

DVD  
附赠光盘

大容量语音教学视频  
直观引导配置操作

网管天下

# Windows Server 2008 服务器架设与网络配置

莫有权 李庆荣 郭亮 等编著



- 理论深刻透彻
- 配置直观明了

清华大学出版社



大容量语音教学视频  
直观引导配置操作

网管天下

# Windows Server 2008

## 服务器架设与网络配置

莫有权 李庆荣 郭亮 等编著

● 理论深刻透彻  
● 配置直观明了

清华大学出版社

## 内 容 简 介

本书以 Windows 最新的服务器操作系统 Windows Server 2008 为平台,以网络管理和网络服务为中线,详细介绍网络管理员在日常工作中,对 Windows Server 2008 操作系统的配置和应用等知识,以帮助解决可能面临的各种问题及给出合理的解决方案。本书具体内容包括 Windows Server 2008 规划与安装、Active Directory 目录服务、用户和组账号管理、磁盘系统的管理、配置与管理文件服务器、配置与管理打印服务器、配置与管理 DNS 服务器、配置与管理 DHCP 服务器、远程管理和终端服务、电子证书服务、路由和远程策略等。

本书由浅入深,通俗易懂,注重实践,适用于中小企业网络管理人员和需要为今后的择业储备更多就业技能的读者,也可作为专业网络技术人员参考手册。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

## 图书在版编目(CIP)数据

Windows Server 2008 服务器架设与网络配置/莫有权等编著. —北京:清华大学出版社,2011.2  
ISBN 978-7-302-24374-8

I. ①W… II. ①莫… III. ①操作系统(软件), Windows Server 2008—应用软件—网络服务器 IV. ①TP316.86

中国版本图书馆 CIP 数据核字(2010)第 258207 号

责任编辑:夏兆彦

责任校对:徐俊伟

责任印制:杨 艳

出版发行:清华大学出版社

<http://www.tup.com.cn>

社 总 机:010-62770175

投稿与读者服务:010-62795954,jsjic@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015,zhiliang@tup.tsinghua.edu.cn

地 址:北京清华大学学研大厦 A 座

邮 编:100084

邮 购:010-62786544

印 刷 者:北京鑫丰华彩印有限公司

装 订 者:三河市金元印装有限公司

经 销:全国新华书店

开 本:190×260 印 张:28 字 数:696 千字

附光盘 1 张

版 次:2011 年 2 月第 1 版

印 次:2011 年 2 月第 1 次印刷

印 数:1~4000

定 价:59.00 元



# FOREWORD

## 前言

本书以 Windows 最新的服务器操作系统 Windows Server 2008 为平台,以网络管理和网络服务为中线,详细介绍网络管理员在日常工作中,对 Windows Server 2008 操作系统的配置和应用等知识,以帮助解决可能面临的各种问题及给出合理的解决方案。

本书具体内容包括 Windows Server 2008 规划与安装、Active Directory 目录服务、用户和组账号管理、磁盘系统的管理、配置与管理文件服务器、配置与管理打印服务器、配置与管理 DNS 服务器、配置与管理 DHCP 服务器、远程管理和终端服务、电子证书服务、路由和远程策略等。

### 1. 本书内容

通过本书的学习,不仅可以学到网络操作系统的基本操作,还可以了解一些常用服务器的配置及应用的相关知识。

本书共分 4 篇 11 章,每一篇都介绍不同操作系统应用的相关内容。

第一篇为服务器基本操作篇(包含第 1~3 章),介绍 Windows Server 2008 服务器的一些管理性内容。

第 1 章为 Windows Server 2008 规划与安装,详细介绍 Windows Server 2008 的安装、账户及权限管理、活动目录应用等。

第 2 章为 Active Directory 目录服务,详细介绍规则 Active Directory 实施、实现 Active Directory、创建组织单位及其对象、控制对 Active Directory 对象的访问等。

第 3 章为用户和组账号管理,详细介绍规划新用户账号、创建用户账号、管理用户账号、组账号管理、组策略管理等。

第二篇为文件及打印服务篇(包含第 4~6 章),介绍服务器操作系统中的磁盘管理、文件服务器配置及管理、打印服务器的配置与管理等。

第 4 章为磁盘系统管理,详细介绍磁盘概述、基本卷的管理、动态磁盘的管理、镜像卷与 RAID-5 卷的修复等。

第 5 章为配置与管理文件服务器,详细介绍文件服务与资源共享、资源访问权限的控制、加密文件系统(EFS)与压缩、数据的备份和还原、分布式文件系统等。

第 6 章为配置与管理打印服务器,详细介绍打印概述、安装打印服务器、打印服务器的管理等。

第三篇为网络管理篇(包含第 7、8 章),介绍 DNS 服务器和 DHCP 服务器的配置及应用。

第 7 章为配置与管理 DNS 服务器,详细介绍 DNS 的基本概念与原理、安装和添加 DNS 服务器、创建和管理 DNS 区域等。

第8章为配置与管理 DHCP 服务器,详细介绍 DHCP 服务及其工作原理、DHCP 服务的安装和配置、配置 DHCP 客户端、复杂网络的 DHCP 服务器的部署等。

第四篇为远程管理篇(包含第9~11章),介绍远程登录、远程桌面、电子证书服务、路由和远程访问等。

第9章为远程管理和终端服务,详细介绍配置和使用远程桌面、配置远程协助、Telnet 服务等。

第10章为电子证书服务,详细介绍数字证书、CA 的层次结构、企业 CA 的安装与证书申请、签名与加密的电子邮件、企业从属 CA 的安装等。

第11章为路由和远程访问,详细介绍软路由、远程访问、远程访问安全机制、虚拟专用网络、验证通信协议、远程访问策略等。

## 2. 本书特色

- 面向职业角度和网管考试安排图书内容,增强了本书的实用性。内容全面,结构完善,形成系统而完备的网管知识体系。
- 通过相关企业征集 30 多个有代表性的工作中经常应用的实例,穿插于书中。将理论知识落实到日常的网络应用实践中,提高读者网络管理的实际应用能力。
- 由具有专业的企业服务器安全管理和网络维护丰富经验的人员编写,并对企业环境中面临的安全问题以及解决措施有独特的见解,能用通俗易懂的语言,深入浅出地表达出来。
- 增加“网管心得”,介绍网管的实际工作环境和职业要求,便于没有工作经验的网络管理员与相关职业接轨,掌握工作中必备技能或者相关知识。

## 3. 读者定位

本书由浅入深,通俗易懂,注重实践,适用于中小企业网络管理人员和需要为今后的择业储备更多就业技能的读者,也可作为专业网络技术人员的手册。

参与本书编写的除了封面署名人员外,还有胡家宏、王海峰、王健、张勇、冯冠、刘好增、赵俊昌、祁凯、孙江玮、田成军、刘俊杰、王泽波、张银鹤、阎迎利、何方、李海庆、王树兴、朱俊成、康显丽、崔群法、孙岩、秦长海、宋素萍、倪宝童、王立新、温玲娟、于会芳、赵喜来、杨宁宁、郭晓俊、方宁、牛丽萍、郭新志、王黎、安征、亢凤林、李海峰等。由于时间仓促,加之编者水平有限,书中疏漏之处在所难免,欢迎读者朋友登录清华大学出版社的网站 [www.tup.com.cn](http://www.tup.com.cn) 与我们联系,帮助我们改进提高。

编者

2010 年 7 月

# CONTENTS

## 目 录

### 第一篇 服务器基本操作篇

|                                                   |    |
|---------------------------------------------------|----|
| 第 1 章 Windows Server 2008 规划与安装 .....             | 2  |
| 1.1 Windows Server 2008 简介 .....                  | 2  |
| 1.1.1 Windows Server 2008 功能及特点 .....             | 3  |
| 1.1.2 Windows Server 2008 的新增功能 .....             | 5  |
| 1.1.3 Windows Server 2008 版本之间的区别 .....           | 9  |
| 1.1.4 网管心得——Windows Server 2008 和 Linux 的区别 ..... | 12 |
| 1.1.5 网管心得——IP 地址和子网掩码 .....                      | 13 |
| 1.2 设置网络地址 .....                                  | 18 |
| 1.2.1 设置计算机名称 .....                               | 18 |
| 1.2.2 设置 IP 地址 .....                              | 19 |
| 1.2.3 检查网络连接是否正确 .....                            | 22 |
| 1.3 使用 Microsoft 管理控制台 .....                      | 24 |
| 1.3.1 MMC 概述 .....                                | 24 |
| 1.3.2 打开 MMC .....                                | 24 |
| 1.3.3 管理单元 .....                                  | 25 |
| 1.3.4 为 MMC 控制台添加管理单元 .....                       | 26 |
| 1.3.5 MMC 模式 .....                                | 26 |
| 1.3.6 MMC 附加功能 .....                              | 28 |
| 1.4 局域网中的专有名词 .....                               | 29 |
| 1.4.1 Windows Server 2008 工作组 .....               | 29 |
| 1.4.2 Windows Server 2008 域 .....                 | 30 |
| 1.4.3 域中的计算机 .....                                | 32 |
| 1.4.4 域树 .....                                    | 33 |
| 1.4.5 森林 .....                                    | 34 |
| 1.5 操作实例 .....                                    | 35 |
| 1.5.1 操作实例——安装 Windows Server 2008 系统 .....       | 35 |
| 1.5.2 操作实例——配置基本外部设备 .....                        | 38 |
| 1.5.3 操作实例——使用 Sysprep 工具审核安装内容 .....             | 43 |
| 第 2 章 Active Directory 目录服务 .....                 | 46 |
| 2.1 Active Directory 概述 .....                     | 46 |
| 2.1.1 名称空间 .....                                  | 46 |
| 2.1.2 对象与属性 .....                                 | 47 |
| 2.1.3 容器与组织单位 .....                               | 48 |
| 2.1.4 信任 .....                                    | 49 |

|                       |                            |     |                      |                              |     |
|-----------------------|----------------------------|-----|----------------------|------------------------------|-----|
| 2.1.5                 | 架构                         | 50  | 3.2.1                | 更改密码                         | 108 |
| 2.1.6                 | 域控制器                       | 52  | 3.2.2                | 备份与还原密码                      | 109 |
| 2.1.7                 | 轻型目录访问协议                   | 53  | 3.3                  | 组账号管理                        | 110 |
| 2.1.8                 | 站点                         | 55  | 3.3.1                | 组介绍                          | 110 |
| 2.1.9                 | 网管心得——活动目录的逻辑和物理结构         | 56  | 3.3.2                | 规则分组策略                       | 112 |
| 2.1.10                | 网管心得——使用活动目录的意义            | 57  | 3.3.3                | 实现组                          | 113 |
| 2.2                   | 活动目录域服务的安装与配置              | 59  | 3.3.4                | 实现本地组                        | 115 |
| 2.2.1                 | 安装 Active Directory 域服务    | 59  | 3.3.5                | 网管心得——计算机账户                  | 116 |
| 2.2.2                 | 安装活动目录                     | 64  | 3.4                  | 组策略及应用                       | 117 |
| 2.3                   | 管理 Active Directory 中的域组账户 | 68  | 3.4.1                | 组策略概述                        | 118 |
| 2.3.1                 | 创建与管理域组                    | 68  | 3.4.2                | 组策略的配置                       | 119 |
| 2.3.2                 | Active Directory 域内置的组     | 71  | 3.4.3                | 脚本策略                         | 121 |
| 2.3.3                 | 删除域控制器与域                   | 75  | 3.4.4                | 软件安装                         | 122 |
| 2.4                   | 提升域与林功能级别                  | 77  | 3.4.5                | 软件限制                         | 124 |
| 2.4.1                 | 提升域功能级别                    | 77  | 3.4.6                | 文件夹重定向                       | 126 |
| 2.4.2                 | 提升林功能级别                    | 79  | 3.4.7                | 硬件访问控制                       | 129 |
| 2.5                   | 将计算机加入或脱离域                 | 80  | 3.4.8                | 网管心得——委派的作用                  | 130 |
| 2.5.1                 | 将 Windows 计算机加入域           | 80  | 3.5                  | 操作实例                         | 131 |
| 2.5.2                 | 利用已加入域的计算机登录               | 82  | 3.5.1                | 操作实例——创建密码重设盘                | 131 |
| 2.5.3                 | 脱离域                        | 83  | 3.5.2                | 操作实例——如何把 Users 组的账号提升为管理员权限 | 133 |
| 2.6                   | 操作实例                       | 83  |                      |                              |     |
| 2.6.1                 | 操作实例——DNS 在活动目录中的应用        | 83  |                      |                              |     |
| 2.6.2                 | 操作实例——站点在活动目录中的应用          | 87  |                      |                              |     |
| 2.6.3                 | 操作实例——LDAP 在活动目录中的应用       | 89  |                      |                              |     |
| <b>第 3 章 用户和组账号管理</b> |                            |     | <b>第二篇 文件及打印服务篇</b>  |                              |     |
| 3.1                   | 用户账号管理                     | 91  | <b>第 4 章 磁盘系统的管理</b> |                              |     |
| 3.1.1                 | 用户账号简介                     | 91  | 4.1                  | 磁盘概念                         | 138 |
| 3.1.2                 | 规划新用户账号                    | 93  | 4.1.1                | MBR 磁盘与 GPT 磁盘               | 138 |
| 3.1.3                 | 创建用户账号                     | 95  | 4.1.2                | 基本磁盘与动态磁盘                    | 140 |
| 3.1.4                 | 管理用户账号                     | 98  | 4.2                  | 磁盘管理概述                       | 142 |
| 3.1.5                 | 用户配置文件                     | 101 | 4.2.1                | 远程管理                         | 142 |
| 3.1.6                 | 创建主文件夹                     | 105 | 4.2.2                | 命令行                          | 144 |
| 3.2                   | 密码的更改、备份与还原                | 108 | 4.2.3                | 网管心得——中小企业服务器磁盘存储管理维护要点      | 147 |
|                       |                            |     | 4.3                  | 分区和卷                         | 149 |
|                       |                            |     | 4.3.1                | 创建卷或分区                       | 149 |
|                       |                            |     | 4.3.2                | 创建扩展分区和逻辑驱动器                 | 152 |
|                       |                            |     | 4.3.3                | 将磁盘转换为动态磁盘                   | 153 |
|                       |                            |     | 4.3.4                | 将磁盘转换为 GPT 磁盘                | 154 |
|                       |                            |     | 4.3.5                | 更改卷的容量                       | 155 |
|                       |                            |     | 4.3.6                | 向卷添加镜像                       | 157 |

|                                                         |     |
|---------------------------------------------------------|-----|
| 4.4 设置磁盘配额                                              | 158 |
| 4.4.1 启用磁盘配额                                            | 158 |
| 4.4.2 设置每用户配额                                           | 159 |
| 4.4.3 导入和导出配额                                           | 161 |
| 4.4.4 网管心得——磁盘配额的含义                                     | 163 |
| 4.5 启用文件加密                                              | 163 |
| 4.6 镜像卷与 RAID-5 卷的修复                                    | 166 |
| 4.6.1 镜像卷的修复                                            | 166 |
| 4.6.2 RAID-5 卷的修复                                       | 168 |
| 4.6.3 网络工具列表                                            | 170 |
| 4.7 操作实例                                                | 174 |
| 4.7.1 操作实例——磁盘碎片整理与<br>磁盘错误检查                           | 174 |
| 4.7.2 操作实例——使用工具对磁盘分区<br>(Acronis Disk Director Server) | 177 |

## 第 5 章 配置与管理文件服务器 179

|                             |     |
|-----------------------------|-----|
| 5.1 文件服务与资源共享               | 179 |
| 5.1.1 安装文件服务器               | 179 |
| 5.1.2 设置资源共享                | 182 |
| 5.1.3 管理共享文件夹               | 184 |
| 5.1.4 访问网络共享资源              | 187 |
| 5.1.5 卷影副本                  | 188 |
| 5.2 资源访问权限的控制               | 190 |
| 5.2.1 NTFS 权限概述             | 191 |
| 5.2.2 设置文件或文件夹的<br>NTFS 权限  | 194 |
| 5.2.3 复制、移动文件和文件夹对<br>权限的影响 | 197 |
| 5.2.4 在 NTFS 上压缩文件和文件夹      | 198 |
| 5.2.5 共享权限                  | 200 |
| 5.3 加密文件系统                  | 202 |
| 5.3.1 加密文件系统概述              | 202 |
| 5.3.2 加密文件或文件夹              | 203 |
| 5.3.3 备份密钥                  | 204 |
| 5.4 数据的备份和还原                | 205 |
| 5.4.1 数据的备份                 | 206 |
| 5.4.2 数据的还原                 | 210 |

|                                         |     |
|-----------------------------------------|-----|
| 5.4.3 网管心得——非常时期容灾<br>备份策略解析            | 212 |
| 5.4.4 网管心得——中小企业的远程<br>备份问题             | 213 |
| 5.5 分布式文件系统                             | 215 |
| 5.5.1 分布式文件系统的概述                        | 215 |
| 5.5.2 配置 DFS 命名空间                       | 217 |
| 5.5.3 在 DFS 命名空间中创建文件                   | 221 |
| 5.6 操作实例                                | 222 |
| 5.6.1 操作实例——安装 Windows<br>Server Backup | 222 |

## 第 6 章 配置与管理打印服务器 224

|                            |     |
|----------------------------|-----|
| 6.1 打印概述                   | 224 |
| 6.1.1 基本概念                 | 224 |
| 6.1.2 共享打印机的连接             | 225 |
| 6.1.3 网管心得——本地与远程<br>打印的理解 | 228 |
| 6.2 安装打印服务器                | 229 |
| 6.2.1 安装本地打印机              | 229 |
| 6.2.2 安装远程打印机              | 231 |
| 6.2.3 安装 Internet 打印机      | 232 |
| 6.2.4 网络接口打印机的安装           | 233 |
| 6.2.5 网管心得——网络打印的要求        | 235 |
| 6.3 共享打印机的高级设置             | 236 |
| 6.3.1 设置打印优先级              | 236 |
| 6.3.2 设置打印机的打印时间           | 237 |
| 6.3.3 设置打印机池               | 239 |
| 6.3.4 打印机的其他设置             | 239 |
| 6.4 设置打印机权限                | 240 |
| 6.4.1 打印机权限分配              | 241 |
| 6.4.2 打印机的所有权              | 242 |
| 6.5 使用分隔页分隔打印文件            | 243 |
| 6.5.1 创建分隔页文件              | 243 |
| 6.5.2 选择分隔页文件              | 245 |
| 6.6 打印机其他设置                | 246 |
| 6.6.1 管理打印队列               | 246 |
| 6.6.2 送纸器设置                | 248 |
| 6.6.3 网管心得——打印与活动目录        | 249 |

|                              |     |
|------------------------------|-----|
| 6.7 操作实例                     | 249 |
| 6.7.1 操作实例——搭建小型公司<br>网络打印服务 | 249 |
| 6.7.2 操作实例——安装打印机<br>客户端     | 252 |

### 第三篇 网络管理篇

|                                   |     |
|-----------------------------------|-----|
| 第7章 配置与管理 DNS 服务器                 | 256 |
| 7.1 DNS 的基本概念与原理                  | 256 |
| 7.1.1 DNS 概述                      | 256 |
| 7.1.2 域名空间结构                      | 258 |
| 7.1.3 区域                          | 260 |
| 7.1.4 DNS 查询模式                    | 261 |
| 7.1.5 DNS 规划与域名申请                 | 262 |
| 7.1.6 网管心得——主要省份城市的<br>DNS 服务器地址  | 264 |
| 7.2 安装和配置 DNS 客户端                 | 266 |
| 7.2.1 安装 DNS 服务                   | 266 |
| 7.2.2 指定 DNS 服务器                  | 267 |
| 7.3 创建和管理 DNS 区域                  | 268 |
| 7.3.1 新建 DNS 区域                   | 269 |
| 7.3.2 内建 DNS 资源记录                 | 272 |
| 7.3.3 创建 DNS 资源记录                 | 273 |
| 7.3.4 添加 DNS 的子域                  | 276 |
| 7.3.5 创建辅助区域                      | 277 |
| 7.3.6 创建反向搜索区域                    | 279 |
| 7.4 操作实例                          | 280 |
| 7.4.1 操作实例——配置 DNS 服务器            | 280 |
| 7.4.2 操作实例——创建区域委派                | 284 |
| 7.4.3 操作实例——启用 DNS 来使用<br>WINS 解析 | 285 |

|                    |     |
|--------------------|-----|
| 第8章 配置与管理 DHCP 服务器 | 289 |
| 8.1 DHCP 服务及其协议原理  | 289 |
| 8.1.1 DHCP 协议原理    | 289 |
| 8.1.2 何时使用 DHCP 服务 | 292 |
| 8.2 DHCP 服务器的安装和配置 | 293 |
| 8.2.1 安装 DHCP 服务器  | 293 |
| 8.2.2 授权 DHCP 服务器  | 296 |

|                       |     |
|-----------------------|-----|
| 8.2.3 创建 DHCP 作用域     | 298 |
| 8.2.4 保留特定的 IP 地址     | 300 |
| 8.2.5 DHCP 配置选项       | 301 |
| 8.2.6 超级作用域           | 303 |
| 8.3 配置 DHCP 客户端       | 305 |
| 8.4 复杂网络的 DHCP 服务器的部署 | 306 |
| 8.4.1 安装多个 DHCP 服务器   | 306 |
| 8.4.2 多宿主 DHCP 服务器    | 307 |
| 8.4.3 跨网段的 DHCP 中继    | 308 |
| 8.5 操作实例              | 310 |
| 8.5.1 操作实例——数据库的备份    | 310 |
| 8.5.2 操作实例——数据库的还原    | 311 |
| 8.5.3 操作实例——数据库的重整    | 312 |

### 第四篇 远程管理篇

|                                   |     |
|-----------------------------------|-----|
| 第9章 远程管理和终端服务                     | 316 |
| 9.1 远程桌面管理                        | 316 |
| 9.1.1 远程桌面管理概述                    | 316 |
| 9.1.2 启用远程桌面                      | 317 |
| 9.1.3 配置远程桌面连接                    | 318 |
| 9.2 配置终端服务                        | 320 |
| 9.2.1 终端服务器概述                     | 320 |
| 9.2.2 安装终端服务器                     | 322 |
| 9.2.3 授权终端服务器                     | 325 |
| 9.2.4 配置终端服务器                     | 328 |
| 9.2.5 管理终端服务器                     | 332 |
| 9.3 远程协助                          | 334 |
| 9.3.1 远程协助概述                      | 335 |
| 9.3.2 配置远程协助                      | 336 |
| 9.3.3 网络工具列表                      | 337 |
| 9.4 Telnet 服务                     | 341 |
| 9.4.1 Telnet 服务器概述                | 341 |
| 9.4.2 配置 Telnet 服务并进行<br>远程登录     | 342 |
| 9.5 操作实例                          | 345 |
| 9.5.1 操作实例——为终端服务器指定<br>用户登录自启动程序 | 345 |
| 9.5.2 操作实例——更改远程桌面<br>使用的默认端口     | 347 |

|                                         |            |                                                            |            |
|-----------------------------------------|------------|------------------------------------------------------------|------------|
| 9.5.3 操作实例——配置及访问<br>RemoteApp 程序 ..... | 352        | 10.5.2 操作实例——Web 服务器 SSL<br>双向认证 .....                     | 393        |
| <b>第 10 章 电子证书服务 .....</b>              | <b>356</b> | <b>第 11 章 路由和远程策略 .....</b>                                | <b>397</b> |
| 10.1 数字证书简介 .....                       | 356        | 11.1 软路由 .....                                             | 397        |
| 10.1.1 数字证书 .....                       | 356        | 11.1.1 路由概述 .....                                          | 397        |
| 10.1.2 PKI .....                        | 358        | 11.1.2 Windows Server 2008 路由器的<br>设置 .....                | 399        |
| 10.1.3 网管心得——PKI 的组成部分 .....            | 360        | 11.1.3 网管心得——路由与远程访问<br>服务特性 .....                         | 400        |
| 10.2 证书认证机构 .....                       | 361        | 11.2 远程访问服务器配置与管理 .....                                    | 402        |
| 10.3 企业 CA 的安装与证书申请 .....               | 362        | 11.2.1 VPN 概述 .....                                        | 402        |
| 10.3.1 企业证书的意义与适用 .....                 | 362        | 11.2.2 远程访问服务器的配置 .....                                    | 404        |
| 10.3.2 CA 模式 .....                      | 363        | 11.2.3 远程访问服务客户端的设置 .....                                  | 409        |
| 10.3.3 安装证书服务并架设<br>企业根 CA .....        | 364        | 11.3 利用 NPS 策略实现安全访问 .....                                 | 411        |
| 10.3.4 申请和使用证书 .....                    | 370        | 11.3.1 NAP 概述 .....                                        | 411        |
| 10.3.5 签名与加密的电子邮件 .....                 | 375        | 11.3.2 配置 VPN 服务器 .....                                    | 414        |
| 10.3.6 企业从属 CA 的安装 .....                | 378        | 11.3.3 配置 NPS 服务器 .....                                    | 417        |
| 10.3.7 网管心得——Web 和证书服务 .....            | 379        | 11.3.4 利用组策略配置 VPN 客户端 .....                               | 423        |
| 10.4 数字证书的管理 .....                      | 381        | 11.3.5 配置 VPN 客户端 .....                                    | 426        |
| 10.4.1 CA 的备份与还原 .....                  | 381        | 11.3.6 网管心得——VPN 隧道技术 .....                                | 429        |
| 10.4.2 自动或手动发放证书 .....                  | 383        | 11.4 操作实例 .....                                            | 432        |
| 10.4.3 吊销证书和证书吊销列表 .....                | 384        | 11.4.1 操作实例——在运行 Windows XP<br>的计算机中设置及<br>使用 VPN 连接 ..... | 432        |
| 10.4.4 导入与导出用户的证书 .....                 | 388        | 11.4.2 操作实例——创建拨号连接 .....                                  | 434        |
| 10.4.5 更新证书 .....                       | 389        |                                                            |            |
| 10.5 操作实例 .....                         | 391        |                                                            |            |
| 10.5.1 操作实例——创建服务器验证<br>字请求 .....       | 391        |                                                            |            |

# **第一篇 服务器基本操作篇**

# 第1章

## Windows Server 2008 规划与安装

Windows Server 2008 不仅是微软最新的服务器操作系统,更代表了下一代 Windows Server 的发展趋势,它不仅改善了用户操作界面,还继承了 Windows Server 2003 操作系统的各种优点,并在此基础上提供了重要的新功能和对原有功能的强大改进,促进应用程序、网络和 Web 服务从工作组向数据中心的转变。

Windows Server 2008 通过加强操作系统和保护网络环境提高了安全性,通过加快 IT 系统的部署与维护,使服务器和应用程序的合并与虚拟化更加简单,通过提供直观管理工具,使得网络管理人员的管理更加灵活。

Windows Server 2008 为网络服务器和网络基础结构奠定了很好的基础。而使用 Windows Server 2008,使得专业人员对其服务器和网络基础结构的控制能力更强。本章将从 Windows Server 2008 的新特性,与另一流行服务器 Linux 的区别及 Windows Server 2008 中的基本概念,如工作组、域、MMC 等方面进行学习。

### 本章学习要点:

- Windows Server 2008 新特性
- Windows Server 2008 和 Linux 的区别
- IP 地址和子网掩码
- 设置网络地址
- 使用 Microsoft 管理控制台
- 了解 MMC 的功能
- Windows Server 2008 工作组和域
- 域中的计算机
- 域树和域林

## 1.1 Windows Server 2008 简介

Windows Server 2008 继承了 Windows Server 2003 服务器操作系统的诸多优点,同时还引进了多项新技术,如虚拟化应用、网络负载均衡、网络安全服务等。

Windows Server 2008 服务器操作系统与 Windows Server 2003 服务器操作系统相同,也开发了适应不同环境的多个版本。并且,各版本之间有各自的优势,为了更好地学习该操作系统,首先介绍该操作系统的特点及各版本之间的区别。

### 1.1.1 Windows Server 2008 功能及特点

Windows Server 2008 是一套和 Windows Vista (代号为 Longhorn) 相对应的服务器操作系统, 两者具有很多的相同功能。作为 Windows 2000 (Advanced) Server 和 Windows Server 2003 的升级版本, Windows Server 2008 融入了很多 Windows Vista 操作系统优美界面及操作方便的特性, 同时也是 Microsoft 公司发布的最后一个 32 位版本的服务器操作系统。

#### 1. 运行 Windows Server 2008 的配置要求

在安装 Windows Server 2008 之前, 首先需要知道计算机能否顺利运行 Windows Server 2008, 除非使用 Windows 部署服务或者不从 CD-ROM 进入 Windows 预安装环境, 否则需要使用 DVD-ROM 驱动器。

Windows Server 2008 除了具有光学介质和支持基本的 VGA 图形能力外, 其他最低配置要求如表 1-1 所示。

表 1-1 Windows Server 2008 配置要求

| 硬件设备     | 操作系统要求                                                                                                                                                       |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU      | 最小速度 1 千兆赫 (GHz) 32 位 (X86) 处理器或 1 千兆赫 (GHz) 64 位 (X64) 处理器, 建议速度为 2 千兆赫 (GHz) 32 位 (X86) 或 64 位 (X64) 处理器, 最佳速度为 3 千兆赫 (GHz) 32 位 (X86) 或 64 位 (X64) 处理器或更快 |
| 内存       | 最小 512MB 内存, 建议为 1GB 内存, 最佳为 2GB 内存 (完全安装) 或 1GB 内存 (服务器核心安装) 或更大                                                                                            |
| 显存       | 128MB 显存 (最低)                                                                                                                                                |
| 可用磁盘空间   | 最小空间 8GB, 建议为 40GB (完全安装) 或 10GB (服务器核心安装), 最佳空间为 80GB (完全安装) 或 40GB (服务器核心安装) 或者更大空间                                                                        |
| 驱动器      | DVD-ROM 驱动器                                                                                                                                                  |
| 显示器和外围设备 | 超级 VGA (800×600) 或更高分辨率显示器; 键盘; Microsoft 鼠标或兼容的指针设备                                                                                                         |



Windows Server 2008 与 Windows Vista 一样, 是从 DVD (而不是 CD-ROM) 驱动器安装的。

#### 2. Windows Server 2008 版本

目前, Windows Server 2008 包括多种不同的版本, 以支持不同单位 (公司) 网络的各种服务器和工作负载需求。

##### ❑ Windows Server 2008 Standard Edition (标准版)

该操作系统包括 32 位和 64 位两种类型, 其中, 32 位 (X86) 版本最多支持 4GB 内存, 在 SMP 配置下最多支持 4 个处理器; 64 位 (X64) 版本最多支持 32GB 内存, 在 SMP 配置下最多支持 4 个处理器。该版本主要面向中小型企业用户。



SMP (Symmetric Multi Processing) 即对称多处理器, 是一项使软件在一台服务器上使用多处理器以提高系统性能的技术。

### ❑ Windows Server 2008 Enterprise (企业版)

该操作系统包括 32 位和 64 位两种类型, 其中, 32 位 (X86) 版本在 SMP 配置下最多支持 64GB 内存和 8 个处理器; 64 位 (X64) 版本在 SMP 配置下最多支持 2TB 内存和 8 个处理器。该版本主要针对大型企业的操作系统, 特别是在运行 SQL Server 2008 Enterprise Edition 和 Exchange Server 2007 应用程序的服务器上。



计算机中的位数是指 CPU 一次能处理的最大位数。32 位是指 CPU 一次最多能处理 32 位的数据; 64 位即 CPU 一次最多能处理 64 位的数据。位数越大代表处理器处理信息的能力越大。

### ❑ Windows Server 2008 Datacenter (数据中心版)

该操作系统包括 32 位和 64 位两种类型, 其中 32 位 (X86) 版本在 SMP 配置下最多支持 64GB RAM 和 32 个处理器; 64 位 (X64) 版本在 SMP 配置下最多支持 2TB RAM 和 64 个处理器。该版本直接针对大规模的企业应用。

### ❑ Windows Web Server 2008

Windows Web Server 2008 同样包括 32 位和 64 位两种类型, 其中 32 位 (X86) 版本在 SMP 配置下最多支持 4GB RAM 和 4 个处理器; 64 位 (X64) 版本在 SMP 配置下最多支持 32GB RAM 和 4 个处理器, 该版本是专门为 Web 应用程序服务器而设计的, 其他角色, 如 Windows 部署服务器和 Active Directory 域服务等, 在 Windows Web Server 2008 上不受支持。

### ❑ Windows Server 2008 for Itanium-Based Systems

与前几种版本不同, Windows Server 2008 for Itanium-Based Systems 是专为 Inter Itanium 64 位处理器架构设计的, 该架构不同于 Intel Core 2 Duo 或 AMD Turion 系列处理器芯片中存在的 X64 架构。这是 Windows Server 2008 可以安装到 1 台基于 Itanium 的计算机上的唯一版本, 并且需要一个 Itanium 2 处理器。该版本在 SMP 配置下最多支持 64 个处理器和 2TB RAM。

## 3. Windows Server 2008 功能

Windows Server 2008 主要用于虚拟化工作负载、支持应用程序和保护网络方面向组织提供最高效的平台。另外, 它也为开发和可靠地承载 Web 应用程序和服务提供了一个安全、易于管理的平台。

### ❑ 更强的控制能力

使用 Windows Server 2008, IT 专业人员能够更好地控制服务器和网络基础结构, 从而可以将精力集中在处理关键业务需求上。例如, 增强的脚本编写功能和任务自动化功能 (Windows PowerShell 等) 可帮助 IT 专业人员自动执行常见 IT 任务; 通过服务器管理器进行的基于角色的安装和管理简化了在企业中管理与保护多个服务器角色的任务; 增强的系统管理工具 (性能和可靠性监视器) 提供有关系统的信息, 能够在潜在问题发生之前向 IT 人员发出警告等。

### □ 增强的保护

Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业的运营和发展奠定了坚实的基础。Windows Server 2008 提供了减小内核攻击面的安全创新（如 Patch Guard），因而使服务器环境更安全、更稳定。

另外，通过保护关键服务器服务使之免受文件系统、注册表或网络中异常活动的影响，Windows 服务强化有助于提高系统的安全性。借助网络访问保护（NAP）、只读域控制器（RODC）、公钥基础结构（PKI）增强功能、Windows 服务强化、新的双向 Windows 防火墙和新一代加密支持，Windows Server 2008 操作系统中的安全性得到了增强。

### □ 更大的灵活性

Windows Server 2008 的设计允许管理员通过修改其基础结构来适应不断变化的业务需求，同时保持了此操作的灵活性。它允许用户从远程位置（如远程应用程序和终端服务网关）执行程序，这一技术为移动工作人员增强了灵活性。例如，在 Windows Server 2008 中使用 Windows 部署服务（WDS）加速对系统的部署和维护。

## 1.1.2 Windows Server 2008 的新增功能

Windows Server 2008 是新一代的 Windows Server 系列操作系统，不仅改善了用户操作界面，而且在此基础上提供了重要的新功能和原有功能的强大改进，与 Microsoft 公司之前发布的 Windows Server 系列操作系统相比，Windows Server 2008 的新特性包括以下几个方面。

### 1. 服务器核心（Server Core）

服务器核心是 Windows Server 2008 新增的功能，它能够提供最简化的模块化安装，是 Windows Server 2008 中最小的安装选择部分，仅包括一个可执行文件和服务器任务。

Server Core 不提供完整的桌面，而是通过命令行来管理 Windows Server 2008，如图 1-1 所示。

| 映像名称                 | PID  | 会话名      | 会话# | 内存使用     |
|----------------------|------|----------|-----|----------|
| System Idle Process  | 0    | Services | 0   | 24 K     |
| System               | 4    | Services | 0   | 2,192 K  |
| smss.exe             | 328  | Services | 0   | 668 K    |
| csrss.exe            | 392  | Services | 0   | 4,640 K  |
| csrss.exe            | 432  | Console  | 1   | 8,688 K  |
| wininit.exe          | 440  | Services | 0   | 3,792 K  |
| winlogon.exe         | 468  | Console  | 1   | 4,644 K  |
| services.exe         | 516  | Services | 0   | 4,732 K  |
| lsass.exe            | 528  | Services | 0   | 8,268 K  |
| lsn.exe              | 536  | Services | 0   | 3,636 K  |
| svchost.exe          | 692  | Services | 0   | 4,616 K  |
| svchost.exe          | 752  | Services | 0   | 5,220 K  |
| \$Lsvc.exe           | 852  | Services | 0   | 9,868 K  |
| svchost.exe          | 908  | Services | 0   | 6,960 K  |
| svchost.exe          | 932  | Services | 0   | 5,604 K  |
| svchost.exe          | 948  | Services | 0   | 26,920 K |
| TrustedInstaller.exe | 964  | Services | 0   | 5,704 K  |
| svchost.exe          | 1008 | Services | 0   | 6,752 K  |
| svchost.exe          | 1072 | Services | 0   | 13,584 K |
| svchost.exe          | 1180 | Services | 0   | 8,456 K  |
| svchost.exe          | 1292 | Services | 0   | 4,868 K  |

图 1-1 Server Core 桌面

由于网络服务器都有可能在网络中执行特定的应用或者担任某些关键的角色任务。全新的 Server Core 安装选项可为运行这些特定应用的服务器或服务器角色提供最简化的环境，从而有助于提高其可靠性与效率，使单位（公司）能更好地利用现有硬件。总的来讲使用 Windows Server 2008 的 Server Core 具有以下两点好处。

#### ❑ 硬件需求更低

在 Windows Server 2008 的 Server Core 版本中除去了许多功能，因此能够在一台运行完全安装版，如 Windows Server 2008 Enterprise 时，出现性能瓶颈问题的计算机上运行 Server Core 版本。另外，也能够使单位（公司）达到利用低配置硬件计算机来安装 Windows Server 2008 的目的。例如，利用原来运行 Windows Server 2000 的低配置硬件计算机来安装 Windows Server 2008。

#### ❑ 攻击面减少

由于 Server Core 能够加载运行核心基础架构角色服务器所需的最少的操作系统组件，即安装的组件更少，因而可以有效减少系统对补丁的需求，也使企图通过补丁危害计算机安全的数量减少，从而提高了核心网络基础架构服务器的可靠性与安全性。

## 2. Internet 信息服务 7.0 (IIS 7.0)

在 Windows Server 2008 中，用户可以有选择性地安装 IIS 7.0，其管理界面也被重新设计，以更方便用户对各种 Web 服务组件的添加、禁止、授权等操作，图 1-2 所示为 IIS7.0 管理界面。



图 1-2 IIS 7.0 管理界面

与早期的 IIS 版本相比，如 IIS 6.0，IIS 7.0 在以下方面进行了改进。

- ❑ 统一的 Web 平台，为管理员和开发人员提供了一个一致的 Web 解决方案。
- ❑ 增强了安全性和自定义服务器，以减少攻击面。
- ❑ 简化了诊断和故障排除功能。

- ❑ 与 Active Directory 相似, 在 IIS 7.0 中, 应用程序和站点的委派管理功能使管理员能够将 Web 服务器不同部分的控制权委派给其他用户, 如网站所有者。
- ❑ IIS 7.0 提供了基于任务的全新 UI (用户界面), 并新增了功能强大的命令行工具。
- ❑ IIS 7.0 引入了新的配置存储, 该存储集成了针对整个 Web 平台的 IIS 和 ASP.NET 的配置。
- ❑ 在 IIS 7.0 中, Web 服务器由多个模块组成, 用户可以根据需要在服务器中添加或删除这些模块。
- ❑ IIS 7.0 Web 服务器可以保证最大程度地实现与现有应用程序的兼容性。

### 3. Hyper-V

Hyper-V 之前称为 Viridian, 是微软最新推出的服务器虚拟化技术, 也是微软第一个采用类似 VMware 和 Citrix 开源 Xen 一样的基于 Hypervisor 的技术。

Hyper-V 提供 Windows Server 2008 中的软件基础结构和基本的管理工具, 可用于创建和管理虚拟化服务器计算环境。此虚拟化环境可用来实现旨在提高效率和降低成本的各种商业目标。例如, 虚拟化服务器环境可以帮助用户解决以下问题。

- ❑ 通过增加硬件的利用率, 降低运行和维护物理服务器的成本。同时, 它还可以减少运行服务器负载所需的硬件数量。
- ❑ 通过减少设置硬件和软件, 以及再现测试环境所需的时间, 提高开发和测试效率。
- ❑ 提高服务器可用性, 转移配置中所需数量的物理计算机。

通常来讲, 用户通过 Hyper-V 可以使用 Windows Server 2008 中的一项技术创建一个虚拟化的服务器计算环境, 利用多个硬件资源来提高计算资源的效率。Hyper-V 的主要特点如下。

- ❑ 基于 64 位本机虚拟机管理程序的虚拟化。
- ❑ 能够同时运行 32 位和 64 位虚拟机。
- ❑ 单处理器和多处理器虚拟机。
- ❑ 它能够捕获正在运行的虚拟机的状态、数据和硬件配置。由于快照记录系统状态, 因此用户可以将虚拟机恢复到以前的状态。
- ❑ 支持较大的虚拟机内存。
- ❑ 支持虚拟的 LAN (局域网络)。
- ❑ 支持 Microsoft 管理控制台 (MMC) 3.0 管理工具。
- ❑ 文档化的 Windows Management Instrumentation (WMI) 界面, 便于编写脚本和进行管理。

### 4. Windows PowerShell 命令行

Windows PowerShell 是一种专门为系统管理设计的基于任务的新命令行 Shell 和脚本语言, 图 1-3 所示为其操作窗口。它构建在 .NET Framework 之上, 可以帮助管理人员管理 Windows 操作系统和应用程序。

内置的 Windows PowerShell 命令称为 cmdlet, 可让用户以命令行的方式管理组织中的计算机。Windows PowerShell 可让用户访问数据存储在注册表和证书存储, 与访问文件系统一样方便。另外, Windows PowerShell 具有丰富的表达式解析程序和完整开发的脚本语言。