

Mastering Windows Server 2003 Upgrade Edition for SP1 and R2

Windows Server 2003

从入门到精通

(SP1和R2中文升级版)

[美] Mark Minasi
Rhonda Layfield 著
Lisa Justice

马树奇 金燕 译



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

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

TP316.86/120

2007

Mastering Windows Server 2003 Upgrade Edition for SP1 and R2

Windows Server 2003 从入门到精通 (SP1 和 R2 中文升级版)

Mark Minasi

[美] Rhonda Layfield 著

Lisa Justice

马树奇 金 燕 译

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书作者在《Windows Server 2003 从入门到精通》的基础上进一步介绍了微软公司新推出的 SP1 及 R2 系统的关键技术和新增功能,其中包括使用 ABE 技术隐藏文件夹、使用数据执行保护(DEP)机制防范 Windows 蠕虫程序、防止间谍软件及锁定端口、封锁 USB 闪存接口、R2 系统新增的打印管理控制台、更好的配额机制、Windows SharePoint Services 的应用、UNIX 与 Windows 的集成、ADAM 技术等。

本书适合所有使用、维护 Windows Server 2003 SP1 及 R2 系统的技术人员、开发人员、高校学生以及所有希望了解 SP1 及 R2 新技术、新功能的相关人士阅读。



Copyright © 2006 by Wiley Publishing, Inc., Indianapolis, Indiana. All rights reserved. This translation published under license. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, without the prior written permission of the publisher. The SYBEX Brand trade dress is a trademark of Wiley Publishing, Inc. in the United States and /or other countries. 本书英文版由美国 Wiley 公司出版,Wiley 公司已将中文版独家版权授予中国电子工业出版社及北京美迪亚电子信息有限公司。未经许可,不得以任何形式和手段复制或抄袭本书内容。

版权贸易合同登记号 图字:01-2007-0570

图书在版编目(CIP)数据

Windows Server 2003 从入门到精通:SP1 和 R2 中文升级版/(美)米纳斯(Minasi,M.)等著;马树奇等译. —北京:电子工业出版社,2007. 8

书名原文:Mastering Windows Server 2003 Upgrade Edition for SP1 and R2

ISBN 978-7-121-04364-2

I. W… II. ①米…②马… III. 服务器—操作系统(软件), Windows Server 2003 IV. TP316. 86

中国版本图书馆 CIP 数据核字(2007)第 065770 号

责任编辑:李 莹

印 刷:北京天竺颖华印刷厂

装 订:三河市金马印装有限公司

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编:100036

北京市海淀区翠微东里甲 2 号 邮编:100036

开 本:787×1092 1/16 印张:42. 875 字数:1090 千字

印 次:2007 年 8 月第 1 次印刷

定 价:70. 00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系及邮购电话:(010)88254888。

质量投诉请发邮件至 zlts@phei. com. cn,盗版侵权举报请发邮件至 dbqq@phei. com. cn。

服务热线:(010)88258888。

致 谢

有许多人坐下来进行写作,而且其中有些人的作品相当富有真知灼见。但是这些真知灼见并不一定都会被写入书中。“写下的内容”与“出版后被成千上万的人看见的内容”之间存在区别,就是要由一小部分人来完成其他大多数的工作,将这些内容编入一部书中。

多年来,有许多读者给我发电子邮件,说书里的字太小,或者说他们无法在工作中使用书籍所附带的 CD 盘,以及诸如此类的问题。而我的回答则只能是礼貌地向大家解释说:“我只负责写书,并不负责编辑、排版、打印、包装、装箱、运输以及销售。”借此机会,我也要感谢那些在幕后辛勤劳动、默默无闻地完成所有这些辅助工作的人们。

首先,我要由衷感谢本书的其他作者,他们是 Christa Anderson、Lisa Justice、Rhonda Layfield、Darren Mar-Elia 以及 C.A.Callahan。我自己当然可以完成本书中大多数关于 SP1 的技术内容并且概述一下 R2 版本中的基本情况,但是 R2 系统中的大部分技术则需要有关特定领域的专门知识,而我自己根本没有时间去学习这些技术。因此让其他聪明的作者来肩负这一部分重担会有效地把我解放出来,以便完成整书的编写工作。本书在前文中谈到许多杰出人物为我们提供了真知灼见的内容,指的就是他们。

此外,我要由衷感谢本书的编辑,他们是 Tom Cirtin、Sarah Groff-Palermo 以及 Jim Kelly,是他们精心地将简单的文字变成了书中生动的内容。他们高效率的工作缩短了全书出版的时间,使之能够更快地与广大读者见面。Ditto 负责全书的生产,Sarah Groff-Palermo、Sally Engelfried、Ian Golder 以及 Chris Gillespie 完成了将本书的电子文件进行排版的最终处理工作。

还要感谢 Waggenger-Edstrom 的工作人员,他们使我们与微软公司相关技术人员能够及时沟通,特别是要感谢 Rob Johnson 在其中的组织工作。微软公司与我们交流的人们都十分友善,总是能够在繁忙的工作中给我们提供帮助。

最后,感谢广大的读者。没有你们的大力支持,我也不会一直写书到现在,而本书是我的第 25 本书。是你们始终如一的信任才使这些书得以问世,使我能够一直从事这项我最钟爱的事业:写作,解释新技术。对此我的感谢之意无法用语言来表示。真心希望广大读者能够从本书中获得自己需要的内容,并且继续支持我以后的作品!

谨以本书献给亲爱的 Rhonda。许多作者都会感谢自己最心爱的人,感谢她们在作者写书期间所付出的耐心与关怀。很幸运,我也有这样一些可以信赖的人帮助我完成这本书。

——Mark

简 介

欢迎读者阅读本书。本书的目标是为读者解释微软公司于 2003 年 4 月推出的“面向生产的(release to manufacturing, RTM)”或简称为 RTM 版的 Windows Server 2003, 与最近新推出的两个新版本 Windows Server 2003 SP1 以及 Windows Server 2003 R2 之间的区别。关于 RTM 版 Windows Server 2003 的相关技术已经在电子工业出版社美迪亚电子信息有限公司于 2004 年出版的《Windows Server 2003 从入门到精通》一书中进行了详细介绍。最近微软公司推出的两个新版本分别是 Windows Server 2003 的 Service Pack 1 (SP1), 以及微软公司为过渡时期推出的 Server 2003 简要升级版 Windows Server 2003 R2。

本书针对的是两个十分接近, 但又不完全相同的用户群: 运行的 Windows Server 2003 系统安装了 SP1 的用户, 以及运行 Windows Server 2003 R2 版系统的用户。这两个用户群并不完全相同, 因为安装了 SP1 以及微软公司提供的其他一些下载功能的 Windows Server 2003 RTM 版系统在很大程度上与 R2 相似, 但两者只是十分“接近”, 因为 R2 版系统中还包含了许多出色的功能, 这些功能是 Windows Server 2003 加上 SP1 所不具备的。(如果有些读者说: “不对! 不是这样的! R2 比 Windows Server 2003 系统增加了许多功能!”, 那么我会很遗憾地告诉读者: 虽然 R2 中有一些功能是其独有的, 但这些功能并不是很多。同时, 这并不是说 R2 中新增的功能不出色, 只是说这些出色的功能从数量上讲并非是像微软公司的市场宣传员所讲的那么多。具体说明读者可以看下文关于“R2 的构成”一节。)

在这本书中, 我和本书的其他作者希望达到的目标与此前 13 年来的一贯做法并无二致, 这就是为读者解释这些新版本的服务器系统提供了哪些新技术, 如何安装、配置、管理这些新功能, 以及如何尽可能简明地对相关的功能进行故障诊断与排除。从本书中, 读者将会看到我们总是尽可能地阐明相关的概念、警告一些容易犯的错误, 并且一步一步地指导大家通过示例掌握这些新技术的使用。

前文已经谈到, 这是一本关于“升级系统”的书, 因此本书假设读者已经了解了 Windows Server 2003 RTM 版即安装 SP1 之前系统的工作方式。如果读者现在对 2003 版系统还不十分熟悉, 虽然也会从本书中找到有价值的内容, 但我们还是强烈建议读者找一本以前出版的《Windows Server 2003 从入门到精通》, 以它作为阅读本书时的参考。(实事求是地讲, 我并不是在推销自己的书, 而是不愿意看到读者在阅读本书时由于出现对前版书的许多引用而感到郁闷。)

换句话说, 本书既可以供以往的 Server 2003 系统管理员用于发现 SP1 带来的重大变化, 也有助于一些对 2003 系统比较挑剔的系统管理员在升级到 R2 系统时发现新系统提供的新技术。至于对 Windows 连网技术仍然十分陌生的人, 本书仍然是有用的, 当然在这种情况下希望读者能够再找一本以前出版过的《Windows Server 2003 从入门到精通》, 以便于参考了解 2003 版系统的连网技术。

那么我为什么要专门写一本关于升级系统的书, 而不是简单地把原来那本书拿过来修改一下, 使之覆盖 SP1 和 R2 系统的内容呢? 原因如下: 首先, 每次我修订以往的书时, 都会收到

一些读者的电子邮件,询问“是否有一些只讲新版技术的书,这样可以省去读者从新版书中自己寻找新内容的麻烦”,因此这一次我想试一试专门写一本关于新增技术和功能的书。(本书的内容基本上都是新内容,只有关于“终端服务”的一章例外。这是因为 SP1 引入的技术改变所致。读者会看到其他各章的内容都是全新的。)其次,许多读者希望购买篇幅短小一些的书,因为上一版的《Windows Server 2003 从入门到精通》实在是个大部头,其内容超过了 1200 页。听说有些读者甚至开玩笑地说:“这本书太大了,它应该有自己的天气系统。”因此我认为,应该写一些内容简练而又实用的书。正如一些市场推广人士所说,这本书就是应读者之需而编写的,希望读者喜欢。

下面还是从最基本的内容谈起。在这篇简介中,我们将介绍以下内容:

- SP1 的特点是什么,它给 2003 系统带来了哪些改变?
- R2 版带来的系统升级并不十分突出,特别是在可以预见的将来,微软公司肯定会在下一版的服务器系统中做更大的升级,在这种情况下微软公司推出 R2 版系统的原因是什么?
- 2003 RTM 系统、SP1 以及 R2 版系统之间有什么关系?

阐明这些问题之后,本文将摘要说明在本书其余的部分将介绍哪些内容。

SP1 的目标:修复错误,增强安全性

“微软公司为什么要为 2003 版系统发布 SP1 呢?”这个问题很容易回答:就是为了修复错误。与 Windows NT 家族的其他所有操作系统版本相同,微软公司会定期发现并修复其操作系统产品中存在的错误,再将这些修复程序合成一个较大的程序包,这样可以比单独地修复每个错误做得更彻底,也就有了 Service Pack,即服务包。微软公司的 Windows Server 2003 系统是于 2003 年 4 月发布的,而 SP1 是在 2005 年发布的,可见其中包含了两年内的所有修复程序。

如果我们看一看 2003 系统的 SP1 程序包,就会发现它是有史以来规模最大的服务包,其容量超过了 329MB。此前人们会认为 XP 系统的 SP2 就够大了,其容量为 267MB。由于 SP1 中包含了大量的 .CAB 文件,即“文件组”文件,是不是微软公司应该考虑在使用 .CAB 文件的方面来个“营养不良的 CAB 文件”瘦身运动了?不会的(抱歉,开个玩笑而已),实际上 XP 系统的 SP2 和 2003 系统的 SP1 之所以如此巨大,均出自同样的原因:为了提高安全性。这也是微软公司为 2003 版系统推出 SP1 的主要原因,出于安全性方面的需要。

我知道读者现在对于安全性这个话题已经感到有些厌烦了。只要有计算机网络,就存在安全性问题。在 2001 年刚刚出现 Code Red 和 Nimda 蠕虫病毒的时候,这个问题就已经显得十分重要,使微软公司总裁比尔·盖茨在 2002 年初下令停止了微软公司所有人员新开展的编程工作,没错,就是停止了所有的新编程工作,以便这些人能够参加培训,编写出更安全、更好的代码。在 2002 年的 2 月和 3 月,Redmond 没有推出任何新的代码。微软公司也将 Windows Server 2003 系统的发布日期由原定的 2002 年初推迟到了 2003 年的第二季度,以便对新版服务器操作系统的代码进行精细的检查。盖茨的这个安全举动也使微软公司几乎停止了对 XP 系统的所有修复工作,直到完成安全培训之后,这就是最终的 XP SP2。也正是这次行动再次促成了新的 Windows Vista 开发项目,它将于 2006 年底或者 2007 年初代替 XP 系统。Vista 之前的所有开发工作都被中止,然后重新开始。他们肯定是希望此后开发的所有新代码

都应具有尽可能高的安全性。

当然,希望总归是希望。Windows 系统中的漏洞仍然是一而再、再而三地被发现,并且不断出现令人害怕的蠕虫程序和特洛伊木马(Trojans)程序。2003 年,人们发现在 SQL Server 2000 中存在一个漏洞,由它产生的一种蠕虫程序在 1 月的一些天中使整个因特网的速度下降;同年 8 月,人们又发现 XP 系统中存在一种可以导致“冲击波”(Blaster)蠕虫病毒的漏洞。“冲击波”蠕虫病毒使微软公司十分难堪,其工作人员又回到 Windows 代码中从头到脚地进行检查。在 XP 系统的 SP2 又一次被推迟发布的日子里,微软公司已经认识到,在 XP 系统通过 SP2 所做的任何重大变化,他们认为这种变化肯定会有,都会通过服务包安装到 Server 2003 和 Windows 2000 Server 中。

在 2004 年 8 月,微软公司终于发布了 XP 系统的 SP2 服务包。在这个服务包中所做的改变之一称为“数据执行保护”,相关内容将在第 3 章中介绍,该技术要求微软公司几乎对 XP 系统中的每一段软件都进行重新编译,这也就意味着 XP2 几乎是 XP 系统的一个全新版本,这也是造成 SP2 服务包如此巨大的原因。XP SP2 中不仅包含了对已知错误的修复以及安全补丁,还包含了许多十分有用的新程序,它们多数都与系统安全有关。此外,在读者阅读第 5 章的过程中将会看到,SP2 改变了 Windows 系统此前使用的一些最基本的通信系统,以提高它们的安全性,并考虑新系统的兼容性问题。微软公司也需要将这些改变应用到服务器系统中,这就是说他们也将 SP1 中重新编译 Server 2003 的几乎全部程序段。所以在 2005 年推出的 SP1 中就出现了大容量的服务包需要下载。与此同时,微软公司决定不再为 2000 系统提供 SP5 以便实施这些修改。这当然不是什么光彩的事,但也并没有出乎人们的意料。与大多数软件供应商相似,微软公司并不喜欢“销售”软件,他们更喜欢一种类似啤酒杯的销售模式——不是销售,而是出租。(并不是只有微软公司才这么做;看一看 Red Hat 公司销售 Linux 的做法,大家就会惊讶地发现,至少从其网站公布的价格上看,Red Hat 公司已经使 Windows XP 成为了一种廉价的桌面操作系统替代产品。)

但是微软公司在 XP SP2 以及 2003 SP1 中并没有停止修复错误并做一些结构性调整工作。他们还增加了几十种新功能,这些功能基本上都与安全性有关,不过读者肯定会发现这些功能都十分有用。遗憾的是,这些功能几乎有一半以上都没有文档说明,因此许多系统管理员并不知道他们已经骄傲地拥有了这些出色的新工具。这也正是编写本书的另一个重要原因——给读者带来好消息。虽然本书并不想介绍 XP SP2,但人们也不可避免地会用到 XP SP2 系统,因为 2003 SP1 中的大多数新功能在 XP SP2 中也有。

2003 SP1 和 XP SP2 很像是一大批补丁程序的集合。它们对于各自操作系统的升级均具有十分重要的意义,值得每一位系统管理员关注。读者不但应该了解它们怎样提供这些新技术和新功能,还应该注意这些功能可能会出现兼容性问题。

R2 版系统的出发点:时间表和 SA

大多数人很容易理解 SP1 中的内容,因为所有的服务包基本上都是一大批补丁程序加上少数一些附加程序。SP1 的特别之处仅仅是个头比较大,附加的新程序比较多而已。那么 Windows Server 2003 R2 又是怎么回事呢?

曾经有一段时间,大约是 1993 年 8 月到 1996 年 7 月,微软公司习惯于每年推出一个新版的 NT Server 系统。NT 3.1 Server 发布于 1993 年,3.5 Server 发布于 1994 年,3.51 Server

发布于 1995 年,而 NT 4.0 发布于 1996 年。有些系统的升级幅度很小,但它们都会带来新技术并在原来的系统上进行提高。但此后微软公司开始致力于开发 NT 5.0。该系统的开发周期比人们预计的更长,一直到 2000 年,读者可能还记得,该系统于 2000 年 2 月推出,命名为 Windows 2000。微软公司曾经希望能够快速推出一种名为 1.1 版的 2000 Server 后续版本,但是如前文所述,2000 年左右的一大堆安全性问题减慢了开发的进度,最终使 1.1 版变成了 Server 2003。所有熟悉 2000 Server 的老系统管理员都知道,Server 2003 实际上就是 2000 Server 的 1.1 版本,而且受到了广泛的欢迎。在 2003 系统中并没有强调为什么要从 2000 系统升级到 2003,而是新系统所花的这 38 个月的努力使许多客户发现,微软公司已经知道了该如何管理大型软件开发项目。

那么客户关注的是什么呢?如果了解这个问题,首先要理解微软公司的主要目标,与大多数大型公司主要关注的事物相似,这就是公司的大客户。我猜想他们的主要财政收入应该来自于与自己相似的财富 500 强企业,以及大型政府机关。他们对这些客户的意见最为重视,读者不要误解我的意思,这并不是说这些公司不关心其他的客户,而是说……限于篇幅,对这些问题我们就不再展开讨论了……

这些大客户都喜欢做财务预算,当然这里包括长期的预算。他们并不希望在 2008 年 5 月发现 2008 年 9 月所有的电子公司都改用直流电源,因此所有的人都必须同时把基于交流电的电子设备扔掉,转而购买直流设备。当然,任何规模的企业机构都会关心这样的问题——那么真正的大型企业与普通企业的区别在于,这样的财政预算几乎不可能被管理者批准;在 2008 年 9 月唯一可能允许支付的资金就是在 2007 年春天申请的经费。在这种情况下工作的人们需要知道在将来怎样做是最经济的,最好是能够提前一两年。我们还回过头来讨论 2000 Server 和 Server 2003。从 1997 年到 2000 年,大量依赖 Windows 软件的机构会询问微软公司:“什么时候会推出新的台式机软件?什么时候推出那种新版服务器系统?”而微软公司对此并不清楚。这样就使客户很头痛,因此微软公司开始努力炮制一个正常发布软件的时间表。

注意:现在我已经出版了许多本书,还在许多杂志、专栏、简报等诸如此类的媒体上发表了文章来介绍微软公司及其产品,当他们的产品出现问题的时候,我也总是毫不留情地予以批评。但当谈到“请准确地告诉我某产品何时可以上市,而且要提前一年半”这个问题的时候,我则会和 Redmond 及其工作人员站在一个立场上。软件开发工作也是一种研究,而且是纯智力工作。对这样的工作人员,人们很难制定一个时间表。从个人角度讲,我更希望他们能够将所有版本的 Windows 产品推迟一些日子发布,只要他们的产品中沒有缺陷就好,也不愿意他们能够准时发布带有缺陷的产品。

微软公司曾经为了“定期”发布软件而做过一些努力,但他们发现每年都推出一个新版的服务器操作系统是无法实现的,而这恰恰是一件好事。NT 系统在 1998 年以前都很少用于大型网络系统,因此当时人们也很少会注意到微软公司每过一年左右的时间都推出了一个新版的 NT 系统。

在最近的十年中,情况与以往正相反,基于微软产品的网络更多地成为了网络环境的主角,并且大多数企业并不希望每过 12 个月都对他们的软件基础系统进行大幅度的调整,不论新版系统的图形用户界面(GUI)做得多么酷。微软公司的大客户似乎是在表明:“不错,我们需要软件方面的革新,但不要那么频繁。”

其次,每年都推出一个新的服务器操作系统版本或者台式机 Windows 操作系统版本,从技术上讲是否有意义也并不确定。为什么呢?读者可能是看到了一些说教,谈到应保证将房门紧闭,没有人从自己的背后偷看。继续看下去,我会在这里等着你……看完了吗?好,我来告诉你关于安全方面的技术秘密:计算机技术发展的速度已经大幅度减慢了。

读者不这么认为吗?我们静下心来想一想。我在 2006 年初发表这种说法的时候,有许多人仍然在运行 Windows NT 4.0 域控制器,因为他们还没有开始采用 Active Directory(活动目录)。Windows NT 4.0 是 1996 年发布的,是十年以前。另外,读者是不是还听说有人仍然在使用 Windows 95! 这就像是在 2000 年,还有人在运行 Windows 3.1 一样,以及在 1992 年有人运行 MS-DOS 3.3。即使在那些时候,这些古老的系统都已经很难找到了。虽然我个人并不希望仍然生活在 Windows 95 的环境中,但可以理解为什么仍然有人在使用它——因为它能够完成一定的工作。他们可以上网,收发电子邮件、玩许多游戏。即使是在过去,有一些事情也是不可能的:在 2000 年会有一些人仍然运行 Windows 3.1,但他们会发现市场上几乎已经没有什么程序可以运行在 3.1 系统上了。但计算技术在近几年中发展的趋势已经平缓,因为硬件厂商在至少两个方面已经发展到了接近极限的程度。第一,Intel 公司已经表明不大可能生产出主频超过 3.8GHz 的 Pentium 芯片;第二,硬盘厂商也宣称在数据记录密度方面走到了尽头。

当硬件发展受阻的时候,对软件肯定会造成不少影响。因为软件领域的变化几乎总是由硬件的变化来推动的。当人们努力寻找能够管理超过 32MB 的硬盘的 DOS 系统时,微软公司及时推出了 DOS 5。一段时间以后,人们开始不再记忆命令行,转而使用更整洁也更具潜力的图形界面时,微软公司通过 Windows 3.x 又大赚了一笔。再往后,人们开始喜欢联网,因此人们开始购买 Windows 95,因为它内建了对因特网软件的支持。由于对 USB 接口的支持,有许多人购买了 Windows 98,当然数量要少一些。随着新开发硬件数量的减少,人们对于“必需”的新型软件需求也开始下降。

请读者不要误解我的意思,我并不是说在计算领域已经没有什么新的事情可做了:我仍然向往着能够把一条火电线缆插到自己的耳朵里,以便于把头脑中所想的事情备份下来,或者在短短数秒钟内就学会新知识。在计算领域里总会有一些创新,但创新的速度会减慢。(读者可以考虑另一个类似的例子,这就是技术对汽车的改变。在上世纪的 50 年代,当装备了空调、各种自动设备、长寿命轮胎的现代汽车第一次出现的时候,人们都热衷于谈论汽车将会怎样继续革新下去,从而人们听说了会飞的汽车、由计算机管理并自动驾驶汽车的高速公路等。这些发明可能有朝一日会出现,也可能不会。在汽车领域里仍然不断地有创新,但不像上世纪的 20 年代到 50 年代来得那么快。)

不管怎样,许多大客户都希望能够事先了解关于新版系统的情况,他们不希望每年都进行系统升级,同时硬件技术发展速度的减慢也使微软公司开始考虑每四年作为一个周期对操作系统进行改进。Windows Server 2003 正如其名称所示,于 2003 年同期推出(读者也不要指望我会在其他书里面也使用“同期”这个词),因此下一版应该于 2007 年或者 2008 年发布,可能会命名为 Windows Server 2007 或者 2008。(在本书中将这两个可能出现的后续版本称为 Windows Server 2007/8,因为我的水晶球可能不那么灵验了。)

但就微软公司而言,四年是一个不短的时间。我的意思是,在这段时间里他们可以推出一些重大的改进,并且他们可能并不想再等两到三年才向市场推出这些重大的改进技术。更重要的是,还有一些使用软件保险(Software Assurance, SA)的客户。

软件保险又称为许可证 6.0,是微软公司最新推出的一种软件收费方式。在过去,人们购买一台计算机后需要为机器中安装的操作系统付费。(现在人们仍然这样做。)如果微软公司于一、两年后又推出了一种新版本的操作系统,那么他们就会推销两种版本的产品。第一个版本是基础版,就像我们在新买的机器中安装的一样,并且其价格不菲。第二个版本实际上基本与上一版本相同,也是一张 CD、一本手册和一个包装盒,但价格便宜一些,这就是“升级版”。只有当用户的机器中拥有老版本系统的时候,才能够安装这个新版本。

在 2001 年,微软公司引入了一种新的收费方式,这就是软件保险(SA)。在使用 SA 方式的时候,微软公司不再提供升级版,而是为刚刚购买了其操作系统产品的客户提供一种“升级保险”,其意思是:向微软公司支付大约刚刚购买的操作系统产品价格的三分之二,只要新版的操作系统在三年内推出,就可以“免费”升级到微软公司的下一个操作系统……(“三年”这种说法可能会有所变化,但这也是一种标准说法。)这样一来,微软公司就不再决定“每四年推出一种操作系统”,而是改成了“提供一种三年升级保险”的做法。就这样,微软公司已经针对购买 XP 和 2003 系统的客户销售了不少 SA 许可证。

只要将“三年 SA 许可证”与“四年软件升级周期”对比一下,就可以得出一个让不少客户讨厌的结论。2003 年购买了一个 2003 标准版的产品如果说花费了 1000 美元,又向微软公司支付了 600 或者 700 美元作为以后三年新推出服务器操作系统的升级权,此后却发现他们于 2007 年推出了另一种新版本的服务器操作系统。

现在 R2 版本存在的第二个原因就比较明显了。它使微软公司有机会修正 2003 系统中存在的重大错误,而不必等到推出下一个服务器操作系统版本,如前文所述,同时还为购买了 SA 的客户提供了应得的产品。从某种意义上讲,这个对 Server 2003 进行了小幅度修正的系统应该命名为 Server 2003 SA,而不是 Server 2003 R2。微软公司还决定不再销售原来的 Server 2003 产品了;如果客户现在要购买服务器操作系统,那么买到的就是 Windows Server 2003 R2。

R2 版本综述:未来、许可证、技术支持和 Active Directory 方面的改变

如前文所述,Windows Server 2003 R2 将不会是唯一的 R2 版本,至少根据微软公司的计划如此。这个 R2 的称呼在未来的服务器版本中将继续使用。例如,假设微软公司于 2007 年或者 2008 年推出下一个服务器操作系统的主版本,命名为 Windows Server 2007/8,那么再下一个主版本服务器操作系统将会是 2011 年,而在 2009 年,我们看到的将是 Windows Server 2007/8 R2 版。

现在购买软件的人都会想:“如果购买了这个产品,会得到怎样的服务呢?”微软公司提供了广泛的服务……但这些服务并不是永久存在的。我们已经看到,微软公司已经排出了定期推出新版本软件的时间表以及进行软件技术支持的时间表。例如,Server 2003 系统的“主流技术支持”(微软公司网站上的称呼)将持续到 2008 年 6 月 30 日,参见网址 <http://support.microsoft.com/lifecycle/?LN=en-us&p1=3198&x=14&y=9>。因此,人们可能认为这暗示着他们对 R2 的支持会在此后增加两年,但实际上并不是这样。当微软公司不再提供对原始 RTM 版 Server 2003 的支持的时候,对 2003 R2 版的技术支持也将于 2008 年中期停止。

那么升级到 R2 版的费用如何呢?首先,如果客户没有购买软件保险(SA),那么就需要购

买一个全新的 Windows Server 2003 R2 版本。与 Server 2003 相同, R2 也有四个不同的版本: Web 版、标准版、企业版和数据中心版。标准版及企业版 R2 系统的价格与 2003 的标准版及企业版相同, 标价分别是 1000 美元和 4000 美元。不过所有购买过基于 Windows 服务器网络系统的人都知道, 最大的一笔支出在于“客户访问许可证”, 简称 CAL, 这是一种每个用户都必须支付的累积费用。是不是还需要购买新的 CAL? 如果已经有了 2003 系统的 CAL, 那么就不需要再为 R2 CAL 支出任何费用了, 因为这两种类型的 CAL 是完全相同的, 参见网址 <http://www.microsoft.com/windowsserver2003/howtobuy/licensing/pricicfaq.mspx#EVF>。因此在网络中增加 Windows Server 2003 R2 系统不需要新的 CAL, 真是好消息!

R2 带来的另一部分费用在于改变 Active Directory。读者可能还记得, 如果自己在基于 2000 系统的 Active Directory(AD)中添加一个基于 2003 系统的域控制器, 必须先使用 adprep 命令修改该树林的架构(schema), 否则无法添加基于 2003 的域控制器(DC), 如《Windows Server 2003 从入门到精通》一书第 8 章所述。与此类似, 如果不提升现有的 Active Directory 架构, 即 Active Directory 的结构, 那么也无法在其中增加基于 2003 R2 的域控制器。就像要在基于 2000 系统的 Active Directory 中添加基于 2003 系统的域控制器一样, 人们也必须先从命令行使用/forestprep 选项运行 adprep 命令。(R2 系统的 adprep 命令位于第二张安装 CD 盘上, 位于其\cmpnents\r2\adprep 文件夹下。R2 系统发布了两张 CD 盘。)添加简单的 R2 成员服务器不需要更改架构。

注意:在以后关于 R2 的章节中, 读者将会看到 R2 提供的两张安装 CD 盘带来了一些有趣的现象。我在安装第一个 R2 服务器时并没有使用第二张 CD 盘, 这样也可以使用 DCPROMO 命令将新的 R2 服务器提升, 并且将它用做域控制器, 没有遇到任何问题。但是当我发现自己忘了运行第二张 CD 盘上的 setup 程序时, 再将第二张盘插入运行, 这张盘则报告说必须先升级架构才能继续安装。

总而言之, 添加 R2 服务器并不需要新的 CAL(好消息), 但如果想添加一个基于 R2 系统的域控制器或者使用 R2 的一些新功能, 那么就必须修改 Active Directory 的架构(这样会给 IT 部门带来麻烦, 因为人们对于修改 Active Directory 架构总是感到比较棘手)。

谁应该升级到 R2

读者不要把前面这些内容看成是对 R2 的挑剔。实际上, 如果读者喜欢 Server 2003, 那么也会喜欢 R2。下列四类情况适合升级到 R2:

- 如果目前正在运行 Windows 2000 Server, 而且想升级, 特别是微软公司正在逐渐撤销对 2000 系统的技术支持, 那么 2003 RTM 应该是不错的升级选择。由于微软公司不再销售 2003 RTM 了, 即这个版本买不到了, 因此只能用同样的价格购买 Server 2003 R2, 它实际上就是 2003 RTM, 并且还包含了更多的内容。可见, 对于较晚加入 Server 2003 行列的用户, 这一段时间的等候也是有收获的, 当然新升级的系统受到的技术支持时间也相应的短一些。
- 对于刚刚接触 Windows 连网技术的人们, 第一个可供选择的服务器操作系统就是 R2, 这同样是因为目前微软公司只销售这个版本。欢迎加入 R2 系统的行列!
- R2 系统确实包含了 Server 2003 所缺乏的一些功能, 尽管数量并不很多。微软公司开

发的这些新功能至少有一个是针对大型客户的,这就是 Active Directory 联合身份验证服务(Active Directory Federation Service),一些大型机构的工作人员告诉我说,他们很快地适应了 R2,就是因为有了这些新功能。

- 如果用户购买了软件保险,那么随之而来的就会得到 R2,不会再有其他费用。如果觉得该系统确实提供了一些有用的功能,那么可以考虑升级,因为后续的升级软件没有其他费用,而且也不需要购买新的 CAL。

哪些用户不应该升级到 R2 呢?如果目前系统中运行的是 Server 2003 的 RTM 版,又添加了 SP1,而且没有看到 R2 的一些专用功能有什么充分的理由使自己再支付大笔费用购买新的服务器许可证,那么可以仍然使用 2003 系统。

需要注意的是,在 2003 系统中虽然没有提供太多的新功能吸引用户现在就升级,但微软公司也会在不久的将来想办法让人们改变这种看法,因为他们会不断地推动人们向 R2 系统转移。在编写本书的时候,我可以想到的有两种推动力。

首先,他们已经改变了 R2 企业版的软件许可证机制,允许人们将一份软件许可证用于最多四台不同的虚拟机上。尽管标准版系统的价格是企业版的四分之一,再加上 R2 标准版许可证不允许创建四台虚拟机,那么 R2 企业版的这种四比一的优势没有什么价值。但对于需要使用企业版又需要使用虚拟机的用户,那么这个改进还是很具有吸引力的。

其次,微软公司发布了一种免费的下载软件,称为身份集成功能包(Identity Integration Feature Pack, IIFP),不久它又会更名为诸如“Windows 元目录服务”之类的名称。IIFP 是一种工具,可以极大地简化拥有多个彼此独立的树林结构网络的管理工作。该工具价格也同样值得期待……但它只能运行在 R2 的企业版。

R2 的构成:R2 中都包含了什么

前面已经谈到,R2 与 2003 加 SP1 是不同的,但并没有解释区别在哪里,而且奇怪的是,试图找出 RTM 版本加上 SP1 与 R2 版之间的区别也并不很简单。至少,一开始的时候我从微软公司的市场宣传材料中也没有发现两者的区别。现在我已经用过了 2003 RTM 版、2003 SP1 以及 R2,因此可以向读者解释 R2 版本的构成。

R2=新增 SP1 功能+可供下载的程序+“仅适用于 R2”的功能

“新增 SP1 功能”指的是当我们把 SP1 安装在 2003 的 RTM 版本中时所获得的功能,就像“Windows 防火墙功能”或者“安全配置向导”这些功能一样。这都是一些相当不错的功能……但如果不购买 R2 版,那么也无法获得这些新功能。在“新增 SP1 功能”这个类别中,我总结了以下各项(别担心,后面会解释这些功能):

- 基于访问权限的列举
- 数据执行保护
- IP 栈的改进
- 更安全的程序到程序通信
- 逐用户的审核
- ActiveX 和浏览器扩展对象的白名单/黑名单组策略
- Windows 防火墙
- 强制 USB 设备为只读

- 终端服务器升级
- 安全配置向导

这些功能虽然可以被称做是 R2 功能,但在任何安装了 SP1 的 2003 RTM 系统中都有。(从安全的角度讲,希望使用 2003 系统的人们都安装了 SP1。)

“可供下载的程序”指的是微软公司在 2003 RTM 系统发布之后又发布了可以自由下载的应用程序。例如,微软公司在 2003 年 3 月发布了“Windows SharePoint Services”供自由下载。(如果读者想知道 Windows SharePoint Services 功能起什么作用,可以参见本书中的相关章节。)根据微软公司网站所述,该功能只能安装在 Server 2003 或者 R2 系统中,这也使 Windows SharePoint Services 成为一个促进人们升级的“免费”程序包。一些人可能会说:“看见了吧? 还不想升级吗? 如果升级了就可以使用共享点功能了!”在“可供下载的程序”类别中包含以下内容:

- 组策略管理控制台
- Windows SharePoint Services 服务
- NFS 服务器支持
- NIS 服务器支持
- UNIX/Active Directory 密码同步
- Active Directory 应用程序模式(ADAM)
- 微软管理控制台 3.0
- .NET 编程框架 2.0(.NET Programming Framework)

上述这些软件有些相当复杂,它们都是可以自由下载的,能够在 2003 RTM 服务器系统上良好地运行,不论是否安装了 SP1 都可以,有些还可以在 2000 Server 甚至 XP 系统上运行。R2 系统的主要区别在于现在已经将这些程序打包在一起,随着 R2 系统的两张安装 CD 一并提供给客户。(可能有些人会问,我只能说出于某些原因,微软公司并没有提供单 DVD 的版本。)由于这些软件是通过 CD 盘发布的,因此人们不再需要下载这些软件了。这样也给人们带来了一些方便,虽然是小小不言的。

最后,我们来看“仅适用于 R2 的功能”,特别是一些由下一代主要操作系统产品借来的功能。只有这些功能可以被称为是只有拥有 R2 许可证的人才能使用的。它们包括:

- 打印管理控制台
- 文件夹屏蔽和配额
- 存储报表管理器
- DFS 命名空间和 DFS-R 替换
- Active Directory 联合身份验证服务(ADFS)
- 硬件 IPMI 管理器
- 存储区网络管理器(SAN)
- 通用日志文件系统

在本书中,我们将介绍所有通过 SP1 提供的功能、可供下载的软件功能以及 R2 新增的功能。这里的介绍可能并非百分之百地覆盖,是因为我们重点讨论对系统管理员有价值的功能。这样一来,本书就不重点介绍一些程序员喜欢的功能如 .NET 2.0 和通用日志文件系统,以及 SAN 或 IPMI,因为后者更多地针对硬件。我认为除此以外的大多数下载程序都易于学习而且有用,即使它们只是让人们为 Server 2007/8 做进一步的准备。

其他作者

在本书 20 余章的内容中,有 11 章不是由我编写的。其余这些章由一些朋友编写,都是此前合作过的同事。下面请允许我介绍这些合作作者。

Christa Anderson 和我在 1994 年编写第一本《……从入门到精通》的时候就已经合作了。最近她又做了大量的其他工作,其中包括临时在微软公司供职,这对于她编写“终端服务器”相关的内容也有很大的帮助。她曾经发表过大量的文章,也曾经为专栏供稿并出版著作。Christa 负责编写第 10 章,解释 SP1 对终端服务有哪些改进,还在第 14 章介绍了 R2 全新引入的打印管理控制台功能(这可能也是 R2 新功能中最出色的一个)。

Lisa Justice 和我在 1996 年曾经合作,当时我们俩一同举办了研讨会。她曾经编写了大量关于 Windows 用户支持技术的文章。她编写的关于用户支持工具的文章很多是针对用户配置文件的,该技术实际上比人们对它的最初设想要复杂得多,而 Lisa 则能够将它们深入浅出地说明白,并且写入了关于 NT 4 服务器操作系统的书中。从 1998 年开始,她曾经从事的工作包括 NT/Windows 技师、SQL 示范、Solaris 系统管理员、Active Directory(AD)设计师等,因此她在本书中编写了第 19~21 章,是介绍 UNIX/Windows 集成工具的不二人选。

Darren Mar-Elia 的工作经历包括 Charles Schwab 的 NT 技术员,现在又是 Quest 的首席技术员(CTO),在此期间他也曾经为微软公司的 Windows 资源工具箱(Windows Resource Kit)写书,还出版了其他几本关于组策略的书,也曾经参加编写我的《Windows 2000 Server 从入门到精通》一书。在此期间,他还曾经休息了一段时间,在一家葡萄酒厂工作了几个月!当我们需要对企业一级的事务提出深入见解并详细解释其运作情况的时候,他当然是理想的人选。因此我邀请他在第 22 章和第 23 章为读者介绍 ADAM 和 ADFS。

C. A. Callahan 和我是在四年前的一次 Windows 研讨会上认识的,她也是一位快要绝迹的 IT 自由职业者。她曾经作过教师、顾问、演讲者以及她自己认为有趣的其他许多角色。她在《Windows Server 2003 从入门到精通》中编写了三章,深受好评。在这本书中她只编写了一章,但也是非常重要的一章,这就是第 18 章关于 Windows 共享点服务的内容。

最后一位,但不是最终的一位,就是 Rhonda Layfield,她在 19 世纪 80 年代初期就已经开始接触计算机技术,当时还在海军服役。这段军旅生涯使她在七年以后仍然选择了从事 IT 顾问和教学的工作,其中包括作为微软公司在网络技术方面的产品支持技术员。她不但知道许多技术功能如何使用,还知道该如何解释这些技术。Rhonda 也是目前为数不多的可以解释 2000 Server 和 Server 2003 系统中的文件复制服务(FRS)的专家之一,因此她非常适合编写第 17 章中关于 R2 系统的新型文件复制服务,即 DFS-R 的内容。她还编写了其他关于存储技术的内容,如在第 15 章中介绍的各种关于存储系统的新增工具以及存储管理报表,还有第 16 章中关于文件夹屏蔽及配额的内容。

本书内容的编排

下面简要介绍一下本书中的内容安排。第 1 章将介绍如何获取及安装 SP1,针对的是一些尚未下载及安装的用户。偶尔如果用户需要卸除 SP1,尽管这种情况很少出现,本章也将介

绍卸载的方法。

第2章介绍的是所谓的基于访问权限的列举技术(Access-Based Enumeration),简称为ABE。读者是否曾经希望能够创建一个文件共享,并且防止未经授权的人看到该共享中的文件?这是一种很方便的办法,可以防止一些不该进入特定位置的人进入指定的位置,而且也是一种好办法,用它简化用户能够看到的指定共享中的内容。除此以外,任何使用过 Novell NetWare 网络的人都会感到奇怪,为什么 Novell 公司许多年前就已经拥有了这项技术,而微软公司却一直没有。至少微软公司在此以前一直没有提供这项功能。因此 ABE 成为 SP1 文档中没有记载的最出色的功能之一。

读者是否想过为什么 XP SP2 和 2003 SP1 容量这么大?第3章将解释数据执行保护(DEP)技术,同时将解开这个谜团。DEP 是 SP1 的一部分,它影响到了 Windows 系统中的所有程序段,也是造成 SP1 和 SP2 容量巨大的原因。它还有能力避免以后可能出现的 Windows 蠕虫程序的攻击,即使人们还没有时间应用相应的补丁程序。

TCP/IP 是因特网使用的语言,是一种用于建立大型、灵活、兼容性强的网络的重要技术,不过这种网络也易于遭受攻击。第4章将介绍 XP1 为 2003 联网软件带来了哪些改变,它们虽然不很明显,但是非常重要。读者还会看到一种出色的功能,能够在系统中发现并删除了间谍软件后恢复被间谍软件修改过的系统设置。

第5章将介绍 SP2、SP1 和 R2 的“安民告示”(我自己的称呼)。当 XP 系统的 SP2 以及 2003 系统的 SP1 刚刚发布的时候,人们曾经对它们感到一些担心,因为有人说它们会使不少应用程序停止工作,而且有人建议不要安装 XP SP2 以及 2003 SP1。实际上不必这么担心,因为只要理解了 2003 SP1 为保护系统安全所做的努力,也就懂得了该如何解决可能出现的任何兼容性问题。

SP1 未记入文档的基本功能之一是“逐用户”审核技术。这项功能采用了一项古老而且并不总是很有用的 NT 技术,这就是安全审核,并且显著增强了它的功能。第6章会为读者介绍逐用户审核技术怎样能够帮助人们精细调整网络的监管。

遗憾的是,关于网络安全保护的工作不是一成不变的。正当人们几乎可以掌握病毒程序造成的威胁的时候,又出现了间谍软件(spyware)。间谍软件传播的方式与病毒程序相似,但造成的危害更令人担忧。病毒程序只想快速地传播,同时给人们造成讨厌的负担或者破坏人们的数据,但间谍软件则是想静静地潜伏下来,表现出一副无辜的样子,同时暗中窃取人们的数据或者身份。坏人在他人系统中安装间谍软件的方法有两种,分别是通过 ActiveX 控件和浏览器扩展对象(Browser Helper Objects, BHO)。在 SP1 中包含了许多新增的组策略设置,可供人们有效地封锁这些 ActiveX 及 BHO。第7章将介绍如何使用这些组策略设置。

第8章介绍的是 SP2 和 SP1 最复杂的一部分功能,这就是 Windows 防火墙。这一章详细地分析了 Windows 防火墙,同时又介绍了另一种文档中没有记载的 SP1 功能——IPsec 旁路。读者只需要快速阅读有关的内容,就可以掌握使用这种工具节省支出的办法。

在现代生活中,流窜的窃贼只要能够真正进入安装了用户计算机的房间,那么窃取其中的数据简直就是太容易了。他可以在用户的计算机中插入一个 USB 驱动器,甚至使用一个普通的 MP3 播放器,就把想要的数据复制出来并带走。除非是安装了 2003 SP1,否则无法改变这种状况。第9章将介绍 SP1 的另一个文档中没有记载的重要功能,这就是将插入 2003 系统任何 USB 端口中的设备限制为只读。也就是说,攻击者可以把文件从 USB 驱动器中复制到 PC

机中,但是无法将 PC 机中的信息复制出来。

在 2003 SP1 中,终端服务也悄悄地进行了重要的改变。Christa Anderson 将在第 10 章为读者做此方面的介绍。第 10 章中的内容是对原来《Windows Server 2003 从入门到精通》关于终端服务的内容加以修改而形成的。(本书中的其他所有章节都是全新的内容,但由于终端服务方面发生的变化十分重要,因此我们决定加入这部分经过修订的内容作为一章。)其中之一,SP1 的终端服务有助于克服终端服务存在问题的一个最重要的方面:打印机。安装了 SP1 之后,人们就可以进行“打印机驱动程序的故障恢复”。SP1 还让终端服务可以使用安全套接层(Secure Sockets Layer,SSL)来加密终端服务器会话,具体内容请看正文。读者还会看到如何使用新的组策略设置来简化集中进行终端服务器控制的工作……其中包括如何解决此前所有 Windows 服务器上最普遍的一个技术支持问题:许可模式不匹配。

系统的“强硬措施”,即禁用某些服务、阻挡特定的端口、要求在指定通信中使用数字签名等,曾经是十分极端的情况下才使用的一些技术,而现在则成了每位网络系统管理员的日常工作。微软公司在 2003 SP1 及 R2 中为我们提供了名为“安全配置向导”的工具,从而使这些工作容易多了。多数向导程序都会有些令人担心,因为人们希望知道它们到底都做了哪些设置、为什么要进行这些设置以及人们该如何将其设置撤销,而不是通过向导程序呢?通过阅读第 11 章,读者将会了解相关的技术。

在第 12 章中,我们开始讨论本书的第二部分:R2 系统中有哪些新技术。R2 部分的第 1 章讨论的是如何准备并安装 R2 系统。这个过程与 2003 系统的安装过程很相似,但也有一些区别——这时就该使用微软公司提供的第二张 CD 安装盘了!

在接下来的内容中,我们将为读者介绍 R2 给一位老朋友带来的变化,这就是第 13 章。在此我们将讨论微软管理控制台(MMC)3.0 版。实际上,MMC 3.0 中引入的大多数改变都是针对程序员的,但也有一些内容会给系统管理员的工作带来一些变化。

在接着的第 14 章中,Christa 又回来为读者展示我最喜欢的 R2 新增功能:打印管理控制台(PMC)。这是个出色的新工具,可以在一个屏幕中查看所有的打印服务器以及打印共享,同时还可以方便地通过 PMC 创建的组策略对象来部署打印机。

在第 15 章中,Rhonda Layfield 开始为我们介绍存储报表管理(Storage Reports Management)。由于廉价磁盘容量不断增加,使得即使最小型企业机构也能够拥有大量的数据,以至于服务器管理员必须通过工具程序才能查清这些磁盘上都是些什么信息,哪些文件需要删除以释放磁盘空间!(毕竟,人们都知道电子邮件服务器对磁盘空间的需求永远也没有止境。)R2 提供了一种基本的磁盘使用报表工具,它也许不会在最近就从企业业务处理中淘汰 Veritas 软件,但也不失为 R2 提供的一个良好的附加程序。

接下来 Rhonda 将带领读者进入下一个 R2 新增的存储功能:文件夹屏蔽和文件夹配额。自从 Windows 系统出现以来,Windows 系统就已经拥有了配额技术,但它们只能应用于完整的磁盘卷,因此其应用也就有一定的限制。而 R2 系统则允许系统管理员为整个文件夹设置配额。R2 还允许系统管理员禁止存储具有指定扩展名的文件,这样就可以阻止具有某些扩展名的文件进入指定的文件夹,从而避免对这些类型的文件进行共享,例如扩展名为“MP3”的文件。这些功能都建立在一个新的名为“文件服务器资源管理器”的管理单元(snap-in)中,相关内容将在第 16 章介绍。

如果读者认为一些新的报表功能、文件夹屏蔽和配额功能就是 R2 版系统所提供的全部新增存储功能的话,那么看到“DFS 命名空间”的功能时肯定会感到意外。读者可能还记得,