GOTOP

Windows Server 2003

Active Directory 配置指南

- Active Directory、域、林
- 用户与群的管理、利用群管理用户的工作环境
- 用户的权限分配原则、安全性原则
- 软件部署、软件包装、软件限制
- 域信任、控制器与 Active Directory 复制
- 操作主机与域修复、Active Directory 数据库的维护

戴有炜 编著

清华大学出版社

Windows Server 2003
Active Directory 配置指南

戴有炜　编著

清 华 大 学 出 版 社
北　京

内 容 提 要

本书作者戴有炜先生是中国台湾地区的微软资深顾问、微软认证讲师、微软认证系统工程师，编写过多本关于 Windows 操作系统的畅销图书。

本书采用图文并茂的方式，结合完整清晰的操作步骤，全面介绍了 Windows Server 2003 Active Directory 的配置方法和管理技巧。主要内容包括：Active Directory 概论、建立 Windows Server 2003 域、域用户与组账户的管理、组策略、利用组策略部署软件、软件限制策略、建立域树与林、域信任关系、Active Directory 的复制、操作主机的管理、Active Directory 数据库的维护、将资源公布到 Active Directory、自动信任根 CA、Active Directory 与防火墙、自定义 MMC 等。

本书主要面向广大计算机爱好者，也可供网络专业人员借鉴和参考，同时也适合作为 MCSA/MCSE 认证考试的参考书籍。

版 权 声 明

北京市版权局著作权合同登记号　图字：01-2004-1116

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目（CIP）数据

Windows Server 2003 Active Directory 配置指南/戴有炜编著
—北京：清华大学出版社，2004.4

ISBN 7-302-08661-3

I. W…　II. 戴…　III. 服务器—操作系统（软件），Windows Server 2003—指南
IV. TP316.86-62

中国版本图书馆 CIP 数据核字（2004）第 047405 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社总机：010-62770175　　**客户服务**：010-62776969

组稿编辑：科海
文稿编辑：陈轶 陈洁
封面设计：杨月静
版式设计：科海
印 刷 者：北京科普瑞印刷有限责任公司
发 行 者：新华书店总店北京发行所
开　　本：787×1092　1/16　　**印张**：23　　**字数**：560 千字
版　　次：2004 年 6 月第 1 版　2004 年 6 月第 1 次印刷
书　　号：ISBN 7-302-08661-3/TP・6212
印　　数：1 ~ 5000
定　　价：39.00 元

出 版 说 明

《Windows Server 2003 用户管理指南》、《Windows Server 2003 网络专业指南》和《Windows Server 2003 Active Directory 配置指南》是我国台湾地区的资深 Windows 培训专家和咨询顾问戴有炜先生的最新力作。

戴有炜先生历任微软认证讲师、微软认证系统工程师、微软资深顾问、综合生活股份有限公司技术支援部技术总监和教育训练中心讲师，拥有十几年使用、咨询和讲授 Windows 操作系统的成功经验，并于 1997 年编撰出版了《Windows NT Server 4.0 专业指南》和《Windows NT Server 4.0 实用指南》，于 2000 年推出了升级版《Windows 2000 网络实用指南》和《Windows 2000 网络专业指南》，这 4 种图书的简体中文版销售累计超过 30 万册，被誉为 Windows NT 4.0 和 Windows 2000 Server 的一般用户和管理员的福音书。

本次推出的 Windows Server 2003 三卷本，秉承了作者一贯的写作风格和体例，凭借丰富的教学与咨询经验，完全从读者使用和学习的角度，以详实的步骤与精到的说明教读者迅速掌握 Windows Server 2003，充分考虑读者操作时可能发生的问题，并提供解决方案，还适应 MCSA/MCSE 认证考试的需求，无疑是最佳实践参考书籍。

- 《Windows Server 2003 用户管理指南》的主要内容是：Windows Server 2003 基本概念、安装 Windows Server 2003、熟悉 Windows Server 2003 环境、创建 Windows Server 2003 域、用户账户的管理、组账户的管理、NTFS 的数据管理功能、访问网络上的文件、分布式文件系统、打印机的设置、设置用户的工作环境、安全设置与审核资源的使用、监控资源的访问行为、注册表编辑器、磁盘系统的管理、自动安装与磁盘复制、系统启动的疑难排除。
- 《Windows Server 2003 网络专业指南》的主要内容是：Windows Server 2003 的网络功能，利用 DHCP 自动分配 IP 地址，解析 NETBIOS 名称，PKI、IPSec 与网络安全，远程访问与 VPN，RADIUS 与 IAS 服务器，Windows Server 2003 路由器，NAT 与基本防火墙，SSL 网络安全连接，终端服务器、IIS 网站、FTP 站点、电子邮件服务器、NNTP 服务器的安装与设置，远程安装服务等。
- 《Windows Server 2003 Active Directory 配置指南》的主要内容是：Active Directory 概论、建立 Windows Server 2003 域、域用户与组账户的管理、组策略、利用组策略部署软件、软件限制策略、建立域树与林、域信任关系、Active Directory 的复制、操作主机的管理、Active Directory 数据库的维护、将资源公布到 Active Directory、自动信任根 CA、Active Directory 与防火墙、自定义 MMC 等。

Windows NT Server 系列和 Windows 2000 系列出版以来，一直受到广大读者的好评和厚爱，希望本次推出的 Windows Server 2003 系列也能对用户有所帮助，继续得到读者朋友的支持。

序

首先要感谢读者长期以来的支持与爱护！本书仍然采用我一贯的写作风格，也就是完全站在读者的角度考虑问题，并且以实用的观点来编写这三本 Windows Server 2003 的书籍。我花费相当多的时间不断测试与验证书中所叙述的内容，并融合多年的教学经验，然后以最容易让您理解的方式将其写到书内。书中完整和清晰的操作步骤，让您能够轻松地安装与使用 Windows Server 2003。

长期以来，对需要参加 MCSA/MCSE 认证考试的读者来说，研读官方的原文教材是一件苦差事，读起来似懂非懂又不知如何操作，而其他引进的英文书籍也一样难以消化，中文翻译书又大都翻译的很“英式中文”，还不如看原版书。现在这些读者有福了，本书特别考虑到 MCSA/MCSE 认证考试的需求，是非常适合这些读者阅读的中文参考书籍，尤其是在实践方面。

本套丛书包括《Windows Server 2003 用户管理指南》、《Windows Server 2003 网络专业指南》、《Windows Server 2003 Active Directory 配置指南》3 本，内容丰富详实，相信这几本书，仍然会不辜负您的期望，在您学习 Windows Server 2003 时，将给予您最大的帮助。

感谢所有让这本书能够顺利出版的朋友们，特别是花费很多精力帮我校稿的李尚白先生，还有“综合生活股份有限公司”，这家专门承接微软技术支持项目的公司，为我提供了各种最新、最快的资源与各种测试设备。

戴有炜

2004 年 4 月

目　录

第1章　Active Directory概论 1

1.1　Active Directory的基本概念 2

1.1.1　适用范围 2

1.1.2　命名空间 2

1.1.3　对象与属性 3

1.1.4　容器与组织单位 3

1.1.5　域树 4

1.1.6　信任 5

1.1.7　林 6

1.1.8　架构 7

1.1.9　域控制器与Active Directory的复制 7

1.1.10　轻型目录访问协议 8

1.1.11　全局编录 9

1.1.12　站点 10

1.2　域功能与林功能 11

1.2.1　域功能的等级 11

1.2.2　林功能等级 12

1.3　目录分区 12

第2章　建立Windows Server 2003域 15

2.1　建立域前的准备工作 16

2.1.1　DNS域名 16

2.1.2　DNS服务器 16

2.1.3　足够的硬盘空间 18

2.1.4　一个NTFS硬盘分区 19

2.2　建立域 19

2.2.1　建立网络中的第一台域控制器 20

2.2.2　添加额外的域控制器 33

2.3　自动安装Active Directory 40

2.4　确认Active Directory是否正常 41

2.4.1　检查DNS服务器内的记录是否完备 41

2.4.2　检查Active Directory数据库文件与SYSVOL文件夹 48

2.4.3　新增加的管理工具 50

2.4.4　查看事件日志文件 50

2.5 删除Active Directory 51
第3章 域用户与组账户的管理 57
3.1 域用户账户 58
3.1.1 组织单位 58
3.1.2 用户登录账户 58
3.1.3 建立UPN的后缀 60
3.1.4 账户的一般管理工作 61
3.1.5 查找用户账户 63
3.1.6 域控制器之间数据的复制 65
3.2 一次同时添加多个用户账户 66
3.2.1 利用CSVDE来添加用户账户 67
3.2.2 利用LDIFDE来添加、修改、删除用户账户 68
3.3 域组账户 69
3.4 提升域功能级别 71
3.5 组的使用准则 72
3.5.1 A，G，DL，P策略 72
3.5.2 A，G，G，DL，P策略 73
3.5.3 A，G，U，DL，P策略 73
3.5.4 A，G，G，U，DL，P策略 74
第4章 组策略 75
4.1 组策略概论 76
4.1.1 组策略的功能 76
4.1.2 组策略对象 77
4.1.3 组策略的应用时机 80
4.2 组策略实例 82
4.2.1 组策略实例1：计算机配置 82
4.2.2 组策略实例2：用户配置 84
4.3 组策略的处理规则 87
4.3.1 一般的继承与处理规则 87
4.3.2 例外的继承配置 88
4.3.3 特殊处理的设置 90
4.3.4 改变管理GPO的域控制器 95
4.4 利用组策略来管理用户环境 97
4.4.1 管理模板策略 98
4.4.2 账户策略 99
4.4.3 用户权限分配策略 103
4.4.4 安全选项策略 104

4.4.5　登录/注销、启动/关机脚本 105
4.4.6　文件夹重定向 111
4.5　组策略的委派管理 115
第5章　利用组策略部署软件 121
5.1　软件部署概论 122
5.2　将软件发布给用户 123
5.2.1　发布软件 123
5.2.2　安装被发布的软件 127
5.2.3　测试自动修复软件的功能 128
5.2.4　取消发布软件 129
5.3　将软件指派给用户或计算机 130
5.4　软件升级与重新部署 132
5.4.1　软件升级 132
5.4.2　重新部署 136
5.5　修改部署的软件 138
5.6　发布“非-MSI”的软件 144
5.7　软件部署的其他设置 147
5.8　软件包装程序 150
第6章　软件限制策略 153
6.1　软件限制策略概论 154
6.1.1　软件限制策略的优先级 154
6.1.2　软件限制策略的规则 154
6.2　启用软件限制策略 156
6.2.1　建立哈希规则 157
6.2.2　建立路径规则 159
6.2.3　建立证书规则 162
6.2.4　建立Internet区域规则 165
第7章　建立域树与林 167
7.1　建立第一个域 168
7.2　建立子域 169
7.3　建立第二个域树 177
7.4　改变域控制器的计算机名 190
第8章　域信任关系 193
8.1　域信任基本概念 194
8.1.1　信任域与被信任域 194

8.1.2 跨域访问资源的流程 194
8.1.3 信任的种类 197
8.2 建立信任 200
8.2.1 建立信任前的注意事项 200
8.2.2 建立快捷方式信任 202
8.2.3 建立林信任 208
8.2.4 建立与Windows NT 4.0域的外部信任 218
8.3 管理与删除信任 220
8.3.1 信任的管理 220
8.3.2 信任的删除 221
第9章 Active Directory的复制 223
9.1 站点与Active Directory的复制 224
9.1.1 同一个站点之间的复制 225
9.1.2 不同站点之间的复制 227
9.1.3 目录分区 227
9.1.4 复制通信协议 228
9.2 默认站点的管理 228
9.2.1 默认的站点 228
9.2.2 Servers文件夹与复制配置 229
9.3 利用站点来管理Active Directory的复制 232
9.3.1 建立站点与子网络 233
9.3.2 建立站点链接 236
9.3.3 将域控制器转移到所属的站点 237
9.3.4 指定“首选bridgehead服务器” 239
9.3.5 站点链接与Active Directory复制配置 240
9.3.6 站点链接桥接器 242
9.3.7 站点链接桥的两个实例讨论 244
9.4 全局编录的功能 246
9.4.1 全局编录 246
9.4.2 全局编录的功能 248
9.4.3 通用组成员缓存 250
9.5 解决Active Directory复制冲突的问题 252
9.5.1 属性戳 252
9.5.2 冲突的种类 252
第10章 操作主机的管理 257
10.1 操作主机的功能 258
10.1.1 架构主机 258

10.1.2　域命名主机 258
10.1.3　RID主机 259
10.1.4　PDC模拟主机 259
10.1.5　基础结构主机 262
10.2　找出操作主机角色的扮演者 262
10.2.1　找出架构主机 263
10.2.2　找出域命名主机 265
10.2.3　找出RID、PDC仿真器与基础结构主机 266
10.3　传送操作主机角色的实例 266
10.4　占用操作主机角色的实例 270
10.4.1　操作主机故障所造成的影响 270
10.4.2　占用操作主机角色实例1 272
10.4.3　占用操作主机角色实例2 275
第11章　Active Directory数据库的维护 281
11.1　Active Directory数据库简介 282
11.2　备份Active Directory数据库 283
11.3　还原Active Directory数据库 284
11.3.1　标准还原 285
11.3.2　强制性还原 287
11.3.3　主要还原 291
11.4　Active Directory数据库的转移与整理 292
11.4.1　转移Active Directory数据库文件 292
11.4.2　整理Active Directory数据库 295
11.5　重设“目录服务还原模式”的系统管理员密码 298
第12章　将资源公布到Active Directory 299
12.1　将共享文件夹公布到Active Directory 300
12.2　查找Active Directory内的资源 302
12.3　公布共享打印机 305
12.3.1　公布打印机 305
12.3.2　利用打印机位置来查找打印机 308
附录A　自动信任根CA 313
A.1　自动信任CA的设置准则 314
A.2　自动信任内部的CA 314
A.3　自动信任外部的CA 320

附录B Active Directory与防火墙 329

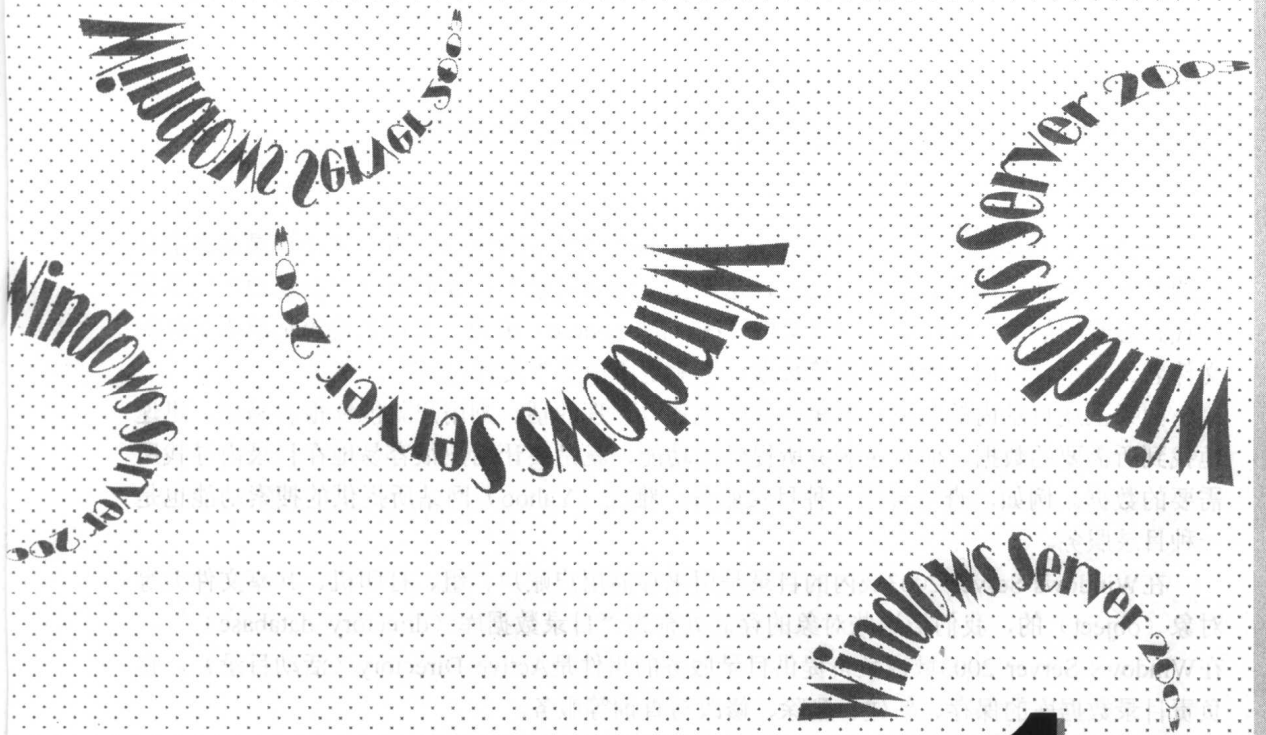
B.1 相关的连接端口 330

B.2 IPSec与VPN连接端口 334

附录C 自定义MMC 337

C.1 MMC与工作台 338

C.2 MMC模式 351



第 1 章

Active Directory 概论

在Windows Server 2003的网络环境中，Active Directory提供组织、管理与控制网络资源的各种功能。

本章主要介绍的内容包括：

- Active Directory的基本概念
- 域功能与林功能
- 目录分区

1.1 Active Directory的基本概念

何谓目录（directory）？以我们日常生活中所用的电话簿来说，电话簿内记录着亲朋好友的姓名、电话、地址、生日等信息，这就是“电话目录”，我们可以很容易地从电话簿内找到想要的信息；以计算机中的文件系统（file system）来说，文件系统内记录着文件的文件名、大小、日期、存储位置等数据，这就是所谓的“文件目录”。

如果上述目录内的数据能够事先系统地加以整理的话，则用户就能够很容易地、迅速地找到所需要的数据，而目录服务所提供的功能，就是要让用户很容易地在目录内寻找所需要的数据。例如，查号台是一种目录服务；雅虎（Yahoo）网站所提供的搜索功能也是一种目录服务。

在Windows Server 2003域内的目录是用来存储用户账户、组、打印机、共享文件夹等对象（object）的，我们把这些对象的存储处称为“目录数据库（directory database）”。在Windows Server 2003域内负责提供目录服务的组件是Active Directory（活动目录），它负责目录数据库的保存、新建、删除、修改与查询等服务。

1.1.1 适用范围

Active Directory的适用范围（Scope）非常广泛，小自一台计算机、一个小型局域网（LAN），大至数个广域网（WAN）的结合。它可以包含此范围中的所有对象，例如文件、打印机、应用程序、服务器、域、用户账户等。

1.1.2 命名空间

所谓“命名空间（Namespace）”，就是一个界定好的区域（bounded area），在这块区域内，我们可以利用某个名称来找到与这个名称有关的信息。举例来说，一本电话簿就是一个“命名空间”，在这本电话簿内（界定好的区域），我们可以根据里面的人名，来找到这个人的电话、地址、生日等数据。又例如Windows XP内的文件系统就是一个“命名空间”，在这个文件系统内，我们可以利用文件名称找到这个文件的大小、修改日期和内容等数据。

在Windows Server 2003的域内，Active Directory就是一个“命名空间”。利用Active Directory，我们可以通过对象的名称找到与这个对象有关的所有信息。

在TCP/IP网络环境里，用域名系统（Domain Name System，DNS）来解析计算机名与IP地址的对应关系，也就是利用DNS来得知另外一台计算机的IP地址。Windows Server 2003的Active Directory与DNS紧密地整合在一起，它的域“命名空间”就是采用DNS的架构，而它的域名（domain name）也采用DNS的格式来命名，例如，可以将Windows Server 2003的域名命名为abc.com、xyz.com。

1.1.3 对象与属性

Windows Server 2003域内的资源以对象（object）的形式存在，如用户、计算机、打印机、应用程序等都是对象，而一个对象是通过“属性（attribute）”来描述其特征的，即对象本身是一些“属性”的集合。举例来说，假设要为用户“王乔治”建立一个账户，则必须新增一个对象类（object class）为“用户”的对象（也就是用户账户），然后在这个用户账户内输入“王乔治”的姓、名、电话号码、电子邮件、地址等数据，这其中的用户账户就是对象，而姓、名、电话号码等数据就是该对象的属性（参见表1-1）。

表1-1

对象	属性
用户（user）	姓
	名
	电话号码
	电子邮件
	城市
	省
	国家
	⋮

图1-1中的“王乔治”就是对象类为“用户（user）”的对象。

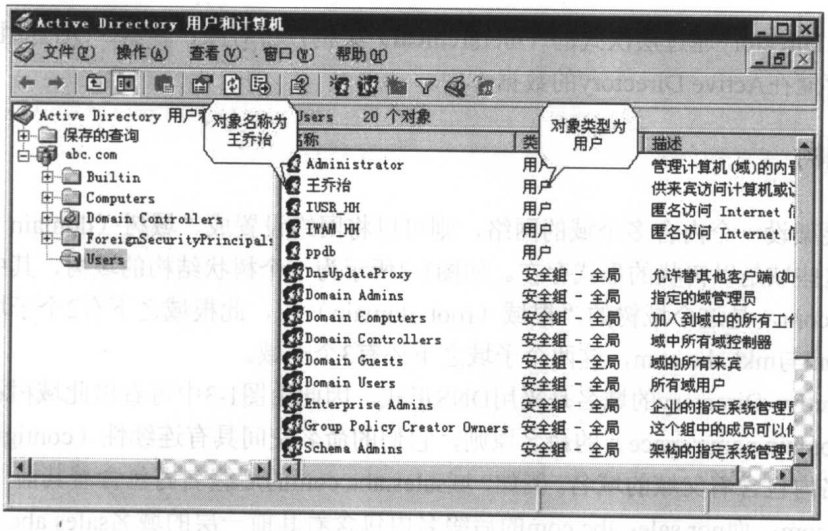


图 1-1

1.1.4 容器与组织单位

容器（Container）与对象相似，有自己的名称，也是一些属性的集合。容器内可以包

含其他的对象，如包含“用户”与“计算机”等对象，也可以包含其他的容器。而组织单位（Organization Units，OU）是Active Directory内一个比较特殊的容器，除了可以包含其他对象与OU之外，还有“组策略（group policy）”的功能。

图1-2所示的就是一个名称为“业务部”的OU，其中包含了两个“用户”对象、两个“计算机”对象和两个OU。

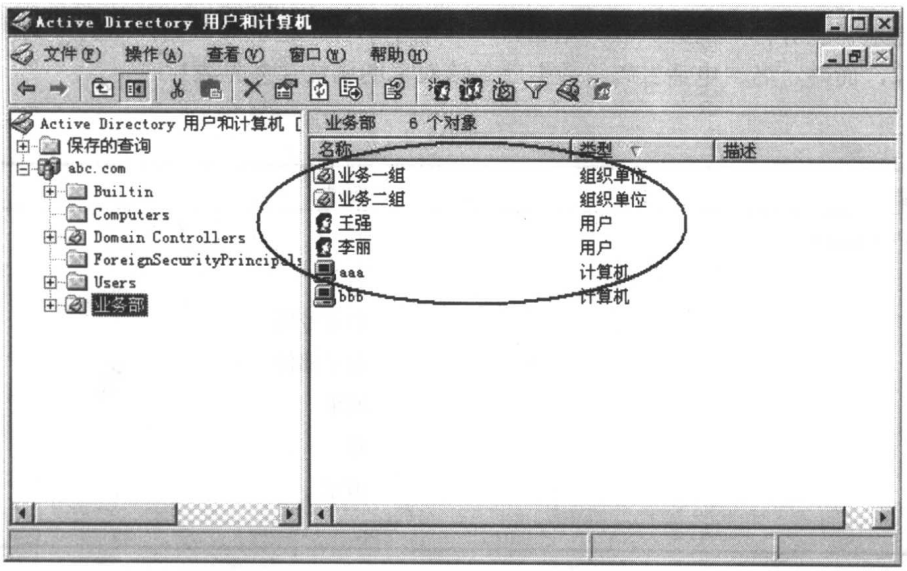


图 1-2

Active Directory通过层次式的（hierarchical）架构，将对象、容器、OU等组合在一起，并将它们存储在Active Directory的数据库中。

1.1.5 域树

假设要架设一个内含多个域的网络，则可以将网络设置成“域树（domain tree）”的架构，即这些域是以树状的形式存在。如图1-3所示为一个树状结构的域树，其中最上层的域名为abc.com，是这个域树的“根域（root domain）”，此根域之下有2个子域，分别是sales.abc.com与mkt.abc.com，这两个子域之下还有3个子域。

由于Active Directory的域名是采用DNS形式，因此由图1-3中可看出此域树符合DNS域名空间（domain name space）的命名原则，它们的命名空间具有连续性（contiguous），即子域的域名内包含着父域的域名。例如，域sales.abc.com的后缀名内包含着其前一层（父域）的域名abc.com；而nor.sales.abc.com的后缀名内包含着其前一层的域名sales.abc.com。

域树内的所有域共享一个Active Directory，即这个域树只有一个Active Directory。这个Active Directory内的数据分散地存储在各个域内，且每一个域内只存储该域内的数据，如该域内的用户账户、计算机账户等。Windows Server 2003将存储在各个域内的对象总称为Active Directory。

您可以将一个新的Windows Server 2003 域加入到现有的域树中。

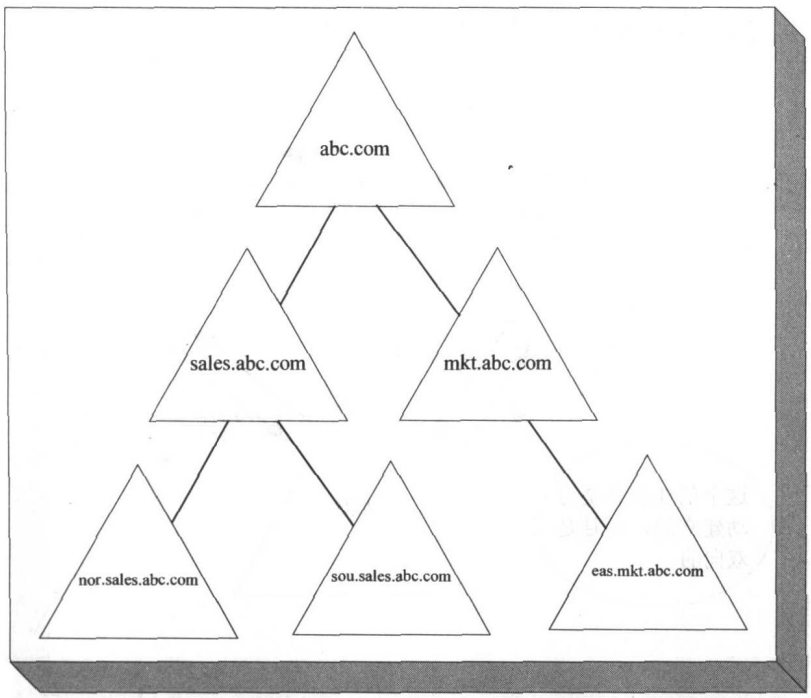


图 1-3

1.1.6 信任

两个域之间必须建立了“信任关系（trust relationship）”之后，才可以访问对方域内的资源。而任何一个Windows Server 2003域被加入到域树后，这个域会自动信任其前一层的父域，同时父域也会自动地信任这个新域，而且这些信任关系具备“双向传递性（two-way transitive）”。这个信任的功能是通过Kerberos安全协议（security protocol）来完成的，因此也被称为Kerberos信任。

Q **域A的用户登录到其所隶属的域后，这个用户可否访问B域内的资源？**

A 只要域B信任域A就可以了。

Q **甲用户隶属于域A，乙计算机隶属于域B，请问甲用户是否可利用乙计算机登录到域A呢？**

A 只要域B信任域A就可以了。

我们通过图1-4来解释双向传递性。图中域A信任域B（箭头由A指向B）、域B又信任域C，因此域A自动信任域C；另外域C信任域B（箭头由C指向B）、域B又信任域A，因此域C自动信任域A，结果是域A和域C之间自动地建立起双向的信任关系。这种因为传递性

而得到的信任关系，称为隐性的信任关系（implicit trust）。

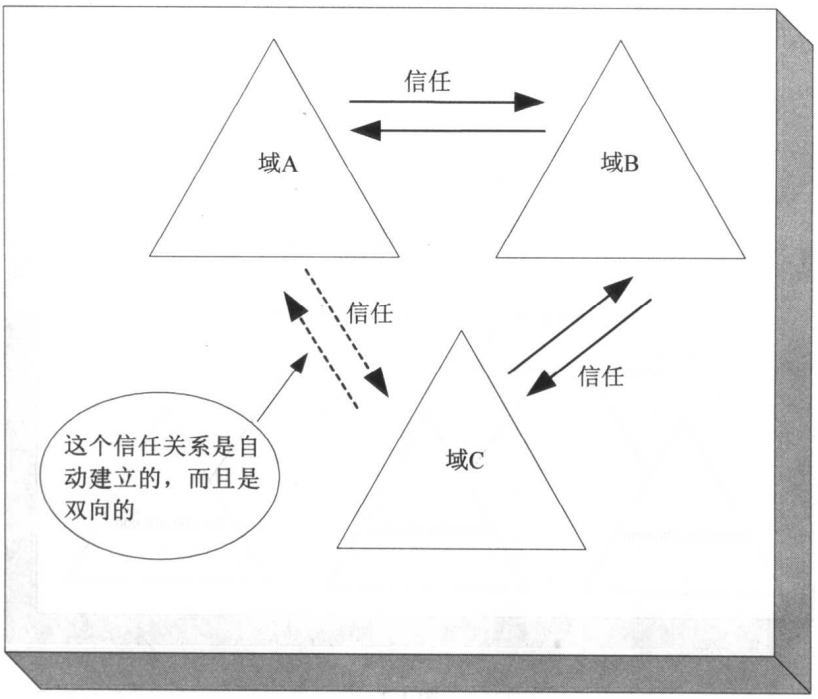


图 1-4

当任何一个Windows Server 2003域加入到域树后，会自动地双向信任这个域树内所有的域。因此只要拥有适当的权限，这个新域内的用户便可以访问其他域内的资源，同理，其他域内的用户也可以访问这个新域内的资源。

说明 也可以以手动的方式，在Windows Server 2003域与Windows NT域之间建立信任关系。

1.1.7 林

若一个网络内含多个域树，则可以将这些域树组合成为一个“林（forest）”，即林是由一或数个域树所组成，且每一个域树都有自己惟一的命名空间。如图1-5所示，其中一个域树内的每一个域名都是以abc.com结尾，而另一个则都是以xyz.com结尾。

所建立的第一个域树的根域就是整个林的根域（forest root domain），同时也是此域的域名，即林名称。图1-5中的abc.com是第一个域树的根域，也是整个林的根域，即林的名称为abc.com。

在建立林时，会自动建立根域（root domain）之间的具有双向传递性的信任关系。由于这种双向信任关系具备传递性，因此每一个域树中的所有域内的用户，只要拥有适当的权限就可以访问其他任何一个域树内的资源，也可以登录其他任何一个域树内的计算机。