万水图解精通系列丛书

Master Active Directory Visually

图解精通 ActiveDirectory

[美]Curt Simmons MCSE MCT 著
张晓明 邓劲生 等译

完全直观的参考书

畅销的三维可视化系列图书

循序渐进地讲解

1000个屏幕抓图

革新的学习方法

带网络管理工具的CD-ROM引导

中国水利水电出版社
www.waterpub.com.cn

Visual

万水图解精通系列丛书

图解精通 Active Directory

[美] Curt Simmons MCSE MCT 著

张晓明 邓劲生 等译

中国水利水电出版社

内 容 提 要

本书采用完全可视化的方法，通过 1000 多张图例全面地介绍了 Windows 2000 活动目录的结构、规划和应用实例。本书首先介绍了活动目录的基本概念、Windows 2000 TCP/IP 联网技术，而后逐步介绍如何安装、配置、规划和搜索活动目录。接下来深入讨论了 Windows 2000 活动目录中的用户、组、计算机的账户管理，组织单位和对象的创建，域和域控制器域信任关系的创建和管理，目录信息的复制和恢复等关键问题。最后，本书从应用的角度出发，阐述了活动目录站点的配置和管理，活动目录的安全特性，活动目录资源的发布，活动目录构架，公共组策略的配置等应用实例。

本书对于希望了解和精通 Windows 2000 活动目录的读者是一本全面的、易学易用的参考书，也适合于技术支持工程师和系统开发工程师等学习。

北京市版权局著作合同登记号：图字 01-2000-3382

图书在版编目（CIP）数据

图解精通 Active Directory/（美）西蒙斯（Simmons, C.）等著；张晓明等译. －北京：中国水利水电出版社，2002

（万水图解精通系列丛书）

书名原文：Master Visually Active Directory

ISBN 7-5084-0946-9

Ⅰ.图… Ⅱ.①西…②张… Ⅲ.窗口软件，Windows 2000－目录－软件工具，Active Directory Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字（2001）第 092444 号

书　　名	**图解精通** Active Directory
作　　者	[美] Curt Simmons MCSE MCT 著
译　　者	张晓明 邓劲生 等
出版、发行	中国水利水电出版社（北京市三里河路 6 号 100044） 网址：www.waterpub.com.cn E-mail：mchannel@public3.bta.net.cn（万水） sale@waterpub.com.cn 电话：（010）68359286（万水）、63202266（总机）、68331835（发行部）
经　　售	全国各地新华书店
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787×1092 毫米 16 开本 23.75 印张 821 千字
版　　次	2002 年 1 月第一版 2002 年 1 月北京第一次印刷
印　　数	0001—5000 册
定　　价	40.00 元（含 1CD）

凡购买我社图书，如有缺页、倒页、脱页的，本社发行部负责调换

译 者 序

在这个 Internet 能够主宰一切的时代里，人们每天面对的都是大量的网络资讯，所以的活动几乎都和网络有着千丝万缕的联系。活动目录服务将网络中的所有对象集中从而使其容易管理，并提供了完善的安全措施，增强了对分布式应用的支持。

活动目录（Active Directory，AD）是 Microsoft 目录服务的解决方案。活动目录的作用是用于组织有关真实网络实体——例如用户、共享、打印机以及应用程序等信息。使用 DNS 命名策略和 TCP/IP 实现的可伸缩性，使目录服务能和公司一起成长。Kerberos 使用强大的加密算法，为目录服务提供双向的安全性保障。通过开放标准的目录访问协议如 LDAP，活动目录实现了和其他目录服务的互操作性。活动目录也设计用于为网络管理员提供单一的管理点。管理员能够找到活动目录中的所有目录信息和那些能够被复制到所有 Windows 2000 域控制器的信息，而不必管理保存着众多资源的多台服务器。资源访问、安全授权以及用户和组账户都可以集中位于一个地方。

面对纷至沓来的众多学习参考书，读者可能会困惑不已。但本书的风格却将带来一场学习的革命。本书没有繁杂晦涩的文字，也一扫长篇累牍的说教风格，而是以一种完全图解的方式，面对面地教会读者如何掌握活动目录。读者将会在一种轻松愉快的状态下，掌握和运用 Windows 2000 活动目录。

本书采用完全可视化的方法，通过 1000 多张图例全面地介绍了 Windows 2000 活动目录的结构、规划和应用实例。活动目录的基本概念、Windows 2000 TCP/IP 联网技术入手；而后接下来深入讨论了 Windows 2000 活动目录中的用户、组、计算机的账户管理，如何安装、配置、规划和搜索活动目录；域和域控制器域信任关系的创建和管理，目录信息的复制和恢复等关键问题。最后，本书从应用的角度出发，阐述了活动目录站点的配置和管理，活动目录的安全特性，活动目录资源的发布，活动目录构架，公共组策略的配置等图解实例。另外，读者使用随书光盘可以在屏幕上直观地浏览本书，本书附带网络管理工具的 CD-ROM 可以帮助读者进一步地学习和掌握 Windows 2000 活动目录。

本书对于希望了解和精通 Windows 2000 活动目录的读者是一本全面的、易学易用的参考书，也适合于技术支持工程师和系统开发工程师等学习。

本书由张晓明、邓劲生组织翻译，灯芯工作室的全体人员参加了翻译、截图、录入、校对和排版等工作。由于全书内容覆盖面广且知识较新，而时间紧迫且水平有限，差错之处在所难免，恳请各位读者批评指正。

译 者

2001 年 4 月

关于作者

Curt Simmons 是 Microsoft 认证系统工程师（MCSE）和 Microsoft 认证培训员（MCT）。他是 Windows 专家，一直从事 Windows 技术书籍的编写。在 Windows 2000 和 Active Directory 的 beta1 版发布以来，Curt 一直从事这方面的工作；他是许多 Microsoft 技术的高级计算书籍的作者。Curt 和妻子女儿一起生活在 Dallas 外的一个得克萨斯小镇。读者可以在 Internet 上访问他的主页 curtsimmons.hypermart.net。

致　　谢

我要感谢从事 IDG 书籍的每一个人，特别是 Martine Edwards 和 Darren Meiss。感谢 Martine 给了我写这本书的机会，并且非常感谢 Darren 为此书所花的时间和精力。我还要感谢我的经济人 Margot Maley，他总是处处为我着想。最后，感谢我的妻子 Dawn，在我花很多时间在电脑上录入文稿的时候，她给予了我很大的耐心和支持。

目　　录

第三部分　规划活动目录

第四部分　安装活动目录

第五部分　用户、组和计算机

第六部分　域和信任关系

第七部分　活动目录站点

第八部分　应用实现

第一部分　理解活动目录

1 活动目录技术

如果读者在最近的两年里已经接触过计算机和网络，就会对活动目录略知一二。其中有些是读者正确理解的，但大部分可能理解得不正确。本书将帮助读者正确理解有关活动目录的所有知识，并且通过一种可视化的方法帮助读者掌握活动目录。但在我们深入了解活动目录的安装和配置细节之前，读者需要了解有关的概念性知识，这样有助于全面了解活动目录。第 1 章、第 2 章和第 3 章介绍了有关概念和背景知识，它有助于读者实现配置和支持活动目录。

什么是目录

在最近的几年中，目录（directory）这个术语大量用于计算环境。由于计算环境变得越来越庞大和复杂，如何能够很好地组织信息，以便网络用户可以定位其所需信息已变得更加重要了。根据定义，目录是指信息存储位置，它使用系统方法或者名称空间来组织信息。电话簿就是一个普通的例子。我们通过城市/地区、姓和名的方式来存储电话簿中的所有信息。在特定的城市/地区中给定一个特定的名称，可以找到这个人的电话号码。电话簿按如下方法使用名称空间：所有的名字都按姓名的字母顺序进行排列。如果电话簿不遵循名称空间——也就是说，如果有些名字按姓氏排列，有些按名称排列，有些按昵称排列，有些按地址排列——那么我们就无法找到所需要的电话号码。

什么是活动目录

活动目录是 Microsoft 目录服务的解决方案。活动目录的作用是用于组织有关真实网络实体——例如用户、共享、打印机以及应用程序等信息。从而用户能够找到所需资源。通过活动目录，用户不必知道哪台服务器拥有哪些资源，或者打印机位于哪里。活动目录能够列举信息，并且信息是完全可搜索的；它还为用户提供标准的文件夹接口，以便用户能够在网络上找到所需信息。

活动目录也设计用于为网络管理员提供单一的管理点。管理员能够找到活动目录中的所有目录信息和那些能够被复制到所有 Windows 2000 域控制器的信息，而不必管理保存着众多资源的多台服务器。资源访问、安全授权以及用户和组账户都可以集中位于一个地方。

理解活动目录特性

活动目录包含许多特性和选项。读者应该首先了解其概貌和设计目标。下面列出了活动目录的主要特性和设计目标：

- 可伸缩性：活动目录是高度可伸缩的，就是指它可以在小规模网络环境中工作，也可以用于整个公司。活动目录支持多个商店，并且可以在每个商店里支持一百多万个对象。商店就是活动目录对象的主要群体，当然活动目录也支持多个商店。
- 可扩展性：活动目录是可扩展的，即指读者可以根据企业的需求进行定制。
- 安全性：活动目录与 Windows 2000 安全性相集成，允许管理员控制访问对象。
- 无缝集成：活动目录与本地网络和 Intranet/Internet 实现无缝集成。
- 开放标准：活动目录基于开放的通信标准，允许与其他的目录服务相集成和通信。例如，Novell 的 NDS。
- 向后兼容性：尽管 Windows 2000 操作系统主要使用活动目录，但活动目录也能够与 Windows 早期版本一起工作。这种特性使得活动目录能够逐步地实现同时保持全网络的正常工作。

理解域和域控制器

如果读者使用 Windows NT，就应该熟悉域和域控制器的概念。域（domain）是多个用户、计算机和资源的分组。实际上，域是一个安全边界，它使得管理员能够控制该域中的资源并且使未授权的用户被拒绝到域外。活动目录正是通过域来创建的。域控制器是管理这些域的服务器，主域控制器（primary domain controller，PDC）和备份域（backup domain）在 Windows 2000 中不再出现；所有的控制器都是对等的。通过信任关系，活动目录可以通过多主机复制的方式进行复制，这就意味着所有的域控制器都有责任维护活动目录和将变化复制到其他域控制器。在本书后面章节中，我们将学到有关管理 Windows 2000 信任关系的更多内容。

DNS 和活动目录

域名系统（Domain Name System，DNS）是实际中应用最广泛的目录名称空间。读者每次使用 Internet，都可以通过 DNS 找到 URL。DNS 提取统一资源定位符（Uniform Resource Locator，URL），例如 www.microsoft.com，并将 URL 解析成 TCP/IP 地址，例如 131.107.2.200，该 IP 地址才是 Internet 上通信所需的地址。由于计算机间必须使用 TCP/IP 地址进行通信，并且用户需要使用语言化的名字进行通信，所以 DNS 的作用就是在两者之间进行解析。

活动目录与 DNS 相集成，活动目录中的命名机制是 DNS 名称。例如，corp.com 是一个有效的 DNS 名称，并且能够用作 Windows 2000 域名。在活动目录中，DNS 用作定位器服务，这样使得局域网（LAN）与 Internet 和 Intranet 之间实现无缝连接。corp.com 可以是 Internet 名称，也可是一个局域名称。并且 Jwilliams@corp.com 既可以是 Internet 电子邮件地址，也可以是一个本地网络的用户名。这种结构使得用户能够在自己的网络中找到所需资源，就像在 Internet 上找到它们一样。

Windows 2000 也支持动态 DNS（Dynamic DNS，DDNS），动态 DNS 是 DNS 标准的新扩充。DDNS 可以根据新值或者变化的值来动态地更新 DNS 服务器，而这在以前必须手工进行更新。由于名字记录可以动态地进行更新，一个完全的 Windows 2000 网络不再需要使用 Windows Internet 命名服务（Windows Internet Naming Service，WINS）。但是，在混合环境中，WINS 用于与 Windows 的老版本保持向后兼容。读者可以在第 5 章和第 6 章中了解到有关 WINS 和 DNS 的相关内容。

理解 LDAP

DNS 是活动目录中使用的名称空间，而轻型目录访问协议（Lightweight Directory Access Protocol，LDAP）指出了读者如何访问活动目录。

为了理解 LDAP，首先回顾一下其历史。X.500 标准是一个目录规范，它引入了目录访问协议（Directory Access Protocol，DAP）以读取和修改目录数据库。DAP 是一个可增强的协议，它可以处理目录请求和目录变化以及目录安全。但是，DAP 将大量的处理开销放在客户端计算机上，它是一个高开销的协议。LDAP 不是在 X.500 规范中定义的协议，它克服了 DAP 的弱点。LDAP 是一个开放的标准，这意味着任何都可以利用它来开发目录服务，而不像 DAP 那样局限于 X.500 目录。LDAP 与 DAP 的另一个主要不同之处在于 LDAP 不是基于客户端的服务。其服务运行在服务器上，而将信息返回到客户端。活动目录不是 X.500 目录，但它支持其信息模型同时不要求系统保证 X.500 的开销。这样基于 LDAP 的目录能够支持高级互操作性。

LDAP 在 Internet 上广泛使用。如果读者已参与到新闻组中或者使用搜索引擎访问万维网，则一定用过 LDAP。活动目录直接支持这个开放的协议，从而用户可以找到所需的资源。

活动目录结构

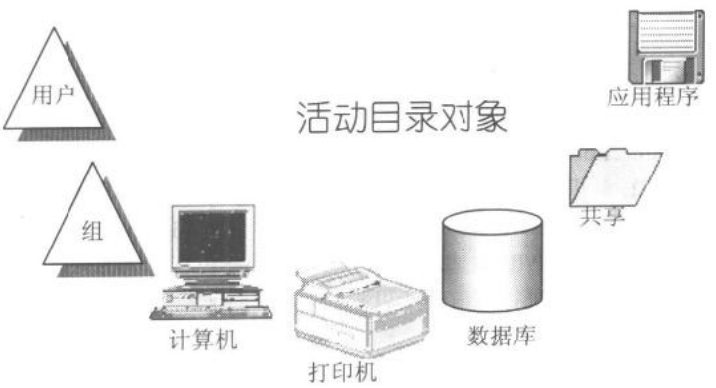
活动目录是一种分层结构，因此在安装和实现活动目录之前，读者首先要理解活动目录的结构及其组件。读者不仅要学会这些组件，而且也必须了解这些组件是相互关联共同构成了活动目录分层结构。

在本章中，我们先介绍分层结构中最小的组件，而后依次向上介绍各种组件，直到分层结构的最上层。本节将给出活动目录分层结构的概貌。

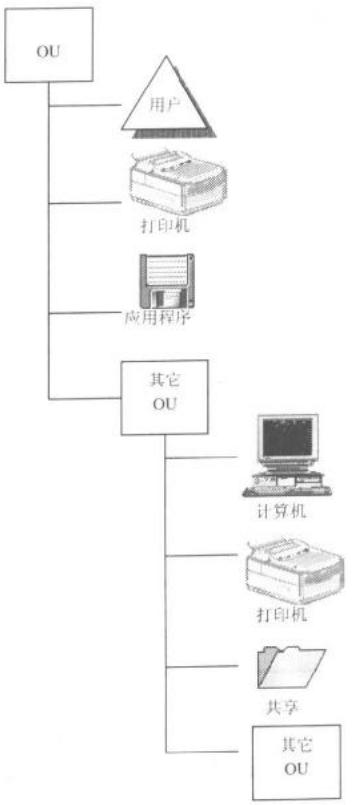
对象

活动目录对象（object）表示网络中的某种物理对象。常见的活动目录对象有用户、组、打印机、共享文件夹、应用程序、数据库、联系等等，每种对象都表示网络中的某个实体。

每个对象都包含属性。属性（attribute）是辅助定义实际对象的度量。例如，用户对象具有用户名，实际名字和电子邮件地址这些属性。在活动目录中，每种对象都具有各自的属性。属性定义了对象本身，而同时又使用户能够搜索到特定的某个对象。从技术上讲，属性被称为“元数据”——简言之，就是“数据的数据”；而且它也是活动目录“架构”的一部分，它定义了什么对象和对象属性能够存在于活动目录中。



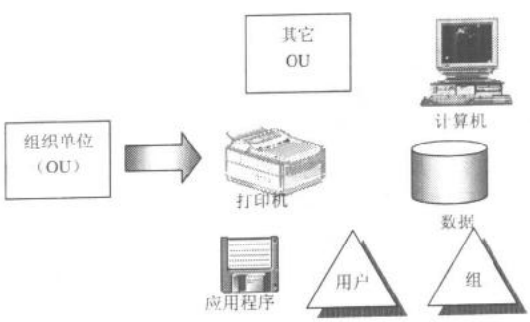
*每个对象持有定义该对象的属性



*包含有 OU 和对象的层次视图

组织单位

组织单位（Organizational Unit，OU）就像文件夹一样。OU 定义用于存放对象（也存放其他的 OU）。它和对象一样，也包含属性，但对其本身不起作用。组织单位的用途是存放其他的对象。顾名思义，OU 有助于组织目录结构。例如，用户可以组织会计 OU 来包含诸如支出账户 OU 和支入账户 OU，而且在这些 OU 中可以包含对象，如用户、组、计算机、打印机等等。

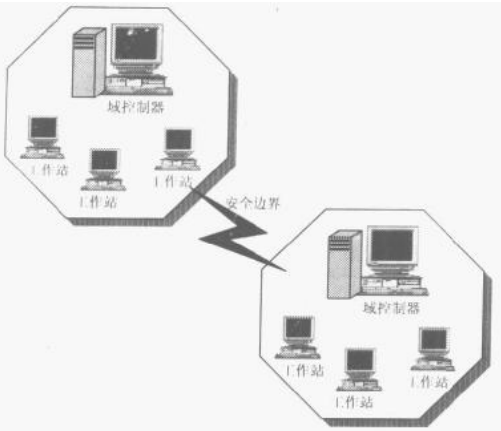


*对象被包容在组织单位中

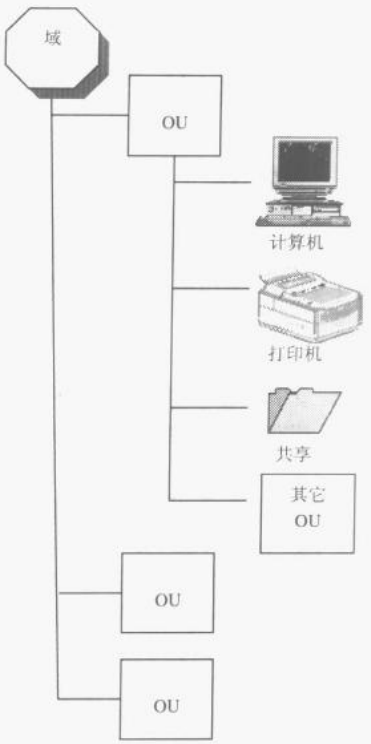
域

从定义上讲，域（domain）是用户和计算机的逻辑分组。域通常位于本地化的地理位置上，但也有例外。实际上，域不仅仅是逻辑分组——它实际上是 Windows 2000 或 NT 网络的安全边界。读者可以将一个网络看成多个域就像居住上的邻居关系。所有的家庭组成了邻居关系，但每个家庭都是一个安全边界，

其中包含了特定对象，而同时与其他对象相隔离。域就像邻居关系中的一个家庭。每个域都有自己的安全策略，并且能够和其他域之间建立信任关系。活动目录由一个或多个域构成。域包含“架构”，而架构定义了哪些对象存放在域中。架构根据类（例如用户类，计算机类等）来定义对象，而属于同一个类的所有对象都称为该类的“实例”。第 27 章介绍了有关活动目录架构的内容。



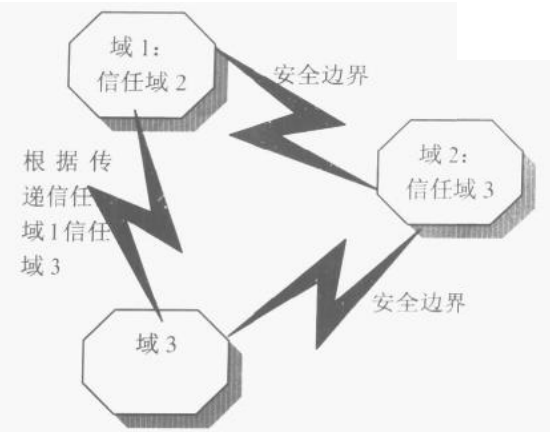
*每个域作为一个安全边界



*域站点位于层次的顶

树

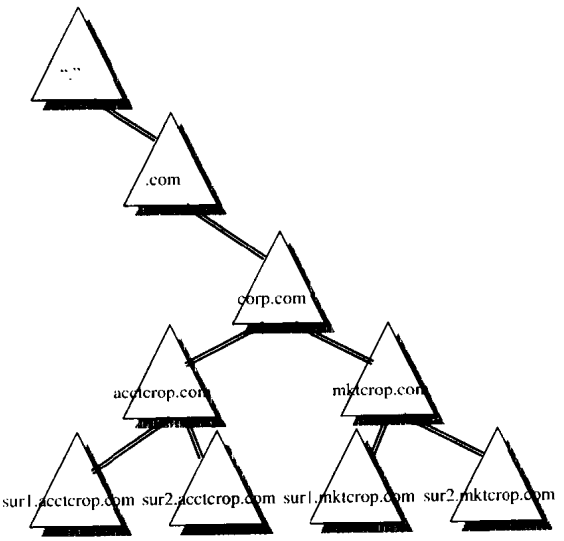
域、组织单位和对象之间的这种分层结构称为树（tree）。树中的对象称为端点（endpoint），而树结构中的 OU 称为结点（node）。与实际的树相类比，可以将树枝看成是 OU 或容器，而将树叶看成是对象，其中每个对象就是树中结点的端点。



域树

当多个域之间通过信任关系相互联系并且共享公共的架构、配置和全局编录时，它们之间就形成域树（domain tree）。Windows 2000 中的信任关系是基于 Kerberos 安全协议的。Kerberos 信任具有传递性。换句话说，如果 1 域信任 2 域并且 2 域信任 3 域，则 1 域也信任 3 域。在同一个树和树林内部，活动目录自动配置其中的信任关系。读者将在第 21 章中了解到有关活动目录中的信任关系的更多内容。

域树也共享连续的名称空间，连续的名称空间在域树中遵循相同的 DNS 命名层次结构。例如，如果根域是 corp.com，并且域树中包含 DomainA 和 DomainB，这两个域的连续名称空间即为 domaina.corp.com 和 domainb.corp.com。如果 A 域位于 corpjp.com，而 B 域位于 corp.com 根处，则这两个域将不能共享一个连续的名称空间。



*邻接名字空间的一个实例。

树林

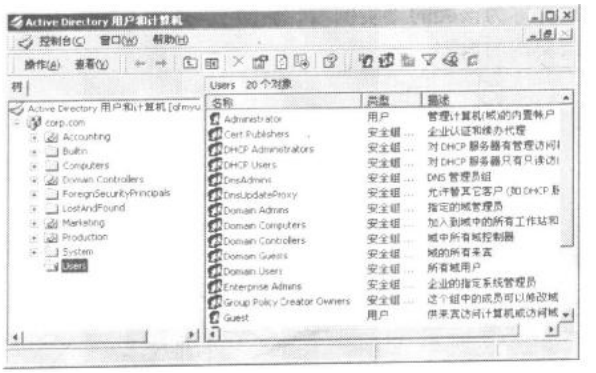
那些不共享连续名称空间的一个或多个树称为树林（forest）。树林中的所有树都具有相同的架构、配置和全局编录，但是这些树不共享同一个连续名称空间。树林中的所有树都通过 kerberos 传递信任关系相互信任。事实上，树林没有一个确切的名字，但这些树都被看成是信任关系的一个层次结构。在层次顶部的树通常代表该树。例如，corp.com、production.corp.com 以及 mgmt.corp.com 形成一个树林，而 corp.com 为该树林的根。

站点

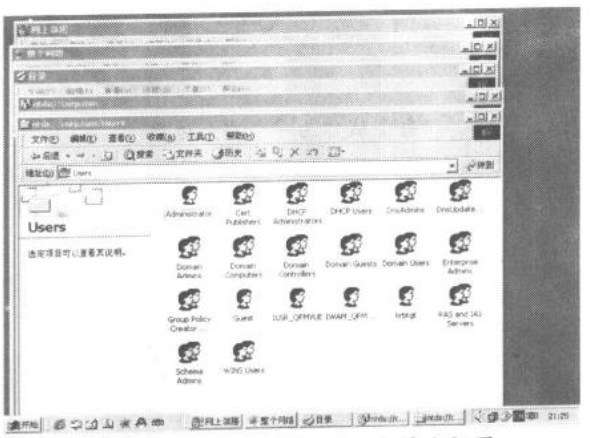
站点（site）实际上并不能认为是活动目录分层结构的一部分，但它是出于复制的目的而在活动目录中进行配置的。站点定义为网络中的某个地理位置，包含有活动目录服务器和一个完美连接的 TCP/IP 子网。完美连接（well-connected）是指网络连接是高可靠的和快速的。管理员使用活动目录来配置站点间的复制。用户不必了解站点配置。就活动目录而言，用户只能看到域一级。

管理员和用户所看到的结构

读者作为管理员可以通过管理工具察看活动目录结构，在第 14 章到第 21 章讲述了有关的详细信息。通过管理工具，读者可以看到域，OU 和对象，这些都是活动目录的一部分。用户可以在“我的网络”中访问并浏览活动目录。用户看到的是域和域内部的组织单位。而对象则位于相应的 OU 中。用户最好通过执行 LDAP 搜索来获取资源，而不是通过浏览（参阅第 13 章）。



*管理员能够查看活动目录的树结构



*用户能够查看活动目录的文件夹视图

活动目录名称

在活动目录中，每个对象，诸如用户、组、计算机、打印机等都有惟一的名字，每个对象分配有四种名称。

首先，每个对象有一个识别名称（distinguished name，DN）。DN 是与其他所有对象相区分的惟一名称，并且包含检索对象所需的完全信息。DN 包含对象所在的域和到达对象的路径。DN 由以下这些属性构成：

- 域组件名称（DC）
- 组织单位名称（OU）
- 公共名称（CN）

例如，如果要访问存放在某一特定域中的文档“Company mission”，DN 将读取：