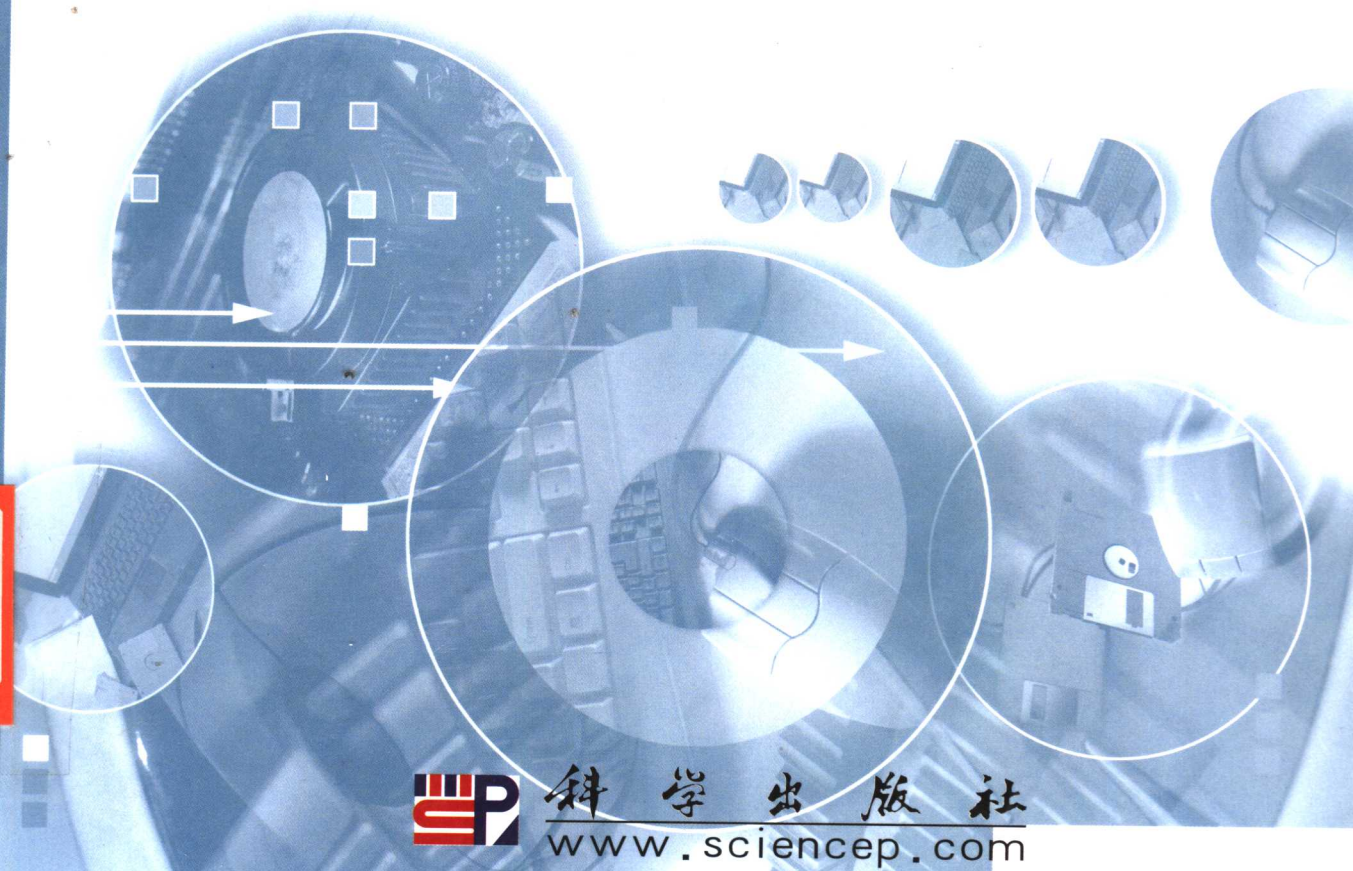
微软认证高级技术培训教材系列

考试号：70—218　课程号：2126

管理Windows 2000网络环境

北京希望电子出版社　总策划
李学军　罗　靖　朱诗兵 等　编　著



科学出版社
www.sciencep.com

管理 Windows 2000 网络环境

微软认证高级技术培训教材系列

考试号：70—218　课程号：2126

管理Windows 2000网络环境

北京希望电子出版社　总策划
李学军　罗　靖　朱诗兵 等　编　著

科学出版社
www.sciencep.com

内 容 简 介

本书是微软认证高级技术培训教材系列之一，是微软操作系统技术认证教材中的一本，课程号为2126。

本书内容新颖全面涵盖Windows 2000环境的基础知识和基本技巧，同时给出了考察和调整Windows 2000系统性能的手段，是Windows 2000认证考试的权威教材。它既适用于参加微软认证考试的各类读者使用，也是从事网络管理的工程技术人员的首选资料。

每章均附有大量的微软认证全真习题，以及详细的分析和答案，凝聚了作者多年科研教学的经验教训。这些练习将极大的帮助读者理解和掌握所学的知识和参加微软认证考试。

需要本书或技术支持的读者，请与北京中关村083信箱（邮编：100080）发行部联系，电话：010-62630301，62524940，62521921，62521724，82610344，82675588（总机）传真：010-62520573，E-mail：kobe@bhp.com.cn。

图书在版编目（CIP）数据

管理Windows 2000网络环境 /李学军等 编著.—北京：科学出版社，2003

ISBN 7-03-012148-1

Ⅰ.管… Ⅱ.李… Ⅲ.服务器—操作系统（软件），Windows 2000 Ⅳ.TP316.86

中国版本图书馆CIP数据核字（2003）第077733号

责任编辑：栾大成 /责任校对：吴胜

责任印刷：双青 /封面设计：王翼

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2003年10月第 一 版 开本：787×1092 1/16

2003年10月第一次印刷 印张：24 1/2

印数：1—5 000 字数：689 000

定价：45.00元

出版说明

为了配合微软高级技术培训的教学与考试，进一步推广微软认证系统工程师（MCSE）、微软认证数据库管理员（MCDBA）、微软认证系统管理员（MCSA）和微软认证产品专家（MCP）的培训和考试，特组织优秀的微软认证讲师（MCT）编写了本套微软认证高级技术培训教材。

全套教材共 7 本：

序号	书　名	对应考试号
1	Windows 2000 网络和操作系统基础	无
2	实现 MS Windows 2000 Professional 和 Server	70-210，70-215
3	实现 MS Windows 2000 网络基础结构	70-216
4	MS Windows 2000 目录服务基础结构设计和管理	70-217，70-219
5	MS SQL Server 2000 数据库管理	70-228
6	MS SQL Server 2000 数据库编程	70-229
7	管理 MS Windows 2000 网络环境	70-218

本套培训教材都由第一线的微软认证高级技术培训中心讲师（MCT）编写，凝聚了 MCT 们多年教学经验，符合中国人阅读习惯，教材的每章都有学习重点，在必要章节附有实验，供学员练习。本套教材还包括大量的模拟试题，所有模拟试题都加入了试题分析和知识点解析以适应不同考生考证使用。力求通过学习本套教材，即可通过 MCSE，MCDBA，MCSA 或 MCP 的考试。

学员通过学习课程 1，2，3，4，5，6，通过对应的考试，可以获得 MCSE 和 MCDBA 两种证书；通过学习课程 1，2，3 或 4，7，通过对应的考试，可获得 MCSA 证书；学习任何一门课程，通过对应的考试，均可获得 MCP 证书。

本套教材既可作为微软认证高级技术培训教材，微软高级技术认证的自学教材，也可供广大网络、数据库技术人员和爱好者学习、参考使用。

编　者

编者序

Windows 2000 是微软公司新一代的操作系统，它是在 Windows NT4.0 操作系统的基础上开发的，集 Windows NT 技术和 Windows9X 的优点于一身，并在此基础上发展了许多新的特性和功能。本书围绕 Windows 2000 网络环境管理的基本概念，以教程的方式向读者介绍了与其相关的大量知识内容。

全书分为 4 个单元，共 11 章。第一章“Windows 2000 活动目录”介绍了 Windows 2000 活动目录的基本概念、活动目录的物理与逻辑结构、活动目录的安装以及管理 Windows 2000 网络。第二章“网络资源发布管理”介绍了网络资源发布概述、打印机发布管理、打印机位置跟踪、共享文件夹发布管理、共享文件夹的访问管理以及网络共享资源的维护与故障排除。第三章“管理活动目录复制”介绍了活动目录的基本概念、活动目录复制的过程、如何使用站点优化活动目录的复制以及如何理解和解决活动目录复制故障。第四章“活动目录的委派管理控制”介绍了委派管理控制的基本概念、活动目录对象与组织单位的管理、如何使用委派管理控制向导、用户和计算机账户管理以及活动目录管理工具。第五章“管理 Internet 服务”介绍了 Web 服务简介、II5.0 的特色与安装、创建配置 Web 与 FTP 站点、创建、配置虚拟目录、管理 Web 站点内容发布、管理 Web 站点的安全性、Web 浏览器的配置与管理 Web 服务器。第六章“管理 DHCP 服务”介绍了 DHCP 的基本概念、DHCP 服务的安装和授权、创建和配置 DHCP 服务的作用域和在路由网络中配置 DHCP 由。第七章“管理名称解析服务”介绍了名称解析的基本概念、主机名称解析、NetBIOS 名称解析、为客户端配置名称解析以及如何解决由名称解析配置错误所引起的网络故障。第八章“管理远程访问服务”介绍了远程访问连接类型、远程访问协议、配置入站、出站连接、配置身份验证协议、配置加密协议、综合配置 DHCP 和路由和远程访问、配置远程访问策略、排除远程访问中的故障。第九章“管理组策略”介绍了组策略的基本概念、组策略对象、组策略对象管理、应用组策略设置以及组策略故障诊断。第十章“管理桌面环境”介绍了用户环境管理概述、管理模板设置、脚本设置、重定向文件夹设置、保护用户环境和配置用户账户策略。第十一章“客户机启动和登录故障诊断”介绍了客户机启动概述、Windows 98 客户计算机启动、Windows 2000 客户计算机启动、使用高级选项启动计算机、使用恢复控制台、保护登录处理和用户登录故障诊断。

本书结构清晰、内容详尽，通过课后练习与思考题来帮助学习者复习和巩固所有的知识、概念和技巧，为参加微软的认证考试打下良好的基础。

本书由李学军、罗靖、杜刚、喻文芳、朱诗兵、穆道生、仲巍、吴刚、周江俊、刘伟、蒋太杰、高晓玲、马君艳、屠东等编写，最后由赵洪利教授统稿审定。在编写过程中得到了张建宽、痕洋的大力支持和帮助，在此深表感谢。

由于时间仓促，编写者水平有限，错误在所难免，恳请读者指正。

目 录

第 1 章　Windows 2000 活动目录简介

- Windows 2000 活动目录概述
- Windows 2000 活动目录的物理结构
- Windows 2000 活动目录的逻辑结构
- Windows 2000 活动目录的安装
- 管理 Windows 2000 网络

本章将简单介绍与 Windows 2000 活动目录有关内容：Windows 2000 活动目录的基本概念、活动目录的物理与逻辑结构、活动目录的安装以及管理 Windows 2000 网络。通过对本章内容的学习和课后练习希望学员可以实现以下目标。

学习目标

- 理解活动目录的基本概念
- 理解活动目录的物理结构
- 理解活动目录的逻辑结构
- 掌握活动目录的安装过程
- 描述管理 Windows 2000 网络的方法

1.1　活动目录概述

- 什么是 Active Directory
- 目录服务的功能
- Active Directory 的优点
- Active Directory 相关名词术语
- Active Directory 架构
- Active Directory 客户
- 轻量目录访问协议

1.1.1　什么是活动目录

活动目录（Active Directory）是用于 Windows 2000 Server 的目录服务。它存储网络上各种对象的有关信息，并使该信息易于管理员和用户的查找及使用。Active Directory 目录服务使用结构化的数据存储作为目录信息的逻辑层次结构的基础，并提供了命名、描述、定位、访问、管理和保护网络资源的统一途径。

理解活动目录的关键就在于“活动”两个字，要脱离原来在 DOS 下目录或 Windows 9X 下的文件夹概念。因为目录是活动的，所以它是动态的，是一种包含服务功能的目录，它可以做到“由此及彼”的关联、映射，如：找到了一个用户名，就可关联到它的帐户、出

生信息、E-mail、电话等所有基本信息，虽然组成这些信息的文件可能不在一块。通过活动目录在不同应用程序之间还可以对这些信息进行共享，减少了系统开发资源的浪费，提高了系统资源的利用效率。

Active Directory 包括两个方面：

- 目录
- 目录服务

目录

目录是存储各种对象的一个物理上的容器，从静态角度来理解这活动目录与以前所认识的“目录”和“文件夹”没有本质区别，仅仅是一个对象，是一个实体。

目录服务

目录服务是使目录中所有信息和资源发挥作用的服务，活动目录是一个分布式的目录服务，信息可以分散在多台不同的计算机上，保证用户能够快速访问，因为多台机上有相同的信息，所以在信息方面具有很强的控制能力，正因如此，不管用户从何处访问或信息处在何处，都对用户提供统一的视图。

1.1.2 目录服务的功能

Active Directory 提供了目录服务功能，包括集中式组织、管理和控制网络资源访问的方法，具体的目录服务功能如下：

- 数据存储，也称为目录，它存储着与 Active Directory 对象有关的信息。这些对象通常包括共享资源，如服务器、文件、打印机、网络用户和计算机帐户。
- 一套规则，即架构，定义了包含在目录中的对象类和属性、这些对象实例的约束和限制及其名称的格式。
- 包含目录中每个对象信息的全局编录。允许用户和管理员查找目录信息，而与目录中实际包含数据的域无关。
- 查询和索引机制的建立，可以使网络用户或应用程序发布并查找这些对象及其属性。
- 通过网络分发目录数据的复制服务。域中的所有域控制器参与复制并包含它们所控制的域的所有目录信息的完整副本。对目录数据所做的任何更改都被复制到域中的所有域控制器。
- 与网络安全登录过程的安全子系统的集成，以及对目录数据查询和数据修改的访问控制。

1.1.3 Active Directory 的优点

Windows 2000 成功和创造性之一就是成功的全面引入了活动目录服务，由于活动目录并不是 Windows 2000 系统必需安装的一种服务，要全面理解它是非常的不容易，那么安装活动目录的意义在哪里呢？它主要体现在以下几个方面：

- 降低了总体拥有成本
- 信息的安全性大大增强
- 引入基于策略的管理，使系统的管理更加明朗
- 具有很强的可扩展性
- 具有很强的可伸缩性
- 智能的信息复制能力
- 与 DNS 集成紧密
- 与其他目录服务具有互操性
- 具有灵活的查询

降低了总体拥有成本

总体拥有成本（TCO）是拥有计算机的实际成本。这些成本包括：维护成本、培训成本、技术支持成本以及升级硬件和软件成本。

通过实施策略，活动目录有助于降低总体拥有成本。在活动目录中应用一个策略，允许在一个集中位置配置桌面环境和安装应用程序。这种做法减少了配置花费的时间和在每一台计算机上安装应用程序的时间。

信息的安全性大大增强

安全性完全与 Active Directory 集成。不仅可在目录中的每个对象上定义访问控制，而且还可在每个对象的属性上定义。Active Directory 提供安全策略的存储和应用范围。安全策略可包含帐户信息，如域范围内的密码限制或对特定域资源的访问权。通过组策略设置执行安全策略。

引入基于策略的管理

Active Directory 目录服务包括数据存储和逻辑分层结构。作为逻辑结构，它为策略应用程序提供分层的环境。作为目录，它存储着分配给特定环境的策略（称为组策略对象）。组策略对象表示了一套商务规则，它包括与要应用的环境有关的设置，通过组策略可确定：

- 目录对象和域资源的访问
- 用户可使用什么域资源（如应用程序）
- 这些域资源是如何配置使用的

例如，组策略对象可以决定当用户登录时用户在他们的计算机上看到什么应用程序，当它在服务器上启动时有多少用户可连接至 SQL Server，以及当用户转移到不同部门或组时他们可访问什么文件或服务。组策略对象使用户可以管理少量策略而不是大量用户和计算机。通过 Active Directory，用户可将组策略设置应用于适当环境中，不管它是用户的整个单位还是用户单位中的特定部门。

具有很强的可扩展性

Windows 2000 的活动目录具有很强的可扩展性，管理员可以在计划中增加新的对象类，或给现有对象类增加新属性。计划包括可以存储在目录中的每一个对象类的定义和对

象类的属性。例如，在电子商务上可以给每一个用户对象增加一个购物授权属性，然后存储每一个用户购买权限作为用户帐号的一部分。

可以通过以下两种方法将对象和属性添加至目录中：

1. 使用 Active Directory 架构。
2. 通过 Active Directory 服务接口(ADSI)或 LDIFDE 或 CSVDE 命令行实用程序创建脚本。

具有很强的可伸缩性

Active Directory 包含一个或多个域，每个域具有一个或多个域控制器，以便用户可以调整目录的规模以满足任何网络的需要。多个域可合并为域树，多个域树可合并为树林。

目录将其架构和配置信息分发给目录中所有的域控制器。该信息存储在域的第一个域控制器中，并且复制到域中任何其他域控制器。当该目录配置为单个域时，添加域控制器将改变目录的规模，而不影响其他域的管理开销。

将域添加到目录使用户可以针对不同策略环境划分目录，并调整目录的规模以容纳大量的资源和对象。

智能的信息复制能力

复制为目录提供了信息可用性、容错、负载平衡和性能优势。Active Directory 使用多主机复制，允许用户在任何域控制器上而不是单个主域控制器上更新目录。多主机模式具有更大容错的优点，因为使用多域控制器，即使任何单独的域控制器停止工作，也可继续复制。

虽然用户可能没有意识到这一点，但是由于进行了多主机复制，它们将更新目录的单个副本。在域控制器上创建或修改目录信息后，新创建或更改的信息将发送到域中的所有其他域控制器，所以其目录信息是最新的。

域控制器需要最新的目录信息，但是要做到高效率，必须把自身的更新限制在只有新建或更改目录信息时。在域控制器之间不加选择地交换目录信息能够迅速搞垮任何网络。Active Directory 已经设计成只复制更改的目录信息。

进行多主机复制时，可能经常会出现完全相同的目录更改发生在多个域控制器的情况。Active Directory 还设计用于跟踪和仲裁对目录的冲突更改，并自动解决几乎所有情况中的冲突。

在一个域中配置多个域控制器能提供容错和负载平衡能力。如果域中的一个域控制器变慢、停止或失败，相同域中的其他域控制器可提供必要的目录访问，因为它们包含相同的目录数据。

与 DNS 集成紧密

Active Directory 使用域名系统(DNS)。DNS 是将更容易理解的主机名(如 mycomputer.hope.com)转换为数字 IP 地址的 Internet 标准服务。它允许识别以及连接 TCP/IP 网络计算机上运行的进程。

DNS 的域名基于 DNS 分层命名结构，这是一种倒置的树状结构。单个根域，在它下面可以是父域和子域(分支和叶子)。如，child.parent.hope.com 这样的 Windows 2000 域名

识别名为 child 的域，它是名为 parent 域的子域，parent 域本身又是根域 hope.com 的子域。

DNS 域中的每台计算机由其 DNS 完全合格域名唯一标识。位于 child.parent.hope.com 域中的计算机的完全合格域名为 computername.child.parent.hope.com。

Active Directory 以三种方式与 DNS 集成：

- Active Directory 和 DNS 具有相同的层次结构。虽然由于不同的用途而独立并以不同方式被执行，但是用于 DNS 的单位名称空间和 Active Directory 具有相同结构。例如，microsoft.com 是 DNS 域和 Active Directory 域。
- DNS 区域可存储在 Active Directory 中。如果用户要使用 Windows 2000 DNS 服务，主区域文件可存储在 Active Directory 中，用于复制到其他 Active Directory 域控制器。
- Active Directory 客户使用 DNS 来定位域控制器。要定位指定域的域控制器，Active Directory 客户查询为特定资源记录配置的 DNS 服务器。

与其他目录服务具有互操性

由于 Active Directory 基于标准的目录访问协议，如轻型目录访问协议（LDAP）第三版和名称服务提供程序接口（NSPI），因此它可与使用这些协议的其他目录服务相互操作。

LDAP 是用于在 Active Directory 中查询和检索信息的目录访问协议。因为它是一种工业标准服务协议，所以可使用 LDAP 开发程序，与同时支持 LDAP 的其他目录服务共享 Active Directory 信息。

Active Directory 支持 Exchange 4.0 和 5.x 客户程序所用的 NSPI 协议，以提供与 Exchange 目录的兼容性。

具有灵活的查询

用户和管理员可使用 Start 菜单、My Network Places 或 Active Directory Users and Computers 上的 Search 命令，通过对象属性快速查找网络上的对象。例如，用户可通过名称、姓氏、电子邮件名、办公室位置或用户帐户的其他属性来查找用户。通过使用全局编录来优化查找信息。

1.1.4　相关名词术语

在正确、深入理解 Active Directory 的概念之前，有必要详细了解一下与 Active Directory 的有关名词或术语。

- 名称空间
- 对象
- 容器
- 目录树
- 域
- 组织单位
- 域树

- 树林
- 站点
- 域控制器

名称空间

从本质上讲，活动目录就是一个名称空间，可以把名称空间理解为任何给定名称的解析边界，这个边界就是指这个名称所能提供或关联、映射的所有信息范围。通俗地说就是在服务器上通过查找一个对象可以查到的所有关联信息总和，如一个用户，如果我们在服务器已给这个用户定义了如：用户名、用户密码、工作单位、联系电话、家庭住址等信息，那上面所说的“总和”广义上理解就是“用户”这个名称的名称空间，因为我们只输入一个用户名即可找到上面所列的一切信息。

名称解析是把一个名称翻译成该名称所代表的对象或信息的处理过程。举例来说，在一个电话目录形成一个名称空间中，可以从每个电话户头的名称解析到相应的电话号码。Windows 操作系统的文件系统也形成了一个名称空间，每个文件名都可以被解析到文件本身（包含它应有的所有信息）。

对象

对象是活动目录中的信息实体，即属性，但它是一组属性的集合，往往代表了有形的实体，比如用户账户、文件名等。对象通过属性描述它的基本特征，比如，一个用户帐户的属性中可能包括用户姓名、电话号码、电子邮件地址和家庭住址等。

容器

容器是活动目录名称空间的一部分，与目录对象一样，它也有属性，但与目录对象不同的是，它不代表有形的实体，而是代表存放对象的空间，因为它仅代表存放一个对象的空间，所以它比名称空间小。比如一个用户，它是一个对象，但这个对象的容器就仅限于从这个对象本身所能提供的信息空间，如它仅能提供用户名、用户密码。其它的如：工作单位、联系电话、家庭住址等就不属于这个对象的容器范围了。

目录树

在任何一个名称空间中，目录树是指由容器和对象构成的层次结构。树的叶子、节点往往是对象，树的非叶子节点是容器。目录树表达了对象的连接方式，也显示了从一个对象到另一个对象的路径。在活动目录中，目录树是基本的结构，从每一个容器作为起点，层层深入，都可以构成一棵子树。一个简单的目录可以构成一棵树，一个计算机网络或一个域也可以构成一棵树。

域

域是网络对象的分组。例如：用户、组和计算机。域中所有的对象都存储在 Active Directory 下。Active Directory 可以常驻在某个域中的一个或多个域控制器下。

在 Windows 2000 中，域是组网的计算机的一个逻辑数据包，这些计算机共同分享同一领域中存储的安全信息。通过域可以提供一种集中化管理网络资源的方法，一台计算机上的用户可以访问同一域中其它计算机上的共享资源，只要该用户拥有适当的权限。

每个域都有一个安全界限，这意味着安全策略和设置（例如系统管理权力、安全策略和访问控制表）不能跨越不同的域，在默认情况下某个域的管理权限只限于该域，例如，具有在一个域中设置安全策略权限的管理员不会自动得到在目录中的任何其他域设置安全策略的授权。特定域的系统管理员有权设置仅属于该域的策略。由于每个域都是一个安全壁垒，因此不同的系统管理员可以在单位中创建和管理不同的域。

要创建域，用户必须将一个或更多的运行 Windows 2000 Server 的计算机升级为域控制器。域控制器为网络用户和计算机提供 Active Directory 目录服务、存储目录数据并管理用户和域之间的交互作用，包括用户登录过程、验证和目录搜索。每个域至少必须包含一个域控制器。

域树

域树由多个域组成，这些域共享同一表结构和配置，形成一个连续的名称空间。树中的域通过信任关系连接起来，活动目录包含一个或多个域树。域树中的域层次越深级别越低，一个“.”代表一个层次，如域 child.hope.com 就比 hope.com 这个域级别低，因为它有两个层次关系，而 hope.com 只有一个层次。

域树中的域是通过双向可传递信任关系连接在一起。由于这些信任关系是双向的而且是可传递的，因此在域树或树林中新创建的域可以立即与域树或树林中每个其他的域建立信任关系。这些信任关系允许单一登录过程，在域树或树林中的所有域上对用户进行身份验证，但这不一定意味着经过身份验证的用户在域树的所有域中都拥有相同的权力和权限。因为域是安全界限，所以必须在每个域的基础上为用户指派相应的权力和权限。

树林

树林是指由一个或多个没有形成连续名称空间的域树组成，它与上面所讲的域树最明显的区别就在于这些域树之间没有形成连续的名称空间，而域树则是由一些具有连续名称空间的域组成。但树林中的所有域树仍共享同一个表结构、配置和全局目录。树林中的所有域树通过 Kerberos 信任关系建立起来，所以每个域树都知道 Kerberos 信任关系，不同域树可以交叉引用其他域树中的对象。树林都有根域，树林的根域是树林中创建的第一个域，树林中所有域树的根域与树林的根域建立可传递的信任关系。

组织单位

包含在域中特别有用的目录对象类型就是组织单位。组织单位是可将用户、组、计算机和其他单元放入活动目录的容器中，组织单位不能包括来自其他域的对象。组织单位是可以指派组策略设置或委派管理权限的最小作用单位。使用组织单位，可在组织单位中代表逻辑层次结构的域中创建容器，这样就可以根据组织模型管理帐户、资源的配置和使用，可使用组织单位创建可缩放到任意规模的管理模型。可授予用户对域中所有组织单位或对单个组织单位的管理权限，组织单位的管理员不需要具有域中任何其他组织单位的管理权，组织单位有点象在 NT 时代的工作组，从管理权限上来讲可以这么理解。

站点

站点是指包括活动目录域服务器的一个网络位置，通常是一个或多个通过 TCP/IP 连接起来的子网。站点内部的子网通过可靠、快速的网络连接起来。站点的划分使得管理员可

以很方便地配置活动目录的复杂结构，更好地利用物理网络特性，使网络通信处于最优状态。当用户登录到网络时，活动目录客户机在同一个站点内找到活动目录域服务器，由于同一个站点内的网络通信是可靠、快速和高效的，所以对于用户来说，可以在最快时间内登录到网络系统中。因为站点是以子网为边界的，所以活动目录在登录时很容易找到用户所在的站点，进而找到活动目录域服务器完成登录工作。

域控制器

域控制器是使用活动目录安装向导配置的 Windows 2000 Server 的计算机。活动目录安装向导安装和配置为网络用户和计算机提供活动目录服务的组件供用户选择使用。域控制器存储着目录数据并管理用户域的交互关系，其中包括用户登录过程、身份验证和目录搜索，一个域可有一个或多个域控制器。为了获得高可用性和容错能力，使用单个局域网（LAN）的小单位可能只需要一个具有两个域控制器的域。具有多个网络位置的大公司在每个位置都需要一个或多个域控制器以提供高可用性和容错能力。

Windows 2000 Server 域控制器扩展了 NT Server 4.0 的域控制器所提供的能力和特性，Windows 2000 Server 多宿主复制使每个域控制器上的目录数据同步，以确保随着时间的推移这些信息仍能保持一致，也就是说是动态的，这就是活动目录的作用。多宿主复制是 WINNT Server 4.0 中使用的主域控制器和备份域控制器模型的发展，在 NT Server 4.0 中只有一个服务器，即主域控制器，拥有该目录的可读写副本。

1.1.5　Active Directory 架构

Active Directory 架构是定义对象种类和对象信息类型的定义集，它可存储在 Active Directory 中。这些定义本身作为对象存储，以使 Active Directory 可以采用管理目录中其余对象所使用的相同对象管理操作来管理架构对象。

架构中有两种类型的定义：属性和对象类（Object Class）也称之为架构对象或元数据，属性与对象类是分开定义的。

每个属性仅定义一次并且可在多个对象类中使用。例如，Description 属性在多个对象类中使用，但是在架构中仅定义一次，以确保一致性。

对象类描述能够创建的目录对象。每一个对象类都包含一组属性。创建对象时，属性存储着描述对象的信息。例如，User 类由许多属性构成，其中包括网络地址、主目录等。Active Directory 中的每个对象都是对象类的实例。

架构的结构和内容由充当架构操作主机角色的域控制器控制。架构的副本被复制到树林中的所有域控制器。这种公用架构的使用确保在整个树林中数据的完整性和一致性。

扩展 Active Directory 架构的推荐方式是通过 Windows 2000 软件开发者工具包中所介绍的 Active Directory 服务接口（ADSI）编程实现。

Active Directory 数据库存储架构信息，在数据库中存储架构将意味着：

- Active Directory 架构是动态更新的，它允许应用程序使用新的属性和对象类来扩展模式，之后立即使用这些模式扩展。
- 对应用程序来说，Active Directory 架构是动态可用的，它允许用户的应用程序可以读

取模式，从而发现哪些对象或属性可用。

- 模式能够使用权限列表保护所有的对象类和属性。权限的使用使得只有授权用户才能修改模式。

1.1.6　Active Directory 客户

Active Directory 客户是连接到 Active Directory 网络的计算机所用的网络客户软件。使用 Active Directory 客户配置的计算机可以通过定位域控制器登录到网络。客户可从 Active Directory 目录的功能中完全受益。

带有 Active Directory 客户的计算机可以是以下两种：

- 运行 Windows 2000 Server 或 Windows 2000 Professional 的计算机
- 运行 Windows 98 或 Windows 95，并安装了附加 Active Directory 客户软件的计算机。

在 Windows 2000 Server 光盘上 Client 文件夹中的单独升级软件包中提供了 Active Directory 客户软件。

1.1.7　轻量目录访问协议

轻量目录访问协议（LDAP—Lightweight Directory Access Protocol）是设计用于在 TCP/IP 网络上使用的通讯协议。LDAP 定义目录客户如何访问目录服务器以及客户如何能进行目录操作并共享目录数据。LDAP 标准由 Internet 工程任务组（IETF）的工作组制定。Active Directory 实现了 LDAP 属性草案规范以及 LDAP 第二版和第三版的 IETF 标准。

由于 LDAP 名称是隐含的，因此 LDAP 被设计成访问目录服务的简单的、有效的方法。因为 LDAP 定义了可进行哪些操作来查询和修改目录中的信息以及如何安全地访问目录中的信息，所以用户可使用 LDAP 查找或列举目录对象并查询或管理 Active Directory。

信息被集中存储在服务器上的 LDAP 目录中。LDAP 目录是一种数据库；然而，它不是关系数据库，LDAP 主要是优化数据读取的性能。LDAP 的目录或数据库的结构与 UNIX 文件系统非常相似：数据按层次存储；有“根”或“基本 DN（专有名称，Distinguished Name）”；目录被进一步细分成组织单位（Organization Units 或 OU）；在这些 OU 中是包含数据的项。这种树—叶结构不仅使 LDAP 变得可扩展，而且当进行简单的搜索或查询时，比传统的关系数据库更快。

LDAP 协议规范约定，活动目录对象由一系列的域组件、组织单位和普通名称表示，它们在活动目录中组成了 LDAP 的命名路径。LDAP 命名路径用于访问活动目录对象，其包含下述内容：

- 可分辨的名称（Distinguished Name）
- 相对可分辨的名称（Relative Distinguished Name）

可分辨名称

例如，hope.com 域、MyOrganizationalUnit 组织单位中名为名为 mycomputer 的计算机的可区分名称是：CN=mycomputer, OU=MyOrganizationalUnit, DC= hope, DC=com。