

Windows Server 2008的Active Directory强化组策略功能并提供更高的可用性，本书提供IT人员必备的知识与技能，让IT专业人员可以充分使用Active Directory管理企业IT环境。

—— 中国台湾微软服务器平台事业部产品营销经理 朱庭辉

Microsoft®

# Windows Server 2008

第5版

## Active Directory 配置指南

光盘内容：本书范例文件

五年磨一剑，百万销量实力保障  
WinServer 2008三卷本之一

戴有炜（中国台湾） 编著

- 微软MCTS、MCITP认证考试最佳实战参考书
- 充分掌握Active Directory Domain Services (AD DS) 的完整知识体系
- 通过虚拟技术，只要一台电脑就可以搭建完整的网络学习环境
- 独家以Active Directory Domain Services配置实战为主题
- 一流专业的叙述，配合丰富的配置范例与图片，清晰易懂
- 随处可见的大量提示，提供专家级的建议指导，汇聚作者多年经验智慧
- 一贯秉持理论与实战兼顾的写作风格，完全以读者立场编写，广受好评

Windows Server 2008  
Active Directory配置指南  
(第5版)

戴有炜 编著

科学出版社  
北京科海电子出版社

## 内 容 提 要

本书作者戴有炜先生是中国台湾微软资深顾问、微软认证讲师、微软认证系统工程师，已编写过多本关于 Windows 操作系统的畅销图书，累计销量近百万。本书为作者的最新力作。

书中采用图文并茂的方式，以完整清晰的操作过程，配以大量演示图例，全面介绍了 Windows Server 2008 关于活动目录的强大功能和使用方法。全书共 13 章，包括 AD DS 基本概念、创建 AD DS 域、域用户与组账户的管理、利用组策略管理用户的工作环境、利用组策略部署软件、限制软件的运行、创建域树和林、管理域与林信任、Active Directory 数据库的复制、操作主机的管理、AD DS 的维护、将资源发布到 AD DS、自动信任根 CA 等内容。

本书面向广大初中级网络技术人员、网络管理和维护人员、网络系统集成人员，也可作为高等院校相关专业和技术培训班的教学用书，同时可以作为 MCTS/MCITP 认证考试的参考用书。

## 版 权 声 明

本书为经台湾基峰资讯股份有限公司独家授权发行的中文简体版。本书中文简体字版在中国大陆之专有出版权属科学出版社所有。在没有得到本书原版出版者和本书出版者书面许可时，任何单位和个人不得擅自摘抄、复制本书的一部分或全部以任何方式（包括资料和出版物）进行传播。本书原版权权属基峰资讯股份有限公司。版权所有，侵权必究。

北京市版权局著作权合同登记号 图字：01-2009-3187

### 图书在版编目（CIP）数据

Windows Server 2008 Active Directory 配置指南/戴有炜编著.  
—5 版. —北京：科学出版社，2009  
ISBN 978-7-03-024716-2

I. W… II. 戴… III. 窗口软件—网络服务器—指南  
IV. TP316.86-62

中国版本图书馆 CIP 数据核字（2009）第 090911 号

责任编辑：刘秀青 / 责任校对：赵丽萍  
责任印制：科海 / 封面设计：洪文婕

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>

北京市艺辉印刷有限公司印刷

科学出版社发行 各地新华书店经销

\*

2009 年 7 月 第 5 版

开本：16 开

2009 年 7 月 第一次印刷

印张：27

印数：0 001~4 000

字数：657 000

定价：49.80 元（含 1CD 价格）

（如有印装质量问题，我社负责调换）

# 出版说明

《Windows Server 2008 安装与管理指南》、《Windows Server 2008 网络专业指南》和《Windows Server 2008 Active Directory 配置指南》三本图书是我国台湾地区的资深 Windows 培训专家和咨询顾问戴有炜先生的最新力作。

戴先生多年担任微软认证讲师、微软认证系统工程师、微软资深顾问、台湾综合生活股份有限公司技术支持部技术总监和教育培训中心讲师，拥有十几年使用、咨询和讲授 Windows 操作系统的成功经验。戴先生于 1997 年编撰出版了《Windows NT Server 4.0 专业指南》、《Windows NT Server 4.0 实用指南》，2000 年推出其升级版《Windows 2000 网络实用指南》和《Windows 2000 网络专业指南》。这 4 种图书的简体中文版销售累计超过 30 万册，被誉为 Windows NT 4.0 和 Windows 2000 Server 用户和管理员的福音书。

2003 年，微软推出新一代操作系统 Windows Server 2003，应中国大陆和台湾地区广大读者的要求，戴先生认真整理并重新编写了 Windows Server 2003 三卷本：《Windows Server 2003 用户管理指南》、《Windows Server 2003 网络专业指南》和《Windows Server 2003 Active Directory 配置指南》。该套图书得到了两岸读者的大力推崇，近几年始终排在同类操作系统图书的前几名，更被多所学校用作教材。

本次推出的 Windows Server 2008 三卷本，作者秉承了一贯的写作风格和体例，凭借丰富的教学与咨询经验，完全从读者使用和学习角度出发，以翔实的步骤与精确的说明引领读者迅速掌握 Windows Server 2008，充分考虑读者操作时可能发生的问题，并提供解决方案。本书内容仍然适应 MCTS/MCITP 认证考试的需求，是您的最佳实用参考书籍。

✎ 《Windows Server 2008 安装与管理指南》的主要内容：Windows Server 2008 基本概念、Windows Server 2008 的安装与基本环境设置、本地用户与组账户的管理、创建 Active Directory 域、NTFS 磁盘的安全与管理、访问网络文件、打印服务器的设置与管理、利用配置文件管理用户工作环境、文件服务器的管理、组策略与安全设置、注册表与注册表编辑程序、远程桌面连接、磁盘系统的管理、利用 WSUS 部署更新程序、AD RMS 企业文件版权管理、分布式文件系统、搭建 iSCSI 文件服务器故障转移群集、系统启动的疑难排除。

✎ 《Windows Server 2008 网络专业指南》的主要内容：Windows Server 2008 基本网络概念、利用 DHCP 自动指派 IP 地址、解析 NetBIOS 名称、解析 DNS 主机名、IIS 网站的架设、PKI 和 SSL 网站与邮件安全、Web Farm 与网络负载均衡、SMTP 服务器的架构、FTP 服务器的架设、IPSec 与网络安全、路由器与网桥的设置、网络地址转换、虚拟专用网络、RADIUS 服务器的架设、网络访问保护。

- ✎ 《Windows Server 2008 Active Directory 配置指南》的主要内容: Active Directory Domain Services (AD DS) 的基本概念、组策略、账户原则、WMI 筛选器、组策略模型、“入门 GPO”、限制用户执行软件、控管用户工作环境、控管客户端计算机环境、一次同时新增多个用户账户、操作主机的管理、AD DS 的备份与还原、Active Directory 数据库的维护与优化、Active Directory 数据库的复制、网站的配置与管理、AD DS 与防火墙等。

戴先生的图书一直以来都受到了广大读者的厚爱与好评，其历年图书的总销量已近百万，实属操作系统类图书的上上乘之作。希望本次隆重推出的 Windows Server 2008 三卷本不会让您失望，能够对您有所帮助，并能得到您的中肯意见与鼎力支持。

# 序 言

首先感谢读者长久以来的支持与爱护！本系列书籍依然采用我一贯的编写风格，也就是完全站在读者的角度来考虑问题，并且以实用的观点来编写这几本 Windows Server 2008 书籍。我花费了相当多的时间不断测试并验证书中所叙述的内容，并融合多年的教学经验，以最容易让您理解的方式将其写入书中，希望能够帮助您更轻松地学习与使用 Windows Server 2008。

这套图书的宗旨是希望读者能通过书中完整而清晰的范例操作，充分了解 Windows Server 2008，从而能够轻松地配置和管理 Windows Server 2008 的网络环境。书中的理论讲解细致清晰，范例丰富。对需要参加微软认证考试的读者来说，这套书更是不可或缺的实际参考书籍。

本套书包括《Windows Server 2008 安装与管理指南》、《Windows Server 2008 网络专业指南》和《Windows Server 2008 Active Directory 配置指南》三本，内容丰富翔实。相信这几本书仍然不会辜负您的期望，在您学习 Windows Server 2008 时能给予最大的帮助。

感谢所有让这套书能够顺利出版的朋友们，包括给予宝贵意见、协助技术校稿、出借测试设备或是提供软件资源的朋友们，尤其是“综合生活股份有限公司”这家专门承接微软技术支持项目的公司，一直都给予我全方位的支持，包含各种最新、最快的资源与各种测试设备。

戴有炜  
2008 年 9 月

注：Windows Server 2008 试用版的微软官方下载地址：

<http://www.microsoft.com/china/windowsserver2008/default.aspx>

**小贴士：**若试用期限已到，但是您暂时不想激活的话，还可以延长试用期。请在 60 天试用期即将到期前运行以下命令：

```
slmgr -rearm
```

待出现命令运行完成画面后重新启动计算机，会将试用期重新配置为 60 天。如已经试用了 59 天，只剩下 1 天可用，此时只要运行此命令，就可以再试用 60 天。最多可以延期 3 次，也就是可试用 240 天。

# 目 录

## Chapter 1 Active Directory Domain Services (AD DS) ..... 1

1-1 Active Directory Domain Services 概述.....	1
1-1-1 Active Directory Domain Services 的适用范围 (Scope) .....	2
1-1-2 名称空间 (Namespace) .....	2
1-1-3 对象 (Object) 与属性 (Attribute) .....	2
1-1-4 容器 (Container) 与组织单位 (Organization Units, OU) .....	3
1-1-5 域树目录 (Domain Tree) .....	3
1-1-6 信任 (Trust) .....	4
1-1-7 林 (Forest) .....	5
1-1-8 架构 (Schema) .....	6
1-1-9 域控制器 (Domain Controller) .....	6
1-1-10 Active Directory 的复制模式.....	7
1-1-11 域中的其他成员计算机.....	7
1-1-12 DNS 服务器.....	8
1-1-13 轻型目录访问协议 (LDAP) .....	8
1-1-14 全局编录 (Global Catalog) .....	10
1-1-15 站点 (Site) .....	10
1-1-16 目录分区 (Directory Partition) .....	11
1-2 Windows Server 2008 域控制器的新功能.....	12
1-2-1 只读域控制器 (RODC) .....	12
1-2-2 可重新启动的 AD DS (Restartable AD DS) .....	13
1-3 域功能级别与林功能级别 .....	14
1-3-1 域功能级别 (Domain Functionality Level) .....	14
1-3-2 林功能级别 (Forest Functionality Level) .....	15
1-4 Active Directory 轻型目录服务 (AD LDS) .....	15

## Chapter 2 创建 AD DS 域..... 17

2-1 创建 AD DS 域前的准备工作.....	17
2-1-1 选择适当的 DNS 域名 .....	18
2-1-2 准备好用来支持 AD DS 的 DNS 服务器 .....	18
2-1-3 选择 Active Directory 数据库的存储地点 .....	20
2-2 创建 AD DS 域.....	21

2-2-1	使用 Windows 窗口界面来安装网络中的第一台域控制器	22
2-2-2	使用应答文件安装网络中的第一台域控制器	30
2-2-3	使用“命令行”来安装网络中的第一台域控制器	31
2-3	确认 AD DS 域是否正常	32
2-3-1	检查 DNS 服务器内的日志是否完整	32
2-3-2	排除注册失败的问题	35
2-3-3	检查 Active Directory 数据库文件与 SYSVOL 文件夹	36
2-3-4	添加新的管理工具	37
2-3-5	查看事件日志文件	38
2-4	提升域与林功能级别	39
2-4-1	提升域功能级别	39
2-4-2	提升林功能级别	39
2-5	添加额外域控制器与 RODC	39
2-5-1	使用 Windows 窗口界面来安装额外域控制器	40
2-5-2	使用应答文件来安装额外域控制器	47
2-5-3	使用“命令行”来安装额外域控制器	49
2-5-4	使用“安装媒体”来安装额外域控制器	49
2-5-5	更改 RODC 的委派与密码复制策略设置	52
2-6	阶段式安装 RODC	53
2-6-1	使用 Windows 窗口界面创建 RODC 账户	53
2-6-2	将服务器附加到 RODC 账户	57
2-7	将 Windows 计算机加入或脱离域	61
2-7-1	将 Windows 计算机加入域	61
2-7-2	使用已加入域的计算机登录	64
2-7-3	脱离域	65
2-8	在域成员计算机内安装 AD DS 管理工具	66
2-9	删除域控制器与域	67
2-9-1	使用 Windows 窗口界面来删除域控制器或域	68
2-9-2	使用应答文件来删除域控制器或域	71
2-9-3	使用“命令行”删除域控制器或域	72
2-10	域升级与在现有域环境中安装域控制器	73
2-10-1	将现有 Windows 2000 或 Windows Server 2003 林升级	73
2-10-2	在现有 Windows 2000 或 Windows Server 2003 林中添加一个 Windows Server 2008 域	75
2-10-3	在现有 Windows 2000 或 Windows Server 2003 域中添加一台 Windows Server 2008 域 控制器	76



<b>Chapter 3 域用户与组账户的管理</b> .....	<b>77</b>
3-1 管理域用户账户 .....	77
3-1-1 创建组织单位与域用户账户 .....	78
3-1-2 用户登录账户 .....	79
3-1-3 创建 UPN 的后缀 .....	81
3-1-4 账户的一般管理工作 .....	82
3-1-5 域用户账户的内容设置 .....	84
3-1-6 查找用户账户 .....	86
3-1-7 域控制器之间数据的复制 .....	87
3-2 一次同时添加多个用户账户 .....	89
3-2-1 利用 csvde.exe 来添加用户账户 .....	89
3-2-2 利用 ldifde.exe 来添加、修改与删除用户账户 .....	91
3-2-3 利用 dsadd.exe 等程序来添加、修改与删除用户账户 .....	92
3-3 域组账户 .....	93
3-3-1 域内的组类型 .....	94
3-3-2 组的作用域 .....	94
3-3-3 域组的创建与管理 .....	95
3-3-4 AD DS 内置的组 .....	96
3-3-5 特殊组账户 .....	98
3-4 组的使用准则 .....	99
3-4-1 A、G、DL、P 策略 .....	99
3-4-2 A、G、G、DL、P 策略 .....	99
3-4-3 A、G、U、DL、P 策略 .....	100
3-4-4 A、G、G、U、DL、P 策略 .....	100
<b>Chapter 4 利用组策略来管理用户的工作环境</b> .....	<b>101</b>
4-1 组策略概述 .....	101
4-1-1 组策略的功能 .....	101
4-1-2 组策略对象 (Group Policy Object) .....	103
4-1-3 策略设置与首选项设置 .....	105
4-1-4 组策略的应用时限 .....	106
4-2 策略设置实战演练 .....	107
4-2-1 策略设置实战演练 1: 计算机配置 .....	107
4-2-2 策略设置实战演练 2: 用户配置 .....	109
4-3 首选项设置实战演练 .....	112
4-3-1 首选项设置实战演练 1 .....	112
4-3-2 首选项设置实战演练 2 .....	117

4-4 组策略的处理规则	121
4-4-1 一般的继承与处理规则	121
4-4-2 特殊的继承设置	122
4-4-3 特殊的处理设置	125
4-4-4 更改管理 GPO 的域控制器	129
4-4-5 更改组策略的应用间隔时间	131
4-5 利用组策略来管理计算机与用户环境	133
4-5-1 计算机配置的管理模板策略	133
4-5-2 用户配置的管理模板策略	134
4-5-3 账户策略	135
4-5-4 用户权限分配策略	139
4-5-5 安全选项策略	141
4-5-6 登录/注销、启动/关机脚本	142
4-5-7 文件夹重定向	145
4-6 利用组策略来限制访问“可移动存储设备”	152
4-7 WMI 筛选器	155
4-8 组策略建模与组策略结果	159
4-8-1 组策略建模	159
4-8-2 组策略结果	163
4-9 组策略的委派管理	165
4-9-1 站点、域或组织单位的 GPO 链接委派	165
4-9-2 编辑 GPO 的委派	166
4-9-3 添加 GPO 的委派	166
4-10 “Starter GPO”的设置与使用	167

## Chapter 5 利用组策略部署软件 169

5-1 软件部署概述	169
5-1-1 将软件分配给用户	170
5-1-2 将软件分配给计算机	170
5-1-3 将软件发布给用户	170
5-1-4 自动修复软件	171
5-1-5 删除软件	171
5-2 将软件发布给用户	171
5-2-1 发布软件	171
5-2-2 客户端安装已发布的软件	174
5-2-3 测试自动修复软件的功能	175
5-2-4 取消已发布的软件	177
5-3 将软件分配给用户或计算机	177

5-3-1 分配给用户	177
5-3-2 分配给计算机	178
5-4 将软件升级与重新部署	179
5-4-1 软件升级	179
5-4-2 重新部署	181
5-5 部署 Microsoft Office	182
5-5-1 部署 Microsoft Office 2003	183
5-5-2 部署 Microsoft Office 2007	188
5-6 发布 ZAP 应用程序	192
5-7 软件部署的其他设置	195
5-7-1 更改部署默认值	195
5-7-2 更改高级部署设置	196
5-7-3 扩展名与软件关联的优先级	197
5-7-4 软件分类	197
5-8 将软件重新包装成“MSI 应用程序”	199

## Chapter 6 限制软件的运行 201

6-1 软件限制策略概述	201
6-1-1 哈希规则	202
6-1-2 证书规则	202
6-1-3 路径规则	202
6-1-4 网络区域规则	202
6-1-5 规则的优先级	203
6-2 启用软件限制策略	203
6-2-1 新建哈希规则	204
6-2-2 新建路径规则	207
6-2-3 新建证书规则	209
6-2-4 新建网络区域规则	212
6-2-5 不要将软件限制策略应用到本地系统管理员	213

## Chapter 7 新建域树和林 215

7-1 新建第一个域	215
7-2 新建子域	216
7-2-1 利用 Windows 窗口界面来新建子域	216
7-2-2 利用应答文件来新建子域	225
7-2-3 使用“命令行”来新建子域	227
7-3 新建林中的第 2 个域树	228
7-3-1 选择适当的 DNS 架构	228

7-3-2	使用 Windows 窗口界面来新建第 2 个域树 .....	230
7-3-3	使用应答文件来新建第 2 个域树 .....	239
7-3-4	使用“命令行”来新建第 2 个域树 .....	240
7-4	删除子域与域树 .....	240
7-4-1	使用 Windows 窗口界面来删除子域或域树 .....	241
7-4-2	使用应答文件来删除子域或域树 .....	244
7-4-3	使用“命令行”来删除子域或域树 .....	246
7-5	更改域控制器的计算机名 .....	246
<b>Chapter 8 管理域与林信任 .....</b>		<b>249</b>
8-1	域与林信任概述 .....	249
8-1-1	信任域与受信任域 .....	249
8-1-2	跨域访问资源的流程 .....	250
8-1-3	信任的种类 .....	252
8-1-4	建立信任前的注意事项 .....	256
8-2	建立“快捷方式信任” .....	258
8-3	新建“林信任” .....	263
8-3-1	建立“林信任”前的注意事项 .....	264
8-3-2	开始建立“林信任” .....	265
8-3-3	“选择性身份验证”设置 .....	272
8-4	建立“外部信任” .....	275
8-5	管理与删除信任 .....	277
8-5-1	信任的管理 .....	277
8-5-2	信任的删除 .....	280
<b>Chapter 9 Active Directory 数据库的复制 .....</b>		<b>283</b>
9-1	站点与 Active Directory 数据库的复制 .....	283
9-1-1	同一个站点之间的复制 .....	284
9-1-2	不同站点之间的复制 .....	286
9-1-3	目录分区与复制拓扑 .....	287
9-1-4	复制协议 .....	287
9-2	默认站点的管理 .....	287
9-2-1	默认的站点 .....	287
9-2-2	Servers 文件夹与复制设置 .....	288
9-3	用站点来管理 Active Directory 复制 .....	290
9-3-1	建立站点与子网 .....	291
9-3-2	建立站点链接 .....	293
9-3-3	将域控制器转移到所属的站点 .....	294

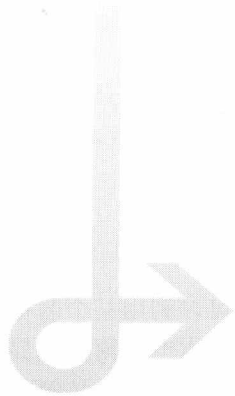
9-3-4 指定“首选的 bridgehead 服务器” .....	296
9-3-5 站点链接与 Active Directory 数据库的复制设置 .....	297
9-3-6 站点链接桥 .....	299
9-3-7 站点链接桥的两个范例 .....	301
9-4 管理“全局编录服务器” .....	303
9-4-1 将属性添加到全局编录内 .....	303
9-4-2 全局编录的功能 .....	304
9-4-3 通用组成员身份缓存 .....	305
9-5 解决 Active Directory 复制冲突的问题 .....	307
9-5-1 属性印章 .....	307
9-5-2 冲突的种类 .....	307
<b>Chapter 10 操作主机的管理 .....</b>	<b>311</b>
10-1 操作主机概述 .....	311
10-1-1 架构操作主机 .....	312
10-1-2 域命名操作主机 .....	312
10-1-3 RID 操作主机 .....	312
10-1-4 PDC 模拟器操作主机 .....	312
10-1-5 基础结构操作主机 .....	315
10-2 操作主机的放置优化 .....	316
10-2-1 基础结构操作主机的放置 .....	316
10-2-2 PDC 模拟器操作主机的放置 .....	316
10-2-3 林级别操作主机的放置 .....	317
10-2-4 域级别操作主机的放置 .....	317
10-3 找出扮演操作主机角色的域控制器 .....	318
10-3-1 找出“架构操作主机” .....	318
10-3-2 找出“域命名操作主机” .....	319
10-3-3 找出“RID”、“PDC 模拟器”与“基础结构”操作主机 .....	320
10-4 转移操作主机角色 .....	320
10-5 夺取操作主机角色 .....	323
10-5-1 操作主机故障所造成的影响 .....	323
10-5-2 夺取操作主机角色实战演练 1 .....	325
10-5-3 夺取操作主机角色实战演练 2 .....	327
<b>Chapter 11 AD DS 的维护 .....</b>	<b>331</b>
11-1 系统状态概述 .....	331
11-1-1 Active Directory 数据库 .....	332
11-1-2 SYSVOL 文件夹 .....	333

11-2	备份 AD DS	333
11-2-1	安装 Windows Server Backup 功能	333
11-2-2	备份系统状态	333
11-3	还原 AD DS	335
11-3-1	进入“目录服务还原模式”的方法	335
11-3-2	执行 AD DS 的“非系统授权还原”	336
11-3-3	针对被删除的 AD DS 对象执行“系统授权还原”	337
11-3-4	还原组成员的隶属关系	341
11-4	Active Directory 数据库的转移与整理	342
11-4-1	可重新启动的 AD DS (Restartable AD DS)	342
11-4-2	转移 Active Directory 数据库文件	342
11-4-3	整理 Active Directory 数据库	347
11-5	重设“目录服务还原模式”的系统管理员密码	350
11-6	更改“可重新启动的 AD DS”的登录设置	351
<b>Chapter 12 将资源发布到 AD DS</b>		<b>353</b>
12-1	将共享文件夹发布到 AD DS	353
12-1-1	利用“Active Directory 用户和计算机”控制台发布	353
12-1-2	利用“计算机管理”控制台发布	355
12-2	查找 AD DS 内的资源	356
12-2-1	通过“网络”查找	356
12-2-2	通过“Active Directory 用户和计算机”控制台查找	358
12-3	将共享打印机发布到 AD DS	361
12-3-1	发布打印机	361
12-3-2	通过 AD DS 查找共享打印机	363
12-3-3	利用“打印机位置”来查找打印机	363
<b>Chapter 13 自动信任根 CA</b>		<b>367</b>
13-1	自动信任 CA 的设置准则	367
13-2	自动信任内部的独立 CA	368
13-2-1	下载独立根 CA 的证书并保存	368
13-2-2	将独立根 CA 的证书导入到“受信任的根证书颁发机构”策略	370
13-3	自动信任外部的 CA	373
13-3-1	下载独立根 CA 的证书并保存	374
13-3-2	创建“证书信任列表 (CTL)”	377

<b>Appendix A AD DS 与防火墙</b> .....	<b>383</b>
A-1 AD DS 相关的端口 .....	383
A-1-1 将客户端计算机加入域和用户登录时会用到的端口 .....	384
A-1-2 计算机登录时会用到的端口 .....	384
A-1-3 创建域信任时会用到的端口 .....	385
A-1-4 验证域信任时会用到的端口 .....	385
A-1-5 访问文件资源时会用到的端口 .....	385
A-1-6 执行 DNS 查询时会用到的端口 .....	385
A-1-7 执行 Active Directory 数据库复制时会用到的端口 .....	385
A-1-8 文件复制服务 (FRS) 会用到的端口 .....	386
A-1-9 分布式文件系统 (DFS) 会用到的端口 .....	386
A-1-10 其他可能需要开放的端口 .....	387
A-2 限制动态 RPC 端口的使用范围 .....	387
A-2-1 限制所有服务的动态 RPC 端口范围 .....	387
A-2-2 限制 Active Directory 数据库复制使用指定的静态端口 .....	389
A-2-3 限制 FRS 使用指定的静态端口 .....	390
A-2-4 限制 DFS 使用指定的静态端口 .....	390
A-3 IPSec 与 VPN 端口 .....	391
A-3-1 IPSec 所使用的协议与端口 .....	391
A-3-2 PPTP VPN 所使用的协议与端口 .....	391
A-3-3 L2TP/IPSec 所使用的协议与端口 .....	391
<b>Appendix B 服务器核心安装选项的管理</b> .....	<b>393</b>
B-1 “服务器核心安装” 概述 .....	393
B-2 “服务器核心安装” 的基本设置 .....	394
B-2-1 更改计算机名称 .....	394
B-2-2 更改 IP 地址 .....	395
B-2-3 启用 “服务器核心安装” .....	396
B-2-4 启用 Windows 防火墙的 “远程管理” 规则 .....	396
B-2-5 加入域 .....	397
B-2-6 将域用户加入本地 Administrators 组 .....	397
B-2-7 更改日期与时间、地区及语言选项 .....	397
B-3 在 “服务器核心安装” 内安装服务器角色 .....	398
B-3-1 查看现有的角色 .....	398
B-3-2 DNS 服务器角色 .....	398
B-3-3 DHCP 服务器角色 .....	399
B-3-4 文件服务角色 .....	399

B-3-5	Hyper-V 角色	400
B-3-6	打印服务角色	400
B-3-7	Active Directory Lightweight Directory Services (AD LDS) 角色	400
B-3-8	Active Directory Domain Services (AD DS) 角色	400
B-3-9	Stream Media Services 角色	400
B-3-10	Web 服务器 (IIS) 角色	401
B-4	在“服务器核心安装”内安装功能	402
B-5	管理“服务器核心安装”	403
B-5-1	在“命令提示符”环境下管理	404
B-5-2	在远程计算机通过“远程桌面”管理	404
B-5-3	在远程计算机通过 TS RemoteApp 管理	405
B-5-4	在远程计算机通过 Windows Remote Shell 管理	408
B-5-5	在远程计算机通过 MMC 管理控制台管理	408
B-5-6	硬件设备的安装	409
B-5-7	其他注意事项	410
B-6	常用命令列表	410
B-6-1	设置与安装命令	411
B-6-2	网络与防火墙命令	412
B-6-3	更新、错误报告与回应	412
B-6-4	服务、程序与性能	413
B-6-5	事件日志	414
B-6-6	磁盘与文件系统	414
B-6-7	硬件设备驱动程序	415





# 1 Chapter

## Active Directory Domain Services (AD DS)

在 Windows Server 2008 网络环境中，Active Directory Domain Services (AD DS) 为您提供用于组织、管理与控制网络资源的各种功能。

- ▼ Active Directory Domain Services 概述
- ▼ Windows Server 2008 域控制器的新功能
- ▼ 域功能级别与林功能级别
- ▼ Active Directory 轻型目录服务 (AD LDS)

### 1-1 Active Directory Domain Services 概述

何谓 **directory** 呢？我们日常生活中使用的电话簿内记录着亲朋好友的姓名、电话与地址等数据，它就是 **telephone directory**（电话目录）；计算机中的文件系统（file system）内记录着文件的文件名、大小与日期等数据，它就是 **file directory**（文件目录）。

如果这些 **directory** 内的数据能够系统地加以整理的话，用户就能够容易且迅速地找到所需文件，而 **directory service**（目录服务）所提供的服务，就是要让用户容易且迅速地在 **directory** 内查找所需文件。在现实生活中，查号台也是一种目录服务；在因特网上，Google 网站所提供的搜索功能也是一种目录服务。

Active Directory 域内的 **directory** 则是用来存储用户账户、计算机账户、打印机与共享文件夹等对象，我们把这些对象的存储地点称为 **目录数据库**（directory database）。Active Directory 域内负责提供目录服务的组件就是 **Active Directory 域服务**（Active Directory Domain Services, AD DS），它负责目录数据库的存储、添加、删除、修改与查询等工作。