科技部科技基础性工作专项资金重大项目
研究成果

项目名称：我国数字图书馆标准规范建设

子项目名称：数字资源检索与应用标准规范研究

项目编号：2002DEA20018

研究成果类型：研究报告

成果名称：LDAP 协议应用指南

成果编号：CDLS-S07-002

成果版本：总项目组推荐稿

成果提交日期：2003 年 2 月

撰写人：张智雄（中国科学院文献情报中心）

项目版权声明

本报告研究工作属于科技部科技基础性工作专项资金重大项目《我国数字图书馆标准规范建设》的一部分，得到科技部科技基础性工作专项资金资助，项目编号为 2002DEA20018。按照有关规定，国家和《我国数字图书馆标准规范建设》课题组拥有本报告的版权，依照《中华人民共和国著作权法》享有著作权。

本报告可以复制、转载、或在电子信息系统上做镜像，但在复制、转载或镜像时须注明真实作者和完整出处，并在明显地方标明“科技部科技基础性工作专项资金重大项目《我国数字图书馆标准规范建设》资助”的字样。

报告版权人不承担用户在使用本作品内容时可能造成的任何实际或预计的损失。

作者声明

本报告作者谨保证本作品中出现的文字、图片、声音、剪辑和文后参考文献等内容的真实性和可靠性，愿按照《中华人民共和国著作权法》，承担本作品发布过程中的责任和义务。科技部有关管理机构对于本作品内容所引发的版权、署名权的异议、纠纷不承担任何责任。

《我国数字图书馆标准规范建设》课题组网站（http://cdls.nstl.gov.cn）作为本报告的第一发表单位，并可向其他媒体推荐此作品。在不发生重复授权的前提下，报告撰写人保留将经过修改的项目成果向正式学术媒体直接投稿的权利。

LDAP 协议应用指南

目　录

1. 协议概述

LDAP（Lightweight Directory Access Protocol，轻量级目录存取协议）是目前广泛应用的目录协议。

在计算机中，目录被认为是一种特殊的数据库，也有人将其称为数据仓库(Data Repository)，它被用于存储一定类型的经过整序的信息。例如，对于有关打印机（对象）的目录，它可能包括一定类型的信息，如打印机的产商，生产地，每分钟的打印页数等信息。

在现实中，White Pages 和 Yellow Page 常被用以描述目录是如何应用的。使用人员可以通过公司名或其它信息来获取公司的更多信息。在计算机中，目录可以提供更多的查询款目以供内容检索。

LDAP 的第一个版本定义在 X.500 Lightweight Access Protocol (RFC 1487)协议中，后来被 Lightweight Directory Access Protocol(RFC 1777)所取代。当前 LDAP 的版本为 3，其核心协议有： Lightweight Directory Access Protocol （v3）(RFC 2251)和 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions（RFC 2252）。

LDAP 定义了在 LDAP 客户和 LDAP 服务器之间进行内容交换的消息模式。这一消息模式定义了客户机所需要的操作（如查询、修改、删除等），服务器所做出的反应，以及这些消息的内容格式。LDAP 消息通过 TCP/IP 协议传输，因此它还包括了在客户机和服务器之间建立连接和关闭连接的机制。

LDAP 目录存储和组织的基本数据结构被称为款目，每个款目有一至多个描述它的属性。每一款目有一个唯一识别（DN）来标识款目。款目依据 DN 被安排进一个类似树的等级结构中，这棵目录款目树被称为目录信息树。通过目录信息树，可以方便地将款目信息分布在不同的服务器上。LDAP 第 3 版提供了参照（referral）功能，当用户查询某个 LDAP 服务器时，如果所需的信息不在此服务器上，则可通过参照链接，将查询指引到可能包含有相应信息的服务器上。

2. LDAP 的特点和应用领域

LDAP 目录经常被描述为一种特殊的数据库，然而这种特殊的数据库与我们通常所讲的关系数据库之间有较大的差别。主要体现在以下几个方面：

- LDAP 目录经常被用以进行读操作（如查询），而不常进行写操作（修改）。由于 LDAP 目录经常需要被大量地查询，因此，这类型的存储方式经常被进行了读取方面的优化。
- LDAP 目录通常不支持事务处理。因此它不适合于存取哪些需要严格数据一致性的信息。

- LDAP 目录和通常意义上的数据库在数据的存取方式上有差别。对于关系数据库系统，可以通过 SQL 语言进行访问，而对于 LDAP 目录，则可以利用更加简单和优化的方式进行存取。
- LDAP 目录提供了一种经济的方式实现大型分布式环境下的数据存取，比数据库管理系统更容易实现互操作。

LDAP 目录服务的功能主要在于提供分布式存取服务，在这种情况下，目录服务的三维组成（信息内容，客户机的位置，服务器的分布情况）都是相互无关的。在企业范围内实现 LDAP 可以让运行在几乎所有计算机平台上的所有的应用程序从 LDAP 目录中获取信息。LDAP 目录中可以存储各种类型的数据：电子邮件地址、邮件路由信息、人力资源数据、公用密匙、联系人列表等等。通过把 LDAP 目录作为系统集成中的一个重要环节，可以简化员工在企业内部查询信息的步骤，甚至连主要的数据源都可以放在任何地方。

3. LDAP 目录的优势

LDAP 目录的优势主要体现在：

- 可以在任何计算机平台上，用很容易获得的而且数目不断增加的 LDAP 的客户端程序访问 LDAP 目录。而且也很容易定制应用程序为它加上 LDAP 的支持。
- LDAP 协议是跨平台的和标准的协议，因此应用程序就不用为 LDAP 目录放在什么样的服务器上操心了。实际上，LDAP 得到了业界的广泛认可，因为它是 Internet 的标准。产商都很愿意在产品中加入对 LDAP 的支持，因为他们根本不用考虑另一端（客户端或服务端）是怎么样的。LDAP 服务器可以是任何一个开发源代码或商用的 LDAP 目录服务器（或者还可能是具有 LDAP 界面的关系型数据库），因为可以用同样的协议、客户端连接软件包和查询命令与 LDAP 服务器进行交互。与 LDAP 不同的是，如果软件产商想在软件产品中集成对 DBMS 的支持，那么通常都要对每一个数据库服务器单独定制。
- 不象很多商用的关系型数据库，你不必为 LDAP 的每一个客户端连接或许可协议付费。
- 大多数的 LDAP 服务器安装起来很简单，也容易维护和优化。
- LDAP 服务器可以用“推”或“拉”的方法复制部分或全部数据，例如：可以把数据“推”到远程的办公室，以增加数据的安全性。复制技术是内置在 LDAP 服务器中的而且很容易配置。如果要在 DBMS 中使用相同的复制功能，数据库产商就会要你支付额外的费用，而且也很难管理。
- LDAP 允许你根据需要使用 ACL(访问控制列表）控制对数据读和写的权

限。例如，设备管理员可以有权改变员工的工作地点和办公室号码，但是不允许改变记录中其它的域。ACI 可以根据谁访问数据、访问什么数据、数据存在什么地方以及其它对数据进行访问控制。因为这些都是由 LDAP 目录服务器完成的，所以不用担心在客户端的应用程序上是否要进行安全检查。

- LDAP 对于这样存储这样的信息最为有用，也就是数据需要从不同的地点读取，但是不需要经常更新。例如，这些信息存储在 LDAP 目录中是十分有效的：公司员工的电话号码簿和组织结构图、客户的联系信息、计算机管理需要的信息，包括 NIS 映射、email 假名、软件包的配置信息、公用证书和安全密匙
- LDAP 独立于厂商和平台的协议，这意味着容易实现互联，这也意味着很容易将 LDAP 协议转换为其它的协议/系统。当前，存在着多种 LDAP 与其它系统的网关，如 LDAP — X.500，HTTP — LDAP，WHOIS++ — LDAP，FINGER — LDAP，E-mail — LDAP，ODBC — LDAP 等。