Microsoft

微软院校认证课程系列教材

活动目录的规划、实现和管理

——以 Windows Server 2003 为例

微软公司　著

高等教育出版社
HIGHER EDUCATION PRESS

微软院校认证课程系列教材

活动目录的规划、实现和管理

——以Windows Server 2003为例

微软公司　著

高等教育出版社

本书的著作权归微软公司所有。未经微软公司书面许可，本书的任何部分不得以任何形式或任何手段复制或传播。著作权人保留所有权利。

图书在版编目（CIP）数据

活动目录的规划、实现和管理——以 Windows Server 2003 为例 / 微软公司著. —北京：高等教育出版社，2005.7

ISBN 7-04-017808-7

Ⅰ.活... Ⅱ.微... Ⅲ.服务器-操作系统（软件），Windows Server 2003-教材 Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2005）第 079680 号

策划编辑 尹 洪 **责任编辑** 萧 潇 **封面设计** 张 楠 **责任绘图** 朱 静
版式设计 史新薇 **责任校对** 金 辉 **责任印制** 宋克学

出 版	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
印 刷	北京中科印刷有限公司		
开 本	787×1092 1/16	**版 次**	2005 年 7 月第 1 版
印 张	18.25	**印 次**	2005 年 7 月第 1 次印刷
字 数	430 000	**定 价**	66.00 元（含光盘）

版权所有 侵权必究

物料号 17808-00

编审委员 刘志鹏　朱之文　田本和　王军伟　郑祖宪
马肖风　王　林　王建国　罗晓中
组织策划 田本和　尹　洪　蒋　斌　周雨阳　蔡　锷
李朝晖　姬　琳
技术编审 蒋　斌　蔡　锷　虞谷晔　袁　一　张　宪
李朝晖　喻艺丹　张广军

Microsoft Official Curriculum 最终用户许可协议

重要须知——请认真阅读——您一旦打开“许可使用内容”包装的密封或以其他方式使用此处的“许可使用内容”，即表示您同意接受本《协议》各项条款的约束：本 Microsoft Official Curriculum 可能包含 Microsoft 或其供应商提供的软件或其他材料（总称“许可使用内容”），其使用应遵守以下各项 Microsoft 提示条款。每个软件程序都受一份最终用户许可协议（《协议》）的约束，而该《协议》是您（个人或单一实体）（“最终用户”）和 Microsoft Corporation（“Microsoft”）之间就允许使用软件及相关介质或印刷材料、“联机”或电子文档和基于 Internet 的服务达成的一份法律协议。本《协议》的修正条款或补充条款可能随软件一起提供。您一旦安装、复制或以其他方式使用“许可使用内容”，即表示您同意接受本《协议》各项条款的约束。如果您不同意，请（a）不要打开“许可使用内容”包装的密封；（b）不要使用软件、文档或其他材料，并且（c）退还“许可使用内容”。

“许可使用内容”随带软件的特别提示

许可证的授予。为与本“许可使用内容”一起使用而提供的任何软件（“软件”）都是 Microsoft Corporation 和（或）其供应商享有著作权的作品。“软件”只授予使用许可，而非出售。任何特定“软件”的使用都应遵守以下各《许可协议》中的一份《许可协议》：

（1）一般使用许可。Microsoft 授予最终用户一份有限的、非独家拥有的、免版权费的许可证，许可其在一台由一位单一用户随时使用或访问的单一计算机上安装和使用“软件”的一份副本，并且最终用户：（a）不得修改“软件”，但下文有明确规定时例外；（b）不得发行“软件”或其任何组成部分；（c）不得出借、出租、租赁、出售、分许可、转让“软件”或将“软件”随附的任何印刷材料用于提供商业运营服务；（d）不得在收费的公立或私立课程中使用“软件”；（e）不得对“软件”进行反向工程、反编译或反汇编；尽管有此项限制，但如果适用法律明确允许上述活动并且仅在适用法律明示允许上述活动的范围内，则例外；并且（f）不得转让“软件”的各项权利，除非本《协议》明确规定。

Microsoft 保留一切其他权利。Microsoft 及其供应商保留“软件”的一切产权和所有权，并且不转让或许可使用“软件”或其任何组成部分的任何权利，除非本《协议》具体说明。

（2）替代使用许可。上述规定的一般使用许可将被任何具体“软件”随附或包括的《许可协议》（如果有）的各项条款取代或替代。除非最终用户首先同意《许可协议》的各项条款，否则将无法安装附带或包括该《许可协议》的“软件”。Microsoft 保留一切其他权利。Microsoft 及其供应商保留“软件”的一切产权和所有权，并且不转让或许可使用“软件”或其任何组成部分的任何权利，除非本《协议》明确说明。

（3）样本代码使用许可。如果将特定代码或一个样本应用程序作为“许可使用内容”中包括的实验室练习的部分提供（“样本代码”），则这类“样本代码”以“现有状况”被提供，并且没有任何类型的保证。Microsoft 授予您一份有限的、非独家拥有的、免版权费的许可证，

此为试读，需要完整PDF请访问：www.ertongbook.com

许可您为了个人使用的目的而安装、使用、修改和复制“样本代码”，条件是您不得：（a）发行“样本代码”或其任何组成部分；（b）出借、出租、租赁、出售、分许可或转让“样本代码”；（c）在收费的公立或私立课程中使用“样本代码”；并且（或者）（d）转让“样本代码”的任何权利。如果您修改“样本代码”，您应该根据 Microsoft 的请求，自付费用为因您或代表您对“样本代码”做出的任何修改而使 Microsoft 和 Microsoft 的分公司、关联公司、董事、高级主管、员工、代理商和独立供应商面临的任何索赔或诉讼提供辩护，并且您须赔偿 Microsoft 因这类索赔而招致的任何费用、损害赔偿和手续费方面的合理开支（其中包括但不限于律师费和其他专业人士收取的费用），并使其免受任何损害。Microsoft 应：（a）以书面形式就任何这类索赔或诉讼向您提供合理的及时提示，并且允许您通过 Microsoft 和您双方都接受的律师对这类索赔或诉讼进行答辩和辩护；（b）在您支付费用的情况下向您提供信息、协助和授权，以帮助您为这类索赔或诉讼进行辩护。您不对 Microsoft 在未经您书面允许的情况下做出的任何和解负责，但您不得以不合理的方式拒绝给予这样的允许。

其他许可限制。安装“软件”仅供最终用户根据适用的《许可协议》使用，并且除非以其他方式在另外一份协议中达成一致意见，否则得不到 Microsoft 或其供应商提供的技术或其他支持服务。法律明确规定：禁止在违反《许可协议》的情况下对“软件”进行任何复制或再发行。明确禁止为进一步复制或再发行软件而将“软件”复制到任何服务器或地点。

美国政府许可使用权利。根据 1995 年 12 月 1 日当天或之后签发的请求而提供给美国政府的所有软件，均根据本协议其他部分规定的商业许可使用权利和限制予以提供。根据 1995 年 12 月 1 日之前签发的请求而提供给美国政府的所有软件，视情况根据 FAR，48 CFR 52.227-14（1987 年 6 月）或 DFAR，48CFR252.227-7013（1988 年 10 月）中规定的“限制权利”予以提供。

免责条款。“软件”仅根据《许可协议》的各项条款对“软件”提供保证（如果提供保证的话）。除非在《许可协议》中提供保证，否则 Microsoft Corporation 和（或）其供应商就“软件”不提供任何的保证和条件，包括适销性、适用性、所有权和不侵权的所有默示保证和条件。

“许可使用内容”随带文档和（或）其他材料的具体说明

允许从“许可使用内容”（“文档”）中打印文档（如实验室说明等），条件是：（a）将这类文档用于您的个人培训，并且不得再出版或在任何网络计算机上张贴或以任何介质形式广播这类文档，并且（b）不得对任何文档做出任何修改。

明确禁止对任何介质上包含的作为“许可使用内容”组成部分的录像、录音、图形和（或）任何其他材料（“其它材料”）进行任何复制或再发行。

“许可使用内容”的各组成部分均受商业包装法律和其他法律的保护，并且不得全部或部分予以复制或模仿。除非 Microsoft 明示允许，否则不得复制或转发“许可使用内容”中的任何徽标、图形、声音或图像。

无保证。Microsoft 和（或）其供应商不对“许可使用内容”中不论为任何目的而可能包含的文档或其他材料中的信息、音像或任何其他内容是否合适提供任何保证，无论该类文档、信息、音像或任何其他内容是为何目的。所有这类文档和其他材料均以“现有状况”提供，没有

任何类型的保证。Microsoft 和（或）其供应商特此就文档和其他材料不提供任何的保证和条件，包括适销性、适用性、所有权和不侵权的所有默示保证和条件。

有关第三方站点链接的说明

至第三方站点的链接。您可以使用“许可使用内容”链接至第三方站点。第三方站点不由 Microsoft 控制，并且 Microsoft 不对任何第三方站点的内容、第三方站点包含的任何链接或第三方站点的任何更改或更新负责。Microsoft 不对从任何第三方站点收到的网站广播或任何其他形式的传输负责。Microsoft 仅为了您的方便向您提供这些至第三方站点的链接，并且包括任何链接并不暗示 Microsoft 认可相应的第三方站点。

有关全部“许可使用内容”的说明

“许可使用内容”中包括的“软件”、文档和其他材料可能包含不准确的技术内容或印刷错误。可能定期对内容进行修订。Microsoft 可随时在不提供通知的情况下对“许可使用内容”中规定的产品和（或）程序进行改进和（或）更改。

免责条款。除非另行说明，否则本《协议》提及的公司、产品、人物、特性和（或）数据均属虚构，并且无意以任何方式代表任何真实的个人、公司、产品或活动。

保留权利和所有权。Microsoft 保留未在本《协议》中明示授予您的一切权利。“许可使用内容”受著作权和其他知识产权法律及条约的保护。Microsoft 或其供应商拥有“许可使用内容”和其中组件的所有权、著作权和其他知识产权。

同意使用数据。您同意：Microsoft 及其关联公司可以收集和使用作为提供给您的产品支持服务的一部分而收集的与“许可使用内容”相关的技术信息（如果有）。Microsoft 可以将此信息仅用于改进我们的产品或为您提供订制的服务或技术，并且不会以能识别您身份的方式披露此信息。

额外软件/服务。除非我们随下列更新、增补、补充组件或基于 Internet 的服务组件一起提供其他应适用的条款，否则本《协议》适用于 Microsoft 在您获得“许可使用内容”的初始副本之日后可能提供给您的或为您准备的“许可使用内容”的更新、增补、补充组件或基于 Internet 的服务组件。就通过使用“许可使用内容”而提供给您的或为您准备的任何基于 Internet 的服务而言，Microsoft 保留停止这类服务的权利。

出口限制。您承认“软件”受美国出口法律管辖。您同意遵守所有适用于“软件”的国际法和国内法，其中包括美国出口管理条例以及由美国和其他国家（地区）政府颁发的最终用户、最终使用和目的地方面的限制。要了解详情，请访问 http://www.microsoft.com/exporting/网站。

许可使用内容的转让。“许可使用内容”的原始最终用户可以将本《协议》和“许可使用内容”永久性地一次直接转让给另外一位最终用户，条件是该原始用户不得保留“许可使用内容”的任何副本，并且必须转让“许可使用内容”的所有部分（包括全部组件、介质及印刷材料、任何升级版本、各《许可协议》和（如果适用）正版标签）。这种转让不得为非直接转让，如以寄售方式转让。在转让之前，接收“许可使用内容”的最终用户必须同意遵守《协议》的

各项条款。如果“许可使用内容”是一个升级版本，任何转让都必须包括“许可使用内容”的所有先前版本。

终止。如果您未遵守本《协议》的各项条款和条件，在不损害其他权利的情况下，Microsoft 可终止本《协议》。如此类情况发生，您必须销毁“许可使用内容”的所有副本及其全部组成部分。

适用法律。本《协议》受中华人民共和国法律管辖。

责任限制。在适用法律所允许的最大范围内，无论损害赔偿是否在履行合约、出现疏忽或发生其他侵权行为时发生，Microsoft 和（或）其供应商绝不就因“许可使用内容”的任何组成部分或所有组成部分的使用或性能、因提供或未能提供服务、或因可从“许可使用内容”得到的信息而引起的或有关的任何特殊的、间接的、或特定的损害赔偿或任何损害赔偿（包括但不限于因营业中断，因使用、数据或利润的丧失，或因任何其他金钱上的损失而造成的损害赔偿）承担赔偿责任。在任何情况下，Microsoft 的全部责任以及您获得的惟一赔偿将限于为“许可使用内容”实际支付的款额或五美元（U.S.$5.00）以两者中的较高款额为准；但是，如果您已经签订了一份 Microsoft 服务协议，Microsoft 对这类服务的全部责任将遵守该协议各项条款的规定。由于某些国家和地区不允许排除或限制责任，上述限制条款可能不适用于您。

全部协议；规定可分割性。本《协议》（包括随“许可使用内容”提供的本《协议》的任何补充条款或修正条款）是您与 Microsoft 之间就“许可使用内容”和支持服务（如果有）达成的全部协议，并且取代“许可使用内容”或本《协议》中所包含的任何其他标的之所有先前或同时存在的口头或书面的通信、建议和声明。如果任何 Microsoft 支持服务的政策或计划的条款与本《协议》的条款有冲突，以本《协议》的条款为准。如果本《协议》的任何条款被认定为作废、无效、不能执行或非法，其他条款应继续完全有效。

如果您对本《协议》有任何疑问，或者如果您由于某种原因希望与 Microsoft 联系，请使用“许可使用内容”中附带的地址信息与微软（中国）有限公司联系，或在http://www.microsoft.com网站访问 Microsoft。

准则和定义

“许可使用内容”是一种专门设计的培训工具，供 Microsoft Certified Technical Education Center（Microsoft CTEC）、Microsoft Certified Partner（MCP）、Microsoft 认证培训讲师（MCT）、IT Academy 计划成员和 Microsoft 可能随时以书面形式指定的其他机构使用。“许可使用内容”旨在使 Microsoft 的技术培训渠道能够向计算机专业人士提供系统、支持和开发培训课程。为了取得最佳成果，“许可使用内容”应该由 Microsoft 认证培训讲师（MCT）在课堂环境或在线学习环境中讲授。

Microsoft Official Curriculum（MOC）：由 Microsoft 开发的系列课程材料，用于提供 Microsoft 产品和技术的培训和解决方案。

Microsoft 认证培训讲师（MCT）：具备必要的教学和技术能力并且由 Microsoft 认证为能够通过 Microsoft CTEC 讲授 Microsoft Official Curriculum 的个人。

Microsoft Certified Technical Education Center（Microsoft CTEC）：已经符合 Microsoft 对

指定其为下列场所的资格要求：（a）一处 Microsoft Certified Partner（MCP）营业点、和（b）一处提供 Microsoft CTEC 服务的任何场所。这些培训中心使用 MCT 向学生提供 MOC 课程培训。

Microsoft Certified Partner：已经符合被指定为 Microsoft Certified Partner 的资格要求的任何场所。

IT Academy 计划成员：已经符合被指定为 IT Academy 计划成员的资格要求的任何院校。

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章　Active Directory 体系结构简介

在当今的商业环境当中，网络已经成为日常商务活动和工作中不可或缺的一部分。大量的业务操作需要调动分散在各处的资源，并且资源的状态也在不断变化和更新之中。为了适应这种需求，现代操作系统需要一种机制来管理分散在网络中的各种元素，并保持对这些元素状态的跟踪。由此引入了目录的概念。通过使用目录，可以标记和组织网络上所有的资源，使用户和应用程序可以很方便地检索和使用资源，而无需关心它们位于何处。基于目录提供的服务即为目录服务。

Active Directory（活动目录）是一种目录服务，它是 Windows 2003 网络的核心元素。Active Directory 就像一本百科全书，将真实世界中的每个对象抽象为目录中的各个元素并分门别类加以管理。真实的网络环境中的应用程序、文件、打印机、计算机，乃至每一个公司成员和相应的资产等，都可以在 Active Directory 中找到相应的对象。基于 Active Directory 的服务即为 Active Directory 目录服务。管理员可以基于 Active Directory 目录服务集中管理和查找分散资源，并指定各种管理权限，实现各种基于网络的管理手段。

本章介绍 Active Directory 目录服务逻辑结构与物理结构及其目录服务功能。本章还介绍 MMC 管理单元、命令行工具、可用于管理 Active Directory 组件的 Windows 脚本宿主服务，另外还概述 Active Directory 的设计、规划和实现过程。

学习完本章后，你将能够：

- 掌握 Active Directory 的体系结构
- 掌握 Active Directory 的工作过程
- 使用管理单元检查 Active Directory 组件
- 掌握 Active Directory 的设计、规划和实现过程

1.1　Active Directory 的体系结构

Active Directory 的体系结构分为逻辑结构和物理结构。必须对 Active Directory 的逻辑结构与物理结构进行规划，才能较好地满足企业的需求。为了管理 Active Directory，必须首先理解这些结构。

学习完本节后，你将能够：

- 掌握 Active Directory 的功能
- 掌握 Active Directory 的逻辑结构
- 掌握 Active Directory 的物理结构
- 掌握操作主机角色

1.1.1　Active Directory 的作用

Active Directory 可以存储用户、计算机和网络资源的信息，并且使资源可以被用户和应用

程序访问。它提供了一种统一的方法来命名、描述、定位、访问、管理和保护这些资源。

Active Directory 具有如下功能：

- 对网络资源的集中控制。通过对诸如服务器、共享文件和打印机等的资源进行集中控制，只有授权用户可以访问 Active Directory 中的资源——例如，可以通过给行政部的激光打印机设置权限，设置只有行政部人员可以使用该打印机——从而避免非法使用和资源浪费
- 集中和分散资源管理。管理员通过一致的管理界面，能够从中心位置管理分布的客户端计算机、网络服务和应用程序。例如，管理员可以编写一个组策略，使得某个应用程序的升级包能够在网络中每个用户开机的时候就自动安装，从而免去了单独部署的麻烦。管理员也能够通过向其他管理员委派资源控制权，从而分散管理任务。例如，管理员可以把销售部的计算机和打印机纳入到一个组织单元中，将它们的管理权限委派给销售部的技术支持人员，从而减少自己的工作量。
- 在逻辑结构中安全地存储对象。Active Directory 使用层次逻辑结构把所有资源作为对象存储。例如，可以按照公司的组织结构和业务需求来组织相应的组织单元（Organizational Unit，OU），将网络资源分布在相应的组织单元中，实现分级管理。Active Directory 还会对存储在其中的对象进行加密，这样可以保证数据的安全
- 优化网络流量。Active Directory 物理结构能够更加高效地使用网络带宽。例如，当用户登录到网络时，能够保证用户是由离他们最近的验证中心进行身份验证，从而减小了网络流量

1.1.2 Active Directory 服务的优势

Windows Server 2003 系列中的 Active Directory 是对 Windows NT 中的扁平域模型的重大改进。Active Directory 集成在 Windows Server 2003 系列中，并具有以下优势：

- 集中的数据存储。Active Directory 中的所有数据都保存在一个独立的分布式数据库中，允许用户从任何位置访问这些信息。和其他数据存储方式相比，独立的数据存储所需的管理和重复劳动更少，并且提高了数据的可用性和可组织性
- 可伸缩性。Active Directory 使管理员能通过配置域和树以及域控制器的放置来调整目录，以满足业务和网络的要求。Active Directory 允许每个域有几百万个对象，并使用索引技术和先进的复制技术来加速处理
- 可扩展性。Active Directory 数据库的架构可以被扩展，以便允许自定义的信息类型
- 可管理性。Active Directory 是基于分级组织结构的。这些组织结构使管理员能更容易地控制管理权限和其他安全设置，并且使用户能更容易地定位网络资源，比如文件和打印机
- 与 DNS（Domain Name System，域名系统）相集成。Active Directory 使用了 DNS，它是一种基于 IP 地址的 Internet 标准服务，可以把可读性好的主机名称转换为 IP 地址。虽然 Active Directory 和 DNS 是分开的，并且由于用途不同而实现方式不同，但是它们有相同的分级结构。Active Directory 客户端使用 DNS 来定位域控制器。在使用 Windows Server 2003 DNS 服务时，可以将主 DNS 区域存储在 Active Directory 中，并启用到其他 Active Directory 域控制器的复制
- 客户端配置管理。Active Directory 提供了新技术来管理客户端配置问题，例如，用户

此为试读，需要完整PDF请访问：www.ertongbook.com