基于 refreshOnly 模式的消费者配置如下：

```
updateref ldap://masterserver.ertw.com
syncrepl rid=1
provider=ldap://masterserver.ertw.com
type=refreshOnly
interval=00:01:00:00
searchbase="dc=ertw, dc=com"
bindmethod=simple
binddn="uid=replica1, dc=ertw, dc=com"
credentials=replica1
```

syncrepl 命令需要 updateref、尝试复制的目录树的信息，以及将要使用的验证凭证。凭证在消费者一方执行，并需要足够权限来读取正被复制的目录树部分，rid 将此消费者标识给主服务器。消费者必须是具有介于 1 到 999 之间的唯一 ID。provider 是指向提供者的 LDAP URI。type 指定只想通过 refreshOnly 进行定期同步，且 interval 是每小时。interval 以 DD:hh:mm:ss 格式指定。

转换到 refreshAndPersist 模式十分简单，只是移除 interval，并将 type 更改为 refreshAndPersist，如下：

```
updateref ldap://masterserver.ertw.com
syncrepl rid=1
provider=ldap://masterserver.ertw.com
type=refreshAndPersist
searchbase="dc=ertw, dc=com"
bindmethod=simple
binddn="uid=replica1, dc=ertw, dc=com"
credentials=replica1
```

当然，不必复制整个 LDAP 目录树，可以通过命令筛选只需复制的数据，筛选条件说明如表 6-5 所示。与 syncrepl 的其他选项一样，这些选项以 key=value 的形式输入。

表 6-5　复制筛选条件项

条　件	说　明
searchbase	指向复制将开始的树节点的 DN
scope	sub、one 或 base 之一。它确定从 searchbase 开始，到树下多深的数据将被复制，默认值为 sub，它涵盖 searchbase 和所有子 searchbase
filter	LDAP 搜索过滤器，例如（objectClass=inetOrgPerson），用于控制复制哪些记录
attrs	将从所选条目中复制的属性列表

一个部分复制的例子如下：

```
syncrepl rid=123
        provider=ldap://provider.example.com:389
        type=refreshOnly
```

```
interval=01:00:00:00
searchbase="dc=example, dc=com"
filter="(objectClass=organizationalPerson)"
scope=sub
attrs="cn, sn, ou, telephoneNumber, title, l"
schemachecking=off
bindmethod=simple
binddn="cn=syncuser, dc=example, dc=com"
credentials=secret
```

在这个例子中，消费者将从 ldap://provider.example.com 的 389 端口连接到提供者来执行每天一次 refreshOnly 模式的同步。它将以 cn=syncuser, dc=example, dc=com 绑定用户名，以密码“secret”进行简单验证。注意要在提供者服务器为 cn=syncuser, dc=example, dc=com 设置适当的访问控制权限以接收想要的复制内容，同步在 dc=example, dc=com 的整个子树搜索 objectClass 是 organizationalPerson 的条目，请求的属性是 cn、sn、ou、telephoneNumber、title、l。schema 检查被关闭，这样当处理来自提供者的更新时，消费者将不会强制对条目进行 schema 检查。

6.3.4 引用机制的部署

如前所述，引用的主要用途是建立分布式目录系统、对目录进行分区，或把多个小的目录系统组合成一个大的虚拟目录。

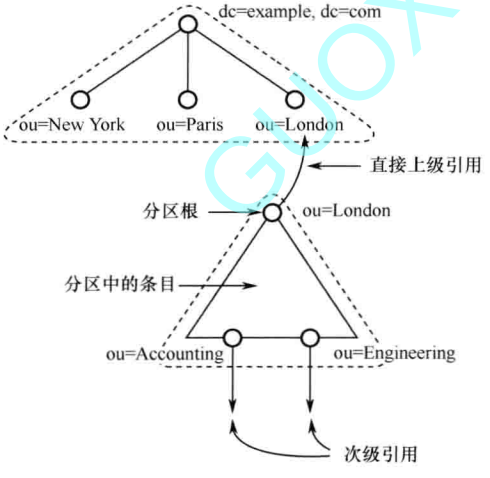

图 6-8 目录数据分区

如图 6-8 所示，该分区根 ou=London, dc=example, dc=com 代表分区的顶部。分区包含分区根目录和它下面的所有条目，除了在 ou=Accounting, ou=London, dc=example, dc=com 和 ou=Engineering, ou=London, dc=example, dc=com 分区包含的条目，也包含了指向总目录树的引用。当在一个分区搜索非本分区的条目时，会返回总体目录的引用。

在目录服务器中，向上引用一般配置在服务器的配置文件中，不出现在目录条目中。

例如，假设服务器 hosta 包含“O=MNN, C=WW”和“CN=Manager, O=MNN, C=WW”条目及以下引用对象：

```
dn: OU=People, O=MNN, C=WW
ou: People
ref: ldap://hostb/OU=People, O=MNN, C=US
ref: ldap://hostc/OU=People, O=MNN, C=US
objectClass: referral
objectClass: extensibleObject
```

```
dn: OU=Roles, O=MNN, C=WW
ou: Roles
ref: ldap://hostd/OU=Roles, O=MNN, C=WW
objectClass: referral
objectClass: extensibleObject
```

第一个引用对象告诉服务器 hosta：服务器 hostb 和 hostc 拥有子树“OU=People, O=MNN, C=WW”，第二个引用对象表明服务器 hostd 拥有子树“OU=Roles, O=MNN, C=WW”。

6.3.5　LDAP 优化

对 LDAP 性能的优化主要包括两个方面，采用索引、缓存技术提高单台服务器的查询性能；采用复制技术使多台服务器同时提供查询服务，以提高系统整体响应能力。

目录服务器采用的缓存技术随产品的不同而不同，如 OpenLDAP 使用配置文件设置服务器的缓存参数，在 slapd.conf 中使用“cachesize 条目数”设置内存中缓存的条目数目，为了提高性能，可以设置缓存尽可能多的条目，或根据实际情况，设置合适的缓存数目，一种极端情况是把所有条目都缓存起来（只有在条目数目较少时可行）。OpenLDAP 使用 DBD 保存数据，通过设置 DBD 的缓存参数，可以优化读写性能，通过“set_cachesize <gbytes> <bytes> <ncache>”参数，设置缓存大小，<gbytes>加<bytes>的值越大，越能减少读写操作访问硬盘的次数。

通过对条目的属性建立索引，能够极大提高查询性能，索引方式随 LDAP 产品的不同而有区别。在 OpenLDAP 中，通过 index 语句在配置文件中建立属性索引。index 的格式为：

```
index attrlist | default indices
```

indices 的取值可为 pres、approx、eq、sub、special 中的一项或多项。pres 在使用“objectclass=person”或“attribute=mail”格式查询时需要；approx 在使用“sn~=perso”格式查询时必须指定。eq 在使用“sn=smith”格式时需要，特别是在使用 EQUALITY 规则而查询条件中没有通配符查询时；sub 在使用“sn=sm*”格式时需要，特别是在查询条件中有通配符时；special 值为 nolang 或 nosubtypes，与 subtypes 有关。

使用 default 指定缺省匹配规则，用在 index 语句中没有指定规则时，例如：

```
index default pres, eq
index cn, sn, uid
```

例如，对 cn、sn、uid 建立索引：

```
index cn pres, eq
index sn pres, eq
index uid pres, eq
```

当单台服务器性能不能满足查询需求时，就需要使用多台服务器对查询进行负载均衡了。使用负载均衡时，一般采用复制方式，所有的写操作都重定向到主服务器，所有的读操作优先使用从服务器。采用的原则是就近提供服务，即在一个分布式服务环境中，所有操作优先访问本地服务。如果本地服务不能提供，则访问中心服务。

6.4 面向 LDAP 的系统设计与开发

6.4.1 LDAP 管理工具

大多数商业和开源的 LDAP 实现会随软件带有目录管理工具，以对目录进行查询和操作，这些工具能够满足大部分目录操作的需求。为了方便用户操作，我们以 OpenLDAP 2.4 版本为例展示这些工具。

从 http://www.userbooster.de/en/download/openldap-for-windows.aspx 下载最新 Windows 版本的 OpenLDAP，根据提示进行安装。

从应用角度来说，对目录的操作无非是增加（ldapadd）、删除（ldapdelete）、修改（ldapmodify）、查询（ldapsearch）条目。ldapadd、ldapmodify、ldapdelete、ldapsearch 是各个 LDAP 产品都支持的命令行工具，它们有比较一致的命令行参数和使用约定。

虽然 ldapadd 和 ldapdelete 实现了条目的增加和删除，但 ldapmodify 实现的功能更多，用 ldapmodify 完全可以替代 ldapadd 和 ldapdelete 的功能，可以说 ldapadd 和 ldapdelete 是 ldapmodify 的简化定制版本，所以我们主要介绍 ldapmodify 和 ldapsearch 两个命令工具。

1. ldapmodify 命令

ldapmodify 的用法：ldapmodify [选项]

操作列表读取自 stdin 或通过-f file 选项读取自文件。具体选项请参考表 6-6 和表 6-7。

表 6-6 ldapmodify 增加或修改选项

选项名称	含义说明	选项名称	含义说明
-a	向目录中增加属性值，缺省情况是替换属性值	-P	使用的协议版本，缺省为 v3
-c	遇到错误跳过，并继续执行	-S file	把跳过执行的操作写到文件 file 中
-f file	从文件 file 读取操作指令		

表 6-7 ldap 工具通用选项

选项名称	含义说明
-d level	将 LDAP 调试级别设置为“level”
-D binddn	绑定 DN
-h host	LDAP 服务器
-p port	LDAP 服务器上的端口
-H URI	指定要查询的服务器 URI（如:ldap://localhost:3389/），常见格式为 ldap(s)://hostname:port，如果使用了-H，就不能使用-h 和-p 参数
-I	使用 SASL 交互模式
-n	显示该做而没有完成的操作
-O props	SASL 安全参数
-v	详细日志模式，诊断信息都输出到标准输出
-V	输出版本信息
-w passwd	简单认证模式下绑定口令
-W	提示输入绑定口令
-x	使用简单认证
-y file	从文件 file 读取口令
-Z	启用 TLS 请求（-ZZ 要求必须得到成功响应）

ldapmodify 可以一次执行目录服务器上的一个或多个更新，ldapmodify 依据 LDIF 文件依次执行更改操作，该 LDIF 文件除了要遵循一般的 LDIF 文件格式外，还要注意数据的次序，比如要确保父节点在子节点之前，用户密码只要写明文即可。虽然 ldapmodify 参数较多，但常用的形式还是比较简单的，如下：

```
ldapmodify -a -h host -p port -D <bind dn> -w <password> -f <ldif file>
```

假定要把 Jensen 的 e-mail 地址改为 abc@example.com，可以采用命令“ldapmodify –h localhost –D "cn=directory manager" –w secret -f updates.ldif”，updates.ldif 的内容为：

```
dn: uid=jensen, ou=people, dc=example, dc=com
changetype: modify
replace: mail
mail: abc@example.com
```

增加一个条目可以用命令“ldapmodify –h localhost –D "cn=directory manager" –w secret –a -f updates.ldif”，updates.ldif 的内容为：

```
version: 1
dn: uid=bjensen, ou=people, dc=example, dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Babs Jensen
givenName: Barbara
sn: Jensen
uid: bjensen
mail: bjensen@example.com
telephoneNumber: +1 408 555 1212
description: Manager, switching products division
```

从上面的例子看出，修改条目属性操作和增加条目操作的命令行参数基本一致，只是 LDIF 文件的内容不同，对于其他 LDIF 操作示例，参考 6.1.7 节“LDIF 数据交换文件”。

2．ldapsearch 命令

与 ldapmodify 类似，ldapsearch 也是从命令行接收查询参数，然后以 LDIF 格式显示搜索结果。ldapsearch 工具的用法如下：

```
ldapsearch [选项] [过滤条件 [属性列表]]
```

其中，“过滤条件”符合 RFC4515 规定的查询过滤规则，“属性列表”包含以空格分隔的属性说明，其中“*”表示全部属性，“+”表示操作属性，“1.1”表示忽略属性。具体选项及过滤条件请参见表 6-8 和表 6-9。

与 ldapmodify 相同，ldapsearch 同样支持表 6-7 所列的选项。

当搜索条件所含表 6-10 中的字符时，必须进行转义。