(DN, Distinguished Name)的属性集合, DN 相当于关系数据库表中的关键字;属性由类型和一个或多个值组成。图 2 中给出了一个 LDAP 目录树结构示例。LDAP 目录条目一般按照地理位置和组织关系进行划分,非常直观。LDAP 把数据存放在文件中,为提高效率可以使用基于索引的文件数据库。LDAP 条目对象类定义由 5 部分构成:对象标识(OID)、类名称、父对象、必有属性、可选属性。

与平面关系型数据库相比,LDAP 目录服务的优势在于:其树状结构的条目式存储方式、快速的数据检索能力、安全的认证机制等。

(1) LDAP 基于条目的树状结构存储适合用于存储网络管理系统中的半结构化信息,这样的信息包括:网络拓扑结构信息;配置管理信息;性能监测公式定义信息等。

等。

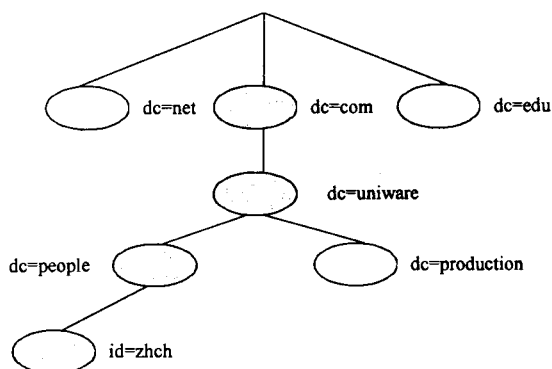


图 2 一个 LDAP 目录树结构示例

(2)由于 LDAP 的分布式存储、安全访问等因素,对于分布式数据网络管理系统来说,选择 LDAP 作为数据存储方式,能够很方便地实现数据的检索,提供安全可靠的数据交换。

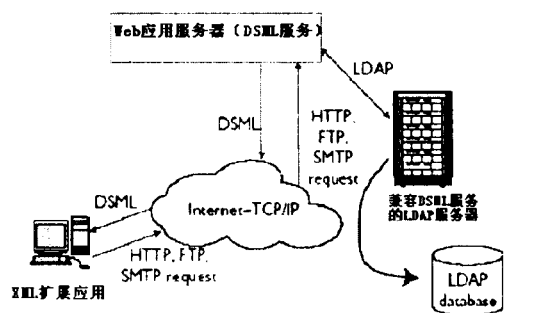
(3)因为 LDAP 模型与 IETF 的策略模型结构的相似性,所以,LDAP 也可以用来存储网络管理策略。这方面的详细情况可以参照 IETF 相关 RFC 文档。

2.2 XML 和 LDAP 的协调发展

XML 是一种简单、与平台无关并被广泛采用的 Web 数据表示标准。由于它被广泛采用并集成到许多基于 Web 的应用中,目录服务也逐渐开发出基于 XML 的相关技术,而且这两种技术在结构上惊人的相似。

目录服务标记语言(Directory Services Markup Language, DSML)是为了使用 XML 来表示目录信息而新提出的一种标记语言。在实际的应用中,它用来在目录服务和含 XML 的应用中起桥梁的作用。在使用 XML 的应用中,通过发送一个请求到含有 DSML 服务的 Web 服务器上,可以取得以 DSML 表示的目录信息。DSML 由一个文档所定义,该文档指定了 DSML 的规则以及约束等内容。

图 3 显示了一个典型的利用 DSML 服务来将 LDAP 条目转换成 DSML 描述的一个事务处理。



将 LDAP 条目转换成 DSML 条目。将目录和 XML 联系起来会影响到数据存储和数据索引。为了能在基于 LDAP 技术的基础上进行有效的 XML 数据的存储和索引,已经存在许多的行之有效的方法^[5,6]。比如:一些受计划驱动的方法,涉及到将 XML 文档对象的模型结点映射到 LDAP 条目上。另外一个方法是为 XML 结点定义一个 LDAP 对象类从而将 XML DOM 结点映射为 LDAP 条目。

3 LDAP 的实现

开发者对于目录的工业标准已经有个清晰明确的认识,并且也已经被大量的应用所进一步采纳,这些应用工作在目录服务网络(Directory Enabled Network, DEN)框架中,该框架包括网络管理应用、系统配置文件、IP 电话等等。

所制定的 DEN 规格致力于建立一个稳定的可扩展的基础下部组织,从而使得不同的网络元素和服务能够从基于 LDAP 的目录和数据存储中通过简单的途径存储和索引数据。基本的 DEN 组件包括 DEN 转换器(<http://carol.science.uva.nl/handree/DEN/D1/index-en.html>)和为了实现多媒体会议的目录服务中间件。

3.1 比较分析主流厂商所开发的目录服务产品的特性

目前许多公司都致力于开发支持 LDAP 的目录服务产品,它们开发出了具有多元化集成能力的成熟有效的基于 LDAP 的实现技术。与这些商业目录服务器软件相比,一系列的开源目录服务软件比如 OpenLDAP 其实也是很有竞争力的。

表 2 列举了目前主流 LDAP 服务器的主要特性,这些主流 LDAP 服务器在平台支持、认证和加密协议以及 DEN 框架上具有很强的相似性。

在这 6 个主要的服务器中,除了 OpenLDAP 提供了对多主源服务器的复制功能外,其它的都没有提供。OpenLDAP 也是唯一的不提供简单网络管理协议监管的主服务器,它通过相关的代理或组件提供有关目录服务器地位及状态等的网络应用信息。

在许多特定的 LDAP 领域集成了 DSML,从这里可以看出 XML 已被目录服务所广泛采用。

Novell 声称它支持 DSML 并且能够实现 DirXML 技术(www.novell.com/products/dirxml)。DirXML 能够提供一种与目录树据进行交互的方式而且可使用 XML 接口来表示数据及改变事件。从本质上来说,通过使用 XML,DirXML 允许 eDirectory 发布有价值的目录数据到其他应用中去。

在 IBM 中典型的 LDAP HTTP API(Slaphapi)通过访问 LDAP 目录能够以纯文本,HTML 或者 DSML 的形式返回输出结果集。IBM 也开发出了一种 XML 数据传递器,这种工具能够在 XML 和结构化数据间(比如关系数据或 LDAP 数据)提供双向数据转换。

与大多数 LDAP 目录所使用的网关不同,Sun ONE 目录服务器提供了对 DSML 本身的支持。通过在 HTTP/SOAP 层面上使用 DSML,Sun ONE 可以使应用脱离对 LDAP 的依赖,从而非 LDAP 客户端也可以与 LDAP 目录交互目录树据。

Microsoft 为活动目录(Active Directory)提供了对 DSML 的支持。它工作在将目录数据映射到 DOM 结构这种机制上。

LDAP 处理器(<http://cococon.apache.org/1.x/ldap.html>)是一种“茧”式处理器,它可以执行 LDAP 查询尔后将结果集解释为 XML 片断,最后将 XML 片断插入到原始文档中。

XMLDAP(<http://xml.coverpages.org/ni2001-03-02-a.html>)允许开发者以多种格式来表示 LDAP 目录数据。

这些支持 LDAP 协议的目录服务器给潜在的 LDAP 客户提供了许多选择。然而在选择某个目录服务器时,阐明使用哪个标准是至关重要的。

3.2 如何选择一个 LDAP 服务器

通过各种不同的实验来比较 LDAP 服务器的性能,用以提供给潜在的客一系列重要的选择标准。

时间需求:典型的 LDAP 服务器执行时间的基准是读数据、查找、写数据以及载入操作。为了增加结果的可信度,通常在实验中都不止对一个数据库进行访问^[7]。

查找功能:这一标准包括查找请求和出错率,查找回复时间和当前查找结果集。查找回复时间依赖于一些因

表 2 主流 LDAP 服务器的特性

特性	OpenLDAP	Sun ONE	Novell	IBM	Oracle	Active Directory
平台	Linux, Windows NT, AIX, BSD, Solaris	Solaris, Linux, IBM AIX, HP-UX, Windows	Linux, Windows, Solaris, AIX, NetWare/HP-UX	Linux, Windows, AIX, Solaris, HP-UX	Unix/Linux, Windows, AIX, Solaris, HP-UX	Windows
安全认证协议	Kerberos, SSL/TLS, Cleartext	SASL, SSL/TLS, X.509 v3	Kerberos, Smartcards, PKI/X.509, SSL	Kerberos, SHA/MID5 Passwd, PKI	SSL/TLS, SASL, certificate	Kerberos, SSL, Smart cards, PKI/X.509
支持数据库	Postgress, SQL, Shell, passwd	Sybase, Berkeley DB	Flaim	IBM DB2	Oracle	MS SQL
多主源复制		◎	◎	◎	◎	◎
DSML 支持	◎	◎	◎	◎	◎	◎
支持目录网络	◎	◎	◎	◎	◎	◎

取带宽优先原则,使得系统具有良好的扩展性和灵活性。服务器由于只处理部分节点视频流信息和控制信息,大大减轻了计算压力和带宽压力,特别是对于点播高峰时间,能够满足更多用户需求,而且实现起来变得容易。

●延迟性:系统的延迟性是个困难问题。节点的离开和加入会带来延迟,数据流层次转发也产生延迟。这里采取限制树高度的办法,假设一棵树节点总数为 N ,平均每个节点带 k 个节点,则 $\log_k N$ 代表树的高度,要求 $\log_k N$ 最小,则可以减少树的过多层次,从而可以减少系统延迟。

5 结束语

设计和讨论了基于 P2P 的流媒体系统模型和关键算法的思想,并对系统的性能做了简要分析。本模型在现有技术条件下,可以方便实现,减轻了服务器和 Internet 骨干网的压力。进一步工作将着手开发原型系统,并检测系统的实际性能。

参考文献:

- [1] Xiang Z, Zhang Q, Zhu W, et al. Peer-to-peer based multimedia distribution service[J]. IEEE Transactions on Multimedia, 2004, 6(4): 343-355.
- [2] Hua K, Cai Y, Sheu S. Patching: A multicast technique for true video-on-demand services[A]. in Proc ACM Multimedia[C]. NY, USA: ACM, 1998.

- [3] Guo Y, Gao L, Towsley D, et al. Seamless workload adaptive broadcast [A]. in Proc of International Packet video Workshop[C]. Pittsburgh, USA: [s. n.], 2002.
- [4] Eager D, Vernon M, Zahorjan J. Bandwidth skimming: A technique for cost-effective video-on-demand[A]. in Proc Multimedia Computing and Networking 2000[C]. San Jose, CA: [s. n.], 2000. 1-10.
- [5] Rejaie R, Handley M, Yu H, et al. Proxy caching mechanism for multimedia playback streams in the internet[A]. In: Proceedings of the 4th International Web Caching Workshop[C]. San Diego, CA: [s. n.], 1999.
- [6] Gadde S, Chase J, Rabinovich M. Web caching and content distribution: a view from the interior[A]. In: Proc. of the 5th international web caching and content delivery workshop[C]. Lisbon, Portugal: [s. n.], 2000.
- [7] 方 炜, 吴明晖, 应 晶. 基于 P2P 的流媒体应用及其关键算法研究[J]. 计算机应用与软件, 2005, 22(5): 35-37.
- [8] Guo Yang, Suh K, Kurose J, et al. P2Cast: peer-to-peer patching scheme for VoD service[A]. Proceedings of the 12th international conference on World Wide Web[C]. NY, USA: ACM, 2003.
- [9] Hefeeda M, Habib A, Botev B, et al. PROMISE: peer-to-peer media streaming using CollectCast[A]. Proceedings of the eleventh ACM international conference on Multimedia[C]. NY, USA: ACM, 2003.

(上接第 44 页)

素,包括:询问过滤器;从哪里开始数据的查找;询问请求属性的个数等等。

缓存管理:因为目录服务器使用目录缓存以改善响应时间,所以度量缓存性能是很重要的。研究人员已经了解了与 LDAP 相关的缓存技术,而且为了提升其性能还提出了改进的算法^[8]。

上文综述了 LDAP 服务器实现技术的不同,比如对于 LDAPv3 的支持,访问控制列表的访问,多主源服务器的复制,但是通过软件开发商以及公共机构的努力,这些不同点都是可以利用的。

4 LDAP 的发展趋势

到目前为止 LDAP 已经发展到第 3 个版本,人们期望它能够与 X.500 目录服务进行更好的交互,从而为全球的目录网络提供更加便利的结构。

凭借着将 XML 技术和 LDAP 技术集成起来,LDAP 在数据管理方面的能力有了很大的提高,尤其在数据存储和数据索引方面。上文所提到的方法也已经在 OpenLDAP 服务器上用来实现 XMLDAP 的相关缓存,而且与传统的缓存技术相比,此种方法在平均访问时间上有了很大的改进。

当前 LDAP 在 Internet 上被广泛应用于数据的管理

工作,其涉及的领域有数据查询、索引、缓存以及安全性等。据此可以预测在将来 LDAP 必将会有更大的用武之地。

参考文献:

- [1] Wahl M, Howes T, Kille S. Lightweight Directory Access Protocol (v3)[S]. IETF RFC 2251, 1997.
- [2] 于 剑, 张 辉, 赵红梅. LDAP 目录服务在 Web 开发中的应用[J]. 计算机应用, 2003, 23(10): 82-83.
- [3] 张慧宇, 袁卫忠. LDAP 研究及其在 CA 中的应用[J]. 计算机应用研究, 2002(10): 37-38.
- [4] 赵宏建, 孙吉贵. 目录服务技术的分析比较及在 PKI 中的实现[J]. 吉林大学自然科学学报, 2001(4): 29-30.
- [5] XLNT Software. Handling XML Documents Using Traditional Databases[EB/OL]. www.surfnet.nl/innovatie/surfworks/xml/xml-databases.pdf. 2002-08.
- [6] Marron P J, Lausen G. On Processing XML in LDAP[A]. Proc 27th Int'l Conf Very Large Databases[C]. [s. l.]: ACM Press, 2001. 601-610.
- [7] Isode. Comparative Performance Benchmarking of Isode Mvaul R10. 1, white paper [EB/OL]. www.isode.com/whitepapers/m-vault-benchmarking.htm. 2003-10.
- [8] Cluet S, Kapitskaia O, Srivastava D. Using LDAP Directory Caches [A]. Proc Symp Principles of Database Systems (PODS)[C]. [s. l.]: ACM Press, 1999. 273-284.