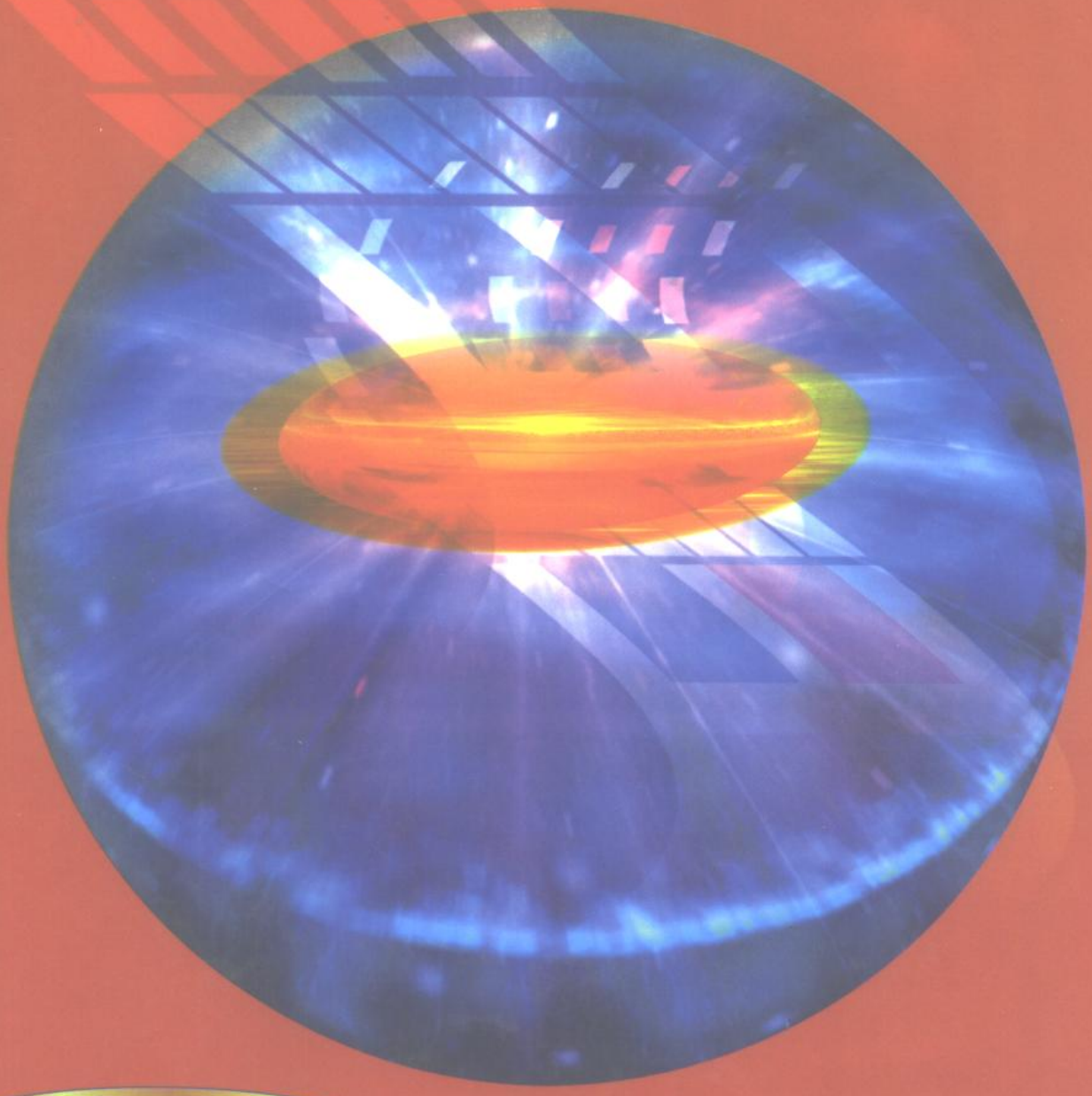
Windows 2000 Server

中文版高级使用指南

徐 英 韩京才 等编



机械工业出版社
China Machine Press

Windows 2000 Server 中文版高级使用指南

徐英　韩京才　宋一中　高秀峰　夏良华 等编

机 械 工 业 出 版 社

本书介绍了 Windows 2000 Server 的最新网络技术，详细介绍了网络连接、活动目录以及网络安全规划和设计；讨论了 Windows 2000 Server 的安装和存储管理、打印管理、索引管理以及监控和诊断、备份与还原恢复、容错、灾难防护等内容。概念、理论介绍和具体操作结合，不仅是 Windows 2000 Server 操作的必备指南，也是深入理解、掌握和开发 Windows 2000 Server 的必备读物。

本书内容翔实、操作简便，是广大计算机爱好者的良师益友。

图书在版编目（CIP）数据

Windows 2000 Server 中文版高级使用指南/徐英等编. —北京：机械工业出版社，2000.4

ISBN 7-111-07979-5

Ⅰ. W… Ⅱ. 徐… Ⅲ. 计算机网络-服务程序，Windows 2000 Server Ⅳ. TP393.09

中国版本图书馆 CIP 数据核字(2000)第 05349 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

责任编辑：曲彩云

封面设计：姚毅 责任印制：何全君

三河市宏达印刷厂印刷 · 新华书店北京发行所发行

2000 年 4 月第 1 版第 1 次印刷

787mm×1092mm1/16 · 28.25 印张 · 682 千字

0001—5000 册

定价：45.00 元

前　言

感谢您使用本书。

未来的世界是一个网络世界，学习和掌握一定的网络技术将成为您提高工作、学习和生活效率与质量的基本技能。我们希望本套丛书将为您打开一扇希望之门，成为您在未来的网络世界中生存、发展的起点（当然了，您打开本套丛书的时候，也可能是打开了一个潘多拉盒子）。

Windows 2000 植根于微软对未来网络世界的基本设想和网络技术未来发展的许多新认识，是为服务器开发的多用途操作系统，可为部门工作组或中小型公司用户提供文件和打印、应用程序、Web 和通讯等各种服务。它是一个性能更好、工作更稳定、更容易管理的网络操作系统平台。

Windows 2000 Server 版是 Windows NT 4.0 Server 的替代品，最重要的改进是“活动目录”技术。活动目录采用了 Internet 标准技术，是集成在系统中的、具有扩展性的多用途目录服务技术。

这套丛书从基本概念、基本操作开始，逐步深入，直至比较核心的高级内容。全书共分三册：《Windows 2000 Server 中文版使用指南》、《Windows 2000 Server 中文版实用大全》和《Windows 2000 Server 中文版高级使用指南》，分别将“操作”、“配置”和“优化”作为自己的核心内容，层层深入、步步提高，有重点地向您介绍 Windows 2000 网络的操作、使用、规划、管理与优化。

在内容编排上，第一册基本假设读者没有关于网络的丰富知识，第二册假设读者对网络底层协议、服务基本了解，第三册则假设读者对网络有比较深刻的认识。尽管如此，不管您是网络初级用户还是高级管理员，每一册书都为您提供了一些新的知识和技能。比如一些基本概念在不同分册中解释的深度是不同的，一些基本操作为什么如此的解释也不相同，所以，您最好把这套丛书当作一个整体。当需要深入理解一个概念时，您可以跳跃式地阅读下一分册，或者进入中高级阶段后，您也可以跳回去阅读前一分册。只有这样，您才能够比较全面、深刻地掌握 Windows 2000 Server。

编写本套丛书时，我们心目中的读者对象主要有四类。

第一是使用 Windows NT 的网络管理员。这些管理员将发现，现在安装、升级、维护和管理网络更轻松了；他们也将发现，Windows 2000 所奠基于其上的网络理念会为他们的工作提供更多新的思想和设计。在必要的时候，作者总是会提醒这些读者，Windows 2000 Server 和 NT 的相似与不同，便于他们顺利地过渡到新的操作系统。

第二是受管理员委托执行一些网络管理任务的用户。这些人没有管理员那样广泛的权力，但他们执行一些特定任务，是维护、管理一个高效网络必不可少的人。这类用户可以轻易地找到解释其完成特定任务所需掌握的基本概念以及操作的基本步骤的章节，比如备份或打印管理等。

第三是那些对联网并不陌生、但并没有深刻理解而工作又离不开网络的人。他们将

从本套丛书中获得有关网络的基本概念、基本协议以及网络工作的基本机制的全面知识。通过阅读本套丛书，加上网络管理员的点拨和自学，这些人将能够从一个只知其然的被动用户过渡到知其所以然的熟练用户。

第四是那些熟悉 Windows 9x 操作系统、希望使用 Windows 2000 Professional 并且期望在 IT 行业谋生的人。这套丛书将为他们提供必要的知识，使之能够循序渐进，在未来的网络世界里找到自己的立锥之地。

本书共分 12 章。第 1 章概括地介绍 Windows 2000 Server 网络安全性；第 2、3、4 章分别介绍了网络安全性配置与分析、验证与审计和公共密钥架构这几个方面的问题。第 5、6、7、8、9 章介绍了 TCP/IP 设置与管理、因特网验证服务与管理、路由、远程访问和 IPSec 设置与管理等有关网络设置方面的知识。第 10 章介绍了目前其他协议设置与管理的情况。第 11、12 章介绍了网络的连接和连接管理者管理工具包的知识。各章在内容编排上始终是理论讨论和具体操作结合。如果您觉得知其然就足够了，您可以专心阅读操作部分内容；如果您要求自己不仅要知其然，还要知其所以然，本书正是为您这样的读者编写的。

这套丛书是多人合作的成果。本书第 1 章由康广先生和徐英女士编写，第 2 章由宋一中先生编写，第 3 章由梁玉英女士和徐英女士编写，第 4 章由高军先生编写，第 5 章由刘建尧先生和徐英女士编写，第 6 章由鄢格青先生和宋一中先生编写，第 7、8 章由鄢格青先生和韩京才先生编写，第 9、10 章由耿斌先生和徐英女士编写，第 11、12 章由高秀峰先生和夏良华先生编写，参加本书审稿和提供资料的还有王力、孙晓、范童、焦叙、齐禾元、刘利、刘结芳。

由于作者水平有限，编写时间仓促，书中难免有疏漏和错误，恳请广大读者提出宝贵意见。

编　者

目　　录

第 1 章　网络安全性概述

提起安全问题，我们常常会想到“坏家伙”偷偷进入网络窃取秘密或进行破坏的一系列场景。其实问题远比这复杂得多，网络的安全不仅包括外部造成的破坏，还包括内部机制不健全引发的损坏。毫无疑问，这是一个极其复杂又极其重要的问题，但是在本书中仅能就问题的几个方面做一些介绍。我们将分几章就网络的安全性与您进行探讨，本章是一个概括性的介绍，后面几章将分别讨论验证与审核、公共密钥结构和安全配置与分析等问题。

本章主要内容：

- 安全综述（Windows 2000 Server 的安全新特性；安全性基本概念等）
- 关于安全性的几个重要问题（服务器；用户、计算机和组；访问控制；委托管理；数据保护；安全模板等）

1.1　安全综述

如今地球已经变成了一个大村落，那种与世隔绝的桃花源式的生活恐怕只有到书中寻觅了。每个人、每个组织与外界信息的交流都日益增加，因此对安全性的要求也越来越高。

在您的计算机环境中建立安全机制能够为您带来以下好处：

首先，一个好的安全系统会验证那些试图访问您的资源的人们的身份。这样可以防止那些非法用户访问、偷窃或破坏系统资源，比如敏感的数据或专门针对某些具体任务设计的计算机程序。

其次，一个好的安全系统能使系统中特殊的资源免受用户不适当访问造成的损坏。例如，通过实行安全机制，您可以确保只有合适的管理人员才可以访问雇员工资的信息。

最后，一个好的安全系统会提供一个简单有效的方法为您的系统建立并维护安全机制。例如，使用口令，这广泛适用于您的系统中所有用户。

通过一个适用于您的特殊业务的系统安全机制，您可以建立一个能够提供用户所需的所有信息和资源的计算机环境，并且能保护这些信息和资源免受损坏和未经授权的访问。

1.1.1 Windows 2000 Server 的安全新特性

安全新特性

Windows 2000 在安全性方面进行了一些改进，实现了一些新特性：

- 对安全策略和帐户信息的中央存储；
- 通过域控制器对所有安全策略和帐户信息进行自动更新并保持同步；
- 对每个对象属性的访问控制；
- 域之间的传递委托关系；
- 验证内部和外部用户的多验证机制，包括使用 Windows NT 4.0 版本的用户；
- 管理访问控制和帐户信息的公用管理工具；
- 智能卡支持对用户安全存储的信任验证；
- 对通过网络传输和存储在磁盘上的数据提供加密技术。

旧工作新方法

下面以表格的形式（见表 1.1）将某些工作在 Windows NT 4.0 和 Windows 2000 中不同的操作方法进行了总结。

表 1.1 Windows NT 4.0 和 Windows 2000 Server 对同一工作的不同操作

工作内容	在 Windows NT 4.0	在 Windows 2000 Server
为域工作组或将登录域控制器的用户授权	使用域用户管理器	使用 Active Directory 用户与计算机
编辑域用户的帐户策略	使用域用户管理器	使用 Active Directory 用户与计算机
编辑组或域控制器或指定计算机的用户的审核策略	使用域用户管理器	使用 Active Directory 用户与计算机
建立域委托关系	使用域用户管理器	使用 Active Directory 用户与计算机
将成员服务器提升为域控制器	没有可用的控件	Active Directory 安装向导
指定文件、文件夹和注册表键的访问权限	相应的对象管理器和属性页	相应的对象管理器和属性页
审核安全事件	域用户管理器	相应的对象管理器和属性页
查看安全日志	事件查看器	事件查看器
创建用户和组	域用户管理器	Active Directory 用户与计算机
管理 a Windows NT 4.0 域	域用户管理器	Windows 2000 域用户管理器

1.1.2　安全性基本概念

在您开始为计算机环境安全性制订计划并准备实施之前，首先应该熟悉一些关于 Windows 2000 安全性的基本概念。这些概念包括：

- 安全模型
- 域结构
- 验证机制
- 授权机制
- 审核机制
- 安全策略
- 委托机制
- 数据保护
- 公共密钥结构

安全模型

Windows 2000 安全模型的主要特征是用户验证和访问控制。为了确保能够方便和有效地管理这些特性，Windows 2000 使用了活动目录。下面的内容描述了安全模型的这些特性。

用户验证

Windows 2000 安全模型包括用户验证的概念，使得用户能够登录到一个系统访问网络资源。在验证模型中，安全系统提供两种验证：

- 交互式登录　验证访问本地计算机或活动目录帐户的用户身份。
- 网络验证　对那些试图访问网络服务的用户身份进行验证。为此，Windows 2000 安全系统包括三种不同验证机制：Kerberos V5，公共密钥证书和 NTLM(为了和 Windows 2000 4.0 系统保持兼容)。

基于对象的访问控制

连同用户验证，Windows 2000 允许管理员控制对网上的资源、对象的访问。Windows 2000 通过允许管理员对存储在活动目录上的对象指定安全描述符来实现访问控制。一个安全描述符列出了准许对一个对象访问的用户和组的名字。安全描述符也规定了准许对一个对象访问的事件。对象实例包括文件，打印机和服务。通过管理对象的属性，管理者可以设置权限（permission），分配所有权，并监控用户访问。

管理者不仅能够控制对一个特定对象的访问，也能控制对一个对象某种属性的访问。例如，通过对对象安全描述符的正确配置，用户可获得访问信息的子集，比如雇员的姓名和电话号码，但不包括其家庭地址。

活动目录和安全机制

通过控制对象和用户的访问资格，活动目录为用户帐户和组信息提供一种受保护的

存储。因为活动目录不仅存储了用户的凭据，而且存储了访问控制信息，登录到网络的用户将同时得到访问系统资源的验证和授权。

例如，当用户登录到网络时， Windows 2000 的安全系统将用存储在活动目录中的信息进行验证。然后，当用户试图访问网络上的服务时，安全系统将检查该服务的 ACL 中定义的属性。

因为活动目录允许管理者创建用户组帐户，所以管理者可以更高效的管理系统的安全。例如，通过调整一个文件的属性，管理者可授权一个组中的所有用户读取该文件，这样就使活动目录对象的访问是基于组成员的。

域

在您的安全管理中采用域，将会使工作更加简单。

域是一群网络对象，比如用户，用户组，计算机。一个域中的所有对象都存储在一个活动目录中。活动目录可以位于一个域控制器下或一个域内的多个域控制器下。

每一个域都是一个安全边界，这意味着安全策略和设置(比如管理权，安全策略和访问控制列表)不能够跨域。某一个域的管理者的权利只在本域内有效。

由于域是一个安全边界，故而不同的管理者能够在组织内创建并管理不同的域。域有以下几个特点：

- 安全策略可以在一个域内实现。
- 包含安全信息的活动目录将定期复制到域中的每个域控制器，以便数据库总能保持同步。
- 可以在组织单元级（OU）组织和管理活动目录中的对象。
- 可以在域目录树的域之间建立传递委托关系。

单对多域

Windows NT 4.0 限制一个目录可以存储的用户数。这样，为了适用大型的计算环境，组织必须创建并管理几个域，每一个域拥有额定用户数目的目录。域一般分为两类：主域(存储用户和组帐户)和资源域(存储文件，打印机，应用服务等等)。

这种多域计算环境称为多主域（multi-masterdomain）模型。多主域模型意味着资源域需要和所有主域之间建立多个信任关系，即资源域具有所有主域的多委托关系。这些委托关系允许主域中的用户访问资源域中的资源。

活动目录通过扩大域存储用户、组和计算机帐户的容量，来取代对多个域的需要。管理员通过使用活动目录，将所有的帐户(从前不得不存储于主域)和所有资源(以前不得不存储在资源域)从多个域合并于一个域中。出于管理上的目的，为了保持对象组的逻辑关系，管理者可以将域内的对象分为组织单元(OUs)。然而，某些情况下，出于策略原因，您可能想保持多个域。

传递委托关系

当您将对象从多个域移入单个域时，等于降低了必须建立和保留的域委托关系的数