MVP Microsoft Most Valuable Professional

文魁資訊 Kings Information Co., Ltd. http://www.kingsinfo.com.tw

顾武雄 编著
张 琦 于金龙 改编
飞思科技产品研发中心 监制

Windows Server 2008

天魔降伏

TOP 46 诀

- Active Directory 绝佳部署
- 全新终端服务活学活用
- 最新 IIS 7.0 网站管理
- Windows SharePoint Services 灵活应用
- 全面掌握 DFS 与文件服务器
- WDS 大量部署服务器与客户端 OS
- 网络访问保护（NAP）终极秘诀
- Server Core 十大绝佳管理秘诀
- iSCSI+ 高可用性群集（Cluster）构建
- Windows Server Virtualization 抢先体验

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

顾武雄 编著
张琦 于金龙 改编
飞思科技产品研发中心 监制

Windows Server 2008

天魔降伏

TOP 46 诀

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

Windows Server 2008 上市是 IT 界的一大盛事，因为它是继客户端操作系统 Windows Vista 上市以来，最令全球 IT 人士所瞩目的 Windows Server 操作系统的全面改版，Windows Server 2008 除了拥有前所未有的最高安全性设计之外，从可靠度、性能优化、系统管理到降低 IT 运营的成本，都将提供给企业绝佳的新体验。通过本书介绍的循序渐进的学习方式，您不需要再进行太多的理论探讨，而是将最关键的精华重点与实作结合为一体，协助您降伏在学习 Windows Server 2008 这条路上的一切魔障。

本书适用于系统与网络管理从业人员、新一代操作系统服务器版学习者及参加微软 MCTS 认证考试的考生。

版权贸易合同登记号 图字：01-2009-1397

图书在版编目（CIP）数据

Windows Server 2008 天魔降伏 TOP46 诀 / 顾武雄编著；张琦，于金龙改编.—北京：
电子工业出版社，2009.4
ISBN 978-7-121-08481-2

I. W… II.①顾…②张…③于… III.服务器—操作系统（软件），Windows Server 2008 IV.TP316.86

中国版本图书馆 CIP 数据核字（2009）第 033922 号

责任编辑：杨　鸽
印　　刷：北京天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
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
开　　本：787×980　1/16　印张：35.5　字数：908.8 千字
印　　次：2009 年 4 月第 1 次印刷
印　　数：4 000 册　　定价：59.00 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。

序

Windows Server 2008 上市是 IT 界的一大盛事，因为它是继客户端操作系统 Windows Vista 上市以来，最令全球 IT 人士所瞩目的 Windows Server 操作系统的全面改版，Windows Server 2008 除了拥有前所未有的最高安全性设计之外，从可靠度、性能优化、系统管理到降低 IT 营运的成本，都将提供企业绝佳的新体验。

在 Windows Server 2008 RC0 的测试版本刚刚出来的时候，笔者就已经开始筹划先出一本使用 Windows Server 2008 的技术精华手册了。为了让这本书适用于入门与进阶级的读者，因此在章节的规划上除了将 Windows Server 2008 大部分的全新特色在本书中一一列出之外，对于 Windows Server 2008 从 Active Directory 的建构快速入门到基础管理技巧也包含其中。

关于本书，简单来说就是一本快速让您成为 Windows Server 2008 使用高手的武功秘籍，全书以循序渐进的方式进行写作，没有太多深涩难懂的内容，只有让您能够快速上手成为武林至尊的绝佳章节指引。

本书是关于 Windows Server 2008 的权威著作，浓缩了笔者多年的实践经验。通过本书介绍的内容，您不需要再进行太多的理论探讨，而是将最关键的精华重点与实作结合为一体，协助您降伏在学习 Windows Server 2008 这条路上的一切魔障。

高杰信股份有限公司

Microsoft 最有价值专家（MVP）

技术顾问 顾武雄

联系方式

咨询电话：（010）88254160　88254161-67

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

反侵权盗版声明

目录

第 1 章　基础管理篇

本章摘要

本章的内容非常适合刚接触 Windows Server 平台与 Active Directory 的读者来阅读，将可以迅速地了解到关于 Windows Server 2008 的新特色，并且可以马上学习到关于域控制器的建立、用户组的管理及 Windows Server 2008 的安装与升级等，这些都是初学者不可或缺的重要课题。

1.1 Windows Server 2008 技术总览

1．Internet Information Services 7.0

Windows Server 2008 在 Web 服务部分提供了一个整合 IIS 7.0（如图 1-1 所示）、ASP .NET、Windows Communication Foundation（WCF）、Windows Workflow Foundation（WWF）、Windows SharePoint Services 3.0 的单一网站发布平台，并且提供了全新设计的管理界面，以及委派管理等各项强化的安全性设计。

图 1-1　IIS 7.0 管理主控台

全新的 IIS 网站服务器 7.0 在全面改版设计上，无论是从部署、管理、安全性设计到效能最佳化运行都有着超越以往所有版本的绝佳改良设计，以及各项新功能特色的添加，以下分类说明几项最具关键的增强特色。

- 模块化架构：这项特色是 IIS 前所未有的架构设计，因为它将整个网站服务器（IIS）

拆解成 40 项模块，让专业的 IT 人员部署时可以根据实际网站设计上的运行需求，来

挑选所需要使用到的模块，这样不仅可以减少可能的攻击面，同时也会降低系统下载并安装更新补丁的时间与效率。

- 提供更广泛的扩展 API 应用：全新的 IIS 7.0 提供了更为扩展且具弹性的架构，让程序开发人员能够有更多更快速的方式，来进行定制化网站的需求设计。在核心的 IIS 7.0 网站特色中，提供了全新的公用网站服务器的 API 子集合，让程序开发人员可以进行呼叫、扩充、取代或是添加功能到网站中，而这些 APIs 可以使用包括了 Win32 APIs 与受管理的.NET Framework APIs。同样地，研发人员也可以运用 IIS 7.0 具有扩展性的优点、事件记录功能、配置及管理工具特色集合，在自行设计的整合产品解决方案上提供给客户更多流畅的使用经验。
- 一致性可分布式配置设置模块：全新设计的丰富管理界面让系统管理人员可以更简便与更有效率地来部署与管理每一个在 IIS 7.0 服务器旗下网站的运行，其中 IIS 7.0 提供给开发人员与系统管理人员可以使用单一的 XML 格式的文档类型来存储所有 IIS 网站与 APS .NET 的一致性设置，这包括整个网站平台中受管理的程序代码设置及所编写的 APIs。新的配置系统支持分布式配置文件，让大量同样需求的网站可以快速完成相同配置的设置。
- 提供更高效率的管理模块：IIS 7.0 提供了更细微的管理界面，可以大幅简化 IT 人员日常维护管理时的复杂度，包括全新的图形管理界面、命令界面工具、全新受管理的 APIs 及 WMI（Windows Management Instrumentation），一次可以提供各项自动化任务的管理需求，所有新的管理特色都提供了 IIS 与 ASP.NET 结合，提供了一种一致性的管理机制。除此之外，也可以进行用户、角色资料及实时诊断信息的管理功能，而在委派授权管理部分，也能够赋予特定的系统用户或开发人员可以远程管理特定的网站。这样的管理机制可以减少管理人员的负担，并且可以通过 HTTP 的远程方式来穿越防火墙进行管理，适用于运行在独立或共享的托管环境中。
- 提供功能更卓越的诊断能力：IIS 7.0 提供了赋予研发人员及系统管理人员更多简易故障排除的方法，来降低网站与应用程序发生服务停止的机会，而这个方法便是由 IIS 7 所提供给系统管理员的实时诊断信息来进行的（例如，你可以知道目前正在执行中的有哪些连接请求、哪些连接请求已经费时多久、哪些网址正在被要求连接中、目前客户端的连接状态等）。此外，IIS 7.0 同样会针对连接失败的情况自动记录详细追踪的事件，而这些诊断功能同样可以进行扩展，因此系统管理人员自定义新的诊断记录也可以加入到自定义的模块中。

总结来说，全新亮相的 IIS 7.0 将可以协助你解决以下几个重点。

- 大幅简化网站的管理、部署及 Web 应用程序的开发时间。
- 借助更有效率的 Web 基础架构管理，降低管理成本。
- 通过更细微的程序配置，大幅减少攻击面及减少更新的频率。
- 部署强而有力的 Web 应用程序，并且能够快速扩展其基础架构。

- 借助快速解决失败的应用程序机制，减少停机的机会。

事实上，全新的 IIS 服务器 7.0 早在 Windows Vista 中就已经提供了此角色功能，只是在 Windows Server 2008 中提供了更多高级的控制能力，因为它毕竟是服务器端的系统，而不只是一个单纯的网站服务程序。Windows Server 2008 下的 IIS 7.0 完整架构可由 40 项安全模块组成，让管理人员在安装与管理上更加具有弹性，对于应用程序所使用不到的程序可以不安装，大幅减少可能会造成恶意人士的攻击面。

2．虚拟化技术（Virtualization）

在 Windows Server 2008 上所提供的全新虚拟技术将通过最新的 I/O 共享模型技术来全面提升虚拟机之前所没有的运行效能，提供给各企业一个动态数据中心与不间断的虚拟机应用服务。

新旧虚拟机技术的比较如表 1-1 所示。

表 1-1　新旧虚拟机器技术的比较

特　色	Virtual Server 2005 R2	Windows Server 2008 Virtualization
32 位虚拟机器支持	是	是
64 位虚拟机器支持	无	是
虚拟机器支持多个 CPU	无	是，最多配置 8 个 CPU 给虚拟机器
虚拟机器内存大小配置	每一个虚拟机器最多为 3.6GB	每一个虚拟机器最多为 32GB
在线增加内存/CPU	无	是
在线增加存储设备/网络	无	是
在线多台物理计算机间的虚拟机器迁移	无	是
可以由 System Center Virtual Machine Manager 来集中控制管理	是	是
Microsoft 丛集架构支持	是	是
Scriptable/Extensible	是	是，WMI
支持虚拟机器的最大数量	64 个	可以依照实际硬件的最大支持超过 64 个
用户界面	Web 界面	MMC 3.0 界面
直接访问离线的虚拟硬盘（VHD）	是	是

3．容错服务（Failover Clustering）

对于存储在 Windows Server 2008 上的文件、数据库及应用程序，可以借助最新的丛集容错技术与界面提供更简易维护管理的高可用性架构（配置设置、移转操作），管理员还可以以所提供的验证工具来确保丛集架构中的每一个系统程序、存储设备、网络设置是可以正常运行的。

4．Windows PowerShell

全新的命令行管理界面在 Windows Server 2008 中提供了超过 130 个的命令工具，让管理人员除了以原有的图形界面管理方式之外，还可以借助系统中各种内建命令进行各种批量管理的操作，还可以进一步将它们写成脚本（Script），来结合计划任务工具的使用进行全自动化的操作管理，并且可以在单一界面中进行跨服务器的多重批处理。此外，你还可以通过它一致化的命令语法及工具组进行各种系统的管理与故障排除工作，例如，Active Directory、网络状态的设置与排错、Terminal Server、IIS 管理等。

5．全新务器管理器界面设计（Server Manager）

哪些 Windows Server 2008 服务器要提供哪些功能在企业的网络中，在以往 Windows Server 2003 的配置管理上，IT 人员必须分别通过管理你的服务器（Manage Your Server）、设置你的服务器（Configure Your Server）及添加或卸载 Windows 程序的方式来完成，现在你只要经由服务器角色的配置或特色的配置方式，如图 1-2 所示就可以更直觉化地来管理每一台网络服务器所扮演的角色，以及确定所要安装的功能。

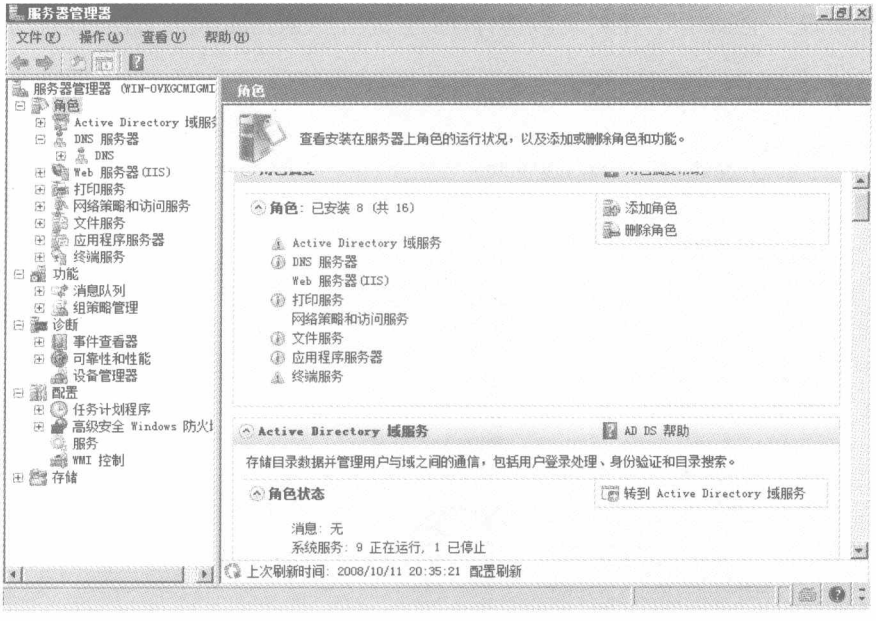

图 1-2　全新服务器角色与功能管理界面

在完成了每一台服务器角色与服务功能的配置之后，往后管理人员便可以很轻易地通过 Windows Server 2008 所提供的“服务器管理器”界面（Server Manager），来集中管理所有不同角色的服务器设置，以及实时监控每一台服务器的运行状态。它排除了以往必须自行通过远

程桌面的连接，或是通过 MMC 的界面手动将每一台服务器纳为管理对象的不便。

6. Terminal Services 的全新特色

企业选择使用 Terminal Services 的架构方式来提供客户端的应用程序使用，其效益不外乎是让客户端计算机上不需要安装相对的应用程序，管理员可以很轻易地集中控制所要开放访问的应用程序，对现有的“WAN-unfriendly”应用程序赋予远程访问的功能。当然，即使发生了远程用户的移动计算机不慎遗失，也不会导致重要数据外流，因为这些数据全部都存储在远程的 Terminal Services 主机上。

说了这么多，究竟全新的 Windows Server 2008 在 Terminal Services 的设计上提供了哪些添加及改良设计的特色在里头呢？

1） Terminal Services RemoteApp

Terminal Services（TS）所提供的 RemoteApp 使用机制（如图 1-3 所示）主要可以让客户端的用户在远程连接使用 TS 主机上的应用程序，就好像在执行本地计算机中的应用程序一般，然而如果用户所执行在相同 TS 主机的不同应用程序超过一个以上时，RemoteApp 将会共享相同的 TS 工作阶段（Session）。用户可以访问 TS 主机上的 RemoteApp 方法有以下几种。

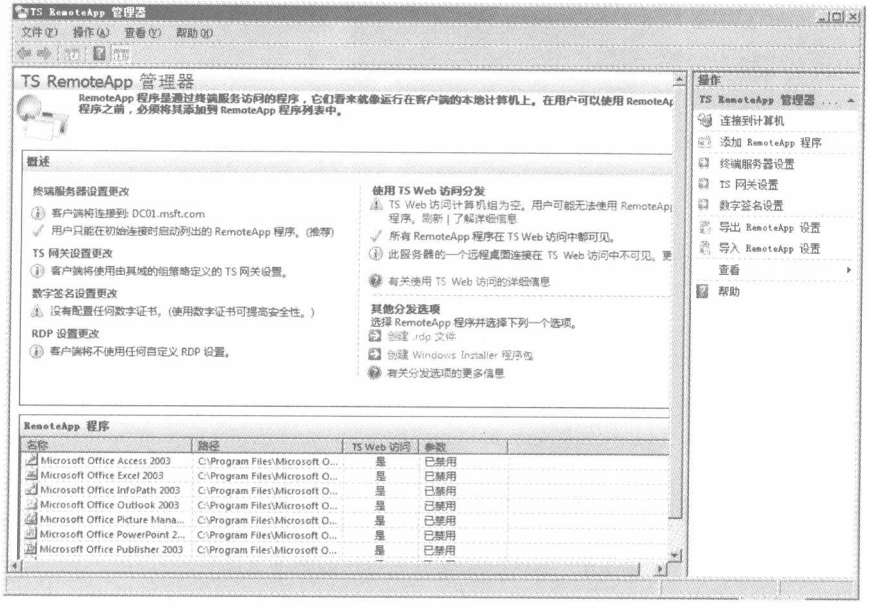

图 1-3　TS RemoteApp 的管理界面

- 用鼠标双击管理员预先部署到客户端计算机桌面上，或者选择“开始”→“所有程序”

中的 TS RemoteApp 应用程序。

- 连续单击任意一个与 TS RemoteApp 相互关联的文件。
- 在连接所提供的 TS Web Access 之后，单击在网站上的 TS RemoteApp 图标即可。

2） Terminal Services Gateway

部署一台 TS Gateway 的服务器角色在企业的 DMZ 网段之中，可以让远程用户直接通过 Remote Desktop Connection（RDC）6.0 连接程序，直接通过 RDP over HTTPS 的方式连接到企业内部的 TS 主机或是开放远程桌面连接的其他计算机上，而管理员只要预先在边缘防火墙上开放 443 的通信端口即可。

通过这一项新技术的运用，可以让远程用户无须预先完成 VPN 网络的连接便可以直接访问，而管理员也可以很轻易地通过如图 1-4 所示的 TS Gateway Management（TS 网关管理器）的 MMC 3.0 管理界面，来一次完成各种读取策略的配置，通过这些访问条件的制定，让必须符合这些条件的用户能够访问到相对应的网络资源。

此外，如果管理员在组织中部署了网络策略服务器（Network Policy Server，NPS），便可以将 TS Gateway 所制定的各项访问策略使用 NPS 进行存储、管理及确认。

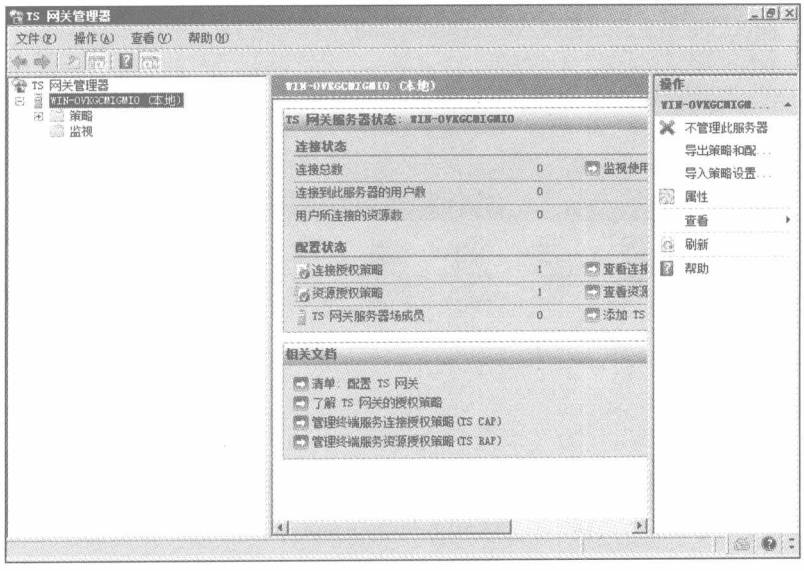

图 1-4 TS 网关管理器

3） Terminal Services Web Access

前面我们所提到的 TS RemoteApp 的建立与使用，用户除了可以经过单击本机桌面图标的执行方法外，如图 1-5 所示通过浏览器以 HTTPS 的安全连接方式，先连接登录到 TS 主机之后再来单击所要执行的 TS RemoteApp 应用程序项目也是可以的，而它的主要优点在于管理员

无须建立 TS Gateway 及部署 TS RemoteApp 的连接程序到客户端计算机中。

4）Terminal Services Session Broker

TS Session Broker 是一个在 Windows Server 2008 上的新功能，它与前一版 Terminal Services 所提供的 Session Directory 用途一样，不过它并不需要结合 Microsoft Network Load Balancing 的使用才能够达到网络负载均衡的机制，而直接可以将客户端的连接自动导向到服务器群集中最少负载的 TS 主机上，对于重新连接的客户端也可以继续保留原有的工作阶段，而客户端则无须知道背后真正连接的 TS 主机是哪一台。然而，之所以可以做到兼顾容错（HA）与网络负载均衡（NLB）的高可用性机制，主要是因为通过 TS Session Broker 这一项功能，可以让服务器集群中的每一台 TS 主机共享相同的 DNS 名称记录。

5）Terminal Services Easy Print

TS Easy Print 也是 Windows Server 2008 上的一项新功能，主要特色在于让远程的用户在访问 TS RemoteApp 的同时，如果想要进行打印的动作，便可以直接选择该应用程序的打印功能，来将所要打印的文件夹传送到所有可以访问的打印机上，最重要的是在 TS 主机上并不需要安装任何打印机驱动程序。IT 管理人员还可以预先将每一位不同部门、不同属性的用户，通过组策略各自配置，来决定哪些用户连接可以使用特定的网络打印机，如图 1-5 所示。

图 1-5　TS Web 与 RemoteApp 的结合

7．网络访问保护（NAP）

这项安全机制是 Windows Server 2008 在网络准入技术上的一大突破，因为它可以针对所有来自远程 VPN、无线网络、局域网客户端，设置 DHCP 和 802.1x 协议及 IPSec 连接的电脑。NAP 需要先完成客户端健康检查，并且确认无误之后才能给与连接，否则会自动将客户端设

备丢到隔离的网络区域中进行各项必要的矫正工作，然后才能再一次进行连接检查，都完成之后才能正常登录到企业网络中。

上面所提到的健康检查项目的依据是借助图 1-6 中 Windows Server 2008 提供的网络策略服务器（NPS）角色制定的，例如它可以预先制定好所要检查的项目，包括系统能够更新检查、防病毒代码更新检查、防火墙设置情况检查、屏幕保护设置的检查等，只要有一项不符合，便可以视为不合法的连接，然后丢到另一个网络隔离区的 IP 网段中。

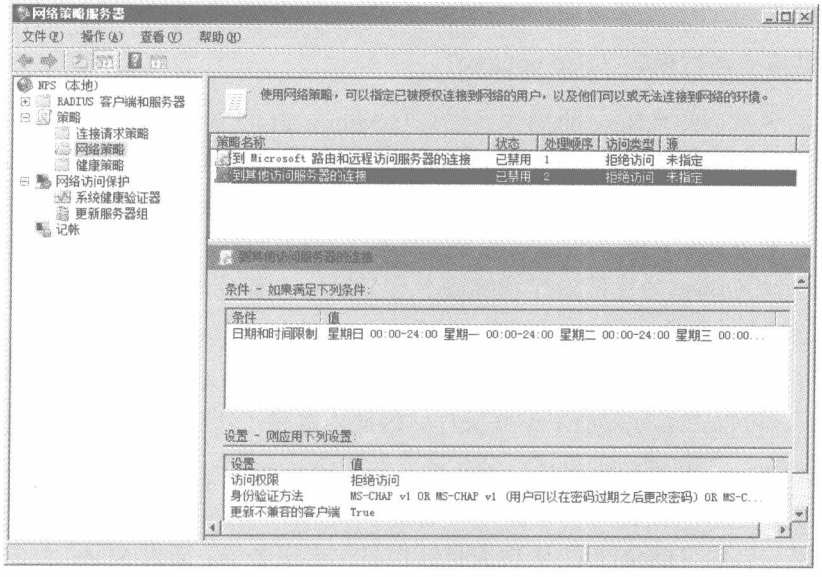

图 1-6　网络策略服务器（NPS）

很显然，Windows Server 2008 所提供的 NAP 保护措施可以有效地预防合法用户所带来的潜在安全隐患，这一项安全机制目前所支持的用户端操作系统有 Windows Vista 及 Windows XP Services Pack 3。

8．只读的域控制器角色（RODC）

想要将一台独立的 Windows Server 2008 服务器或是成员服务器升级为域控制器的角色，则必须通过服务器角色界面的设置来完成。然而值得注意的是，在域控制器的角色配置中，目前多了一个只读的域控制器角色（Read-Only Domain Controller，RODC），这个角色的设计主要是解决分公司域控制器安全性的问题。这是因为，以往我们希望分公司网络的客户端计算机在登录公司域时的速度可以更顺畅，各部署一台域控制器在各分公司，那是当时唯一的解决办法。

可是满足了以上需求之后，你可能会遭遇两个管理上的问题，第一是想要在远程将某一台计算机升级成为域控制器，则必须使用域管理员的身份登录之后才有权限进行。第二点是万一