在 Sun 被 Oracle 收购后，Sun Java 系统目录服务器成为 Oracle 目录服务器企业版（ODSEE）的一部分。

Sun 目录服务支持 LDAP v2 和 LDAP v3 相关 RFC 标准，包括：RFC2079，RFC2246，RFC2247，RFC2307，RFC2713，RFC2788，RFC2798，RFC2831，RFC2849，RFC2891，RFC3045，RFC3062，RFC3296，RFC3829，RFC3866，RFC4370，RFC4422，RFC4505，RFC4511，RFC4512，RFC4513，RFC4514，RFC4515，RFC4516，RFC4517，RFC4519，RFC4522，RFC4524，RFC4532。

Sun 目录服务器支持在以下平台上安装运行：Solaris 9 和 10 操作系统、OpenSolaris、Red Hat Enterprise Linux、SuSE Linux、HP-UX、Windows Server。

6.2.3 Novell eDirectory

Novell 公司的 eDirectory（前身为 Novell 目录服务，有时也称为 NetWare 目录服务）是一个兼容 X.500 的目录服务软件产品，最初发布于 1993 年。eDirectory 是层次化的面向对象的数据库，它用逻辑树的方式表示组织资产，这些资产包括：组织机构、组织单位、人、位置、服务器、卷、工作站、应用程序、打印机、服务和团体。eDirectory 是高度可伸缩的高性能安全目录服务，支持安全套接层（Secure Socket Layer，SSL）上的 LDAP v3 协议，提供复制和分区功能。

eDirectory 中使用权限动态继承机制，支持全局和局部访问控制。目录树中对象访问权限在被访问时确定，每个对象可以依据在目录树中的位置、安全等级、个体赋值等确定访问权限。该软件支持在树中的任何一点上进行分区，以及复制任何分区到任意数量的服务器上。服务器之间周期性地进行增量复制。每个服务器都可以充当主服务，向其他服务器赋值它拥有的信息。此外，可以设置从服务器只接收定义的属性以提高复制速度（例如，可以配置一个从服务器，其只包括公司地址簿上的姓名和电话号码，而不是使用整个目录的用户配置文件）。

eDirectory 支持引用完整性、多主复制、并具有模块化的认证架构。它支持通过 LDAP、DSML、SOAP、ODBC、JDBC、JNDI 和 ADSI 访问。

eDirectory 服务器支持在以下平台上安装运行：Novell NetWare、Solaris、Red Hat Enterprise Linux、SuSE Linux、HP-UX、Windows Server、IBM AIX。

6.2.4 GBase 8d

南大通用目录服务系统是原南开创元目录服务（ITEC-iDS）系统的升级版，其核心产品 GBase 8d 已经广泛应用于我国省级 CA 和部委级 CA 等 PKI/PMI 系统中，以及大型企事业单位的身份标识管理系统中，并在省市级的电子政务建设中得到应用。

GBase 8d 是南大通用目录服务产品线的核心和基础，其主要由 LDAP Server 和 Slurpd（镜像复制）Server 以及相关的管理软件和应用开发套件构成。

GBase 8d 具有以下特性：

① 遵循轻型目录访问协议 LDAP v2 和 v3。

② 支持 Windows 2000/2003、Linux、Solaris、AIX、HP-UX 操作系统。

③ 单服务器管理容量可达千万级条目。

④ 支持 LDIF 格式的导入/导出。

⑤ 支持 RFC 规范定义的分页标准（规范定义的分页标准 RFC2696）。

⑥ 支持匿名、用户名/简单密码、用户名/摘要密码等多种身份认证方式。

⑦ 对于主体的授权，可基于主体的位置特征、主体的属性特征进行策略授权。

⑧ 支持 SSL 和 TLS 实现的安全通道，实现信息传递的私密性保护。

⑨ 支持全库统计条目及子树统计条目。

⑩ 支持 Schema 的扩展，可实现用户自定义 Schema 文件的载入，用户自定义对象类和属性的加入。

⑪ 支持 LDAP 的引用（referral）功能。

⑫ 提供图形化的管理界面，管理员可同时管理多个目录服务器。

⑬ 使用中文作为 DN，支持 UTF-8 和 GB 两套汉字编码体系。

6.2.5　OpenLDAP

OpenLDAP 项目开始于 1998 年，是轻型目录访问协议的开源实现，在 OpenLDAP 许可证下发行，并已经包含在众多流行的 Linux 发行版中。OpenLDAP 可以运行于 BSD 变种操作系统、AIX、Android、HP-UX、Mac OS X、Solaris、Windows 等操作系统。

OpenLDAP 项目在 2007 年 10 月发布了 OpenLDAP 2.4 版本，引入了多主复制、热备主服务、动态删除和修改 Schema 元素等特性。

OpenLDAP 软件包含 3 个主要组件：

① slapd：LDAP 守护进程及相关模块和工具。

② 库：实现 LDAP 协议和 ASN.1 基本编码规则（BER）。

③ 客户端软件：ldapsearch、ldapmodify、ldapmodrdn 及其他。

OpenLDAP 服务器在系统架构上分为前端和后端两个部分，前端负责网络访问和协议处理，后端负责数据存储处理。由于采用模块化技术，OpenLDAP 支持多种后端存储模式，包括数据存储后端、代理后端、动态后端。

① 数据存储后端：进行实际数据存储，如 back-bdb、back-ldif 等。

② 代理后端：充当其他存储系统的网关，如 back-ldap、back-sql 等。

③ 动态后端：动态产生数据如 back-config、back-sock 等。

OpenLDAP 支持使用在 RFC4533 中指定的内容同步复制机制，除了基本规范，也支持称为 delta-syncrepl 的增强功能。其他增强功能已经实现，支持多主复制。欲了解复制的更多信息，请参阅 RFC4533。

6.2.6　Microsoft Active Directory

活动目录（Active Directory）是微软 Windows Server 中负责构建中大型网络环境的集中式目录服务，从 Windows 2000 Server 开始内置于 Windows Server 产品中，它处理了组织中的网络对象（对象可以是用户、组群、计算机、域名控制站、邮件、设置文件、组织单元、树系等），只要是在活动目录 Schema 中定义的对象，就可以存储在活动目录数据文件中，并利用活动目录服务接口（Service Interface）来访问。实际上，许多活动目录的管

理工具都利用这个接口来调用并使用活动目录的数据。

活动目录最早在 1996 年出现，并在 Windows 2000 中首次问世，研发代号为 Cascade，并历经 Windows 2000、Windows Server 2003 的演化，目前活动目录已成为成熟的目录服务组件，在 Windows Server 2008 中，活动目录服务更将其角色扩充至 5 种服务（包含网络目录服务、凭证服务、联邦服务、轻量级服务、权限管理服务等）。

6.3 LDAP 部署与优化

6.3.1 复制介绍

通过把目录中的数据放在多个位置，可以提高目录服务的可靠性。如果一台服务器出现故障，目录客户端和应用程序可以与不同目录服务连接。通过复制机制，提高了应用系统的可用性。使用目录复制的内容，多个客户端目录数据请求可以负载到多个服务器上，从而改善目录服务的性能。

在复制系统中，我们使用提供者和消费者分别代表数据源和目的地，提供者服务器发送更新到另一台服务器，消费者服务器接收这些变化。提供者和消费者角色不是相互排斥的，一个服务器可能既是提供者又是消费者。

提供者和消费者的服务器的配置信息称为复制协议。此配置信息通常包括复制的单元，主机名和远程服务器的端口，以及复制间隔等其他信息。复制协议描述了哪个消费者应该接收更新、目录哪一部分被复制、该如何连接提供者和消费者，以及如何验证消费者。

在大多数目录服务器软件中，目录分区的单元也是复制的单元，所以分区方案决定了复制单元。一些目录服务器软件允许创建目录子集的副本，只有目录的一部分复制到消费者服务器中。

一致性程度说明在任何时刻，提供者和消费者之间数据的一致程度。强一致性复制指在任何时刻，提供者和消费者的数据是一致的。弱一致性复制允许消费者服务器数据和提供者服务器数据在一段时间内有偏离，但数据最终会趋向一致。

目录复制支持增量更新和全部更新，增量更新指消费者服务器只更新变化部分，全部更新指消费者服务器同步所有数据。在初始化复制时，必须进行一次全复制，保证消费者与提供者数据的一致性。

一般情况下，目录的整个分区都复制到消费者，如图 6-5 所示，子树 ou=Accounting, dc=example, dc=com 被完整复制到消费者服务器上。

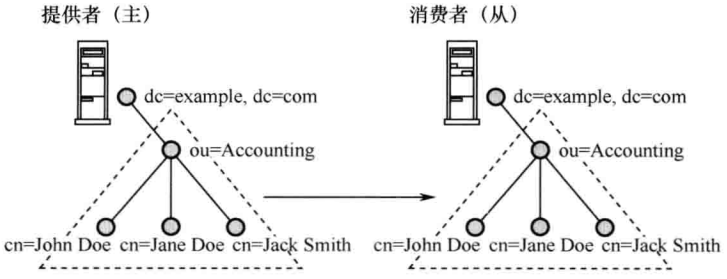

图 6-5　复制条目子树

当然，在某些情况下，只需要复制条目的部分属性，如图 6-6 所示，防火墙之外的副本中 John Doe 的条目包含了比防火墙内的主服务更少的属性。

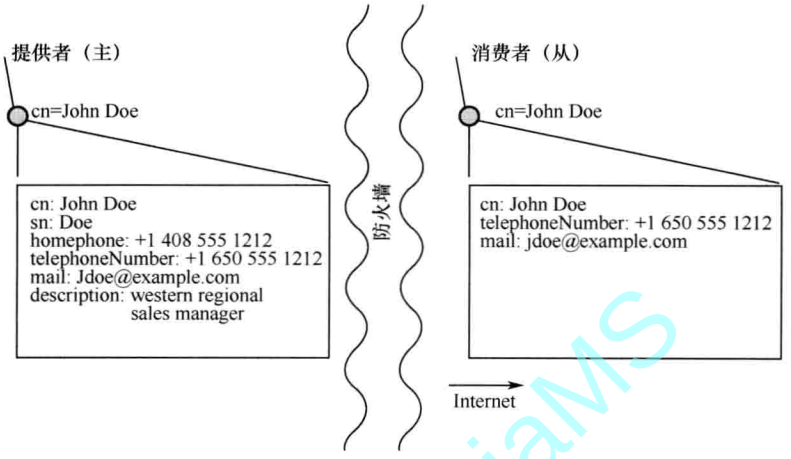

图 6-6　部分属性复制

在某些情况下，我们可能只需要复制子树下的部分条目，如图 6-7 所示，使用对象类选择复制条目，只有子树 ou=Accounting, dc=example, dc=com 下的组织单元（organizational Unit）和个人（person）条目被复制。

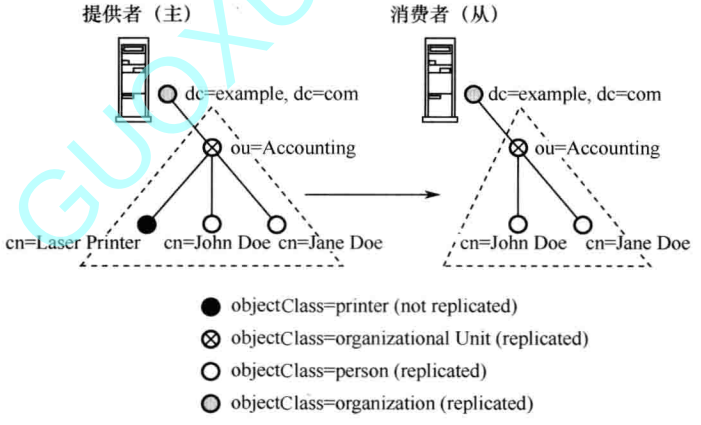

图 6-7　部分子树复制

目录复制方式主要包括一主多从或多主复制，一主多从表示只有一个主目录（提供者），只有主目录可写，从目录只读，所有对从目录的写都会重定向到主目录。多主复制是指配置多个目录服务充当主目录的角色，每个主目录都可写入，写入的数据会同步到其他主目录。由于多主复制容易造成数据的不一致，所以在实际部署中多采用一主多从部署模式。

6.3.2　引用机制介绍

引用可以看作是一个别名，别名包含另一个对象的 DN，而引用包含一个或多个对象的 URL，通常情况此 URL 是 LDAP 的 URL。LDAP URL 中包含服务器的主机/端口和一个

对象的 DN，主机/端口的信息可以指向不同的目录服务器。别名解析由服务器处理，引用返回给客户端，由客户端负责处理它。

引用是用不同的名称来标识一个对象，它们允许目录管理员设置“搜索路径”，用于收集来自多个服务器的结果。它们还可以用于部署高速缓存或只读服务器副本返回所有更新请求的引用。可以使用引用实现只读副本的负载均衡策略。

例如，服务器 A 包含"DC=example, DC=net"，服务器 B 包含"DC=sub, DC=example, DC=net"，服务器 A 含有引用对象"DC=sub, DC=example, DC=net"，它的 ref 属性值为"ldap://B/DC=sub, DC=example, DC=net"。

dn: DC=sub, DC=example, DC=net
dc: sub
ref: ldap://B/DC=sub, DC=example, DC=net
objectClass: referral
objectClass: extensibleObject

一般情况下，引用对象和被引用对象的 DN 相同，如果 ref 有多个值，在 LDAP URL 中的 DN 值应该一致。管理员在配置目录服务时需要避免引用循环。

6.3.3 复制机制的部署

不同厂家的目录服务器在复制机制实现上会有差别。我们以 OpenLDAP 2.4 版本为例，说明复制机制的部署。

OpenLDAP 2.4 版本实现了 RFC4533（LDAP Content Synchronization Operation）复制技术，称为 syncrepl，对目录树的所有写入进行跟踪，对副本的写操作被拒绝，并返回主服务引用。

syncrepl 从服务器启动，现在将其命名为消费者，主服务器角色称为提供者。在 syncrepl 中，消费者连接到提供者以更新目录树。在最基本的仅刷新（refreshOnly）模式中，消费者接收自上一次更新以来的所有更改条目，请求状态标记（cookie）跟踪上一次同步的更改，然后断开连接。在下一次连接时，将状态标记呈现给提供者，它仅发送自上一次同步之后更改的条目。

另一个 syncrepl 模式称为更新并保持（refreshAndPersist），如 refreshOnly 操作一样启动；但是不会断开连接，消费者保持连接以接收任何更新。在最初更新后发生的任何更改都会立即通过连接由提供者发送到消费者。

提供者的配置如下：

```
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

syncprov-checkpoint 100 10 告诉服务器每 100 次写操作或每隔 10 分钟将 contextCSN 的值存储到磁盘中。contextCSN 是 cookie 的一部分，它可以帮助消费者找到自上一个复制周期之后的某个位置。syncprov-sessionlog 100 的意思是将写操作存储到磁盘中，100 表示最大会话日志的数量。