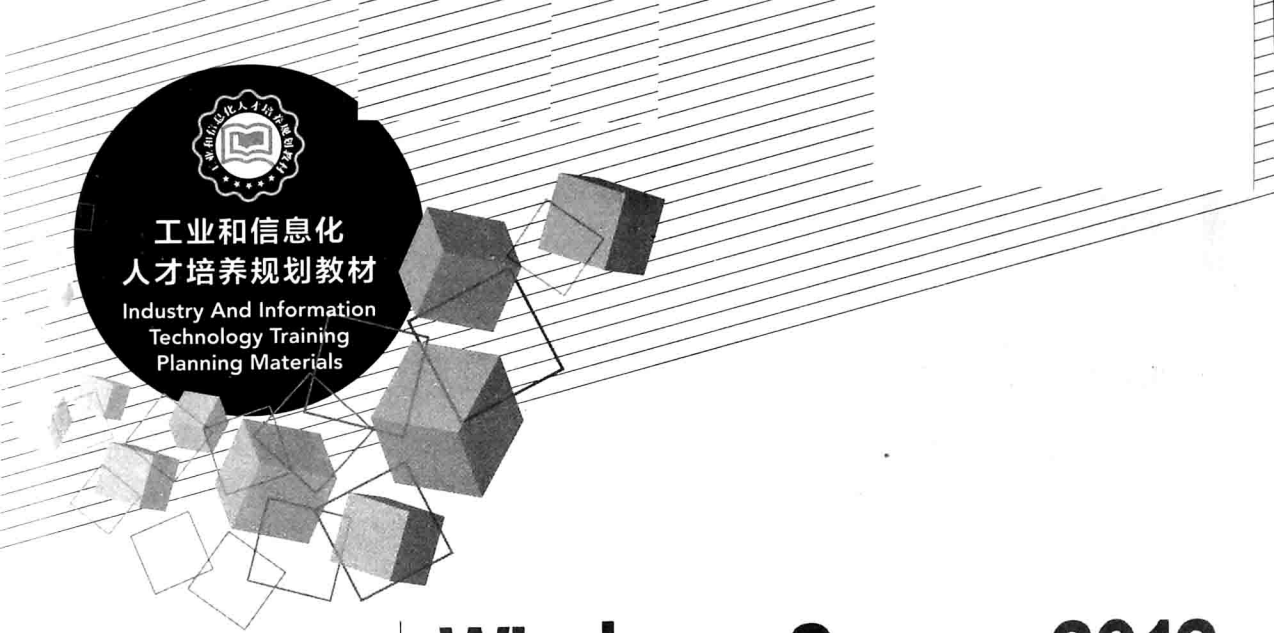
Windows Server 2012 活动目录项目式教程

Windows Server 2012 Active Directory

黄君羡 ◎ 编著

+ 以**实际的企业应用**为案例，展现活动目录的强大功能；
+ **26** 个项目，**7** 大部分，内容**由浅入深**；
+ 项目背景→相关知识→项目分析→项目操作→项目验证→习题与上机**展开教学**

人民邮电出版社
POSTS & TELECOM PRESS



Windows Server 2012 活动目录项目式教程

Windows Server 2012 Active Directory

黄君羡 ◎ 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

Windows Server 2012 活动目录项目式教程 / 黄君羡编著. -- 北京 : 人民邮电出版社, 2015.5
工业和信息化人才培养规划教材
ISBN 978-7-115-38297-9

Ⅰ. ①W… Ⅱ. ①黄… Ⅲ. ①Windows操作系统－网络服务器－教材 Ⅳ. ①TP316.86

中国版本图书馆CIP数据核字(2015)第014860号

内 容 提 要

本书围绕系统管理员、网络工程师等岗位对企业活动目录架构、实施与维护能力的要求，通过引入行业标准和职业岗位标准，以基于 Windows Server 2012 平台构建网络主流技术和主流产品为载体，引入企业应用需求将活动目录基础知识和服务架构融入到各项目中。书中涉及的项目均取材于真实企业网络建设工程项目。

本书适合计算机相关专业的学生使用，也可作为社会培训教材使用。

◆ 编　　著　黄君羡
责任编辑　范博涛
责任印制　杨林杰

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：17.25　　2015 年 5 月第 1 版
字数：427 千字　　2015 年 5 月北京第 1 次印刷

定价：42.00 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前言 PREFACE

活动目录服务是微软 Windows 操作系统最重要的服务，而 Windows Server 2012 是其最新的服务版本，经过两年多的市场应用，目前已经成为业界的主流应用版本。

活动目录的配置与管理是网络系统管理工程师、网络系统运维工程师的典型工作任务，是计算机网络技术高技能人才必须具备的核心技能，也是高职和应用型本科计算机网络类专业的一门重要专业核心课程。本书以培养读者活动目录的构建、应用、维护与管理技能为目标，详细介绍活动目录的构建、域用户和组的管理、域文件服务的构建、OU 与组策略的规划应用、活动目录的维护与管理等内容。

本书将以实际的企业应用案例为读者展现强大的活动目录功能，通过每一个工作任务的训练让读者快速掌握活动目录的操作技能，并通过举一反三，让读者快速的将 Windows Server 2012 活动目录的知识和技能与自身工作联系起来。

全书共计 26 个项目，以由简入难为原则，分为 7 个部分。

第 1 部分为活动目录概述，将详细介绍活动目录的基本概念、活动目录的逻辑结构、活动目录的物理结构等知识。

第 2 部分为虚拟化实战环境搭建，将详细介绍如何应用当前流行的 VMware 构建活动目录的网络和服务器实训环境。

第 3 部分为活动目录实战环境搭建，将详细介绍域控制服务器的创建；将用户和计算机加入到域；子域的加入；额外域控制器的创建；全局编录；域的删除等内容。

第 4 部分为管理域用户和组，将详细介绍域用户的导入与导出；个性化登录；用户数据漫游；将域成员设定为特定客户机的管理员；管理计算机加入到域的权限；组的管理与 AGUDLP 原则等内容。

第 5 部分为域文件服务的构建，将详细介绍活动目录环境下多用户隔离 FTP 服务的构建；DFS 分布式文件系统的配置与管理；DFS 文件服务的负载均衡与容灾等内容。

第 6 部分为 OU 与组策略的规划应用，将详细介绍 OU 的规划与权限管理；在 AD 中发布资源；组策略在计算机策略中的应用；组策略在用户策略中的应用；组策略在软件部署的应用；通过组策略管理用户环境；组策略的管理等内容。

第 7 部分为域的维护与管理，将详细介绍提升林和域的功能级别；部署多元化密码策略；操作主机角色的转移与强占；站点的创建与管理；AD 的备份与还原等内容。

活动目录是初级网络管理员和在校学生很少接触到的技术，因此学习起来会感觉抽象，不好理解，所以本书在每一个项目中力求通过【项目背景】引入企业应用需求，通过【相关知识】导入解决该应用所需的知识和技能，通过【项目分析】描述通过何种知识和技能可以解决本项目应用需求，通过【项目操作】详细呈现解决企业应用需求的过程，通过【项目验证】验证本项目的实施效果，最后通过【习题与上机】进行知识的复习和项目的实战巩固本项目对应的知识和技能。

本书若作为教学用书，参考学时为 48～64 学时，建议采用理论实践一体化教学模式，各项目的参考学时为 2 学时。

学时分配表

内容模块	课 程 内 容	学　时
第 1 部分	第一部分 活动目录概述	2～4
第 2 部分	项目 1 构建网络实训环境	1~2
第 3 部分	项目 2 构建林中的第一台域控制器	1~2
	项目 3 将用户和计算机加入到域	1~2
	项目 4 额外域控制器与全局编录的部署	2~3
	项目 5 子域的加入、域的删除	2~3
第 4 部分	项目 6 修改用户的密码策略	1~2
	项目 7 域用户的导出与导入	2~3
	项目 8 用户个性化登录、用户数据漫游	2~3
	项目 9 将域成员设定为客户机的管理员	1~2
	项目 10 管理将计算机加入域的权限	1~2
	项目 11 组的管理与 AGUDLP 原则	3~4
	项目 12 AGUDLP 项目实战	2~3
第 5 部分	项目 13 AD 环境下多用户隔离 FTP 实验	2~3
	项目 14 DFS 分布式文件系统的配置与管理（独立根目录）	1~2
	项目 15 DFS 分布式文件系统的配置与管理（域根目录）	2~3
第 6 部分	项目 16 OU 规划与权限管理	2~3
	项目 17 在 AD 中实现资源发布	2~3
	项目 18 通过组策略限制计算机无法使用系统的部分功能（计算机策略）	1~2
	项目 19 通过组策略限制用户无法使用系统的部分功能（用户策略）	1~2
	项目 20 通过组策略实现软件部署	2~3
	项目 21 通过组策略管理用户环境	2~3
	项目 22 组策略的管理	2~4
第 7 部分	项目 23 提升林和域的功能级别,部署多元密码策略	1~2
	项目 24 操作主机角色的转移与强占	2~3
	项目 25 站点的创建与管理	2~3
	项目 26 AD 的备份与还原	2~3
课程考核	课程考评	2
课时总计		48～64

本书由黄君羡编著，此外在编写过程中，得到了吴海东、李琳、许兴鹃、欧薇、徐务棠、章丽鸿的大力支持和帮助，在此深表感谢。

由于编者水平和经验有限，书中难免有欠妥和错误之处，恳请读者批评指正。

编　者

2015 年 1 月

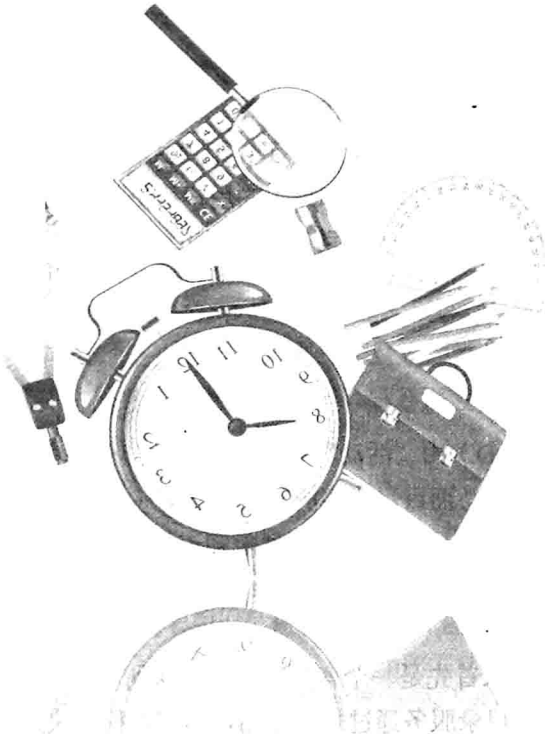
目　录　CONTENTS

第 1 部分　活动目录概述

第 2 部分　虚拟化实战环境搭建

第 3 部分　活动目录实战环境搭建

第 6 部分　OU 与组策略的规划应用



第1部分

活动目录概述

在规模较小的企业环境中，可以使用工作组的形式来组织和管理计算机。如果企业的网络规模较大，地理位置分散，计算机和用户数量多，工作组模式将没有办法集中管理，这就需要使用域的形式来组织，以便进行集中的管理和集中的用户身份验证。

本部分将详细介绍活动目录的基本概念、活动目录的逻辑结构、活动目录的物理结构等知识。

第一节　什么是活动目录

活动目录（Active Directory，AD）由“活动”和“目录”两部分组成，其中“活动”是用来修饰“目录”，其核心是“目录”，而目录代表的是目录服务（Directory Service）。

对于目录，大家最熟悉的就是书的目录，通过它就能知道书的大致内容。但目录服务和书的目录不同，目录服务是一种网络服务，它存储着网络资源的信息并使用户和应用程序能访问这些资源。

在活动目录管理的网络中，目录首先是一个容器，它存储了所有的用户、计算机、应用服务等资源，同时对于这些资源，目录服务通过规则让用户和应用程序快捷访问这些资源。

例如，在工作组的计算机管理中，如果一个用户需要使用多台计算机，那么网络管理员需要到这些计算机上为该用户创建账户并授予相应访问权限。如果有大量的用户有这类需求，那么网络管理员的管理难度将十分繁杂。但在活动目录的管理方式下，用户作为资源被统一管理，每一个员工拥有唯一的活动目录账户，通过对该用户授权允许访问特定组的计算机即可完成该工作。通过比较不难得出 AD 在管理大量用户和计算机时所具有的优势。

对于活动，可以解释为动态的，可扩展的，主要体现在以下两个方面。

（1）AD（活动目录）对象的数量可以按需增减或移动。

AD 中的对象可以按需求增加、减少和移动，如新购置了计算机、有部分员工离职、员工变换工作岗位，这些都必须相应的在 AD 中改变。

（2）AD（活动目录）对象的属性是可以增加的。

每一个对象都是用它的属性进行描述的，AD 对象的管理实际上就是对对象属性的管理，而对象的属性是可能发生变化的。例如，联系方式这个属性原先只有通信地址、手机、电子邮件等，可随着社会发展，用户的联系方式可能需要增加微信号、微博号等，而且这些变化还在持续变化，在 AD 中支持对象属性的增加，AD 管理员只需通过修改 AD 架构来增加属性，然后 AD 用户就可以在 AD 中使用这个属性了。

需要注意的是，AD 对象的属性可以增加，但是不可以减少，如果一些对象属性不允许使用，可以禁用它。

综上，活动目录是一个数据库，它存储着网络中重要的资源信息。当用户需要访问网络中的资源时，就可以到活动目录中进行检索并能快速查找到需要的对象。而且活动目录是一种分布式服务，当网络的地理范围很大时，可以通过位于不同地点的活动目录数据库提供相同的服务来满足用户的需求。

1．活动目录对象

简单地说，在 AD 中可以被管理的一切资源都称为 AD 对象，如用户、组、计算机账户、

共享文件夹等。AD 的资源管理就是对这些 AD 对象的管理，包括设置对象的属性、对象的安全性等。每一个对象都存储在 AD 的逻辑结构中，可以说 AD 对象是组成 AD 的基本元素。

2．活动目录架构

架构（Schema）就是活动目录的基本结构，是组成活动目录的规则。

AD 架构中包含两个方面内容：对象类和对象属性。其中，对象类用来定义在 AD 中可以创建的所有可能的目录对象，如用户、组等；对象属性用来定义在每个对象可以有哪些属性来标识该对象，如用户可以有登录名、电话号码等属性。也就是说 AD 架构用来定义数据类型、语法规则、命名约定等内容。

当在 AD 中创建对象时，需要遵守 AD 架构规则，只有在 AD 架构中定义了一个对象的属性才可以在 AD 中使用该属性。前面叙述的 AD 中对象的熟悉是可以增加的，这就要通过扩展 AD 架构来实现。

AD 架构存储在 AD 架构表中，当需要扩展时只需要在架构表中进行修改即可，在整个活动目录林中只能有一个架构，也就是说在 AD 中所有的对象都会遵守同样的规则，这将有助于对网络资源进行管理。

3．轻型目录访问协议

轻型目录访问协议（Light Directory Access Protocol，LDAP）或称简便的目录访问协议，是访问 AD 的协议，当 AD 中对象的数量非常大时，如果要对某个对象进行管理和使用就需要查找定位该对象，这时就需要有一种层次结构来查找它，LDAP 就提供了这样一种机制。

例如，现实中的找人，如果要找张三这个人，需要知道他在哪个城市、区、街道、大楼、楼层、房间号，最后才能找到他，这就是一种层次结构，和 LDAP 是类似的。

在 LDAP 协议中指定了严格的命名规范，按照这个规范可以唯一地定位一个 AD 对象，如表 0-1 所示。

表 0-1　LDAP 中关于 DC、OU 和 CN 的定义

名字	属性	描述
DC	域组件	活动目录域的 DNS 名称
OU	组织单位	组织单位可以和实际中的一个行政部门相对应，在组织单位中可以包括其他对象，如用户、计算机等
CN	普通名字	除了域组件和组织单位外的所有对象，如用户、打印机等

按照这个规范，假如在域 edu.cn 中有一个组织单位 software，在这个组织单位下有一个用户账户 tom，那么在活动目录中 LDAP 协议用下面的方式来标识该对象：

```
CN=tom,OU=software,DC=edu,DC=cn
```

LDAP 的命名包括两种类型：辨别名（Distinguished Names）和相关辨别名（Relative Distinguished Names）。

上面所写的“CN=tom,OU=software,DC=edu,DC=cn”就是 tom 这个对象在 AD 中的辨别名。而相关辨别名是指辨别名中唯一能标识这个对象的部分，通常为辨别名中最前面的一个。在上面这个例子中“CN=tom”就是 tom 这个对象在 AD 中的相关辨别名，该名称在 AD

中必须唯一。

4．活动目录的特点与优势

与非域环境下独立的管理方式相比，利用 AD 管理网络资源有以下特点：

（1）资源的统一管理

活动目录的目录是一个能存储大量对象的容器，它可以统一管理企业中成千上万分布于异地的计算机、用户等资源，如统一升级软件等，而且管理员还可以通过委派下放一部分管理的权限给某个用户账户，让该用户替管理员执行特定的管理用户。

（2）便捷的网络资源访问

活动目录将企业所有的资源都存入 AD 数据库中，利用 AD 工具，用户可以方便地查找和使用这些资源。并且由于 AD 采用了统一身份验证，用户仅需一次登录就可以访问整个网络资源。

（3）资源访问的分级管理

通过登录认证和对目录中对象的访问控制，安全性和活动目录加密集成在一起。管理员能够管理整个网络的目录数据，并且可以授权用户能访问网络上位于任何位置的资源及权限。

（4）减低总体拥有成本

总体拥有成本（TCO）是指从产品采购到后期使用、维护的总的成本，包括计算机采购的成本、技术支持成本、升级的成本等。例如，AD 通过应用一个组策略，可以对整个域中的所有计算机和用户生效，这将大大减少分别在每一台计算机上配置的时间。

第二节　活动目录的逻辑结构

在活动目录中有很多资源，要对这些资源进行很好的管理就必须把它们有效组织起来，活动目录的逻辑结构就是用来组织资源的。

活动目录的逻辑结构可以和公司的组织机构图结合起来理解，通过对资源进行逻辑组织，使用户可以通过名称而不是通过物理位置来查找资源，并且使网络的物理结构对用户透明化。

活动目录的逻辑结构包括域（Domain）、域树（Domain Tree）、域目录林（Forest）和组织单位（Organization Unit，OU），如图 0-1 所示。

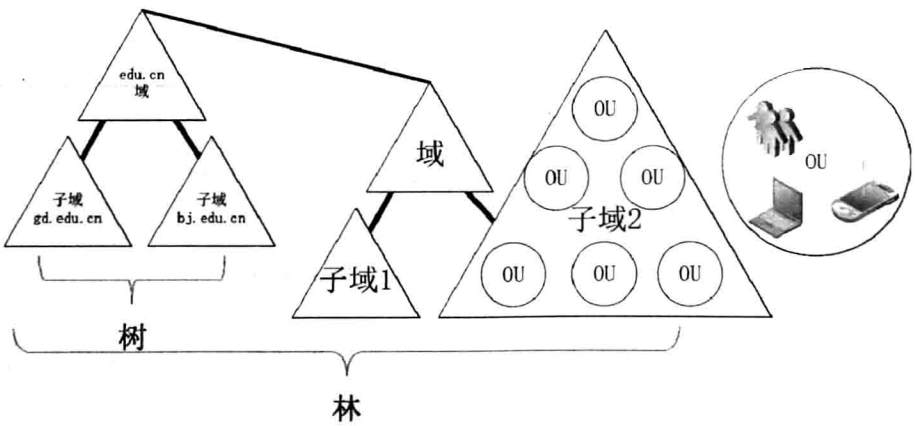


图 0-1　活动目录的逻辑结构

1．域的概念

域是活动目录的逻辑结构的核心单元，是活动目录对象的容器。同时域定义了3个边界：安全边界、管理边界、复制边界。

（1）安全边界。域中所有的对象都保存在域中，并且每个域只保存属于本域的对象，所以域管理员只能管理本域。安全边界的作用就是保证域的管理者只能在该域内拥有必要的管理权限，而对于其他域（如子域）则没有权限。

（2）管理边界。每一个域只能管理自身区域的对象，例如，父域和子域是两个独立的域，两个域的管理员仅能管理自身区域的对象，但是由于它们存在逻辑上的父子信任关系，因此两个域的用户可以相互访问，但是不能管理对方区域的对象。

（3）复制边界。域是复制的单元，是一种逻辑的组织形式，因此一个域可以跨越多个物理位置。如图0-2所示，EDU公司在北京和广州都有公司的相关机构，它们都隶属edu.cn域，北京和广州两地通过ADSL拨号互联，同时两地各部署了一台域控制器。如果edu.cn域中只有一台域控制器在北京，那么广州的客户端在登录域或者使用域中的资源时都要通过北京的域控制器进行查找，而北京和广州的连接是慢速的，这种情况下，为了提高用户的访问速率可以在广州也部署一台域控制器，同时让广州的域控制器复制北京域控制器的所有数据，这样广州的用户只需通过本地域控制器即可实现快速登录和资源查找。由于域控制器的数据是动态的（如管理员禁用了一个用户），所以域内的所有域控制器之间还必须实现数据同步。域控制器仅能复制域内的数据，其他域的数据不能复制，所以域是复制边界。

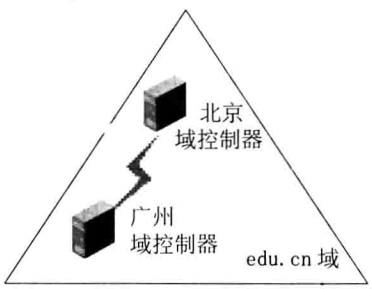


图0-2　活动目录的逻辑结构——域

综上所述，域是一种逻辑的组织形式，能够对网络中的资源进行统一管理，要实现域的管理，必须在一台计算机上安装活动目录才能实现，而安装了活动目录的计算机就成为域控制器。

2．登录域和登录到本机的区别

登录域和登录到本机是有区别的，在属于工作组的计算机上只能通过本地账户登录到本机，在一台加入到域的计算机上可以选择登录到域或者登录到本机，如图0-3所示。

图0-3　在域上的计算机登录界面

在登录到本机时必须输入这台计算机上的本地用户账户的信息，在“计算机管理”控制台下可以查看这

些用户账户的信息，登录验证也是由这台计算机完成的。本地登录账户通常为“计算机名\用户名”，如 SRV1\tom 。

在登录到域时必须输入域用户账户的信息，而域用户账户的信息只保存在域控制器上。因此用户无论使用哪台域客户机，其登录验证都是由域控制器来完成的，也就是说默认情况下，域用户可以使用任何一台域客户机。域登录账户通常为“用户名@域名”，如 tom@edu.cn。

在域的管理中，基于安全考虑，客户机的所有账户都会被域管理员统一回收，企业员工仅能通过域账户使用客户机。

3．域树

域树是由一组具有连续命名空间的域组成的。

例如，EDU 公司最初只有一个域名 edu.cn，后来公司发展了，在北京成立了一个分公司，出于安全的考虑需要新创建一个域，可以把这个新域加入到 edu.cn 域中，这个 bj.edu.cn 就是 edu.cn 的子域，edu.cn 是 bj.edu.cn 的父域。

组成一棵域树的第一个域成为树的根域，图 0-4 中左边第一棵树的根域为 edu.cn，树中其他域称为该树的结点域。

4．树和信任关系

域树是由多个域组成的，而域的安全边界作用使得域和其他域之间的通信需要获得授权。在活动目录中这种授权是通过信任关系来实现的。在活动目录的域树中父域和子域之间可以自动建立一种双向可传递的信任关系。

如果 A/B 两个域直接有双向信任关系，则可以达到以下结果。

（1）这两个域就像在同一个域一样，A 域中的账号可以在 B 域中登录 A 域，反之亦然。

（2）A 域中的用户可以访问 B 域中有权限访问的资源，反之亦然。

（3）A 域中的全局组可以加入 B 域中的本地组，反之亦然。

这种双向信任关系淡化了不同域之间的界限，而且在 AD 中父子域之间的信任关系是可以传递的，可传递的意思是如果 A 域信任 B 域，B 域信任 C 域，那么 A 域也就信任 C 域。在图 0-4 中 gd.edu.cn 域和 bj.edu.cn 域由于各自同 edu.cn 建立了父子域关系，所以它们也相互信任并允许相互访问，也可以称它们为兄弟域关系。由于有这种双向可传递的信任关系存在，实际上就把这几个域融为一体了。

5．域目录林

域目录林是由一棵或多棵域树组成的，每棵域树使用自身连续的命名空间，不同域树之间没有命名空间的连续性，如图 0-4 所示。

域目录林具有以下特点：

（1）目录林中的第一个域称为该目录林的根域，根域的名字将作为目录林的名字。

（2）目录林的根域和该目录林中的其他域树的根域直接存在双向可传递的信任关系。

（3）目录林中的所有域树拥有相同的架构和全局编录。

在活动目录中，如果只有一个域，那么这个域也称为一个目录林，因此单域是最小的林。前面介绍了域的安全边界，如果一个域用户要对其他域进行管理，则必须得到其他域的授权，但在目录林中有一个特殊情况，那就是在默认情况下目录林的根域管理员可以对目录林中所