第16章　LDAP：目录服务

作者：Mark Kadrich

本章内容包括：

- 为什么使用目录服务
- 目录服务功能
- IP上的目录服务
- OSI X.500目录模型
- LDAP结构p
- 目录系统代理和访问协议
- 轻型目录访问协议
- LDAP服务器 —— 服务器通信
- 设计LDAP服务
- LDAP配置
- 产品环境
- 选择LADP软件

轻型目录访问协议 (LDAP)是功能非常强大且健壮性非常好的协议，实现起来相当复杂。LDAP自身就要用几百页纸来描述，正如在《理解、开发 LDAP目录服务》一书中所见到的一样。这一章涵盖了LDAP的卓越之处同时尽量给出LDAP的总体描述。

16.1　为什么使用目录服务

如果用户已经在考虑这个问题，说不定已经收集了关于不同主题的许多文件。问题不是收集这些信息，而是当用户需要这些信息时使之成为有价值的东西。为了记录这些大量信息，用户可能要在机器上创建目录以表示这些知识的含义。用户可能有一个购买信息目录、一个生产信息目录，还有一个故障目录。每个信息目录用图16-1中的一条竖线表示。这些信息对用户而言是很有价值的，因为它代表了有关用户主题的全部知识。然而，用户所拥有的信息只是更大量信息的一部分。

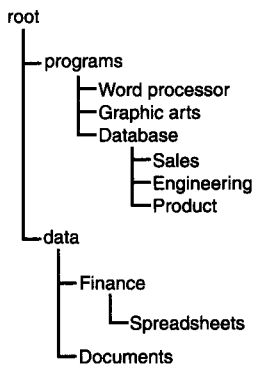

图16-1　一个目录结构例子

由于互联网络的普及使得用户可以获得大量信息，信息的收集就成为日常工作。用户可以收集关于自己所从事学科的各种信息。如果想知道更多生产塑料、亚麻鸟的信息，可以到 Internet上去找。

Internet提供的新服务使得搜索信息变得比以前更容易。像Yahoo!和Infoseek这样的搜索引擎使得信息发现工作只需通过点击来完成。然而用户现在已经找到了所需的信息，问题是如何管理它们？答案是目录服务。

16.2　目录服务的功能

虽然可能没有意识到，但是用户以前确定使用过目录服务。电话号码簿和电视收看指南

是使用目录很好的例子。在电话号码本的例子中，包括名字、地址以及电话号码。在电视收看指南的例子中包括电视的时间、名字、描述、播出时间、主题等。用户甚至可以使用电视收看指南来对VCR进行编程。如果安装了VCR的VCR+，就可以输入目录号，之后，VCR能自动对自身编程记录下用户选择的节目。这样使得使用VCR和访问广播节目变得更容易管理。

和VCR+一样，LDAP为在网络中定位信息提供了一种比其他协议，如域名服务(DNS)，更容易的途径。和只是用于定位计算机的DNS不一样，LDAP允许用户记录找到的目录信息。LDAP目录保留了关于用户及其计算机的信息。与电话号码簿和电视收看指南不一样，LDAP目录是动态的。它们保留的信息可以按需进行更新。LDAP目录也是分布的，这样就不容易遭到破坏。

16.3 IP上的目录服务

在网际协议(IP)上有许多其他的目录服务在运行。IP是使用号码来标识Internet上计算机和网络的系统，它的功能就像用几个数来标识一所公寓内的房间一样。其中楼号和网络号相似，公寓号相当于子网号，房间号可以认为等价于主机号。比如，用户不使用Deep Creek街1234号128号公寓，而是使用名字如John Smith来发送信息。

如果用户使用过Web浏览器，就使用过DNS。它的工作方式与LDAP相似：客户程序给服务器发出一个请求，服务器处理该请求并返回应答。

图16-2和表16-1画出了在本地查找过程中IP地址如何与DNS进行映射。

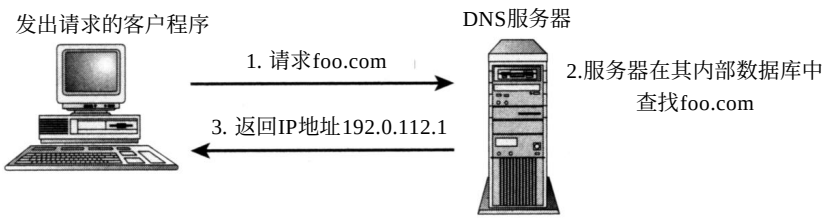

图16-2 本地DNS查找过程

表16-1 联系主机名和IP地址的DNS表实例

主 机 名	IP 地 址
foo.com	192.0.112.1
foo	192.0.112.1

如果本地服务器没有地址信息，会给上级服务器发送一个请求，请求会沿着一棵倒置的树进行，非常类似于LDAP使用的结构。这一点可以从图16-3中看出来。

whois、finger、YP和DAP也是运行在IP上的目录服务。用户可能还记得黄页，现在通常称为网络信息服务(Network Information Service，NIS)。NIS是一种识别用户、主机的服务，在NIS+中，其他的信息由系统管理员维护。NIS是一种使管理员负责一个大型的LAN或WAN来集中管理用户信息的服务。如图16-4所示，一旦用户登录，就要从主机发一请求给YP服务器。这个请求将包含用户信息，如UID、口令以及主机信息。YP服务器会把返回信息发送给用户主机，告诉它是否允许被访问还是被拒绝访问。

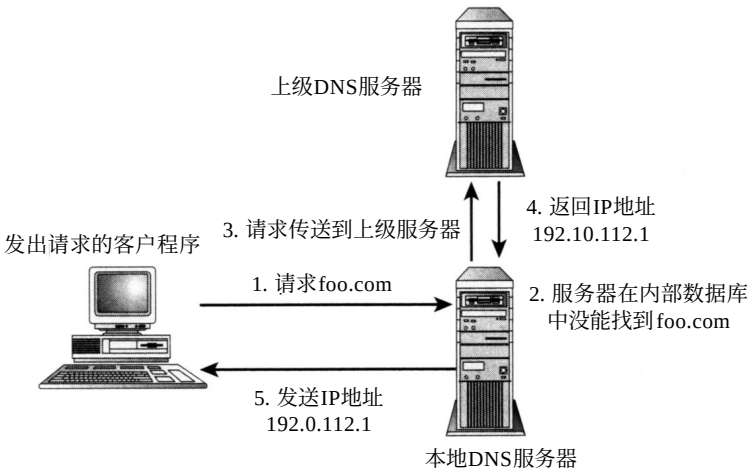

图16-3 发送到上级服务器的DNS查询

管理员喜欢这种服务，因为它能利用网络自身。在网络内可以设置辅助 (Secondary)NIS服务器以确保可靠性并减小延迟。这已经成为安装局部NIS服务器的标准操作规程以减少下行时间，这种情况在停机或高流量负载时尤其重要。

主控(Master)NIS服务器在预先设置的时间间隔内把用户信息“推”给辅助 (Secondary)服务器。这通常在夜间流量小时与网络备份及系统更新一起进行。

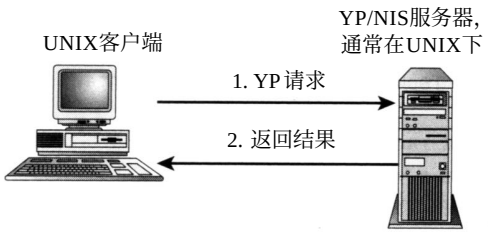

图16-4 UNIX环境中的黄页或网络信息服务

有时，对用户信息的变化需要立即更新。在特殊情况下，如当一个对公司心怀不满的员工被解雇时，系统管理员就需要一种立即删除用户访问权限的方法。有时新的用户，如承包商，需要有访问权限以便开始工作。承包商通常按小时付费，所以让他们尽快早点开始工作是有利的。正是因为这些原因， NIS也允许手动更新辅助服务器。系统管理员能改变并手动更新特定的网络服务器。

警告 手动“推”操作既是有用的也是危险的。一个匆忙的系统管理员发出“ fat fingered”命令不小心把大部分用户的访问权限删除，这种情况出现过多次。这是一个用来检测分组交换机和语音邮件系统健壮性非常好的一个方法。

Whois是一个基于文本的目录服务，存储有关主机、服务器、 IP地址和网络信息。一个whois请求会得到相当数量的信息。 whois数据库中通常会存储如下信息：联系名、记账地址、电话号码及域服务器。 Macmillan whois产生如下信息：

```
Registrant:Macmillan Magazine Limited ( MACMILLAN-DOM)
4-6 Crinan Street London EnglandN1 9XW

UK Domain Name: MACMILLAN.COM
Administrative Contact, Technical Contact, Zone Contact: Humphreys,
➥    Mark ( MH177)
```

```
postmaster@MACMILLAN.COM +44 71 836 6633
Billing Contact: Humphreys, Mark ( MH177)
➥   postmaster@MACMILLAN.COM +44 71 836 6633
Record last updated on 05-Aug-98.
Record created on 11-Aug-94.
Database last updated on 11-Jul-99 19:39:33 EDT.
Domain servers in listed order:
NS0-M.DNS.PIPEX.NET 158.43.129.77
NS1-M.DNS.PIPEX.NET 158.43.193.77
AUTH01.NS.UU.NET 198.6.1.81
```

16.4 OSI X.500目录模型

OSI X.500标准位于OSI协议栈表示层之上用于处理分析请求和应答。直接位于表示层之上，相关控制服务元(Association Control Service Element，ACSE)和远程操作服务元(Remote Operation Service Element, ROSE)可以使下面的通信层通过抽象文法标示 (ASN.1)来交换信息。通过对数据如何交换文法的标准化， ASN.1提供了一种在两种不同计算机系统之间交换信息的方法。这样也使得X.500应用程序能在网络上的计算机之间交换信息。

ASCE提供了在两个应用层实体之间通信的方法。在 X.500模型中，ROSE使目录系统代理与目录用户代理之间的通信成为可能 (参见图16-5)。

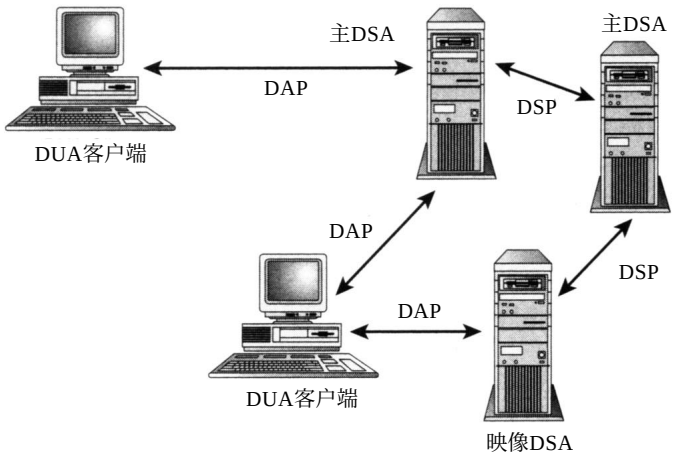

图16-5 基于X.500模型的目录访问协议组成部分

X.500目录服务模型由三个基本单元组成。包括：

- 目录信息库(DIB)
- 目录系统代理(DSA)
- 目录用户代理(DUA)

DIB中包含的信息由 DSA管理，这样 DUA能访问使用它。 DUA使用目录访问协议 (DAP)来访问DUA。在这种以客户 /服务器类型的组织中， DUA既可以是人也可以是其他应用进程，如电子邮件客户程序。 DSA能通过目录系统协议 (DSP)与其他DSA进行通信，就像DNS服务器之间彼此通信的原因一样。然而和 DNS不一样，在DNS中，当没有找到IP地址时会查询上一

级服务器，而DSA是对等的。在今天的大型网络中，这一点提供了可扩展性。

16.4.1 早期的X.500

在80年代，国际电报电话联盟(CCITT)开始致力于存储和检索诸如电话号码和电子邮件地址的工作。同时，另一个组织 —— 国际标准化组织(ISO)开始寻找一个合适的服务来支持 OSI 网络中的名字服务。最后，两个组织认识到他们的工作有重复并最终一起努力形成了今天的X.500标准。

最终的结果是一个具有一些有趣特性的目录服务。 LDAP是其中最重要的，作为一个开放式标准，LDAP不属于某个个别生产商。其次， LDAP使通用目录服务能支持大量信息。第三，LDAP极具扩展性和分布性。X.500一开始就是用于支持广泛的且演变的网络结构，并且做得非常好。最后，LDAP在安全框架内支持丰富的搜索功能。图16-5画出了LDAP的主要组成部分。

X.500并不是没有缺陷。如在早期开发过程中就发现的， LDAP复杂且需要大量资源，而且要仔细规划。 LDAP也是为OSI而开发，而不是今天使用的 TCP/IP标准。OSI从来也没有真正实现过，并且TCP/IP的速度和简单性也是OSI所不及的。显然需要对DAP作一些改动。

16.4.2 今天的X.500

X.500已经演变成一组非常完整的规范。其中的核心是目录访问协议 (DAP)，DAP被认为是整个目录请求的中心。 DAP的不足，也可以认为是 DAP的优点，是因为它想要同时解决所有问题。所以， DAP所提供的大量神秘的服务在桌面机环境中很少有什么实际用处。在桌面机上完全实现DAP要小心考虑。为了减小复杂性，开发了一个服务 LDAP作为桥梁。

16.5 LDAP结构

LDAP开发的目的是为了简化 DAP。然而在X.500与LDAP之间有很大的相似性。 LDAP使用目录系统代理和目录用户代理；然而在 LDAP中，它们被简单认为是LDAP服务器和客户机。LDAP也使用相同的OSI体系结构。LDAP应用程序位于表示层之上，通过 LDAP应用程序编程接口与底层进行通信。

LDAP服务的基本元素包括：

- LDAP服务器
- LDAP客户机

这里的主要差别在于对 API的依赖而不在于对 IP栈填加的栈“ 隙片 ”，这个栈“ 隙片 ”把X.500与通信栈连接起来。主要的相同点是网络配置结构和数据存储方式。与 X.500一样，LDAP服务是分层次的。

16.5.1 LDAP层次结构

LDAP信息结构类似于前面描述的文件系统。在图 16-6中，读者可以看到LDAP起始于根。LDAP信息的基本单元是项。项是指现实世界关于某对象的信息集合，在本例中，对象是组织自身。

在许多情况下，目录结构是组织结构的反映。它起始于组织描述，向下细划为项，如部门、资源最后到人。

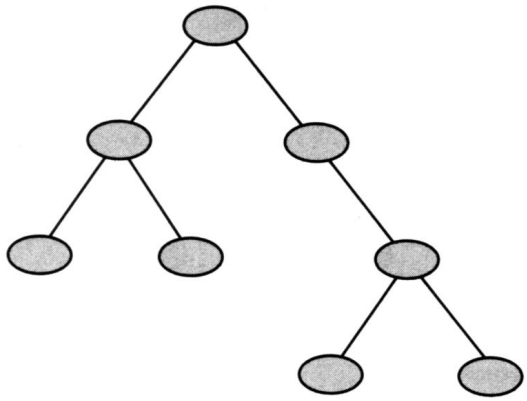

图16-6 LDAP目录结构的倒向树

16.5.2 名字结构

在目录项内部是一组属性，这组属性描述了被选对象的一个品质。属性由一个类型域和一个或多个值组成。属性类型描述属性内包含的信息。值是属性对应的值。比如属性的电话号码值是1 800 555 1234。

为了有效地进行搜索，对象分类提供了一种元素命名方式，如：objectclass=人。

可以使对所有定义为人的对象的搜索不会搜索服务器或建筑物，因此使搜索耗时更小。

接下来的属性cn，意思是通用名字，如图16-7所示，通用名经常是个人或资源的全名。

完整的目录列表起始于可辨别的名字 (dn)，这个名字包含对象类别及个人或资源的信息。

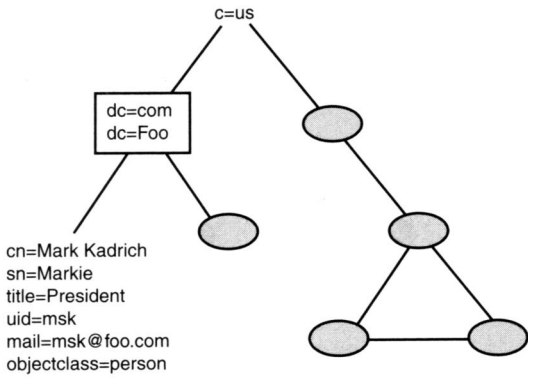

图16-7 名字空间示例，目录信息树

因为LDAP不像DAP一样支持从目录树顶到其他目录的连接，所以LDAP引入了别名支持这种功能，这可以通过把用户整个的 DIT看作另一个DIT的叶节点实现。

16.6 目录系统代理和访问协议

开始时，DSA负责目录信息管理。目录信息库驻留在 DSA上。DSA由位于客户机上的目录用户代理访问。再次参考图 16-5，DUA使用DAP访问包含DIB的DSA。看起来很简单，实际上并非如此。 DSA被设计成分布的。当 DIB变大时，可能需要把一部分移到其他服务器上或者和其他DSA连接在一起。这可以通过目录服务协议完成。和支持用户查询的 DAP不一样，DSP用于DSA之间交换信息、传递请求、复制或映像目录，以及提供管理支持。

16.7 轻型目录访问协议

如前面所讨论的，LDAP从早期协议演化而来。这些早期协议，如 DAP，在其应用之前开

发出来。设计人员对各种格式信息的更大需要导致了这些协议的复杂性。

像DAP这样的解决方案对于小型桌面系统而言太复杂，对于管理员而言也太复杂。需要更简单的协议。商业团体帮助削减了一些在桌面机工作环境中的要求，但仍能使管理员在分布式系统繁忙时重新获得对大量丢失配置的控制，最终的解决方案演化为LDAP。

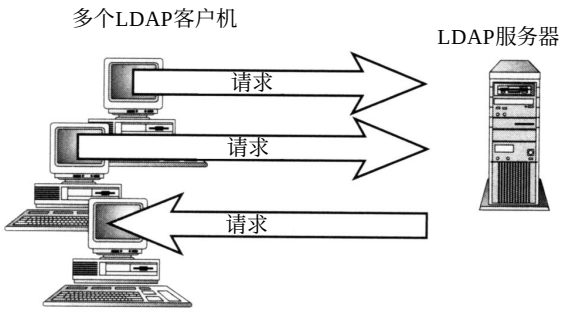

图16-8 基本的LDAP消息传递协议

LDAP是一个基于网络计算客户机 /服务器模型的消息传递协议。服务器保留信息，并接收网络上的客户机请求。服务器形成应答并发回至客户机。图16-8显示了客户机的请求如何作为独立消息发送至服务器。

16.7.1 查询信息

用户及其应用程序查询当前信息的能力构成了一个功能强大且健壮的平台，这种能力就建造在这个平台之上。

在LDAP模型中，假设数据被读取的次数比其被写入的次数多许多倍。正因如此， LDAP对访问进行优化。在通常的局域网中，像 DNS这样的服务是高事务服务。换句话说，其他的服务依赖于目录服务功能来应答信息请求。

如前面所提到的， LDAP是基于客户机/服务器模型的协议。这使得服务器为某些特定过程进行优化 —— 在这种情况下，是指搜索和查询信息并把信息发送到网络上。 LDAP服务器不包括外部过程和用户接口信息，而是包括那些管理数据和服务器的信息。

过程起始于绑定到服务器上的客户机发出信息查询请求。绑定是在主机和服务器之间建立会话的过程。图 16-9显示了基本工作过程。客户程序构造一个请求，查询某项，比如查询用户的电话号码，客户把这个消息传给服务器。服务器通过发送包含请求信息的消息应答给客户机，并发回一个结果码消息。结果码消息会告诉客户机请求是否成功，如果不成功，错误原因是什么。

在需要有多条消息要发给客户机才能正确应答时，最后一条消息是结果码消息，如图16-10所示。

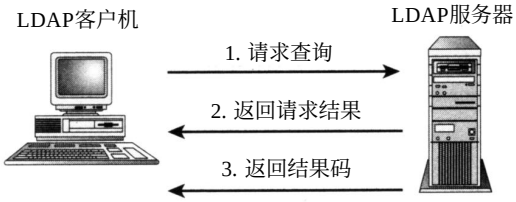

图16-9 基本的LDAP工作过程

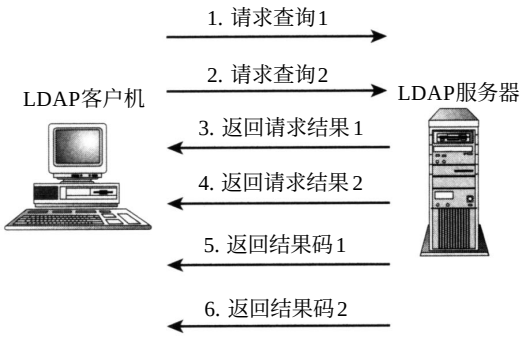

图16-10 通过LDAP发送多条消息请求

基于消息协议的特点是其允许同时发送多条消息。LDAP会处理这些不相关的消息请求并对每一个请求作出应答并发送结果码消息。

在有认证和控制的情况下，LDAP提供绑定操作，去除绑定操作和放弃操作，绑定是客户机必须要做的第一件事，初始化到服务器的会话。在这个阶段，客户机会向服务器确认自身并提供凭证，这和安全协议一起工作来防止对数据库的非授权访问。

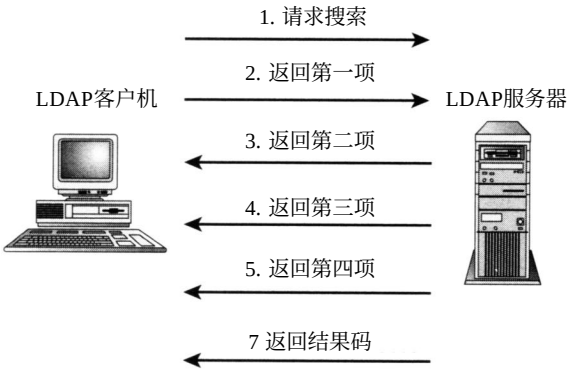

图16-11 通过一个消息发送多个请求

去除绑定(unbind)通知服务器客户机LDAP会话结束，发出LDAP请求的应用程序得到信息，用户继续使用应用程序。

当客户机发送了一个放弃消息时，它告诉服务器其不再需要信息。用户可能已经中止了正在请求信息的应用程序或者应不正常结束。这种情况下，要求操作系统发送放弃消息。图16-11显示了从开始到结束的整个事务过程。

16.7.2 存储信息

存储信息属于维护和收集操作，LDAP通过支持下面三个功能提供这些操作：

- 加入 —— 加入功能只是加入一个新用户和属性值到一个已有的数据库上。
- 删除 —— 删除操作从数据库中删除掉属性或整个项。这个操作在用户离开时用得上。然而大多数系统管理员仅仅把用户设为非活跃的。
- 修改 —— 对系统管理员而言，修改函数可能是最有用的，考虑到该操作被使用的频率，删除操作可能是第二个用户最常使用的操作。修改函数使系统管理员和用户可以修改目录中的信息。典型情况下，用户只能修改自身信息的一小部分。数据项如电话号码和个人头发颜色可以由用户任意修改。

要仔细考虑权限问题。你也许想让自己的部分用户有能修改他们个人信息的权力。这意味着你应该特别注意他们对用户目录的访问权限。

16.7.3 访问权限和安全

在最近一次对Internet上可访问LDAP服务器的测试中，发现所有LDAP服务器的绝大部分是可访问的。任何信息安全专家会说出最危险的事情是赋予某人的访问权。如果一个黑客能访问服务器，他就拥有了服务器上的数据。

用户必须有一个程序来确保自己的服务器 (不论是UNIX还是Windows-NT)以安全方式配置。同时建议实施一个安全策略不断的服务器进行检查。可以获得大量商业应用程序对用户服务器进行检查以发现操作系统和数据库自身在安全方面的脆弱性。

对用户目录的访问权限及适应程度因使用的服务器应用程序不同而不同。一定要小心理解应用程序如何与操作系统一起工作来提供安全性。

16.8 LDAP服务器-服务器通信

虽然许多用户只看到LDAP协议中的客户机至服务器部分，但是还有一些用户看不到的操作以保证用户能可靠地查询服务器。

可靠性毫无疑问是针对于单点失败问题的健壮性设计要求。它也意味着使延迟保持最小。延迟作为可靠性的一个方面需要理解为至少从用户的角度看是这样。如果用户要用很长时间来访问基于网络的服务，他们会以为网络崩溃，不可靠。如果管理员设置 LDAP服务为一个单点失效服务器，就将面临其用户的埋怨。

16.8.1 LDAP数据互换格式(LDIF)

LDAP使用标准方法产生请求消息和应答消息，消息以文本文件进行交换，这种文件采用一种预定义的LDAP数据互换格式 —— LDIF(LDAP Data Interchange Format)。一个典型的LDIF如下：

```
dn: uid=msk, ou=people, dc=starwizz, dc=com
objectclass: top
objectclass: person
objectclass: managementPerson
objectclass: corpmgntPerson
cn: Mark Kadrich
cn: markie
givenname: Mark
sn: Kadrich
uid: msk
mail: msk@starwizz.com
telephonenumber: +1 408 555 1212
description: President, Starwizz Enterprises

dn: uid=ma, ou=people, dc=starwizz, dc=com
objectclass: top
objectclass: person
objectclass: managementPerson
objectclass: corpmgntPerson
cn: Mitch Anderson
cn: mitchie
givenname: Mitch
sn: Anderson
uid: ma
mail: ma@starwizz.com
telephonenumber: +1 408 555 1212
description: Vice President, Starwizz Enterprises
```

最上面一行是相对可辨别名字 (RDN)，用于跟踪对象。在这个例子中，用户可以得到有关人的姓名和组织情况。读者会注意到这个格式与电子邮件地址向右解析的工作方式相似。称此为“小结尾(little-endian)”顺序。在这种格式中，最低级元素先写，最高级元素加在最右边。如：

msk @ host.division.state.starwizz.com

16.8.2 LDAP复制

复制是一种多刻面服务，它提供了增强的可靠性和性能。通过在整个网络环境中分布目录信息，用户可以降低发生服务器以及网络相关故障时的脆弱性。正如图 16-12中所看到的一样，如果一个LDAP服务器副本失效，内部的请求会发送到其他的 LDAP副本或至主服务器自身。没有LDAP副本，网络A和B上的客户机将得不到LDAP服务。

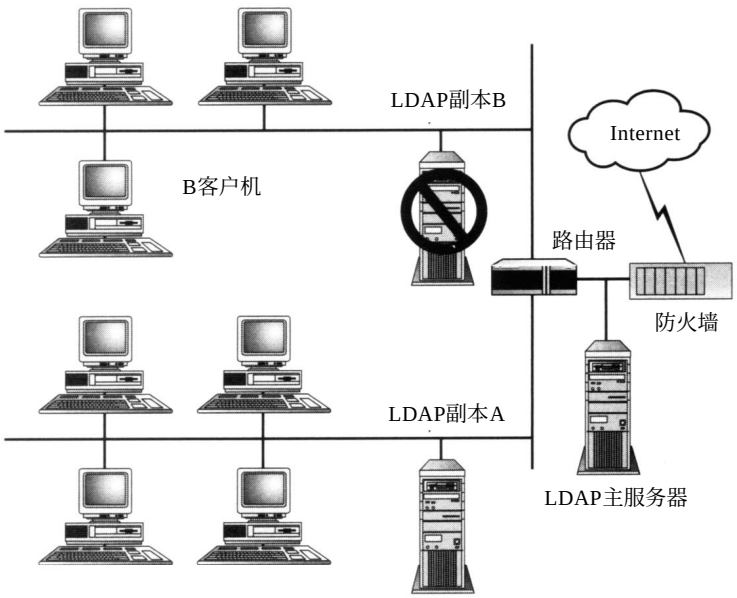

图16-12 广域网上分布式LDAP提供了冗余和可靠性

从性能的角度考虑也会带来好处，因为本地 LDAP请求不必通过路由器。局部请求可以由局部资源处理，所以减轻了网络的流量负载。

副本不必包含整个目录树。为了安全和维护方便， DIT中只有特定部分被复制，用户可以有选择地复制运行在相关网络上的服务。在图 16-12中，B副本只包含网络B上的特定目录项。对网络B之外信息的服务请求将被传送到主 LDAP服务器。

16.9 设计LDAP服务

定义需求是一个非常重要的问题。要花些时间来考查信息环境如何工作以及随着时间的变化情况。

16.9.1 定义需求

当用户建立目录服务查需求时，需要考虑许多方面。这一节会论述用户群体对工作的信息环境的需求。这意味着设计人员必须考虑用户及其使用的工具，包括：

- 用户需求
- 用户的期望
- 应用需求

- 配置限制
- 配置问题
- 其他

我们所做的一切都是为了满足用户和他们的期望。设计人员总是给用户太高的期望，目的是向他们出售解决方案。而这些解决方案并不以用户的需求为基础，而是只考虑一些其他人的想法——一个好的解决方案是什么样的。当现实情况不是这样时，用户就会感到不满意。一个成功的解决方案必须满足用户的期望，因为他们才是决定解决方案是否成功的人。

这里我们考虑LDAP应用程序以及这些应用程序在用户环境中的配置。设计人员当然要考虑以后会出现什么情况，不建议把这部分所提供的内容作为现成的方案。这并不是说不应考虑新的应用，而是说要考虑这些计划中的应用在不是为每一种可能的情况都设计一个目录的情况下将如何影响设计。

设计者应仔细考虑用户如何使用和保护数据。什么是个人信息，什么不是个人信息对用户而言是个很广泛的概念。准确性是另一个考虑。数据被更新的频率是多少？用户期望使用精确的数据。

应用需求是一个主要的设计元素。所需信息类型和访问频率是一个应仔细考虑的主要因素。和DNS驱动应用程序使用 Web的方式相似，用户应用程序会驱使目录服务设计比任何其他服务更有力量。

16.9.2 设计策略

设计者应该拥有尽可能多的信息，这说起来容易。然而，信息越多，为了给一个查询作出正确的应答就需查找更多的信息。设计者也不要想一个最小的解决方案，因为那样或许不能满足用户及其应用的需求。

数据的来源和数据自身同等重要。设计者要回避不能被证实或不是最新的数据源。做到这一点要考虑组织内的其他数据源。像 HR和helpdesk这样的领域保留了可能包含相同信息的数据库。使用数据库术语，这被称为冗余数据。

一些基本问题包括：

- 太多的信息
- 太少的信息
- 不正确的信息

最后一项不易讨论，因为它涉及到数据库中的信息质量问题。有时，用户浏览器发出的不仅仅是一条查询。在一些情况下，要以LDAP服务器中包含的信息来作出决定。这个过程中，决定可能是以旧的、过时的信息为基础作出的。当考虑最坏情况时，这样是可怕的。考虑这样的一个例子，一个对公司不满的雇员因为总是给其同事制造麻烦而被解雇。而且， LDAP服务器给已经授权的员工访问的权力。不难看出，这里面有潜在的危险性。

配置一个策略来确保用户数据的暂时性和安全性是个好想法。记住，这个数据库中很有可能包含个人信息，设计数据策略应考虑如下几个方面：

- 存储
- 访问权
- 修改

• 维护
• 合法性
• 异常

1. 存储指南

存储指南讨论在数据库中应存储什么样的数据。数据大小和数据源的限制也属于这个范畴。一个例子是大于15K的数据元素不应存储在数据库中。

2. 访问指南

访问指南决定谁能看到并访问信息。如果在数据库中存储了敏感数据，这就是很重要的问题。

3. 修改指南

修改指南决定谁能修改信息以及信息怎样被修改。最重要的问题——是否用户能更新自己的信息，属于这个范畴。认证和加密方法也在这个范围内。

4. 维护指南

数据维护是一个互相联系的问题，它包含的策略是非常有用的。维护指南应包括数据被检查的频率及冗余数据被检查的频率。其他数据库问题，如 HR的out-of-syn数据问题在这里处理。

5. 合法性问题

一些数据比其他数据更敏感，如果被不该看的人或组织得到，它的损失是金钱所不能衡量的。它可能会破坏组织的好名声。让法律部门检查一下数据库可能需要一些时间，但从长远考虑这是值得的。

6. 异常指南

一个没有考虑变化或异常情况的策略，其生存时间可以以天计。设计者应包含一种机制允许异常和变化发生。这些变化应被最高级认可。

16.9.3 性能

一个需要一直使用的服务会很快受到损坏。当设计师考虑构造 LDAP服务时，必须考虑服务所使用的环境。一些要考虑的问题包括：

• LDAP服务器所处的局域网/广域网类型。
• LDAP服务器所提供服务的多少。
• 硬件的开销。

用户所连局域网或广域网的类型会影响用来支持用户需求的 LDAP服务器数量。在简单的局域网环境中，一台服务器可以满足所有需要 (如图16-13)。一台路由器把局域网和 Internet连接起来，用户计算机通过网络集线器和局域网相连。防火墙是标准的安全设备，它控制局域网和Internet之间的报文流。这一点将在 16.9.5节中讨论。

在大型组织中，网络会比图 16-13中画出的网络复杂得多，广域网内部子网由多个路由器互联，每一个子网又包含许多局域网。使用这些技术让成千的计算机分布在全世界，这种情况非常可能。在这样更复杂的环境中，设计者要考虑使用倒置的树结构来配置 LDAP服务器，如图16-14所示。

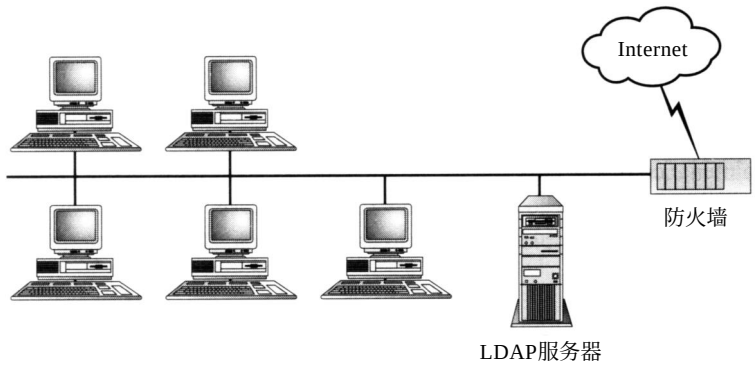

图16-13 简单的基于局域网的LADP配置

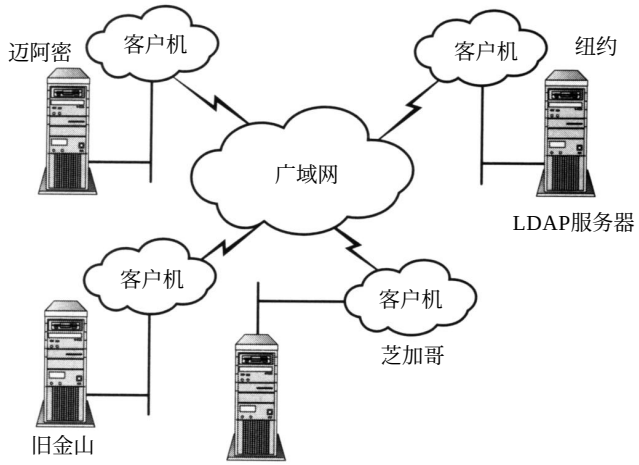

图16-14 具有分布式LDAP服务器的复杂广域网

16.9.4 网络功能

可靠性和可用性有时称为网络“功能”。可靠性直接影响可用性，这是因为如果一个服务器是不可靠的，它提供的服务就是不可用的。在网络环境中，不仅仅包含服务器，还有支持网络的设备。如前面讨论过的，一些网络是大型分布式的，为了使网络具有可用性，会使用冗余设备，如路由器、交换机和不间断电源 (UPS)。并不是所有的设备都冗余配置。一些路由器和交换机及一些贵重设备，装备了冗余电源来避免最常见的电源失效。在网络中，使用两个设备，当一个不能工作时，另一个可以接替。这种称为 fail-over的配置类型具有高度的可用性。读者在图16-15中可以看出，这种配置需要有多条到 Internet的连接。

一种更健壮的实现称为 fault resilient，这种方案通常使用 fail-over类型的配置但小心地确保设备内冗余尽可能做到最高。这种方案的例子是使用两个路由器，每个路由器采用双电源供电、一个UPS以及到Internet的不同连接。

这些方案的基本不足是设计者必须花两倍或更多的钱来购买硬件和软件，而一个时刻只有一个设备在工作。

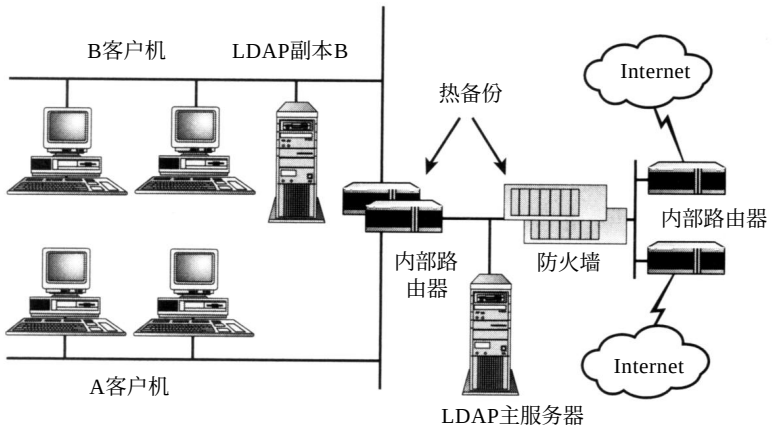

图16-15 冗余路由器和热交换(hot stand-by)路由器

这样看来，只有IBM的服务器具有高可用性。 Novell HA服务器所使用的网络框架在卖出之时，线路被抛弃了。

最可靠的配置称为容错 (fault tolerant)，意思是说任何一个组件发生故障都不会导致整个设备失效。

对于容错设备，有许多共同之处。如价格贵，产品少。从这一点看来，只有像 Tandem这样公司的大型机才是真正容错的。

另一个决定可靠级别的方法是允许故障时间。如表 16-2所示，一般的服务器能忍受一年内有3.5天故障时间，然而，容错系统只允许一年中有 5分钟的故障时间。

表16-2 用时间衡量的可靠性设计

正常运行时间比率	一年中最大当机时间	可用性设计
99%	3.5天	常规
99.9%	8.5小时	高可靠
99.99%	1小时	错误恢复
99.999%	5分钟	容错

LDAP服务器应该至少是高可用性的设计。如果是错误恢复 (fault resilient)当然更好。

另一个缓解单点失效问题的方法是在整个网络环境中分布 LDAP服务。美国西海岸的一个地方有自己的服务器，东海岸的一个地方也有自己的服务器。两个服务器会向集中服务器报告，以便更新和复制。这种类型的配置能利用网络的可靠性因素。因此，能提高整个系统的可靠性。参考图16-14理解其如何工作。

16.9.5 安全

许多系统经受过小的攻击，使一些恶意攻击者窃取了珍贵信息。 LDAP服务器和网络上的其他服务器没有什么区别 —— 不正确配置，任何一个懂得一点安全漏洞的人就可以访问到数据。

安全不仅仅是防止对数据的非授权访问，而是一种有意识的态度，是对风险、威胁、减轻危险以及安全所带来好处的理解。安全问题出现时，设计者必须对风险和利益进行评估。设计者也要认识到有许多不同的安全级别。一些信息是公共的，而另一些信息却是非常敏感

的，其他的信息介于这两个极端情况之间。

问题是什么？简单的讲就是，LDAP使一个组织能把大量信息放到服务器上，以可靠且快速的方式提供查询应答。

1. 安全威胁

人们经常把计算机安全威胁和黑客联系起来。但并不总是这样，实际上，绝大多数安全破坏来源于组织内部人员。Peter Shipley所作的最新统计表明在1999年Blackhat Briefings会议之前大量公司的LDAP服务器可以通过Internet访问(Blackhat Briefings每年召集政府、公司和私人安全专家在Las Vegas集会)。而且，那些可访问的服务器几乎没有安全机制。使用 nmap 工具(可以从Internet上获得)的如下命令：

```
nmap -p0 -p 636,639 192.168.0.0/24
```

进行扫描的结果显示出大量脆弱的服务器。相同的命令用于用户的 IP地址，能够确定用户的服务器是否可以从Internet上访问。

> **注意** 如果读者从Internet上特别是从黑客站点上下载了一些软件，在把它应用到网络上之前首先要在可控环境下运行它。如果不这样，会因下载了特洛伊木马或病毒而感到气恼。特洛伊木马是一些伪装成一些东西而实际上却不是那些东西的软件。换句话说，读者可能认为正下载的软件是一个很好的新工具，而实际上却是包含恶意代码的工具。

Shipley也发现几乎没有服务器使用安全方法进行信息交换。安全套接字层 (Secure Sockets Layer，SSL)是对信息进行加密的标准方法，可以确保数据的私有性。

有几种基本的安全破坏方法。因为，安全破坏如 LDAP自身一样相当复杂，所以本节只包括一些基本知识。基本的安全破坏包括：

- 非授权访问
- 非授权数据修改
- 拒绝服务攻击

非授权访问是指一些不具有访问权的人对服务器的访问，这样做通常是为了窃取证书、劫持会话或嵌入软件。

窃取证书非常类似于口令窃取，只是它能在更广的范围内进行。入侵者会伪装成 CIO或任何他们想伪装的人。不只一次发生过这种情况：一个人被别人中止，被中止的人认为是自己的老板而实际上却是他的同事。当错误发现时，破坏已经造成了。前面提及的不满员工经常采取这种方法。

虽然需要对局域网进行物理访问，但是劫持会话能够在用户认证自己后完成。攻击者简单地插入到服务器的报文流并发送 TCP复位到无辜的用户。用户认为网络暂时“不畅”因而继续进行。这是另一个要确保网络可靠的原因。防止会话劫持的简单方法是使用加密，如 SSL，防止对网络报文的访问。

嵌入软件是更复杂攻击者的标志。通过特洛伊木马，攻击者能做任何想做的事情。一些特洛伊木马仅仅监听网络并把信息发送给攻击者，而其他的特洛伊木马却提供访问系统的后门。后门会使大部分主机安全机制丧失作用。

对数据非授权地修改能造成严重的危害。通过改变“发到”的账户，可以把用户银行账户上的金额转至攻击者的私人瑞士户头上。

拒绝服务(DOS)攻击是直接停止LDAP服务器。在应用程序一级有两种类型的 DOS攻击：直接和间接资源消耗。

在直接资源消耗攻击中，用户不断地请求大量数据。消耗掉系统资源，其他人就不能发出请求了。限制一个客户机能使用的目录资源数是减轻这种攻击危害性的标准方法。

间接攻击更难防范，因为它不是攻击LDAP应用自身，而是攻击LDAP服务器所使用的资源。比如，假设服务器中引入了特洛伊木马，而它要做的就是发出磁盘请求。拒绝 LDAP对磁盘文件的访问请求，攻击者就能停止LDAP服务器。防止这种类型的攻击遵循前面已述及的安全策略。使用小型正版的操作系统软件，以及时刻保持警惕至少会使检测这种攻击变得更容易。

2. 主机安全

主机级安全是黑客首先要观察的，也是服务器配置中最容易被忽视的方面。依赖于环境，服务器产生于需求而且不能脱离已存在的环境。这意味着配置操作系统是一个问题。不幸的是，如果服务器运行起来，所有配置就被接受了。

UNIX服务器安全是众所周知的主题。许多书论述这一点。而且，大量商业软件产品能检查机器配置并给用户提供指导使其安全。

提示 如果不需在服务器上提供服务，就把该服务删掉。不要仅仅把无用软件置成不能(disable)状态，而是要删掉它。一般性的服务如Telnet和FTP不应在LDAP服务器上支持。

打开日志生成功能并把日志发送到一个特定设置的计算机能存储和归档的系统日志。

3. 应用安全

首要也是最重要的一点，如果不需要该应用，就不要让它运行。

看起来这是一条简单规则。然而，许多系统管理员被迫极大限度地使用系统，因此造成了不安全因素。

4. 其他安全问题

物理安全是另一个被忽略的方面。由于不是防火墙或文件服务器， LDAP服务器可能不像其他更重要的服务一样被提供相同的保护级。记住许多这样的服务依赖于 LDAP，也正因为如此，LDAP服务器应该受到保护和监控。

让LDAP服务器放在上了锁的房间里，并且对房间的访问进行控制。至少应该采取键盘锁定和带口令的屏幕保护。

5. 工具

有一些工具可以用来使服务器安全，包括：

- 认证
- 检查
- 加密

认证不仅仅指用户ID和口令。强大的认证系统，如来源于安全 ID和Axent技术的系统，提供交换安全口令的令牌使口令只使用一次。每次用户访问系统，就使用新的口令。所有用户要记住的只是PIN。

检查是基本的安全措施。通过检查系统的审查日志，管理员能确定是否发生了不安全行为。许多安全管理人员会说这是一项枯燥且费脑筋的工作，但却是必要的。

作者曾听许多加密算法的创造者 Whit Diffie说过：“ 不是加密自身的缺陷，而是加密如何使用会造成缺陷 ”。当考虑使用加密作为许多安全工具的基础时，这一点很重要。 SSL使用加

密把报文转换成不可读的垃圾，只有目标机能读它。证书使加密生效，数字签名文档告诉接收方文档是真实的。

表16-3表示了用户访问信息是如何配置的情况。系统管理员对数据有完全的访问，虽然表中没有包括，但对系统管理员工作站的访问应该使用强大的认证机制来保护。

表16-3 LDAP属性及相关访问权和保护

属 性	审 核 员	访 问 级 别	安 全
cn,sn, givenName, middleInitial,name	所有	读	无
cn,sn, givenName, middleInitial,name	系统管理员	读/写	SLL和证书
mail	所有认证的	读	口令
mail	系统管理员	读/写	SLL和证书
mail	自己	读/写	口令
homeAddress homePhone	所有	用户选择	口令
homeAddress homePhone	自己	读/写	口令
postalAddress telephoneNumber	所有	读	口令
postalAddress telephoneNumber	系统管理员	读/写	SLL和证书
salary	自己	读	口令
salary	管理	读/写	SLL和证书

16.10 LDAP配置

配置是另一个瓶颈。设计人员必须和其他部门一起工作来负责网络服务和应用。在许多情况下，这些部门会设计专门的 Windows程序进行配置。他们也经常使用配置网络服务的过程，如测试和接受。

考虑配置所需服务的先后顺序。如果设计人员依赖于 LDAP支持工作流应用，就有可能在没有LDAP时一些部分不能正常工作。没有什么事能比如下的事情更令用户气愤的了：当用户通过电话号码本查到另一个用户并和他联系上时而系统却说此用户不存在。

如果每个部门均有自己的应用集，就必须保证部门选择工具时的各种驱动因素是否考虑了敏感性。

16.11 产品环境

虽然许多产品环境不同，但它们却有一些共同之处。首先，它们都包括人。其次，这些人都在那里，因为他们有工作要做。所以设计人员可以以相同方式建造 LDAP服务。从工程计划开始，这个计划具有一些可测量的因素和阶段目标 (里程碑)。之后，实施计划。使用计划作为蓝图来开始工作并衡量是否成功。

16.11.1 创建计划

计划应该包含足够的细节，当其他人接管项目时，不至于看不懂。好的计划会描述许多元素，如：

- 资源
- 项目计划自身
- 成功标准
- 市场规划，这要依赖于所在组织

有许多工具可以使用以创建一个计划。作者使用 Microsoft Project工具。MS Project能够把任务和资源以一种方式结合起来，这种方式使得预计未来情况很容易，设计人员也可以随意使用提供了相同功能的工具。图 16-16示出了应遵循的基本步骤。正如读者所看到的，资源在计划中被命名，前提任务再向下展开之前列出来。

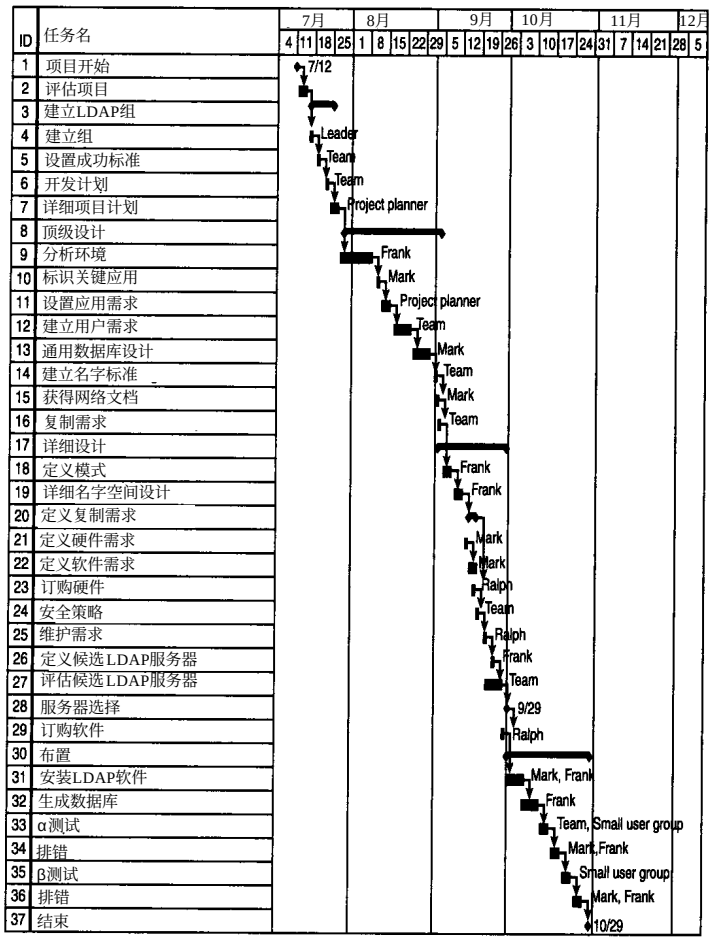

图16-16 LDAP展开计划示例

好的项目计划也是与管理人员进行交流的好方式。

成功标准的制定应基于需求。LDAP服务器的加入是为了访问一个新应用吗？如果是这样，

LDAP服务器能运行应作为一个阶段目标，然而应用实际可以使用 LDAP服务器应是最后成功的标准。这需要小组共同努力，如果小组解散，没有人能说：“ 新应用确实是一个工艺品而LDAP服务器确实不错 ”，他们会把LDAP服务器连同应用扔到垃圾桶中去。

这就是为什么需要市场计划来帮忙的原因。一个执行赞助商发表声明，印刷电子邮件、发送备忘录能带来巨大的好处。赞助商能帮着制定期望，提供设计人员所需的时间来构造优质服务。

16.11.2 有价值的建议

注意细节！作为体系结构设计师，有责任揭示和自身组织相关的细节。

可能急需把计划付诸实践，不要那样做。如果还没准备好，就不要付诸实践。

当计划展开时，可能会发现一些东西要发生变化。这就是项目计划起的作用—帮助设计人员理解一些不知道情况和因素的影响。

不要隐藏什么。如果一些东西遭到破坏或发生问题，处理之后继续工作。如果他们不信任通讯员，他们就不会相信消息。换句话说，如果他们不信任设计人员，他们就不会信任设计人员设计的服务。

管理计划。很容易在细节中迷失，不知道重点在哪里。在找不到重点的时候，可怕的灾难会进入到项目中来。作者看到许多项目因细节问题没处理最终导致夭折。

小心任何事情。任何偶然事件都要找到答案。一个好的项目管理员会注意“ 当项目发生问题该如何处理 ”。如果硬件晚到怎么办？如果编码器坏了怎么办？这个过程很困难，但必须要经历。

16.12 选择LDAP软件

和其他软件一样，满足设计需要的选择过程很重要。软件是否具有增值性，或者仅仅是在系统遭到破坏时管理员使用的一个应用程序。这些问题设计人员都要考虑并且要选择一个供货商。

基本的问题可以分解成如下元素：

- 核心特征
- 管理特征
- 安全特征
- 标准兼容性
- 灵活性
- 可靠性
- 互操作性
- 性能
- 可扩展性
- 价格
- 其他，通常是政治因素

1. 核心特点

在这里要看一下软件是否能在所选择的硬件上运行。最后要做的是为 UNIX环境购买NT

软件。

软件是否支持用户应用程序所需的LDAP特性？如果不支持，就不要选择这个软件。

在用户拓扑结构中支持复制特性是一个重要的问题。如果设计师计划在整个环境中分布LDAP服务器，这一点就要优先考虑。

所有软件如何支持数据的载入？用户必须痛苦地敲入数据的每一位还是软件有导入(import)特性？

最后一点是归档和支持。用户必须通过Braille来安装软件还是有足够的联机帮助文档。

2. 管理特性

找一些管理容易的工具。所选软件有能力支持脚本操作会带来额外的好处。

应该找一个工具使较困难任务(如配置安全访问权限)的执行过程更简单。完成配置甚至要采用参数文件的形式。能够设计用户类型之后进行拷贝才能真正节省时间。

有时，当管理员要管理服务器时，却不在服务器面前，这样就引入了远程管理的想法。确保所要使用的软件支持安全的远程管理功能，因为这样才能在网络上发送敏感的信息而又不想未授权的用户窃取到该信息。

3. 安全特性

基本的访问控制对LDAP服务器而言是必须的。确保能完成解析和粒度要求的控制访问。管理员可能赋予某个特定用户访问控制权而不是某组用户。

健壮的LDAP服务器会支持加密功能，如SSL或传输层安全(transport layer security，TLS)。如果要做任何远程管理或复制就必须具有这一关键特性。

广泛的认证选项是前提条件。基本的LDAP认证，如证书和口令令牌，应该包括在基本特性之内。

因为需要其他管理员甚至一些用户来关注他们自己的数据，所以授权功能是重要的。

4. 标准兼容

基本上讲，解决方案要和所有的LDAPv2及LDAPv3 RFC兼容。查看一下RFC 1777~1779以及RFC 2251~2256。安全规范定义在RFC 2222中，简单认证和安全层也应和RFC兼容。为了远程管理和网络管理，必须和SNMP v2 MIB(管理信息块)相兼容。

读者可以在站点http://www.mozilla.org/directory/standards.html上找到相当全的有关LDAP信息。

有许多应该兼容的应用程序接口(API)，如为Jave和C相关的API。也有一些标准的API，特别是那些来自微软及其活动目录服务接口(Active Directory Services Interface，ADSI)的API，所以不要混淆。

5. 灵活性

很少有不要配置的软件产品，假设用户网络的某个方面与任何其他网络均不相同。配置这些不同点是关键。所选的LDAP服务器应很灵活，能满足特定需要。配置是否可以调整来满足不同的硬件要求？毕竟，不是每个人都有256M存储器。

另一个问题是加入和扩展模式。管理员是否能够不需要完全重新安装软件就能操作数据结构？新的应用可能引入新的数据元素，因而管理员必须扩展模式来适应变化。

6. 可靠性

如果数据库中一些数据发生错误，其他数据就成为不可靠的。如果服务器不可用，依赖

于它的其他应用将不能运行。为了解决这些事情，设计者必须清楚一些重要问题。服务器是否能从故障中恢复而不丢失任何数据？服务器如何处理事务？

必须具有运行24×7的功能。很少有用户能忍受管理员为了备份而中止 LDAP服务器服务。

寻找能支持fail-over或其他高可靠类型的解决方案。虽然硬件能提供可靠性，但是必须要在主服务器和热备份服务器之间交换信息，热备份机包含了目录的一个拷贝。否则，在故障之后，管理员必须处理丢失的数据并要面对气恼的用户。

7. 互操作性

简单的讲，互操作性是指LDAP服务器与应用程序及其支持程序互相操作的能力。

提示 不论以什么形式出现，首先要确保服务器能工作。许多生产商宣称自己的方案有高的可靠性；然而，它们只是工作在特定的环境中。要保证服务器软件也能在设计人员的特殊环境中工作。

8. 性能

由于LDAP是基于网络的服务，因此基本问题是延迟和吞吐量。设计人员必须要提前弄清楚用户忍受的延迟是多少。之后要检查服务器是否能满足这一要求。服务器是否能在不崩溃的情况下同时处理多条连接？是否能监控自身性能，是否能通过修改参数来增强性能？

知道服务器的理论权限是个不错的想法。服务器的性能往往和硬件配置相关，但有时却不是这样。可能没有内部缓冲或所需方法来超越性能平台。为了规划目的，设计人员应知道这个限制。

9. 可扩展性

一些应用程序可以容易地扩展功能，超越最初的程序。一些应用程序通过支持脚本设计来扩展功能，而其他的(如Netscape)使用软总线方法，通过插入模块来进行功能扩展。

可扩展功能对于开发自己的应用非常有用。

10. 价格

如果设计者能说：“我喜欢花100美元购买蓝色的”，那就很好。不幸的是，价格不是一个容易说清的问题，生产商已经使 LDAP服务器的价格和买一辆新轿车一样让人捉摸不定。一些生产商按位置定价，一些生产商按服务器数定价，另一些生产商按项数定价。一些受到灵感启发的生产商销售无限的许可权。通常，价格是上面所有因素的集合体。

如果维护按年来付费，不要感到奇怪。同样，考虑必须每天完成的工作，如备份和更新。

一些LDAP服务器和特定操作系统捆绑在一起。微软的活动目录就属于这种情况，必须使用Windows 2000才能利用它的全部优点。

也有一些LDAP服务器要在特定硬件上运行。一些操作系统要求很大的硬件投资，不要忘记考虑这些因素。

培训和支持也是必须要考虑的。一些生产商免费提供培训，但是必须为管理员付费。

11. 其他：通常是政治考虑

从商业角度考虑所购产品的生产商。是否长年提供产品？公司有多大？是否能开发满足LDAP新扩展的产品？

考虑生产商在目录服务市场中的位置。虽然设计人员最喜欢使用其他生产商的产品，但是要看到自己的生产商正在花费金钱来研究和开发产品以使其与标准兼容。公司也应该进行互操作测试以保证与其他生产商产品的兼容性。

16.13 小结

LDAP会成为网络世界潜在的大型组织者。能够在一个目录信息源上点击应用程序大大减轻了网络管理员的负担。这不但使应用程序设计者更容易设计，也使系统管理员的工作更容易。系统管理员不再管理许多应用程序来保证用户的连接性。用户会透明地连接所需的服务和信息。

然而，LDAP是复杂的服务，需要非常注意细节。规划和测试在成功 LDAP实现中起主要作用。

随着网络服务的增长，读者会看到将更依赖于像 LDAP这样基于网络的目录服务。或许有一天，它会代替电话号码和电视收看指南。