

Netscape Directory SDK for Java Programmer's Guide

网络安全核心技术内幕

网络服务器目录管理 和应用软件开发指南

〔美〕 John Shum 主 编

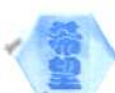


本书配套光盘内容包括：
与本书配套的电子书



北京希望电子出版社

Beijing Hope Electronic Press
www.bhp.com.cn



21世纪网络安全认证技术丛书

00015081

3

TP393.07
06



Netscape Directory SDK for Java Programmer's Guide

网络安全核心技术内幕 网络服务器目录管理 和应用软件开发指南

〔美〕 John Shum 主 编



本书配套光盘内容包括：
与本书配套的电子书



C0491383



北京希望电子出版社

Beijing Hope Electronic Press

www.bhep.com.cn

内 容 简 介

本套丛书由三本书组成,本书是其中的一本。这是一本基于 Java 语言软件工具包如何开发网络服务器目录管理和应用软件的指导书。全书由 17 章构成,主要内容包括:LDAP 协议, Netscape Directory SDK 简介, LDAP 的目录结构,如何编写 Netscape Directory 客户端程序,目录服务器的连接和认证,查询目录信息,使用过滤器和过滤器配置文件以提高查询效率,使用推荐服务器和异常处理,对目录中的条目进行修改等。

LDAP 是一个由密歇根大学开发的目录服务和访问协议。它以 TCP/IP 协议为基础协议,在 Internet 和 Intranet 上即可实现通讯,并且该协议去除了早期 X.500 协议的一些缺点,用简化的 X.500 目录结构和简化的目录访问方法,试图提供不同目录之间,用户、管理员和目录之间交流的标准办法。LDAP 定义了目录信息的访问和存储方法,目录服务器不需要使用 LDAP 结构既可用 LDAP 访问。因此相对于以前的目录访问协议(DAP)而言称为轻便目录访问协议(Lightweight Directory Access Protocol)。

Netscape Directory Server 既用 LDAP 标准的目录结构,也用其标准的访问方法。用户可以用 Netscape Communicator 客户机来访问 Netscape Directory Server。本书介绍的 Netscape Directory SDK for Java 是一个基于 Java 语言的软件开发工具包。它采用 LDAP 协议并定义了一系列的类和方法来实现用户到目录服务器的连接、认证以及查询、修改等各种操作。在此基础上,用户可以很容易地开发自己的目录管理和应用软件。

本书不但是从事网络安全认证系统开发和应用的广大从业人员的重要的开发指导书,同时也是网络安全认证系统网络管理员、网络安全和维护人员的重要参考手册,高等院校相关专业的师生自学、教学用书和各科研院所、科技图书馆的馆藏读物。

本书光盘包含与本书配套的电子图书。

系 列 书: 21 世纪网络安全认证技术丛书(3)

书 名: 网络安全核心技术内幕——网络服务器目录管理和应用软件开发指南

文本著作者: [美] John Shum 主编

责任编辑: 周凤明

CD 制作者: 希望多媒体创作中心

CD 测试者: 希望多媒体测试部

出版、发行者: 北京希望电子出版社

地 址: 北京海淀路 82 号, 100080

网址: www.bhp.com.cn E-mail: lwm@hope.com.cn

电话: 010-62562329, 62541992, 62637101, 62637102

010-62633308, 62633309 (图书发行, 技术支持)

010-62613322-215 (门市) 010-62531267 (编辑部)

经 销: 各地新华书店、软件连锁店

排 版: 希望图书输出中心

CD 生产者: 北京中新联光盘公司

文本印刷者: 北京双青印刷厂

开本 / 规格: 787 毫米×1092 毫米 16 开本 9 印张 197 千字

版次 / 印次: 2000 年 7 月第 1 版 2000 年 7 月第 1 次印刷

印 数: 0001-3000 册

本 版 号: ISBN7-900044-25-6/TP·25

定 价: 30.00 元 (1CD, 含配套书)

说明: 凡我社光盘配套图书若有自然破损、缺页、倒页、脱页, 本社发行部负责调换。

JS93/23

编者的话

在 Internet 和 Intranet 高速发展的今天, 如何管理和利用丰富的网络资源已成为一个很重要的问题。对于公司内部网络 Intranet 而言, 方便、高效的管理更是必不可少的, 否则也就失去了其发展的意义。

目录服务器主要用来管理 Intranet 内部大量的服务器和用户, 实现 Intranet 的基本结构。从根本上来讲, 目录服务器是一个用户信息数据库, 其中存放着用户所在组织、机构的名称以及用户个人信息——包括电话、地址、E-mail 地址等。由于在目录服务器发展的初期, 没有一个统一的标准, 因此存在着多种目录结构和访问标准。这对于 Intranet 的发展是一个很大的障碍。

LDAP 是一个由密歇根大学开发的目录服务和访问协议。它以 TCP/IP 协议为基础协议, 在 Internet 和 Intranet 上即可实现通讯, 并且该协议去除了早期 X.500 协议的一些缺点, 用简化的 X.500 目录结构和简化的目录访问方法, 试图提供不同目录之间, 用户、管理员和目录之间交流的标准办法。LDAP 定义了目录信息的访问和存储方法, 目录服务器不需要使用 LDAP 结构既可用 LDAP 访问。因此相对于以前的目录访问协议(DAP)而言称为轻便目录访问协议 (Lightweight Directory Access Protocol)。

Netscape Directory Server 既用 LDAP 标准的目录结构, 也用其标准的访问方法。用户可以用 Netscape Communicator 客户机来访问 Netscape Directory Server。本书介绍的 Netscape Directory SDK for Java 是一个基于 Java 语言的软件开发工具包。它采用 LDAP 协议并定义了一系列的类和方法来实现用户到目录服务器的连接、认证以及查询、修改的等各种操作。在此基础上, 用户可以很容易的开发自己的目录管理和应用软件。

本书是 Netscape Directory SDK for Java 的一个快速入门和提高教材, 适合于初次接触目录管理的专业人士。对于介绍的每种方法, 书中都提供了实际应用的例子, 利用这些例子, 读者很容易就可以构建自己的程序。下面是本书的一些主要内容:

第 1 章~第 3 章对目录服务器和 LDAP 协议以及 Netscape Directory SDK for Java 进行了简单的介绍。其中涉及到一些重要的基本概念如条目、属性和目录组织结构等。

第 4 章~第 10 章介绍如何用 Netscape Directory SDK for Java 开发客户端程序。这是全书的主体部分, 从连接到服务器开始详细讲述了有关目录的各种操作和相关知识。包括到服务器的认证、异常处理、推荐服务器 (以上为连接到服务器的内容), 查询目录、使用过滤器配置文件、修改条目以及比较条目的值 (以上为目录操作), 最后介绍了如何用 LDAP URL 来实现对目录的查询。

第 11 章~第 17 章针对于高级用户, 主要讲述服务器信息的获取, 安全套接字层(SSL)上的连接, LDAP 控制的使用方法, SASL 认证, JNDI 服务提供者, 以及 LDAP 扩展操作和异步接口的使用。这些方法有助于提高目录管理的安全性和效率。

这里把本书介绍给读者, 希望能对大家的学习和工作有所帮助。另外, 由于知识有限, 时间也比较仓促, 书中难免出现一些错误, 希望广大读者能够批评指正。

本书由 John Shum 博士主编。参加本书编写的有杨小军、刘东红、李漪、胡成松、谭可、杨涛、邵宏刚、冯丹琴、吴环保、朱俊、叶立建、靳江涛、李刚、董毅、肖栓良、宋洁、姜海玲、赵卿等。在本书编写过程中得到杨立明、郑涛等同志的热心帮助, 这里一并表示感谢。

目 录

第一部分 LDAP 和 Netscape Directory SDK for Java 简介

第 1 章 LDAP 简介..... 3	Java 7
1.1 目录服务器的工作方式3	2.1 理解 LDAP 的 Java 类.....7
1.2 LDAP 服务器组织目录的方式4	2.2 Netscape Directory SDK for Java 初步7
1.3 LDAP 客户端和服务器的生活方式5	第 3 章 快速入门 12
1.4 了解 LDAP 协议版本 36	3.1 了解该客户端样本12
1.5 其他内容.....6	3.2 样本代码12
第 2 章 使用 Netscape Directory SDK for	

第二部分 用 Netscape Directory SDK for Java 编写客户端

第 4 章 编写 LDAP 客户端..... 17	6.7 读取一个条目46
4.1 概述: 设计一个 LDAP 客户端17	6.8 列出子条目47
4.2 创建连接并设置优先权18	第 7 章 使用过滤器配置文件 50
4.3 连接到 LDAP 服务器19	7.1 理解过滤器配置文件50
4.4 LDAP 服务器的认证和绑定19	7.2 理解配置文件的语法50
4.5 执行 LDAP 操作21	7.3 理解过滤器参数52
4.6 断开到服务器的连接22	7.4 载入过滤器配置文件52
第 5 章 使用 LDAP Java 类 23	7.5 检索过滤器53
5.1 获取 SDK 相关信息23	7.6 给过滤器添加前缀和后缀55
5.2 异常处理23	第 8 章 添加、更新和删除条目 60
5.3 处理推荐26	8.1 添加新条目60
5.4 使用内存缓冲区28	8.2 修改条目63
5.5 克隆连接31	8.3 删除条目67
5.6 使用分辨名(DN)32	8.4 更改条目的名称68
第 6 章 查询目录 33	第 9 章 比较条目中的值 71
6.1 概述: 用 LDAP Java 类进行查询33	9.1 比较一个属性的值71
6.2 发送查询请求33	第 10 章 使用 LDAP URL 73
6.3 获取查询结果39	10.1 了解 LDAP URL73
6.4 对查询结果进行排序43	10.2 LDAP URL 举例74
6.5 取消查询44	10.3 获取 LDAP URL 的组件75
6.6 示例: 查询目录44	10.4 执行 LDAP URL75

第三部分 高级篇

第 11 章 获取服务器信息	79	14.1 理解 SASL	111
11.1 理解 DSE	79	14.2 准备使用 SASL 认证	111
11.2 获取根 DSE	79	14.3 在客户端使用 SASL	114
11.3 确定服务器是否支持 LDAP 版本 3	81	14.4 有关的更多信息	116
11.4 获取模式信息	83	第 15 章 使用 JNDI Service Provider	117
第 12 章 SSL 层上的连接	89	15.1 JNDI 的运行方式	117
12.1 Netscape Directory SDK for Java 中对 SSL 的操作	89	15.2 安装 Service Provider	117
12.2 在 SSL 层上连接的先决条件	90	15.3 JNDI 的环境属性	119
12.3 在 SSL 上连接到服务器	91	15.4 控制操作	121
12.4 使用基于身份确认的客户端认证	91	第 16 章 使用扩展操作	124
第 13 章 使用 LDAP 控制	92	16.1 扩展操作的执行方式	124
13.1 LDAP 控制的运行方式	92	16.2 在服务器上安装扩展操作的支持软件	124
13.2 使用 LDAP Java 类中的控制	93	16.3 确定支持的扩展操作	125
13.3 确定服务器所支持的控制	93	16.4 执行扩展操作	125
13.4 使用服务器端排序控制	96	16.5 举例：扩展操作	125
13.5 使用持续查询控制	103	第 17 章 使用异步接口	127
13.6 使用条目更改标志控制	107	17.1 同步与异步连接的对比	127
13.7 使用虚拟列表视图控制	108	17.2 异步接口的一般用途	127
13.8 使用管理 DSA IT 控制	108	17.3 异步接口中的新类	128
13.9 使用口令原则控制	109	17.4 执行异步查询	128
13.10 使用代理授权控制	109	17.5 相关信息	131
第 14 章 使用 SASL 认证	111	附录 词汇表	132

第一部分

LDAP 和 Netscape Directory SDK for Java 简介

第1章 LDAP 简介

本章介绍 LDAP 协议及其思想。

第2章 使用 Netscape Directory SDK for Java

本章描述 Lightweight Directory Access Protocol(LDAP) Java 类和 Netscape Directory SDK for Java。

第3章 快速入门

本章介绍了一个用 Netscape Directory SDK for Java 编写的简单的 LDAP 终端的客户。

第 1 章 LDAP 简介

本章介绍 LDAP 协议及其思想。

LDAP(Lightweight Directory Access Protocol, 即轻便目录访问协议)是 Internet 目录协议。这个协议由位于 Ann Arbor 的 Michigan 大学和 Internet Engineering Task Force 联合开发成功, 其目的就是为目录服务器进行访问和管理。

本章由下面几节组成:

- 目录服务器的工作方式
- LDAP 服务器组织目录的方式
- LDAP 客户端和服务器的生活方式
- 了解 LDAP 协议 3.0 版
- 其他内容

如果对 LDAP 已经比较熟悉, 可以直接跳到第 2 章。

1.1 目录服务器的工作方式

目录由包含描述信息的条目(Entry)组成。例如, 可能会包含描述人或打印机、传真机等网络资源的条目。

描述信息保存在条目的属性中。每个属性描述一种特定的信息。例如, 描述人的属性可能包括这个人的姓名(常用名或其他名字)、电话号码以及 Email 地址。

例如, Barbara Jensen 的条目可能包含以下一些属性:

```
cn:Barbara Jensen  
mail:babs@ace.com  
telephoneNumber:555-1212  
roomNumber:3995
```

对应一个属性, 可以有多个值, 例如, 一个属性可能有两个常用名(一个正式名和一个昵称)或者两个电话号码:

```
cn: Barbara Jensen  
cn: Jenny Jensen  
mail: jen@ace.com  
telephoneNumber: 555-1213  
telephoneNumber: 555-2059  
roomNumber: 3996
```

属性也可以包含二进制数据。例如, 一个人的属性可能包括这个人的 JPEG 格式的照片或保存在音频格式文件中的声音。

目录服务器是一个分布式数据库软件, 用来管理目录中的条目和属性。它也使得条目和属性可以被用户或其他应用软件访问。Netscape Directory Server 就是目录服务器的一

个例子。

例如，用户可以使用目录服务器来查找某个人的电话号码；而另一个软件可能用它来得到一个 Email 地址的列表。

LDAP 是定义目录服务以及如何访问这些服务的协议。它基于客户—服务器模式。LDAP 服务器提供目录服务，而 LDAP 客户端使用目录服务来访问条目和属性。

LDAP 服务器的一个例子就是 Netscape Directory Server，它管理并提供用户信息和用户所在的团体和部门等组织结构信息。而 Netscape Directory Server 的 HTTP 网关、Netscape Navigator 以及 Netscape Communicator 等都称为 LDAP 客户。网关使用目录服务器来查找、更新和添加用户信息。

1.2 LDAP 服务器组织目录的方式

由于 LDAP 要提供全球目录服务，因此其数据是以分层结构组织的：从根部向下分支为各个单独的条目。

在分层机构的最顶层，各个条目代表比较大的机构。在这些机构的下面可能是比较小的机构，而最终分层结构可能以单个的人或资源作为条目。

图 1.1 展示了 LDAP 目录服务中各个条目的一个分层结构。

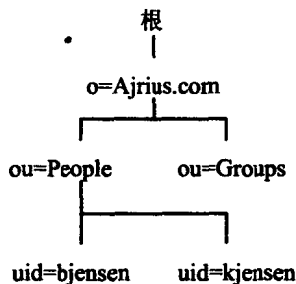


图 1.1 目录中条目的一个分层结构

每一个条目通过一个分辨名（distinguish name）相互区别。这个分辨名包括在这个层次上唯一确定这个条目的名称（例如，bjensen 和 kjensen 是不同的使用者 ID，它们用来区分在同一层次上的不同条目）和一个由名称组成的路径，沿这个路径可以从当前层返回到层级树的根部。

例如，下面是唯一标识 bjensen 这个条目的名字：

uid=bjensen, ou=People, o=Ajrius.com

这里，uid 表示条目的使用者 ID，ou 表示这个条目所在的机构单位，而 o 则表示这个条目所在的更高级机构。

图 1.2 展示了在目录层级机构中，分辨名如何确定每个独特的条目。

目录中保存的数据可以分散到几个 LDAP 服务器中。例如，一个在 Ajrius.com 的 LDAP 服务器可能包含表示 North American 组织单位和雇员的条目，而其它 LDAP 服务器可能包含表示 European 组织单位和雇员的条目。

一些 LDAP 服务器设置为可以把请求推荐到其他 LDAP 服务器。例如，如果在

Airius.com 的 LDAP 服务器上收到一个雇员信息，而这个雇员在 Pacific Rim 分部，此时服务器可以把这个请求转交给 Pacific Rim 分部的 LDAP 服务器。通过这种方法，LDAP 服务器看起来就像是一个单独的目录信息源。即使一个 LDAP 服务器上并没有所需要的信息，它也会为用户查找另一个包含这个信息的服务器。

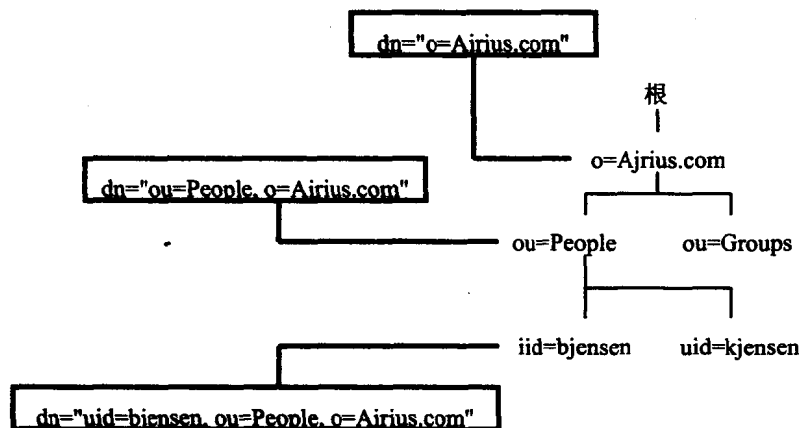


图 1.2 目录中一个分辨名

1.3 LDAP 客户端和服务器的生活方式

在 LDAP 的客户—服务器模型中，LDAP 服务器（如 Netscape Directory Server）使得 LDAP 可以访问关于个人、机构和资源的信息。LDAP 协议定义了客户端用来查找和更新目录的操作。下面列出了 LDAP 客户可以执行的部分操作：

- 在目录中查找并获取条目
- 向目录增加新的条目
- 更新目录中的条目
- 从目录中删除条目
- 给目录中的条目重命名

比如，要更新目录中的一个条目，LDAP 客户可以把这个条目分辨名以及更新的属性信息提交给 LDAP 服务器。LDAP 服务器使用条目的分辨名来找到这个条目并执行一个修改操作，这样就更新了目录中的条目。

要执行这些 LDAP 操作中的任何一个，LDAP 客户端都需要建立与 LDAP 服务器的连接。LDAP 协议指定使用 TCP/IP 的 389 号端口，尽管服务器可能运行在其它端口上。

LDAP 协议还定义了一个简单的鉴别方法。LDAP 服务器可以设置为拒绝对目录的访问。在 LDAP 客户端执行对 LDAP 服务器的操作之前，客户端必须通过向服务器提供一个分辨名和口令来通过鉴别。如果由分辨名识别的用户没有执行某些操作的许可，服务器就不执行这些操作。

1.4 了解 LDAP 协议版本 3

许多 LDAP 服务器支持版本 2 LDAP 协议。这个版本在 RFC 1777 中有详细说明（可以在 <http://www.ietf.org/rfc/rfc1777.txt> 得到这个 RFC 的复件）。

最新提出 LDAP 协议的标准是版本 3，在 RFC 2251 中有详细说明（可以在 <http://www.ietf.org/rfc/rfc2251.txt> 得到这个 RFC 的复件）。一些 LDAP 服务器支持这个更新版本的协议，例如 Netscape Directory Server 3.0 及以后的版本。

Netscape Directory SDK for Java 4.0 支持这两个版本的协议。用这个 SDK 建立的客户端可以和 LDAP 的版本 2、版本 3 服务器进行连接。

LDAP 协议的版本 3 包括以下一些新的特征：

- 可以定义控制来扩展 LDAP 操作的功能（在服务器或客户端都可以）。
- 可以请求服务器执行扩展操作（标准 LDAP 操作之外的操作）。
- 可以使用 Simple Authentication and Security Layer(简单鉴别和安全层次——SASL) 机制来通过鉴别访问目录。
- 服务器具有 DSE (DSA-specific entries——DSA 描述条目，这里 DSA 是一个目录服务器)，它可以提供 LDAP 协议的版本信息，控制列表，扩展操作信息，服务器支持的 SASL 机制的信息，以及服务器的命名环境信息（描述目录树上由该服务器来管理的部分）。
- 服务器提供其概要给客户端（可以从根 DSE 得到一个目录服务器的概要）。
- 客户端和服务器都支持 UTF-8 格式的数据。客户端现在可以请求并得到用语言信息标记的数据。

1.5 其他内容

Netscape Directory Deployment Guide (Netscape Directory Deployment 指南) 的第一章“Welcome to the Directory Server”（目录服务器简介）中对 LDAP 协议和目录服务器进行了更详细的介绍。

第 2 章 使用 Netscape Directory SDK for Java

本章描述了 Lightweight Directory Access Protocol(LDAP)的 Java 类和 Netscape Directory SDK for Java。

下面是本章所包含的几个小节：

- 理解 LDAP 的 Java 类
- Netscape Directory SDK for Java 初步

2.1 理解 LDAP 的 Java 类

Netscape Directory SDK for Java 包括 LDAP Java 类，它可以用来建立 LDAP 客户端。LDAP Java 类允许编写与服务器相联系的 Java 程序和应用软件，并执行标准的 LDAP 操作（例如，可以用这些程序来查找或添加、更新、删除条目）。

这个类由以下一些组件构成：

- `netscape.ldap` 包括了主要的 LDAP Java 类，其中一些类允许用户与 LDAP 服务器相连，对项目 and 属性进行操作，以及获取查询结果。
- `netscape.ldap.beans` 包括 LDAP JavaBeans。可以在一些开发环境中使用这些 Beans，比如 Sun 公司的 Bean Development Kit(BDK)。
- `netscape.ldap.ber.stream` 包括执行 Basic Encoding Rules(基本编码规则——BER)以转换句法的 LDAP Java 类。关于 BER 的内容可以在 <http://www.iso.ch/> 参考 ISO/IEC 8825。
- `netscape.ldap.controls` 包括执行特殊 LDAP 版本 3 控制的 LDAP Java 类。这些控制包括请求服务器端分类和持续搜索。
- `netscape.ldap.util` 包括一些工具类，例如对 LDIF 数据进行分析的类和一些过滤器，这些过滤器允许匹配某些规则的符号。
- `com.netscape.sasl` 包括接口以及用来使客户端在 SASL 机制下进行鉴别的类。
- `com.netscape.jndi` 包括 Netscape 的 LDAP Service Provider 和它所基于的类。这个 JNDI 工具将在第 15 章进行详细介绍。

典型的，客户端同步执行 Netscape Directory SDK for Java 中的程序。所有 LDAP 操作在完成之前拥塞在一起（唯一不同的是查询操作，它可以在得到所有结果之前返回信息）。

同样，在需要与 LDAP 服务器进行低层次交互的环境下也提供异步的接口。在第 17 章中对异步接口有更完整的论述。

下面几章将介绍如何使用这些 LDAP Java 类。

2.2 Netscape Directory SDK for Java 初步

本节涉及到以下主题：

- 获取并安装 SDK
- SDK 简介
- 准备使用 SDK
- 用 SDK 编写 Java 小程序
- 通过一个程序检测类的版本
- 使用 LDAP JavaBeans
- 使用 JavaScript 中的类

2.2.1 获取并安装 SDK

可以从 Netscape 的 DevEdge 网站得到 Netscape Directory SDK for Java, 网址如下:

<http://developer.netscape.com/tech/directory/index.html>

SDK 给 UNIX 环境提供一个以 GNU 格式压缩的档案文件, 而提供给 Windows 的是一个自解压的可执行文件, 在 Macintosh 下是一个 Stuffit 文档。

安装 SDK:

- 下载与所运行系统相匹配的文件
- 扩展这个文件 (其中包括一些子目录)

2.2.2 SDK 简介

Netscape Directory SDK for Java 包括以下目录:

- **beans**

这个目录下有 LDAP JavaBean 的类文件, 这是 `netscape.ldap.beans` 插件的一部分。注意, 这些类在 Netscape Communicator 中并没有包括。因此, 如果要用这些类编写程序或软件, 必须把这些类提供给用户。

这个目录还包括一个 `makejars.bat` 文件和一个 `makejars.sh` 外壳程序。可以用这些来为 LDAP JavaBeans 创建 JAR 文件。

- **examples**

这个目录包括一些 LDAP 软件的 Java 源代码, 这些例子按下面的子目录分类:

- **java** 包括一些添加条目和搜索条目的标准的 LDAP 操作的例子。还包括一些使用 LDAP 控制的例子。
- **java/beans** 包括一些使用 LDAP JavaBeans 的例子。
- **java/ldapfilt** 包括一个通过 LDAP 过滤器类来使用 LDAP 过滤器配置文件的例子 (注意, Netscape Communicator 中不包括 LDAP 过滤器类)。
- **js** 包括一个使用 LiveConnect 来创建并管理 JavaScript 中 LDAP Java 对象的例子 (LiveConnect 是 Netscape 的一种技术, 它可以在一个页面上实现各种元素之间的通信, 包括 JavaScript, HTML, 插件和 Java 小程序)。

- **packages**

这个目录包括下面两个 JAR 文件:

- **ldapjdk.jar**——这个 JAR 文件包括 `netscape.ldap`、`netscape.ldap.controls`、`netscape.ldap.util` 和 `com.netscape.sasl` 等组件中的类。

- `ldapfilt.jar`——这个 JAR 文件包括 `netscape.ldap.util` 和 `com.oroinc.text.regex` 组件中的过滤器类。

`com.oroinc.text.regex` 是 ORO Java Software 中的 OROMatcher™ 规则表达式软件包。因此，如果要单独使用 OROMatcher 组件（不通过 Netscape Directory SDK for Java 类），必须从 ORO Java Software 获得使用 OROMatcher 组件的许可（也可以直接从 ORO 得到 OROMatcher 文档）。

- `tools`

这个目录包括的一些 Java 类与 Netscape Directory Server 4.0 和 Netscape Directory C SDK 中的命令程序相似（注意，这些 Java 工具并不完全支持其它程序所用到的所有命令行参数）。

2.2.3 准备使用 SDK

在编译任何程序或应用软件之前，必须把下面的内容添加到 CLASSPATH 环境变量中：

- `packages/ldapjdk.jar` 文件，这个文件中包括主要的 LDAP Java 类。
- `packages/ldapfilt.jar` 文件，如果要用到任何 LDAP Java 过滤器类，就必须添加这个文件。
- `classes` 目录，如果要用到任何 LDAP JavaBean 类，就需要添加这个目录。

2.2.4 用 SDK 编写 Java 小程序

在 Netscape Communicator 中，程序可以和任何主机上的服务器相连接，当然，其中不包括运行该程序的主机。这个功能是新签定的程序安全框架的一部分。

要利用这个功能，程序类（实现 LDAP 连接的类）必须是已注册的。程序类在与其他服务器连接之前需要获得某些特殊的权利。

本节下面的部分总结了使程序和其它 LDAP 服务器相连接所要采取的步骤。

1. 从所在机构的认证部门（如果所在机构内部发放证明）获得证明，也可以从第三方的认证部门，如 RSA 或 ATT。

用户应该在 Communicator 证书数据库中具有认证部门的证明。

2. 用自己的类创建 JAR 文件并对其进行注册。

可以用 JAR 文件管理工具来实现这一步，这个工具在下面的站点可以找到：

<http://developer.netscape.com/software/signedobj/>

在下面的站点可以找到关于 Netscape Object Signing 技术的附加文件：

<http://developer.netscape.com/docs/manuals/signedobj/>

3. 把下面一行添加到线程的程序代码中需要调用 `LDAPConnection.connect` 的位置。

```
PrivilegeManager.enablePrivilege("Universalconnect");
```

在代码的这个位置，程序的用户会得到一个提示对话框，其中对注册类的作者进行确认并请求得到访问 LDAP 服务器的权利。用户可以只允许这一次的访问，也可以允许永久访问。

如果希望在不使用对象注册和认证的情况下测试程序，使之与其它主机进行连接（除去运行该程序的主机），例如想在等待发放认证的时候对程序进行测试，可以把

Netscape Communicator 设置为忽略这次测试。

首先,退出 Communicator(或确认 Communicator 没有运行)。然后在 prefs.js 文件中添加以下代码:

```
user_pref("signed.applets.codebase_principal_support",true);
```

2.2.5 通过一个程序检测类的版本

Netscape Communicator 4.0 和更新的版本都包括一个 LDAP Java 类的复件。不同的 Communicator 版本具有不同版本的类。

下面的表格列出了到目前为止已经发布的 LDAP Java 类的几个不同版本。

表 2.1 最近发布的几个 LDAP Java 类版本

版本	说明
3.03	和 Netscape Directory SDK for Java 3.0 一起发布
3.1	和 Netscape Directory SDK for Java 3.1 一起发布
4.0	在 http://developer.netscape.com/software/ldap 可以找到

LDAP Java 类的 3.03 版以及更高的版本都包括诸如 LDAPCache 和 LDAPSchemas 等新类。如果要在程序中使用这些类,就必须检测浏览器中所提供的 LDAP Java 类的版本。

要得到版本信息,需要调用 LDAPConnection.getProperty 方法,并传入常量 LDAPConnection.LDAP_PROPERTY_SDK。版本号是一个 Float 类型的数。例如:

```
...
Float sdkVersion=(Float)myconn.getProperty(myConn.LDAP_PROPERTY_SDK);
System.out.println("LDAP Java Classes version:"+sdkVersion);
...
```

如果需要了解当前版本和以前版本中的 LDAP Java 类之间有何不同,可以在下面的站点查看发布说明:

<http://developer.netscape.com/tech/directory/index.html?content=java40relnotes.html>

2.2.6 使用 LDAP JavaBeans

Netscape Directory SDK for Java 包括一组 LDAP JavaBeans,可以在诸如 Sun Microsystems 的 BeanBox 或 Symantec 的 Visual Cafe 设计环境下使用它们。

这些 Bean 是 netscape.ldap.beans 组件的一部分,在 beans 目录下可以找到其类文件。

下面列出了 Netscape Directory SDK for Java 中所包括的 JavaBeans:

- LDAPGetEntries Bean 允许搜索目录并得到一个查找到的 DN 数组。可以用这个 Bean 的这些属性来指定搜索的标准。GetEntries 方法执行搜索并设置 Result 属性为所查找到的 DN 数组。
- LDAPGetProperty Bean 允许在目录中查找一个条目,并获取该条目中一个指定属性的值。可以用这个 Bean 属性来指定搜索的标准。GetProperty 方法执行搜索并设置 Result 属性为一个数组,其中有指定属性的字符串值。
- LDAPIsMember Bean 确定用户是否是一个团体的成员(用户和团体可以用这个 Bean 的属性类确定)。IsMember 方法把 Result 属性设置为字符串“Y”或“N”来指明用户是否是一个成员。

- LDAPSimpleAuth Bean 对 LDAP 服务器进行验证。Authenticate 方法执行验证并把 Result 属性设置为字符串“Y”或“N”来指明验证是否成功。

Netscape.ldap.beans 组件还包括下面一些类:

- LDAPBasePropertySupport 类是派生出其它 Bean 类的基类。其它 Bean 类继承这个类定义的存取程序。
- DisplayString 类派生出 jav.awt.TestArea 类, 它的作用是显示其它一些 Bean 的结果。

在某个开发环境中使用 Bean 之前, 必须确认已经把 CLASSPATH 环境变量设置为包括 LDAP Java 类。例如:

- 如果用 Sun Microsystems BeanBox 工具, 需要确认在 run.bat 文件、make 描述文件、当前处理程序或控制台窗口中, CLASSPATH 环境变量包括 ldapjdk.jar 文件的路径。例如:

```
set CLASSPATH=classes;D:\netscape\ldapjdk\packages\ldapjdk.jar
```

- 如果用 Symantec Visual Cafe 2.x, 需要确认在 VisualCafe\bin\sc.ini 文件中, CLASSPATH 条目包括 ldapjdk.jar 文件的路径。例如:

```
CLASSPATH=.;...<other_paths>;  
D:\NETSCAPE\LDAPJDK\PACKAGES\LDAPJDK.JAR
```

下面, 设置开发环境使之包括 Netscape Directory SDK for Java 的 beans 目录下的 JAR 文件。例如:

- 如果使用 BeanBox 工具, 把 JAR 文件复制到 BDJ/jars 目录下。则当运行 BeanBox 时, 就会自动载入 LDAP JavaBeans。
- 如果使用 Visual Cafe, 选择 View|Component Library 菜单命令, 弹出 Component Library 窗口。在确认当前已经打开一个工程之后, 选择 Insert|Component Into Library 菜单命令并选择一个包括在 LDAP JavaBean 中的 JAR 文件。这样就把该 Bean 加到了自己的组件库。

注意, LDAP JavaBean 是不可见 Bean, 而不是 UI 组件。

这些 Bean 具有 Debug 属性, 如果希望打印调试信息就可以设置这个属性。这样, 调试信息就打印到标准输出中了。因此, 如果在 BeanBox 或程序浏览器测试程序, 调试信息就输出到控制台窗口或外壳程序窗口。

2.2.7 使用 JavaScript 中的类

使用 Netscape Communicator 的 LiveConnect 功能, 可以利用来自于 HTML 页中 JavaScript 代码的 LDAP Java 类 (LiveConnect 使得 JavaScript 和 Java 程序之间的以及 JavaScript 和页面上载入的插件之间可以进行信息传递)。

examples/js 目录下的 HTML 文件中的 JavaScript 例子展示了如何实现这一功能。要更多地了解 LiveConnect, 可以查阅 Netscape JavaScript Guide 和 Tech Note TN-JSCR-03-9707 中的有关章节。这两本书的电子版可以分别在下面两个站点找到:

<http://developer.netscape.com/docs/manuals/js/client/jsguide/index.htm>

http://developer.netscape.com/docs/technote/javascript/liveconnect/liveconnect_rh.html