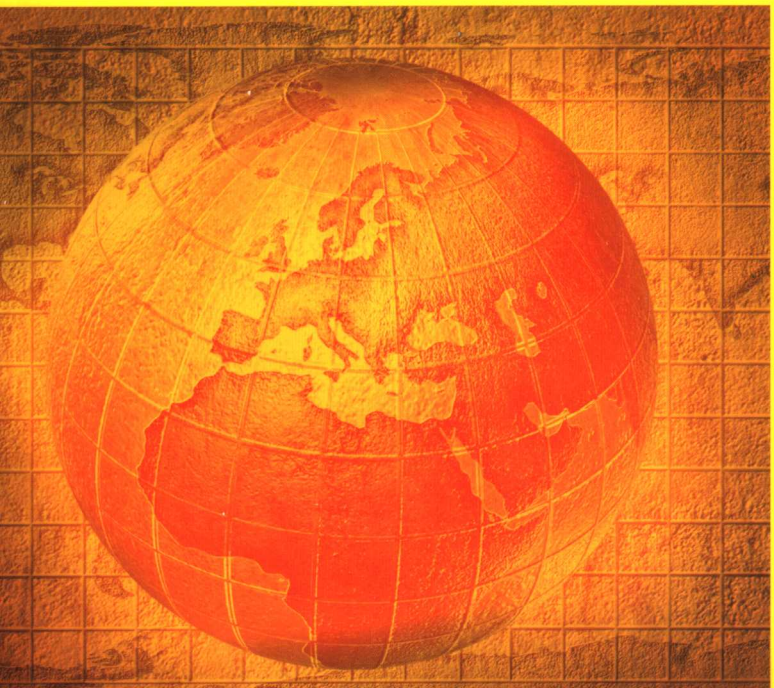
Windows Server 2003

活动目录

实战指南

刘晓辉　王淑江　等　编著



- 活动目录整体规划
- 域控制器具体部署
- 用户权限全面管理
- 策略认证深入应用
- 状态性能远程监控
- 目录故障诊断排除

人民邮电出版社
POSTS & TELECOM PRESS

Windows Server 2008

活动目录

Windows Server 2003
活动目录实战指南

刘晓辉　王淑江　等编著

人 民 邮 电 出 版 社
北　京

图书在版编目（CIP）数据

Windows Server 2003 活动目录实战指南 / 刘晓辉等编著.
—北京：人民邮电出版社，2007.3
ISBN 978-7-115-15706-5

Ⅰ. W... Ⅱ. 刘... 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（2006）第 161758 号

内 容 提 要

本书从活动目录的实际应用入手，引导读者理解活动目录的原理与操作，掌握活动目录的设计与实施，以满足网络服务和管理的需要。书中内容涉及活动目录林和域的规划与设计，组织单元、用户和用户组的管理，域控制器的管理与维护，组策略、动态 DNS、身份认证、权限管理等网络目录应用，以及活动目录的性能监控与故障排除。

本书内容全面、语言简练、深入浅出、图文并茂、贴近实战，是一本不可多得的活动目录技术参考书。

本书适用于技术支持人员、系统管理人员、网络管理人员、MCSE 应试人员，以及对计算机系统维护和网络管理感兴趣的计算机爱好者。

Windows Server 2003 活动目录实战指南

◆ 编　　著　刘晓辉　王淑江　等
责任编辑　陈　昇

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
人民邮电出版社河北印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787 × 1092　1/16
印张：47.5
字数：1 509 千字　　2007 年 3 月第 1 版
印数：1–5 000 册　　2007 年 3 月河北第 1 次印刷

ISBN 978-7-115-15706-5/TP

定价：78.00 元

读者服务热线：(010)67132705　印装质量热线：(010)67129223

前　言

随着网络资源的不断丰富和网络应用的不断深入，对用户安全和访问权限的要求也就越来越高，对用户实现自动化管理的需要也就越来越迫切。在这种情况下，安装一台或多台域控制器、创建活动目录，实现网络用户访问权限、身份认证、用户界面的统一管理，就成为一种必要。

活动目录作为网络资源的集合，不仅容纳了网络内所有的共享资源（共享文件夹、共享打印机等），而且也容纳了网络内的所有用户和用户组。因此，借助活动目录，不仅可以让用户迅速、容易地寻找到所需要的数据，而且可以轻松实现对用户访问权限的限制与管理。

作为定制用户桌面与安全的组策略，与活动目录紧密联系在一起。借助组策略，可以有效地实现对网络客户的控制与管理，从而实现对用户访问权限的控制，并实现软件分发、系统更新、远程安装等管理任务，最大限度地保证客户端、乃至整个网络的安全。此外，许多网络服务（如动态 DNS 服务、DFS 服务等）和网络安全认证（如 IIS 认证、VPN 认证、IEEE802.1x 认证等）也都依赖于活动目录。

由此可见，活动目录在网络中拥有不可替代的重要位置。作为一本对活动目录的配置和应用进行全面阐述图书，相信一定会得到广大系统管理员的认同和欢迎。

作为一个系统管理员，在网络搭建完成并实现一些基本的网络服务之后，接下来要考虑的就是如何保障网络资源的访问安全，如何保证数据的存储安全；如何避免对网络的滥用；如何实现系统的快速维护，以及操作系统和应用软件的快速分发。尽管可以采取的措施非常多，但是，所有的技术手段都离不开活动目录的支持。因此，只有安装并配置了活动目录，才能很好地实现这一切。

既然活动目录如此重要，而许多系统管理员对活动目录又知之甚少，那么，我们现在适时推出这样一本专门的图书，应当说与网络的发展步伐是合拍的，与网络发展需求是吻合的，也必然会得到广大系统管理员的认同。本书从实际应用的角度出发，全面深入地探讨了活动目录管理的方方面面，包括了规划设计、对象管理、配置维护、认证应用、故障排除、性能监控等所有关于活动目录的理论与技术。

本书由刘晓辉、王淑江编著，田俊乐、王春海、李海宁、陈志成、韩文智、赵卫东、刘淑梅、李文俊、杨伏龙、许广博、白晓明、肖丽芳等也参与了部分章节的编写工作。笔者长期从事系统维护和网络管理工作，具有一定的理论水平和丰富的实践经验，迄今为止，已经出版了 50 余部计算机类图书，均以易读、易学、实用的特点，受到众多读者的一致好评。本书是作者的又一呕心沥血之作，希望能对大家的系统维护和网络管理工作有所帮助。由于笔者水平所限，书中难免存在一些错误与不足，希望读者不吝赐教。另外，如果读者对本书有何疑问或需要获得技术支持，请发 E-mail 至 hslxh@163.com。

编　者

2007.1

目　录

第 1 章　活动目录概述

活动目录（Active Directory）是 Windows 2000 Server 和 Windows Server 2003 系统中的目录服务。Active Directory 是一种网络服务，它标识网络上的所有资源，信息可以分散在多台不同的计算机上，保证快速访问和容错；同时，无论用户从何处访问或信息处在何处，它对用户都提供统一的视图。活动目录不仅集成了关键服务和关键应用，还集成了当今关键的数据访问。

1.1　活动目录概述

活动目录（Active Directory）是指存储网络资源信息的目录，以及让这些信息可供网络用户使用的所有服务。网络中所有的资源，包括用户账户、文件数据、打印机、服务器、数据库、组、计算机和安全策略等，都可以存放于活动目录中，从而使用户的检索、使用和管理变得更加简单和方便。

1.1.1　活动目录的重要意义

电话簿中记录着亲朋好友的姓名、电话、地址、生日等信息，可以很容易地从中找到自己想要的信息，这就是电话目录。Windows 资源管理器中记录着文件的文件名、大小、创建和修改日期、存储位置等数据，便于用户迅速查找自己所需要的文件，这就是文件目录。也就是说，目录服务所提供的功能，就是让用户很容易地在目录内寻找所需要的数据。例如，114 查号台是一种目录服务，百度（Baidu）网站所提供的搜索功能也是一种目录服务。在 Windows Server 2003 域内提供目录服务的组件就是活动目录，它负责目录数据库的保存、新建、删除、修改与查询等服务。

活动目录的意义在于以下几方面。

- 简化管理。谈到活动目录就不能不说起域，域是指网络服务器和其他计算机的一种逻辑分组，凡是在共享域逻辑范围内的用户都使用公共的安全机制和用户账户信息，每个使用者在域中只拥有一个账户，每次登录的是整个域。

活动目录用于将域中的资源分层次地组织在一起。每个域都包含一个或多个域控制器。域控制器是一台运行 Windows 2000 Server 或 Windows Server 2003 的计算机，它存储域目录的一份完整的副本。为了简化管理，域中的所有域控制器都是对等的。可以在任意一台域控制器上进行修改，更新的内容将被复制到该域中所有其他的域控制器。活动目录为管理网络上的所有资源提供一个单一入口，从而进一步简化了管理。因为活动目录提供一个单一的入口来登录所有网络资源，所以管理员可以登录任意一台计算机并管理网络中任何计算机上的对象。

- 提升网络安全性。安全性通过登录身份验证及目录对象的访问控制集成在活动目录之中。通过单击网络登录，管理员可以管理分散在网络各处的目录数据和组织单位，经过授权的网络用户可以访问网络任意位置的资源。基于策略的管理则简化了网络的管理，即便是那些最复杂的网络也是如此。

活动目录通过对象访问控制列表及用户凭据保护其存储的用户账户和组信息，因为活动目录不但可以保存用户凭据，还可以保存访问控制信息，所以登录到网络上的用户既能够获得身份验证，也可以获得访问系统资源所需的权限。例如，在用户登录到网络上的时候，安全系统首先会利用存储在活动目录中的信息验证用户的身份，然后，在用户试图访问网络服务的时候，系统会检查在服务的自由访问控制列表（DCAL）中所定义的属性。

因为活动目录允许管理员创建组账户，管理员可以更加有效地管理系统的安全性。例如，通过调整文件的属性，管理员能够允许某个组中的所有用户读取该文件。通过这种办法，系统将根据用户组的成员身份控制其对活动目录中对象的访问操作。

- 具有很强的可扩展性。Windows Server 2003 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，或者给现有的对象类增加新的属性。计划包括可以存储在目录中的每个对象类的定义和属性。例如，在电子商务上可以给每个用户对象增加一个购物授权属性，然后存储每个用户购买权限作为用户账户的一部分。
- 具有很强的可伸缩性。活动目录可包含在一个或多个域中，每个域可以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。多个域可组成为域树，多个域树又可组成为树林，活动目录也就随着域的伸缩而伸缩，较好地适应了单位网络的变化。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中。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。信息复制为目录提供了信息可用性、容错、负载平衡和性能优势，活动目录使用多主机复制，允许用户在任何域控制器上同步更新目录。多主机模式具有更大容错的优点，因为使用多域控制器时，即使任何单独的域控制器停止工作，也可继续复制。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中，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的时候，以免在网络高峰期进行同步而影响网络速度。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。通过活动目录就能达到只复制更改的目录信息，而不至于大量增加域控制器的负荷。
- 与 DNS 集成紧密。活动目录使用域名系统（DNS）来为服务器目录命名，DNS 是将更容易理解的主机名转换为 IP 地址的 Internet 标准服务，利于在 TCP/IP 网络中计算机之间的相互识别和通信。DNS 的域名基于 DNS 分层命名结构，这是一种倒置的树状结构，在单个根域下面可以是父域和子域（分支和叶子）。
- 与其他目录服务具有互操作性。由于活动目录是基于标准的目录访问协议，许多应用程序界面（API）都允许开发者进入这些协议，例如活动目录服务界面（ADSI）、轻型目录访问协议（LDAP）第 3 版和名称服务提供程序接口（NSPI），因此它可以和使用这些协议的其他目录服务相互操作。LDAP 是用于在活动目录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活动目录信息。活动目录支持 Microsoft 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。
- 灵活的信息查询。加入活动目录管理的任何用户均可使用“开始”菜单、“网上邻居”或“活动目录用户和计算机”上的“搜索”命令，通过对象属性快速查找网络上的对象。例如可以通过名字、姓氏、电子邮件名、办公室位置或用户账户的其他属性来查找用户等。

1.1.2 活动目录对象

所谓的 Active Directory 对象就是指域控制器中包含相同属性的实体组成的集合，例如计算机、用户、打印机等。属性就是用来描述目录对象可以标识的数据，例如一个用户的属性可能是用户姓名和电子邮件地址等。安装活动目录后依次单击“开始”→“管理工具”→“Active Directory 用户和计算机”，这里显示的都是活动目录的对象。

1. 默认容器对象

在安装活动目录过程中就已经自动创建了一些默认的容器（Container）对象，这些容器对象中都包