浅谈LDAP协议体系与结构

李 婕
（四川美术学院网络工作部 重庆 401331）

[摘 要] LDAP以其开放性、可扩展性、易于开发等优势成为当前目录服务的标准协议。本文探讨LDAP的基本概念、基本协议模型、信息模型、命名模型、功能模型和安全模型体系及结构，对其在用户身份认证管理中的实际应用具有指导意义。

[关键词] LDAP；目录服务

1.LDAP基本介绍

1.1 LDAP的基本概念

LDAP即轻量目录访问协议，是一项快速增长的对通用目录信息进行存取的技术。它运行在TCP/IP之上，可被用来提供独立的目录服务，是目录服务的前端访问协议，简化了X.500的许多操作，省去使用频率极少的那些特征，用一些操作仿真其他操作，使用简单的串编码大多数属性，使之成为低开销访问X.500目录的方法，适用于任何平台，便于实现互联网全球性目录服务[3]。

LDAP协议访问模式为LDAP客户端向服务器端发送请求，服务器发回相应的应答信息，其请求、应答信息的格式和约定遵照LDAP协议规定。

1.2 LDAP的优点

①LDAP是一个开放的标准，独立于计算机厂商、硬件和操作系统平台，并且为绝大多数厂商所支持；

②LDAP具备定义完善的API（Application Programming Interface 应用编程接口），使用目录服务的应用程序可以通过API方便的访问所需要的目录信息；

③LDAP具备扩展特性，需要特殊类型数据的应用程序可以通过扩展LDAP来满足自己的需求；④LDAP消耗很少的系统资源实现目录服务功能，使得LDAP特别适合在互联网上的使用；⑤LDAP具有良好的可靠性及安全性；⑥LDAP已经被大多数的面向网络的中间件所包含和实现，绝大多数网络操作系统及网络应用程序都支持LDAP。如同HTTP、FTP一样，LDAP最终将成为互联网上的标准的独立协议群。

1.3 LDAP的应用范围

由于LDAP具有查询效率高、树状的信息管理模式、分布式的部署框架以及灵活的访问控制，使LDAP广泛的应用于基础性、关键性信息的管理，如网络资源信息等。

①网络资源定位：这是目录服务最广泛的应用之一，LDAP作为 “网络资源访问数据库”，可以组织和索引网络信息。

②网络管理应用：LDAP可以把应用程序私有目录中的用户信息统一管理在可被应用程序访问的简单目录中。目录数据库中的信息还可以被不同的应用程序所访问，可以消除不同私有目录间信息交换和同步的负责操作。

③信息安全应用：LDAP在网络安全方面具有非常重要的作用。首先，LDAP目录服务可以作为安全认证数据库，其次当用户的身份被识别后，它可以控制用户对网络资源、应用程序以及其他网络服务的访问。

2.LDAP的四种体系结构的分析

在LDAP基本协议模型的基础上，LDAP定义了信息模型、命名模型、功能模型和安全模型四种基本目录服务模型。通过这些协议，LDAP可提供不同私有目录之间的相互操作，引导用户使用目录服务，同时简化、规范了目录服务、目录服务器、访问目录服务客户端软件的设计。目录信息的范围、目录客户端的分布和目录服务器的分布也体现在这些基本模型中。

2.1 LDAP基本协议模型

LDAP基本协议模型遵循客户机/服务器模式，由用户客户（LDAP client）提交符合LDAP协议的目录服务请求，目录服务（LDAP server）在接收到服务请求后，经过协议分析及数据处理，向用户客户（LDAP client）应答信息或报错。

2.2 LDAP信息模型

LDAP信息模型描述条目，条目是目录的基本信息单元。条目由属性组成，属性由一个属性类型和一个或多个属性值组成。属性的约束用来限制属性值的类型及长度。目录模式（schema）规定了一个属性是必须属性还是可选属性。

2.3 LDAP命名模型

LDAP的命名模型也就是LDAP中的条目定位方式，描述LDAP中的数据如何组织。在LDAP中每个条目均有自己的DN（distinguish name）和RDN（relative distinguish name）。DN是该条目在整个树中的唯一名称标识，标识由目录名和该目录根部的路径所组成；RDN是该条目在本层子目录中的唯一名称标识，它是DN的一个子集。如同文件系统中，带路径的文件名是DN，文件名是RDN。

2.4 LDAP功能模型

LDAP功能模型描述LDAP中数据操作访问方式。操作大致分为三类。查询类操作允许用户搜索目录并取回目录数据；更新类操作允许用户对目录条目进行添加、删除和修改；认证、控制类操作运行用户想目录证明自己的身份，并进行会话控制。

2.5 LDAP安全模式

LDAP中安全模式主要通过身份认证、通讯安全和访问控制来实现。

①身份认证

认证被用来在客户端和服务器端之间建立会话。在LDAP中提供三种认证机制，即匿名、基本认证和SASL认证。匿名认证即不对用户进行认证；基本认证通过用户名和密码进行身份认证，又分为简单密码和摘要密码；SASL认证即LDAP提供的在SSL和TLS安全通道基础上进行的认证，包括数字证书的认证。

②通讯安全

使用数据加密手段防止对目录信息的非法窃听，使用TLS来建立加密的LDAP会话。在LDAP中提供基于SSL/TLS的通讯安全保障。SSL/TLS是基于PKI信息安全技术的，是目前互联网上最广泛采用的安全服务。LDAP通过StartTls方式启动TLS服务，可提供通讯中的数据保密性、完整性保护；通过强制客户端证书认证的TLS服务，同时可以实现对客户端身份和服务器端身份的双向验证。

③访问控制

目前LDAP中无访问控制的标准，但LDAP访问控制非常灵活和丰富。在LDAP中是基于访问控制策略语句来实现访问控制的，不同于关系型数据库系统和应用系统。

3.小结

LDAP作为一种目录信息的访问协议，提供了简易、高效、可定制的目录服务。因其高效的查询速度，广泛的应用于用户身份认证管理、电子商务资源管理、数字证书服务等领域。本文通过对LDAP基本概念、优势、协议模式及LDAP协议四种基本模型：信息模型、命名模型、功能模型和安全模型等的分析和研究为其在用户身份认证管理中的实际应用具有指导意义。