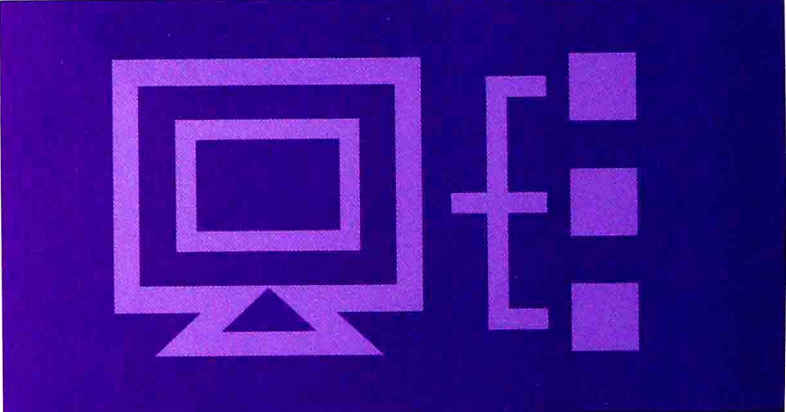


Windows Server 2012 网络管理与架站



戴有炜 编著

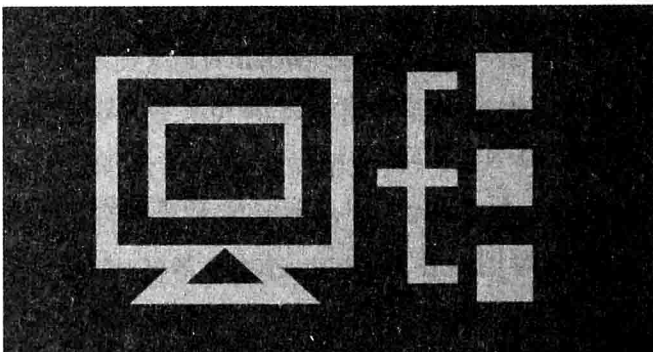
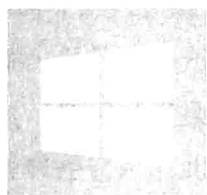
持续畅销·惠及百万读者

- 微软MCSM、MCSE与MCSA认证考试最佳实用参考书
- 独家详述SSTP VPN、IKEv2 VPN、DirectAccess与Web Farm的配置
- 秉持作者一贯兼具理论与实践的写作风格，广获读者支持
- 导入虚拟技术，一台实体电脑就可以拥有完整的虚拟网络环境
- 充分掌握Windows Server 2012网站与网络的整体相关知识

Windows

Server²⁰¹²

网络管理与架站



戴有炜 编著

清华大学出版社
北京

本书版权登记号：图字：01-2013-8758

本书为基峰资讯股份有限公司授权出版发行的中文简体字版本。

内 容 简 介

本书由台湾知名的微软技术专家戴有炜先生倾力编著，是他最新推出的 Windows Server 2012 三卷力作中的网络管理与建站篇。

书中延续了作者的一贯写作风格：大量的实例演示兼具理论，以及完整清晰的操作过程，以简单易懂的文字进行描述，内容丰富且图文并茂。本书共分 12 章，内容包括 Windows Server 2012 基本网络概念、利用 DHCP 自动分配 IP 地址、解析 DNS 主机名称、IIS 网站的配置、PKI 与 SSL 网站、FTP 服务器的配置、路由器与网桥的设置、网络地址转换、虚拟专用网络、通过 DirectAccess 直接访问内部网络资源、RADIUS 服务器的配置以及网络访问保护。

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

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 2012 网络管理与建站 / 戴有炜编著. — 北京：清华大学出版社，2014

ISBN 978-7-302-35138-2

I. ①W… II. ①戴… III. ①Windows 操作系统—网络服务器 IV. ①TP316.86

中国版本图书馆 CIP 数据核字 (2014) 第 012430 号

责任编辑：夏非彼

封面设计：王 翔

责任校对：闫秀华

责任印制：杨 艳

出版发行：清华大学出版社

网 址：<http://www.tup.com.cn>，<http://www.wqbook.com>

地 址：北京清华大学学研大厦 A 座 邮 编：100084

社 总 机：010-62770175 邮 购：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

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

印 刷 者：清华大学印刷厂

装 订 者：三河市新茂装订有限公司

经 销：全国新华书店

开 本：190mm×260mm 印 张：43.75 字 数：1120 千字

版 次：2014 年 4 月第 1 版 印 次：2014 年 4 月第 1 次印刷

印 数：1~4000

定 价：99.00 元

产品编号：056142-01

序

首先要感谢读者长久以来的支持与爱护！这一系列书籍仍然采用我一贯的编写风格，也就是完全站在读者的立场思考，并且以实用的观点来编写这几本Windows Server 2012书籍。我花费了相当多时间不断地测试与验证书中所述内容，并融合多年的教学经验，以最容易让您了解的方式将其写到书中，希望这本书能帮助您快速学会Windows Server 2012。

本套书的宗旨是希望能够让读者通过书中完整与清楚的实际操作，来充分了解Windows Server 2012，进而能够轻松地管理Windows Server 2012的网络环境，因为此书不但理论解说清楚，而且范例充足。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参考书籍。

学习网络操作系统，要注重实际操作，只有掌握操作中所介绍的各项技术，才能充分了解与掌控它，因此建议使用类似Windows Server 2012 Hyper-V的虚拟化软件，来配置各种网络测试环境。

本套书分为《Windows Server 2012系统配置实务》、《Windows Server 2012网络管理与架设》和《Windows Server 2012 Active Directory配置实务》三本，内容丰富详实，相信这几本书仍然不会辜负您的期望，在学习Windows Server 2012时给予您最大的帮助。

感谢所有让这本书能够顺利出版的朋友们，他们在给予宝贵意见、帮助版面排版、协助技术审校、出借测试设备以及提供软件资源等方面都给予了很大帮助。

目 录

第 1 章 Windows Server 2012 基本网络概念	1
1.1 Windows Server 2012 的网络功能	2
1.2 TCP/IP 通信协议简介	2
1.2.1 IP 地址	3
1.2.2 IP 类型	3
1.2.3 子网掩码	5
1.2.4 默认网关	6
1.2.5 私有 IP 的使用	7
1.3 IPv6 的基本概念	7
1.3.1 IPv6 地址的语法	7
1.3.2 IPv6 地址分类	9
1.3.3 IPv6 地址的自动设定	18
1.4 Windows Server 2012 的管理工具	21
第 2 章 利用 DHCP 自动分配 IP 地址	24
2.1 主机 IP 地址的设置	25
2.2 DHCP 的工作原理	25
2.2.1 向 DHCP 服务器索取 IP 地址	26
2.2.2 更新 IP 地址的租约	27
2.2.3 Automatic Private IP Addressing (APIPA)	28
2.3 DHCP 服务器的授权	29
2.4 DHCP 服务器的安装与测试	30
2.4.1 安装 DHCP 服务器角色	31
2.4.2 DHCP 服务器的授权、解除授权	33
2.4.3 建立 IP 作用域	34
2.4.4 测试客户端是否可租用到 IP 地址	36
2.4.5 客户端的其他设置	38



2.5	IP 作用域的管理.....	39
2.5.1	一个子网只可以建立一个 IP 作用域.....	39
2.5.2	租期该设置多久.....	40
2.5.3	建立多个 IP 作用域.....	41
2.5.4	保留特定 IP 地址给客户端.....	42
2.5.5	筛选客户端计算机.....	43
2.5.6	多台 DHCP 服务器的 split scope 高可用性.....	44
2.5.7	子网延迟配置.....	46
2.5.8	DHCP 拆分作用域配置向导.....	47
2.6	DHCP 的选项设置.....	49
2.6.1	DHCP 选项设置的级别.....	50
2.6.2	通过策略来分配 IP 地址与选项.....	52
2.6.3	DHCP 服务器处理策略的方式.....	57
2.6.4	DHCP 的类选项.....	57
2.7	DHCP 中继代理.....	63
2.8	超级作用域与多播作用域.....	70
2.8.1	超级作用域.....	70
2.8.2	多播作用域.....	72
2.9	DHCP 数据库的维护.....	73
2.9.1	数据库的备份.....	74
2.9.2	数据库的还原.....	74
2.9.3	作用域的协调.....	75
2.9.4	将 DHCP 数据库迁移到其他的服务器.....	76
2.10	监视 DHCP 服务器的运行.....	76
2.11	IPv6 地址与 DHCPv6 的设置.....	79
2.11.1	手动设置 IPv6 地址.....	79
2.11.2	DHCPv6 的设置.....	81
2.12	DHCP 故障转移.....	83
第 3 章	解析 DNS 主机名.....	91
3.1	DNS 概述.....	92
3.1.1	DNS 域名空间.....	92
3.1.2	DNS 区域.....	94
3.1.3	DNS 服务器.....	95



3.1.4	“唯缓存”服务器	95
3.1.5	DNS 的查询模式	96
3.1.6	反向查询	97
3.1.7	动态更新	97
3.1.8	缓存文件	97
3.2	DNS 服务器的安装与客户端的设置	97
3.2.1	DNS 服务器的安装	98
3.2.2	DNS 客户端的设置	99
3.2.3	使用 HOSTS 文件	100
3.3	DNS 区域的建立	101
3.3.1	DNS 区域的类型	102
3.3.2	创建主要区域	103
3.3.3	在主要区域内新建资源记录	106
3.3.4	建立辅助区域	112
3.3.5	建立反向查找区域与反向记录	116
3.3.6	子域与委派域	121
3.3.7	存根区域	126
3.4	DNS 区域的高级设置	131
3.4.1	更改区域类型与区域文件名	131
3.4.2	SOA 与区域传送	132
3.4.3	名称服务器的设置	134
3.4.4	区域传送的相关设置	134
3.5	动态更新	135
3.5.1	启用 DNS 服务器的动态更新功能	135
3.5.2	DNS 客户端的动态更新设置	136
3.5.3	DHCP 服务器的 DNS 动态更新设置	139
3.5.4	DnsUpdateProxy 组	141
3.5.5	DHCP 名称保护	142
3.6	“单标签名称”解析	143
3.6.1	自动附加后缀	143
3.6.2	GlobalNames 区域	146
3.7	求助于其他 DNS 服务器	149
3.7.1	“根提示”服务器	149
3.7.2	转发器的设置	150





3.8 检测 DNS 服务器	152
3.8.1 监视 DNS 设置是否正常	152
3.8.2 利用 Nslookup 命令来查看记录	153
3.8.3 缓存区的清除	155
3.9 DNS 的安全防护——DNSSEC	155
3.9.1 DNSSEC 基本概念	156
3.9.2 DNSSEC 实例演示	157
3.10 清除过期记录	168
第 4 章 IIS 网站的配置	172
4.1 环境设置与安装 IIS	173
4.1.1 环境设置	173
4.1.2 安装 Web 服务器 (IIS)	175
4.1.3 测试 IIS 网站是否安装成功	176
4.2 网站的基本设置	177
4.2.1 网页存储位置与默认首页	177
4.2.2 新建 default.htm 文件	180
4.2.3 HTTP 重定向	181
4.2.4 导出配置与使用共享的配置	182
4.3 物理目录与虚拟目录	184
4.3.1 实例演示——物理目录	184
4.3.2 实例演示——虚拟目录	185
4.4 新建网站	187
4.4.1 利用主机名来标识网站	188
4.4.2 利用 IP 地址来标识网站	191
4.4.3 利用 TCP 端口来标识网站	193
4.5 网站的安全性	195
4.5.1 添加或删除 IIS 网站的组件	195
4.5.2 验证用户账号的名称与密码	195
4.5.3 通过 IP 地址来限制连接	201
4.5.4 通过 NTFS 或 ReFS 权限来增加网页的安全性	205
4.6 远程管理 IIS 网站与功能委派	205
4.6.1 IIS Web 服务器的设置	206
4.6.2 执行管理工作的计算机的设置	209





4.7 通过 WebDAV 来管理网站上的文件	212
4.7.1 网站的设置	213
4.7.2 WebDAV 客户端的 WebDAV Redirector 设置	216
4.7.3 WebDAV 客户端的连接测试	217
4.8 网站应用程序的设置	219
4.8.1 ASP.NET 应用程序	219
4.8.2 PHP 应用程序	224
4.8.3 快速安装应用程序	230
4.9 网站的其他设置	234
4.9.1 页尾文件	235
4.9.2 启用连接日志	237
4.9.3 性能设置	237
4.9.4 自定义错误页	238
4.9.5 SMTP 电子邮件设置	239
第 5 章 PKI 与 SSL 网站	240
5.1 PKI 概述	241
5.1.1 公钥加密法	241
5.1.2 公钥验证	242
5.1.3 SSL 网站安全连接	243
5.1.4 服务器名称指示 (SNI)	244
5.2 证书颁发机构 (CA) 概述与根 CA 的安装	245
5.2.1 CA 的信任	246
5.2.2 AD CS 的 CA 种类	247
5.2.3 安装 AD CS 与配置根 CA	247
5.3 实例演示——SSL 网站证书	255
5.3.1 让网站与浏览器计算机信任 CA	256
5.3.2 在网站上创建证书申请文件	257
5.3.3 申请证书与下载证书	258
5.3.4 安装证书	262
5.3.5 建立网站的测试网页	264
5.3.6 SSL 连接测试	266
5.4 从属 CA 的安装	268
5.4.1 配置企业从属 CA	268





5.4.2	配置独立从属 CA.....	269
5.5	证书的管理.....	277
5.5.1	CA 的备份与还原.....	277
5.5.2	管理证书模板.....	279
5.5.3	自动或手动颁发证书.....	280
5.5.4	吊销证书与 CRL.....	281
5.5.5	导出与导入网站的证书.....	284
5.5.6	续订证书.....	286
第 6 章	FTP 服务器的配置.....	289
6.1	安装 FTP 服务器.....	290
6.1.1	建立测试环境.....	290
6.1.2	安装 FTP 服务与建立 FTP 站点.....	291
6.1.3	测试 FTP 站点是否配置成功.....	296
6.2	FTP 站点的基本设置.....	298
6.2.1	文件存储位置.....	298
6.2.2	FTP 站点的绑定设置.....	299
6.2.3	FTP 站点的信息设置.....	300
6.2.4	验证用户名称与权限设置.....	303
6.2.5	检查当前连接的用户.....	304
6.2.6	通过 IP 地址来限制连接.....	305
6.3	物理目录与虚拟目录.....	305
6.3.1	物理目录实例演示.....	305
6.3.2	虚拟目录实例演示.....	307
6.4	FTP 站点的用户隔离设置.....	309
6.4.1	不隔离用户，但是用户有自己的主目录.....	310
6.4.2	隔离用户、有专用主目录，但无法访问全局虚拟目录.....	312
6.4.3	隔离用户、有专属主目录，可以访问全局虚拟目录.....	316
6.4.4	通过 Active Directory 来隔离用户.....	317
6.5	具备安全连接功能的 FTP over SSL.....	322
6.6	防火墙的 FTP 设置.....	323
6.6.1	FTP 主动模式.....	324
6.6.2	FTP 被动模式.....	325
6.7	虚拟主机名.....	329





第 7 章 路由器与网桥的设置	331
7.1 路由器的原理	332
7.1.1 一般主机的路由表	332
7.1.2 路由器的路由表	336
7.2 设置 Windows Server 2012 路由器	340
7.2.1 启用 Windows Server 2012 路由器	341
7.2.2 查看路由表	343
7.2.3 添加静态路由	344
7.3 筛选进出路由器的数据包	347
7.3.1 入站筛选器的设置	348
7.3.2 出站筛选器的设置	349
7.4 动态路由 RIP	350
7.4.1 RIP 路由器概述	350
7.4.2 启用 RIP 路由器	352
7.4.3 RIP 路由接口的设置	353
7.4.4 RIP 路由筛选	355
7.4.5 与相邻路由器的交互设置	355
7.5 网桥的设置	356
第 8 章 网络地址转换 (NAT)	359
8.1 NAT 的特色与原理	360
8.1.1 NAT 的网络架构实例图	360
8.1.2 NAT 的 IP 地址	362
8.1.3 NAT 的工作原理	362
8.2 NAT 服务器配置实例演示	365
8.2.1 路由器、固接式 xDSL 或电缆调制解调器环境的 NAT 设置	365
8.2.2 非固接式 xDSL 环境的 NAT 设置	369
8.2.3 内部网络包含多个子网	376
8.2.4 新增 NAT 网络接口	376
8.2.5 内部网络的客户端设置	377
8.2.6 连接错误排除	379
8.3 DHCP 分配器与 DNS 中继代理	380
8.3.1 DHCP 分配器	380
8.3.2 DNS 中继代理	381





8.4	开放因特网用户来连接内部服务器	381
8.4.1	端口映射	381
8.4.2	地址映射	383
8.4.3	地址池的设置	384
8.4.4	地址映射的设置	384
8.5	因特网连接共享 (ICS)	385
第 9 章	虚拟专用网	388
9.1	虚拟专用网 (VPN) 概念	389
9.1.1	VPN 的部署场合	389
9.1.2	远程访问协议	390
9.1.3	验证协议	390
9.1.4	VPN 协议	391
9.2	PPTP VPN 实例演示	395
9.2.1	准备好测试环境中的计算机	395
9.2.2	域控制器的安装与设置	395
9.2.3	配置 PPTP VPN 服务器	397
9.2.4	赋予用户远程访问的权利	403
9.2.5	PPTP VPN 客户端的设置	403
9.2.6	NetBIOS 计算机名称解析	409
9.2.7	VPN 客户端为何无法上网——Part 1	410
9.2.8	VPN 客户端为何无法上网——Part 2	412
9.3	L2TP VPN 实例演示——预共享密钥	414
9.4	L2TP VPN 实例演示——计算机证书	416
9.4.1	建立初始测试环境	416
9.4.2	安装企业根 CA	417
9.4.3	L2TP VPN 服务器的设置	417
9.4.4	L2TP VPN 客户端的设置	420
9.4.5	测试 L2TP VPN 连接	423
9.5	SSTP VPN 实例演示	425
9.5.1	建立初始测试环境	425
9.5.2	安装企业根 CA	425
9.5.3	SSTP VPN 服务器的设置	428
9.5.4	SSTP VPN 客户端的设置	436





9.5.5	测试 SSTP VPN 连接	437
9.6	IKEv2 VPN 实例演示——用户验证	440
9.6.1	建立初始测试环境	440
9.6.2	安装企业根 CA	440
9.6.3	IKEv2 VPN 服务器的设置	445
9.6.4	IKEv2 VPN 客户端的设置	448
9.6.5	测试 IKEv2 VPN 连接	449
9.7	IKEv2 VPN 实例演示——计算机验证	453
9.7.1	IKEv2 VPN 服务器的设置	453
9.7.2	IKEv2 VPN 客户端的设置	454
9.8	站点对站点 PPTP VPN 实例演示	457
9.8.1	请求拨号	458
9.8.2	A 网络 VPN 服务器的设置	458
9.8.3	B 网络 VPN 服务器的设置	464
9.8.4	测试请求拨号功能是否正常	466
9.8.5	设置请求拨号筛选器与拨出时间	468
9.9	站点对站点 L2TP VPN——预共享密钥	468
9.9.1	建立初始测试环境	468
9.9.2	由 VPNS1 通过请求拨号来发起连接到 VPNS2	469
9.9.3	由 VPNS2 通过请求拨号来发起连接到 VPNS1	470
9.10	站点对站点 L2TP VPN——计算机证书	472
9.10.1	建立初始测试环境	473
9.10.2	在 Server1 上安装独立根 CA	473
9.10.3	VPN 服务器 VPNS1 的设置	473
9.10.4	VPN 服务器 VPNS2 的设置	475
9.10.5	测试采用计算机证书的站点对站点 L2TP VPN	475
9.11	利用浏览器申请计算机证书	477
9.11.1	VPN 服务器所需的计算机证书	477
9.11.2	利用浏览器申请计算机证书	478
9.11.3	将证书迁移到计算机证书存储区域	482
9.12	网络策略	486
9.12.1	新建网络策略	487
9.12.2	是否接受连接的详细流程	492





第 10 章 通过 DirectAccess 直接访问内部网络资源	495
10.1 DirectAccess 概述	496
10.2 DirectAccess 实例演示之 1——内部网络仅包含 IPv4 主机	500
10.2.1 准备好测试环境中的网络环境	500
10.2.2 准备好测试环境中的计算机	504
10.2.3 域控制器的安装与设置	505
10.2.4 资源服务器 APP1 的设置	506
10.2.5 DirectAccess 客户端 Win8PC1 的设置	507
10.2.6 在 DC1 针对 DirectAccess 客户端建立安全组	508
10.2.7 将 DirectAccess 服务器加入域	509
10.2.8 DNS 与 DHCP 服务器 SERVER1 的设置	509
10.2.9 客户端 Win8PC1 的基本网络功能测试	511
10.2.10 在 DirectAccess 服务器 DA1 上安装与设置“远程访问”	512
10.2.11 将客户端 Win8PC1 移动到内部网络来应用组策略设置	518
10.2.12 将客户端 Win8PC1 移动到因特网来测试 DirectAccess	522
10.3 DirectAccess 实例演示之 2——客户端位于 NAT 之后	526
10.4 DirectAccess 实例演示之 3——内部网络包含 IPv4 与 IPv6 主机	532
10.4.1 准备好测试环境中的计算机	532
10.4.2 域控制器 DC1 的设置	533
10.4.3 资源服务器 APP1 的设置	542
10.4.4 IPv4 资源服务器 APP2 的设置	545
10.4.5 DirectAccess 服务器 DA1 的设置	547
10.4.6 将客户端 Win8PC1 移动到内部网络来应用组策略设置	557
10.4.7 将客户端 Win8PC1 移动到因特网来测试 DirectAccess	560
10.4.8 将客户端 Win8PC1 移动到客户网络来测试 DirectAccess	565
10.4.9 启用对 Windows 7 客户端的支持	571
第 11 章 RADIUS 服务器的配置	573
11.1 RADIUS 概述	574
11.1.1 RADIUS 服务器	574
11.1.2 RADIUS 代理服务器	575
11.2 网络策略服务器 (NPS)	576
11.2.1 安装网络策略服务器 (NPS)	577
11.2.2 登录网络策略服务器	578





11.3 RADIUS 服务器与客户端的设置.....	579
11.3.1 RADIUS 服务器的设置	580
11.3.2 RADIUS 客户端的设置	582
11.4 RADIUS 代理服务器的设置.....	584
11.4.1 连接请求策略	584
11.4.2 建立远程 RADIUS 服务器组	585
11.4.3 修改 RADIUS 服务器组的设置	586
第 12 章 网络访问保护 (NAP)	588
12.1 网络访问保护 (NAP) 概述	589
12.1.1 NAP 基本架构	589
12.1.2 将不健康客户端修复为健康客户端	590
12.1.3 监控 NAP 客户端的健康情况	591
12.1.4 NAP 强制执行点的运行	591
12.2 DHCP NAP 实例演示	591
12.2.1 准备好测试环境中的计算机	592
12.2.2 域控制器 DC1 的安装	593
12.2.3 NAP 健康策略服务器的配置	593
12.2.4 DHCP 服务器的设置	600
12.2.5 NAP 客户端的 DHCP 功能测试	607
12.2.6 将域控制器 DC1 指定为 NAP 更新服务器	609
12.2.7 将 NAP 客户端加入域后的 DHCP 测试	613
12.2.8 验证自动修复功能是否正常	619
12.2.9 进一步验证健康策略功能是否正常	620
12.3 VPN NAP 实例演示	622
12.3.1 准备好测试环境中的计算机	623
12.3.2 域控制器 DC1 的安装	624
12.3.3 NAP 健康策略服务器的搭建	625
12.3.4 VPN 服务器的设置	636
12.3.5 组策略的 NAP 设置	642
12.3.6 NAP VPN 客户端测试	647
12.3.7 验证自动修复功能是否正常	650
12.3.8 进一步验证健康策略功能是否正常	651
12.4 DirectAccess NAP 实例演示	653



12.4.1	准备好服务器 HRA-NPS1	654
12.4.2	准备好健康证书模板	655
12.4.3	HRA 服务器与 NAP 健康策略服务器的搭建	661
12.4.4	组策略的 NAP 设置	670
12.4.5	DirectAccess 服务器的设定	674
12.4.6	NAP DirectAccess 客户端测试	678
12.4.7	验证自动修复功能是否正常	680
12.4.8	进一步验证健康策略功能是否正常	680



1

第 1 章 Windows Server 2012 基本网络概念

Windows Server 2012提供了各种不同的网络解决方案, 让企业可以利用它来构建各种不同的网络环境。我们将通过本章来介绍Windows Server 2012的网络功能与不可或缺的TCP/IP通信协议, 包含IPv4与IPv6。

- ✎ Windows Server 2012的网络功能
- ✎ TCP/IP通信协议简介
- ✎ IPv6的基本概念
- ✎ Windows Server 2012的管理工具