微软公司核心技术书库

Windows 2000 Active Directory 程序设计

（美） Charles Oppermann 著
王 磊 王 毳 等译
蒋 蕊 审校

机械工业出版社
China Machine Press

本书介绍了Active Directory 的基本结构和使用Active Directory 编程的方法。主要内容包括：Active Directory 的体系结构，Active Directory 编程接口，使用Active Directory 编程的方法，扩展Active Directory模式，使用Windows脚本管理Active Directory等。本书深入浅出、介绍详细，既适合Active Directory的初学者学习，也适合网络管理人员及程序开发人员阅读。

本书版权登记号：图字：01-2001-4438

图书在版编目（CIP）数据

Windows 2000 Active Directory 程序设计/（美）奥普曼（Oppermann, C.）著；王磊等译. - 北京：机械工业出版社，2002.1

（微软公司核心技术书库）

书名原文：Microsoft Windows 2000 Active Directory Programming

ISBN 7-111-09359-3

Ⅰ. W… Ⅱ. ①奥… ②王… Ⅲ. 窗口软件，Windows 2000 - 软件工具，Active Directory Ⅳ. TP316.7

中国版本图书馆CIP数据核字（2001）第066352号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：宋燕红 张鸿斌

北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行

2002年1月第1版第1次印刷

787mm × 1092mm 1/16 · 19.75印张

印数：0 001-4 000册

定价：46.00元（附光盘）

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

前　言

Active Directory或许是Windows 2000操作系统最为重要的特性。社会组织和企业可以使用Active Directory集中管理网络信息，这些信息原先存储在各种各样互不兼容的数据库中。Active Directory可以在整个网络上分发信息，允许采用安全、稳固的方式访问这些信息。

但是，随着Windows 2000变得广为使用，许多网络管理员和开发者逐步认为Active Directory过于复杂而且难于使用。由于我撰写了本书，我发现他们的一些疑虑是可以理解的，但其他的却毫无理由。在给定的领域，Active Directory是较为直观的，它所提供的好处远远超过最初学习所花费的精力。

由于Active Directory允许软件开发者轻松地访问许多网络资源丰富的存储信息，他们对Active Directory的潜能尤为感到兴奋。可以添加新的属性和类到Active Directory，能够扩展现有的信息以满足客户应用的需要。

本书的目标在于帮助应用开发者和网络管理员真正地理解Active Directory，以便能够创建启用目录的应用，自动完成管理任务。

本书包括的内容

Active Directory和它的主要编程接口Active Directory服务接口（ADSI）是一个大型主题，编写一本全面的书需要几年时间，而且会是一本非常厚的丛书或系列。本书并不是从A到Z的包罗万象的参考书，重点在于为开发者提供尽快入手和上路需要知道的东西。贯穿本书，我提供了完整的例子，读者可以在自己的应用中使用它们。全部例子采用易于理解的方式书写，而且都有清晰的注释。

本书分为三个部分。在第一部分“Active Directory概述”（从第1章到第3章）中，我讲述了我认为在开始深入讨论Active Directory之前，对掌握Active Directory有所帮助的背景知识。我提供了目录服务的历史回顾，提供了Active Directory的基本结构，为开发者指出了重点概念，然后说明了用于与Active Directory通信的两个基本编程接口——LDAP和ADSI。

在第二部分“使用Active Directory编程”（从第4章到第8章）中，我说明了如何使用ADSI以及C++、Visual Basic和VBScript发现并使用存储在Active Directory中的信息。我讲述了开发者和管理员所要面临的常规任务，展示了能够用于执行这些任务和解决常见问题的例子代码程序。

在第三部分“特殊主题”（从第9章到第11章）中，说明了如何使用新属性和类扩展Active Directory，以及如何使用脚本执行一些网络管理任务。在最后一章，通过介绍如何编写用于Web的Active Directory程序以及介绍Active Directory在Windows下一版本中如何变化，我预测了Active Directory的未来。

虽然ADSI允许你与包括Active Directory在内的各种目录服务通信，我并没有讲述ADSI的方方面面，例如，我没有讨论创建ADSI提供者，ADSI提供者允许目录销售商生产一个代码层，这

个代码层允许ADSI与专用目录服务进行通信。有关使用ADSI访问Active Directory之外的其他目录的更多信息，参见随书光盘上的ADSI软件开发工具箱（SDK），或访问下列网站：http://www.microsoft.com/adsi/或http://www.microsoft.com/windows2000/。

本书的适用读者

本书主要是一本编程方面的书，所关心的是如何编写应用程序以管理存储在Active Directory中的信息。但是，它对于一定范围的计算机专业人员是很有吸引力的。我所提供的信息和示例能够为以下人员带来好处：有兴趣使用脚本实现任务自动处理的企业网络管理员，以及使用Visual Basic和C++建立网络管理工具和全面启用目录应用程序的开发者。

在阅读本书以前，希望对Active Directory 有一些背景知识了解的IT专业人员来说，有两本非常好的参考书，它们是由Daniel Blum编写的《Understanding Active Directory Services》（Microsoft出版社1999年出版发行）和由David Iseminger编写的《Active Directory Services for Microsoft Windows 2000 Technical Reference》（Microsoft出版社2000年出版发行）。

读者需要预先掌握的知识

可以在几个编程语言和环境中访问Active Directory特性，但是要从本书得到最大的收益，你至少应该可以使用JavaScript或VBScript编写基本的脚本程序，对Visual Basic或C++有一个基本的了解也有助于本书的学习。

本书使用的Active Directory编程接口是使用组件对象模型（Component Object Model，COM）提供的，因而对COM了解得越多，就能越好地掌握本书。由于Visual Basic和脚本语言对开发者隐藏了许多COM实现细节，如果你使用上述环境工作，理解COM就不是那么重要了。还有，知道所涉及的概念有助于设计更好的Active Directory应用。如果你并不熟悉COM，也不必担心，我在第3章提供了有关COM的入门知识，以帮助你顺利地开始学习。

随书光盘内容

随书光盘包含各种文件和资源，当使用Active Directory时，能够对你有所帮助。下面是随书光盘上包括的一些项目：

- 本书所提供的全部代码示例。
- 本书的电子版本。
- Windows 95、Windows 98和Windows NT 4.0 的Active Directory客户。
- 来自Microsoft平台软件开发工具箱中需要用于编译一些代码示例的文件。
- ADSI 2.5软件开发工具箱。
- 目录服务文档，其中包括Active Directory、ADSI和ADSI Exchange编程信息，以及有关Active Directory模式的完整电子参考。
- 与Windows证书程序有关的文件。

系统要求

要编译本书示例，系统需要以下条件：

- Windows 2000、Windows NT 4.0或Windows 98（推荐使用带有服务包1的Windows 2000操作系统）。
- Microsoft Visual C++ 6.0（推荐使用服务包3或更新版本）。
- Microsoft Visual Basic 6.0。
- Microsoft平台软件开发工具箱（所需的平台软件开发工具箱文件包括在随书CD上）。

要运行代码示例，需要下列配置之一：

- 安装Active Directory的Windows 2000服务器或Windows 2000高级服务器（推荐使用Windows 2000服务包1）。
- 运行Windows 98、Windows NT 4.0或加入Windows 2000域的Windows 2000的网络客户计算机。如果客户计算机运行Windows 98或Windows NT 4.0，必须安装Active Directory客户。在随书光盘中可以得到Active Directory客户。

注意 一些代码示例要求在Windows 2000上运行，还有一些代码示例要求执行者具有管理员权限。

创建测试网络与开发环境

在本书写作期间，我花费了大量时间一次又一次地创建开发环境，用来编写示例程序。下面几节提供一些指导，以帮助你创建自己的测试与开发网络。我所讲述的方法仅仅是许许多多建立Windows 2000域方法中的一种。如果你并不熟悉Windows 2000网络概念和技术，例如域、DNS、TCP/IP、DHCP以及其他的众多术语，在使用本书例子之前，我建议你提前阅读一些背景知识。Microsoft域名系统（Domain Name System，DNS）作为一个重要的网络组件，使用Active Directory管理网络地址和计算机名称。通过亲身去做，你将发现即使是DNS或Active Directory配置中极其微小的问题，也会导致后续的故障。严密规划和仔细配置至关重要。

建立服务器

首先，你需要一个可操作的Windows 2000域。Windows 2000域不同于早期的Windows NT域。如果你的部门正在运行Windows 2000，而且你具有查看和操作部门的Active Directory的安全权限，你就万事俱备了，但是我并不赞成将部门的Active Directory用作自己的开发环境，尤其当你打算修改模式时，更不应该这样做。这种类型的操作一般总是要仔细规划，并首先在一个测试实验室环境中试用。

如果你创建了自己的Windows 2000域，或在现有Windows 2000域中建立了一个子域，你将需要一台服务器类别的计算机，具有快速的处理器（500MHZ或更高）以及至少128兆内存。这应该当作是最小配置，因为服务器的交互操作将需要更多的内存。如果有一个以上的开发者打算访问域的目录，你需要考虑添加额外的服务器，并将诸如DNS和DHCP之类的服务分布到其他计算机上。如果你计划使用Microsoft Exchange 2000服务器处理电子邮件和合作应用，更要按照上述要求做。应该在你所使用的每台服务器上安装Windows 2000服务器。如果支持4个以上处理器或集群技术，并且希望拥有故障自动切换的能力，也可以使用Windows 2000高级服务器。

要启动创建一个域的过程，你可以运行Configure Your Server（配置你的服务器），方法如下：

点击Start（开始）按钮、指向Programs（程序）、指向Administrative Tools（管理工具），然后点击Configure Your Server（配置你的服务器）。作为一种选择，也可以从Run（运行）对话框运行DCPromo程序。如何配置你的服务器取决于许多因素，例如互联网连接、互联网域名注册以及个人喜好。更多信息，请阅读《Microsoft Windows 2000 Server Resource Kit》（Microsoft出版社2000年出版发行），或参考《Windows 2000 Planning and Deployment Guide》，可以在http://www.microsoft.com/windows2000/library/planning/default.asp网址找到本书。

注意 我推荐使用DCPromo.exe创建Active Directory域，而不要使用Configure Your Server（配置你的服务器）工具。人们在DCPromo向导提供的提示下似乎很少被搞糊涂。

很多人开始使用Active Directory时，在最初的设置过程中会遇到困难。正如我所提到的，Active Directory对于网络的DNS配置以及网络硬件和协议非常敏感。我极力推荐认真阅读本书前面所列出的书。

Microsoft产品支持提供了许多在升级Windows NT或创建新的Active Directory时，人们所遇到问题的有关信息。可以在http://support.microsoft.com/support/win2000/dns.asp上找到这些信息。

注意 Microsoft提供了一个更新的域控制器诊断（Domain Controller Diagnostic，DCDiag）工具，具有诊断域控制器故障的新特性。可以从http://www.microsoft.com/technet/win2000/win2ksrv/dnsreq.asp下载这个工具。

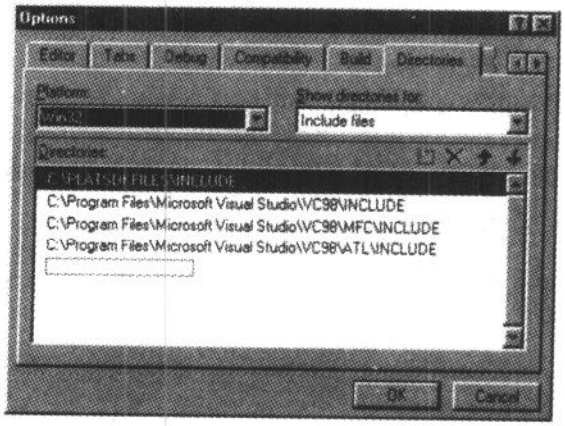
开发工作站

至于开发工作站，虽然你可以使用运行Active Directory的同一台计算机，但我建议使用Windows 2000专业版。正如我在前面所提到的，可以使用带有Active Directory客户的Windows NT 4.0或Windows98，但这两者我都不建议使用。当安装Windows 2000专业版时，要确保加入你计划使用的域。如果在你的开发计算机上已经运行着Windows 2000，使用System Propertier（系统特性）下的Network Identification（网络标识）标签页将工作站加入到计划使用的域中。

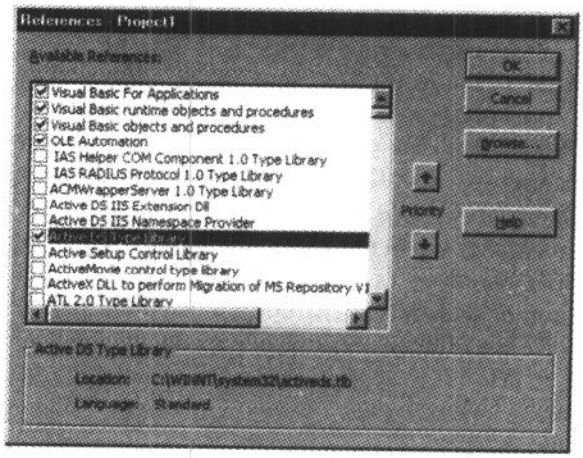
本书的代码示例使用Visual C++ 6.0和安装了服务包4的Visual Basic 6.0编写。Visual C++开发者应该注意ADSI所需要的文件并不包括在Visual C++中。你可以在平台软件开发工具箱中找到它们。你所需要的平台软件开发工具箱组件是“Build Environment\Network and Directory Services\ Active Directory Services Interface”和“Build Environment\Win32 API\Win32 API”。可以从http://msdn.microsoft.com/downloads下载这些平台软件开发工具箱组件。需要用于编译本书所提供的代码示例的平台软件开发工具箱文件包括在随书光盘上。一定要配置Visual C++，让它访问这些头文件和库文件，它们应该被放在目录列表的顶部。下图显示了Options（选项）对话框的Directories（目录）标签页，在目录列表的顶部具有所需的平台软件开发工具箱头文件。

Visual Basic用户需要在他们的Visual Basic项目文件中引用Active DS Type Library（活动目录服务类型库），如下所示：

如果你打算只是用脚本例子，就不需要Visual C++和Visual Basic了。在使用脚本时，Microsof Script Debugger（脚本调试器）非常有用。它包括在Windows 2000中，也可以从Microsoft的Web站点http://msdn.microsoft.com/sctipting/下载。其它的开发环境，例如Borland公司的Delphi，也可以使用Active Directory，这完全取决于自己，我只使用了前面所提到的软件写作本书。



要远程管理Active Directory，应该在Windows 2000开发计算机上安装管理包（Administration Pack），可以在Windows 2000服务器或Windows 2000高级服务器CD上的I386文件夹中找到Adminpak.msi文件，通过运行该文件就可以安装管理包程序。Microsoft安装器包会加载用于管理Active Directory所必需的管理控件。当一个域被创建时，同样的工具会自动安装到服务器上。其它可用的工具可以在Windows 2000 CD（所有版本）中找到。Windows 2000支持工具含有许多很好的网络诊断工具，其中包括LDAP浏览器和强大的ADSI编辑工具。我将在第2章结束部分详细说明这些工具的使用方法。要安装支持工具，请运行Windows 2000 CD Support、Tools文件夹下的Setup.exe文件。



测试工作站

尽管并不是必须的，但我仍然建议使用第三个工作站作为你的测试环境。这台计算机应该被配置为大部分网络用户所具有的相似模式，它应该只含有你的部门所应用的软件。有那么多的程序在开发工作站上运行得很好，却在最终用户计算机上导致崩溃或运行得一塌糊涂，这是多么令人吃惊啊。这通常是DLL冲突或假设一个特定配置存在而导致的结果。

如果你的程序需要运行在Windows 98、Windows NT上，或在两者上都要运行，你应该安装

合适的Active Directory客户（在随书光盘上可以得到）。还有，要在测试工作站上做几个磁盘分区，安装不同操作系统。不要将操作系统混装在同一个分区中，这样会不可避免地引发冲突。每个操作系统分区应该是干净的，就像用户得到一台新的计算机时一样。还有，考虑具有多个Windows 2000分区——一个使用FAT文件系统格式化，另外一个使用NTFS文件系统格式化。使用多种分区能够暴露与文件和文件夹安全许可有关的错误。

良好的公民权力与义务

通过为应用开发者创建一系列的指导原则，Microsoft多年以来一直致力于使用它的产品提高终端用户的经验。作为一种吸引软件提供商使用这些原则的手段，Microsoft创建了Windows程序认证。与这些方针一致并且通过一个无关性测试的应用可以将Windows标志作为它们产品行销和包装的一部分。

作为一名开发者，你应该尽可能地遵循这些原则。它们考虑了用户的广泛需求（就像你正在为其编写应用的用户），并帮助用户采用边缘尖端技术。另外，客户——尤其是大宗交易的大型组织，对认证产品给予更为认真的考虑。这会给你的产品带来十分必要的优势，让它比竞争对手的产品更容易成功。

启用Active Directory产品的开发者要特别注意到包含在《Application Specification for Microsoft Windows 2000 Server》中的要求。这个说明包含与Active Directory集成的服务器应用要求的有关信息，例如如何正确地使用Active Directory，以及在扩展Active Directory时，如何坚持可扩展性准则。

要了解特定要求和证书信息的更多相关内容，请参阅随书光盘上的Certification（证书）文件夹。在光盘上还包括测试工具和一个帮助文档模式扩展的程序。要了解最新的Windows认证程序信息，请访问网址http://msdn.microsoft.com/certification/。

现在，让我们继续学习Active Directory吧！

本书英文原书书名：Microsoft Windows 2000 Active Directory Programming

英文原书号：ISBN 0-7356-1037-1

第一部分 Active Directory概述

第1章 目录服务介绍

Active Directory是Microsoft进入目录服务领域的入口，它的设计令各方用户能够更好且更方便地进行网络计算——例如用户、网络管理员和开发者。要理解Active Directory的问题以及理解为Active Directory所编写的程序如何能够让管理并运行一个网络更为简单，回顾网络计算的历史以及目录服务的发展很有帮助。

1.1 网络计算历史

在加入Microsoft之前，我在一些小公司工作，这些公司的雇员通常不足100人，而且一般没有专职的信息技术(IT)人员。作为许多小公司的规矩，喜欢围着计算机捣鼓的人最终负责管理网络。术语“管理”或许措辞太强硬了，退一步说网络管理包括连接打印机，让它们运行并完成任务，确保新的小组助理能够访问他们所辅助的人的文件。虽然全部计算机被连接到一起，但对于绝大部分人来说就像在孤岛上工作，只有在打印和偶而访问共享文件时才使用网络。

我在1994年开始在Microsoft工作，作为Microsoft Bob一个部件的程序管理员。(有人还记得那个产品吗？)在那时，我对能够使用更为复杂的系统感到异常兴奋。我猜想Microsoft会有一个非常庞大的网络装置，可以将它的能力发挥到极限。来到公司后，我得到了四个口令——两个Microsoft Windows口令用于登录到我所拥有的两台计算机，一个口令用于我的Microsoft公司网络账户，最后一个口令用于我的Microsoft电子邮件账户。每天，仅仅为了阅读我的电子邮件，我必须至少输入三个不同的口令。这还是在Microsoft Mail(邮件)和Microsoft LAN Manager(局域网管理器)的日子里，因此如果我要发送一封电子邮件给同事，我不能仅仅输入那人的名字，我必须知道他的“短名”——在电子邮件地址中出现在@符号左边的八个字符或少于八个的字符。如果我不知道这个人的电子邮件名字，我可以给他或她打电话，但没有更简单的方法来查找电话号码。对这些信息的需求通常令我将电话打到电话接线员那里，或走进资料室，在那里我可以翻找一本称为《Microsoft Company Directory》的厚书。这本打印的姓名地址簿每个月发行一次，含有公司每个人员的全名、电子邮件名、电话号码以及办公地点。图1-1显示了一种设置，其中用户需要多个口令才能访问不同的资源。

这些困难很快被联机版本的公司姓名地址簿解决。认识到个人信息是如何使用的，负责电子邮件的专家组开始将目录特性添加到Microsoft Mail(邮件)以及Microsoft Excnange服务器中。这种想法看起来非常合理：将公司里每个人的全名以及他们的电子邮件名、办公地点和电话号码存储在一个特殊的目录中，这个目录是Microsoft电子邮件产品的一个组成部分。这个目录还

包括雇员经理的名字，以防我发送电子邮件的人没有回应我的查询。但是，即使使用这种电子版本的公司姓名地址簿，我仍然拥有不同的口令用于我的计算机、网络和电子邮件账户。使用Windows NT，安全模型提高到新的高度，其中用户的网络账户验证用户对计算机和网络资源的访问，但是仍然有不同的账户——一个用于网络，另外一个用于电子邮件系统。

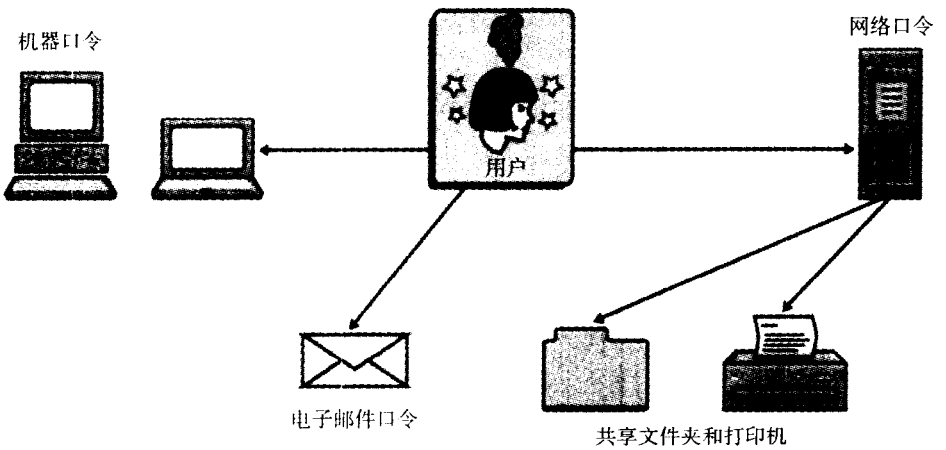


图1-1　一个用户与许多网络资源和账户

另外，就像其他公司一样，人力资源部拥有大型数据库，存储着每个雇员薪水、病假、业绩报告以及福利计划的详细资料。所以尽管只需要我输入网络账户信息来登录并阅读电子邮件，但我必须提供一个不同的口令才能访问我的健康保健计划或查看我已经休了多少天假。虽然Exchange提供了有关雇员和经理的简单分层信息，但是这些信息不能用于正式的公司组织图或用于其他目的，这通常是由于一些必要的数据没有包含在电子邮件目录中。依赖电子邮件目录中的信息仍然要假设每个雇员有一个电子邮件账户，虽然这在Microsoft不是一个问题，Microsoft的每个员工都有自己的电子邮件账户，但在当时对许多其他公司来说的确是一个问题。

在那些日子里，另外一个困难就是打印一个文档的简单任务。如果没有一个直接连接到计算机的打印机，就必须使用网络打印机。一些网络打印机提供彩色、双面打印和核对功能，但并不是全部网络打印机都有这样的能力。我会走进大厅，查看摆放在储藏室内的打印机，记下打印机的型号以及打印机是否具有我所需要的选项，匆忙记下打印机的通用命名约定(Universal Naming Convention，UNC)(诸如\\prnsrv05\hpoffjet)。然后跑回办公室，输入打印机的名字，并希望每件事都运行得毫无差错。当然很少这样做，150页标准PostScript语言(一种具有很强图形功能的通用程序设计语言,是由John Warnock开发的。)输出会让一个不知道PostScript的打印机产生300页冗繁而难解的文字或语言。

这些例子表明最终用户所要面对的挑战。网络管理员有一个更为艰辛的工作。他们管理成百上千的打印与文件服务器，努力将各种类型的文件描述名调整为8.3字符名(DOS使用的文件名约定，使用8个或少于8个字符+3个扩展名表示一个完整的文件名——译者注)。他们不断被要求对用户的账户做出非常琐碎的更改。在线商务应用(例如人力资源受益跟踪系统)的开发者必须创建他们自己的数据库以便存储用户信息。当然，只要雇员离开或加入公司、搬家到新的住址或

更改他们的名字，许多数据库和目录就需要被更新。潜在的错误和违例十分巨大，更不要说维护这些信息所要耗费的劳动力代价了。

对这类问题的一个解决方案是单一企业目录。不需要维护很多雇员数据库，一个分层目录就可以集中全部信息。目录可用于从网络上每一连接点进行查找。类似于打印的纸张姓名地址簿每个月发行一次，可以以分钟的方式复制一个网络目录，并将它发布到网络中最远处的服务器上。

Microsoft并没有发明网络目录，但是他们利用Active Directory，以及Microsoft Windows 2000服务器中包含的目录和服务集改进了这门技术的目前状态。Active Directory建立在多年网络计算的经验之上，并结合了Windows NT、Exchange Server以及其他产品。要更好地理解Active Directory，让我们进一步说明目录以及它们在网络计算中的使用。

1.2 什么是目录

简单地说，目录就是一个数据容器，就象我以前常常使用的公司姓名地址簿。另外一种目录是电视节目收视指南，它列出了电视节目及播映时间。这些传统目录都是打印的而且以固定时间间隔发行。它们不需要更改，而是由更新一期的目录替代，因此它们可以被认为是脱机目录。脱机目录通常用于发行只读信息。

一个联机目录是可以通过计算机网络进行电子访问与更新的目录，网络可以是局域网(LAN)、广域网(WAN)，甚至是因特网。许多脱机目录有一个联机或电子副本。电话公司在Web上发行它们的清单以及电话黄页(电话号码簿上按营业范围分类的部分，用黄纸印刷——译者注)，并提供了一个易于使用的界面。

其他类型的联机目录包括应用目录和专用任务目录。应用目录依赖于一个软件应用——例如Lotus Notes或Novell GroupWise，二者均使用为应用专门需求而设计的专用目录。

专用任务目录可由任意应用使用，但它依赖于为一个有限范围目标而存储的数据。这种类型的目录的一个非常好的例子是因特网使用的域名系统(Domain Name System，DNS)。虽然许多不同的应用使用DNS，但目录中含有的信息只能用于明确任务——名称与IP地址解析。

网络目录是联机目录，存储有关网络资源与服务的信息。通常，这些信息包括用户信息、安全数据，以及可用的服务清单，例如打印机和发行服务。

Active Directory被认为是一个网络目录，但是它允许存储其他数据。例如，Microsoft在Active Directory中已经实现了Windows 2000的动态DNS服务。通过使用一个标准化的数据模型和称为LDAP(稍后会更多地介绍)的程序接口，任何应用程序都可以使用目录信息。应用程序甚至可以修改数据模型，以含有用于特殊目的的新的信息种类。

1.3 什么是目录服务

当被问到："什么是目录服务"时，许多人会回答："为你查找人们电话号码的态度友好的电话接线员"。当然这是一个正确的答案。如果目录是实际数据——人与电话号码的列表——那么接线员和打电话给他们的方法就是目录服务。在电子世界中与之不同的地方不仅如此，图1-2显示了传统电话目录服务和电子目录服务之间的对比。

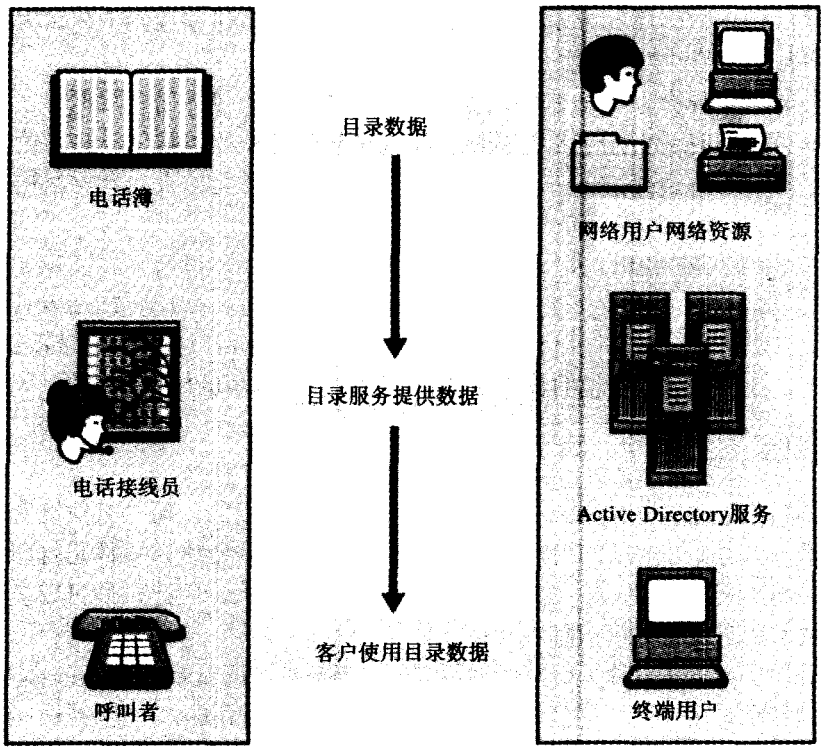


图1-2　目录与目录服务

目录服务为用户和应用程序提供目录信息的存储与提取。目录服务必须解决的问题是性能、安全、可靠性、可用性和易于使用。(“易于使用”意味着开发者不需要进行大量难度较大的编程就可以编写访问目录信息的应用)。

考虑下面一个例子。大部分大型购物商场都有广告亭，按照商场所卖产品的类型，分类列出了商场中的货物。商场提供的服务，例如休息室、电话、保安和报刊亭，也被列出并有地图指示。这些广告亭就是实际的目录。现在想像一下商场只有一个目录广告亭，它位于商场的中心位置。许多人会走向广告亭，每个人都想在同一时间得到信息。如果广告亭非常小，而且上面的文字难于阅读，会怎么样？人们会花费许多时间查找并发现某个只卖袜子的专卖店。(非常奇怪吧！我的女朋友就非常喜欢这种商店)。想像一下人们正在努力阅读商场目录时，一个管理员走过来将广告亭拿走更新或清除。这无可否认是一个非常愚蠢的例子，但它表明了目录服务中对性能、可靠性、可用性和易于使用的需要。通过在购物中心的周围放置很多广告亭并让它们易于理解，商场可以容纳许许多多的购物者。

网络目录提供了相似的解决方案。为了确保高可用性，目录信息被复制到许多服务器上(电子“广告亭”)。访问目录信息的计算机可以从最近的服务器获取信息，从而导致性能的提高。由于可以用多种方式收集并提供目录信息，最终用户易于存取访问它。

目录服务令开发者、管理员和最终用户的任务变得简单。如果你是一名开发者，目录服务

易于存储并查找有关网络资源的信息。应用可以将信息发布并存储在网络目录中，并由其他应用使用。网络管理员得到的好处包括增加了安全性以及易于管理，最为重要的是，通过利用应用之间共享的数据以及不再需要记住目录中的特定资源项——例如去往大厅的打印机的网络路径，用户从一个通用安全模型中受益(避免使用多个口令)。

1.4 目录简史

网络目录为用户、信息技术专业人员和开发者带来的许多好处显而易见。这些好处是从何而来的，尤其是Active Directory是如何发展的，完全与网络目录发展密不可分，尤其是与DNS、X.500和LDAP三种早期目录服务的发展与进步密不可分。图1-3显示了在目录发展史上一些重大事件的时间坐标。

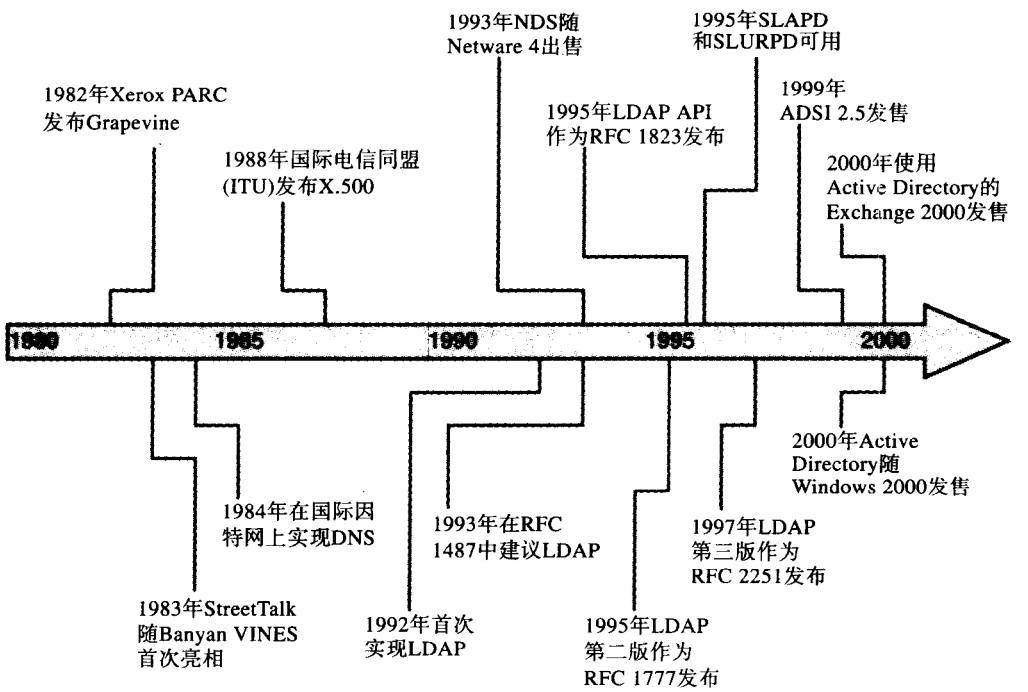


图1-3 目录发展史

1.4.1 域名系统

域名系统(Domain Name System，DNS)作为一个首先使用的重要的电子目录，在因特网上将域名和与其对应的难于记忆的因特网(IP)地址进行匹配。就像人们拥有电话号码一样，在TCP/IP网络上的计算机有IP地址。为了让一台计算机能够与网络上的其他计算机通信，这台计算机必须知道其他计算机的IP地址。DNS使用的信息在本地创建，并在全球发布。我可以将一台新计算机

添加到网络中，将它命名为copper1，并告诉我的DNS服务器新计算机的名称和IP地址。

由于在因特网上有成千上万的计算机，复制全部信息到所有的DNS服务器是非常浪费资源的。实际上，当一个DNS服务器无法理解所给予的名字时，它求助于网络链上的另外一个DNS服务器。最终，系统将发现负责coppersoftware.com域的服务器，要求它查找copper1并返回IP地址。由于DNS具有不可思议的强大功能，通过指定网络的完整域名copper1.coppersoftware.com，连接到因特网上的所有计算机都可以与copper1通信。DNS是专用任务目录的一个很好例子。不必奇怪，Microsoft在Active Directory内部实现了自己的DNS版本。

注意 如果你自己建立了一个启用Active Directory的网络，完全了解DNS和Active Directory是如何一起工作的非常有用，这有助于避免许多常见错误。请参考Microsoft出版社出版的由David Iseminger编写的《Windows 2000 Server Resource Kit》和《Active Directory Services for Microsoft Windows 2000 Technical Reference》。另外，对于常见的Active Directory/DNS建立设置问题，参阅Microsoft位于http://support.microsoft.com/support/win2000/dns.asp网址上的技术支持文档。

1.4.2 X.500目录服务

网络应用的蓬勃发展增加了对实现通用编程接口的标准化目录的需求，多个应用程序可以访问同样的信息。这个新纪元开始于20世纪80年代中期，几个大型企业和教学机构寻求一种通用目录解决方案。在1988年，国际电信同盟(ITU)发布了x.500目录服务建议，并定义了目录访问协议(Directory Access Protocol，DAP)。这个标准是由国际电话与电报顾问委员会(International Telephone and Telegraph Consultative Committee，CCITT，现在称为ITU-T)与国际标准化组织(International Standardization Organization，ISO)通力合作制订的，形成一个全球目录服务标准。X.500标准在1993年被更新，并于1997年再次更新。

X.500与DAP从一开始就面向全面包容的全局目录服务，但它们被认为是难于实现的，没有得到广泛的商界认可接受。另外一个限制因素是下面一个事实：X.500依赖于开放式系统互联(Open System Interconnect，OSI)网络协议，而不是当前流行的基于TCP/IP的因特网模型。虽然x.500是惟一具有分布式本性并且对目录具有强大的查找功能的标准，但获得这些优点需要大量的计算资源开销。

当软件商看到X.500时，他们意识到接口的复杂性令人畏而止步，并没有看到这个强大而开放的标准所带来的潜在好处。软件商没有意识到全球目录服务的重要性，专用目录只是简单地随着使用它们的软件得到发展。图1-4显示了一个X.500系统的组件。

技术继承

使用X.500开发个人计算应用程序是一个大趋势：建立在先前技术之上，进行了技术改进，并保留客户的当前设备投资。尽管Windows是从MS-DOS发展而来的，而MS-DOS又是从CP/M发展而来的，但X.500标准从本质上说却是从零开始的，要求实现者编写大量的新代码。当新技术明显不同于由绝大多数已安装系统所使用的技术时，不管它们具有多大好处，都要承受缓慢采用的过程。第一版的Windows NT在1993年几乎很少

有人问津，尽管Microsoft极力推动软件开发者采用NT的32位编程接口，这是由开发者所熟悉的16位Windows应用程序接口适度地升级而来的。Microsoft在它的整个发展历史中，已经领会了循序渐进地推动已安装系统和软件开发者逐步采用新技术的重要性。Active Directory也不例外，完全建立在Windows NT以及诸如Exchange服务器和Microsoft站点服务器等产品的技术之上。

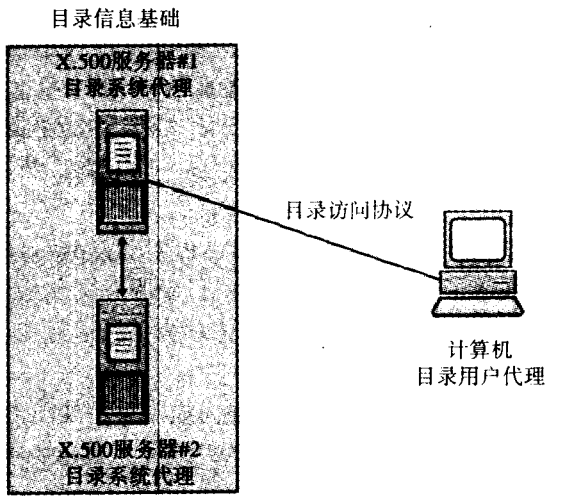


图1-4 X.500组件

1.4.3 LDAP的出现

早期版本的合作应用程序例如Microsoft Mail和Lotus Notes使用了目录，但是在某种意义上它们是专用目录，只有在特定情形下才能由其他客户互用。灵活性、安全性和复制功能都非常弱或根本不存在。像Banyan VINES、Microsoft Windows NT和Novell NetWare这样的网络操作系统开始实现各种形式的目录去管理用户和网络资源。NetWare拥有Bindery，Windows NT具有安全账户管理器(SAM)数据库。Bindery开创了一个被称为StreetTalk的集成化目录服务，它具有创新性，但从未收到广泛的商业成功。每个目录存储有关网络用户和资源的信息，但是每个目录都针对安全与验证做出调整，这是当时网络操作系统的主要需求。

到1993年，随着X.500第二版获得少量商业利润，密歇根州立大学(采用早期X.500的站点)的一个研究组正在开发X.500中复杂DAP接口的替代品，目标是为X.500目录创建一个较为简单的访问协议。这个研究小组创建了一个协议，新协议废除了许多妨碍开发者使用的X.500元素，特别是废除了OSI网络模型，取消了许多DAP未使用的函数。这个带有倾向性且有意义的DAP版本最初称为DIXIE(RFC 1249)，后来称为轻量目录访问协议(Lightweight Directory Access Protocol，LDAP)。虽然第一版LDAP是复杂X.500 DAP的一个巨大改进，但花费了一些时间才让商家认可。

直到LDAP第二版发布(在RFC 1487中被推荐使用，在RFC 1777中作为标准推出)，LDAP和开放目录服务才真正起步。

注意 LDAP的正式定义包含在称为《Requests For Comments》的文档中，或简称RFC。RFC已经发展成为标准化Internet使用技术的一种手段。许多技术和说明，从DNS到如何传递电子邮件，都由RFC文档定义。因特网工程工作小组(internet engineering task force，Http://www.ietf.org)检查并维护RFC文档。在第三章含有与LDAP有关的RFC清单。

最初，LDAP只是作为X.500 DAP的替代品。然而，由于LDAP定义了协议，开发者可以自由实现他们自己的目录服务，只要符合LDAP的要求即可，而不需要X.500。这并不奇怪，LDAP第一次是在密歇根州立大学实现的，在1995年开发成功SLAPD(独立运行的LDAP后台进程)和它的复制伙伴SLURPD(独立运行的LDAP更新复制后台进程)。SLAPD是一个简单的LDAP服务器，能够与几个用作目录的不同数据库通信。SLURPD是一个程序，将一个目录数据库中的更改复制到其他用作目录服务器的计算机。

对LDAP成功同样起着重要作用的是C语言LDAP应用程序接口(或API)的开发。这个API在RFC 1823中定义，包括一组开发者可以用于访问目录服务的函数。Windows NT与Windows 2000作为操作系统的组成部分支持这个API，上述系统允许运行在这些平台上的应用访问基于LDAP的目录。

LDAP的部分组件已经经过多年改进提高，面向提供可扩展能力做了大量工作。LDAP的最新版本被称为LDAPv3，最初于1997年作为RFC 2251发布，这个版本是LDAPv2的超集，包括一些新特性，例如扩展控件以及展示目录数据定义或模式的能力。LDAPv3的一个重要特性是LDAP目录展示所提供服务有关信息的能力。许多商家在第二版时就支持LDAP完成这些工作，这些v2级上的LDAP混有来自LDAPv3的一些特性。Active Directory支持带有一些自定义扩展能力的LDAPv2和LDAPv3，这些自定义扩展称为控件。

注意 有趣的是用作网络消息的ITU标准X.400遭遇了与X.500相似的命运。虽然LDAP在很大程度上替代了X.500，但是简单邮件传输协议(Simple Mail Transfer Protocol，SMTP)变为Internet电子邮件的事实标准。

1.5 目录的现状

大规模目录、远程站点之间的高可连接性、以及提供可用的开放与可扩展程序接口的需求，推动诸如Microsoft这样的商家支持LDAP的使用，并且基于LDAP创建目录解决方案。由来自密歇根州立大学的一些LDAP开发者所领导的Netscape推出了它自己的Netscape目录服务器产品。Novell在1990年已经开发了一个称之为Novell目录服务(Novell Directory Services，NDS)的专用网络目录，开始使用LDAP，并最终采用了一些X.500特性。Microsoft在它的一些应用产品中实现了对LDAP服务器的支持，最为著名的是Exchange Server 5和Microsoft Site Server 3。Exchange的最新版本Exchange 2000服务器使用Active Directory替换了原先的目录结构。许多产品集成了对基于LDAP目录访问的支持，其中包括大量的电子邮件应用，例如Microsoft Outlook和Lotus Notes。Windows与支持基于LDAP目录的简单地址簿应用程序一同发售。

网络目录的发展趋势朝着强化独立的应用目录和网络操作系统目录前进，同时提供与后台操作系统的紧密集成。这种集成承诺降低网络管理员的工作量，并使终端用户具有更好的经验，它还为开发者创建新类型的网络应用创造了机会。存储在目录中的数据变为普遍可用的且易于管理，开发者可以自由地实现自己的数据存储和安全方法，并且能够将精力完全集中到网络应用的功能上。

1.6 Active Directory特性

Active Directory是一个真正的网络目录服务，含有传统目录服务所不具有的特性和优点。下面是Active Directory主要特性的概述：

- 层次性。包含在Active Directory中的信息可以分层组织。例如，管理员可以遵循公司使用的相同组织层次安排网络用户。Active Directory使用称为域、树和森林的结构来表示不同的数据分区，全部数据都在同一个目录之中。我将在第2章详细介绍这些结构。
- 可升级性。Active Directory基于域模型。每个域由一个或多个连接在一起的工作站和服务器组成。被称为域控制器(domain controllers，DC)的特殊服务器保存目录数据的本地拷贝，并让该拷贝对客户可用。随着一个组织的增长，包含在目录中的数据也随之扩张，可以添加更多的域以满足企业的需求。我将在第2章略微谈到Active Directory的升级能力。
- 复制性。包含在Active Directory中的信息被复制到组织内部的所有域控制器上。每个域可以有多个GC用于容错和负载均衡。在第2章我将说明复制以及程序员应该牢记的相关话题。
- 互用性。将LDAP用作目录访问协议确保了大量用户可以使用存储在目录中的信息。Active Directory服务接口(ADSI)使用LDAP从目录得到信息并将信息存入目录。ADSI基于组件对象模型(Component Object Model，COM)，并且允许使用脚本。在第3章，我将提供LDAP和ADSI编程的概述。贯穿本书，代码示例将为你展示更为详细的例子。
- 安全性。可以分别对Active Directory中的每个对象进行安全控制访问。目录对象可以有多个安全级别，允许特定用户具有更新一些信息的能力，而不是更改全部信息。在Active Directory中的安全与Windows 2000总体安全模型紧密地集成，后者使用Kerberos第五版验证协议。在讨论各种编程技术时，我在全书中都将略微谈到安全话题。
- 集成性。Active Directory在本质上与Windows 2000融为一体。服务器管理工具依赖于Active Directory，并且终端用户将会注意到使用基于操作系统通用用户接口的应用含有引用，这些引用访问和使用Active Directory中的信息。在第八章，我将讨论一些Active Directory提供的用户接口组件，在创建应用时，开发者可以使用它们。
- 可扩展性。Active Directory提供了许多对象类和大量的属性。每个类，例如计算机、用户或打印机，都表示一个数据对象，类还说明该类对象可用的属性。开发者可以添加自己的对象类，甚至可以向现有类中添加新属性。我在第9章讨论扩展Active Directory。

很明显，Microsoft致力于正确的目录发展方向——Active Directory。单单可扩展性、安全性和集成性就足以保证开发者和网络管理员具有精密检查的可能性。在下一章，将深入研究Active Directory的细节。