

Windows 2003 网管专家系列
Windows 2003 Network Management Expert Series

最新版

优秀经典
畅销书

Windows 2003 Server 网络管理手册

李 劲 / 编著

- 由于扎实的内容，本书的 Windows 2000 版本已持续畅销多年，成为经典
 - 本书由具有丰富经验的台湾高级网络管理专家精心编著，内容实用而权威
 - 重点讲述以 Windows 2003 Server 作为网络服务器的高级配置与管理技巧
 - 步骤讲解详细、图例丰富，是一本难得的 Windows 2003 Server 网管指南
 - 本书全面系统、结构合理，是您成为高级网管人员必不可少的参考学习手册
- 专家编著 + 内容系统 + 图例详尽 = 高级指导教程



中国青年出版社



文魁资讯股份有限公司

华北水利水电学院图书馆



209087815

TP316.86
L185

Windows 2003 网管专家系列

Windows 2003 Server

网络管理手册 (最新版) 李 劲 / 编著



中国青年出版社
CHINA YOUTH PRESS

· 908781

(京)新登字 083 号

本书由文魁资讯股份有限公司授权中国青年出版社独家出版。未经出版者书面许可,任何单位和个人均不得以任何形式复制或传播本书的部分或全部。

版权贸易合同登记号: 01-2003-6468

图书在版编目(CIP)数据

Windows 2003 Server 网络管理手册 / 李劲编著, —北京: 中国青年出版社, 2004

ISBN 7-5006-5581-9

I. W... II. 李... III. 服务器—操作系统(软件), Windows 2003 Server—技术手册 IV. TP316.86-62

中国版本图书馆 CIP 数据核字(2003)第 110696 号

书 名: Windows 2003 Server 网络管理手册

编 著: 李 劲

出版发行: 中国青年出版社

地址: 北京市东四十二条 21 号 邮政编码: 100708

电话: (010) 84015588 传真: (010) 64053266

印 刷: 中国农业出版社印刷厂

开 本: 787 × 1092 1/16 印 张: 28.25

版 次: 2004 年 3 月北京第 1 版

印 次: 2004 年 3 月第 1 次印刷

书 号: ISBN 7-5006-5581-9/TP · 362

定 价: 45.00 元

序

自千禧年Microsoft以雷霆万钧之势推出Windows 2000 Server操作系统至今已三年有余，在这些日子里Windows 2000 Server急速扩张了服务器操作系统的版图。同时，Microsoft也在这些日子里积累了实际测试的经验，并确立了细微调整的方向。为了改进原先的缺点与不足，Microsoft在2003年推出Windows Server 2003，除了继续强化Windows 2000 Server原本就很好的领域（如：目录整合、管理工具、远端桌面连接等）之外也加入了一些新功能（如：整合.NET Framework、阴影复制、UDDI等）。

Windows Server 2003的设计宗旨为：协助企业快速连接组织中的资源，除此之外，Windows Server 2003的.NET Framework 1.1与同步推出的Microsoft Visual Studio .NET 2003紧密配合，不仅提升其延展性，并提供从开发、部署到管理的最佳解决方案，让程序开发人员能轻松地设计出更安全、更高效的应用程序。

本书的内容包含广泛，从Windows Server 2003各版本的差异、功能的简介、新增的功能、域的概念乃至活动目录的观念与建立都有介绍。整本书的架构可分为系统的功能介绍与设置、管理工具介绍、资源的管理、域的概念与设置、网络服务与监控等几大部分。对于初学者而言，依照本书的进度学习，您一定会了解Windows Server 2003的操作与精髓。

Windows Server 2003在当做独立服务器或是域控制器时会有不同的表现，在本书的前几章会分开介绍。因此，读者在一开始设置Windows Server 2003时无论其服务器的角色为何都可以很清楚、轻松地学习。如果您急着要设置域，则需要先了解Active Directory、添加域成员、设定DNS、DHCP等网络服务，这些内容都是在第10章以后。但就算是一开始便依照第11章的步骤建立了域而让您的服务器变成域控制器，也不会影响前面几章的操作方式，因此您可以自行选择服务器的角色来学习Windows Server 2003。

最后祝您能凭借此书轻松地学会Windows Server 2003的系统操作与管理。

李 劲

May. 2003于台北

025117/04

目录



第1章 Windows Server 2003 简介

1-1 Windows Server 2003 的版本说明	2
1-2 Windows Server 2003	5
1-3 Windows Server 2003 的新增功能 与改善	8
1-3-1 Active Directory	8
1-3-2 应用程序服务器	10
1-3-3 群集技术	12
1-3-4 文件与打印服务器	15
1-3-5 IIS 6.0	17
1-3-6 管理服务	18
1-3-7 网络与通讯服务	21
1-3-8 安全性功能	23
1-3-9 存储管理功能	25
1-3-10 终端服务器	27
1-3-11 Windows Media 服务	28
1-3-12 企业 UDDI 服务	29
1-4 Windows Server 2003 支持的文件 系统	31

第2章 安装 Windows Server 2003

2-1 安装前计划	34
2-2 升级安装	36
2-3 由光盘全新安装	39
2-3-1 执行安装程序	39
2-3-2 执行安装向导	41
2-3-3 网络设置	43
2-3-4 完成安装	44

第3章 Windows Server 2003 的系 统设置

3-1 系统设置	48
3-2 设置多重硬件配置文件	52
3-3 设置任务栏及开始菜单环境	52
3-4 任务管理器	58

3-5 安装新硬件	60
-----------------	----

第4章 用户账户设置与管理

4-1 Windows Server 2003 的用户账户 ...	66
4-2 用户账户管理工具	67
4-2-1 本机用户账户管理工具	67
4-2-2 域用户账户管理工具	68
4-3 新增用户账户	69
4-3-1 新增本机用户账户	69
4-3-2 新增域用户账户	71
4-4 设置账户属性	74
4-4-1 账户	74
4-4-2 隶属于	76
4-4-3 拨入	78
4-4-4 安全	78
4-5 管理用户账户	81

第5章 用户组设置与管理

5-1 Windows Server 2003 的内置 用户组	84
5-1-1 本地域组	84
5-1-2 全局组	86
5-1-3 本地组	87
5-1-4 通用组	88
5-2 新增用户组	88
5-2-1 新增本地用户组	88
5-2-2 新增域用户组	90
5-3 设置用户组属性	93
5-3-1 成员	93
5-3-2 隶属于	94

第6章 管理工具

6-1 计算机管理	98
6-1-1 系统工具	98
6-1-2 存储	101

6-1-3 服务和应用程序	102
6-2 授权管理	104
6-2-1 授权模式	105
6-2-2 管理与追踪使用权	107
6-3 任务计划管理	109
6-4 管理控制台	112
6-4-1 MMC 的作者模式	114
6-4-2 建立 MMC 控制台	116
6-4-3 查看控制台窗口中的树状 目录	118
6-4-4 添加项目至“收藏夹” 列表	119
6-4-5 设置控制台选项	120

第7章 文件管理

7-1 资源管理器的基本操作	124
7-1-1 文件的复制/移动/删除	125
7-1-2 文件的移动	125
7-1-3 文件的删除与还原	126
7-1-4 文件的查看	127
7-1-5 资源管理器的高级使用	130
7-2 文件与目录的安全设置	133
7-2-1 文件与目录的访问权限	134
7-2-2 文件与目录的访问审核	136
7-2-3 文件与目录的所有者	137
7-3 设置共享目录	138
7-3-1 新建共享文件夹	138
7-3-2 停止共享文件夹	141
7-3-3 设置共享文件夹	141
7-3-4 共享文件夹的卷影副本服务	143

第8章 磁盘系统管理

8-1 磁盘管理	148
8-1-1 基本磁盘管理	150
8-1-2 动态磁盘管理	153
8-2 磁盘重整工具	156
8-3 磁盘信息查看	158
8-4 磁盘空间配额	159

第9章 打印与传真服务器

9-1 打印术语说明	164
9-2 添加打印机	165
9-3 打印机资源设置	168
9-3-1 常规	168
9-3-2 共享	170
9-3-3 连接	171

9-3-4 高级	172
9-3-5 安全	174
9-3-6 在 Active Directory 中搜寻 打印机	174
9-4 在用户端建立打印机	176
9-5 添加网络打印机	178
9-6 管理打印机	179
9-6-1 打印机的权限设置	179
9-6-2 暂停打印	180
9-6-3 取消所有文件的打印	181
9-6-4 以脱机方式使用打印机	181
9-7 管理文件	181
9-8 设置打印服务器	184
9-9 Internet 打印	186
9-10 监视打印队列性能	187
9-11 设置传真服务	189

第10章 Active Directory 介绍

10-1 Active Directory 服务的功能	192
10-2 Active Directory 的观念与结构	193
10-3 Windows 的网络模式	197
10-4 复制与信任关系	198
10-4-1 全局编录 (Global Catalog)	198
10-4-2 复制	199
10-4-3 域间的信任关系	199
10-5 ADSI	202

第11章 Active Directory 管理

11-1 安装 Active Directory	204
11-2 删除 Active Directory	210
11-3 Active Directory 对象	212
11-4 创建 Active Directory 对象	212

第12章 管理安全性设置

12-1 安全性策略管理	218
12-2 账户策略	219
12-3 本机策略	221
12-4 事件记录	222
12-5 系统服务、登录以及文件系统	223
12-6 重新整理安全设置	225

第13章 审核与事件查看器

13-1 事件查看器	228
13-2 筛选与寻找事件	229
13-3 清除与存储日志文件	231

13-4 读取已存储的日志文件	232
13-5 事件查看器的其他功能	233
13-6 审核的介绍	235
13-7 设置文件与目录的审核事件	237
13-8 设置打印机的审核事件	238
13-9 设置 Active Directory 对象的 审核事件	239
13-10 在事件查看器中查看安全审核	241

第14章 性能监视器

14-1 性能监视器说明	244
14-2 系统监视器	245
14-2-1 添加/删除性能对象与 计数器	246
14-2-2 从性能监视中建立 HTML 报告	248
14-3 性能日志和警报	250
14-3-1 建立计数器日志文件	251
14-3-2 建立跟踪日志	253
14-3-3 建立警报	255
14-3-4 日志文件资料的使用	256

第15章 网络的安装与设置

15-1 局域网组件的安装	260
15-2 局域网组件的设置	264
15-2-1 Microsoft 网络客户端组件	265
15-2-2 Microsoft 网络的文件和打 印机共享组件	265
15-2-3 Internet 协议 (TCP/IP) 组件	266
15-3 网络识别设置	269
15-4 局域网连接的禁用与启动	271
15-5 测试 TCP/IP 的设置	272
15-6 映射网络驱动器	275
15-7 搜寻网络上的对象	277
15-8 安装拨号网络	278

第16章 DHCP 服务器管理

16-1 了解 DHCP 服务	286
16-2 安装 DHCP 服务	287
16-2-1 安装 DHCP 服务器	288
16-2-2 设置 DHCP 客户端	289
16-2-3 用户端取得设置的运行 原理	291
16-3 启用 DHCP 服务器	292
16-3-1 DHCP 服务器授权	292

16-3-2 添加作用域	294
16-3-3 设置排除地址	299
16-3-4 设置保留区	300
16-3-5 设置作用域选项	301
16-3-6 管理用户端租用	303
16-3-7 计划路由 DHCP 网络	304
16-3-8 为 DHCP 加入管理成员	304
16-4 设置 DHCP 服务器选项	305

第17章 WINS 服务器管理

17-1 了解 WINS 服务	308
17-2 安装与设置 WINS 服务器	309
17-2-1 安装 WINS 服务器	309
17-2-2 设置 WINS 客户端	310
17-3 设置静态配置 IP 地址	312
17-4 WINS 服务器选项设置	315
17-4-1 常规	315
17-4-2 间隔	316
17-4-3 数据库检查	316
17-4-4 高级	317
17-5 维护 WINS 数据库	318
17-5-1 备份 WINS 数据库	319
17-5-2 还原 WINS 数据库	319
17-6 DHCP 对 WINS 的支持	320

第18章 DNS 服务器管理

18-1 了解 DNS	324
18-1-1 DNS 意义与运行	324
18-1-2 DNS 名称解析运行程序	325
18-1-3 Windows Server 2003 DNS 特色	326
18-2 安装 DNS	327
18-2-1 安装 DNS 服务器	327
18-2-2 设置 DNS 用户端	329
18-3 DNS 的区域	330
18-4 建立正向查找区域	331
18-4-1 建立正向标准主要区域	331
18-4-2 建立正向标准辅助区域	333
18-4-3 删除区域	335
18-4-4 添加主机记录	335
18-4-5 添加主机别名	337

第19章 索引服务

19-1 索引服务的基本概念	340
19-2 安装索引服务	341
19-3 设置索引服务	342

19-4 进行查询	345
19-4-1 使用“开始”菜单中的 “搜索”功能	345
19-4-2 使用索引服务的查询表格	348
19-5 建立索引编录	349
19-6 建立索引文件	351
19-7 调整索引服务性能	352

第20章 网络资源监控

20-1 监控共享文件夹的访问	356
20-2 监控用户连接	357
20-3 发送控制台消息给用户	358
20-4 网络监视器	360
20-5 管理远程计算机	362

第21章 用户端连接

21-1 将 Windows 95/98 加入域	366
21-1-1 安装网络适配器与通讯 协议	366
21-1-2 设置网络适配器与通讯 协议	366
21-1-3 设置登录的域	367
21-2 加入 Windows 2000/2003 独立 服务器	368
21-3 将 Windows 2000/XP 加入域	370
21-3-1 资源共享	370
21-3-2 加入域	372
21-4 终端服务器	373
21-4-1 终端服务器的需求与主要 功能	373
21-4-2 安装终端服务器	375
21-4-3 激活终端服务器授权	376
21-4-4 安装远程桌面连接程序	378
21-4-5 远程桌面连接	381

第22章 资料备份与还原

22-1 资料备份	384
22-1-1 使用备份向导备份一般资料	385
22-1-2 使用备份功能表备份资料	389
22-1-3 备份类型	390
22-1-4 建立自动备份任务	391
22-2 资料还原	393
22-3 查看资料备份与还原的报告	396
22-4 资料备份与还原选项设定	397
22-4-1 常规	398
22-4-2 备份日志	398

22-4-3 排除文件	399
-------------------	-----

第23章 Windows Server 2003 的注册表

23-1 注册表的结构	402
23-2 注册表编辑器	403
23-3 注册表键值类型	404
23-4 导出注册表文件	405
23-5 修改注册表键值	407
23-6 导入注册表	408
23-7 查找项	409
23-8 安全控制	410

第24章 Internet 服务器

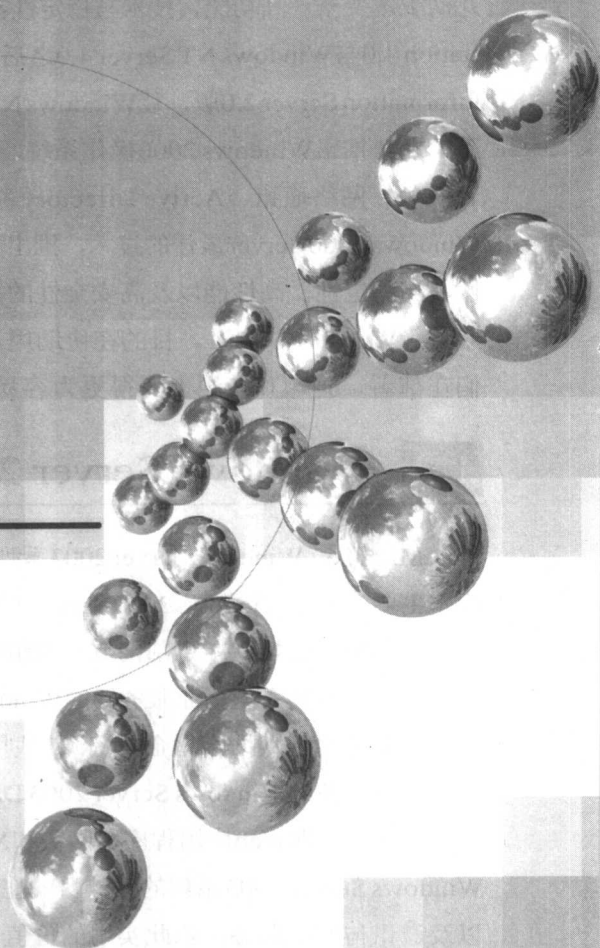
24-1 安装 IIS 6.0	412
24-2 测试安装的 IIS 6.0	414
24-3 IIS 6.0 的功能简介	415
24-3-1 可靠性	415
24-3-2 安全性	415
24-3-3 性能	417
24-3-4 管理性	417
24-3-5 扩展性	417
24-3-6 Internet 标准	418
24-4 Internet 信息服务 (IIS) 管理 工具	418
24-5 架设网站	421
24-5-1 添加虚拟目录	421
24-5-2 虚拟目录属性管理	425
24-5-3 添加网站	426
24-6 设置 Web 服务器	428
24-6-1 网站	429
24-6-2 性能	431
24-6-3 主目录	431
24-6-4 目录安全设置	433
24-7 架设 FTP 服务器	436
24-7-1 FTP 站点	438
24-7-2 安全设置账户	438
24-7-3 消息	439
24-7-4 主目录	440
24-7-5 目录安全设置	440
24-8 存储网站的设置	441
24-9 备份与还原 IIS 设置值	442
24-9-1 备份 IIS 的设置	442
24-9-2 还原 IIS 设置	442
24-10 WebDAV 发行	443
24-10-1 设置 WebDAV 发行目录	443

Windows Server 2003

网络管理手册

Chapter 1

Windows Server 2003 简介



自从Microsoft在1988年成立Microsoft Windows NT程序开发小组开发新的32位兼容操作系统以来,已有15年的历史。虽然只有15的历史,但在这些年当中Windows NT历经了几次版本变革,其功能、技术与稳定性都有长足的进步。在1996年推出Windows NT Workstation 4.0与Windows NT Server 4.0之后,由于使用简便、网络传输量增加更包含了Internet Information Server 2.0版,让Windows NT 4.0受到广大用户的支持。2000年Microsoft以雷霆万钧之势推出Windows 2000操作系统,不管是在服务器安装与设置、Web应用、文件与列表服务、网络通讯、Active Directory各方面都有长足的改进。2003年,Microsoft应用了Windows 2000 Server最佳的技术,推出了Microsoft Windows Server 2003,它是兼具高整合性、高稳定性、高性能以及高安全性的操作平台,是以XML为基础的综合应用服务与网络服务(Web Services),目的在协助用户降低信息管理成本,并增加管理上的效益,让我们在部署、打印和使用上变得更为容易。

1-1 Windows Server 2003的版本说明

Microsoft Windows Server 2003系列是Windows 2000 Server操作系统的下一代产品,该版本主要建立在Windows 2000 Serv设置的功能上。Microsoft提供四种不同版本的Windows Server 2003,包括适用于部门或小型组织等小型商业环境的Windows Server 2003标准版;与适用于中型到大型企业服务器的Windows Server 2003企业版,可支持32位与64位两种规格;以及适用于数据库、企业资源规划(ERP)软件、大量即时异动处理及服务器整合等大型关键任务的Windows Server 2003 DataCenter版,可支持32位与64位两种规格;还有适用于建立和管理Web应用程序、网页和XML Web Services的Windows Server 2003 Web版。Windows Server 2003系列的设计目的在于提供更优良的网络操作环境、应用程序执行环境以及通讯与网络服务。除此实用的价值外并兼具安全性、可靠性、扩展性、经济性以及易于管理的特性。

不管是哪个版本的Windows Server 2003,都有一个关键性的新功能Microsoft .NET Framework,它是用来建立、部署和执行XML Web Services和应用程序的方法。.NET Framework提供了高产能、标准化、多种开发语言的环境,将现有的系统与新一代的应用程序与服务加以整合,同时具备灵活性,能够解决、部署与操作Internet规模应用程序带来的挑战,而Windows Server 2003则提供了一个基础结构和应用程序开发平台。Microsoft .NET是Micr设置t的一个主要策略性开创行动,它让组织内荷柚茂间能够拥有更优良的连接能力。Windows Server 2003包括了许多支持这种与.NET连接能力的核心功能,包括:

- Microsoft .NET Framework。
- Microsoft XML Web Services平台。
- 深入整合Microsoft .NET Passport与Active Directory服务。

- 原生性支持以SOAP为基础的XML Web Services, 通过.NET Framework使用XML Web Services进行COM+组件架构的完全整合。

各版本之功能差异请参考表1-1, √表示全部功能支持, Δ则表示部分功能支持:

表1-1 Windows Server 2003各版本功能差异表

主要功能	Standard	Enterprise	DataCenter	Web
.Net 应用程序服务				
.Net Framework 是一个设置、部署及执行 XML Web Services 和其他应用程序的环境, 但是不支持 64 位版本的 Windows Server 2003 操作系统	√	√	√	√
Internet Information Services (IIS) 6.0 是一个全功能的网站服务器	√	√	√	√
ASP.NET 是一个针对网页应用程序与服务设计的引擎, 提供了快速开发环境, 将程序逻辑与界面区隔开	√	√	√	√
Enterprise UDDI Services 是一个提供企业或组织间使用 UDDI 服务的网络服务 (Web Services)	√	√	√	
业集技术				
网络负载均衡 (Network Load Balancing/NLB) 可以分散多个服务器间的 TCP/IP 流量	√	√	√	√
簇集服务 (Cluster Services) 是一群相互独立的电脑, 一起执行应用程序的共同资料集 (Common Set)		√	√	
通讯及网络服务				
虚拟专用网络 (Virtual Private Network/VPN) 是一种用户透过 Point-to-Point Tunneling Protocol (PPTP) 或 Layering Two Tunneling Protocol (L2TP) 从外面访问组织内部网络的方法	√	√	√	Δ
Internet 验证服务 (Internet Authentication Service/IAS) 支援验证与远端连线要求的授权服务	√	√	√	
网络桥接器 (Network Bridge) 让用户可以连接不同的区域网络区段	√	√	√	
Internet 连接共享 (Internet Connection Sharing/ICS) 可以将你家里的网络或办公室网络连接到 Internet 上, 还可以对所有电脑提供网络位置转换 (NAT)、定址以及名称解析服务	√	√		
IPv6 是下一代的 Internet 标准协定, 主要是为了解决 IP 位址缺乏、安全性以及延伸扩展性等问题	√	√	√	√
目录服务				
Active Directory 是以一种结构化的方式存储网络上物件的资讯, 并提供逻辑性、阶层组织的目录资讯, 让管理者与用户可以轻易地使用与搜寻	√	√	√	Δ
Microsoft Metadirectory Services (MMS) 是一个集中式服务, 存储与组织多个目录中的用户、应用程序以及网络资源等资讯, 以解决组织中资讯存储在不同记忆体所导致的问题		√	√	

(续表)

档案与打印服务				
分散式档案系统 (Distributed File System/DFS) 允许单一服务器上管理多个 DFS, 减低管理与硬盘上的成本	✓	✓	✓	✓
加密档案系统 (Encrypting File System/EFS) 提供另一层的资料防护与访问控制	✓	✓	✓	✓
阴影复制还原 (Shadow Copy Restore) 为网络目录共用提供一致的时间点版本, 用户可以访问先前共用时意外删除的资料夹, 管理者也可以查看过去时间点网络资料夹的内容	✓	✓	✓	✓
便携式与远端存储装置 (Removable and Remote Storage) 可以将较少使用的资料复制到卸除媒体中, 降低存储成本	✓	✓	✓	
传真服务可以让你通过数据机来传真, 也可以让你从应用程序来传送传真	✓	✓	✓	
Macintosh 服务让 Macintosh 用户透过 TSP/IP 或 AppleTalk 协定, 可以访问与打印 Windows 的文件资料	✓	✓	✓	
管理服务				
IntelliMirror 可以透视规则的定义, 让管理者对 Windows 2000 或 Windows XP 专业版做更多的控制	✓	✓	✓	Δ
组原则结果 (Group Policy Results) 除了可以让管理者看到组原则执行的结果外, 还可以让管理者规划、监控以及除错	✓	✓	✓	Δ
Windows Management Instrumentation (WMI) 命令列可以透过命令的方式提供一致性方法, 来访问本地与远端系统的管理功能, 让管理者可以利用命令主控台来进行大部分的管理工作	✓	✓	✓	✓
远端操作系统安装使用了组原则、远端安装服务以及前置启动执行环境, 可以快速地安装一个干净的 Windows 环境与初始设定	✓	✓	✓	✓
远端安装服务 (Remote Installation Services/RIS) 让管理者可以从网络管理电脑, 并可协助管理者建立系统映像与部署服务器	✓	✓	✓	
多媒体服务				
Windows Media Services 在网络上提供影音数位串流服务, 例如: 多重播送、无线网络支援以及 Internet 验证等	✓	✓	✓	
延展性				
Intel Itanium 电脑 64 位元支援提供很大的虚拟记忆体空间与 Paged Pool 区域, 增加了可靠度与用户、边线数量的处理		✓	✓	
Host Add Memory 允许在不重新启动电脑的情况下, 加入记忆提供操作系统与应用程序使用, 但是不支援 64 位元版本的 Windows Server 2003 操作系统		✓	✓	
Non-Uniform Memory Access (NUMA)		✓	✓	
Data Center Program 提供客户一个整合性的软件、硬件与服务			✓	

(续表)

安全性设定服务				
Internet 连线防火墙 (ICF)	√	√		√
公开密钥基础结构、凭证服务及智慧卡	√	√	√	△
终端机服务				
远端桌面管理就是远端管理模式的终端机服务, 让管理者可以在网络上进行服务器管理	√	√	√	√
终端机服务器提供一个服务让客户端用户, 可以在没有支援视窗化系统的情况下, 执行视窗化应用程序	√	√	√	
终端机服务器工作阶段 (Session) 目录让用户能够轻易地连接在负载平衡终端服务器上已断线的 Session, 而 Session 目录相容于负载平衡服务		√	√	

1-2 Windows Server 2003

Windows Server 2003 整个系列的设计目的在于提供最优良的作业环境, 这些功能最重要的作用在于降低资讯管理费用, 并实现可协助公司获得实际竞争利益的新一代商业解决方案。因为 Windows Server 2003 是整合过去 Windows 2000 上的经验与客户意见, 加强了整体系统稳定性与扩展性的提升、完整的 Internet 与应用程序服务以及提供功能强大的点对点管理, 以降低整体拥有成本 (Total Cost of Ownership/TCO)。因此 Windows Server 2003 的特点可说明如下:

- **安全性:** 由于 Internet 的发展, 使得各行各业在网络的使用变得非常普遍, 因此选择一个安全的系统网络, 以确保信息的安全性, 也比以往更为重要。Windows Server 2003 提供了整合的基础架构, 让整个安全性提高许多; Windows Server 2003 提出许多安全性方案, 不管是 Active Directory 的识别管理功能, 或是全局语言执行阶段 (Common Language Runtime/CLR), 都改善了程序设计的错误与安全性漏洞的数目。CLR 主要提供一个共通的执行阶段, 它不仅可以确保程序码的正确性与类别的安全性, 也可以验证程序的错误与否, 并针对使用权限加以检查, 是 .NET Framework 的基础, 因此可用以防止病毒及其他居心不良程序码造成的损害。Windows Server 2003 中自动注册及自动更新的功能, 提供了公共密钥基础结构 (Public Key Infrastructure/PKI) 的最佳选择, 也让我们在部署智能卡及证书时变得更容易。Windows Server 2003 针对 Kerberos 认证协议进行改善, 在分布式操作环境中, Kerberos 是目前功能最强大的安全保护协议, 使得保障 Windows Server 2003 的安全性更为容易。除此之外, 为了增加网页服务器的安全, IIS (Internet Information Services) 6.0 从设计之初就被设置为最高的安全性, 众多的新功能让您可以在网站上安全地引导业务进行。
- **易于部署、管理及使用:** Windows Server 2003 提供弹性化的工具, 让用户可以轻松地

设计、管理服务器。通过向导简化了特定服务器角色的安装设置及日常服务器的管理任务，例如：文件服务器、打印服务器、远程访问服务器以及其他的角色等，因此没有固定的系统管理员，也一样可以很容易地管理。通过新的组策略管理控制面板（Group Policy Management Console/GPMC），让系统管理员可以更容易地部署与管理用户相关设置、安全性以及漫游设置档规则等工作。管理服务也提供了命令行工具，让系统管理员可以编写程序码以及达到自动化管理功能，让系统管理员可以通过命令行的方式完成管理工作。软件更新服务（Software Update Services/SUS）有助于自动化的系统更新。在备份、还原以及系统局域网（System Area Network/SAN）管理性任务的部分，则可以利用磁盘区卷影副本服务。此外，系统管理员还有一些新改进的功能设计，让部署Active Directory更为容易。例如：大量的Active Directory复本可以从备份媒体中部署，使用可复制密码及编写指定码的Active Directory Migration Tool（ADMT），让较早期服务器操作系统（Microsoft Windows NT等）升级更容易。还有重新命名及重新定义架构能力的新功能，让系统管理员在处理可能发生的组织变动时更有弹性，使得Active Directory的维护更加容易。此外，通过远距信任模型，让系统管理员可以在拥有自治权又不牺牲整体性的情况下，连结Active Directory各树系。最后，系统管理员也可以使用远程安装服务（Remote Installation Services/RIS），让系统管理员可以从网络来管理计算机，并协助系统管理员快速地建立系统映像及部署服务器。因此，只要系统管理员能够善用这些工具，相信系统管理就能变成一件轻松的差事了。

- **可靠性、可用性、扩展性以及性能：**Windows Server 2003通过一连串新功能的提升，例如：IIS 6.0状态侦测、Active Directory安全性设置、应用程序验证、Internet防火墙以及操作系统更新管理等功能，增强了可靠性。在可用性部分，Windows Server 2003群集（Cluster）服务现在支持多达八个节点群集及分开地区节点，如果群集中的某一个节点因为错误或维护而无法使用，其他的节点就会立即提供服务，具备了兼容移植的能力。Windows Server 2003也支持网络负载平衡（Network Load Balancing/NLB），它会平衡一个群集内所有节点中进入的Internet通讯协议（IP）数据流。此外，由单一处理器系统扩展至32个处理器系统，并同时支持32位和64位处理器的能力，提供了更佳的扩展性。整体而言，Windows Server 2003的文件系统性能，比Windows 2000 Server速度增加达140%，在Active Directory、XML Web Services、终端机服务以及网络的性能上也有明显的改善。
- **降低成本：**Windows Server 2003提供许多先进的技术，有助于企业降低整体拥有成本。通过系统管理与存储方面的改良，还有自动化工作与更新程序，让用户可以自行处理的事情增多，不仅可以降低经常性的成本费用，对于系统管理员和用户的效率也会提

升许多，又能够保持可用性和安全性。例如：Windows Resource Manager让系统管理员可在服务器应用程序设置，供处理器及内存使用的资源，并通过组策略管理控制面板（GPMC），使组策略的管理更为容易，也让更多企业能够加以善用Active Directory服务，进而运用其强大的管理功能，降低整体拥有成本。在存储及备份操作部分也有很大的改良，用户可使用磁盘区卷影副本服务，抓取旧版的文件或已删除文件，以及针对网络共享进行时间点（Point-in-time）的备份，而不需专业支持人员的协助，从而大幅降低系统管理员的工作负担。此外，分布式文件系统（Distributed File System/DFS）及加密文件系统（Encrypting File System/EFS）的改良，则使文件的共享和存储更具弹性，也提供了用户无论身在何处都一致的文件访问方式。这些易于使用的完整解决方案，都能够让你在部署与管理上达到最佳化，进而降低整体拥有成本（TCO）。

- **动态内部网络与网站：**Windows Server 2003提供了整合的网站服务器与数据流媒体服务器，帮助我们轻易地建立安全的动态内/外部网络。内含在Windows Server 2003的网站服务器IIS 6.0，在安全性功能上增强许多，例如：密码编译服务、摘要验证以及访问控制器等，大幅提高整体的可靠性以及存留时间，使得业务信息能够安全地在网站上流通。此外，Microsoft Windows Media服务也提供了强大的数据流媒体服务，包括了新的Windows Media Player、Windows Media Encoder、音频/视频解码器与Windows Media软件开发套件，通过动态的属性设计以及更快更可靠的性能提升，让建立数据流媒体解决方案变得更容易。Microsoft .NET Framework巧妙地整合入Windows Server 2003操作系统中，目前支持多种语言开发，例如：Visual Basic.NET、C#等，它也提供了一个Web应用程序开发模型Microsoft ASP.NET。Microsoft ASP.NET启动了高性能的网络应用程序，程序开发人员除了不必再撰写乏味冗长的程序码，还可以用他们已熟知的程序语言及工具有效率的工作，通过ASP.NET动态的Web Forms控制器项及其他工具，开发人员可以快速地建立互动网络应用程序及服务。Windows Server 2003提供多种功能，可增进开发人员生产力及应用程序的价值，现存的应用程序亦可容易地重新封装为XML Web Services，UNIX应用程序也可容易地整合或移植。
- **XML Web Services：**Windows Server 2003提供的整合工具让我们可以轻易地连结XML Web Services、内部应用程序以及上下游组织。XML Web Services提供了建立在业界标准上可重复使用的组件，不论应用程序的建构方式如何，应用程序间可以共享资料，还可以调用其他应用程序的功能。而这样的网络服务，主要是通过企业全局描述、查询与整合（Enterprise Universal Description, Discovery, and Integration/UDDI）服务，让系统开发人员、系统管理员、用户以及合作伙伴之间，可以快速地搜寻及重复使用XML Web Services，使资料可以轻易地被采用与转换。UDDI是一种跨平台的开放架

构，主要架构于XML技术之上，通过Internet可以让组织与应用程序间快速、容易以及动态地搜寻Web Services，进而发现商机并进行商业交易。这样动态弹性的基础结构，可让组织内/外部网络使用自己内部的UDDI服务，有助于组织资源的分类配置，例如：地理位置、Quality of Service (QoS) 等，并可建立一个稳定且结构化的方式来描述与探索服务。

- **专业认证与服务：**Microsoft在全球拥有超过450,000名的认证系统工程师（Microsoft Certified Systems Engineer/MCSE）与专家（Microsoft Certified Professional, MCP），可以从中获取解决方案与专家意见。
- **软硬件支持：**我们可以很轻易地添加硬件设备或应用程序，因为Microsoft拥有750,000家协力的独立软件厂商（Independent Software Vendor/ISV）所提供的数以千计已认证过的硬件驱动程序和软件应用程序。此外，Microsoft解决方案产品（Microsoft Solutions Offerings/MSO）也协助企业组织建立有效的解决方案，以解决困难的商务挑战。

1-3 Windows Server 2003的新增功能与改善

Windows Server 2003所提供的新功能与改善，都比Windows 2000 Server有了长足的进步，下面按服务器所扮演的角色不同分别进行说明。

1-3-1 Active Directory

- **ADMT version 2.0：**Active Directory Migration Tool（ADMT）2.0可以让我们从Windows NT4.0移植密码到Windows 2000与Windows Server 2003，也可以让我们从Windows 2000将密码移植到Windows Server 2003的域（Domains）。
- **更改域名称：**更改DNS名称，或者Active Directory森林树系中存在的NetBIOS名称，管理员可以在部署完后，弹性地修改Active Directory，因此在设计决策时较具可逆性，不仅可以将其合并，也可以选择重新架构整个目录结构。
- **重新定义Schema：**Schema是存放在Active Directory中的对象类别与属性描述。Active Directory是一个具高度弹性的目录服务，允许我们对目录中的属性与类别重新定义，以达到较佳的安全性。
- **AD/AM（Active Directory in Application Mode）：**AD/AM能够对可执行目录结构的应用程序，完成部署情境剧本（Scenarios）。它并不需要在域控制器上部署，而且可以将多个独立的AD/AM实例（Instances）放在同一部服务器上同步执行。
- **改善组策略：**在Windows Server 2003中，组管理控制面板（GMPC）对于组策略的管理提供了单一的解决方式，让组策略管理更趋一致。GMPC让管理员能够以简单的拖曳式用户界面，在一个域树系中的多个域，进行组策略管理。在此版本的操作系统中，

也让管理员能够自行定制情境剧本与自动化管理备份（Backup）、导入（Import）、复制（Copy）以及回存（Restore）等组策略对象（Group Policy Objects/GPOs），让我们的组策略管理更容易，也更符合成本效益。

- **更强大的用户界面：**管理控制面板（Microsoft Management Console/MMC）赋予了拖曳（Drag-and-Drop）功能、多重对象选择、组策略以及存储查询与重复使用的能力，这些改善的界面都使得管理员在管理与整合时更有效率。管理员可以同时编辑多个用户对象、重置访问控制表（Access Control List/ACL）权限、找出有效的安全权限以及继承权限。
- **跨树系信任关系验证（Cross-Forest Authentication）：**Windows Server 2003采用了Kerberos或NRLM为验证基础的跨树系（Forests）的传递式信任关系。使用者可以透过不同等级的安全性群组，从一个树系中跨越到另一个树系，去访问其物体与资源，却只需要一组账号与密码。
- **跨树系信任关系授权（Cross-Forest Authorization）：**让管理员很轻易地从信任树系中选取用户与组，以加入本机组或访问控制表（ACL）中，这个功能主要使存在信任关系的森林树系间安全问题更具完整性。因此，在信任关系中的用户想要访问某一被防护的信息资源时，就会有安全识别（Security Identifiers/SIDs）方面的限制，以杜绝非法的入侵。
- **加强跨域验证（Cross-Certification Enhancements）：**在Windows Server 2003中，提供了两种跨域验证层次：部门层次（Department Level）与全局层次（Global Level）。
- **IAS与跨树系信任关系验证：**如果域间的信任关系是双向信任关系模式，则通过Internet验证服务/远程验证拨号用户服务（Internet Authentication Services/Remote Authentication Dial-In User Services, IAS/RADIUS）可以从一个树系验证另一个树系的账户，让管理员可以使用既有的IAS/RADIUS，轻易地整合新树系资源。
- **Credential Manager：**Credential Manager存储了验证用户身份的安全性资料，包含用户密码与X.509证书格式标准，让用户可以不用在每次执行应用程序时，都必须重新输入身份资料以进行验证。只要在第一次登录时需要输入验证资料，一旦取得授权后，则该应用程序与身份验证资料就会取得关联，以后如果再执行该程序时，就可以直接使用了。
- **软件限制策略：**为了预防我们的操作环境被入侵者通过网络环境，安装或执行不知名、非信任软件，而导致其他非预期状况发生，我们可以通过软件限制策略的初始值设置，来规定这些不知名软件是否能够执行，以及能够执行的最低安全范围。
- **更易于登录远程办公室：**如果一个分公司自己本身拥有域控制器（Domain