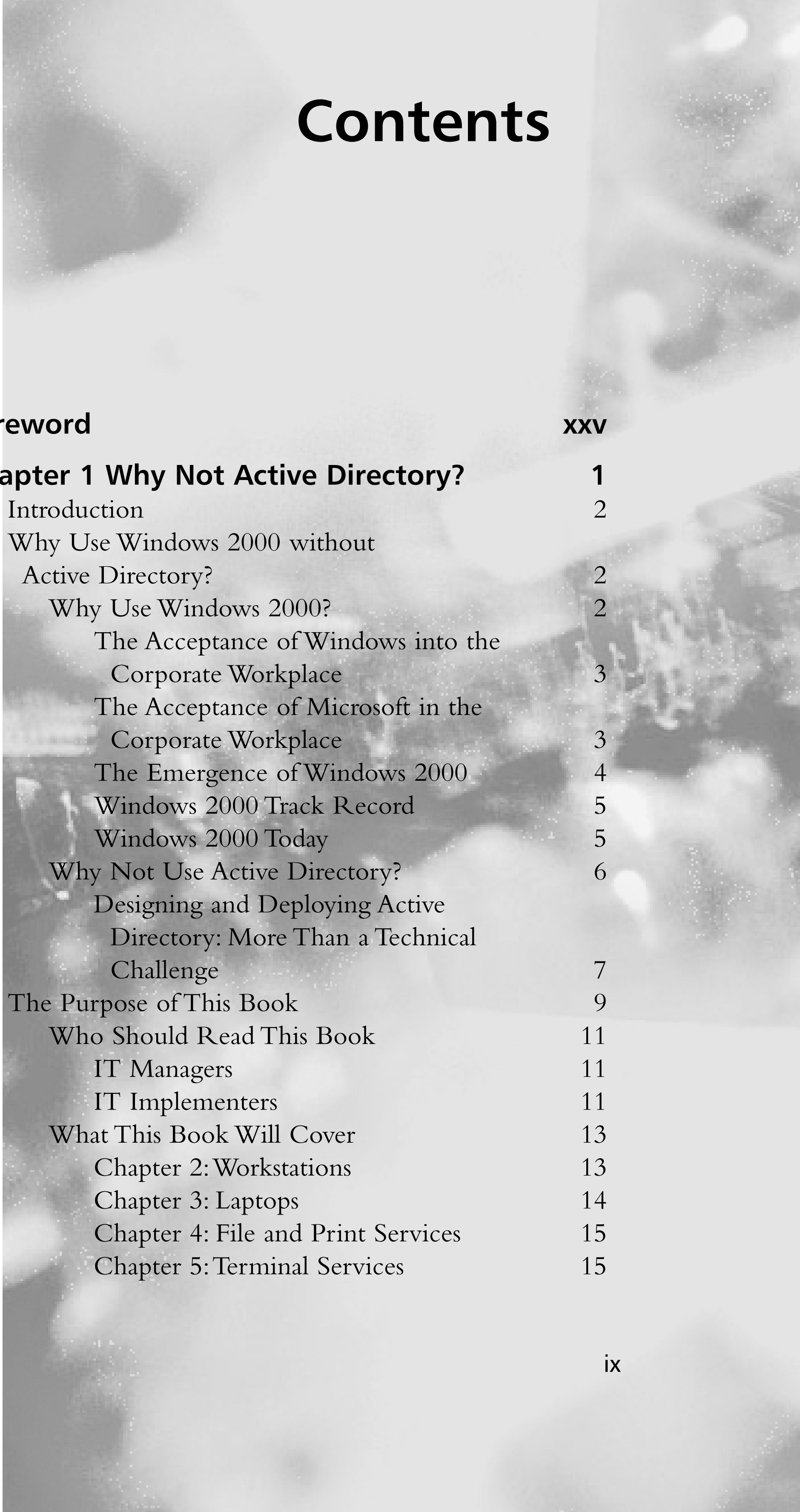

Contents

Why Use Windows 2000 without Active Directory?

There is more to Windows 2000 than just Active Directory features—as this book shows. But there's no doubt that Windows 2000 was written with Active Directory in mind, which is reflected in the standard documentation that accompanies the software. Chapter 1 will begin to answer these questions.

Foreword xxv

Chapter 1 Why Not Active Directory? 1

Introduction 2

Why Use Windows 2000 without Active Directory? 2

  Why Use Windows 2000? 2

    The Acceptance of Windows into the Corporate Workplace 3

    The Acceptance of Microsoft in the Corporate Workplace 3

    The Emergence of Windows 2000 4

    Windows 2000 Track Record 5

    Windows 2000 Today 5

  Why Not Use Active Directory? 6

    Designing and Deploying Active Directory: More Than a Technical Challenge 7

The Purpose of This Book 9

  Who Should Read This Book 11

    IT Managers 11

    IT Implementers 11

  What This Book Will Cover 13

    Chapter 2: Workstations 13

    Chapter 3: Laptops 14

    Chapter 4: File and Print Services 15

    Chapter 5: Terminal Services 15

Chapter 6: Networking Services—DNS, DHCP, WINS, NLB 16
Chapter 7: Internet Services—IIS5 and Certificate Services 17
Chapter 8: Secure Communication—IPSec 18
Chapter 9: Remote Access—RAS, VPN, IAS, and CMAK 18
Chapter 10: Internet Connectivity—ICS, NAT, and ISA Server 19
Appendix A: The Windows 2000 Microsoft Management Console 20
What This Book Won't Cover 21
Exchange 2000 and Other Active Directory Dependent Applications 22
Intellimirror Features 25
Enterprise Related Group Policy Objects 28
Quick Resource Searches across the Enterprise Network, with the Ability to Extend the Schema 29
Universal Groups, Group Nesting, and Changes in Group Membership 32
Task Delegation 33
Kerberos Rather Than NTLM Authentication 34
Automatic Transitive Trusts 35
Multimaster Domain Controllers 36
Enterprise Encrypting File System (EFS) Recovery Agents 38
Enterprise Certificate Authorities 39
Quality of Service 40
Active Directory Integration 43
Migrating Networks 45
Fractional Networks 46
Dangers of Fractional Networks Running Active Directory 47
External Networks 47

Walkthrough: Managing User Accounts and Securing the Local Administrator Account 49
Summary 56
Solutions Fast Track 57
Frequently Asked Questions 59

Chapter 2 Workstations 65
Introduction 66
Using Local Group Policy 67
Group Policy Objects 69
Locating Local Group Policy 70
Local Security Policy 71
Complete Local Group Policy Settings 71
Configuring Local Group Policy 73
Useful Group Policy Objects 75
Computer Startup/Shutdown and User Logon/Logoff Scripts 76
Password Options 77
Internet Explorer Settings 81
Disabling Installation from Removable Media 81
Controlling Access to Control Panel and Components 81
Screen Saver Options 83
Disabling the Command Prompt, Disabling the Registry Editor, Running Only Specified Windows Applications 83
Deploying Local Group Policy Objects 84
Security Configuration Using Templates 84
Security Templates 85
Default Security Template 87
Secure Security Template 87
Highly Secure Template 87
Compatible Template 88
Out of the Box Templates 88
Viewing and Modifying Templates 88
Viewing Template Settings 88

TIP

You can always check the current version of Windows (build and Service Pack if applied) by running **WinVer.exe**, which displays the About Windows dialog box.

Modifying Template Settings 91
Applying Templates 91
Security Configuration and Analysis 92
Configure Computer Now 92
Analyze Computer Now 94
Deploying Security Templates Automatically with Secedit 95
Secedit /Configure Options 95
Improvements in System Reliability 96
Device Driver Signing 97
Driver Signing Options 98
Driver Signing Verification 98
Windows File Protection and System File Checker 99
How Windows File Protection and System File Checker Work 100
WFP Configuration Options 102
WFP Limitations 104
Service Pack Application 105
Slip-Streaming Service Packs 105
Limitations of Service Packs 106
Improvements in Usability 107
Desktop Changes 108
Personalized Menus 109
Start Menu Settings 109
Display Options 111
Folder Options 112
Hardware Support 113
Wizards and Help 114
Wizards 114
Help 116
Walkthrough: Configuring Local Group Policy 119
Summary 122
Solutions Fast Track 123
Frequently Asked Questions 125

Chapter 3 Laptops 129
Introduction 130
Integrating Mobile Computing with the Corporate Network 131
Switching between Working Environments 133
Power Management and Preservation 133
Offline Files and Synchronizing Data 140
Dialup Access 151
Securing Data Outside the Company Environment 153
Encrypting Folders and Files 155
Limitations and Considerations when Using EFS 156
Disabling EFS 156
Remote Access Security 158
Mobile Maintenance and Troubleshooting 158
Safe Mode and the Recovery Console 159
Using the Recovery Console 163
Task Scheduler 165
Configuring Scheduled Tasks 166
Task Manager 168
Walkthrough: Using Offline Files 172
Summary 176
Solutions Fast Track 178
Frequently Asked Questions 180

Switching between Working Environments

There are a number of features that help users switch seamlessly between their different working environments. These include:

- Power management and preservation
- Offline folders and synchronizing data
- Dialup access

Chapter 4 File and Print Services 185
Introduction 186
Sharing Data: Storing and Retrieving 187
Distributed File System (DFS) 191
Configuring Dfs 194
Volume Mount Points 197
Configuring Mounted Drives 199
Indexing Service 200
Configuring Index Catalogs 204

NOTE

The general advice when planning disk space for indexing is to allow at least 30 percent and preferably 40 percent of the total amount of disk space you index (known as the *corpus*). It would also be prudent to host the index catalogs on a different disk from the operating system.

Sharing Printers: Installing and Managing 207
Standard TCP/IP Port Monitor 210
IP Printing 210
Printing Permissions Over the Internet 214
Better Monitoring 214
User Options 216
Managing Servers 216
Disk Management 217
Using the Disk Management Utility 220
Data Management 222
Remote Storage 222
Windows 2000 Backup Utility 224
Disk Quotas 225
Configuring Disk Quotas 226
Monitoring 229
Counter Logs 232
Alerts 232
Trace Logs 233
Using Performance Data 233
Auditing Events and the Security Log 234
Auditing the Registry 236
Auditing Administrative Actions 237
Configuring Counter and Alert Logs 238
Configuring and Using the Event Logs 240
Walkthrough: Setting an Audit Policy 244
Summary 252
Solutions Fast Track 253
Frequently Asked Questions 256

Chapter 5 Terminal Services 261

Introduction 262
Why Use Windows 2000 Terminal Services? 263
Fast Connections Over Low Bandwidths 264
Remote Administration 265
Remote Administration Using Terminal Services 266

Understand the specific technical features and options available with Windows 2000 Terminal Services, including:

- Fast connections over low bandwidths
- Remote administration
- Tighter security
- Shadowing (remote control)
- Seamless integration between PC and server

Terminal Services Remote Management Limitations 267
Recovering from Disconnected Sessions 269
Tighter Security 270
Using the Application Security Tool 274
Shadowing Users 276
Seamless Integration Between PC and Server 278
Clipboard Copy and Paste 279
Drive Mappings 280
Local Printer Support 280
Profiles 281
Home Directories 282
Multilanguage Support 283
Preinstallation Considerations 283
Licensing 284
Installing Terminal Services Licensing 286
How Terminal Service Licensing Works 288
Activating a Terminal Services License Server 290
Upgrading from TSE 293
Unattended Installations 295
Application Suitability 295
Capacity and Scaling 298
Limitations 301
Configuring and Managing Windows 2000 Terminal Services 302
Configuring Clients to Use Terminal Services 308
Terminal Services Client 308
Terminal Services Advanced Client 314
Automating Terminal Services Client Setup 317
Using TSAC as a Diagnostic Utility 319
Walkthrough: Remotely Administering a Windows 2000 Server With Terminal Services 321
Summary 327
Solutions Fast Track 329
Frequently Asked Questions 332

Chapter 6 Networking Services 337
Introduction 338
Name Resolution with DNS 340
Do You Need to Run DNS? 340
Advantages of Microsoft's Windows 2000 DNS 344
Dynamic Updates 345
WINS Integration 347
Service Records 349
Unicode and the Underscore 352
Incremental Transfers 355
Easy to Use GUI Administration 356
Integrating Microsoft DNS and UNIX DNS 357
Server Roles and Zones 357
Transferring Zones 360
Importing Zone Files 361
DHCP for Central Configuration and Control of Addresses 363
TCP/IP Configuration Options 366
Vendor and User Class Options 367
BOOTP and Multicast Scopes 368
Automatic Private IP Addressing (APIPA) 370
Superscopes 371
Multinets 372
Server Consolidation 373
Migrating Users from One Scope to Another (Address Reallocation) 374
Name Resolution with WINS 375
Improved WINS Manager 380
Data Integrity 381
Backup Policy 383
Controlling Replication Partners 383
Replication Policy 383
Removing Old Mappings 384
Database Verification 385

Justifications for running DNS include:

- Having UNIX computers
- Running Internet services
- Running Active Directory
- Preparing for Active Directory
- Looking to integrate UNIX and Microsoft communication

High Performance 386
Burst Mode Handling 386
Persistent Connections 386
High Availability with Network Load Balancing (NLB) 388
Network Load Balancing Components 392
Addresses and Priorities 393
Port Rules 395
The WLBS Command Line Utility 398
Configuring Network Load Balancing 399
Configuring Cluster Parameters 400
Configuring Host Parameters 402
Configuring Port Rules 402
Monitoring and Administering Network Load Balancing 405
Walkthrough: Configuring DNS Primary and Secondary Zones 407
Summary 413
Solutions Fast Track 414
Frequently Asked Questions 418

NOTE

Internet Explorer 3.0, Netscape Navigator 2.0, and later versions of both browsers support the use of host header names. Older browsers do not. Additionally, you cannot use host headers with SSL because the host header will be encrypted—this is an important point for Web servers using SSL for additional security.

Chapter 7 Internet Services 423
Introduction 424
Installing IIS5 425
Improvements in Reliability 427
Application Protection 427
Setting Application Protection 428
IISreset 429
Restarting IIS from the Internet Information Services Snap-In 429
Restarting IIS Using the Command Line 429
Additional Control When Stopping IIS Services 430
Backup/Restore Configuration 431
Limitations of Backup/Restore Configuration 433

FTP Restart 433
Limitations of FTP Restart 433
Improvements in Administration and Management 434
Wizards and Tools 435
Security Settings Permission Wizard 435
Windows 2000 Internet Server Security Configuration Tool 437
Certificate Wizard and Certificate Trust Lists Wizard 438
IIS Migration Wizard 440
Improved Logging for Process Accounting 440
Improved Remote Administration 441
Web Site Operators 443
Improvements in Security 444
Windows Integrated 446
Digest 446
Fortezza 447
Improvements in Performance 447
HTTP Compression 448
Configuring HTTP Compression 449
ASP Improvements 451
Bandwidth Throttling 452
Configuring Bandwidth Throttling 452
Process Throttling 453
Socket Pooling 454
Document Collaboration with WebDAV 455
Using WebDAV 456
Certificate Services 458
Certificate Authorities and Roles 459
Installing and Configuring a Standalone CA 461
Server Certificates 462
Installing the Web Server's Certificate Offline with a Standalone CA 463
How Users Request and Manage Certificates 465

Using Secure Communication (SSL) on the Web Server 468

Client Certificate Mapping 469

Configuring One-to-One Account Mappings 470

Configuring Many-to-One Account Mappings 472

Walkthrough: Configuring Multiple Web Sites on a Single Web Server 474

Summary 483

Solutions Fast Track 484

Frequently Asked Questions 488

Chapter 8 Secure Communication 491

Introduction 492

IPSec Planning—Working Out What You Want to Secure and How 493

Password Based 496

Certificate Based 497

IP Security Utilities—For Configuring and Monitoring Secure Communication 498

Using IP Security Policies on Local Machines 499

Using IP Security Monitor 500

Using the IPSec Policy Agent Service 502

Using TCP/IP | Advanced | Options 503

Using Certificates Snap-In 504

Using the Security Log 505

Using the NetDiag Support Tool 507

IPSec Built-in Policies—For Minimal Administrator Configuration 508

Client (Respond Only) 509

Server (Request Security) 510

Secure Server (Require Security) 510

IPSec Policy Components 511

IP Filter Rules and Lists 511

Secure communication can be broken down into the following five components:

- Nonrepudiation
- Antireplay
- Integrity
- Confidentiality
- Authentication

Recommendations for Defining Filter Lists 514
IP Filter Actions 514
Recommendations for Defining Filter Actions 516
Other IP Rule Components—Authentication, Tunnel Setting, and Connection Type 517
Setting Computer Authentication Using Preshared Keys 518
Setting Authentication Using Certificates 518
IP Security Protocols and Algorithms 523
Data Authentication Algorithms 525
Data Encryption Algorithms 525
Key Exchange and Management 526
Configuring Session Key Settings 528
Security Associations 531
Walkthrough 8.1: Setting and Testing Custom IPSec Policies 534
Walkthrough 8.2: Using IPSec to Protect a Web Server 542
Summary 550
Solutions Fast Track 551
Frequently Asked Questions 554
Chapter 9 Remote Access 559
Introduction 560
Using and Configuring Remote Access Policies 561
Remote Access Administration Models 562
Granting Remote Access Authorization—By User 564
Access by Policy on a Standalone Server in a Workgroup 565
Access by Policy on a Member Server in an NT4 Domain 566
Remote Access Policy Components 567

Configuring Windows 2000 Routing and Remote Access 568
Configuring General Server Properties 570
Configuring Security Server Properties 570
Configuring IP Server Properties 572
Automatic Private IP Address 573
DHCP Address Allocation 573
TCP/IP Configuration Options 574
Configuring IPX Server Properties 577
Configuring NetBEUI Server Properties 577
Configuring PPP Server Properties 578
Configuring Event Logging Server Properties 579
Configuring Dialup and VPN Connections 579
Configuring L2TP VPN Connections 582
Modifying the Default L2TP/IPSec Policy 586
Using and Configuring Internet Authentication Service (IAS) 590
Configuring RRAS and IAS 592
IAS Configuration with ISPs 595
Configuring Remote Clients with the Connection Manager Administration Kit 598
Manually Defining Connections 600
Using the Connection Manager Administration Kit 601
Preparation: Creating a Static Phone Book 602
Preparation: Creating a Dynamic Phone Book 605
Running the Connection Manager Administration Kit 606
Refining Details 609
How Users Install and Use Connection Manager 611

Setting the Tunneling Value, Necessary for L2TP/IPSec Support

VpnStrategy Value	Description
1	PPTP only (the default)
2	Try PPTP and then L2TP/IPSec
3	L2TP/IPSec only
4	Try L2TP/IPSec and the PPTP (Windows 2000 default)

Q: I'm interested in publishing a VPN server behind the ISA Server. I understand IPSec can't be translated, but is there a good reason why I can't run a PPTP server on my internal network configured as a SecureNAT client?

A: There is a good reason why this won't work—the SecureNAT element works only with TCP and UDP ports. PPTP uses the GRE protocol (number 47) in addition to TCP port 1723, and there's no way to translate this when it comes into the ISA server from an external client. You can create VPN connections from the internal network, and you can run a VPN server on the ISA server itself or on a DMZ, but you cannot publish a VPN server as a SecureNAT client.

Walkthrough: Configuring Remote Access Policies 614
Summary 617
Solutions Fast Track 617
Frequently Asked Questions 620

Chapter 10 Internet Connectivity 625

Introduction 626
Using and Configuring Internet Connection Sharing (ICS) 628
ICS Settings 630
Using and Configuring RRAS Network Address Translation (NAT) 632
Installing NAT 633
Adding NAT to RRAS 635
Configuring NAT 637
Configuring Global NAT Properties 638
Configuring NAT Internet Interface Properties 641
Monitoring NAT 642
Controlling Connections 645
Configuring Demand-Dial Restrictions 646
Configuring Internet Filters 647
Using and Configuring Internet Security and Acceleration (ISA) Server 649
Security Features 653
Caching Features 658
Additional Features 660
Reporting Features 662
Bandwidth Priorities 663
Extensible Platform 663
ISA Clients 664
Web Proxy Client 665
SecureNAT Client 665
Firewall Clients 666
Upgrading Issues 667

Walkthrough: Configuring NAT to Publish a Web Server 670
Summary 674
Solutions Fast Track 676
Frequently Asked Questions 679

Appendix The Windows 2000 Microsoft Management Console 683
Introduction 684
MMC Basics 684
Saving Configuration Changes 687
Exporting Information from MMC Snap-Ins 687
Adding Servers 688
Remote Administration 690
Command Line 690
Configuring and Creating Your Own MMCs 693
Using URL Links 695
Using Favorites in MMCs 696
Organizing Favorites 698
Saving Custom MMCs 699
Changing the Custom MMC View 702
Advanced MMC Configuration: Using Taskpads 703
The New Taskpad View Wizard 704
Adding Taskpad Views and Non-Snap-In Commands 710
Further Customization and Development with MMCs 711
Distributing MMCs 713
Summary 714

Index 715

Taskpad views are HTLM pages that can contain a number of items:

- MMC Favorites
- Wizards
- Scripts
- Programs
- URLs