The ultimate in-depth reference

Hundreds of timesaving solutions

Supremely well-organized, packed with expert advice

Microsoft

Windows Server Inside OUT

Updated for Windows Server 2025

Orin Thomas

FREE SAMPLE CHAPTER

Microsoft

Windows Server Inside Out

Updated for Windows Server 2025

Orin Thomas

Windows Server Inside Out: Updated for Windows Server 2025
Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

Copyright © 2026 by Orin Thomas

Hoboken, New Jersey

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit *www.pearson.com/global-permission-granting.html*.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-534589-4
ISBN-10: 0-13-534589-8

Library of Congress Control Number: 2025949234
$PrintCode

Trademarks
Microsoft and the trademarks listed at *http://www.microsoft.com* on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Warning and Disclaimer
Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

Program Manager: Loretta Yates
Acquisitions Editor: Shourav Bose
Development Editor: Rick Kughen
Managing Editor: Sandra Schroeder
Senior Project Editor: Charlotte Kughen
Copy Editor: Charlotte Kughen
Indexer: Cheryl Lenser
Technical Editor: Vince Averello
Cover Designer: Twist Creative, Seattle
Compositor: Bronkella Publishing, Inc.

Figure Credits
Figure 26-1: © 2025 Ollama
Figure 26-2: BrainDrive LLC
Figure 26-4 to 26-6: Copyright © 2025 Open WebUI

Contents at a Glance

Chapter 1
Administration tools 1

Chapter 2
Installation options 57

Chapter 3
Deployment and configuration 73

Chapter 4
Active Directory 109

Chapter 5
DNS, DHCP, and IPAM 189

Chapter 6
Hyper-V 223

Chapter 7
Storage 269

Chapter 8
File servers 317

Chapter 9
Azure Arc and hybrid services 355

Chapter 10
Windows Server in Azure 397

Chapter 11
Windows Subsystem for Linux 427

Chapter 12
Hardening Windows Server 433

Chapter 13
Hardening Active Directory 473

Chapter 14
Security systems and services 497

Chapter 15
Internet Information Services 523

Chapter 16
Containers 553

Chapter 17
Clustering and high availability 573

Chapter 18
Active Directory Certificate Services 597

Chapter 19
Active Directory Federation Services 643

Chapter 20
Active Directory Rights Management Services . . . 661

Chapter 21
Routing and remote access 681

Chapter 22
Remote Desktop Services 707

Chapter 23
Monitoring and maintenance 729

Chapter 24
Upgrade and migration 757

Chapter 25
Troubleshooting 787

Chapter 26
Hosting large language models on Windows Server 799

Index 809

This page intentionally left blank

Table of Contents

About the Author xxi
Acknowledgments xxi

Introduction xxii

Notes on mature roles and features xxiii
Conventions xxiii
Errata, updates, and book support xxiv

Chapter 1 Administration tools 1

Remote not local 2
Principle of least privilege 2
Privileged Access Workstations 3
Windows Admin Center 5
- Installing Windows Admin Center 7
- Windows Admin Center extensions 9
- Show script 10

Remote Server Administration Tools 10
- RSAT consoles 10
- Server Manager console 14

PowerShell 15
- Modules 17
- PowerShell Gallery 17
- Remoting 18
- One-to-many remoting 19
- PowerShell ISE 20
- PowerShell Direct 23

Remote Desktop 23
Copilots and agents 25
SSH 26
- Windows Server 2025 26
- SSH Server Key Management 27
- Windows Server 2022 and earlier 28

Services console 29
Task Scheduler 31
Control Panel tools 34

Command-line tools 34
Sysinternals tools 39
Process Explorer 39
Process Monitor 41
ProcDump 42
PsTools 42
VMMap 44
SigCheck 45
AccessChk 45
Sysmon 46
AccessEnum 48
ShellRunAs 49
LogonSessions 50
Active Directory Explorer 50
Insight for Active Directory 53
PsPing 54
RAMMap 54

Chapter 2 Installation options 57

Windows Server editions 57
Windows Server Licensing Options 58
Windows Server servicing branches 59
Long Term Servicing Channel 59
Annual Channel 59
Insider Preview Builds 59
Server Core 60
Server Core interface 61
Updating PowerShell on Server Core 63
Server Core graphical tools 64
Server Core roles 64
Server Core App Compatibility Features on Demand 68
When to deploy Server Core 69
Server with Desktop Experience 70
Roles and features 71

Chapter 3 Deployment and configuration 73

Bare-metal versus virtualized 73
Windows images 74
Modifying Windows images 74
Servicing Windows images 75
Mounting images 76
Adding drivers and updates to images 76
Adding roles and features 77
Committing an image 78
Build-and-capture 79

Answer files . . . 79
Infrastructure configuration as code . . . 82
Package-management utilities . . . 83
Winget . . . 83
PowerShell packages . . . 85
PowerShell Gallery . . . 85
Chocolatey . . . 85
Desired State Configuration . . . 87
View resources . . . 88
DSC v3 configurations . . . 88
Exporting DSC configuration . . . 89
DSC shell completion scripts . . . 89
Windows Deployment Services . . . 90
WDS requirements . . . 90
Managing images . . . 92
Configuring WDS . . . 92
Configuring transmissions . . . 96
Driver groups and packages . . . 98
Virtual Machine Manager . . . 98
Virtual machine templates . . . 98
VMM storage . . . 99
VMM networking . . . 101
Adding a WDS to VMM . . . 105
VMM host groups . . . 106

Chapter 4 Active Directory . . . 109

Managing Active Directory . . . 109
Remote rather than local administration . . . 110
Active Directory Administrative Center . . . 110
Active Directory Users and Computers console . . . 113
Active Directory Sites And Services console . . . 115
Active Directory Domains and Trusts console . . . 115
Group Policy Management console . . . 116
Domain controllers . . . 116
Deployment . . . 117
Server Core . . . 121
Virtualized domain controllers . . . 121
Global catalog servers . . . 122
Decommissioning a domain controller . . . 122
Read Only Domain Controllers . . . 123
Virtual domain controller cloning . . . 126
AD DS structure . . . 127
Domains . . . 127
Multidomain Active Directory environments . . . 128

Domain trees . . . 128
Intra-forest authentication . . . 129
Domain functional levels . . . 129
Forests . . . 131
Account and resource forests . . . 131
Organizational units . . . 131
Flexible Single Master Operations roles . . . 132
Trust relationships . . . 135
Managing sites . . . 141
Managing replication . . . 147
Accounts . . . 151
User accounts . . . 151
Computer accounts . . . 152
Group accounts . . . 153
Default groups . . . 153
Service accounts . . . 156
Group Policy . . . 161
GPO management . . . 161
Policy processing . . . 166
Loopback processing . . . 169
Group Policy preferences . . . 170
Administrative templates . . . 172
Reverting settings configured by Group Policy . . . 173
Active Directory database optimization . . . 174
Active Directory snapshots . . . 174
Active Directory backup . . . 175
Restoring deleted items . . . 176
Active Directory Recycle Bin . . . 178
Authoritative restore . . . 179
Active Directory snapshots . . . 181
Managing AD DS with PowerShell . . . 182
Active Directory module . . . 182
Group Policy module . . . 185
ADDSDeployment module . . . 186

Chapter 5 DNS, DHCP, and IPAM . . . 189

DNS . . . 189
DNS zone types . . . 189
Zone delegation . . . 193
Forwarders and conditional forwarders . . . 193
Stub zones . . . 195
GlobalNames zones . . . 195
Resource records . . . 196
Zone aging and scavenging . . . 197

DNSSEC . . . 198
DNS event logs . . . 199
DNS options . . . 200
Delegated administration . . . 204
Managing DNS with PowerShell . . . 204
DHCP . . . 206
Scopes . . . 207
Server and scope options . . . 208
Reservations . . . 208
DHCP filtering . . . 209
Superscopes . . . 209
Multicast scopes . . . 210
Split scopes . . . 210
Name protection . . . 210
DHCP failover . . . 211
DHCP server authorization . . . 212
DHCP relay agent . . . 213
Managing DHCP with PowerShell . . . 214
IPAM . . . 216
Deploy IPAM . . . 216
Configure server discovery . . . 217
IPAM administration . . . 217
Managing IPAM with PowerShell . . . 219

Chapter 6 Hyper-V . . . 223

Dynamic memory . . . 224
Smart paging . . . 225
Resource metering . . . 226
Guest integration services . . . 226
Generation 2 VMs . . . 227
Enhanced Session Mode . . . 228
Discrete Device Assignment . . . 228
GPU partitioning . . . 230
VM resource groups . . . 231
VM CPU groups . . . 232
Hypervisor scheduling types . . . 232
Nested virtualization . . . 233
Nested virtualization dynamic memory . . . 233
Nested virtualization networking . . . 234
PowerShell Direct . . . 234
HVC for Linux . . . 235
Virtual hard disks . . . 235
Fixed-size disks . . . 236
Dynamically expanding disks . . . 236

Differencing disks 236
Hot-add virtual hard disks....237
Modifying virtual hard disks....237
Pass-through disks....238
Managing checkpoints....239
Virtual Fibre Channel adapters 240
Storage QoS....240
Hyper-V storage optimization....241
Deduplication 241
Storage tiering 241
Hyper-V virtual switches 242
External switches 242
Internal switches....242
Private switches 243
Virtual machine network adapters....243
Optimizing network performance 244
Bandwidth management....244
SR-IOV 244
Dynamic virtual machine queue 244
Virtual machine NIC teaming....245
Virtual machine MAC addresses 245
Network isolation 246
Hyper-V replica 246
Configuring Hyper-V replica servers 247
Configuring VM replicas 247
Replica failover 248
Hyper-V replica broker....249
Hyper-V failover clusters 249
Hyper-V host cluster storage 249
Cluster quorum....250
Cluster networking 252
Force Quorum Resiliency....252
Cluster Shared Volumes 253
Preferred owner and failover settings 253
Hyper-V guest clusters....253
Using GPU-P with clusters....254
Hyper-V guest cluster storage 255
Shared virtual hard disk 255
Hyper-V VHD Sets 256
Live migration 256
Storage migration 258
Exporting, importing, and copying VMs 258
Exporting and migrating VMs with virtual TPMs....259
VM Network Health Detection 260

VM drain on shutdown. . . . 261
Domain controller cloning . . . 261
Dynamic Processor Compatibility Mode . . . 262
Shielded virtual machines . . . 263
Managing Hyper-V using PowerShell . . . 263

Chapter 7 Storage . . . 269

Storage spaces and storage pools . . . 269
Storage pools . . . 270
Storage space resiliency . . . 274
Storage space tiering . . . 275
Thin provisioning and trim . . . 277
Creating virtual disks . . . 279
Storage Spaces Direct . . . 280
Storage Replica . . . 288
Supported configurations . . . 289
Configuring replication . . . 290
Configuring SMB . . . 293
SMB compression . . . 294
SMB encryption . . . 295
SMB signing . . . 296
SMB NTLM blocking . . . 297
SMB over QUIC . . . 297
SMB Direct . . . 299
iSCSI . . . 299
Server for NFS . . . 303
Deduplication . . . 305
Storage Quality of Service . . . 307
ReFS . . . 308
Storage-related PowerShell cmdlets . . . 310
Deduplication . . . 310
iSCSI . . . 310
iSCSITarget . . . 311
NFS . . . 311
Storage . . . 312
Storage Replica . . . 315

Chapter 8 File servers . . . 317

Shared folder permissions . . . 318
Using File Explorer . . . 319
Windows Admin Center . . . 320
Server Manager . . . 321
File Server Resource Manager . . . 324
Folder-level quotas . . . 324
File screens . . . 326

Storage reports . . . 330
File classification . . . 332
File management tasks . . . 334
Access-denied assistance . . . 336
Distributed File System . . . 337
DFS namespace . . . 337
DFS replication . . . 340
BranchCache . . . 343
SMB over QUIC . . . 346
Certificate requirements . . . 346
Configuring the file server for SMB over QUIC . . . 348
Configure SMB-over-QUIC client access control . . . 348
PowerShell commands . . . 349
Shared folder cmdlets . . . 349
File Server Resource Manager cmdlets . . . 350
BranchCache cmdlets . . . 351
DFS cmdlets . . . 353
Dynamic Access Control cmdlets . . . 354

Chapter 9 Azure Arc and hybrid services . . . 355

Microsoft Entra ID . . . 355
Microsoft Entra Connect . . . 355
Microsoft Entra Cloud Sync . . . 368
Self-Service Password Reset . . . 372
Microsoft Entra Password Protection . . . 374
Understanding Entra identities . . . 375
Azure Arc–enabled servers . . . 382
Onboarding . . . 383
Virtual machine extensions . . . 387
Azure Policy . . . 388
Azure Automation and Hybrid Runbook Workers . . . 389
Azure network adapter . . . 390
Azure File Sync . . . 391
Create Azure File Sync Service . . . 391
Create sync groups . . . 392
Create cloud endpoints . . . 392
Register servers . . . 393
Create server endpoints . . . 393
Configure cloud tiering . . . 394
Monitor File Sync . . . 394
Migrate DFS to Azure File Sync . . . 395

Chapter 10 Windows Server in Azure . . . 397

Windows Server IaaS VMs . . . 397
Creating Azure IaaS VMs . . . 398
Login with Entra ID . . . 401

IaaS VM networking 401
IaaS virtual networks 401
IP addressing 403
Network Security Groups 405
Default outbound access 406
VPNs and IaaS virtual networks 406
IaaS VM administration 407
Windows Admin Center 407
Remote PowerShell 409
Azure Bastion 409
Just In Time VM Access 410
IaaS VM operations 411
Azure Automanage 411
Azure Monitor 412
Resizing a VM 414
IaaS VM backup 415
IaaS VM encryption 416
Azure Site Recovery 417
Entra Domain Services 419
Deploying Entra Domain Services 420
Entra Domain Services domain join 422
Integrate AD DS and Entra Domain Services 423
Create a forest trust between on-premises AD DS and Entra Domain Services 424
Managing the Entra Domain Services Active Directory Domain Services instance 425

Chapter 11 Windows Subsystem for Linux 427

Linux on Windows Server 427
Installing WSL 427
WSL 2.0 429
WSL networking 430
Configuring port forwarding for WSL 430
Configure mirrored networking for WSL 431

Chapter 12 Hardening Windows Server 433

Hardening Windows Server 433
User rights 434
Service accounts 438
Just Enough Administration 441
Privileged Access Management 447
Windows Local Administrator Password Solution 451
Advanced auditing 453
Windows Firewall with Advanced Security 455
Shielded VMs 465
Guarded fabric 468

Chapter 13 Hardening Active Directory 473

Hardening domain controllers 474
Least-privilege 476
Role-Based Access Control 477
Password policies 479
Account security options 480
Protected accounts 482
Authentication policies silos 483
Configure msDS-MachineAccountQuota 485
Constrained delegation 485
Configure Kerberos-constrained delegation 486
Configure resource-based constrained delegation 486
Disable NTLM 486
Enforce LDAP signing 487
Enforce LDAP channel binding 488
LSASS as a protected process 488
Block server operators from scheduling tasks 489
KRBTGT account password 489
Enforce AES for Kerberos 490
Auditing, logging, and monitoring 491
Regular backup of Active Directory 492
Enhanced Security Administrative Environment forest 492

Chapter 14 Security systems and services 497

Security Compliance Toolkit 498
Policy Analyzer tool 498
Local Group Policy Object tool 500
Attack Surface Analyzer 500
OSConfig 501
Control Flow Guard 503
Virtualization-based security 504
Hypervisor-Protected Code Integrity 505
Windows Defender Application Control 506
Credential Guard 508
Controlled Folder Access 510
Exploit Protection 512
Attack surface reduction rules 515
Windows Defender 517
Microsoft Defender SmartScreen 518
Entra ID Password Protection 519
Entra ID Password Protection requirements 520
Entra ID Password Protection deployment 520

Chapter 15 Internet Information Services 523

Managing sites 523
Adding websites 524
Test certificates 527
Virtual directories 527
Modifying site settings 528
Adding web applications 529
Configuring TLS certificates 529
Enable TLS 1.3 531
Enable HTTP/3 on IIS 532
Site authentication 532
Modifying custom error response 534
Adding or disabling the default document 535
Directory browsing 536
IP address and domain name filtering 536
URL authorization rules 538
Request filters 539
Application pools 541
Creating application pools 541
Configuring application pool recycling settings 542
IIS users and delegation 544
IIS user accounts 545
Delegating administrative permissions 545
IIS configuration backup and recovery 546
Managing FTP 547
Managing IIS using PowerShell 549

Chapter 16 Containers 553

Container concepts 553
Isolation modes 555
Process isolation 555
Hyper-V isolation 556
Managing containers with Docker 556
Installing Docker 557
Daemon.json 557
Retrieving container OS image 560
Container registries and images 560
Managing containers 562
Starting a container 562
Modifying a running container 563
Creating a new image from a container 563
Using Dockerfiles 564
Managing container images 565
Service accounts for Windows containers 565
Applying updates 566

Container networking 567
NAT 568
Transparent 570
Overlay 570
Layer 2 Bridge 571

Chapter 17 Clustering and high availability 573

Failover clustering 573
Cluster quorum modes 574
Cluster storage and cluster shared volumes 576
Cluster networks 576
MPIO 577
Cluster Aware Updating 577
Failover and preference settings 578
Multisite clusters 579
Stretch clusters 580
Cloud Witness 581
Storage Spaces Direct Campus Clusters 582
Virtual machine failover clustering 583
Rolling upgrades 584
Workgroup clusters 586
Cluster sets 587
Managing failover clustering with PowerShell 588
Network Load Balancing 591
Network Load Balancing prerequisites 591
NLB cluster operation modes 592
Managing cluster hosts 593
Port rules 594
Filtering and affinity 594
Managing NLB with PowerShell 595

Chapter 18 Active Directory Certificate Services 597

CA types 597
Enterprise CA 599
Standalone CAs 608
Certificate revocation lists 612
CRL distribution points 612
Authority Information Access 613
Revoking a certificate 613
Publishing CRLs and delta CRLs 615
Certificate Services role services 617
Certificate templates 618
Template properties 619
Adding and editing templates 625
Certificate autoenrollment and renewal 626

CA management 628
Handling certificate requests 630
CA backup and recovery 631
Key archiving and recovery 633
CAPolicy.inf 638
Managing Certificate Services using PowerShell 639
Managing Certificate Services using Certutil.exe and Certreq.exe 641

Chapter 19 Active Directory Federation Services 643

AD FS components 643
Claims, claim rules, and attribute stores 644
Claims provider 645
Relying party 645
Relying party trust 645
Claims provider trust 646
Configuring certificate relationship 647
Attribute stores 648
Claim rules 648
Relying party trust claim rules 649
Claims provider trust claim rules 649
Configure Web Application Proxy 650
Workplace Join 653
Multifactor authentication 655
Managing AD FS with PowerShell 656
Managing Web Application Proxy with PowerShell 659

Chapter 20 Active Directory Rights Management Services 661

Dynamic Access Control 661
Configuring Group Policy to support DAC 662
Configuring user and device claims 663
Configuring resource properties 664
Central access rules 666
Central access policies 667
Staging 668
Access Denied Assistance 669
Installing AD RMS 670
AD RMS certificates and licenses 671
AD RMS templates 672
AD RMS Administrators and Super Users 675
Trusted User Domains and Trusted Publishing Domains 677
Exclusion policies 677
Apply AD RMS templates automatically 677
Managing AD RMS with Windows PowerShell 678

Chapter 21 Routing and remote access 681

Remote Desktop Gateway 681
RD Gateway connection and resource policies 682
Configuring server settings 683
Configuring clients to use RD Gateway 683
Virtual private networks 685
IKEv2 Always On VPN protocol 685
SSTP VPN protocol 687
L2TP/IPsec protocols 687
PPTP VPN protocol 687
VPN authentication 688
Deploying a VPN server 688
Disable VPN protocols 689
Enable VPN protocols 689
Granting Access to a VPN server 690
LAN routing 693
Network Address Translation (NAT) 694
DHCP Relay Agent 695
DirectAccess 696
DirectAccess topologies 697
DirectAccess server 698
Network Location Server 700
Configuring DirectAccess 700
Managing Remote Access using PowerShell 704

Chapter 22 Remote Desktop Services 707

Deployment 707
Remote Desktop Connection broker 709
Deployment properties 710
Remote Desktop Session Host 711
Session collection settings 712
Personal session desktops 714
RemoteApp 714
Group Policy configuration 715
Remote Desktop Virtualization Host 719
Virtual machine preparation 720
Virtual desktop collections 721
Pooled virtual desktops 722
Personal virtual desktops 722
DDA and RemoteFX 723
Remote Desktop Web Access 723
Remote Desktop licensing 723
Installing RDS CALs 724
Activating a license server 725
Managing Remote Desktop Services using PowerShell 725

Chapter 23 Monitoring and maintenance 729

Data collector sets 729
Alerts 731
Event Viewer 731
Event log filters 731
Event log views 732
Event subscriptions 733
Event-driven tasks 734
Network monitoring 735
Resource Monitor 735
Packet Monitor 736
Azure Monitor 737
Windows Server Backup 739
Backup locations 740
Backing up data 741
Role- and application-specific backups 742
Restore from backups 742
Restore to an alternative location 743
Azure Backup 743
Preparing Azure Backup 744
Backing up data to Azure Backup Agent 745
Restore from Azure Backup 745
Vssadmin 746
Windows Server Update Services 747
Products, security classifications, and languages 748
Autonomous and replica modes 748
Update files 748
WSUS security roles 749
WSUS groups 749
WSUS policies 750
Deploying updates 751
Automatic approval rules 751
Azure Update Manager 753
Monitoring- and maintenance-related PowerShell cmdlets 754
WSUS-related PowerShell cmdlets 755

Chapter 24 Upgrade and migration 757

Supported upgrade and migration paths 757
Upgrading roles and features 758
Converting the evaluation version to a licensed version 759
Upgrading editions 760
Windows Server Migration Tools 760

Active Directory 763
FRS to DFSR migration 764
Migrating to a new forest 765
Active Directory Certificate Services 768
Preparation 770
Migration 771
Verification and post-migration tasks 772
DNS 772
DHCP 773
Preparing to migrate DHCP 774
Migration 776
Verification and post-migration tasks 777
File and storage servers 777
Migrate file servers using Storage Migration Service 777
Migrate file and storage servers using WSMT 783

Chapter 25 Troubleshooting 787

Troubleshooting methodology 787
Redeployment 788
Symptoms and diagnosis 789
Dependencies 790
Ranking hypothetical solutions 791
Applying solutions 792
Using Windows Debugger 793
Crash dump analysis 793
Analyze performance problems 795
Using Driver Verifier to diagnose suspect drivers 796
Windows Memory Diagnostic 796

Chapter 26 Hosting large language models on Windows Server 799

Ollama on Windows Server 799
Using Ollama from the command line 801
Integrating Ollama into VS Code 802
Using Open WebUI with Ollama 802
Azure Foundry Local on Windows Server 804
Using Foundry Local from the command line 804
Configuring Foundry Local as a service 806
Use Open WebUI with Foundry Local 806

Index 809

About the Author

Orin Thomas is a Principal Cloud Advocate at Microsoft. A recognized cloud and data center subject matter expert, he has written more than 40 books for Microsoft Press and has been writing books on Windows Server for more than 20 years. He works with the Windows Server product group at Microsoft to create product documentation and training materials. He is the architect of the Windows Server Hybrid Administrator Associate certification.

Acknowledgments

I'd like to thank Shourav Bose, Rick and Charlotte Kughen, Vince Averello, and Loretta Yates for the assistance they provided in bringing this text to print. For the last seven years, I've been working with the Windows Server product team and other people at Microsoft and can't express how useful it has been to seek the advice of Ned Pyle, Jeff Woolsey, Robin Harwood, Dan Cuomo, Rob Hindman, Ben Armstrong, James Seymour, Tony Jamieson, Rob Barefoot, Elden Christiensen, Theo Tran, Yash Shekar, Rick Claus, and too many others to note. Their help has been invaluable for helping me understand and know how to explain Windows Server and other Microsoft technologies.

Finally my endless and eternal gratitude and love to my beautiful partner, Lynette.

Introduction

This book is primarily written for IT professionals who work with Windows Server operating systems on a regular basis. As such, it's likely that Windows Server 2025 isn't the first version of Windows Server that you've been responsible for managing. This is because the majority of Windows Server administrators have been working with some version of the operating system for more than a decade, with a good percentage having experience going back to the days of Windows NT 4.

This book is also written under the assumption that as an experienced IT professional, you know how to use a search engine or LLM chatbot to find relevant technical information. This leads to an obvious question: "Why would I buy a book if I can find relevant technical information by asking an LLM to explain this to me?" The answer is that even though you may be good at tracking down technical information and have experience filtering useful knowledge from wildly inaccurate guesses, you can only ask an AI for information about something if you have an idea about it in the first place. In Douglas Adam's *Hitchhiker's Guide to the Galaxy*, Deep Thought—the ultimate AI mega-computer—after eons of cogitation, provided the famous answer 42. When asked to provide some context as to what 42 actually meant, Deep Thought had to design an even bigger computer to be built by the planet engineers of Magrathea to calculate the nature of the actual question. This all is a roundabout way of saying if you don't know about a role, feature, or bit of functionality, how can you ask an LLM to explain it to you? Just by flipping through the pages of this book, you're likely to encounter things you weren't aware of and wouldn't have thought to ask about.

When presenting at conferences and user groups on Windows Server topics, I regularly encounter IT professionals who have worked with Windows Server for many years who are unaware of specific functionality or techniques related to the product, even if that functionality or technique has been available for many years. This can even be true with people I work with on the Windows Server product team who are deeply knowledgeable about their specific role or service but might not know much about other functionality they haven't worked on. This is because Windows Server includes so many roles, features, and moving parts that you're unlikely to know everything about the operating system.

My aim with this book is to give you comprehensive coverage so that you'll learn things that you didn't know or simply missed, possibly because when you've been solving a critical problem, you've been focused on the specifics of that problem and haven't had time to explore every facet of what the Windows Server operating system is capable of. I'm constantly adding new things to my notes as I learn them, and even though I've been writing Windows Server books for more than 20 years and published several million words on the subject, there are still interesting facets of Windows Server that I and members of the product team discover on a regular basis.

Notes on mature roles and features

Windows Server includes a large number of roles and features that no longer receive substantive updates but are still supported for the lifetime of the server. Sometimes these features are listed as deprecated. Deprecated features are still in the operating system but may be removed at some point in the future. It's important to note that if the operating system ships with a feature, it will be supported for the lifetime of the operating system.

Although a role or feature may be deprecated, it doesn't mean it's going away. WINS is still in the operating system, and it's fair to say that few organizations have needed that functionality for more than 20 years.

Other features have reached a level of maturity where there really isn't much more that needs to be added. We're more likely to see improvements in Hyper-V and Active Directory in future releases of Windows Server than we are to see any changes in services like DHCP, basic file shares, and DNS. Over the coming years and decades, we'll see incremental, rather than revolutionary, improvements to Windows Server.

Conventions

The following conventions are used in this book:

- **Boldface** type is used to indicate text that you type.
- *Italic* type is used to indicate new terms, measures, calculated columns, tables, and database names.
- The first letters of the names of dialogs, dialog elements, and commands are capitalized. For example, the Save As dialog.
- The names of ribbon tabs are given in ALL CAPS.
- Keyboard shortcuts are indicated by a plus sign (+) separating the key names. For example, Ctrl+Alt+Delete means that you press the Ctrl, Alt, and Delete keys at the same time.

Errata, updates, and book support

We have made every effort to ensure the accuracy of this book and of its companion content. If you find an error, please submit it to us at

MicrosoftPressStore.com/windowsinsideout/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit

MicrosoftPressStore.com/Support

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to

support.microsoft.com.

CHAPTER 4

Active Directory

Managing Active Directory 109
Domain controllers 116
AD DS structure 127
Managing Sites 141
Managing Replication 147
Accounts 151
Group Policy 161
Active Directory database optimization 174
Active Directory snapshots 174
Active Directory backup 175
Restoring deleted items 176
Managing AD DS with PowerShell 182

Active Directory, the identity glue that binds on-premises Microsoft networks, is at the center of almost all on-premises networks. Although each computer can have its own unique individual user and service accounts, Active Directory provides a central user, computer, and service account store.

But Active Directory is more than an identity store; it can also be used to store data for Active Directory–aware applications. One example of this is Microsoft Exchange Server, which stores server configuration information in Active Directory. Other applications, such as Microsoft Configuration Manager (formerly System Center Configuration Manager), are also highly dependent on Active Directory.

In this chapter, we look at managing Active Directory. We also cover deploying domain controllers, forests, domains, sites, Group Policy, user, computer, and service accounts, and a host of other Active Directory administrative tasks.

Managing Active Directory

Domain controllers are one of, if not the, highest value target for attackers on your network. An attacker who is able to take control of a domain controller has control over every domain-joined computer in the organization. Having control of a domain controller, which is also known as "domain dominance," means having control of all the authentication and authorization processes in the domain.

While we will discuss server hardening in more detail in Chapter 12 and Active Directory hardening in Chapter 13, one strategy for increasing server security is to reduce the attack surface. Where possible, you should deploy roles on computers installed in the Server Core configuration because this configuration has a smaller attack surface than a server that includes desktop

components. Server Core is a great option for domain controller deployment because it provides a reduced attack surface, which strengthens the security of the installation.

Remote rather than local administration

You should perform Active Directory management tasks remotely using Windows Admin Center, management consoles, or PowerShell rather than signing on to the domain controller directly using RDP. If you're doing all your administrative tasks remotely, it won't make any difference to you that you've deployed the domain controller in the Server Core configuration. Using remote consoles also reduces the chance of malware being introduced to the domain controller. There are countless stories of organizations having their security compromised because an administrator signed in to a server using Remote Desktop, went to download a utility from the Internet using the built-in web browser, and ended up with more than they bargained for in terms of malware because they weren't careful about their browsing destinations.

There are a number of consoles that you can use to perform Active Directory administrative tasks. These include the following:

- Active Directory Administrative Center
- Active Directory Users And Computers
- Active Directory Sites And Services
- Active Directory Domains And Trusts
- Group Policy Management Console

Windows Admin Center provides some Active Directory administrative functionality, but not nearly enough that AD administrators could use it as their primary tool for managing Active Directory.

Active Directory Administrative Center

Active Directory Administrative Center was introduced with Windows Server 2008 R2, but it never really caught on as the primary method of managing Active Directory for most administrators. Active Directory Administrative Center (ADAC) allows you to manage users, computers, and service accounts to perform tasks with the Active Directory, such as the Recycle Bin, and to manage functionality, such as Dynamic Access Control.

Active Directory Administrative Center has better search functionality than the other consoles listed in this chapter, which haven't substantively changed since the release of Windows 2000.

You can use Active Directory Administrative Center to manage the following:

- User, computer, and service accounts
- Domain and forest functional level

- Fine-grained password policies
- Active Directory Recycle Bin GUI
- Authentication policies
- Dynamic Access Control

ADAC is built on PowerShell, meaning that it provides a graphical interface to build and enact PowerShell cmdlets. You can use the PowerShell History Viewer, shown in Figure 4-1, to see which cmdlets were used to carry out a task that you configured in the GUI. This simplifies the process of automating tasks because you can copy code straight out of the PowerShell history and then paste it into tools such as PowerShell ISE or Visual Studio Code.

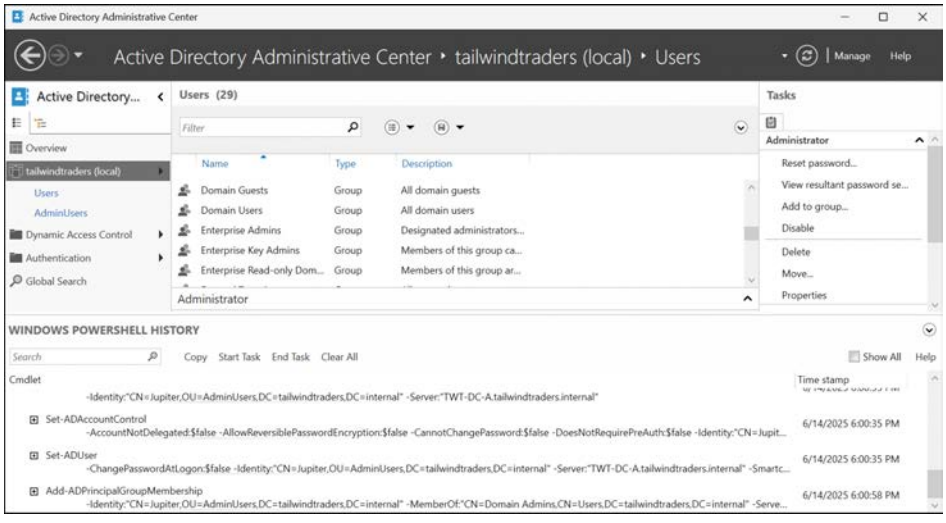

Figure 4-1 Active Directory Administrative Center

One of the most useful elements of Active Directory Administrative Center is the search functionality. You can use this functionality to locate accounts that might require further attention, such as users who haven't signed in for a certain period of time, users configured with passwords that never expire, or users with locked accounts. Using the Add Criteria option in the Global Search node of the Active Directory Administrative Center, you can search based on the following criteria:

- Users with disabled/enabled accounts
- Users with expired passwords
- Users whose passwords have an expiration date or no expiration date

- Users with enabled but locked accounts
- Users with enabled accounts who have not signed in for more than a given number of days
- Users with a password expiring in a given number of days
- Computers running as a given domain controller type
- Last modified between given dates
- Object type is `user/inetOrgPerson/computer/group/organizational unit`
- Directly applied password settings for a specific user
- Directly applied password settings for a specific global security group
- Resultant password settings for a specific user
- Objects with a given last known parent
- Resource property lists containing a given resource property
- Name
- Description
- City
- Department
- Employee ID
- First name
- Job title
- Last name
- `SamAccountName`
- State/province
- Telephone number
- UPN
- Zip/postal code

- Phonetic company name
- Phonetic department
- Phonetic display name
- Phonetic first name
- Phonetic last name

There are several tasks that you can't do with Active Directory Administrative Center or with PowerShell, such as running the Delegation Of Control Wizard.

Active Directory Users and Computers console

The Active Directory Users and Computers console is the one that many system administrators use to perform basic AD-related tasks. They use this console primarily out of habit because almost all functionality present in this console is also present in the Active Directory Administrative Center. Active Directory Users and Computers has been around since the days of Windows 2000 Server.

Active Directory Users and Computers allows you to perform tasks, including

- Running the Delegation Of Control Wizard
- Administering different domains within the forest
- Selecting which domain controller or LDAP port the tool connects to
- Finding objects within the domain
- Raising the domain functional level
- Managing the RID Master, PDC Emulator, and Infrastructure Master FSMO role locations
- Creating and editing the properties of
    - Computer accounts
    - User accounts
    - Contacts
    - Groups
    - `InetOrgPerson`
    - `msDS-ShadowPrincipalContainers`

- msDS-DelegatedManagedServiceAccount
- msImaging-PSPs
- MSMQ Queue Alias
- Organizational unit
- Printers
- Shared Folder

- Resultant Set of Policy planning

The View Advanced Features function allows you to see more details of the Active Directory environment. You enable this from the View menu of Active Directory Users And Computers. Enabling this view allows you to see containers that aren't visible in the standard view. If you've ever read a set of instructions that tell you to locate a specific object using Active Directory Users And Computers, and you haven't been able to find that object, chances are that you haven't enabled the View Advanced Features option as shown in Figure 4-2.

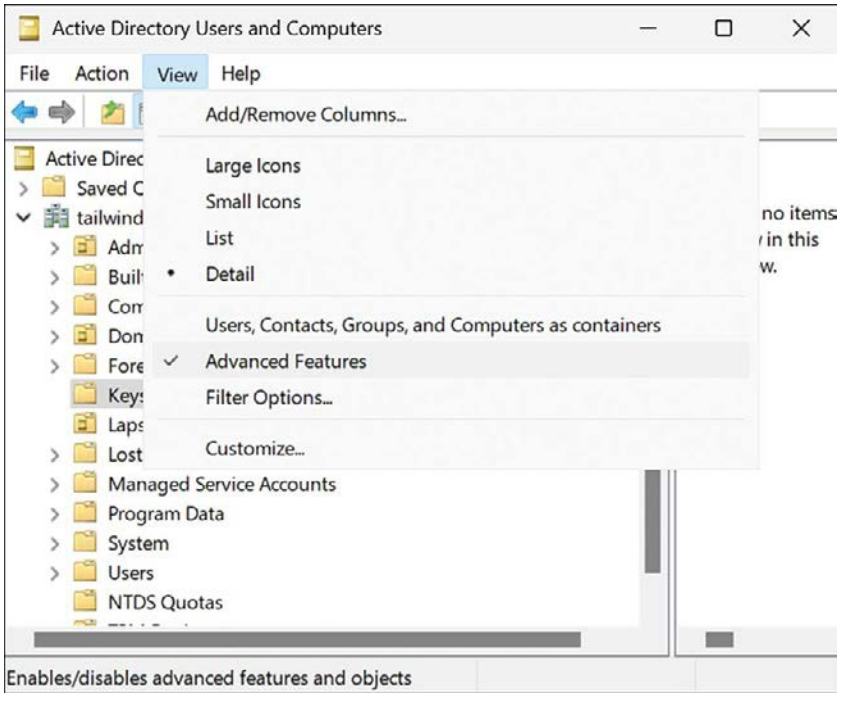

Figure 4-2 Active Directory Users and Computers Advanced Features

The Delegation Of Control Wizard is only available in Active Directory Users And Computers. This wizard allows you to delegate control over the domain and organizational units (OU). For example, you use this wizard to delegate the ability for a specific group to reset user passwords in an OU. This wizard is useful when you want to delegate some privileges to a group of IT ops staff, but you don't want to grant them all the privileges that they'd inherit if you made them a member of the Domain Admins group. You'll learn more about delegating permissions in Chapter 13, "Hardening Active Directory."

Active Directory Sites And Services console

You use the Active Directory Sites And Services console to manage Active Directory sites, which indirectly allows you to control a number of things, including replication traffic and which server a client connects to when using products such as Exchange Server. Sites are configured for the forest, with each domain in the forest sharing the same set of sites.

An Active Directory site is a collection of TCP/IP subnets. Sites allow you to define geographic locations for Active Directory on the basis of TCP/IP subnets. You can have multiple TCP/IP subnets in a site. You should put subnets together in a site where the hosts in that site have a high-bandwidth connection to each other. Usually, this means being in the same building, but it could also be multiple buildings with very-low-latency gigabit links between them.

You'll learn more about Active Directory sites and replication later in this chapter.

Active Directory Domains and Trusts console

You use the Active Directory Domains And Trusts console to configure and manage trust relationships. By default, all domains in a forest trust each other. Your primary use of this console is to create trust relationships between

- Domains in separate forests
- Separate forests
- Kerberos V5 realms

When creating a trust, you can choose between the following types:

- **One-Way: Incoming** In this trust relationship, your local domain or forest is trusted by a remote domain or forest.
- **One-Way: Outgoing** In this trust relationship, your local domain or forest trusts a remote domain or forest.
- **Two-way** In this trust relationship, your local domain or forest trusts (and is trusted by) a remote domain or forest.

You'll learn about trust relationships later in this chapter.

Group Policy Management console

The Group Policy Management console, shown in Figure 4-3, is the primary method by which Group Policy is managed in a standard Windows Server environment. This tool allows you to view Group Policy items from the forest level down. It provides information on which GPOs are linked at the domain, site, and OU levels. You can see a list of all GPOs in a domain under the Group Policy Objects node. There is also a WMI Filters node that contains all WMI filters configured for the domain, a Starter GPOs node that contains all starter GPOs, a Group Policy Modeling node, and a Group Policy Results node. By right-clicking a GPO and selecting Edit, you can edit a GPO in the Group Policy Management Editor. You can output information about a GPO, including which settings are configured and where the GPO is linked, to a file in HTML format using the `Get-GPOReport` cmdlet. You'll learn more about managing Group Policy later in this chapter.

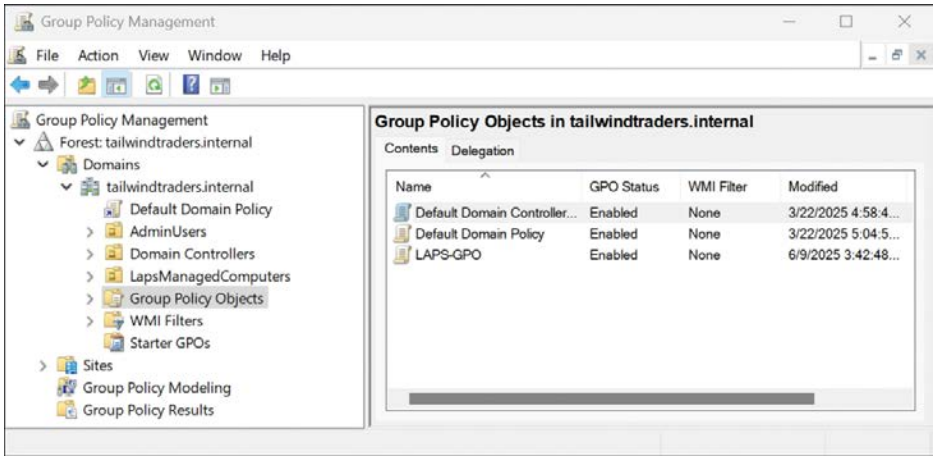

Figure 4-3 Group Policy Management Console

Domain controllers

Domain controllers (DCs) are the heart of Active Directory. Their primary role is to host the Active Directory database, stored in the `ntds.dit` file. Given their importance, you should limit who can sign on locally to a domain controller.

Inside OUT

Make sure you double-up!

Ensure that you have at least two domain controllers in each domain, and make sure you make regular backups and keep some of them offline. In the event that one domain controller fails, the other one is still there to perform all necessary functionality. Imagine you only have one domain controller and you don't have a backup. If that DC fails, you're going to need to rebuild your domain from scratch.

Deployment

Although the wizard for deploying a domain controller has been updated from what it looked like back in Windows Server 2008 R2, the process is still functionally the same. You choose whether you want to

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

To deploy a domain controller, perform the following steps:

1. Using Add Roles and Features in Server Manager, add the Active Directory Domain services role. You need to add this role, shown in Figure 4-4, before you can promote a server to function as a domain controller.

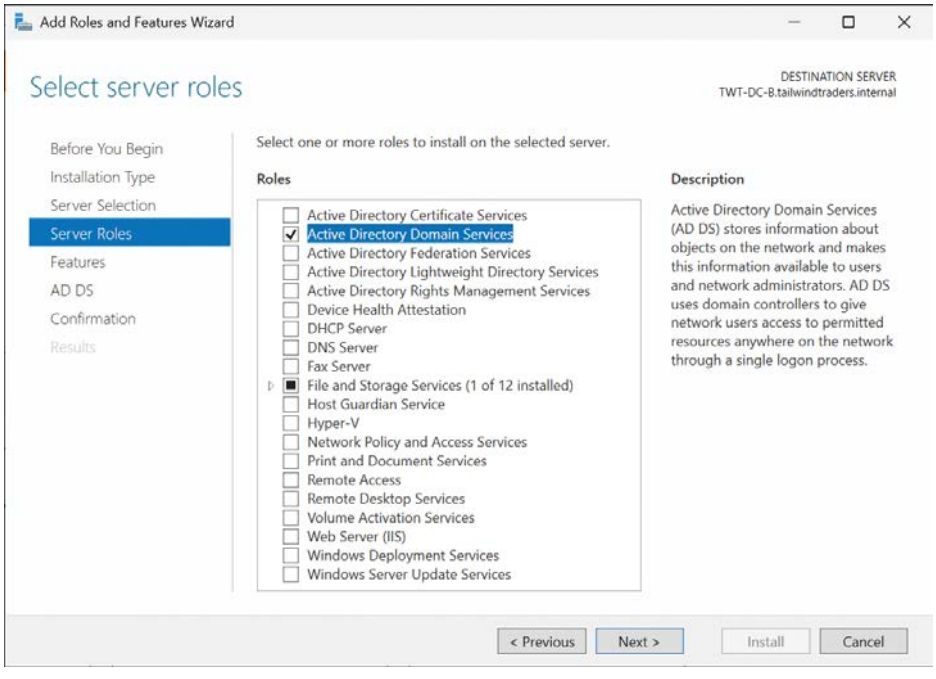

Figure 4-4 Add the Active Directory Domain Services role

2. Once the role files are installed, you'll be able to promote the server to function as a domain controller. You can do this from the Server Manager console by selecting the notification icon and then clicking Promote this server to a domain controller, as shown in Figure 4-5.

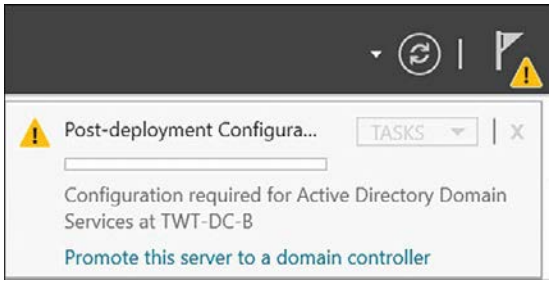

Figure 4-5 Promote this server to a domain controller in Server Manager

3. On the Deployment Configuration page of the Active Directory Domain Services Configuration Wizard, you'll be asked whether you want to add a domain controller to an existing domain, add a new domain to an existing forest, or add a new forest. To add a domain controller to an existing domain, you'll need to have the credentials of a member of the Domain Admins group. To add a new domain to an existing forest, you'll need an account that is a member of the Enterprise Admins group. You can specify this account on the Deployment Configuration page, as shown in Figure 4-6.

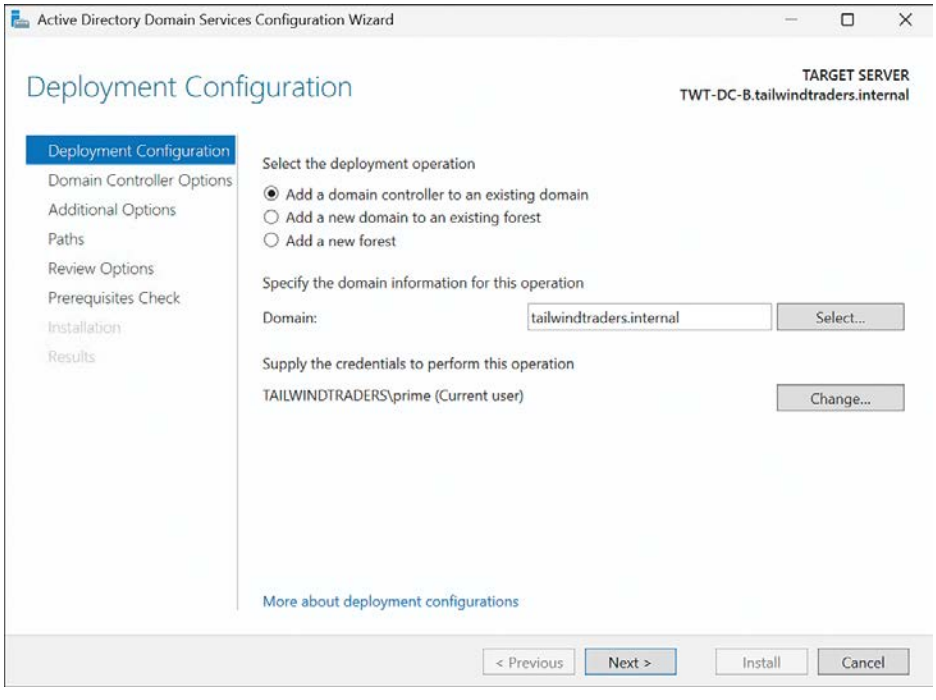

Figure 4-6 Deployment Configuration

If you're adding a domain controller to an existing domain, have the computer domain joined before promoting it. When you add a new domain to an existing forest, choose between adding a child domain or a tree domain. When you add a tree domain, you create a new namespace within an existing forest. For example, you can create the *Adatum.com* domain in the existing *contoso.com* forest. *Contoso.com* remains the root domain of the forest.

Microsoft's recommendation is that you use a registered root domain name, such as *Contoso.com* for the domain name, rather than a nonexternally resolvable domain name like *contoso.internal*. Having a registered externally resolvable domain name simplifies the process when configuring synchronization with Azure AD Connect.

Windows Server supports split DNS, which means that you can configure zones so that a subset of records is resolvable for clients on external networks. Many organizations still use nonresolvable domain names, and you should only take the Microsoft advice into account if you're deploying a new forest or reconfiguring a domain in preparation for synchronizing with Entra in Azure.

When you add a new child domain to an existing forest, you specify the parent domain. For example, you could add the *australia.contoso.com* child domain to the *contoso.com* domain. After you've done that, you can add the *victoria.australia.contoso.com* child domain to the *australia.contoso.com* parent domain. Adding a child domain requires Enterprise Administrator credentials in the forest.

Domain controllers can also host the DNS service and function as global catalog servers. In Windows Server environments, DNS is almost always hosted on domain controllers. You'll learn more about DNS configuration and options in Chapter 5, "DNS, DHCP, and IPAM." Global Catalog servers are covered later in this chapter.

When deploying a domain controller in an environment with multiple sites configured, you can select which site you want the domain controller to belong to. You can change this after deployment using the Active Directory Sites And Services console.

Generally, the default paths for the Database folder, log files folder, and SYSVOL folder are appropriate. The primary reasons to alter this location are for performance reasons or if you have concerns about the amount of storage available on the volume that hosts the Windows Server operating system.

Directory Services Restore Mode passwords

Directory Services Restore Mode (DSRM) allows you to perform an authoritative restore of deleted objects from the Active Directory database. You must perform an authoritative restore of deleted items because if you don't, the restored item is deleted the next time the AD database synchronizes with other domain controllers, where the item is marked as deleted. Authoritative restores are covered later in this chapter. You configure the Directory Services Restore Mode password on the Domain Controller Options page of the Active Directory Domain

Services Configuration Wizard, as shown in Figure 4-7. You can use Windows LAPs, covered in Chapter 12, "Hardening Windows Server," to centrally manage Directory Services Restore Mode Passwords and ensure they're unique for each domain controller.

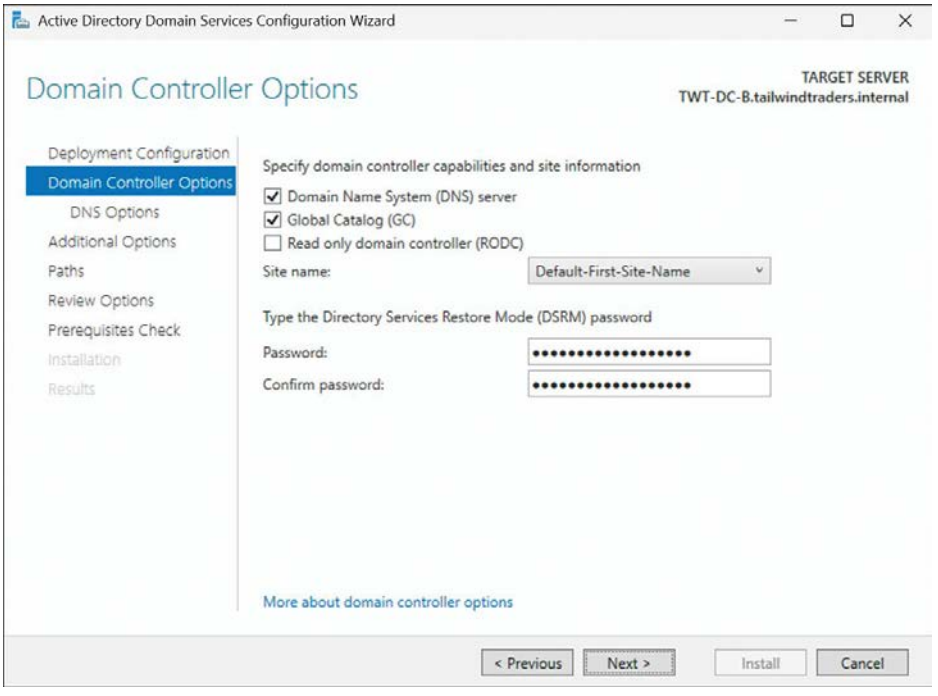

Figure 4-7 Configuring Domain Controller Options

In the event that you forget the DSRM password and you are not using Windows LAPs to manage them, you can reset it by running `ntdsutil.exe` from an elevated command prompt and entering the following command at the `ntdsutil.exe prompt`, at which point you are prompted to enter a new DSRM password:

```
Reset password on server null
```

Advanced installation options

One of the advanced installation options for domain controllers is to install from media. Installing from media gives you the option of prepopulating the AD DS database for a new DC from a backup of an existing DC's AD DS database, rather than having that database populated through synchronization from other domain controllers in your organization. This is very useful when you need to deploy a DC at a remote location that has limited WAN connectivity and you don't want to flood the WAN link with AD DS database synchronization traffic during domain controller deployment. Instead, you ship a backup of the AD DS database to the remote site,

and that backup is used to perform the initial AD DS database population. After the newly installed DC connects to other domain controllers, it performs a synchronization, bringing the database up to date with a much smaller synchronization than what would be required when synchronizing from scratch.

Server Core

As the reduced attack surface area of Server Core deployments makes it more secure, domain controllers—which don't have a GUI dependency—are one of several perfect workloads for Server Core deployments. Microsoft recommends deploying domain controllers using the Server Core deployment option and managing those servers remotely.

To configure a computer running Server Core as a domain controller, you can

1. Remotely connect to the server using the Server Manager console.
2. Run the Add Roles And Features Wizard to remotely install the Active Directory binaries on the server.
3. Run the Active Directory Domain Services Configuration Wizard to promote the computer to a domain controller.

You can also use Windows Admin Center to deploy the AD DS feature, but at the time this book was written, you couldn't configure the feature once it was deployed. As an alternative to using the wizard or console, you can run the following PowerShell commands, either locally or remotely, to install the AD DS binaries and promote the server to a domain controller:

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Install-ADDSDomainController -DomainName contoso.internal -InstallDNS:$True
-credential (Get-Credential)
```

In addition to running this set of commands, you also need to specify a Directory Service Restore Mode password before the computer running Server Core completes the domain controller promotion process. You'll need to use the `Install-ADDSForest` cmdlet if you're installing the first domain in a new forest, as shown here:

```
Install-ADDSForest -DomainName contoso.internal -InstallDNS
```

Virtualized domain controllers

Domain controllers can be run on supported virtualization platforms, including the latest version of VMware and Hyper-V. With the Production Checkpoints feature available in Windows Server 2019 and later Hyper-V, domain controllers can be restored from a checkpoint without causing problems. Microsoft recommends that you run virtualized domain controllers as shielded VMs on a guarded virtualization fabric because this will minimize the chance that a nefarious or compromised virtualization administrator account could be used to access the contents of the DC VM. You can learn more about production checkpoints, shielded VMs, and guarded fabrics in Chapter 6, "Hyper-V."

Global catalog servers

Global catalog servers host a full copy of all objects stored in their host directory and a partial, read-only copy of all other objects in other domains in the same forest. They're used when it's necessary to perform a check of other objects in the forest, such as when a check is performed of a universal group's membership, which could contain members from other domains in the forest.

You can use the Active Directory Sites And Services console to configure a server to function as a global catalog server by right-clicking the NTDS settings of the server. Alternatively, you can run the `Set-ADObject` cmdlet. For example, to configure the DC MEL-DC1 in the `Melbourne-Site` site as a global catalog server, run the following command:

```
Set-ADObject "CN=NTDS Settings,CN=MEL-DC1,CN=Servers,CN=Melbourne-Site,CN=Sites,CN=Confi
guration,DC=Contoso,DC=Internal" -Replace @{options='1'}
```

Decommissioning a domain controller

In some circumstances, you want to remove an existing domain controller from your domain. When you do this, you want to ensure that all traces of the domain controller are removed from Active Directory and DNS. To demote a domain controller when the domain controller is accessible and online, perform the following steps:

1. Ensure that the server you want to demote hosts no FSMO roles. You'll learn how to locate and transfer these roles later in the chapter.
2. In Server Manager, go to Manage and then select Remove Roles and Features.
3. Select the server you want to demote and click Next.
4. On the Remove Server Roles screen, uncheck Active Directory Domain Services (AD DS) and choose Remove Features.
5. The wizard will prompt you to demote the domain controller. Click on Demote This Domain Controller as shown in Figure 4-8.
6. On the credentials page, provide the credentials. You don't need to use the Force The Removal Of This Domain Controller option unless the server is unable to contact the domain or this is the last domain controller in the domain or forest.
7. You'll be promoted on the Warnings page with a checkbox to proceed with removal, and you can't choose Next until you select this option.
8. On the Password page, you'll be asked to provide a password for the default local Administrator account. Unless the domain controller was the last in the domain or forest, the computer will still be domain-joined after the operation.
9. On the Review Options page, you'll be able to click Demote. The server will be restarted automatically upon completion. You can then remove the Active Directory Domain Services role files.

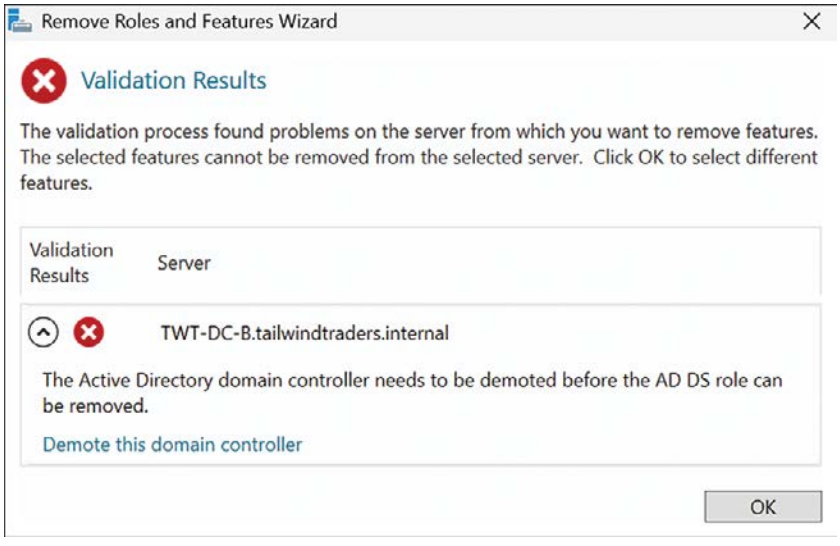

Figure 4-8 Configuring Domain Controller options

If you can't gracefully remove a domain controller because it's offline, forcibly seize any FSMO roles and then delete the domain controller's computer account using Active Directory users and computers. Deleting the account will remove the domain controller's metadata from Active Directory and DNS.

To remove server metadata using ntdsutil, issue the following command, where `<ServerName>` is the distinguished name of the domain controller whose metadata you want to remove from Active Directory:

```
Ntdsutil "metadata cleanup" "remove selected server <ServerName>"
```

Read Only Domain Controllers

Read Only Domain Controllers (RODC) are a special type of domain controller. They host a read-only copy of the AD DS database. Rather than storing the passwords for all users in the domain, RODCs only store the passwords of a specific set of accounts that you configure. The first domain controller in a new domain or forest cannot be an RODC.

The justification for RODCs is that DCs sometimes need to be located in places where servers have poor physical security and might be stolen. For example, many organizations had branch offices where servers were located under someone's desk. A good rule of thumb is that you should consider a location insecure if it is accessible to anyone other than IT. If a janitor can pull out a computer's power cord to power a vacuum cleaner, the computer isn't in a secure location.

If a server that hosts a domain controller is stolen, the best practice is to reset the account passwords that might have been compromised because it's possible, with the correct tools, to extract passwords from the AD DS database if you have direct access to it. If an ordinary DC is stolen, you would, in theory, need to reset the passwords of every account in the domain because you could never be sure that someone hadn't gained access to the Active Directory database and found a way to extract the passwords of people in your organization.

With shielded VMs and shielded fabrics, it's possible to run a DC in a manner where the VM itself is protected by encryption. In the event that the host server is stolen, the AD DS database cannot be recovered because the contents of the virtualization server's storage are encrypted using BitLocker.

Inside OUT

RODC and Writeable DC Deployment

Concerns about the physical security of a DC are the primary reason to deploy an RODC, so it's extremely unlikely that you would have both an RODC and a writable DC at the same site. RODCs are for sites where the domain controller was once placed in a location that wasn't secure. Though if you do have concerns about the security of a location, it's probably not a great idea to deploy a domain controller at that location!

Passwords on RODCs

One of the most important steps in configuring an RODC is limiting which passwords can be replicated down to the server from a writable domain controller. The default configuration of an RODC has it store almost everything from Active Directory except for user and computer account passwords. In the event that a user or computer account needs to be authenticated against Active Directory, the RODC acts as a proxy for a writable Windows Server DC. The authentication occurs, but it depends on the WAN link to be functional because if you could host a writable DC locally, you wouldn't need the RODC.

Although you can configure an RODC to not cache any passwords locally, you can configure an RODC to cache the passwords of select staff working at a branch office to speed their login. Caching passwords also allows branch office users to log in if the WAN link fails. If the WAN link fails and the user's credentials are not cached, the user is simply unable to log in to the domain.

You configure which accounts can authenticate using the RODC by using the Password Replication Policy, as shown in Figure 4-9. By default, only members of the Allowed RODC Password Replication group can use the RODC to authenticate. This is only the case if the user account is not a member of the Account Operators, Administrators, Backup Operators, Server Operators, or Denied RODC Password Replication Group groups.

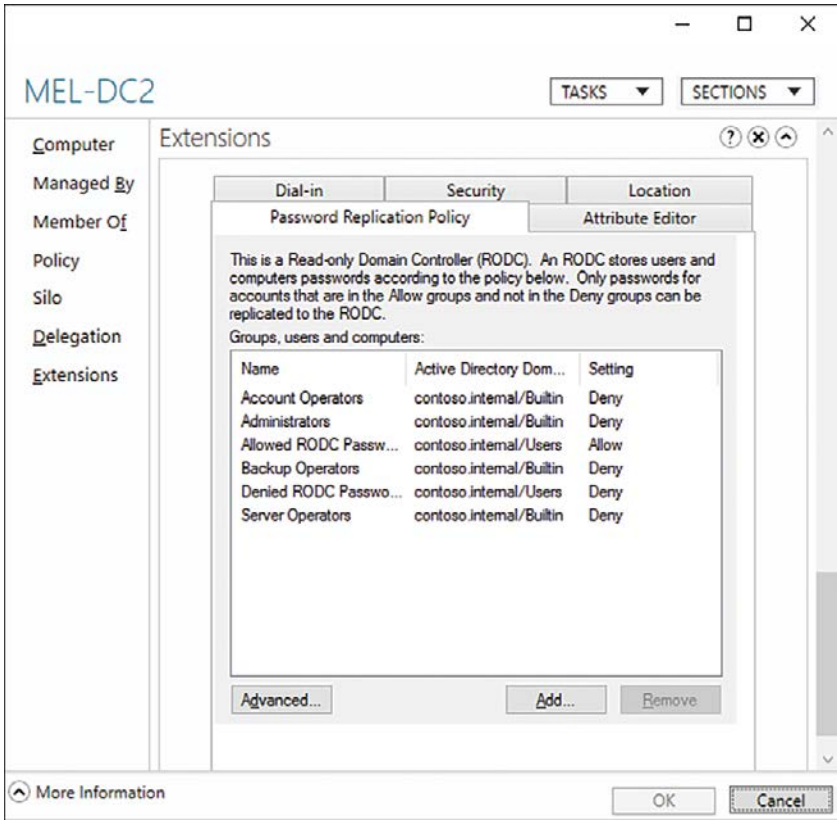

Figure 4-9 Password Replication Policy

RODC partial attribute set

You can configure Active Directory so that only specific attributes on AD DS objects are replicated to an RODC. You would do this because some applications are configured to store sensitive data, such as passwords or encryption keys, as attributes for an object. If you add these sensitive attributes to the filtered attributes set, you can ensure that this information will not be replicated and stored on an RODC.

It's not possible to add system-critical attributes to the RODC filtered attribute set. Attributes that cannot be added to the filtered attribute set are those required for AD DS, the Local Security Authority (LSA), Security Accounts Manager (SAM), and Microsoft-specific security services providers to be able to function correctly. You mark an attribute as confidential by removing the Read permission for that attribute for the Authenticated Users group.

RODC local administrators

Because you deploy RODCs as a security measure, they are almost always placed at branch office sites. Because resources at branch office sites are often sparse, it's also likely that you'll co-locate other services on the server hosting the RODC role. For example, a server that functions as an RODC can also function as a file server, DNS server, DHCP server, and local intranet server.

You can allow a user without Domain Admin privileges to deploy an RODC if you have pre-created an RODC account and added it to the appropriate Active Directory Domain Services site, and the user is a member of the local Administrators group on the computer. You can perform this task in PowerShell or the Active Directory Administrative Center.

If the computer hosting the RODC role also needs to host other roles, you might need to grant administrator access to a user who works at the branch office (but who is not a member of your organization's usual IT staff) in case your normal remote administration techniques don't work. RODCs differ from normal domain controllers in that you can grant local administrator access without having to make the user a member of the Domain Admins group.

To configure a user to function as a local administrator on the computer that hosts the RODC role, edit the properties of the RODC's computer account and configure a security group for the Managed By setting.

In Chapter 12, you learn about Just Enough Administration, a technology that you could use to allow a user to perform remote administrative tasks on an RODC without being made an RODC local administrator.

Decommissioning an RODC

If you suspect that an RODC has been compromised, you can delete the RODC's account from the Domain Controllers container in Active Directory Users And Computers. When you do this, you get the option of resetting all passwords for user and computer accounts that were cached on the RODC, as well as the option of exporting a list of all potentially compromised accounts.

Virtual domain controller cloning

Windows Server supports virtual domain controller cloning. Rather than redeploying domain controllers from scratch each time you need one, domain controller cloning allows you to take an existing virtual machine, make a copy of it, and deploy that copy.

Virtual domain controller cloning has the following prerequisites:

- Hypervisor must support VM-Generation ID. The version of Hyper-V included with all supported versions of Windows supports this technology, as do the most recent versions of VMware.
- The source domain controller needs to be running Windows Server 2012 or later.

- The domain controller that hosts the PDC Emulator role must be online and contactable by the cloned DC. The computer that hosts the PDC Emulator role must also be running Windows Server 2012 or later.
- The source DC must be a member of the Cloneable Domain Controllers group.

You also need to create the `DCCloneConfig.xml` file. You can do this by using the `New-ADDC-CloneConfig` cmdlet in PowerShell. When running this cmdlet, you need to specify the cloned DC's IPv4 address information and the site the cloned DC is deployed to. For example, to create the clone configuration file for a clone DC that has the IP address `10.10.10.42` with the subnet mask `255.255.255.0`, default gateway of `10.10.10.1`, DNS server address of `10.10.10.10`, and site name `MEL-SITE`, issue this command:

```
New-ADDCCloneConfigFile -IPv4Address 10.10.10.42 -IPv4DefaultGateway 10.10.10.1
-IPv4SubnetMask 255.255.255.0 -IPv4DNSResolver 10.10.10.10 -Static -SiteName MEL-SITE
```

After the clone configuration file is created, you import the VM using this file and specify a copy of the source DC's exported virtual hard disk.

AD DS structure

Active Directory is made up of forests and domains. A forest is a collection of Active Directory domains that share a schema and some security principals. The majority of organizations in the world have a single forest domain. Larger, geographically dispersed organizations generally use multiple domain forests.

Domains

For the majority of organizations in the world, a single domain would be sufficient. There are two general reasons for having multiple domains in a forest. The first is that your organization is geographically dispersed, and there are issues around domain replication traffic. The second is that your organization is very large. A single domain can hold a staggering number of objects. Unless your organization has tens of thousands of users, a single domain is usually more than enough.

A domain tree is a collection of domains that share a namespace in a parent-child relationship. For example, the domains *australia.contoso.com* and *tonga.contoso.com* would be child domains of the *contoso.com* domain.

You should always deploy at least two domain controllers per domain for redundancy purposes. Make sure that if you have a multidomain forest, you are making regular backups of the domain controllers in the root domain. There has been more than one organization with a multidomain forest that has had the root domain controllers fail irreparably, making it necessary to redeploy the entire forest from scratch.

Multidomain Active Directory environments

The majority of current AD DS deployments in small and medium-sized enterprises have a single domain. This hasn't always been the case because earlier versions of the Windows Server operating system, such as Windows NT 4, supported far fewer accounts. Supporting a smaller number of accounts often necessitated the use of multiple domains, and it wasn't unusual to see medium-sized organizations that used complicated domain structures.

Each Windows Server domain controller can create approximately 2.15 billion objects during its lifetime, and each domain supports the creation of up to approximately 2.15 billion relative identifiers (RIDs). Given this, however, few administrators implement multiple-domain forests because they need to support a large number of users.

There are many reasons why organizations implement multidomain forests. These can include (but are not limited to) the following:

- **Historical domain structure** Even though newer versions of the Windows Server operating system handle large numbers of objects more efficiently, some organizations have retained the forest structure that was established when the organization first adopted AD DS.

- **Organizational or political reasons** Some organizations are conglomerates, and they might be composed of separate companies that share a common administrative and management core. An example of this is a university faculty in Europe or Australia, such as a Faculty of Science, that consists of different departments or schools, such as the School of Physics and the Department of Botany. For political or organizational reasons, it might have been decided that each department or school should have its own domain that is a part of the overall faculty forest. AD DS gives organizations the ability to create domain namespaces that meet their needs, even if those needs might not directly map to the most efficient way of accomplishing a goal from a strict technical perspective.

- **Security reasons** Domains enable you to create authentication and authorization boundaries. You can also use domains to partition administrative privileges so that you can have one set of administrators who are able to manage computers and users in their own domain, but who are not able to manage computers and users in a separate domain. Although it's possible to accomplish a similar goal by delegating privileges, many organizations prefer to use separate domains to accomplish this goal.

Domain trees

A *domain tree* is a set of names that share a common root domain name. For example, *contoso.com* can have *pacific.contoso.com* and *atlantic.contoso.com* as child domains, and these domains can have child domains themselves. A forest can have multiple domain trees. When you create a new tree in a forest, the root of the new tree is a child domain of the original root domain. In Figure 4-10, *adatum.com* is the root of the new domain tree in the *contoso.com* forest.

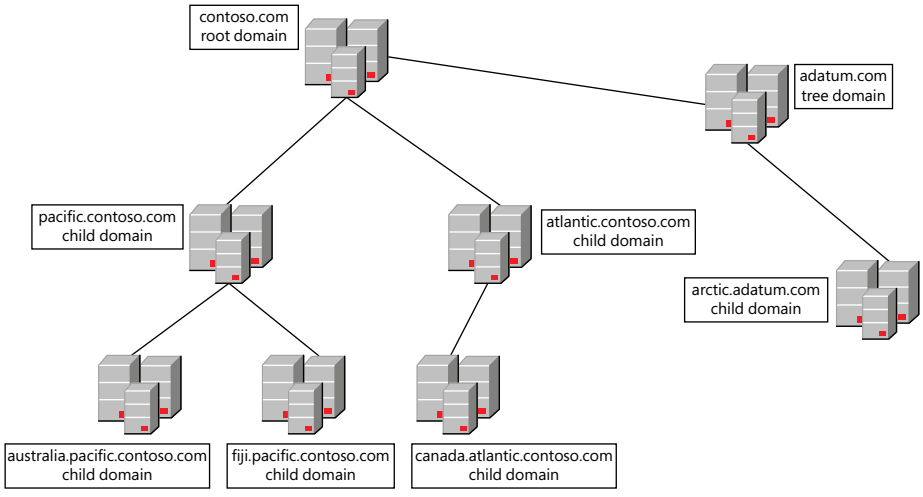

Figure 4-10 *Contoso.com* as the root domain in a two-tree forest

The depth of a domain tree is limited by a domain having a maximum fully qualified domain name (FQDN) length for a host of 64 characters.

Intra-forest authentication

All domains within the same forest automatically trust one another. This means that in the environment shown earlier in Figure 4-10, you can assign a user in the *Australia.pacific.contoso.com* permissions to a resource in the *arctic.adatum.com* domain without performing any extra configuration.

Because of the built-in automatic trust relationships, a single forest implementation is not appropriate for separate organizations, even when they're in partnership with one another. A single forest makes it possible for one or more users to have administrative control. Most organizations aren't comfortable even with trusted partners having administrative control over their IT environments. When you do need to allow users from partner organizations to have access to resources, you can configure trust relationships or federation.

Domain functional levels

The domain functional level determines which Active Directory features are available and which operating systems can participate as domain controllers within the domain. The domain functional level determines the minimum domain controller operating system. For example, if the domain functional level is set to Windows Server 2016, domain controllers must run Windows Server 2016 or later. This rule does not apply to member servers. You can have a domain running at the Windows Server 2016 functional level that still has servers running the Windows Server 2012 R2 operating system. Table 4-1 lists the maximum domain functional level given the

minimum domain controller operating system. Assuming you are running supported versions of Windows Server and later, which means you are running domain controllers where the oldest operating system is Windows Server 2016, you can either have the domain functional level set to Windows Server 2016 or, if all your domain controllers are running Windows Server 2025, have the domain functional level set to Windows Server 2025.

Table 4-1 Maximum domain functional level

Minimum domain controller operating system	Maximum domain functional level
Windows Server 2016	Windows Server 2016
Windows Server 2019	Windows Server 2016
Windows Server 2022	Windows Server 2016
Windows Server 2025	Windows Server 2025

Inside OUT

Run DC at the highest OS level

Because domain controllers are so important to your network, Microsoft recommends that, from a security perspective, you always run domain controllers with the most recent operating system. Microsoft argues that the most recent operating system is the most secure and that you should pay special attention to the security of your organization's domain controllers.

You can introduce a DC running Windows Server 2025 to a domain at the Windows Server 2016 functional level as long as all the appropriate updates are installed. You can also perform an in-place upgrade of a Windows Server 2012 R2 domain controller to Windows Server 2025. You can raise the functional level after you've retired existing domain controllers running older versions of the Windows Server operating system. If all your domain controllers are running Windows Server 2025, you should update your domain functional level to the Windows Server 2025 functional level.

Inside OUT

Check your functional level

Even when older Windows Server DCs have long been removed, it's not unusual for people to have forgotten to elevate the functional level. Because you get greater functionality by raising functional levels, and there is no downside to doing so beyond not being able to introduce a domain controller running an operating system below that of the functional level, you should raise functional levels as high as possible.

Forests

A forest is a collection of domains that share a schema. There are automatic trust relationships between all domains in a forest. Accounts in one domain in a forest can be granted rights to resources in other domains. As mentioned earlier in this chapter, forests don't need to have a contiguous namespace. For example, a forest can contain both the *contoso.com* and *Adatum.com* domains.

There are several reasons why an organization might have multiple forests with trust relationships configured between those forests. The most common is that one organization has acquired another, and multiple forests exist until such a time that the users and resources hosted in the forest of the acquired organization are moved to the forest of the acquiring organization. A less common one is that an organization is splitting off a part of itself, and users need to be migrated out of the existing forest and into a new forest prior to the split occurring.

Forest functional levels are determined by the minimum domain functional level in the forest. After you've raised the domain functional levels in the forest, you can raise the forest functional level. Unlike in previous versions of Active Directory, it's possible to lower both the forest and domain functional levels after they have been raised. An important caveat with this is that the forest functional level must be lowered so that it's never higher than the lowest intended domain functional level.

Account and resource forests

Organizations are increasingly deploying what are known as Enhanced Security Administrative Environment (ESAE) forests. In an ESAE forest design, all of the accounts used for administrative tasks in the production forest are hosted in a second forest known as the ESAE, bastion, or administrative forest. The ESAE forest is configured with one-way trust relationships with the production forest.

In their native administrative forest, the accounts used for administrative tasks in the production forest are traditional unprivileged user accounts. These accounts and the groups that they are members of in the administrative forest are delegated privileges in the production forest.

The advantage of this approach is that, should one of these accounts become compromised, it can't be used to alter any permissions or settings in the administrative forest because the account only has privileges in the production forest.

Organizational units

The benefit of a comprehensive OU structure is that it simplifies the delegation of permissions over objects and allows you to apply GPOs closer to the accounts that they influence. While it's possible to filter GPOs based on security groups or WMI queries, it's important to remember that each GPO within a computer and user account's scope must be checked to see if it applies.

If you have all of your GPOs applied at the domain level and filtered on the basis of security group or WMI query, your Group Policy processing time at startup and sign-on is going to be substantially longer than if you apply GPOs as close to the accounts they influence as possible.

Better privilege delegation targeting is also a great reason to have a good OU structure. When delegating privileges, you want to ensure that you only delegate privileges over an appropriate set of objects. For example, imagine that you want to allow each department's administrative assistant to have the ability to reset passwords for users within their respective department. If all the user accounts for your organization are located in one OU, you won't be able to do this because, at best, you'll provide each administrative assistant with the ability to reset every user's password in the organization. If user accounts are located in department-specific OUs, you can then delegate the ability to reset passwords on a per-OU basis. This way, the administrative assistant for the Marketing department can be granted the ability to change passwords for user accounts located in the Marketing OU without granting them the ability to change passwords for user accounts located in the Accounting OU.

Inside OUT

OU structures don't always relate to organizational structure

Many organizations have had an AD deployment for more than a decade and a half. A big problem for many is that while the company goes through regular reorganizations, the OU structure doesn't go through a similar reorganization. This might mean that the OU structures don't in any way represent the organizational structure. You should periodically review your organization's OU structure to ensure that it maps sensibly to the organizational structure. While you might not implement GPOs at the OU level or delegate privileges, it doesn't mean that you won't do so at some point in the future.

When you create OUs in Windows Server 2019 and later, the OUs are automatically configured so that accidental deletion protection is enabled.

Flexible Single Master Operations roles

The Flexible Single Master Operations (FSMO) roles are five special roles present on domain controllers. Two of these roles, the schema master and the domain naming master, are unique within each forest. The other three roles, PDC Emulator, infrastructure master, and RID master, must be present within each domain in the forest. For example, in a three-domain forest, there is only one schema master and domain naming master, but each domain in the forest has its own PDC emulator, infrastructure master, and RID master.

By default, FSMO roles are allocated to the first domain controller in a domain. After you have more than one domain controller in each domain, you should manually start to move the FSMO roles to other domain controllers. This protects you from a situation where the first domain

controller deployed in each domain goes offline and all FSMO roles become unavailable. When you do need to take a domain controller offline for an extended period of time, ensure that you transition any FSMO roles that it hosts to another domain controller in the same domain.

Schema master

The schema master is the single server in the forest that is able to process updates to the Active Directory schema. The Active Directory schema defines the functionality of Active Directory. For example, by modifying the schema, you can increase the available attributes for existing objects as well as enable Active Directory to store new objects. Products, including Exchange Server and Configuration Manager, require that the default Active Directory schema be extended prior to product installation so that each product can store important data in Active Directory.

The domain controllers that host the schema master role should be located in the root domain of the forest. If you need to extend the schema prior to installing products such as Exchange Server, do so either on the computer that hosts the schema master role or on a computer in the same site. The account used to extend the schema needs to be a member of the Schema Admins security group.

You can determine which computer hosts the schema master role by running the following PowerShell command:

```
Get-ADForest contoso.internal | FT SchemaMaster
```

Domain naming master

The domain naming master is a forest-level role that is responsible for managing the addition and removal of domains from the forest. The domain naming master also manages references to domains in trusted forests. In a multidomain environment, the domain controller that hosts this forest-level role should be deployed in the root forest.

The domain naming master is also contacted when new instances of AD DS application directory partitions are added, such as when you configure a limited directory partition replication scope for an AD DS-integrated DNS zone. If you can't add new domains or partitions, the computer hosting this FSMO role may not be available.

You can determine which server hosts the domain naming master role by running the following PowerShell command:

```
Get-ADForest contoso.internal | FT DomainNamingMaster
```

PDC emulator

The PDC emulator role is a domain-level FSMO role that is responsible for handling both changes to account passwords as well as domain time synchronization. PDC emulators in child domains synchronize time against the PDC emulator in the forest root domain. You should

ensure that the PDC emulator in the forest root domain synchronizes against a reliable external time source. If users are unable to change passwords or accounts can't be unlocked, the PDC emulator may have failed.

To determine which domain controller in a specific domain hosts the PDC emulator role, run the following PowerShell command:

```
Get-ADDomain contoso.internal | FT PDCEmulator
```

Infrastructure master

The computer that hosts the infrastructure master role keeps track of changes that occur in other domains in the forest as they apply to objects in the local domain. The infrastructure master FSMO role holder updates an object's SID (Security Identifier) and distinguished name in a cross-domain object reference. If group names or memberships for groups hosted in other domains don't appear current in the local domain, it may be that the infrastructure master has failed.

You should avoid having the infrastructure master role co-located with a domain controller that hosts the global catalog server role unless all domain controllers in the domain are configured as global catalog servers. You can determine which computer in a domain hosts the infrastructure master role by running the following PowerShell command:

```
Get-ADDomain contoso.internal | FT InfrastructureMaster
```

RID master

The RID master processes relative ID requests from domain controllers in a specific domain. Relative IDs and domain Security IDs are combined to create a unique Security ID (SID) for the object. There is an RID master in each domain in the forest. When a new security principal object, like a group or user account, is created, a unique SID is attached to that object. SIDs consist of

- The domain SID that will be the same for all SIDs created in the host domain
- An RID that is unique to each security principal SID created in a domain

Each AD DS DC has a pool of RIDs that it can allocate to security principals it creates. When this pool becomes exhausted, the DC will query the RID master for additional RIDs to add to this pool. If the RID master is not available, the pool cannot be replenished, and new accounts cannot be created.

You can use the following PowerShell command to determine which computer hosts the RID Master role:

```
Get-ADDomain contoso.internal | FT RidMaster
```

Seizing FSMO roles

In some cases, a domain controller hosting an FSMO role fails, and you need to seize the FSMO role to move it to another domain controller. For example, to move the RID Master, Infrastructure Master, and Domain Naming Master roles to a domain controller named MEL-DC2, run the following command:

```
Move-ADDirectoryServerOperationMasterRole -Identity MEL-DC2 -OperationMasterRole RIDMast
er,InfrastructureMaster,DomainNamingMaster -Force
```

Trust relationships

Trust relationships allow security principals in one Active Directory environment to access resources in another Active Directory environment. Trusts make it possible for users in one domain to be authenticated by domain controllers in a separate domain. For example, if there is a bidirectional trust relationship between the domains *contoso.local* and *adatum.remote*, users with accounts in the *contoso.local* domain are able to authenticate in the *adatum.remote* domain. By configuring a trust relationship, it's possible to allow users in one domain to access resources in another, such as being able to use shared folders and printers or being able to sign on locally to machines that are members of a different domain than the one that holds the user's account.

Some trusts are created automatically. For example, domains in the same forest automatically trust each other. Other trusts, such as external trusts, realm trusts, shortcut trusts, and forest trusts, must be created manually. Trusts use the Kerberos V5 authentication protocol by default, and they revert to NTLM if Kerberos V5 is not supported. You configure and manage trusts using the Active Directory Domains and Trusts console or the `netdom.exe` command-line utility with the `/trust` switch.

Although trusts themselves are relatively easy to come to terms with, the terminology around trusts tends to confuse many people. It's important that you understand the difference between a trusting and a trusted domain and how trust direction, incoming or outgoing, relates to which security principals are able to authenticate.

To understand trusts, you have to understand the difference between a trusting domain or forest and a trusted domain or forest. The trusting domain or forest contains the resources to which you want to grant security principals from the trusted domain or forest access. The trusted domain or forest hosts the security principals that you want to allow to access resources in the trusting forest. For example, if you want to grant users in the *adatum.remote* domain access to resources in the *contoso.local* domain, the *adatum.remote* domain is the trusted domain and the *contoso.local* domain is the trusting domain. In bidirectional trust relationships, a domain or forest is both trusting and trusted.

Trust transitivity

A transitive trust extends beyond the original trusting domains. For example, if you have a trust between two domain forests and that trust is transitive, all of the domains in each of the forests trust each other. Forest trusts are transitive by default. External trusts are not transitive by default. When you create a trust, keep in mind that there may be domains beyond the one you're establishing the relationship with that may be included. You might trust the administrator of *adatum.remote* not to allow access by nefarious users, but do you trust the administrator of *subdomain.adatum.remote*?

Trust direction

When you create a new trust, you specify a trust direction. You can choose a two-way (or bidirectional) trust or a unidirectional trust, which is either one-way incoming or one-way outgoing.

When you configure a one-way incoming trust, users in the local domain are authenticated by their local domain and authorized for access to resources in the remote domain, realm, or forest. Remember that if you're configuring a one-way incoming trust between the single domain forests *contoso.local* and *adatum.remote*, users with accounts in *contoso.local* can access resources in *adatum.remote*. Similarly, if you're configuring a one-way outgoing trust between the single-domain forests *contoso.local* and *adatum.remote*, users with accounts in *adatum.remote* can access resources hosted in *contoso.local*.

The terminology around trusts can be a little confusing. The key thing to remember is that the direction of trust is the opposite of the direction of access, as shown in Figure 4-11. An outgoing trust allows incoming access, and an incoming trust allows outgoing access.

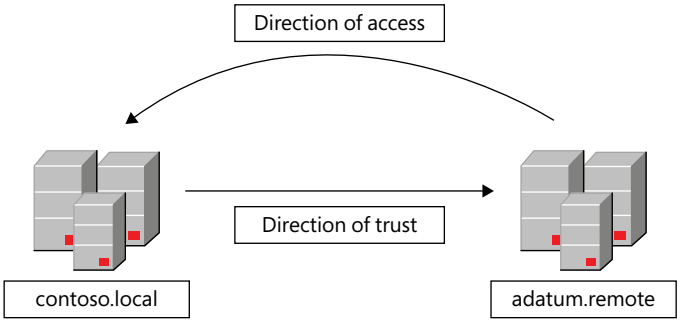

Figure 4-11 The direction of trust and direction of access

Forest trusts

When you configure a forest trust, one AD DS forest trusts the other one. Forest trusts are transitive. When you configure a forest trust, you can allow any domain in the trusting forest to be accessible to any security principal in the trusted forest. Forest trusts can be bidirectional

or unidirectional. You are most likely to configure forest trusts if your organization has two or more AD DS forests. You can configure a trust between a forest hosted in Azure and one hosted on-premises.

You can configure one of two authentication scopes when you configure a forest trust. The type of authentication scope that you configure depends on your security requirements. The options are

- **Forest-wide authentication** When you choose forest-wide authentication, users from the trusted forest are automatically authenticated for all resources in the local forest. You should use this option when both the trusted and trusting forests are part of the same organization.
- **Selective authentication** When you configure this option, Windows does not automatically authenticate users from the trusted forest. You can then configure specific servers and domains within the forest to allow users from the trusted forest to authenticate. Use this option when the two forests are from different organizations, or you have more stringent security requirements.

Configuring selective authentication

Configuring selective authentication means granting specific security principals in the trusted forest the Allowed To Authenticate (Allow) permission on the computer that hosts the resource to which you want to grant access. For example, assume you had configured a forest trust with selective authentication. You want to grant users in the Research universal group from the trusted forest access to a Remote Desktop Services (RDS) server in the trusting forest. To accomplish this goal, you can configure the properties of the RDS server's computer account in Active Directory Users And Computers and grant the Allowed To Authenticate permission to the Research universal group from the trusted forest. Doing this only allows users from this group to authenticate; you still have to grant them access to RDS by adding them to the appropriate local group on the RDS server.

External trusts

External trusts enable you to configure one domain in one forest to trust a domain in another forest without enabling a transitive trust. For example, you configure an external trust if you want to allow the *auckland.fabrikam.com* domain to have a trust relationship with the *wellington.adatum.com* domain without allowing any other domains in the *fabrikam.com* or *adatum.com* forests to have a security relationship with each other.

Shortcut trusts

Shortcut trusts enable you to speed up authentication between domains in a forest that might be in separate branches or even separate trees. For example, in the hypothetical forest shown in Figure 4-12, if a user in the *canada.atlantic.contoso.com* domain wants to access a resource in

the *arctic.adatum.com* domain, authentication needs to travel up through the *atlantic.contoso.com* and *contoso.com* domains before passing across to the *adatum.com* domain and finally back to the *arctic.adatum.com*. If you implement a shortcut trust between the *canada.atlantic.contoso.com* and *arctic.adatum.com* domains, authentication traffic instead travels directly between these two domains without having to traverse the two domain trees in the forest.

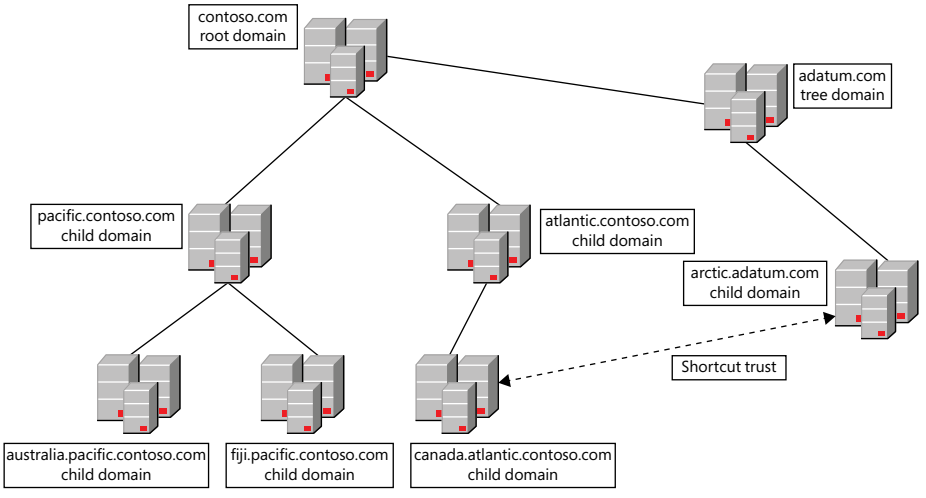

Figure 4-12 Shortcut trust

You configure a shortcut trust using the Active Directory Domains And Trusts console by editing the properties of one domain and triggering the New Trust Wizard on the Trusts tab. Shortcut trusts can be unidirectional or bidirectional. As is the case with the creation of other trusts, ensure that you have name resolution working properly between the trusting and the trusted domains, either by having the DNS zones propagate through the forest, by configuring conditional forwarders, or by configuring stub zones.

Realm trusts

You use a realm trust to create a relationship between an Active Directory Domain Services domain and a Kerberos V5 realm that uses a third-party directory service. Realm trusts can be transitive or nontransitive. They can also be unidirectional or bidirectional. You're most likely to configure a realm trust when you need to allow users who use a UNIX directory service to access resources in an AD DS domain or users in an AD DS domain to access resources in a UNIX Kerberos V5 realm.

You can configure a realm trust from the Active Directory Domains And Trust console. You do this by selecting the Realm Trust option, as shown in Figure 4-13. When configuring a realm trust, you specify a realm trust password that you use when configuring the other side of the trust in the Kerberos V5 realm.

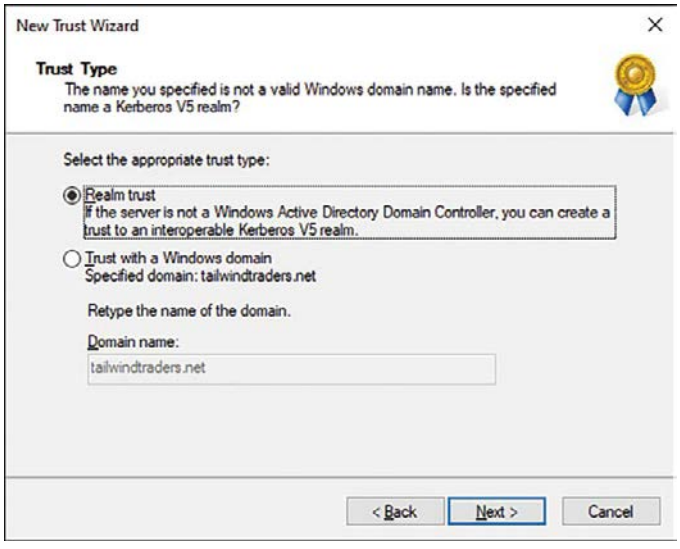

Figure 4-13 Configure the realm trust

Netdom.exe

You use `netdom.exe` with the `trust` switch to create and manage forest, shortcut, and realm trusts from the command line. When using `netdom.exe`, you specify the trusting domain name and the trusted domain name.

The syntax of `netdom.exe` with the `/trust` switch is shown in Figure 4-14.

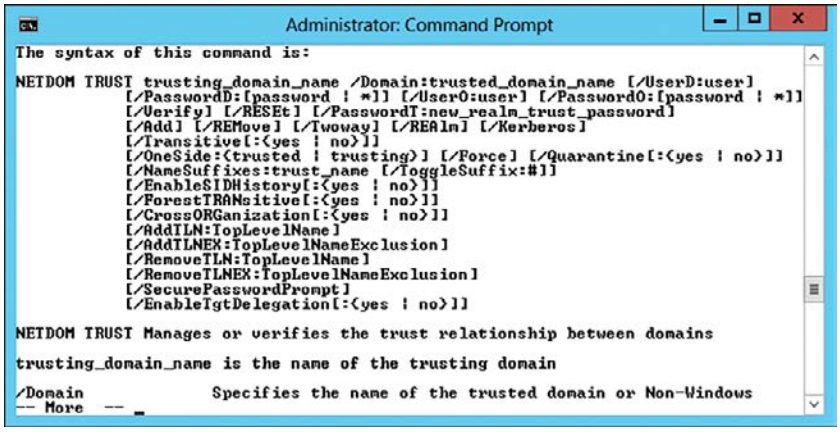

Figure 4-14 The command syntax for `netdom.exe`

PowerShell doesn't include much in the way of cmdlets for creating and managing trust relationships beyond the `Get-ADTrust` cmdlet, which allows you to view the properties of an existing trust.

SID filtering

In a trusted domain, it's possible, though extremely difficult, for a malicious administrator to add foreign SIDs (for example, Domain Admins from the resource forest) into a user's sIDHistory. If those foreign SIDs aren't filtered at the trust boundary, they would be honored in the user's token and could grant unintended privileges.

To block this type of configuration, Windows Server enables *SID filtering*, also known as *domain quarantine*, on all external trusts. When you enable SID filtering on an external trust, the trusting domain accepts only SIDs from the directly trusted domain and drops all others (including foreign sIDHistory).

It's possible to verify SID filtering settings on a trust using the `Get-ADTrust` cmdlet in a PowerShell session run by a user with administrative privileges. For example, to verify that SID filtering is enabled on the trust with the *tailwindtraders.com* forest, issue the following command:

```
Get-ADTrust -identity tailwindtraders.com -properties SIDFilteringForestAware | fl *SID*
```

To disable SID filtering for the trusting forest, use the netdom trust command with the following option:

```
/enablesidhistory:Yes
```

Enabling SID history allows you to use SIDs that don't have the domain SID of the trusting domain. You enable or disable SID filtering on the trusting side of the trust. For example, if you are an administrator in the *contoso.com* domain and you want to disable SID filtering, you can issue the following command from an elevated command prompt:

```
Netdom trust contoso.com /domain:tailwindtraders.com /enablesidhistory:Yes
```

In the same scenario, if you want to reenable SID filtering, you can issue the following command:

```
Netdom trust contoso.com /domain:tailwindtraders.com /enablesidhistory:Yes
```

The default configuration, where SID filtering is enforced by default on trusts, is something that you should probably leave as it is. In the past, it was necessary to allow SID history when trusts were created with forests running Windows 2000 Server domain controllers. Since Windows 2000 is no longer supported by Microsoft, and SID history is not necessary for trust relationships with Windows Server 2003 or later domain controllers, you probably won't need to disable it.

Name suffix routing

Name suffix routing enables you to configure how authentication requests are routed when you configure a forest trust between two AD DS forests. When you create a forest trust, all unique name suffixes are routed. Name suffix routing assists when users sign on with a UPN, such as *rick_claus@contoso.com*. Depending on the UPNs that are configured, you might want to allow or disallow the use of specific UPN suffixes. You do this by configuring name suffix routing on the Name Suffix Routing tab of the trust's properties.

Managing sites

AD DS sites enable you to configure AD DS so that it understands which network locations have a fast local network connection. Generally, this means the computers are in the same building, although if your organization has a group of buildings in the same area that are connected by a high-speed network, you use a single AD DS site configuration.

An Active Directory site is a collection of TCP/IP subnets. Sites allow you to define geographic locations for Active Directory on the basis of TCP/IP subnets. You can have multiple TCP/IP subnets in a site. You should put subnets together in a site where the hosts in that site have a high-bandwidth connection to each other. Usually, this means being in the same building, but it could also mean multiple buildings with very-low-latency gigabit links between them.

For example, imagine that your organization has its head office in Melbourne and a branch office in Sydney. You can set up two sites: one site for Melbourne and the other for Sydney. This ensures that computers in the Melbourne location interact as much as possible with resources located in Melbourne, and computers in the Sydney location interact as much as possible with resources located in Sydney.

You associate the TCP/IP subnets in the head office with the Melbourne site and the TCP/IP subnets in the branch office with the Sydney site. After you do this, functionality such as replication topology is automatically configured.

You configure sites by associating them with IP address ranges. For example, you might associate the subnet 192.168.10.0 /24 with the AD DS Site BNE-Site. Any computers that have an IP address in this range would be located in that site. You can configure network addresses using IPv4 or IPv6 networks. When you install AD DS for the first time, a default site, named Default-First-Site-Name, is created. You configure sites using the Active Directory Sites And Services console, shown in Figure 4-15.

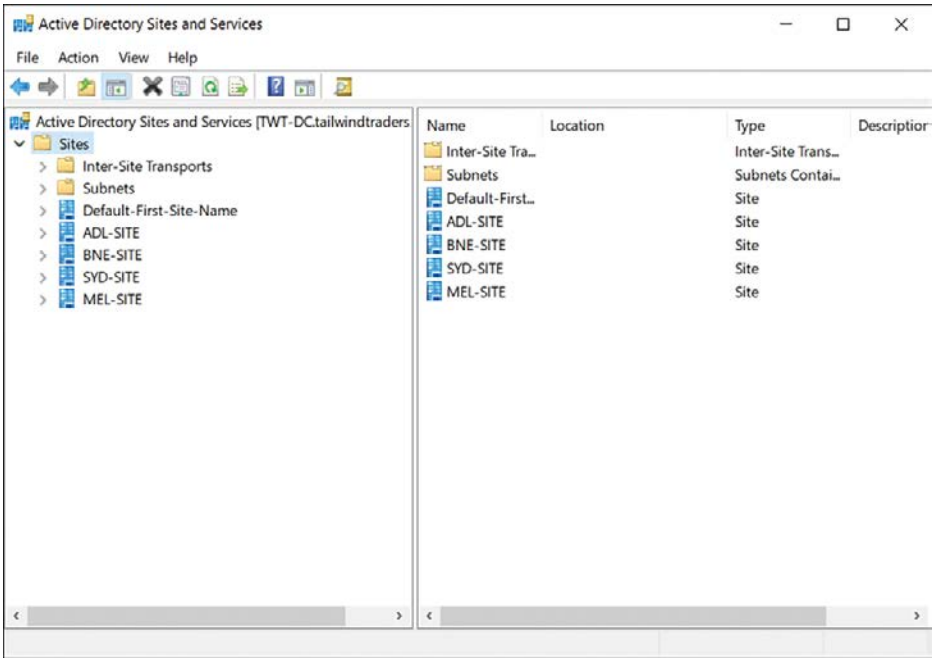

Figure 4-15 The Active Directory Sites And Services console

It's important that you add sites for each separate location in your organization. If you don't, AD DS assumes that all computers are located on the same fast network, and this might cause problems with other products as well as with AD DS. Microsoft products such as Exchange Server use AD DS site information when generating network topologies.

Sites enable you to do the following:

- **Separate different locations that are connected by a slow WAN or expensive WAN link** For example, if your organization has a branch office in Sydney and another branch office in Melbourne, and these branch offices are connected by a WAN link that is rated at 512 kilobits per second (Kbps), you configure the Sydney and Melbourne branch offices as separate sites.

- **Control which domain controllers are used for authentication** When users log on to the network, they perform authentication against an available domain controller located in their AD DS site. Although users are still able to sign on and authenticate against a DC in another site if one isn't available in their local site, you should strongly consider placing a domain controller at any site with a sufficient number of users. What counts as "a sufficient number of users" varies depending on the speed and reliability of the site's connection to the rest of the organization's network. In some cases, you might deploy an RODC to aid authentication at some branch office sites.

- **Control service localization** Many Microsoft products, such as Exchange Server, and technologies, such as BranchCache and DFS, use AD DS sites as a way of determining network topology. To ensure that these products and technologies work well, you should ensure that each AD DS site is configured properly.
- **Control AD DS replication** You can use AD DS sites to manage domain controller replication. The default settings make it possible for replication to occur 24 hours a day, 7 days a week. Instead, you can use AD DS site configuration to configure the replication to occur according to a specific schedule.

Creating sites

To add a new Active Directory site, right-click the Sites node in the Active Directory Sites And Services console and select New Site. Specify the site name and select a site link object, and then select OK twice.

A site link object represents a connection between two sites. The default site link object is named DEFAULTIPSITELINK. You can change the site link object later. Figure 4-16 shows the creation of a site named *Sydney*.

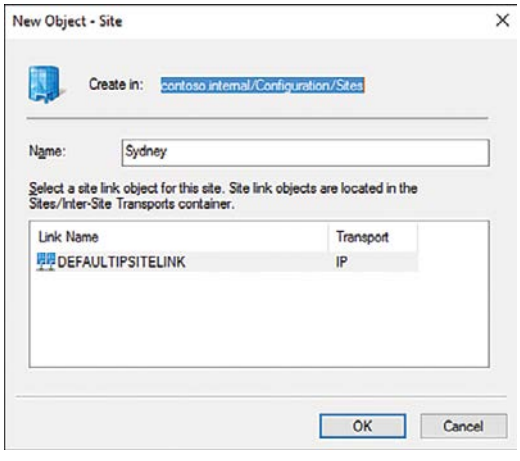

Figure 4-16 Creating a new site

You can use the `New-ADReplicationSite` PowerShell cmdlet to create a new site. For example, to create a new site named HBA-SITE that is associated with the default IP site link, issue this command:

```
New-ADReplicationSite HBA-SITE
```

After you've created a site, you need to associate it with IP address ranges. You can't do that until you've added IP address ranges as subnets. When you create a subnet, you specify an

IPv4 or IPv6 network prefix. For an IPv4 network, you specify the network address and the subnet in CIDR notation. For example, you specify network 192.168.15.0 with a subnet mask of 255.255.255.0 as 192.168.15.0 /24.

Creating subnets

To add a subnet, right-click the Subnets node in Active Directory Sites And Services and then select New Subnet. You can specify the new subnet in IPv4 or IPv6 format. After you've specified the subnet, you have to specify which site the subnet is associated with. Figure 4-17 shows the 10.10.10.0/24 subnet associated with the Melbourne site.

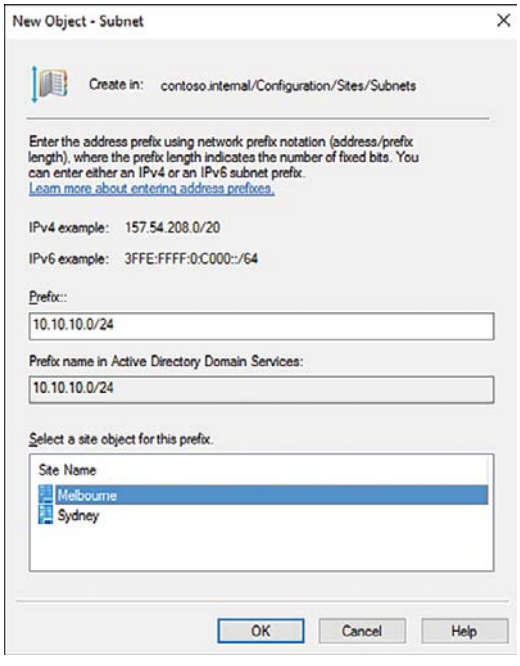

Figure 4-17 New subnet

You can create a new subnet from PowerShell with the `New-ADReplicationSubnet` cmdlet. For example, to create a new subnet that has the address 192.168.16.0/24 and associate it with the HBA-SITE site, issue the command:

```
New-ADReplicationSubnet –Name "192.168.16.0/24" –Site HBA-SITE
```

You can verify which subnets are associated with a particular AD DS site by viewing the properties of that site. You can't change which subnets are associated with a site by editing the site properties; you can only do so by editing the subnet properties. You can associate multiple subnets with an AD DS site, but you can't associate multiple AD DS sites with a specific subnet.

Creating site links

Site links enable you to specify how different AD DS sites are connected. When you add a site, you're asked to specify the site link, and the DEFAULTIPSITELINK site link is the default option even if another site link is available. Sites that are connected to the same site link are able to replicate with each other directly. For example, if all the sites in Figure 4-18 are associated with the DEFAULTIPSITELINK site link, each site assumes that it could replicate directly with the others. When troubleshooting replication, determine whether you want all sites connected to DEFAULTIPSITELINK or if you want them to use separate site links for alternative replication paths. For example, a domain controller in the Melbourne site attempts to replicate directly with a domain controller in the Canberra site. With this topology, you instead configure site links for Melbourne-Sydney, Adelaide-Sydney, and Canberra-Sydney. This way, domain controllers in Canberra, Melbourne, and Adelaide only replicate with the Sydney site rather than attempting to replicate with each other directly.

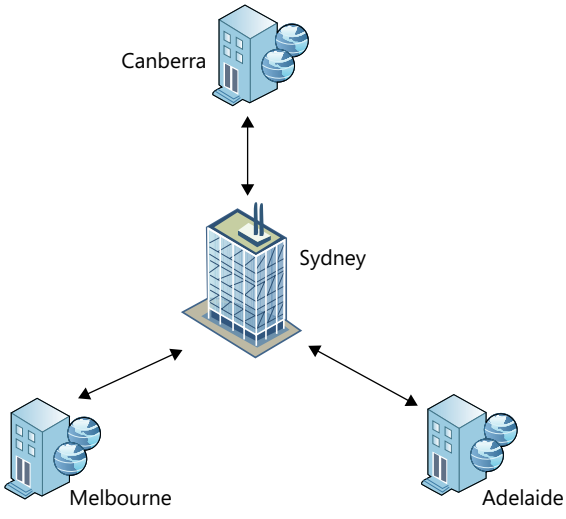

Figure 4-18 Configuring site links that mirror network topology

You can create a new IP site link using the Active Directory Sites And Services console. When you create a site link, you specify the sites that use the link. You can configure the cost and replication schedule of a site link after it's created by editing the Site Link properties. The default Cost is 100, and site links that have lower costs are preferred for replication over site links that have a higher cost. Replication occurs every 180 minutes by default, 24 hours a day. You can modify when replication occurs by configuring a replication schedule.

If you want replication to occur as quickly as possible, you can enable the Use Notify replication option by modifying a site link's options attribute. You can perform this task by using the Attribute Editor tab in the site link's properties.

You can create a site link using the `New-ADReplicationSiteLink` cmdlet. For example, to create a new site link named ADL-CBR that links the ADL-SITE and CBR-SITE sites, issue this command:

```
New-ADReplicationSiteLink "ADL-CBR" –SitesIncluded ADL-SITE, CBR-SITE
```

Members of the Enterprise Admins security group can create and modify site links. Members of the Domain Admins security group in the forest root domain can also perform site link management tasks. User accounts that are only members of the child domain but not the forest root domain's Domain Admins security group are unable to manage site links.

Creating site link bridges

Site link bridges create transitive links between site links. Each site link in a bridge must have a site in common with another site link in the bridge. It's only necessary to create a site link bridge with complex network topologies, as site link bridges are automatically created based on the topology created when you configure site links. You likely need to create a site link bridge if

- Your IP network is not fully routed. If you disable the Bridge All Site Links option, all site links will be treated as nontransitive. You can then use your own site link bridges to reflect the manner in which traffic is routed across your network.
- You need to control replication flow between sites. By disabling the Bridge All Site Links for the site link IP transport and creating a site link bridge, you can create a disjointed network. This ensures that site links within the bridge can route AD DS traffic transitively, but they will not route traffic outside of the site link bridge.

Moving domain controllers

When you deploy a new domain controller, the domain controller promotion process performs a lookup to determine which AD DS site the domain controller should be a member of based on its IP address. If you haven't created a subnet in the Active Directory Sites And Services console that maps to the IP address of the server that you are promoting to the domain controller, the domain controller is instead assigned to the first AD DS site, which is Default-First-Site-Name unless you have changed it.

The domain controller does not automatically reassign itself to a new site if you create the subnet and site objects in the Active Directory Sites And Services console, if it has already been added to the Default-First-Site-Name site. In this instance, you need to move the domain controller to the new site manually. You can move the domain controller using the Active Directory Sites And Services console by right-clicking the domain controller that you want to move, selecting Move, and selecting the destination site in the Move Server dialog.

You can also move a domain controller to a different site using the `Move-ADDirectoryServer` PowerShell cmdlet. For example, to move the server PERTH-DC to the Perth-Site AD DS site, execute the following command:

```
Move-ADDirectoryServer –Identity "PERTH-DC" –Site "Perth-Site"
```

Managing replication

Replication makes it possible for changes that are made on one AD DS domain controller to be replicated to other domain controllers in the domain and, in some cases, to other domain controllers in the forest. Rather than replicating the AD DS database in its entirety, the replication process is made more efficient by splitting the database into logical partitions. Replication occurs at the partition level, with some partitions only replicating to domain controllers within the local domain, some partitions replicating only to enrolled domain controllers, and some partitions replicating to all domain controllers in the forest. AD DS includes the following default partitions:

- **Configuration partition** This partition stores forest-wide AD DS structure information, including domain, site, and domain controller location data. The configuration partition also holds information about DHCP server authorization and Active Directory Certificate Services certificate templates. The configuration partition replicates to all domain controllers in the forest.

- **Schema partition** The schema partition stores definitions of all objects and attributes as well as the rules for creating and manipulating those objects. There is a default set of classes and attributes that cannot be changed, but it's possible to extend the schema and add new attributes and classes. Only the domain controller that holds the Schema Master FSMO role is able to extend the schema. The schema partition replicates to all domain controllers in the forest.

- **Domain partition** The domain partition holds information about domain-specific objects such as organizational units, domain-related settings, user, group, and computer accounts. A new domain partition is created each time you add a new domain to the forest. The domain partition replicates to all domain controllers in a domain. All objects in every domain partition are stored in the Global Catalog, but these objects are stored only with some, not all, of their attribute values.

- **Application partition** Application partitions store application-specific information for applications that store information in AD DS. There can be multiple application partitions, each of which is used by different applications. You can configure application partitions so that they replicate only to some domain controllers in a forest. For example, you can create specific application partitions to be used for DNS replication so that DNS zones replicate to some, but not all, domain controllers in the forest.

Active Directory supports attribute-level replication. Rather than replicate the entire object when a change is made to an attribute on that object, such as when group membership changes for a user account, only the attribute that changes is replicated to other domain controllers. Attribute-level replication substantially reduces the amount of data that needs to be transmitted when objects stored in AD DS are modified.

Understanding multimaster replication

AD DS uses multimaster replication. This means that any writable domain controller is able to make modifications to the AD DS database and to have those modifications propagate to the other domain controllers in the domain. Domain controllers use *pull replication* to acquire changes from other domain controllers. A domain controller may pull changes after being notified by replication partners that changes are available. A domain controller notifies its first replication partner that a change has occurred within 15 seconds and additional replication partners every 3 seconds after the previous notification. Domain controllers also periodically poll replication partners to determine whether changes are available so that those changes can be pulled and applied to the local copy of the relevant partition. By default, polling occurs once every 60 minutes. You can alter this schedule by editing the properties of the connection object in the Active Directory Sites And Services console.

Knowledge Consistency Checker (KCC)

The Knowledge Consistency Checker (KCC) runs on each domain controller. The KCC is responsible for creating and optimizing the replication paths between domain controllers located at a specific site. In the event that a domain controller is added or removed from a site, the KCC automatically reconfigures the site's replication topology. The KCC topology organization process occurs every 15 minutes by default. Although you can change this value by editing the registry, you can also trigger an update using the `repadmin` command-line tool with the KCC switch.

Store and forward replication

AD DS supports store-and-forward replication. For example, the Canberra and Melbourne branch offices are enrolled in a custom application partition. These branch offices aren't connected, but they are connected to the Sydney head office. In this case, changes made to objects stored in the application partition at Canberra can be pulled by the domain controller in Sydney. The Melbourne domain controller can then pull those changes from the domain controller in Sydney, as shown in Figure 4-19.

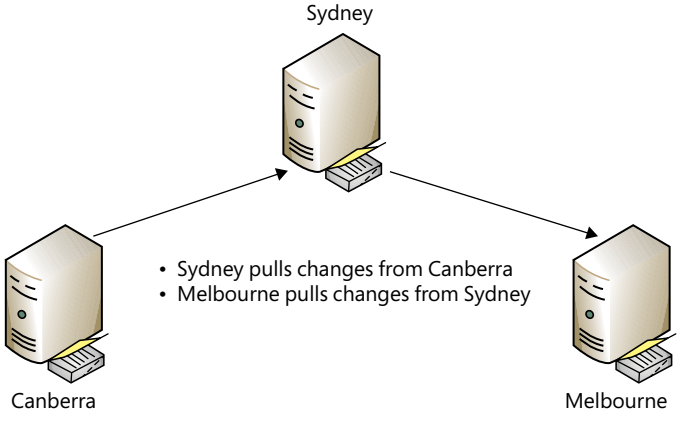

Figure 4-19 An example of store-and-forward replication

Conflict resolution

In an environment that supports multimaster replication, updates may be made to the same object at the same time in two or more different places. Active Directory includes sophisticated technologies that minimize the chance that these conflicts will cause problems, even when conflicting updates occur in locations that are distant from each other.

Each domain controller tracks updates by using *update sequence numbers (USNs)*. Each time a domain controller updates, either by processing an update performed locally or by processing an update acquired through replication, it increments the USN and associates the new value with the update. USNs are unique to each domain controller, as each domain controller processes a different number of updates to every other domain controller.

When this happens, the domain controller that wrote the most recent change, known as the last writer, wins. Because each domain controller's clock might not be precisely synchronized with every other domain controller's clock, the last write isn't simply determined by a comparison of time stamps. Similarly, because USNs are unique to each domain controller, a direct comparison of USNs is not made. Instead, the conflict resolution algorithm looks at the attribute version number. This is a number that indicates how many times the attribute has changed and is calculated using USNs. When the same attribute has been changed on different domain controllers, the attribute with the higher attribute version number wins. If the attribute version number is the same, the attribute modification time stamps are compared, with the most recent change being deemed authoritative.

If you add or move an object to a container that was deleted on another domain controller at the same time, the object is moved to the LostAndFound container. You can view this container when you enable the Advanced Features option in the Active Directory Users and Computers console.

RODC replication

The key difference between an RODC and a writable domain controller is that RODCs aren't able to update the Active Directory database, and they only host password information for a subset of security principals. When a client in a site that only has RODCs needs to make a change to the Active Directory database, that change is forwarded to a writable domain controller in another site. When considering replication, remember that all RODC-related replication is incoming and that other domain controllers do not pull updates from the AD DS database hosted on an RODC.

RODCs use the usual replication schedule to pull updates from writable domain controllers, except in certain cases, RODCs perform inbound replication using a replicate-single-object (RSO) operation. These cases include

- The password of a user whose account password is stored on the RODC is changed.
- A DNS record update occurs where the DNS client performing the update attempts to use the RODC to process the update and is then redirected by the RODC to a writable DC that hosts the appropriate Active Directory Integrated DNS zone.
- Client attributes, including client name, DnsHostName, OsName, OsVersionInfo, supported encryption types, and LastLogonTimeStamp, are updated.

These updates occur outside the usual replication schedule because they involve objects and attributes that are important to security. An example is when a user at a site that uses RODCs calls the service desk to have their password reset. The service desk staff member, located in another site, resets the password using a writable domain controller. If a special RSO operation isn't performed, it's necessary to wait for the change to replicate to the site before the user is able to sign on with the newly reset password.

Monitor and manage replication

You can use the Active Directory Sites And Services console to trigger replication. You can trigger replication on a specific domain controller by right-clicking the connection object and selecting Replicate Now. When you do this, the domain controller replicates with all of its replication partners.

You can also monitor replication as it occurs using DirectoryServices performance counters in Performance Monitor. Through Performance Monitor, you can view inbound and outbound replication, including the number of inbound objects in the queue and pending synchronizations.

Repadmin

You can use the `repadmin` command-line tool to manage and monitor replication. This tool is especially useful at enabling you to diagnose where there are problems in a replication topology. For example, you can use `repadmin` with the following switches:

- `replsummary` Generates information showing when replication between partners has failed. You can also use this switch to view information about the largest interval between replication events.
- `showrepl` Views specific inbound replication traffic, including objects that were replicated and the date stamps associated with that traffic.
- `prp` Determines which user account passwords are being stored on an RODC.
- `kcc` Forces the KCC to recalculate a domain controller's inbound replication topology.
- `queue` Enables you to display inbound replication requests that a domain controller must make to reach a state of convergence with source replication partners.
- `replicate` Forces replication of a specific directory partition to a specific destination domain controller.
- `replsingleobj` Use this switch when you need to replicate a single object between two domain controllers.
- `rodcpwdrepl` Enables you to populate RODCs with the passwords of specific users.
- `showutdvec` Displays the highest USN value recorded for committed replication operations on a specific DC.

Accounts

Accounts represent the identities of security principals in an Active Directory environment. The most common type of account is a user account, which represents a person as they interact with the Windows environment. IT Ops personnel also need to regularly deal with computer accounts, group accounts, and service accounts.

User accounts

User accounts almost always represent real people in an Active Directory environment, with the caveat that some user accounts are used for services rather than traditional users signing in to their desktop computers.

In many organizations, a user account is nothing more than a username, a password, and a collection of group memberships. User accounts can contain substantial additional information, including

- First name
- Last name
- Middle initial
- Full name
- Office information
- Email address
- Web page
- Job title
- Department
- Company
- Manager
- Phone numbers (main, home, mobile, fax, pager, IP phone)
- Address
- User profile location
- Log-on script
- Home folder

- Remote desktop service profile
- Dial-in permissions
- Published certificates
- Remote Desktop Sessions settings
- Remote Control settings

You should configure important accounts to be protected from deletion by enabling the Protect From Accidental Deletion option, as shown in Figure 4-20. Unless this option is removed, the account can't be deleted. This setting doesn't stop an account from being removed deliberately, but it does stop the account from being deleted accidentally.

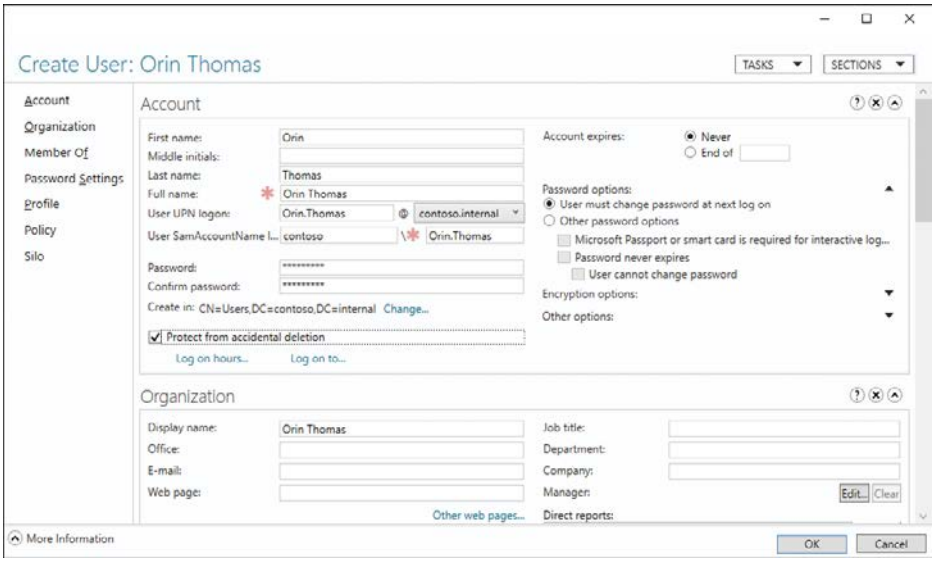

Figure 4-20 User account properties

Computer accounts

Computer accounts represent the computer within Active Directory. You often move computer accounts to specific OUs and then apply group policies to those OUs as a way of configuring the computer. When you join a computer to the domain, the computer account is automatically placed in the default Computers container.

If a computer account becomes desynchronized from the domain of which it is a member and loses its trust relationship, you can repair the relationship by signing in with the local Administrator account and running the following PowerShell command:

```
Test-ComputerSecureChannel -Credential Domain\<AdminAccount> -Repair
```

If you don't know the local Administrator account password but suspect that cached domain administrator credentials might be present, disconnect the computer from the network, either by physically removing the Ethernet connection or disconnecting the virtual network adapter, sign in using those credentials, and then run the PowerShell command previously mentioned. The Local Administrator Password Solution, which ensures that you don't forget the local Administrator account password, is covered in Chapter 12.

Group accounts

Active Directory supports three different types of group account scopes: domain local, global (the default), and universal. It also supports two group types: Security and Distribution. You use security groups to control access to resources, delegate permissions, and for email distribution. Distribution groups can only be used for email distribution. If your organization uses Exchange Server, you manage distribution groups through Exchange. Best practice is to place users within global groups, add those global groups to domain local groups, and assign permissions and rights directly to the domain local groups. By default, members of the Account Operators, Domain Admins, or Enterprise Admins groups can modify the membership of groups.

Universal

A universal group can hold accounts and groups from the same forest. Universal groups are stored in the global catalog. If you change the membership of a universal group, this change replicates to all global catalog servers in the forest. Universal groups are great in single forest environments where replication traffic isn't an issue or where there are few changes to universal group membership. Universal groups can be nested within other universal groups, or they can be added to domain local groups.

Global

Global groups can contain user accounts from their home domains. Global groups can also contain other global groups from its home domain. Global groups can be members of universal groups and domain local groups.

Domain local

Domain local groups can have universal groups, global groups, and domain local groups as members. Domain local groups can host accounts from any domain in the forest and accounts from domains in trusted forests. Domain local groups can only be added to domain local groups within their own domain. A domain local group can only be assigned rights and permissions within its own domain. Domain local groups cannot be added to global or universal groups.

Default groups

The groups listed in Table 4-2 are included in a Windows Server domain by default.

Table 4-2 Important groups

Group	Function
Access Control Assistance Operators	Members can query authorization attributes and permissions for resources on the computer.
Account Operators	Members can manage domain user and group accounts.
Administrators	Built-in administrators group. On a DC, this provides unlimited access to the computer and domain.
Allowed RODC Password Replication Group	Members can have their passwords replicated to RODCs.
Backup Operators	Members can override security restrictions to back up or restore files.
Cert Publishers	Members can publish certificates to AD DS.
Certificate Services DCOM Access	Members can connect to Certification Authorities.
Cloneable Domain Controllers	Domain controllers that can be cloned.
Cryptographic Operators	Can perform cryptographic operations.
Denied RODC Password Replication Group	Members cannot have their passwords replicated to RODCs.
Distributed COM Users	Can launch, activate, and use Distributed COM objects.
DNSAdmins	DNS administrators group.
DNSUpdateProxy	Group for DNS clients who are able to perform dynamic updates on behalf of services, such as DHCP servers.
Domain Admins	Members can administer the domain. Automatically add members of the local Administrators group on every computer in the domain. The default owner of all objects created in Active Directory.
Domain Computers	All computers that are members of the domain.
Domain Controllers	All domain controllers in the domain.
Domain Guests	Hosts the built-in domain guest account.
Domain Users	Hosts all user accounts in the domain.
Enterprise Admins	Only present in the root domain of a forest. Can make forest-wide changes, such as raising the forest functional level or adding domains.
Enterprise Key Admins	Members can perform administrative tasks on key objects at the forest level.
Enterprise Read-only Domain Controllers	Group for enterprise read-only domain controllers.
Event Log Readers	Can view the contents of event logs on the computer.
Group Policy Creator Owners	Members can create and modify GPOs.
Hyper-V Administrators	Can manage Hyper-V on the local machine.

Group	Function
IIS_IUSRS	Internet Information Services built-in group.
Incoming Forest Trust Builders	Members can create incoming, one-way trusts to the forest.
Key Admins	Members can perform administrative tasks on key objects at the domain level.
Network Configuration Operators	Members can configure networking features.
Performance Log Users	Members can schedule logging of performance counters and collect event traces.
Performance Monitor Users	Members can access performance counter data locally and remotely.
Pre-Windows 2000 Compatible Access	A group that exists for backward compatibility.
Print Operators	Members can manage printers deployed on domain controllers.
Protected Users	Members of this group have stricter security controls applied to their accounts.
RAS and IAS Servers	Members in this group are able to access the remote access settings of user accounts.
RDS Endpoint Servers	Servers in this group host VMs used with RemoteApp programs and personal virtual desktops.
RDS Management Servers	Servers in this group can perform administrative actions on other servers running the Remote Desktop Services role.
RDS Remote Access Servers	Servers in this group enable users of RemoteApp programs and personal virtual desktops to access resources.
Read-only Domain Controllers	Read-only domain controllers in the domain.
Remote Desktop Users	Granted the right to sign on using Remote Desktop.
Remote Management Users	Members can access WMI resources over management protocols.
Replicator	Group supporting file replication at the domain level.
Schema Admins	Root domain group. Members are authorized to make changes to the Active Directory Schema.
Server Operators	Members can administer domain member servers.
Storage Replica Administrators	Members can manage storage replicas.
Terminal Server License Servers	Members can update Active Directory information about terminal services licensing.
Users	Built-in Users group.
Windows Authorization Access Group	Have access to the computed `tokenGroupGlobalAndUniversal` attribute on User objects.

Service accounts

Service accounts are functionally user accounts used by services to interact with the operating system and resources on the network. By assigning rights to the service account, you can limit what the service can or cannot do.

One of the key things to remember about a service account is that it should not have the right to log on locally to a computer but should have the log on as a service right. This is important because administrators in many organizations have bad habits where they grant service accounts unnecessary rights and even go as far as to give all service accounts the same non-expiring password. Sophisticated attackers know this and use this to compromise service accounts and use them as a way to gain privileged access.

Local System

The Local System (`NT AUTHORITY\SYSTEM`) account is a built-in account. It has privileges equivalent to a local administrator account on the local computer. It acts with the computer account's credentials when interacting on the network. This is the most powerful service account, and generally, you should be reluctant to assign this service account manually to a service given its extensive privileges.

Local Service

The Local Service (`NT AUTHORITY\LocalService`) account has the same level of privilege as user accounts that are members of the local Users group on a computer. This account has fewer local privileges than the Local System account. Any services assigned to this account access network resources as a null session without credentials. Use this account when the service doesn't require network access or can access network resources as an anonymous user and requires only minimal privileges on the computer it is being used on.

Network Service

The Network Service (`NT AUTHORITY\NetworkService`) account is similar to the Local Service account in that it has privileges on the local computer equivalent to those assigned to a member of the local Users group. The primary difference is that this account interacts with the computer account's credentials to access resources on the network.

GMSA

A group managed service account (GMSA) is a service account that is managed by the domain. This means that rather than having to update the service account's password manually, Active Directory updates the password in line with the domain password policy. Many organizations that use regular user accounts as service accounts tend to set a static password for these accounts, which is often simple rather than complex.

Group Managed Service Accounts require the forest functional level to be Windows Server 2012 or higher. Forests at the Windows Server 2008 level support a version of a GMSA called an MSA, but this is more limited than a GMSA, with each MSA only being able to be installed on a single machine.

Prior to using GMSAs, you'll need to create a Key Distribution Services (KDS) root key. You can do this with the following command:

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

You manage GMSAs using Windows PowerShell. To create a GMSA, specify the name of the account, a DNS hostname associated with the account, and the name of the security principals that are allowed to use the account. For example, to create a GMSA named `MEL-SQL-GMSA` for the `contoso.internal` domain that can be used by servers in the MEL-SQL-Servers security group, enact the following command:

```
New-ADServiceAccount MEL-SQL-GMSA -DNSHostname MEL-SQL-GMSA.contso.internal
-PrincipalsAllowedToRetrieveManagedPassword MEL-SQL-Servers
```

To install the account on a specific server so that you can use it, run the `Install-ADService-Account cmdlet`. For example, to install the `MEL-SQL-GMSA account` on a server so that you can assign the account to services, enact the command:

```
Install-ADServiceAccount MEL-SQL-GMSA
```

Prior to running this command, you may need to install the RSAT ADDS Tools on the local server. You can do this by running the command:

```
Install-WindowsFeature RSAT-ADDS-Tools
```

When assigning the account to a service, you should clear the Password and Confirm Password textbox. You'll need to append $ to the account name when configuring it as shown in Figure 4-21. Windows Server recognizes that the account is a GMSA and manages the password settings.

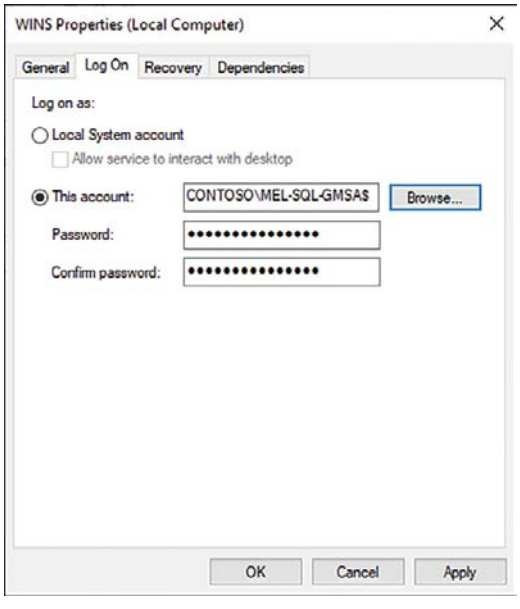

Figure 4-21 GMSA configuration

dMSA

A Delegated Managed Service Account (dMSA) is a new type of service account introduced in Windows Server 2025. dMSAs are tied to specific machine identities in Active Directory, ensuring that only designated devices can authenticate using the account. This binding enhances security by preventing unauthorized use of service account credentials. dMSAs benefit from automatic password management, with secrets stored exclusively on domain controllers.

When used with Credential Guard, dMSAs leverage virtualization-based security to protect secrets, mitigating risks associated with credential theft techniques like Kerberoasting.

To install and configure a dMSA, ensure that the KDS root key exists using

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

Create the dMSA using the following PowerShell command:

```
$params = @{
  Name = "ServiceAccountName"
  DNSHostName = "DNSHostName"
  CreateDelegatedServiceAccount = $true
  KerberosEncryptionType = "AES256"
}
New-ADServiceAccount @params
```

Use the following command to allow a specific computer account to interact with the dMSA password, substituting `Machine$` with `ComputerName$`:

```
$params = @{
  Identity = "DMSA Name"
  PrincipalsAllowedToRetrieveManagedPassword = "Machine$"
}
Set-ADServiceAccount @params
```

Configure the appropriate delegation state using the following command:

```
$params = @{ Identity = "dMSAsnmp"; Properties = @{ "msDS-DelegatedMSAState" = 3 } }
Set-ADServiceAccount @params
```

Then, on the target computer, run the following command to install the dMSA:

```
Install-ADServiceAccount -Identity "ServiceAccountName"
```

You can then configure a service to use the dMSA by setting the service to log on as the dMSA account in the format `domain\dMSA$`.

Virtual account

A virtual account is the local equivalent of a group-managed service account. Virtual accounts are supported by products such as SQL Server as an alternative to the default built-in accounts.

You can create virtual service accounts by editing the properties of a service and setting the account name to `NT Service\<ServiceName>`.

Kerberos delegation

Kerberos constrained delegation restricts how and where application services can act on a user's behalf. You can configure accounts so that they can be used only for specific tasks. For example, Figure 4-22 shows configuring the delegation of the account for computer SYD-B, for delegation through Kerberos, for the time service on computer SYD-A. You can configure Kerberos delegation using the `Set-ADComputer`, `Set-ADServiceAccount`, and `Set-ADUser` cmdlets with the `PrincipalsAllowedToDelegateAccount` parameter.

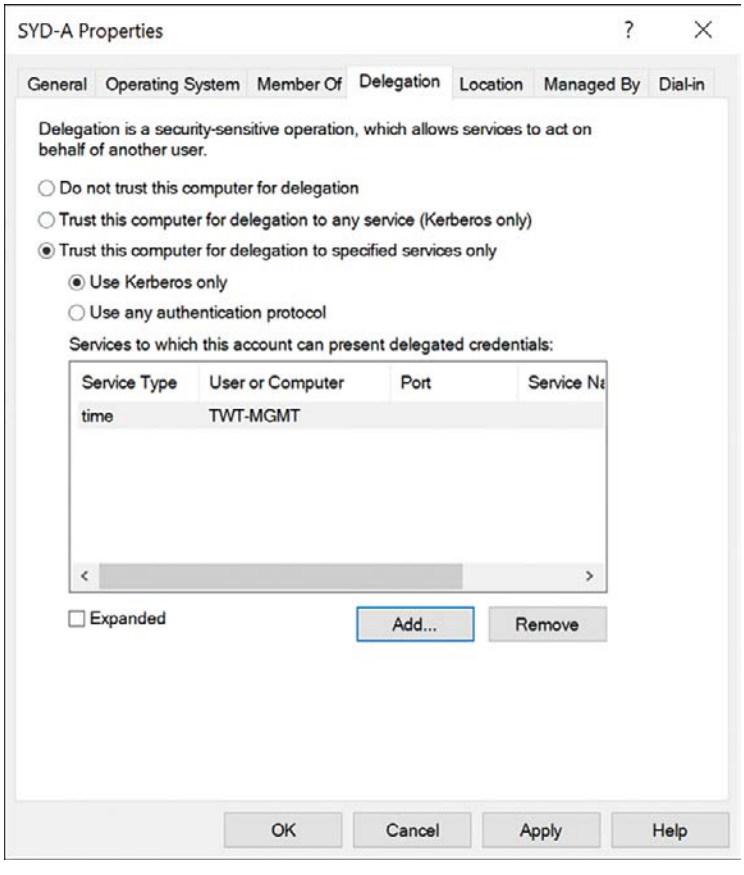

Figure 4-22 Kerberos delegation

Kerberos policies

Kerberos policies determine how the service and user tickets are used in the Authentication function in an Active Directory domain. Like password and account lockout policy, Kerberos policy is applied at the domain level. Kerberos policies applied at the site and organizational level do not affect the resultant Kerberos policy. Kerberos policies are located in the `Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Kerberos Policy` node.

You can configure the following Kerberos policies:

- **Enforce User Logon Restrictions** Ensures that Kerberos checks every request for a session ticket, also known as a service ticket.
- **Maximum Lifetime For Service Ticket** Configures the maximum lifetime of a service ticket, which is also known as a session ticket. The default value for this policy is 10 hours. The value of this policy must be less than or equal to the value specified in the Maximum Lifetime For User Ticket policy.
- **Maximum Lifetime For User Ticket** Determines the maximum lifetime of a user ticket, also known as a ticket-granting ticket (TGT). The default value of this policy is 10 hours.
- **Maximum Lifetime For User Ticket Renewal** Specifies the maximum TGT renewal period. The default is seven days.
- **Maximum Tolerance For Computer Clock Synchronization** Specifies how much drift there can be in domain controller clocks before ticket errors occur. The default setting is five minutes.

Service principal name management

Kerberos clients use a service principal name (SPN) to identify a unique instance of a service on a given computer. If there are multiple instances of the same service hosted on computers in a domain or forest, each service requires a unique SPN. Service instances can be configured with multiple SPNs, as long as those SPNs are unique.

You can use the SetSPN command-line utility to configure SPNs for computers running Windows Server. SetSPN uses this syntax: `setspn serviceclass/host:portnumber servicename`. You can use `SetSPN /?` to see a list of all SPN switches. For example, to register the HTTP service using the standard port on a computer named MEL-DC in the *contoso.com* domain using a GMSA named SYD-SRVC, issue this command:

```
setpspn –s http/MEL-DC.contoso.com CONTOSO\SYD-SRVC
```

Group Policy

Group Policy provides a central way of managing user and computer configuration. You can use Group Policy to configure everything from password and auditing policies to software deployment, desktop background settings, and mappings between file extensions and default applications.

> **Inside OUT**
>
> ***Not the only configuration management option***
>
> **It's fair to say that Group Policy is really starting to show its age. On the server side, Microsoft is pushing Desired State Configuration as the primary method of managing server configuration. On the client side, you often get a better result using tools such as Configuration Manager for on-premises deployments and Intune for clients that aren't domain joined.**

GPO management

After you get beyond editing GPOs to configure settings, you need to start thinking about issues such as GPO maintenance. For example, if an important document is lost, you need to know how to recover it from backup. Do you know what to do if someone accidentally deletes a GPO that has hundreds of settings configured over a long period of time?

The main tool you'll use for managing GPOs is the Group Policy Management Console (GPMC), shown in Figure 4-23. You can use this console to back up, restore, import, copy, and migrate. You can also use this console to delegate GPO management tasks.

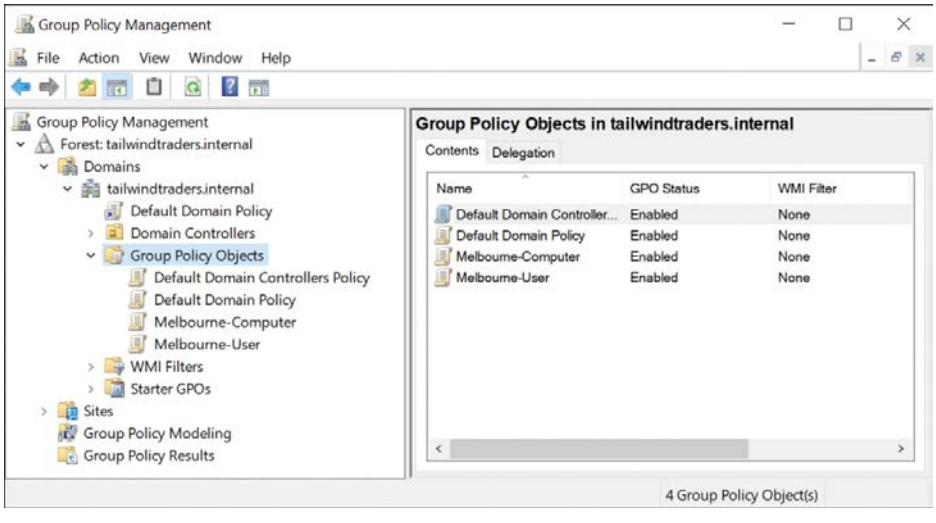

Figure 4-23 Group Policy Management Console

In larger environments, there is more than one person in the IT department. In very large organizations, one person's entire job responsibility might be creating and editing GPOs. Delegation enables you to grant permission to perform specific tasks to a specific user or group of users. You can delegate some or all of the following Group Policy management tasks:

- GPO creation
- GPO modification
- GPO linking to specific sites, organizational units (OUs), or domains
- Permission to perform Group Policy Modeling analysis at the OU or domain level
- Permission to view Group Policy Results information at the OU or domain level
- Windows Management Instrumentation (WMI) filter creation

Users in the Domain Admins and Enterprise Admins groups can perform all Group Policy management tasks. Users who are members of the Group Policy Creator Owners domain group can create GPOs. They also have the right to edit and delete any GPOs that they've created. You can delegate permissions to GPOs directly using the GPMC.

There are also a substantial number of cmdlets available in the PowerShell Group Policy module, including the following:

- `Get-GPO` Enables you to view GPOs
- `Backup-GPO` Enables you to back up GPOs
- `Import-GPO` Enables you to import a backed-up GPO into a specified GPO
- `New-GPO` Enables you to create a new GPO
- `Copy-GPO` Enables you to copy a GPO
- `Rename-GPO` Enables you to change a GPO's name
- `Restore-GPO` Enables you to restore a backed-up GPO to its original location
- `Remove-GPO` Enables you to remove a GPO

Creating GPOs

Creating a GPO is simply creating a new Group Policy Object. Newly created GPOs have no settings applied. Follow these steps to create a new GPO:

1. Open the Group Policy Management Console.
2. Under `Forest\Domains\Domain Name`, right-click Group Policy Objects and select New.
3. Provide a name for the new GPO and select OK.

If you want to delegate the ability for users to create GPOs, you can add them to the Group Policy Creator Owners group. You can also explicitly permit them to create GPOs using the GPMC. To do this, perform the following steps:

1. Open the GPMC from the Tools menu of Server Manager.
2. Expand the domain in which you want to delegate the ability to create GPOs, select Group Policy Objects, and select the Delegation tab.
3. Select Add and select the group or user that you want to give the ability to create GPOs in that domain.

Editing GPOs

To edit a GPO, users must be either a member of the Domain Admins or Enterprise Admins group. Users can edit a GPO if they

- Created it
- Have been given Read/Write permissions on the GPO through the GPMC

To grant a user permission to edit a GPO, perform the following steps:

1. Select the GPO in the GPMC.
2. Select the Delegation tab.
3. Select Add, specify the user or group that should have permission to edit the GPO, and then specify the permissions that you want to give this user or group. You can choose from one of the following permissions:
    - Read
    - Edit Settings
    - Edit Settings, Delete, Modify Security

Linking GPOs

Linking a GPO to an object such as a domain or OU involves navigating to the location in the Group Policy Management Console, right-clicking on that location, and selecting Link Existing GPO. You then select which of the existing GPOs you want to link to the domain or OU. You can also create and link a GPO using this method.

To enable a user to link a GPO to a specific object, you need to edit the permission on that object. You can perform this task in the GPMC. For example, to grant a user or group permission to link a GPO to an OU, select the OU in the GPMC, select the Delegation tab, select Add, and then select the user or group to which you want to grant this permission.

Backup GPOs

Backing up a GPO enables you to create a copy of a GPO as it exists at a specific point in time. A user must have read permission on a GPO to back it up. When you back up a GPO, the backup version of the GPO is incremented. It's good practice to back up GPOs prior to editing them so that if something goes wrong, you can revert to the unmodified GPO.

You should back up GPOs before you or other people modify them. If a problem occurs, it's quicker to restore a backup than it is to reconfigure the modified GPO with the existing settings.

To back up a GPO, perform the following steps:

1. Open the GPMC.
2. Right-click the GPO that you want to back up and select Back Up. In the Back Up Group Policy Object dialog, enter the location of the backup and a description for the backup, and then select Back Up.

You can restore a GPO using the `Restore-GPO` cmdlet. Restoring a GPO overwrites the current version of the GPO if one exists or re-creates the GPO if the GPO has been deleted. To restore a GPO, follow these steps:

1. Right-click the Group Policy Objects node in the GPMC and select Manage Backups.
2. In the Manage Backups dialog, select the GPO you want to restore and select Restore.
3. If multiple backups of the same GPO exist, you can select which version of a GPO to restore.

Import and copy GPOs

Importing a GPO enables you to take the settings in a backed-up GPO and import them into an existing GPO. To import a GPO, perform the following steps:

1. Right-click an existing GPO in the GPMC and select Import Settings.
2. In the Import Settings Wizard, you are given the option of backing up the destination GPO's settings. This enables you to roll back the import.
3. Specify the folder that hosts the backed-up GPO.
4. On the Source GPO page of the Import Settings Wizard, select the source GPO. You can view the settings that have been configured in the source GPO prior to importing it. Complete the wizard to finish importing the settings.

Remember that when you import settings from a backed-up GPO, the settings in the backed-up GPO overwrite the settings in the destination GPO.

Copying a GPO creates a new GPO and copies all configuration settings from the original to the new. You can copy GPOs from one domain to another. You can also use a migration table when copying a GPO to map security principals referenced in the source domain to security principals referenced in the destination domain.

To copy a GPO, perform the following steps:

1. Right-click the GPO that you want to copy and select Copy.
2. Right-click the location that you want to copy the GPO to and select Paste.
3. In the Copy GPO dialog, choose between using the default permissions and preserving the existing permissions assigned to the GPO.

Fixing GPO Problems

Windows Server includes command-line utilities that allow you to repair a GPO after you perform a domain rename or re-create default GPOs. If you need to re-create the default GPOs for a domain, use the `DCGPOFix` command. If you perform a domain rename, you can use the `GPFixup` command to repair name dependencies in GPOs and Group Policy links.

Migrate Group Policy Objects

When moving GPOs between domains or forests, you need to ensure that any domain-specific information is accounted for, so locations and security principals in the source domain aren't used in the destination domain. You can account for these locations and security principals using migration tables. You use *migration tables* when copying or importing GPOs.

Migration tables enable you to alter references when moving a GPO from one domain to another, or from one forest to another. An example is when you are using GPOs for software deployment and need to replace the address of a shared folder that hosts a software installation file so that it's relevant to the target domain. You can open the Migration Table Editor (MTE) by right-clicking Domains in the GPMC and selecting Open Migration Table Editor.

When you use the MTE, you can choose to populate from a GPO that's in the current domain or to populate the MTE from a backed-up GPO. When you perform this action, the MTE will be populated with settings that reference local objects. If there are no results, then no local locations are referenced in the GPO that you're going to migrate.

Inside OUT

Restoring GPO doesn't restore links

Note that restoring a GPO does not restore the GPO's links, such as links to specific OUs. You can, however, determine where the GPO was linked prior to restoring the GPO by viewing information about the backed-up GPO.

Policy processing

Group policy is processed in the following order, with subsequent policies overriding previously applied policies where conflicts exist:

- **Local** Settings configured at the local level apply first. If multiple local policies apply, settings in machine policies apply first, settings in admin and nonadmin local policies override them, and settings in per-user policies override any configured at the machine and admin/nonadmin levels.
- **Site** Policies based on location apply next. Any settings configured at the site level override settings configured at the local level. You can link multiple GPOs at the site level. When you do this, policies with a lower numerical link order override policies with a higher numerical link order.
- **Domain** Settings applied at the domain level override settings applied at the site and local levels. You can link multiple GPOs at the domain level. The Default Domain Policy is linked at this level.
- **Organizational unit (OU)** Settings applied at the organizational unit level override settings applied at the domain, site, and local levels. When an account is a member of a child OU, policies applied at the child OU level override policies applied at the parent OU level. You can apply multiple GPOs at the OU level. Policies with a lower numerical link order override policies with a higher numerical link order.

For example, if one policy configures a setting at the AD site level and another policy configures the same setting at the OU level, the policy that configures the setting at the OU level is applied.

The exception to this is when you configure one of the following settings:

- **Block Inheritance** The Block Inheritance option allows you to block upstream policies from applying. You can configure this option at the Domain or OU level. It blocks all upstream settings except those configured through a policy that has the No Override setting.
- **No Override** You use the No Override setting to stop the Block setting. Use this on policies that you need to have enforced.

Every setting that is configured in a Group Policy item will be examined during the Group Policy processing. Configuring settings you don't need increases Group Policy processing times, which can increase startup and logon times.

Resultant Set of Policy tool

The Resultant Set of Policy tool allows you to generate a model of Group Policy application, allowing you to figure out which policies apply to particular objects within the domain. Resultant Set of Policy allows you to figure out why the Group Policy application isn't behaving in the way that you expect and allows you to resolve Group Policy conflicts.

There are two ways you can calculate the Resultant Set of Policy. The first is to use Group Policy Modeling. The second is to use Group Policy Results. The difference between these is as follows:

- **Group Policy Modeling** Allows you to view the impact of altering site membership, security group membership, filtering, slow links, loopback processing, and the movement of accounts to new OUs on the application of policy.
- **Group Policy Results** Allows you to troubleshoot the application of policy by telling you which settings apply to a specific user or computer account.

By default, members of the Domain Admins and Enterprise Admins groups can generate Group Policy Modeling or Group Policy Results information. You can delegate permissions so users can perform these tasks at the OU or domain level.

Inside OUT

Policy in multidomain forests

Policies linked at the site level in multidomain forests are stored in the root domain. This can cause challenges with Group Policy application in scenarios in which a site-linked policy applies but where no DC with a root domain membership is present in the local site.

Filtering

GPO filtering allows you to determine whether a linked GPO applies based on group membership or the results of a WMI query. By default, a linked GPO will have the security filter set so it applies to Authenticated Users and no WMI filter set, as shown in Figure 4-24. If a GPO is only supposed to apply to a specific group of users or computers in the domain, site, or OU, specify the security group and remove the Authenticated Users group.

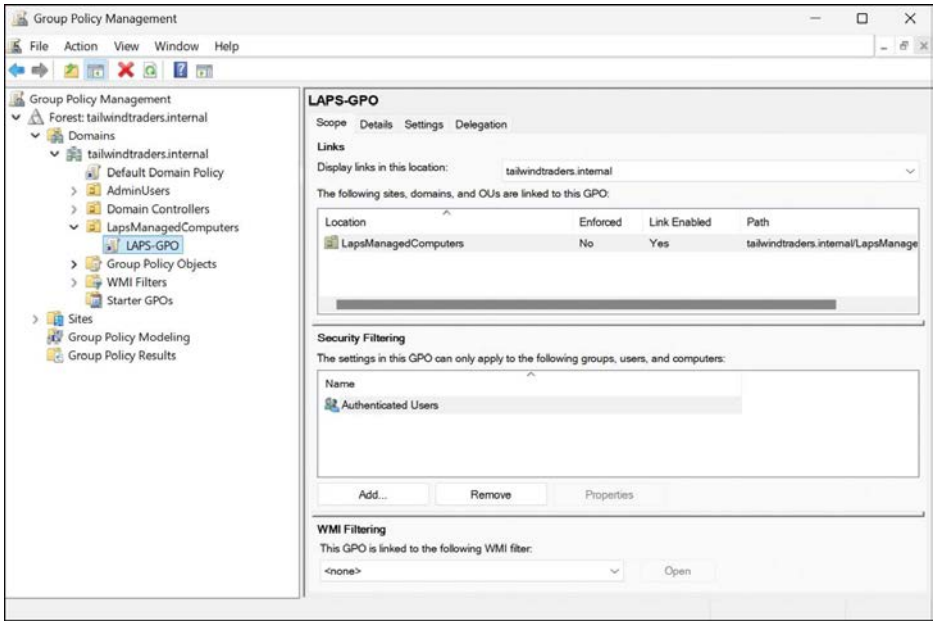

Figure 4-24 GPO filtering

For example, you could write a WMI query that performs a check so that a GPO only applies if the computer has more than 4 GB of RAM. If the computer has more than 4 GB of RAM, the policy applies normally. If the computer has less than 4 GB of RAM, the GPO does not apply. WMI filters must be assessed, which can slow down Group Policy processing. Many of the scenarios in which WMI filtering might have been appropriate 20 years ago can be better accomplished using PowerShell scripts.

Inside OUT

Site-linked GPOs

If Group Policy processing takes too long because of site-linked GPOs, the simplest solution is not to link polices at the site level; instead, you apply the links at the domain level and use Group Policy filtering through a WMI query to ensure location-specific GPOs are applied. An alternative is to place domain controllers that have root domain membership at each site, although this is likely to be more expensive than the policy filtering option.

Loopback processing

Each GPO has two distinct sections: Computer Configuration and User Configuration. The resultant policies for a user are based on the cumulative user configuration settings in GPOs that apply to the user's accounts at the site, domain, and OU settings. The resultant computer policies are applied based on the cumulative computer configuration settings in GPOs that apply to the computer's account at the site, domain, and OU level.

In some situations, you'll want only the GPOs that apply to the computer account to apply. You might want to do this with conference room computers, for which you want people to be able to sign on with domain accounts but to have a very controlled configuration. When you enable loopback processing, user settings are determined based on the settings in the User Configuration settings area of GPOs that apply to the computer account.

There are two types of loopback processing that you can configure by setting the Group Policy loopback processing mode policy. This policy is located under the `Computer Configuration\Administrative Templates\System\Group Policy` node and can be configured with the following settings:

- **Replace** When you configure Replace, only the GPOs that apply to the computer account will apply. Settings in the User Configuration area of the GPOs that apply to the computer account will apply.
- **Merge** The settings in the User Configuration area of GPOs that apply to the user account will still apply but will be overridden by settings in the User Configuration area of GPOs that apply to the computer account.

Slow-link processing enables you to configure Group Policy application to be performed differently, depending on the speed of the connection from the client to the domain controller. It enables you to block activities such as software deployment when the connection between Active Directory and the client is detected as falling below a particular threshold. You configure slow-link detection by configuring the Group Policy slow-link detection policy located under `Computer Configuration\Administrative Templates\System\Group Policy`. When a slow link is detected, Registry settings from administrative templates, security policies, EFS recovery policy, and firewall policies are applied. Policies related to application deployment, scripts, folder redirection, and disk quotas will not be applied.

Group Policy caching

Group Policy caching reduces the amount of time taken to process Group Policy during computer startup and user sign-on. Rather than retrieve the Group Policies that apply to the computer from a domain controller when a computer starts up or a user signs on, the client will use a cached copy of the last Group Policies downloaded from the domain controller. After this initial application of the cached policies during startup and user sign-on, policies will be retrieved and applied normally from a domain controller. You enable Group Policy caching by configuring the Configure Group Policy Caching policy. This policy is located under `Computer Configuration\Policies\Administrative Templates\System\Group Policy`.

Force Remote Group Policy update

Remote Group Policy update allows you to force a remote computer to perform a Group Policy update without having to sign on to the computer and run the `GPUpdate` command or the `Invoke-GPUpdate` PowerShell cmdlet. Remote Group Policy requires that the following firewall rules be enabled on clients:

- Remote Scheduled Tasks Management (RPC)
- Remote Scheduled Tasks Management (RPC-EPMAP)
- Windows Management Instrumentation (WMI-In)

You can run a remote Group Policy update from the Group Policy Management Console by right-clicking on a container or OU. An update will run on all computers within the container or OU, as well as on any computer accounts stored within child OUs. You can also use the `Invoke-GPUpdate` PowerShell cmdlet to trigger a remote Group Policy update. The advantage of the PowerShell cmdlet is that you can target a specific computer rather than all computer accounts in an OU.

Group Policy preferences

Group Policy preferences work around the idea of eliminating (or at least substantially reducing) the need for traditional start-up and log-in scripts. Log-in scripts have a way of becoming convoluted over time. Group Policy preferences allow simplification of common log-in and start-up script tasks, such as drive mappings and setting environment variables.

By reducing or eliminating some of the complexity of log-in scripts, you can use Group Policy preferences to reduce configuration errors. You can use Group Policy preferences to configure the following settings:

- Applications
- Drive mappings
- Environment variables
- File updates
- Folders
- `Ini` files
- Registry settings
- Shortcuts

- Data sources
- Devices
- Folder options
- Internet settings
- Local users and groups
- Network options
- Network shares
- Power options
- Printer settings
- Regional options
- Scheduled tasks
- Start Menu settings

Some of these items can also be configured using a traditional Group Policy. In the event that an item is configured in the same GPO using both policy and preferences, the traditional setting takes precedence. The difference between a Group Policy preference and a normal Group Policy setting is that users can change a Group Policy preference if they have the appropriate permissions. For example, users can unmap a mapped network drive. The drive would remain unmapped until the user logged in again, at which point it would be remapped. Generally, if you want to enforce a setting, use a standard Group Policy. If you want to apply the setting and allow users to change it, use a Group Policy preference. The closest you can come to enforcing a Group Policy preference is to disable the Apply Once And Do Not Reapply setting in the policy item's configuration. This way, the preference is applied each time Group Policy refreshes.

You can target Group Policy preferences so that different preferences can apply to the same item types within a single GPO. You can use the following items to restrict how a Group Policy preference applies:

- The computer has a battery.
- The computer has a specific name.
- The computer has a specific CPU speed.
- Apply by or after a specific date.
- The computer has a certain amount of disk space.

- The computer is a member of a domain.
- The computer has a particular environment variable set.
- A certain file is present on the computer.
- The computer is within a particular IP address range.
- The computer uses specific language settings.
- The computer meets the requirements of an LDAP query.
- The computer has a MAC address within a specific range.
- The computer meets the requirements of a WMI query.
- The computer uses a specific type of network connection.
- The computer is running a specific operating system.
- The computer is a member of a specific OU.
- The computer has PCMCIA.
- The computer is portable.
- The computer uses a specific processing mode.
- The computer has a certain amount of RAM.
- The computer has a certain registry entry.
- User or computer is a member of a specific security group.
- The computer is in a specific Active Directory site.
- The computer has a Remote Desktop Setting.
- That a specific time range is present.
- The user has a specific name.

Administrative templates

Group Policy Administrative Templates allow you to extend Group Policy beyond the settings available in GPOs. Common software packages, such as Microsoft Office, often include Administrative Templates that you can import to manage software-specific settings. In early versions of Windows Server, Administrative Templates were available as files in ADM format. Since the release of Windows Server 2008, Administrative Templates are available in a standards-based XML file format called ADMX.

To be able to use an Administrative Template, you can import it directly into a GPO using the Add/Remove Templates option when you right-click the Administrative Templates node. A second option is to copy the Administrative Template files to the Central Store, located in the `c:\Windows\Sysvol\sysvol\<domainname>\Policies\PolicyDefinitions` folder on any domain controller. You might need to create this folder if it does not already exist. After the folder is present, the template is then replicated to all domain controllers, and you can access the newly imported Administrative Templates through the Administrative Templates node of a GPO.

Reverting settings configured by Group Policy

Removing or unlinking a GPO does not always revert the affected settings on client machines. The outcome depends on the type of policy, how it was applied, and the nature of the setting. Consider the following when trying to revert settings applied using Group Policy:

- Group Policy Preferences write their values directly into the standard registry or system configuration areas, not the special policy areas. This process is sometimes termed "tattooing." When the GPO or preference is removed, the setting remains at its last-applied value and is not reverted or reset to the previous or default state. The original value is overwritten and lost, so the system retains the "tattooed" configuration until it's changed by another means.
- Some policy settings do not revert to their previous or default state when the GPO is set to "Not Configured" or removed. Instead, the system keeps the last value set by the policy. This is especially common with certain registry-based settings.
- Changes to service startup types, file/folder permissions, or other system configurations that are not managed exclusively through policy areas may persist after a GPO is removed.

Inside OUT

Like that before I got here

In scenarios where group policies have been used with systems that have been in production for some time, settings might have been configured long ago by policies that have since been removed. You might need to use Desired State Configuration or manual tools to change settings back to defaults that were altered by a no longer applied Group Policy Object.

Active Directory database optimization

There are several steps you can take to optimize your Active Directory database, including defragmenting the database, performing a file integrity check, and performing a semantic integrity check.

When you defragment the Active Directory database, a new copy of the database file, `Ntds.dit`, is created. You can defragment the Active Directory database or perform other operations only if the database is offline. You can take the Active Directory database offline by stopping the AD DS service, which you can do from the Update Services console or by issuing the following command from an elevated PowerShell prompt:

```
Stop-Service NTDS –force
```

You use the `ntdsutil.exe` utility to perform the defragmentation using the following command:

```
ntdsutil.exe "activate instance ntds" files "compact to c:\\" quit quit
```

After the defragmentation has completed, copy the defragmented database over the original located in `C:\windows\NTDS\ntds.dit` and delete all log files in the `C:\windows\NTDS` folder.

You can check the integrity of the file that stores the database using the `ntdsutil.exe` by issuing the following command from an elevated prompt when the AD DS service is stopped:

```
ntdsutil.exe "activate instance ntds" files integrity quit quit
```

To verify that the AD DS database is internally consistent, you can run a semantic consistency check. The semantic check can also repair the database if problems are detected. You can perform a semantic check using `ntdsutil.exe` by issuing the following command:

```
ntdsutil.exe "activate instance ntds" "semantic database analysis" "verbose on" "go
fixup" quit quit
```

Active Directory snapshots

You can use `ntdsutil.exe` to create snapshots of the Active Directory database. A *snapshot* is a point-in-time copy of the database. You can use tools to examine the contents of the database as it existed at that point in time. It's also possible to transfer objects from the snapshot of the Active Directory database back into the version currently used with your domain's domain controllers. The AD DS service must be running to create a snapshot.

To create a snapshot, execute the following command:

```
Ntdsutil snapshot "Activate Instance NTDS" create quit quit
```

A GUID identifies each snapshot. You can create a scheduled task to create snapshots on a regular basis. You can view a list of all current snapshots on a domain controller by running the following command:

```
Ntdsutil snapshot "list all" quit quit
```

To mount a snapshot, make a note of the GUID of the snapshot that you want to mount and then issue the following command:

```
Ntdsutil "activate instance ntds" snapshot "mount {GUID}" quit quit
```

When mounting snapshots, you must use the {} braces with the GUID. You can also use the snapshot number associated with the GUID when mounting the snapshot with the `ntdsutil.exe` command. This number is always odd.

When the snapshot mounts, take a note of the path associated with the snapshot. You use this path when mounting the snapshot with dsamain. For example, to use dsamain with the snapshot mounted as `c:\$SNAP_201212291630_VOLUMEc$\`, issue this command:

```
Dsamain /dbpath 'c:\$SNAP_201212291630_VOLUMEC$\Windows\NTDS\ntds.dit' /ldapport 50000
```

You can choose to mount the snapshot using any available TCP port number; `50000` is just easy to remember. Leave the PowerShell windows open when performing this action. After the snapshot is mounted, you can access it using Active Directory Users And Computers. To do this, perform the following steps:

1. Open Active Directory Users And Computers.
2. Right-click the root node and select Change Domain Controller.
3. In the Change Directory Server dialog, enter the name of the domain controller and the port, and select OK. You can then view the contents of the snapshot using Active Directory Users And Computers in the same way that you would the contents of the current directory.

You can dismount the snapshot by using Ctrl+C to close `dsamain`, and then executing the following command to dismount the snapshot:

```
Ntdsutil.exe "activate instance ntds" snapshot "unmount {GUID}" quit quit
```

Active Directory backup

AD DS is backed up when you perform a backup of the server's system state. This occurs when you back up all critical volumes on a domain controller. The primary tool you use for backing up this data is Windows Server Backup, which is not installed by default on computers running Windows Server. You can install Windows Server Backup using the following PowerShell command:

```
Install-WindowsFeature -IncludeAllSubFeature -IncludeManagementTools
Windows-Server-Backup
```

The majority of restore operations occur because Active Directory objects were accidentally (rather than deliberately) deleted. You can configure objects to be protected from accidental deletion by editing the object properties. When you attempt to delete an object that is protected from accidental deletion, a dialog will inform you that the object can't be deleted because it's protected from accidental deletion. This protection option must be removed before you or anyone else can delete the object.

Restoring deleted items

Sometimes, an Active Directory account, such as a user account or even an entire OU, is accidentally—or on occasion, maliciously—deleted. Rather than re-create the deleted item or items, you can restore the items. Deleted items are retained within the AD DS database for a period of time specified as the *tombstone lifetime*. You can recover a deleted item without having to restore the item from a backup of Active Directory as long as the item was deleted within the Tombstone Lifetime window.

The default tombstone lifetime for an Active Directory environment at the Windows Server 2008 forest functional level or higher is 180 days. You can check the value of the tombstone lifetime by issuing the following command from an elevated command prompt (substituting `dc=Contoso,dc=Internal` for the suffix of your organization's forest root domain):

```
Dsquery * "cn=Directory Service,cn=Windows NT,cn=Services,cn=Configuration,dc=Contoso,dc
=Internal" -scope base -attr tombstonelifetime
```

For most organizations, the 180-day default is fine, but some administrators might want to increase or decrease this value to give them a greater or lesser window for easily restoring deleted items. You can change the default tombstone lifetime by performing the following steps:

1. From an elevated command prompt or PowerShell session, type **ADSIEdit.msc**.
2. From the Action menu, click Connect To. In the Connection Settings dialog, click Configuration, as shown in Figure 4-25, and then click OK.
3. Right-click the CN=Services, CN=Windows NT, CN=Directory Service node and click Properties.
4. In the list of attributes, select tombstoneLifetime, as shown in Figure 4-26, and click Edit.
5. On the Integer Attribute Editor dialog, enter the new value for the tombstone lifetime and click OK twice.
6. Close the ADSI Edit console.

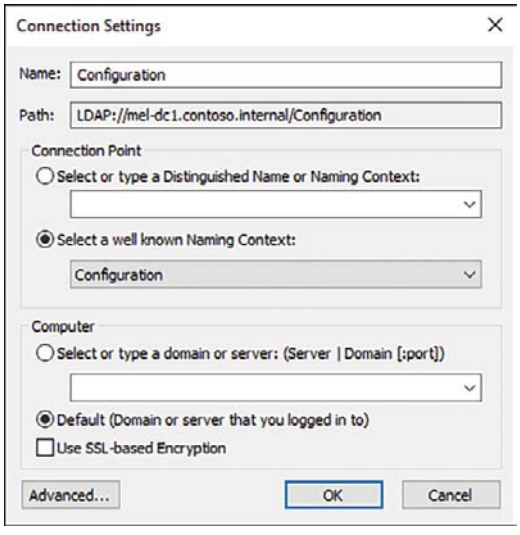

Figure 4-25 Connection settings

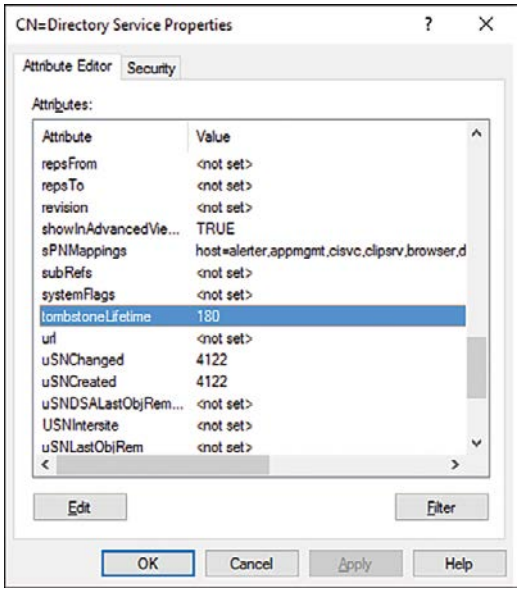

Figure 4-26 Tombstone lifetime

Active Directory Recycle Bin

Active Directory Recycle Bin allows you to restore items that have been deleted from Active Directory but are still present within the database because the tombstone lifetime has not been exceeded. Active Directory Recycle Bin requires that the domain functional level be set to Windows Server 2008 R2 or higher.

Inside OUT

Enable AD Recycle Bin first

You can't use the Active Directory Recycle Bin to restore items that were deleted before you enabled Active Directory Recycle Bin.

Once activated, you can't deactivate the Active Directory Recycle Bin. There isn't any great reason to want to deactivate AD Recycle Bin once it's activated. You don't have to use it to restore deleted items if you still prefer to go through the authoritative restore process.

To activate the Active Directory Recycle Bin, perform the following steps:

1. Open the Active Directory Administrative Center and select the domain that you want to enable.
2. In the Tasks pane, click Enable Recycle Bin, as shown in Figure 4-27.

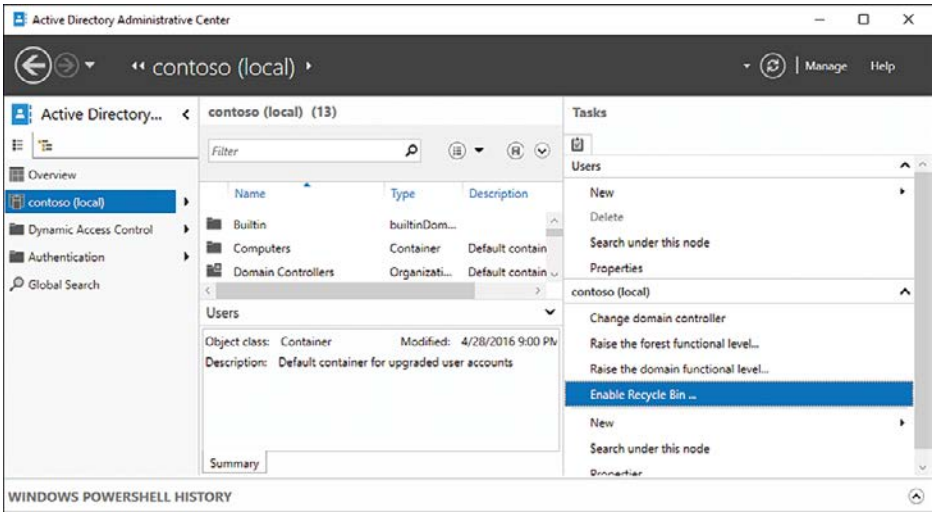

Figure 4-27 Enable Recycle Bin

After you've enabled the AD Recycle Bin, you can restore an object from the newly available Deleted Objects container. This is, of course, assuming that the object was deleted after the Recycle Bin was enabled and assuming that the tombstone lifetime value has not been exceeded. To recover the object, select the object in the Deleted Items container and then click Restore or Restore To. Figure 4-28 shows a deleted item being selected, which can then be restored to its original location. The Restore To option allows you to restore the object to another available location, such as another OU.

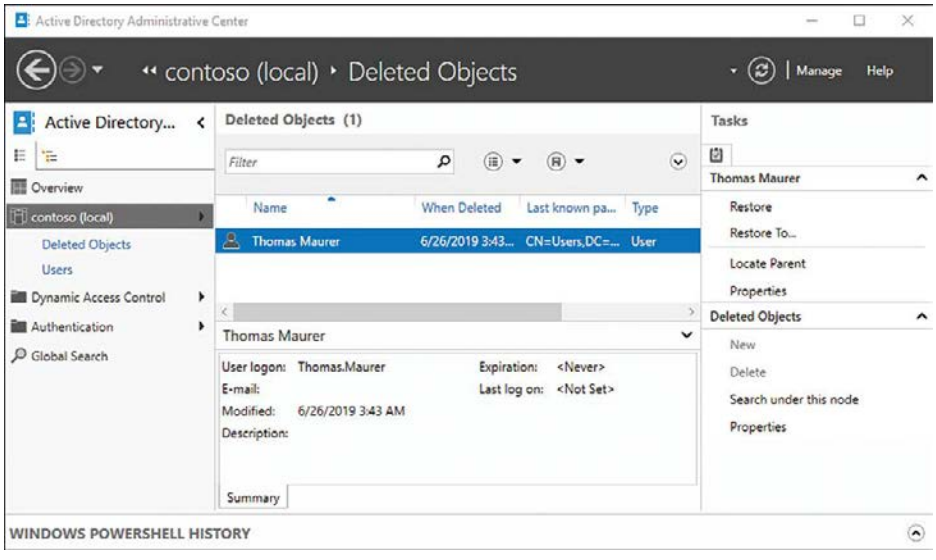

Figure 4-28 Deleted Objects container

Authoritative restore

An authoritative restore is performed when you want the items you are recovering to overwrite items that are in the current Active Directory database. If you don't perform an authoritative restore, Active Directory assumes that the restored data is simply out of date and overwrites it when it's synchronized from another domain controller. If you perform a normal Restore on an item that was backed up last Tuesday, when it was deleted the following Thursday, the item is deleted the next time the Active Directory database is synchronized. You do not need to perform an authoritative restore if you only have one domain controller in your organization because there is no other domain controller that can overwrite the changes.

An authoritative restore is useful in the following scenarios:

- You haven't enabled Active Directory Recycle Bin.
- You have enabled Active Directory Recycle Bin, but the object you want to restore was deleted before you enabled Active Directory Recycle Bin.
- You need to restore items that are older than the tombstone lifetime of the AD DS database.

To perform an authoritative restore, you need to reboot a DC into Directory Services Restore Mode. If you want to restore an item that's older than the tombstone lifetime of the AD DS database, you also need to restore the AD DS database. You can do this by restoring the system state data on the server. You'll likely need to take the DC temporarily off the network to perform this operation, because if you restore a computer with old system state data and the DC synchronizes, all the data that you want to recover will be deleted when the domain controller synchronizes.

You can configure a server to boot into Directory Services Restore Mode from the System Configuration utility. To do this, select the Active Directory Repair option on the Boot tab as shown in Figure 4-29. After you've finished with Directory Services Restore Mode, use this same utility to restore normal boot functionality.

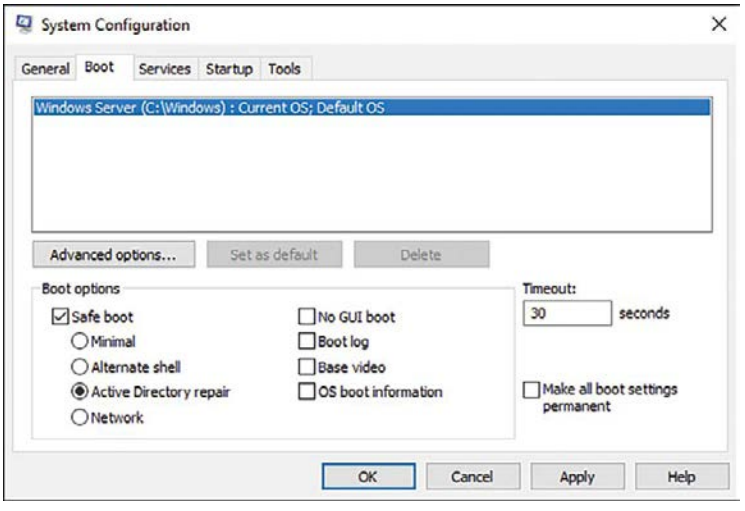

Figure 4-29 System Configuration

To enter Directory Services Restore Mode, you need to enter the Directory Services Restore Mode password.

To perform an authoritative restore, perform the following general steps:

1. Choose a computer that functions as a global catalog server. This DC functions as your restore server.
2. Locate the most recent system state backup that contains the objects that you want to restore.
3. Restart the restore server in DSRM mode. Enter the DSRM password.

4. Restore the system state data.

5. Use the following command to restore items (where `Mercury` is the object name, `Planets` is the OU that it is contained in, and *contoso.com* is the host domain):

```
Ntdsutil "authoritative restore" "restore object
cn=Mercury,ou=Planets,dc=contoso,dc=com" q q
```

6. If an entire OU is deleted, you can use the Restore Subtree option. For example, if you deleted the Planets OU and all the accounts that it held in the *contoso.com* domain, you could use the following command to restore it and all the items it contained:

```
Ntdsutil "authoritative restore" "restore subtree OU=Planets,DC=contoso,DC=com" q
q
```

Active Directory snapshots

You can use the Active Directory database mounting tool, `dsamain.exe`, to mount the contents of the AD DS database as it exists in snapshots or in backups so that you can interact with it using the Active Directory Users and Computers console. This provides you with a quick way of checking the state of a snapshot or backup without actually having to restore it to a production or development environment. For example, you might do this if you want to check what the AD DS database looked like at a specific point in time to determine the state of particular accounts or organizational units.

If you restored the AD DS database file, `ntds.dit`, to the location `c:\restore`, you could mount this file using the `dsamain.exe` utility on port 51389 by entering the following command:

```
Dsamain.exe /dbpath C:\restore\ntds.dit /ldapport 51389
```

You can then use Active Directory Users And Computers to connect to the specified port, in this case, port 51389, to view the mounted version of the AD DS database.

You can also create snapshots of the AD DS database that you can interact with without having to make a backup. A snapshot is a copy of the AD DS database as it exists at a specific point in time. You create a snapshot of the AD DS database by running the following command from an elevated command prompt on a domain controller:

```
Ntdsutil "Activate Instance NTDS" snapshot create quit quit
```

You can list all current snapshots of the AD DS database on a domain controller by running the following command:

```
Ntdsutil snapshot "list all" quit quit
```

Each snapshot has an odd number associated with it next to the date the snapshot was taken. To select and mount a snapshot, use the command:

```
Ntdsutil snapshot "list all" "mount 1" quit quit
```

This mounts `snapshot 1`. Make a note of the path on which the snapshot is mounted. You can then use the `dsadmin.exe` command to mount the snapshot so that it is accessible as an LDAP server. For example, to make the snapshot at path `C:\$SNAP_201606100306_VOLUMEC$\` accessible on port 51389, use the command

```
Dsamain.exe /dbpath C:\$SNAP_201606100306_VOLUMEC$\WINDOWS\NTDS\ntds.dit /ldapport 51389
```

You can then use Active Directory Users And Computers to connect to the specified port to view the mounted snapshot. Only members of the Domain Admins and Enterprise Admins groups can view snapshots. While you can't directly copy objects from a snapshot to the production version of the AD DS database, you can use utilities such as CSVDE and LDIFDE to export information from a snapshot and then later import it into the production AD DS database.

Managing AD DS with PowerShell

Many Active Directory administrative tasks are repetitive. If you're likely to perform a task more than once, it's better to script it in PowerShell than work your way through the appropriate wizard multiple times.

There are three PowerShell modules related to Active Directory. The `Active Directory PowerShell` module (Table 4-3) is the one you're likely to use on a regular basis when managing Active Directory. The `GroupPolicy` module (Table 4-4) allows you to manage Group Policy from PowerShell.

Active Directory module

As already mentioned, the `Active Directory PowerShell` module (see Table 4-3) is the one you're likely to use regularly when managing Active Directory.

Table 4-3 Active Directory module cmdlets

Noun	Verbs	Function
`ADAccount`	`Unlock`, `Search`, `Enable`, `Disable`	Allows you to find, unlock, enable, or disable a user, computer, or service account.
`ADAccountAuthentication-PolicySilo`	`Set`	Allows you to configure the authentication policy or authentication policy silo of an account.
`ADAccountAuthorizationGroup`	`Get`	Gets the security groups for a specified user, computer, or service account based on its token. Uses the global catalog to determine this information.

Noun	Verbs	Function
ADAccountControl	Set	Modifies the user account control values of an Active Directory user or computer account.
ADAccountExpiration	Set, Clear	Configure account expiration.
ADAccountPassword	Set	Configure the password of a user, computer, or service account.
ADAccountResultant-PasswordReplicationPolicy	Get	Gets the password replication policy for a user, computer, or service account on a specific RODC.
ADAuthenticationPolicy	Set, Remove, New, Get	Manipulate the properties of the AD DS authentication policy.
ADAuthenticationPolicy-Expression	Show	Displays Edit Access Control Conditions, Windows Update, or SSDL security descriptors.
ADAuthenticationPolicySilo	New, Remove, Get, Set	Manipulate Active Directory Domain Services authentication policy silos.
ADAuthenticationPolicy-SiloAccess	Revoke, Grant	Manage membership of authentication policy silos.
ADCentralAccessPolicy	Remove, Get, Set, New	Manage central access rules and policies.
ADCentralAccessPolicyMember	Remove, Add	Add and remove rules from a central access policy.
ADCentralAccessRule	New, Set, Remove, Get	Manage central access rules.
ADClaimTransformLink	Set, Clear, Remove	Manage claims transforms from being applied to one or more cross-forest trust relationships.
ADClaimTransformPolicy	New, Set, Get	Manage claim transformation policy objects from Active Directory.
ADClaimType	New, Get, Remove, Set	Manage Active Directory claim types.
ADComputer	Remove, New, Set, Get	Manage Active Directory computer accounts.
ADComputerServiceAccount	Remove, Add, Get	Add service accounts from Active Directory to a local computer.
ADDCCloneConfigFile	New	Generates a clone configuration file for a domain controller.
ADDCCloningExcluded-ApplicationList	Get	Manage which Active Directory applications are excluded when cloning the configuration of a domain controller.

Noun	Verbs	Function
ADDefaultDomainPassword-Policy	Set, Get	Manage the default password policy for a domain.
ADDirectoryServer	Move	Use this cmdlet to move a DC to another AD site.
ADDirectoryServerOperation-MasterRole	Move	Move an operations master role to another computer.
ADDomain	Set, Get	View and manage the properties of a domain.
ADDomainController	Get	View the properties of a domain controller.
ADDomainController-PasswordReplicationPolicy	Remove, Get, Add	Manage which accounts can be replicated to an RODC.
ADDomainMode	Set	Set the domain functional level.
ADFineGrainedPasswordPolicy	Remove, Get, Set, New	Manage AD fine-grained password policy.
ADFineGrainedPassword-PolicySubject	Get, Remove, Add	Manage the application of fine-grained password policies.
ADForest	Set, Get	Manage forest properties.
ADForestMode	Set	Configure the forest functional level.
ADGroup	Get, Set, Remove, New	Manage AD groups.
ADGroupMember	Get, Remove, Add	Manage AD group membership.
ADObject	Get, Restore, Rename, Set, Move, Remove, Sync, New	Manage AD objects.
ADOptionalFeature	Disable, Get, Enable	Configure AD optional features.
ADOrganizationalUnit	Set, Get, New, Remove	Manage AD OUs.
ADPrincipalGroupMembership	Remove, Add, Get	Manage group membership on the basis of the user account.
ADReplicationAttribute-Metadata	Get	View replication metadata for AD object attributes.
ADReplicationConnection	Get, Set	Manage the properties of an AD replication connection.
ADReplicationFailure	Get	View information about AD replication failure.

Noun	Verbs	Function
ADReplicationPartnerMetadata	Get	View information about AD replication partners.
ADReplicationQueueOperation	Get	View all operations in the AD replication queue.
ADReplicationSite	Set, Get, Remove, New	Manage AD replication sites.
ADReplicationSiteLink	Set, New, Get, Remove	Manage AD replication site links.
ADReplicationSiteLinkBridge	Get, Remove, New, Set	Manage AD replication site link bridges.
ADReplicationSubnet	New, Get, Set, Remove	Manage AD replication subnets.
ADReplicationUpToDateness-VectorTable	Get	Displays Update Sequence Numbers (USNs) for domain controllers.
ADResourceProperty	Set, New, Remove, Get	Manage Active Directory resource properties.
ADResourcePropertyList	Remove, Set, New, Get	Manage Active Directory resource property list.
ADResourcePropertyListMember	Remove, Add	Add and remove resource properties from an Active Directory resource property list.
ADResourcePropertyValueType	Get	View a resource property value type.
ADRootDSE	Get	View the root of a Directory Server information tree.
ADServiceAccount	Get, Test, Set, Install, New, Remove, Uninstall	Manage the AD Managed Service Account.
ADServiceAccountPassword	Reset	Reset the AD Managed Service Account password.
ADTrust	Get	View the properties of an AD Trust.
ADUser	New, Set, Get, Remove	Manage an Active Directory user.
ADUserResultantPassword-Policy	Get	Use this cmdlet to determine the resultant password policy for an account that has multiple fine-grained password policies applied to it.

Group Policy module

As mentioned earlier, the `GroupPolicy module` (see Table 4-4) allows you to manage Group Policy from PowerShell.

Table 4-4 Group Policy module cmdlets

Noun	Verbs	Function
GPInheritance	Get, Set	View and manage which GPOs are applied and whether inheritance is blocked.
GPLink	Remove, New, Set	Manage whether a GPO is linked.
GPO	Restore, Import, New, Remove, Rename, Backup, Get, Copy	Manage GPOs, including backup restore and copy.
GPOReport	Get	Generate a report on a GPO.
GPPermission	Set, Get	Manage permissions on policies.
GPPrefRegistryValue	Remove, Set, Get,	Manage registry-based policy preference settings. Microsoft maintains spreadsheets that map Group Policy settings to registry settings. To use this cmdlet to set registry settings, you need to consult the spreadsheet.
GPRegistryValue	Remove, Get, Set,	Manage registry-based policy settings.
GPResultantSetOf-Policy	Get	View the resultant set of policy information.
GPStarterGPO	New, Get	Manage the starter GPO.
GPUpdate	Invoke	Triggers a Group Policy update.

ADDSDeployment module

As previously mentioned, you use the ADDSDeployment (see Table 4-4) module when performing deployment tasks.

Table 4-4 Active Directory module cmdlets

Noun	Verbs	Function
ADDSDomain	Install	Installs a new Active Directory Domain Services domain.
ADDSDomainController	Install, Uninstall	Use to add or remove a domain controller.
ADDSDomainControllerInstallation	Test	Runs a prerequisite check prior to installing a domain controller.
ADDSDomainControllerUninstallation	Test	Runs a prerequisite check prior to removing a domain controller.

Noun	Verbs	Function
ADDSDomainInstallation	Test	Checks the prerequisites for a new Active Directory Domain Services domain.
ADDSForest	Install	Allows you to install a new Active Directory Forest configuration.
ADDSForestInstallation	Test	Allows you to perform a prerequisite check prior to performing an Active Directory forest installation.
ADDSReadOnlyDomainController-Account	Add	Use this cmdlet to create an RODC account in the AD DS database.
ADDSReadOnlyDomainController-AccountCreation	Test	Allows you to check that the necessary prerequisites are in place before you create an RODC account.

Index

A

A records (DNS), 196
AAAA records (DNS), 196
AccessChk, 45
access control for VPN servers, 690-693
Access Denied Assistance, 336-337, 669-670
AccessEnum, 48-49
accidental deletion, protecting from, 176
accounts (AD DS), 151-160
computer, 152-153
group, 153-155
service, 156-160
user, 151-152
activating license servers, 725
Active Directory Administrative Center (ADAC), 110-113
Active Directory Certificate Services. *See* AD CS (Active Directory Certificate Services)
Active Directory Domain Services. *See* AD DS (Active Directory Domain Services)
Active Directory Domains and Trusts console, 115
Active Directory Explorer (AD Explorer), 50-53
Active Directory Federation Services. *See* AD FS (Active Directory Federation Services)
Active Directory Migration Tool (ADMT), 766-768
Active Directory Recycle Bin, 178-179
Active Directory Rights Management Services. *See* AD RMS (Active Directory Rights Management Services)
Active Directory Sites and Services console, 115
Active Directory Users and Computers console, 113-115
Active Directory–integrated zones (DNS), 189-191
AD CS (Active Directory Certificate Services), 597-642
automatic enrollment/renewal, 626-628
CAs, 597-611
certificate revocation, 598
enterprise CAs, 599-608
hierarchies, 597-598
management, 628-642
migrating, 603
standalone CAs, 608-611
certificate templates, 618-625
deleting, 618
duplicating, 625
editing, 625
properties, 619-625
CRLs, 612-617
AIA points, 613
CDPs, 612
publishing, 615-617
revoking certificates, 613-615
hardening. *See* hardening Active Directory
migration, 768-772
preparing for, 770-771
requirements, 768-769
steps in, 771-772
verifying, 772
role services, 617
upgrades, 769
AD DS (Active Directory Domain Services), 109-187
accounts, 151-160
computer, 152-153
group, 153-155
service, 156-160
user, 151-152
administration, 109-116
Active Directory Domains and Trusts console, 115
Active Directory Sites and Services console, 115
Active Directory Users and Computers console, 113-115
ADAC, 110-113
Group Policy Management console, 116
remote versus local, 110
backing up, 175-176
creating forest trust with Entra Domain Services, 424-425
database optimization, 174
domain controllers. *See* domain controllers (DCs)
forest migration, 765-768
FRS to DFS migration, 764-765
Group Policy. *See* Group Policy
hardening. *See* hardening Active Directory
integration with Entra Domain Services, 423-424
managing Entra Domain Services instance, 425-426

PowerShell cmdlets, 182-187
replication, 147-150
conflict resolution, 149
KCC, 148
monitoring, 150
multimaster, 148
repadmin, 150
RODCs, 149-150
store-and-forward, 148
restoring deleted items, 176-182
Active Directory Recycle Bin, 178-179
authoritative restore, 179-181
snapshots, 181-182
site management, 141-146
moving domain controllers, 146
site creation, 143-144
site link bridge creation, 146
site link creation, 145-146
subnet creation, 144
snapshots, 174-175
creating, 174
dismounting, 175
mounting, 175
restoring deleted items, 181-182
structure, 127-141
domain functional levels, 129-130
domains, 127
domain trees, 128-129
ESAE forests, 131
forests, 131
FSMO roles, 132-135
intra-forest authentication, 129
multidomain forests, 128
organizational units, 131-132
trust relationships, 135-141
AD Explorer (Active Directory Explorer), 50-53
AD FS (Active Directory Federation Services), 643-659
attribute stores, 648
certificate relationships, 647-648
claim rules, 648-650
claims-based authentication components, 644-645
claims provider trust, 646-647
components, 643
hardening. *See* hardening Active Directory
Microsoft Entra Connect and, 357
multifactor authentication, 655-656
PowerShell cmdlets for, 656-659
relying party servers, 645
relying party trust, 645-646
web application proxy configuration, 650-653
Workplace Join, 653-655
AD RMS (Active Directory Rights Management Services), 319, 661-679
Access Denied Assistance, 669-670
applying templates automatically, 677-678
central access policies, 667-668
central access rules, 666-667
DAC, 661-663
exclusion policies, 677
hardening. *See* hardening Active Directory
installing, 670-676
certificates and licenses, 671-672
steps in, 670-671
templates, 672-675
user groups, 675-676
PowerShell cmdlets, 678-679
resource properties, 664-665
staged permissions, 668-669
Trusted User Domains/Trusted Publishing Domains, 677
ADAC (Active Directory Administrative Center), 110-113
adding
memory, 224
physical disks to storage pools, 272-273
roles and features, 71-72
S2D cluster nodes, 287
S2D volumes to clusters, 284-285
virtual hard disks, 237
WDS servers to VMM, 105-106
website default documents, 535-536
websites to server, 524-527
to Windows images, 76-78
address blocks (IP), 218
Add Roles and Features Wizard, 71
ADInsight (Insight for Active Directory), 53
administration. *See also* remote administration; *names of specific administration tools*
AI in, 25
automation and, 2
recommended practices, 1-3
administrative permissions, delegating, 545-546
administrative privileges
DNS servers, 204
IPAM servers, 217-219
Administrative Templates in Group Policy, 172
administrative unit management in Microsoft Entra ID, 380-381
administrators in AD RMS, 675
admin-trusted attestation, 468-470
ADMT (Active Directory Migration Tool), 766-768
advanced audit policies, 453-455
auditpol and, 455
expression-based policies, 454
file and folder auditing, 454

AES for Kerberos policy, 490-491
affinity for NLB clusters, 594-595
aging and scavenging (DNS), 197-198
AIA (Authority Information Access) points, 613
AI (artificial intelligence). *See also* LLMs (large language models)
administration with, 25
chatbots, troubleshooting solutions from, 787-788
running locally, requirements for, 800
alert rules, creating in Azure Monitor, 413-414
alerts
for event logs, 492
performance monitoring with, 731
alias (CNAME) records (DNS), 196
Always On IKEv2 VPN protocol, 685-686
AMA (Azure Monitor Agent), 388, 412-413
Annual Channel container images (SAC), 59
answer files, 79-81
App Compatibility Features on Demand (FOD), 68-69
application data, containers and, 555
application partitions, 147
application pools, 541-543
configuring recycling settings, 542-543
creating, 541-542
application-specific backups, 742
approving certificate requests, 630-631
Apt-get utility, 83
archiving private keys, 633-638
artificial intelligence. *See* AI (artificial intelligence)
ASP.NET Core Runtime container image, 561
ASR (attack surface reduction) rules, 515-517
ASR (Azure Site Recovery), 417-419
assigning user rights, 434-437
assume breach security philosophy, 497
attack surface, reducing, 109
Attack Surface Analyzer, 500-501
attack surface reduction (ASR) rules, 515-517
attack targets, domain controllers as, 109
attribute stores, 644, 648
auditing Active Directory, 491-492
auditpol, 455
audit policies, advanced, 453-455
auditpol and, 455
expression-based policies, 454
file and folder auditing, 454
authentication
CredSSP, 257
forest trust scopes, 137
inter-forest, 131
intra-forest, 129
Kerberos, 257
methods of, 532-534
in Microsoft Entra Connect, 356-357
multifactor, 655-656
VPN protocols, 688
authentication exemptions, 460-461
authentication policy silos, 483-484
authoritative restore, 119, 179-181
Authority Information Access (AIA) points, 613
authorization, DHCP servers, 212
authorization rules for websites, 538-539
automatically applying templates in AD RMS, 677-678
automatic approval rules in WSUS, 751-752
automatic certificate enrollment/renewal, 626-628
automation of administrative tasks, 2
autonomous mode (WSUS), 748
Azure AI Foundry Local, 804-808
command-line options, 804-805
configuring as a service, 806
installing, 804
Ollama comparison, 808
Open WebIU with, 806-808
requirements, 804
Azure Arc, connecting to, 384
Azure Arc–enabled servers, 382-390
Azure File Sync, 391-396
cloud endpoint creation, 392
cloud tiering configuration, 394
DFS migration, 395-396
monitoring, 394-395
server endpoint creation, 393
server registration, 393
storage sync service deployment, 391
sync group creation, 392
Azure Network Adapter, 390
Azure Policy assignments, 388-389
capabilities of, 382
HRWs, 389-390
onboarding to, 383-387
connecting to Azure Arc, 384
Microsoft Entra ID–managed identities, 383-384
with PowerShell, 385-386
requirements, 383
with service principal-based deployment, 386-387

SQL Server, 385
from Windows Server, 385
VM extensions, 387-388
Azure Arc Setup wizard, 385
Azure Automanage, 411
Azure Automation, HRWs and, 389-390
Azure Backup, 743-746
backup settings, 745
configuring in Windows Admin Center, 744-745
restoring from, 745-746
Azure Bastion, 409-410
Azure edition (Windows Server 2025), 57
Azure File Shares, creating, 392
Azure File Sync, 336-337, 391-396
cloud endpoint creation, 392
cloud tiering configuration, 394
DFS migration, 395-396
monitoring, 394-395
server endpoint creation, 393
server registration, 393
storage sync service deployment, 391
sync group creation, 392
Azure IaaS VMs
administration, 407-410
Azure Bastion, 409-410
JIT VM Access, 410
RBAC roles, 407
Remote PowerShell, 409
Windows Admin Center, 407-408
backing up, 415
benefits of, 397-398
creating, 398-401
domain-joining with Entra Domain Services, 419-426
creating forest trust, 424-425
deploying Entra Domain Services, 420-422
managing AD DS instance, 425-426
password synchronization, 423-424
login with Entra ID, 401
networking, 401-406
default outbound access, 406
IP addressing, 403-404
NSGs, 405-406
virtual networks, 401-403
VPN gateways, 406
resizing, 414-415
support services, 411-419
ASR, 417-419
Azure Automanage, 411
Azure Monitor, 412-414
encryption, 416-417
Azure Monitor, 412-414, 737-739
Azure Monitor Agent (AMA), 388, 412-413
Azure Network Adapter, 390
Azure Policy, 388-389
Azure Site Recovery (ASR), 417-419
Azure Update Manager, 753-754

B

backups
Azure Backup, 743-746
backup settings, 745
configuring in Windows Admin Center, 744-745
restoring from, 745-746
of Active Directory, 175-176, 492
of Azure IaaS VMs, 415
of CAs, 631-633
of GPOs, 164
of IIS configuration, 546
security of, 740
VSS, 746-747
Windows Server Backup, 739-743
locations for backups, 740-741
methods for backups, 741
PowerShell cmdlets, 754
restoring from backups, 742-743
role- and application-specific backups, 742
bandwidth management for VMs, 244
bare-metal servers, virtualized versus, 73
base OS images, 553-554
retrieving, 560
updating, 567
blocking
insecure passwords, 374-375
scheduled tasks, 489
block storage in VMM, 99
Blue Screen of Death (BSOD), 793
boot images, 92
boot options in WDS, 94-95
BranchCache, 343-346, 351-352
bridge networking for WSL, 431
BSOD (Blue Screen of Death), 793
build-and-capture, 79

C

cache locking (DNS), 201
caching in Group Policy, 169
campus clusters, 582
canary users, 752
CAPolicy.inf file, 638-639
CAPs (Connection Authorization Policies), 682
capture images, 92
CAs (certificate authorities), 597-611
certificate revocation, 598
enterprise CAs, 599-608
benefits of, 599
enterprise root CAs, 599-607
enterprise subordinate CAs, 608
limitations of, 599
standalone CAs versus, 608

hierarchies, 597-598
management, 628-642
approving certificate requests, 630-631
backup and recovery, 631-633
CAPolicy.inf file, 638-639
certreq.exe, 642
certutil.exe, 641-642
key archiving and recovery, 633-638
permissions, 628-630
PowerShell cmdlets, 639-641
migrating, 603
standalone CAs, 608-611
benefits of, 609
configuring client trust, 609-610
enterprise CAs versus, 608
offline root CAs, 611
standalone root CAs, 611
standalone subordinate CAs, 611

CAU (Cluster Aware Updating), 577-578
CCI (Configurable Code Integrity). *See* WDAC (Windows Defender Application Control)
CDPs (CRL distribution points), 612
Center for Internet Security (CIS), 434
central access policies, 667-668
central access rules, 666-667
certificate authorities. *See* CAs (certificate authorities)
certificate relationships, configuring, 647-648
certificate requests, approving, 630-631
certificate requirements, SMB over QUIC, 346
certificate revocation lists. *See* CRLs (certificate revocation lists)
certificates. See also AD CS (Active Directory Certificate Services)
in AD RMS, 671-672
automatic enrollment/renewal, 626-628
for DirectAccess servers, 699
for RD Gateway servers, 683
renewing, 599
revoking, 598, 613-615
TLS
configuring, 529-531
self-signed, 527
trust relationships, 598
for VPNs, 685
for web application proxy servers, 651-653
Windows Admin Center and, 8
Certificate Services. *See* AD CS (Active Directory Certificate Services)
certificate templates, 618-625
deleting, 618
duplicating, 625
editing, 625
properties, 619-625
certreq.exe, 642
certutil.exe, 641-642
CFG (Control Flow Guard), 503-504
channel binding (LDAP), 488
chatbots, troubleshooting solutions from, 787-788
checkpoints, 239-240
Chocolatey, 85-87, 563
choosing Storage Layouts, 274-275
CIS (Center for Internet Security), 434
claim rules, 644, 648-650
claims, 644, 663
claims-based authentication, 644-645
claims providers, 645
claims provider trust, 646-647
claims provider trust claim rules, 649-650
classic scheduler (Hyper-V), 232
classification in FSRM, 332-334
classification properties, configuring, 332-333
classification rules, configuring, 333-334
cleaning up file servers, 336
client access control, configuring in SMB over QUIC, 348
client configuration in RD Gateway, 683-685
Client Naming Policy (in WDS), 94
cloning
domain controllers, 261-262
virtual domain controllers, 126-127
cloud endpoints, creating, 392
cloud tiering, configuring, 394
Cloud Witness, 581-582
Cluster Aware Updating (CAU), 577-578
clustering. *See* failover clustering
cluster management for NLB clusters, 593-594
cluster networks, 576
cluster nodes (S2D)
adding, 287
maintenance on, 288
cluster operation modes for NLB, 592-593
cluster quorum modes, 574-575
clusters in AD RMS, 670
cluster sets, 587-588
Cluster Shared Volumes (CSVs), 253, 576, 583
clusters. *See* failover clusters; guest clusters
cluster-to-cluster configuration (Storage Replica), 289
cmdlets, functions versus, 443. *See also* PowerShell
CNAME (alias) records (DNS), 196

command-line options
Foundry Local, 804-805
Ollama, 801-802
command-line tools, 34-39
committing Windows images, 78
compatibility, security controls and, 433
compression (SMB), 294-295
computer accounts, 152-153, 481-482
computer configuration settings (GPOs), 169
conditional forwarders, 194
Configurable Code Integrity (CCI). *See* WDAC (Windows Defender Application Control)
configuration management, Desired State Configuration, 72
configuration partitions, 147
configuring. *See also* enabling
application pool recycling settings, 542-543
Azure AI Foundry Local as a service, 806
Azure Backup, 744-745
certificate relationships, 647-648
classification properties, 332-333
classification rules, 333-334
client access control in SMB over QUIC, 348
client trust, 609-610
client in RD Gateway, 683-685
cloud tiering, 394
data collection rules, 413
DirectAccess, 700-703
Docker Engine settings, 557-560
file servers for SMB over QUIC, 348
group policies for BranchCache, 344-346
group policies for Remote Desktop Session Host, 715-719
IPsec in firewall, 458-460
multiforest AD DS synchronization, 367-368
object filters, 366
password synchronization, 367
recovery agents, 634-637
remote website management, 544
resource properties, 664-665
selective authentication, 137
sites (AD DS), 141-142
TLS certificates, 529-531
WDS options, 92-96
WDS transmissions, 96-97
web application proxy, 650-653
conflict resolution, 149, 340
Connection Authorization Policies (CAPs), 682
connection request policies, 690-691
connection security rules, 460-465
consoles (RSAT)
list of, 10-13
Server Manager, 14-15
constrained delegation, 485-486
containerd, 557
container hosts, 555
container images, 553-554
creating, 563-565
on DockerHub registry, 560-561
managing, 565
container registries, 555, 560-561
containers, 553-571
application data and, 555
Chocolatey and, 563
configuring Docker Engine settings, 557-560
creating container images, 563-565
defined, 553
dockerfiles, 564-565
Docker syntax, 556
installing Docker, 557
isolation modes, 555-556
Linux Containers on Windows, 429
managing images, 565
modifying, 563
naming, 562
networking, 562, 567-571
L2 Bridge, 571
NAT, 568-569
overlay, 570
transparent, 570
types of modes, 567-568
retrieving base OS images, 560
service accounts for, 565-566
starting, 562-563
terminology, 553-555
updating, 566-567
Control Flow Guard (CFG), 503-504
Controlled Folder Access, 510-512
control panels, 34
converting
evaluation version to licensed version of Windows Server, 759-760
virtual hard disk formats, 237-238
copilot add-ons, 25
copy process in Storage Migration Service, 781-782
copying
GPOs, 165
VMs, 259
core scheduler (Hyper-V), 232
CPU groups, 232
crash dump analysis, 793-795
Credential Guard, 508-510
CredSSP (Credential Security Support Provider), 257
CRL distribution points (CDPs), 612
CRLs (certificate revocation lists), 612-617
AIA points, 613
CDPs, 612

publishing, 615-617
revoking certificates, 613-615
cryptographic options for private keys, 603-604
CSVs (Cluster Shared Volumes), 253, 576, 583
custom error messages for websites, 534-535
cutover process in Storage Migration Service, 782

D

DAC (Dynamic Access Control), 319, 354, 661-663
daemon.json, 557-560
DANE (DNS-based Authentication of Named Entities), 202
database optimization (Active Directory), 174
Datacenter edition (Windows Server 2025), 57
data collection rules, configuring, 413
data collector sets, 729-731
DCs. *See* domain controllers (DCs)
DDA (Discrete Device Assignment), 228-229, 723
debugging. *See* troubleshooting
decommissioning
domain controllers, 122-123
RODCs (Read Only Domain Controllers), 126
deductive reasoning in troubleshooting, 788
deduplication
enabling, 318
in Hyper-V, 241
of storage, 305-307, 310
default documents for websites, 535-536
default gateways in failover clustering, 577
default group accounts, 153-155
default outbound access for Azure IaaS VMs, 406
Defense Information Systems Agency (DISA), 434
delegated administration
DNS servers, 204
IPAM servers, 217-219
delegated Managed Service Accounts (dMSAs), 158, 440-441
delegating
administrative permissions, 545-546
constrained delegation, 485-486
GPO management tasks, 162
privileges, 477-479
Delegation Of Control Wizard (Active Directory), 115
deleted items, restoring, 176-182
Active Directory Recycle Bin, 178-179
authoritative restore, 179-181
snapshots, 181-182
deleting. *See also* removing
certificate templates, 618
users in Microsoft Entra ID, 376
delta CRLs (certificate revocation lists), 612, 615-617
dependencies, troubleshooting, 790-791
deploying. *See also* installing
AD DS PowerShell cmdlets, 186-187
with answer files, 79-81
domain controllers, 117-121
Entra Domain Services, 420-422
Entra ID Password Protection, 520-521
IPAM servers, 216
Log Analytics workspaces, 412
RDS, 707-709
S2D, 282
S2D clusters, 283-284
Server Core, when to deploy, 69
Storage Migration Service, 780
storage sync services, 391
virtualization hosts, 73-74
with VMM, 98-108
adding WDS servers, 105-106
host groups, 106-108
networking, 101-105
storage, 99-100
VM templates, 98-99
VMs, PowerShell scripts for, 82
VPN servers, 688-689
with WDS, 90-98
configuring options, 92-96
configuring transmissions, 96-97
driver groups/packages, 98
image management, 92
requirements, 90-91
steps in, 90
with Windows images, 74-79
build-and-capture, 79
committing images, 78
modifying images, 74-75
mounting images, 76
servicing images, 75-78
WSUS updates, 751
Deployment Image Servicing and Management (DISM), 74
deployment properties for RDS, 710-711
Desired State Configuration (DSC), 72, 87-89
detached mode for containers, 562-563
device claims, 663
Device Guard. *See* WDAC (Windows Defender Application Control)
DFS (Distributed File System), 337-343
as file share witnesses, 574
migrating from FRS, 764-765
migrating to Azure File Sync, 395-396
namespaces, 337-339
PowerShell cmdlets, 353

replication, 340-343
Windows Server 2008 mode, 339
DHCP (Dynamic Host Configuration Protocol) servers, 206-216
DHCP failover, 211-212
DHCP filtering, 209
DHCP relay agents, 213-214, 695-696
DHCP server authorization, 212
management with PowerShell, 214-216
migration, 773-777
preparing for, 774-776
steps in, 776
verifying, 777
name protection, 210
options, 208
reservations, 208
scopes, 207
multicast scopes, 210
options, 208
split scopes, 210
superscopes, 209
DHCP failover, 211-212
DHCP filtering, 209
DHCP relay agents, 213-214, 695-696
DHCP server authorization, 212
diagnostic hypothesis, 790
differencing virtual hard disks, 236-237
DirectAccess, 696-703
configuring, 700-703
NLS and, 700
server requirements, 698-700
topologies, 697-698
direction of trust, 136
directly attached disks, 238-239
directory browsing on websites, 536
Directory Services Restore Mode (DSRM), 119-120
disabling
NTLM, 486-487
VPN protocols, 689
website default documents, 535-536
DISA (Defense Information Systems Agency), 434
disaster recovery, 116. *See also* backups
discover images, 92
Discrete Device Assignment (DDA), 228-229, 723
disks. *See* physical disks; virtual disks
DISM (Deployment Image Servicing and Management), 74
dismounting snapshots (Active Directory), 175
Distributed File System. *See* DFS (Distributed File System)
dMSAs (delegated Managed Service Accounts), 158, 440-441
DNS-based Authentication of Named Entities (DANE), 202
DNS cache locking, 201
DNS (domain name system) servers, 189-206
conditional forwarders, 194
delegated administration, 204
DNSSEC, 198-199
event logs, 199-200
forwarders, 194
management with PowerShell, 204-206
migration, 772-773
options, 200-203
DANE, 202
DNS cache locking, 201
DNS recursion, 201
DNS socket pool, 200
netmask ordering, 201-202
response rate limiting, 202
policies, 203
resource records, 196-197
zone aging and scavenging, 197-198
zone delegations, 193
zone types, 189-196
Active Directory–integrated zones, 189-191
GlobalNames zones, 195-196
primary zones, 191-192
reverse lookup zones, 192-193
secondary zones, 192
stub zones, 195
DNS recursion, 201
DNS socket pool, 200
DNSSEC (Domain Name System Security Extensions), 198-199
DNSSEC Key Master, 199
Docker
configuring Docker Engine settings, 557-560
installing, 557
managing container images, 565
syntax, 556
Docker Engine on Windows, 556-557
dockerfiles, 564-565
DockerHub registry, 560-561
documentation for PowerShell, 16
domain-based namespaces, 338
domain controllers (DCs), 116-127. *See also* AD DS (Active Directory Domain Services)
as attack targets, 109
cloning, 261-262
virtual domain controllers, 126-127
converting evaluation version to licensed version, 760
decommissioning, 122-123
deploying, 117-121
DirectAccess requirements, 699
disaster recovery, 116

global catalog servers, 122
hardening, 474-476
moving, 146
operating system level, 130
RODCs, 123-126
Server Core configuration, 121
upgrading, 763-764
virtualized, 121
domain-joining Azure IaaS VMs, 419-426
creating forest trust, 424-425
deploying Entra Domain Services, 420-422
managing AD DS instance, 425-426
password synchronization, 423-424
domain local groups, 153
domain name filtering, 536-538
Domain Name System Security Extensions (DNSSEC), 198-199
domain name system servers. *See* DNS (domain name system) servers
domain names, 119
domain naming master role, 133
domain partitions, 147
domain quarantine. *See* SID filtering
domain trees, 127-129
domains, 127
functional levels, 129-130
intra-forest authentication, 129
multidomain forests, 128
trust relationships. *See* trust relationships
downloading files, 70
drift control (OSConfig), 503
driver groups/packages in WDS, 98
drivers
adding to Windows images, 76-77
troubleshooting, 796
Driver Verifier, 796
DSC (Desired State Configuration), 72, 87-89
DSRM (Directory Services Restore Mode), 119-120
dump files, 793-795
duplicating certificate templates, 625
Dynamic Access Control. *See* DAC (Dynamic Access Control)
Dynamic Host Configuration Protocol servers. *See* DHCP (Dynamic Host Configuration Protocol) servers
dynamic MAC addresses for VMs, 245
dynamic memory, 224-225, 233
dynamic optimization in VMM virtualization hosts, 108
Dynamic Processor Compatibility Mode, 262-263
dynamic quorum, 251-252
dynamic updates, 190
dynamic virtual hard disks, 236
dynamic virtual machine queue, 244

E

EAP-MS-CHAPv2, 688
editing. *See also* modifying
certificate templates, 625
file groups, 327-328
GPOs, 163
editions of Windows Server
list of, 57
switching when upgrading, 760
enabling. *See also* configuring
authentication methods, 533
deduplication, 318
directory browsing on websites, 536
HTTP/3, 532
MAC address spoofing, 234
MPIO, 577
NAT on VMs, 234
TLS 1.3, 531
VPN protocols, 689
encryption
Azure IaaS VMs, 416-417
SMB, 295-296
encryption-supported VMs, 470
end of support, 758
endpoints (JEA), 446-447
Enhanced Security Administrative Environment (ESAE) forests, 131, 492-495
Enhanced Session Mode, 228
enterprise CAs, 599-608
benefits of, 599
enterprise root CAs, 599-607
enterprise subordinate CAs, 608
limitations of, 599
standalone CAs versus, 608
enterprise root CAs, 599-607
enterprise subordinate CAs, 608
Entra. *See* Microsoft Entra
error messages for websites, customizing, 534-535
ESAE (Enhanced Security Administrative Environment) forests, 131, 492-495
Essentials edition (Windows Server 2019), 58
evaluation version of Windows Server, converting to licensed version, 759-760
event-driven tasks, 734-735
event logs
alerts for, 492
DNS servers, 199-200
Event Viewer, 731-735
event-driven tasks, 734-735
filters, 731-732
PowerShell cmdlets, 754
subscriptions, 733-734
views, 732-733
exclusion policies, 677

expanding S2D volumes, 285-287
Exploit Protection, 512-515
exporting
DSC configurations, 89
VMs, 258-259
attacks via, 465
with vTPMs, 259-260
WinGet package list, 84
expression-based audit policies, 454
extensions
in VMM, 102
for VMs, 387-388
Windows Admin Center, 9
external switches, 242
external trusts, 137

F

failover
with ASR, 417-419
DHCP, 211-212
in Hyper-V replication, 246-248
failover clustering, 573-590. *See also* guest clusters
campus clusters, 582
CAU, 577-578
Cloud Witness, 581-582
cluster networks, 576
cluster quorum modes, 574-575
cluster sets, 587-588
enabling MPIO, 577
in Hyper-V, 249-253
CSVs, 253
deploying with guest clusters, 253-254
failover settings, 253
Force Quorum Resiliency, 252
networking, 252
preferred owner, 253
quorum modes, 250-252
storage management, 249-250
multisite clusters, 579-580
PowerShell cmdlets for, 588-590
preference settings, 578-579
rolling upgrades, 584-586
shared storage, 576
stretch clusters, 580-581
virtual machine hosting, 583-584
workgroup clusters, 586-587
failover settings in failover clusters, 253
failsafe admin accounts, 494
fan-out administration (PowerShell), 19
fault domains, 579
features
adding, 71-72
in Windows images, adding, 77-78
Features on Demand (FOD), 68-69
federation, 643. *See also* AD FS (Active Directory Federation Services)
Federation Proxy. *See* web application proxy
Federation Server, 643
Fibre Channel virtual adapters, 240
file and folder auditing, 454
file classification in FSRM, 332-334
File Explorer, shared folder permissions, 319-320
file groups in FSRM, 327-329
file management tasks in FSRM, 334-335
File Replication System. *See* FRS (File Replication System)
file screen templates, 329-330
file screens in FSRM, 326-330
File Server Resource Manager. *See* FSRM (File Server Resource Manager)
file servers, 317. *See also* Azure File Sync
BranchCache, 343-346, 351-352
cleaning up, 336
deduplication, enabling, 318
DFS, 337-343
namespaces, 337-339
PowerShell cmdlets, 353
replication, 340-343
Windows Server 2008 mode, 339
FSRM, 324-337
access-denied assistance, 336-337
file classification, 332-334
file management tasks, 334-335
file screens, 326-330
PowerShell cmdlets, 350
quotas, 324-326
storage reports, 330-332
migration, 777-786
with Storage Migration Service, 777-782
with WSMT, 783-786
ransomware avoidance, 511
shared folder permissions, 318-323
with File Explorer, 319-320
PowerShell cmdlets, 349
with Server Manager, 321-323
with WAC, 320-321
SMB over QUIC, 346-349
file storage in VMM, 99
File Transfer Protocol (FTP), managing, 547-549
files, downloading, 70
filtered attribute set (RODCs), 125
filtering
DHCP, 209
GPOs, 167-168
IP addresses and domain names, 536-538
NLB clusters, 594-595
SID, 140
filters in Event Viewer, 731-732
finding WinGet packages, 83
firewall profiles, 456-457

firewalls. *See* WFAS (Windows Firewall with Advanced Security)
fixed-size virtual hard disks, 236
Flexible Single Master Operations roles. *See* FSMO (Flexible Single Master Operations) roles
FOD (Features on Demand), 68-69
folder auditing, 454
folder targets (DFS), 340-341
Force Quorum Resiliency, 252
forest migration, 765-768
forests, 127-131
ESAE, 131
intra-forest authentication, 129
multidomain, 128
forest trusts, 136-137, 424-425
formats for virtual hard disks, 235
converting between, 237-238
forwarders, DNS servers, 194
forwarding event logs, 733-734
Foundry Local, 804-808
command-line options, 804-805
configuring as a service, 806
installing, 804
Ollama comparison, 808
Open WebUI with, 806-808
requirements, 804
FRS (File Replication System), migration to DFS, 764-765
FSMO (Flexible Single Master Operations) roles, 132-135
domain naming master, 133
infrastructure master, 134
PDC emulator, 133
RID master, 134
schema master, 133
seizing, 135
FSRM (File Server Resource Manager), 324-337
access-denied assistance, 336-337
file classification, 332-334
file management tasks, 334-335
file screens, 326-330
PowerShell cmdlets, 350
quotas, 324-326
storage reports, 330-332
FTP (File Transfer Protocol), managing, 547-549
full-mesh topology, 342
functional levels
for domains, 129-130
for forests, 131
functions, cmdlets versus, 443

G

Generation 1 VMs, 243
Generation 2 VMs, 227-228, 243
Get-Credential (PowerShell), 18
global catalog servers, 122
global groups, 153
GlobalNames zones (DNS), 195-196
gMSAs (group Managed Service Accounts), 156-157, 438-440, 565-566
GPMC (Group Policy Management Console), 116, 161
GPOs (Group Policy Objects), 161-165
backing up, 164
copying, 165
creating, 162-163
delegating management tasks, 162
editing, 163
filtering, 167-168
importing, 164
LGPO, 500
linking, 163
migrating, 165
Policy Analyzer, 498-500
PowerShell cmdlets, 162
repairing, 165
restoring, 164
site-linked, 168
user and computer configuration settings, 169
GPU-P (GPU Partitioning), 230-231, 254
graphical tools in Server Core, 64
group accounts, 153-155
group Managed Service Accounts (gMSAs), 156-157, 438-440, 565-566
group management in Microsoft Entra ID, 377-379
Group Policy, 161-173
Administrative Templates, 172
caching, 169
configuring
for BranchCache, 344-346
for Remote Desktop Session Host, 715-719
DAC support configuration, 662
DirectAccess requirements, 699
forced updates, 170
GPO management, 161-165
backing up, 164
copying, 165
creating, 162-163
delegating tasks, 162
editing, 163
filtering, 167-168
importing, 164
linking, 163
migrating, 165
PowerShell cmdlets, 162
repairing, 165
restoring, 164
loopback processing, 169
order of processing, 166
PowerShell cmdlets, 185-186
preferences, 170-172
Resultant Set of Policy tool, 167
reverting settings, 173
Windows LAPS, 452
WSUS options in, 750-751

Group Policy Management Console (GPMC), 116, 161
Group Policy Objects. *See* GPOs (Group Policy Objects)
groups
in PAM, 449
in WSUS, 749
guarded fabric, 468-470
guest clusters in Hyper-V, 253-256
deploying with failover clusters, 253-254
GPU-P with, 254
shared virtual hard disks, 255-256
storage management, 255
VHD Sets, 256
guest integration services, 226-227

H

hard disks, virtual, 235-239
converting between formats, 237-238
differencing, 236-237
dynamic, 236
fixed-size, 236
formats for, 235
hot-adding, 237
hot-removing, 237
pass-through disks, 238-239
resizing, 238
shared, 255-256
Storage QoS, 240
hardening Active Directory, 473-495
AES for Kerberos policy, 490-491
auditing, logging, monitoring, 491-492
authentication policy silos, 483-484
backups, 492
blocking scheduled tasks, 489
constrained delegation, 485-486
disabling NTLM, 486-487
domain controller hardening, 474-476
ESAE forests, 492-495
highly privileged account security, 480-483
KRBTGT account password, 489-490
LDAP channel binding, 488
LDAP signing, 487-488
least-privilege, 476-477
LSASS as protected process, 488-489
msDS-MachineAccountQuota attribute, 485
password policies, 479-480
Protected Users security group, 482-483
RBAC, 477-479
hardening Windows Server, 433-471
advanced audit policies, 453-455
auditpol and, 455
expression-based policies, 454
file and folder auditing, 454
JEA, 441-447
benefits of, 441-442
endpoints, 446-447
limitations of, 442
PAM and, 450
role-capability files, 442-444
session-configuration files, 445
jump servers, 5
PAM, 447-450
benefits of, 447-448
components of, 448-449
JEA and, 450
roles, 449-450
users and groups, 449
PAWs, 4
service accounts
dMSAs, 440-441
gMSAs, 438-440
types of, 438
shielded VMs, 465-471
encryption-supported VMs versus, 470
guarded fabric for, 468-470
requirements, 466-467
shielding data file, 470-471
third-party guides, 433
user rights, 434-437
WFAS, 455-465
connection security rules, 460-465
firewall profiles, 456-457
inbound rules, 457-458
IPsec configuration, 458-460
outbound rules, 458
Windows LAPS, 451-453
group policies, 452
installing, 451-452
password management, 452
requirements, 451
hardware limitations of Windows Server 2025, 58
help commands (PowerShell), 16
HGS (Host Guardian Service), 468
high availability
with failover clustering, 573-590
campus clusters, 582
CAU, 577-578
Cloud Witness, 581-582
cluster networks, 576
cluster quorum modes, 574-575
cluster sets, 587-588
enabling MPIO, 577
multisite clusters, 579-580
PowerShell cmdlets for, 588-590
preference settings, 578-579
rolling upgrades, 584-586
shared storage, 576
stretch clusters, 580-581
virtual machine hosting, 583-584
workgroup clusters, 586-587

with NLB, 591-595
cluster management, 593-594
cluster operation modes, 592-593
filtering and affinity, 594-595
port rules, 594
PowerShell cmdlets for, 595
system requirements, 591-592
highly privileged accounts, 480-483
host groups in VMM, 106-108
Host Guardian Service (HGS), 468
host records (DNS), 196
host reserves in VMM virtualization hosts, 108
hot-adding
memory, 224
virtual hard disks, 237
hot-removing
memory, 225
virtual hard disks, 237
HRWs (Hybrid Runbook Workers), 389-390
HTTP/3, enabling, 532
hub-and-spoke topology, 342
HVC for Linux, 235
HVCI (Hypervisor-Protected Code Integrity), 505-506
Hybrid Runbook Workers (HRWs), 389-390
Hyper-V, 223-267
checkpoint management, 239-240
cloning domain controllers, 261-262
copying VMs, 259
DDA, 228-229
dynamic memory, 224-225
Dynamic Processor Compatibility Mode, 262-263
Enhanced Session Mode, 228
failover clusters, 249-253
CSVs, 253
deploying with guest clusters, 253-254
failover settings, 253
Force Quorum Resiliency, 252
networking, 252
preferred owner, 253
quorum modes, 250-252
storage management, 249-250
Generation 2 VMs, 227-228
GPU-P, 230-231
guest clusters, 253-256
deploying with failover clusters, 253-254
GPU-P with, 254
shared virtual hard disks, 255-256
storage management, 255
VHD Sets, 256
guest integration services, 226-227
HVC for Linux, 235
importing/exporting VMs, 258-260
live migration, 256-258
MAC addresses, 245-246
nested virtualization, 233-234
network adapters, 243
network isolation, 246
network performance optimization, 244-245
PowerShell cmdlets, 263-267
PowerShell Direct, 234-235
replication, 246-249
resource metering, 226
scheduling types, 232-233
shielded VMs, 263
smart paging, 225
storage migration, 258
storage optimization, 241-242
virtual Fibre Channel adapters, 240
virtual hard disks, 235-239
converting between formats, 237-238
differencing, 236-237
dynamic, 236
fixed-size, 236
formats for, 235
hot-adding, 237
hot-removing, 237
pass-through disks, 238-239
resizing, 238
shared, 255-256
Storage QoS, 240
virtual switches, 242-243
VM CPU groups, 232
VM drain on shutdown, 261
VM Network Health Detection, 260
VM resource groups, 231
Hyper-V isolation mode, 556
Hyper-V server edition (Windows Server 2019), 58
Hypervisor-Protected Code Integrity (HVCI), 505-506
hypothetical solutions
applying, 792-793
ranking, 791-792

I

IaaS (Infrastructure as a Service), benefits of, 397-398. *See also* Azure IaaS VMs
identify federation, 643. *See also* AD FS (Active Directory Federation Services)
identity management in Microsoft Entra ID, 375-381
administrative units, 380-381
groups, 377-379
users, 376-377
IGMP (Internet Group Management Protocol) multicast mode (NLB), 593
IIS (Internet Information Services), 523-550
application pools, 541-543
configuration backup and recovery, 546
FTP management, 547-549

PowerShell cmdlets, 549
remote management
configuring, 544
delegating permissions, 545-546
user accounts, 545
website administration PowerShell cmdlets, 550
website management, 523-541
adding websites to server, 524-527
authentication methods, 532-534
changing website settings, 528
configuring TLS certificates, 529-531
custom error messages, 534-535
default documents, 535-536
directory browsing, 536
enabling HTTP/3, 532
enabling TLS 1.3, 531
IP address and domain name filtering, 536-538
request filters, 539-541
self-signed TLS certificates, 527
URL authorization rules, 538-539
virtual directories, 527-528
web applications, 529
Windows Admin Center and, 8
IIS Manager, 523-524
IKEv2 Always On VPN protocol, 685-686
image dependencies, 554
image management in WDS, 92
images. *See* container images; Windows images
importing
GPOs (Group Policy Objects), 164
images into WDS (Windows Deployment Services), 92
VMs, 258-260
inbound port configuration, 399
inbound rules, 457-458
incremental backups, 741
Infrastructure as a Service (IaaS), benefits of, 397-398. *See also* Azure IaaS VMs
infrastructure configuration as code, 82-83
infrastructure master role, 134
in-place upgrade. *See* upgrade
insecure passwords, blocking, 374-375
Insider Preview Builds, 59
Insight for Active Directory (ADInsight), 53
install images, 92
installation account requirements (Microsoft Entra Connect), 360-361
installation options (Windows Server 2025)
Nano Server, 70
Server Core, 60, 70
Server with Desktop Experience, 60, 68-70
switching between, 68
installing. *See also* deploying
AD RMS, 670-676
certificates and licenses, 671-672
steps in, 670-671
templates, 672-675
user groups, 675-676
Azure Monitor, 737-739
Azure Monitor Agent, 412-413
Docker, 557
domain controllers from media, 120
enterprise root CAs, 600-607
Foundry Local, 804
Microsoft Entra Cloud Sync, 369-370
Microsoft Entra Connect, 358, 361-364
Ollama, 800-801
Open WebUI, 803
PowerShell, 15
RDS CALs, 724-725
RSAT, 10
Server Core App Compatibility Features on Demand (FOD), 69
symbols files, 793
Windows Admin Center, 7-8
Windows Debugger, 793
Windows LAPS, 451-452
Windows Server Backup, 175
WinGet packages, 84
WSL, 427-429
WSMT, 762
integration services, 226-227
interactive sessions for containers, 562-563
interfaces
Sconfig, 61
Server Core, 61-63
inter-forest authentication, 131
internal switches, 242
Internet access for Azure IaaS VMs, 406
Internet Group Management Protocol (IGMP) multicast mode (NLB), 593
Internet Information Services. *See* IIS (Internet Information Services)
Intl.cpl, 64
intra-forest authentication, 129
intuitive thinking in troubleshooting, 788
inventorying source servers with Storage Migration Service, 781
IP address blocks, 218
IP address filtering, 536-538
IP Address Management servers. *See* IPAM (IP Address Management) servers
IP address pools, 105
IP address tracking, 219

IP addressing for Azure IaaS VMs, 403-404
IPAM (IP Address Management) servers, 216-221
delegated administration, 217-219
deployment, 216
management with PowerShell, 219-221
server discovery, 217
IPsec, configuring in firewall, 458-460
iSCSI, 299-302, 310-311
Iscsicpl.exe, 64
isolation modes for containers, 555-556
isolation rules, 461-462
IT staff accounts, 3, 477

J

JEA (Just Enough Administration), 441-447
benefits of, 441-442
endpoints, 446-447
limitations of, 442
PAM and, 450
role-capability files, 442-444
session-configuration files, 445
JIT (Just In Time) Administration. *See* PAM (Privileged Access Management)
JIT (Just-In-Time) VM Access, 410
jump servers, 5

K

Kahneman, Daniel, 788
KCC (Knowledge Consistency Checker), 148
Kerberos, 257
AES for Kerberos policy, 490-491
time discrepancies, 492
Kerberos-constrained delegation, 486
Kerberos delegation, 159
Kerberos policies, 160
key management (SSH Server), 27-28
Key Signing Key (KSK), 199
Knowledge Consistency Checker (KCC), 148
KRBTGT account, changing password, 489-490
KSK (Key Signing Key), 199

L

L2 (Layer 2) Bridge networks, 568, 571
L2 (Layer 2) Tunnel networks, 568
L2TP/IPsec VPN protocol, 687
LAN routing, 693-694
large language models. *See* LLMs (large language models)
LDAP channel binding, 488
LDAP signing, 487-488
least privilege, principle of, 2-3, 476-477
legacy network adapters, 243
LGPO (Local Group Policy Object), 500
licensed version of Windows Server, converting evaluation version to, 759-760
licensing
AD RMS, 672
RDS, 723-725
activating license servers, 725
installing licenses, 724-725
switching retail and volume licenses, 760
Windows Server 2025 options, 58
linking GPOs, 163
Linux. *See also* WSL (Windows Subsystem for Linux)
HVC for Linux, 235
on Windows Server, 427
Linux Containers on Windows, 429
live migration
in Hyper-V, 256-258
VM drain on shutdown, 261
LLMs (large language models), 799-808
administration with, 25
Azure AI Foundry Local, 804-808
command-line options, 804-805
configuring as a service, 806
installing, 804
Ollama comparison, 808
Open WebUI with, 806-808
requirements, 804
Ollama, 799-804
command-line options, 801-802
Foundry Local comparison, 808
installing, 800-801
integrating into VS Code, 802
Open WebUI with, 802-804
load balancing
NLB. *See* NLB
of virtual machines, 583-584
Loaded Modules (lm) command, 795
local administration, remote administration versus, 110
local administrators for RODCs, 126
local AI, requirements for, 800
Local Group Policy Object (LGPO), 500
Local Security Authority (LSA), 488-489
Local Service account, 156, 438
local storage in VMM, 99
Local System account, 156, 438
locations
for backups, 740-741
for restoring backups, 743
of update files, 748
lockout policies, 480

Log Analytics workspaces, deploying, 412
logging. *See also* event logs; Event Viewer
Active Directory, 491-492
firewall logs, 456-457
logging into Azure IaaS VMs with Entra ID, 401
logical networks in VMM, 101-105
logical switches in VMM, 102
LogonSessions, 50
Long Term Servicing Channel (LTSC), 59
loopback processing in Group Policy, 169
LSA (Local Security Authority), 488-489
LSASS, as protected process, 488-489
LTSC (Long Term Servicing Channel), 59

M

MAC address pools, 104
MAC address spoofing, enabling on VMs, 234
MAC addresses for VMs, 245-246
MADCAP (Multicast Address Dynamic Client Allocation Protocol) scopes, 210
mail exchanger (MX) records (DNS), 197
managed identities, onboarding to Azure Arc–enabled servers, 383-384
managed pipeline mode for application pools, 541
MARS (Microsoft Azure Recovery Services) Agent, 743
Maximum Memory, 224
media, installing domain controllers from, 120
memory
dynamic, 224-225, 233
smart paging, 225
troubleshooting, 796-797
Memory Buffer, 224
Memory Integrity, 505-506
memory management (RAMMap), 54-55
Memory Weight, 224
metadata in FSRM, 332-334
Microsoft 365 groups, 377
Microsoft Azure Recovery Services (MARS) Agent, 743
Microsoft Defender SmartScreen, 518
Microsoft Entra Cloud Sync, 368-372
installing, 369-370
Microsoft Entra Connect comparison, 370-371
troubleshooting, 372
Microsoft Entra Connect, 355-368
installing, 358, 361-364
Microsoft Entra Cloud Sync comparison, 370-371
monitoring synchronization health, 364-365
multiforest AD DS synchronization configuration, 367-368
object filter configuration, 366
optional features, 356
password synchronization configuration, 367
requirements, 358-361
for installation account, 360-361
for server, 358-360
for SQL Server, 360
user sign-in options, 356-357
Microsoft Entra Connect Health, 364-365
Microsoft Entra Domain Services, 419-426
creating forest trust, 424-425
deploying, 420-422
domain-joining, 422
integration with AD DS, 423-424
managing AD DS instance, 425-426
Microsoft Entra ID, 355-381
Azure IaaS VM login with, 401
identity management, 375-381
administrative units, 380-381
groups, 377-379
users, 376-377
managed identities, onboarding to Azure Arc–enabled servers, 383-384
Microsoft Entra Cloud Sync, 368-372
Microsoft Entra Connect, 355-368
Microsoft Entra Password Protection, 374-375
SSPR, 372-373
Microsoft Entra ID Password Protection, 374-375
components of, 519
deploying, 520-521
requirements, 520
Microsoft SQL Server container image, 561
Microsoft Update Catalog, 75
migration. *See also* upgrades
Active Directory
forest migration, 765-768
FRS to DFS, 764-765
AD CS, 768-772
preparing for, 770-771
requirements, 768-769
steps in, 771-772
verifying, 772
CAs, 603
defined, 757
DFS to Azure File Sync, 395-396
DHCP servers, 773-777
preparing for, 774-776
steps in, 776
verifying, 777
DNS servers, 772-773

file servers, 777-786
with Storage Migration Service, 777-782
with WSMT, 783-786
GPOs, 165
permissions, 784
WSMT, 760-762
migration tables, 165
Minimum Memory, 224
mirrored networking for WSL, 431
mirroring, 275
modifying. *See also* editing
containers, 563
website settings, 528
Windows images, 74-75
modules (PowerShell), 17
monitoring. *See also* network monitoring; performance monitoring
Active Directory, 491-492
Azure File Sync, 394-395
replication, 150
synchronization, 364-365
mounting
snapshots (Active Directory), 175
Windows images, 76
moving
domain controllers, 146
VMs, attacks via, 465
MPIO (multipath I/O), enabling, 577
msDS-MachineAccountQuota attribute (Active Directory), 485
MSInfo32.exe, 64
MSLab project, 82
Multicast Address Dynamic Client Allocation Protocol (MADCAP) scopes, 210
multicast mode (NLB), 593
multicast options (WDS), 95-96
multicast scopes (DHCP), 210
multidomain forests, 128
multifactor authentication, 655-656
multiforest AD DS synchronization, configuring in Microsoft Entra Connect, 367-368
multimaster replication, 148
multipath I/O (MPIO), enabling, 577
multisite clusters, 579-580
MX (mail exchanger) records (DNS), 197

N

name protection (DHCP servers), 210
namespaces (DFS), 337-339
name suffix routing, 141
naming containers, 562
Nano Server, 70, 249
Nano Server container image, 554, 560
NAT (Network Address Translation), 694-695
for containers, 567-569
enabling on VMs, 234
nested resiliency (S2D), 282
nested virtualization, 233-234
nesting groups in Microsoft Entra ID, 379
.NET Framework 3.5, 78
netdom.exe, 139-140
netmask ordering (DNS), 201-202
network adapters for VMs, 243
Network Address Translation (NAT), 694-695
for containers, 567-569
enabling on VMs, 234
Network File System (NFS), 303-305, 311
network isolation in Hyper-V, 246
Network Load Balancing. *See* NLB (Network Load Balancing)
Network Location Server (NLS), 700
network monitoring, 735-737
with Packet Monitor, 736-737
with Resource Monitor, 735-736
network performance optimization for VMs, 244-245
network policies, 690-693
networking
Azure IaaS VMs, 401-406
default outbound access, 406
IP addressing, 403-404
NSGs, 405-406
virtual networks, 401-403
VPN gateways, 406
for ASR, 419
for containers, 562, 567-571
L2 Bridge, 571
NAT, 568-569
overlay, 570
transparent, 570
types of modes, 567-568
in failover clustering, 576
for Hyper-V failover clusters, 252
in nested virtualization, 234
in VMM, 101-105
in WSL, 430-431
Network Security Groups (NSGs), 405-406
Network Service account, 156, 438
NFS (Network File System), 303-305, 311
NIC teaming for VMs, 245
NLB (Network Load Balancing), 591-595
cluster management, 593-594
cluster operation modes, 592-593
filtering and affinity, 594-595
port rules, 594
PowerShell cmdlets for, 595
system requirements, 591-592
NLS (Network Location Server), 700
Node and Disk Majority cluster quorum mode, 250

Node and File Share Majority cluster quorum mode, 251
Node Majority cluster quorum mode, 250
node weight (for failover clusters), 251
nodes in failover clustering, 574-575
No Majority: Disk Only cluster quorum mode, 251
Notepad.exe, 64
NSGs (Network Security Groups), 405-406
NTLM, disabling, 486-487
NTLM blocking (SMB), 297

O

object filters, configuring in Microsoft Entra Connect, 366
offline root CAs, 611
Ollama, 799-804
command-line options, 801-802
Foundry Local comparison, 808
installing, 800-801
integrating into VS Code, 802
Open WebUI with, 802-804
onboarding to Azure Arc–enabled servers, 383-387
connecting to Azure Arc, 384
Microsoft Entra ID–managed identities, 383-384
with Power Shell, 385-386
requirements, 383
with service principal-based deployment, 386-387
SQL Server, 385
from Windows Server, 385
one-to-many remoting (PowerShell), 19
on-premises VMs, Azure IaaS VMs versus, 397-398
Open WebUI
with Foundry Local, 806-808
installing, 803
with Ollama, 802-804
operating system level for domain controllers, 130
optimization. *See* performance optimization
order of processing for Group Policy, 166
OSConfig, 501-503
OUs (organizational units), 131-132
outbound rules, 458
overlay networks, 568-570

P

package-management utilities, 83-87
Apt-get, 83
Chocolatey, 85-87
in PowerShell, 85
PowerShell Gallery, 85
security and, 86
WinGet, 83-84
Packet Monitor, 736-737
PAM (Privileged Access Management), 447-450
benefits of, 447-448
components of, 448-449
JEA and, 450
roles, 449-450
users and groups, 449
PAP (Password Authentication Protocol), 688
parity, 275
partitioning with GPU-P, 230-231
partitions (AD DS), types of, 147
pass-through authentication in Microsoft Entra Connect, 357
pass-through disks, 238-239, 257
Password Authentication Protocol (PAP), 688
password policies, hardening Active Directory, 479-480
password synchronization
configuring in Microsoft Entra Connect, 367
with Entra Domain Services, 423-424
in Microsoft Entra Connect, 357
passwords. *See also* hardening Windows Server; security
blocking insecure, 374-375
DSRM, 119-120
Entra ID Password Protection, 519-521
components of, 519
deploying, 520-521
requirements, 520
KRBTGT account, changing, 489-490
managing in Windows LAPS, 452
resetting, 372-373
on RODCs, 124-125
PAWs (privileged-access workstations), 3-4, 477
PDC emulator role, 133
PDK file, 470-471
PEAP (Protected EAP), 688
performance monitoring
with alerts, 731
Azure IaaS VMs, 412-414
with Azure Monitor, 737-739
with data collector sets, 729-731
with Event Viewer, 731-735
event-driven tasks, 734-735
filters, 731-732
PowerShell cmdlets, 754
subscriptions, 733-734
views, 732-733
performance optimization
Active Directory database, 174
for VM networks, 244-245
performance problems, analyzing, 795

permissions. *See also* AD RMS (Active Directory Rights Management Services)
AD RMS, 319
for CAs, 628-630
complications with, 319
delegating, 545-546
DNS servers, 204
Dynamic Access Control, 319, 354
IPAM servers, 217-219
for migration, 784
shared folders, 318-323
with File Explorer, 319-320
PowerShell cmdlets, 349
with Server Manager, 321-323
with WAC, 320-321
persistent memory support, 270
personal session desktops for Remote Desktop Session Host, 714
personal virtual desktops for Remote Desktop Virtualization Host, 722
physical disks, adding/removing from storage pools, 272-274
physically deployed servers, virtualized versus, 73
physical security, virtual security versus, 466
pipeline mode for application pools, 541
placement rules in VMM virtualization hosts, 107
planned failover in Hyper-V replication, 246-248
pointer (PTR) records (DNS), 197
policies
DNS, 203
Group Policy. *See* Group Policy
Policy Analyzer, 498-500
policy processing order, 166
pooled virtual desktops for Remote Desktop Virtualization Host, 722
port forwarding for WSL, 430-431
port mappings, 569
port profiles in VMM, 103
port rules (NLB), 594
PowerShell, 15-23
Active Directory cmdlets, 182-185
ADAC and, 111
AD CS cmdlets, 639-641
AD DS deployment cmdlets, 186-187
AD FS cmdlets, 656, 659
AD RMS cmdlets, 678-679
Azure IaaS VM administration, 409
BranchCache cmdlets, 351-352
cmdlets versus functions, 443
DFS cmdlets, 353
DHCP management, 214-216
DNS management, 204-206
documentation, 16
DSC v3 and, 87-89
Dynamic Access Control cmdlets, 354
Event Viewer cmdlets, 754
failover clustering cmdlets, 588-590
FSRM cmdlets, 350
GPO management cmdlets, 162
Group Policy cmdlets, 185-186
help commands, 16
Hyper-V cmdlets, 263-267
IIS management cmdlets, 549
installing, 15
IPAM management, 219-221
JEA. *See* JEA
modules, 17
NLB cmdlets, 595
onboarding Azure Arc with, 385-386
package-management utilities in, 85
PowerShell Direct, 23
PowerShell Gallery, 17
PowerShell ISE, 20-22
RDS cmdlets, 725-727
remote access cmdlets, 704-706
remote sessions, 18-19
scripts for VM deployment, 82
shared folder cmdlets, 349
storage-related cmdlets, 310-316
updating, 63-64
viewing source code in Windows Admin Center, 10
web application proxy cmdlets, 659
website management cmdlets, 550
Windows Defender cmdlets, 517
Windows Server Backup cmdlets, 754
WSUS cmdlets, 755
PowerShell Desired State Configuration (PSDSC), 87
PowerShell Direct, 23, 234-235
PowerShell Gallery, 17, 85
PowerShell ISE (Integrated Scripting Environment), 20-22
PPTP VPN protocol, 687-688
preferences
for failover clustering, 578-579
in Group Policy, 170-172
preferred owner in failover clusters, 253
preparing
for AD CS migration, 770-771
for DHCP migration, 774-776
for WSMT migration, 784-785
prerequisites. *See* requirements
primary zones (DNS), 191-192
Primordial pool, 270
principle of least privilege, 2-3, 476-477
private keys
archiving and recovery, 633-638
cryptographic options for, 603-604

private switches, 243
private VLANs (PVLANs), 105
Privileged Access Management. ***See*** **PAM (Privileged Access Management)**
privileged-access workstations (PAWs), 3-4, 477
privileges
delegating, 477-479
highly privileged accounts, 480-483
problem-solving. ***See*** **troubleshooting**
ProcDump, 42
Process Explorer, 39-41
process isolation mode, 555
Process Monitor, 41-42
processing order for Group Policy, 166
production checkpoints, 239
profiles (firewall), 456-457
Protected EAP (PEAP), 688
protected process, LSASS as, 488-489
Protected Users security group, 482-483
provisioning data file, 470-471
PSDSC (PowerShell Desired State Configuration), 87
PsPing, 54
PS Tools Suite, 42-43
PTR (pointer) records (DNS), 197
public inbound port configuration, 399
publishing CRLs, 615-617
PVLANs (private VLANs), 105
PXE response settings (in WDS), 93

Q–R

quorum modes for Hyper-V failover clusters, 250-252
quotas in FSRM, 324-326
RAMMap, 54-55
ranking hypothetical solutions, 791-792
ransomware, 510-512
RAP (Resource Authorization Policy), 683
RBAC (Role-Based Access Control), 407, 477-479
RD (Remote Desktop) Gateway, 681-685
client configuration, 683-685
connection and resource policies, 682-683
server settings configuration, 683
RDS (Remote Desktop Services), 707-727
deploying, 707-709
deployment properties, 710-711
licensing, 723-725
activating license servers, 725
installing licenses, 724-725
PowerShell cmdlets, 725-727
Remote Desktop Connection Broker, 709-710
Remote Desktop Session Host, 711-719
benefits of, 711
Group Policy configuration, 715-719
personal session desktops, 714
RemoteApp and, 714
session collection settings, 712-714
Remote Desktop Virtualization Host, 719-723
DDA and RemoteFX, 723
personal virtual desktops, 722
pooled virtual desktops, 722
requirements, 719-720
virtual desktop collections, 721-722
VM preparation, 720
Remote Desktop Web Access, 723
RDS CAL (Remote Desktop Services Client Access License), 723-725
Read Only Domain Controllers (RODCs)
replication, 149-150, 190
security, 123-126
realm trusts, 138-139
recovering
CAs, 631-633
private keys, 633-638
recovery agents, configuring, 634-637
recursion (DNS), 201
recycling settings (application pools), configuring, 542-543
redeployment as troubleshooting solution, 788-789
ReFS (Resilient File System), 308-309
Regedit.exe, 64
Regedt32.exe, 64
registering servers with storage sync services, 393
relay agents (DHCP), 213-214
relying party servers, 645
relying party trust, 645-646
relying party trust claim rules, 649
remote access technologies, 681-706
DHCP Relay Agent, 695-696
DirectAccess, 696-703
configuring, 700-703
NLS and, 700
server requirements, 698-700
topologies, 697-698
NAT, 694-695
PowerShell cmdlets for, 704-706
RD Gateway, 681-685
client configuration, 683-685
connection and resource policies, 682-683
server settings configuration, 683

VPNs, 685-693
authentication protocols, 688
certificates for, 685
disabling, 689
enabling, 689
granting access to, 690-693
IKEv2 Always On protocol, 685-686
L2TP/IPsec protocol, 687
PPTP protocol, 687-688
server deployment, 688-689
SSTP protocol, 687
remote administration
jump servers, 5
local administration versus, 110
PAWs, 3-4
PowerShell, 18-19
Remote Desktop, 2, 23-25
RSAT, 10-15
consoles, list of, 10-13
installing, 10
Server Manager console, 14-15
SSH Server, 26-29
key management, 27-28
in Windows Server 2022 and earlier, 28-29
in Windows Server 2025, 26-27
of websites
configuring, 544
delegating permissions, 545-546
Windows Admin Center, 5-10
certificate trust and, 8
default tools, 6
extensions, 9
installing, 7-8
viewing PowerShell source code, 10
RemoteApp, 714
Remote Desktop, 2, 23-25
Remote Desktop Connection Broker, 709-710
Remote Desktop (RD) Gateway. *See* RD (Remote Desktop) Gateway
Remote Desktop Services. *See* RDS (Remote Desktop Services)
Remote Desktop Services Client Access License (RDS CAL), 723-725
Remote Desktop Session Host, 707, 711-719
benefits of, 711
Group Policy configuration, 715-719
personal session desktops, 714
RemoteApp and, 714
session collection settings, 712-714
Remote Desktop Virtualization Host, 707, 719-723
DDA and RemoteFX, 723
personal virtual desktops, 722
pooled virtual desktops, 722
requirements, 719-720
virtual desktop collections, 721-722
VM preparation, 720
Remote Desktop Web Access, 723
RemoteFX, 229, 723
Remote PowerShell, Azure IaaS VM administration, 409
Remote Server Administration Tools. *See* RSAT (Remote Server Administration Tools)
remote storage in VMM, 99
remote tabs in PowerShell ISE, 21
removing. *See also* deleting
memory, 225
physical disks from storage pools, 272-274
virtual hard disks, 237
WinGet packages, 84
renewing certificates, 599
repadmin, 150
repairing GPOs, 165
replica brokers (Hyper-V), 249
replica mode (WSUS), 748
replication
Active Directory–integrated zones (DNS), 190
AD DS, 147-150
conflict resolution, 149
KCC, 148
monitoring, 150
multimaster, 148
repadmin, 150
RODCs, 149-150
store-and-forward, 148
with ASR, 417-419
DFS, 340-343
FRS to DFS migration, 764-765
in Hyper-V, 246-249
with Storage Replica, 288-293, 315
replication groups, 342
request filters, 539-541
requirements
AD CS migration, 768-769
DAC, 662
DirectAccess servers, 698-700
Entra ID Password Protection, 520
Foundry Local, 804
local AI, 800
Microsoft Entra Connect, 358-361
for installation account, 360-361
for server, 358-360
for SQL Server, 360
Microsoft Entra Password Protection, 374
NLB, 591-592
onboarding to Azure Arc–enabled servers, 383
Remote Desktop Virtualization Host, 719-720
SMB over QUIC, 346

shielded VMs, 466-467
SSPR, 372
VMM virtualization hosts, 107
WDS, 90-91
Windows LAPS, 451
reservations (DHCP servers), 208
resetting passwords, 372-373
resiliency (S2D), 282-283
Resilient File System (ReFS), 308-309
resizing
Azure IaaS VMs, 414-415
virtual hard disks, 238
Resource Authorization Policy (RAP), 683
resource-based constrained delegation, 486
resource groups, 231
resource metering, 226
Resource Monitor, 735-736
resource properties, configuring, 664-665
resource records (DNS), 196-198
response rate limiting (DNS), 202
restoring
from Azure Backup, 745-746
from backups, 742-743
deleted Active Directory items, 176-182
Active Directory Recycle Bin, 178-179
authoritative restore, 179-181
snapshots, 181-182
GPOs, 164
IIS configuration, 546
restricted management administrative units, 381
REST service, configuring Foundry Local as, 806
Resultant Set of Policy tool, 167
retail license, switching to volume license, 760
retrieving base OS container images, 560
reverse lookup zones (DNS), 192-193
reverting Group Policy settings, 173
revoking certificates, 598, 613-615
RID master role, 134
Rights Policy Templates, 672-675
RODCs (Read Only Domain Controllers)
replication, 149-150, 190
security, 123-126
Role-Based Access Control (RBAC), 407, 477-479
role-capability files, 442-444
role-specific backups, 742
roles
in AD CS, 617
adding, 71-72
in PAM, 449-450
in Server Core, 64, 67
rolling upgrades of failover clusters, 584-586
Root CAs, 597
enterprise root CAs, 599-607
offline root CAs, 611
standalone root CAs, 611
routing, LAN, 693-694
RSAT (Remote Server Administration Tools), 10-15
consoles, list of, 10-13
installing, 10
Server Manager console, 14-15

S

S2D (Storage Spaces Direct), 280-288, 582
adding cluster nodes, 287
deployment, 282-284
maintenance on cluster nodes, 288
managing volumes, 284-287
nested resiliency, 282
properties, 281
resiliency, 282-283
resources for information, 282
SAC (Annual Channel container images), 59
Samba, 780
sandboxes, 554
Scale-Out File Server (SoFS), 302-303
scheduled tasks, blocking, 489
schedulers (Hyper-V), 232-233
schedules
for replication, 343
for tasks, 31-33
schema master role, 133
schema partitions, 147
Sconfig interface, 61
scopes (DHCP servers), 207
multicast scopes, 210
options, 208
split scopes, 210
superscopes, 209
scripts. *See also* PowerShell ISE
shell completion, 89
for VM deployment, 82
SCT (Security Compliance Toolkit), 498-500
search functionality in ADAC, 111
secondary zones (DNS), 192
Secure Shell. *See* SSH Server
security, 497-521. *See also* hardening Windows Server
ASR rules, 515-517
assume breach philosophy, 497
Attack Surface Analyzer, 500-501
of backups, 740
CFG, 503-504
Controlled Folder Access, 510-512
Credential Guard, 508-510
domain controllers
as attack targets, 109
operating system level, 130

Entra ID Password Protection, 519-521
components of, 519
deploying, 520-521
requirements, 520
Exploit Protection, 512-515
HVCI, 505-506
LGPO, 500
Microsoft Defender SmartScreen, 518
OSConfig, 501-503
package-management utilities and, 86
Policy Analyzer, 498-500
principle of least privilege, 2-3, 476-477
RODCs, 123-126
SCT, 498-500
shielded VMs, 73
SSH Server, 26-29
key management, 27-28
in Windows Server 2022 and earlier, 28-29
in Windows Server 2025, 26-27
VBS, 504-505
WDAC, 506-508
Windows Defender, 517-518
Security Compliance Toolkit (SCT), 498-500
security controls, compatibility and, 433
security roles in WSUS, 749
Security Technical Implementation Guide (STIG), 434
security updates, end of support, 758
seizing FSMO roles, 135
selecting Storage Layouts, 274-275
selective authentication, configuring, 137
Self-Service Password Reset (SSPR), 372-373
self-signed TLS certificates, 527
server authorization (DHCP), 212
Server Core, 60, 70, 761
App Compatibility Features on Demand (FOD), 68-69
domain controller configuration, 121
graphical tools, 64
interface, 61-63
PowerShell updates, 63-64
roles in, 64, 67
security of, 109
when to deploy, 69
server discovery (IPAM), 217
server endpoints, creating, 393
Server for NFS, 303-305
Server Manager, shared folder permissions, 321-323
Server Manager console (RSAT), 14-15
Server Message Block. *See* SMB (Server Message Block) protocol
server settings (RD Gateway), 683
Server with Desktop Experience, 60, 68-70
server-to-server configuration (Storage Replica), 289
server-to-server rules, 462-463
servers
registering with storage sync services, 393
Microsoft Entra Connection requirements, 358-360
service accounts, 156-160
for containers, 565-566
dMSAs, 158, 440-441
gMSAs, 156-157, 438-440
Kerberos delegation, 159
Kerberos policies, 160
Local Service, 156
Local System, 156
Network Service, 156
SPNs, 160
types of, 438
virtual, 158
service principal names (SPNs), 160, 486
service principal-based deployment, onboarding Azure Arc with, 386-387
services console, 29-31
servicing
branches of Windows Server 2025, 59-60
Windows images, 75-78
session collection settings for Remote Desktop Session Host, 712-714
session-configuration files, 445
shadow principals (PAM), 448
shared folder permissions, 318-323
with File Explorer, 319-320
PowerShell cmdlets, 349
with Server Manager, 321-323
with WAC, 320-321
shared nothing live migration, 256
shared storage
in failover clustering, 576
live migration, 257
of virtual machines, 583
shared virtual hard disks, 255-256
shell completion scripts, 89
ShellRunAs, 49-50
shielded template disks, 471
shielded VMs, 73, 263, 465-471
encryption-supported VMs versus, 470
guarded fabric for, 468-470
requirements, 466-467
shielding data file, 470-471
shielding data file, 470-471
shortcut trusts, 137-138
SID filtering, 140
SigCheck, 45

sign-in, Microsoft Entra Connect, 356-357
signing (LDAP), 487-488
signing (SMB), 296
silo claims, 484
Simple Mail Transfer Protocol (SMTP) gateways, 193
single CA deployments, 600
Single Root I/O Virtualization (SR-IOV), 244
site link bridges (AD DS), creating, 146
site links (AD DS), creating, 145-146
site management (AD DS), 141-146
moving domain controllers, 146
site creation, 143-144
site link bridge creation, 146
site link creation, 145-146
subnet creation, 144
site-linked GPOs, 168
sites (AD DS)
configuring, 141-142
creating, 143-144
defined, 115
purpose of, 141-143
slow-link processing, 169
smart paging, 225
SMB (Server Message Block) protocol, 293-299
compression, 294-295
encryption, 295-296
NTLM blocking, 297
signing, 296
SMB Direct, 299
SMB over QUIC, 297-299
versions, 293-294
SMB Direct, 299
SMB over QUIC, 297-299, 346-349
SMTP (Simple Mail Transfer Protocol) gateways, 193
SMT (Symmetric Multi-Threading), 232
snapshots (Active Directory), 174-175
creating, 174
dismounting, 175
mounting, 175
restoring deleted items, 181-182
snippets in PowerShell ISE, 22
socket pool (DNS), 200
SoFS (Scale-Out File Server), 302-303
solutions
applying, 792-793
ranking, 791-792
source code, viewing in Windows Admin Center, 10
source servers, inventorying with Storage Migration Service, 781
split-brain scenarios, 580
split DNS, 119
split scopes (DHCP), 210
SPNs (service principal names), 160, 486
spoofing, 200
SQL Server
Microsoft Entra Connect requirements, 360
onboarding to Azure Arc, 385
SR-IOV (Single Root I/O Virtualization), 244
SSH Server, 26-29
key management, 27-28
in Windows Server 2022 and earlier, 28-29
in Windows Server 2025, 26-27
SSPR (Self-Service Password Reset), 372-373
SSTP VPN protocol, 687
Stack Trace (k) command, 795
staged permissions, 668-669
standalone CAs, 608-611
benefits of, 609
configuring client trust, 609-610
enterprise CAs versus, 608
offline root CAs, 611
standalone root CAs, 611
standalone subordinate CAs, 611
standalone namespaces, 338
standalone root CAs, 611
standalone subordinate CAs, 611
standard checkpoints, 239
Standard edition (Windows Server 2025), 57
starting containers, 562-563
Startup Memory, 224-225
static MAC addresses for VMs, 245
STIG (Security Technical Implementation Guide), 434
storage
deduplication, 305-307, 310
devices
iSCSI, 299-302, 310-311
Server for NFS, 303-305
SoFS, 302-303
migration in Hyper-V, 258
optimization for VMs, 241-242
PowerShell cmdlets, 310-316
quotas in FSRM, 324-326
in VMM, 99-100
storage classifications, 101
Storage Layouts, choosing, 274-275
storage management
for guest clusters, 255
for Hyper-V failover clusters, 249-250
Storage Migration Service, 777-782
advantages of, 777
copy process, 781-782
cutover process, 782
deploying, 780
inventorying source servers, 781
limitations of, 778-779
Storage Migration Service Orchestrator, 780

storage pools
adding physical disks to, 272-273
choosing Storage Layouts, 274-275
creating new, 270-272
creating virtual disks, 279-280
definition of, 269-270
removing physical disks from, 272-274
thin provisioning virtual disks, 277-278
Trim process, 278
Storage QoS (Quality of Service), 240, 307-308
Storage Replica, 315, 288-293, 580
storage reports in FSRM, 330-332
storage spaces
creating from existing storage pools, 279-280
definition of, 269-270
resiliency, 274-275
resources for information, 274
thin provisioning, 277-278
tiering, 275-277
Trim process, 278
Storage Spaces Direct. *See* S2D (Storage Spaces Direct)
storage sync services
deploying, 391
registering servers with, 393
storage tiering, 241
storage-class memory, 270
store-and-forward replication, 148
stretch cluster configuration (Storage Replica), 289
stretch clusters, 580-581
stub zones (DNS), 195
subnets (AD DS), creating, 144
subordinate CAs, 597
enterprise, 608
standalone, 611
subscriptions in Event Viewer, 733-734
superscopes (DHCP), 209
Super Users group in AD RMS, 676
support, end of, 758
switches, virtual, 242-243
switching
retail and volume licenses, 760
Windows Server editions, 760
symbols files, installing, 793
Symmetric Multi-Threading (SMT), 232
sync groups, creating, 392
synchronization. *See also* Microsoft Entra Cloud Sync; Microsoft Entra Connect
installing domain controllers, 120
monitoring, 364-365
multiforest AD DS, configuring, 367-368
passwords, 367, 372-373
Synchronization Rules Editor, 366
Synchronization Service Manager, 365
synthetic network adapters, 243
Sysinternals tools, 39-55
AccessChk, 45
AccessEnum, 48-49
AD Explorer, 50-53
ADInsight, 53
LogonSessions, 50
ProcDump, 42
Process Explorer, 39-41
Process Monitor, 41-42
PsPing, 54
PS Tools Suite, 42-43
RAMMap, 54-55
ShellRunAs, 49-50
SigCheck, 45
Sysmon, 46-48
VMMap, 44
Sysmon (System Monitor), 46-48
system requirements
AD CS migration, 768-769
DAC, 662
DirectAccess servers, 698-700
Entra ID Password Protection, 520
Foundry Local, 804
local AI, 800
Microsoft Entra Connect, 358-361
for installation account, 360-361
for server, 358-360
for SQL Server, 360
Microsoft Entra Password Protection, 374
NLB, 591-592
onboarding to Azure Arc–enabled servers, 383
Remote Desktop Virtualization Host, 719-720
SMB over QUIC, 346
shielded VMs, 466-467
SSPR, 372
VMM virtualization hosts, 107
WDS, 90-91
Windows LAPS, 451
SYSVOL replication, 764-765

T

Task Manager, 64, 795
tasks, attaching to events, 734-735
Task Scheduler, 31-33
template virtual hard disks, 471
templates
in AD RMS, 672-675
applying automatically, 677-678
certificate templates, 618-625
deleting, 618
duplicating, 625
editing, 625
properties, 619-625
file screens, 329-330
Group Policy Administrative Templates, 172
for VMs, 98-99

tenant keys, 471
Terminal Services. *See* Remote Desktop Session Host
***Thinking, Fast and Slow* (Kahneman), 788**
thin provisioning, 277-278
tiering storage spaces, 275-277
TimeDate.cpl, 64
time discrepancies in Kerberos, 492
TLS 1.3, enabling, 531
TLS certificates
configuring, 529-531
for DirectAccess servers, 699
for RD Gateway servers, 683
self-signed, 527
token-decrypting certificates, 648
token-signing certificates, 647
tombstone lifetime, 176-177
topologies for replication, 342
TPDs (Trusted Publishing Domains), 677
TPM-trusted attestation, 468-470
tracking IP addresses, 219
transitive trusts, 136
transmissions (WDS), configuring, 96-97
transparent networks, 568-570
Trim process, 278
troubleshooting, 787-797
AI chatbot solutions for, 787-788
applying hypothetical solutions, 792-793
with command-line tools, 34-39
dependencies, 790-791
with Driver Verifier, 796
intuitive thinking versus deductive reasoning, 788
Microsoft Entra Cloud Sync, 372
ranking hypothetical solutions, 791-792
redeployment as solution, 788-789
symptoms and diagnosis of problems, 789-790
with Sysinternals tools, 39-55
AccessChk, 45
AccessEnum, 48-49
AD Explorer, 50-53
ADInsight, 53
LogonSessions, 50
ProcDump, 42
Process Explorer, 39-41
Process Monitor, 41-42
PsPing, 54
PS Tools Suite, 42-43
RAMMap, 54-55
ShellRunAs, 49-50
SigCheck, 45
Sysmon, 46-48
VMMap, 44
with Windows Debugger, 793-795
with Windows Memory Diagnostic, 796-797
trust anchors, 199
trust relationships, 135-141
certificates, 598
external trusts, 137
forest trusts, 136-137
inter-forest authentication, 131
intra-forest authentication, 129
name suffix routing, 141
netdom.exe, 139-140
realm trusts, 138-139
shortcut trusts, 137-138
SID filtering, 140
terminology, 135
transitivity, 136
trust direction, 136
types of, 115
trusted attestation, 468-470
trusted domains, 135
Trusted Publishing Domains (TPDs), 677
trusting domains, 135
TUDs (Trusted User Domains), 677
tunnel rules, 464-465

U

unicast mode (NLB), 592
universal groups, 153
unknown records (DNS), 197
unplanned failover in Hyper-V replication, 246-248
update sequence numbers (USNs), 149
updates
adding to Windows images, 76-77
Azure Update Manager, 753-754
to base OS images, 567
to containers, 566-567
end of support, 758
forced in Group Policy, 170
to PowerShell, 63-64
to WSL, 429
WSUS, 747-753
automatic approval rules, 751-752
autonomous and replica modes, 748
deploying updates, 751
Group Policy options, 750-751
groups, 749
locations of update files, 748
PowerShell cmdlets, 755
product, classification, language settings, 748
security roles, 749
upgrades. *See also* migration
Active Directory domain controllers, 763-764
AD CS, 769
defined, 757-758
evaluation version, converting to licensed version, 759-760
to failover clusters, 584-586

limitations on, 758
switching editions, 760
to WinGet packages, 84
uplink port profiles in VMM, 102
URL authorization rules, 538-539
user accounts, 151-152, 545
user claims, 663
user configuration settings (GPOs), 169
user groups in AD RMS, 675-676
user management in Microsoft Entra ID, 376-377
user rights, assignment policy, 434-437
user sign-in, Microsoft Entra Connect, 356-357
users in PAM, 449
USNs (update sequence numbers), 149

V

VBS (virtualization-based security), 504-505
VDI (Virtual Desktop Infrastructure), 707, 719
verifying
AD CS migration, 772
DHCP migration, 777
VHD Sets, 256
viewing source code in Windows Admin Center, 10
views in Event Viewer, 732-733
virtual accounts, 439-441
virtual desktop collections for Remote Desktop Virtualization Host, 721-722
Virtual Desktop Infrastructure (VDI), 707, 719
virtual directories, 527-528
virtual domain controllers, cloning, 126-127
virtual Fibre Channel adapters, 240
virtual hard disks, 235-239. *See also* storage spaces
converting between formats, 237-238
creating, 279-280
differencing, 236-237
dynamic, 236
fixed-size, 236
formats for, 235
hot-adding, 237
hot-removing, 237
iSCSI, 301
mirroring, 275
parity, 275
pass-through disks, 238-239
resizing, 238
shared, 255-256
Storage QoS, 240
virtualization. *See also* Hyper-V; Remote Desktop Virtualization Host; VMM (Virtual Machine Manager)
infrastructure configuration as code, 82-83
PowerShell Direct, 23
virtualization fabric attacks, 465
virtualization hosts, deploying, 73-74
virtualization-based security (VBS), 504-505
virtualized domain controllers, 121
virtual LANs (VLANs), 105
Virtual Local Area Network (VLAN) tags, 246
virtual machine export attacks, 465
virtual machine movement attacks, 465
virtual machine networks in VMM, 104
virtual machines. *See* VMs (virtual machines)
virtual memory (VMMap), 44
virtual networks, Azure IaaS VMs in, 401-403
virtual port profiles in VMM, 103
virtual private networks. *See* VPNs (virtual private networks)
virtual security, physical security versus, 466
virtual service accounts, 158
virtual switches, 242-243
virtual Trusted Platform Modules (vTPMs), exporting VMs with, 259-260
Visual Studio Code (VSCode), 22, 802
VLANs (virtual LANs), 105
VLAN (Virtual Local Area Network) tags, 246
VMMap, 44
VMM (Virtual Machine Manager), 98-108
adding WDS servers to, 105-106
host groups, 106-108
networking, 101-105
storage, 99-100
VM templates, 98-99
VM Network Health Detection, 260
VMs (virtual machines). *See also* Azure IaaS VMs; Hyper-V; VMM (Virtual Machine Manager)
checkpoints, 239-240
cloning domain controllers, 261-262
copying, 259
CPU groups, 232
DDA, 228-229
deploying, PowerShell scripts for, 82
drain on shutdown, 261
dynamic memory, 224-225
Dynamic Processor Compatibility Mode, 262-263

Enhanced Session Mode, 228
exporting, attacks via, 465
extensions, 387-388
failover clustering and, 583-584
Generation 2, 227-228
GPU-P, 230-231
guest integration services, 226-227
HVC for Linux, 235
Hyper-V replication, 246-249
importing/exporting, 258-260
live migration, 256-258
MAC addresses, 245-246
moving, attacks via, 465
nested virtualization, 233-234
network adapters, 243
network performance optimization, 244-245
PowerShell cmdlets, 263-267
PowerShell Direct, 234-235
preparation for Remote Desktop Virtualization Host, 720
resource groups, 231
resource metering, 226
shielded, 73, 263, 465-471
encryption-supported VMs versus, 470
guarded fabric for, 468-470
requirements, 466-467
shielding data file, 470-471
smart paging, 225
storage migration, 258
storage optimization, 241-242
virtual Fibre Channel adapters, 240
VM Network Health Detection, 260

volume license, switching from retail license, 760

Volume Shadow Copy Services (VSS), 746-747

volume signature catalog, 471

volumes (S2D)
adding to clusters, 284-285
expanding, 285-287

VPN gateways in IaaS virtual networks, 406

VPNs (virtual private networks), 685-693
authentication protocols, 688
certificates for, 685
disabling, 689
enabling, 689
granting access to, 690-693
IKEv2 Always On protocol, 685-686
L2TP/IPsec protocol, 687
PPTP protocol, 687-688
server deployment, 688-689
SSTP protocol, 687

VSCode (Visual Studio Code), 22, 802

Vssadmin, 746-747

VSS (Volume Shadow Copy Services), 746-747

vTPMs (virtual Trusted Platform Modules), exporting VMs with, 259-260

W

WAC. *See* Windows Admin Center

WDAC (Windows Defender Application Control), 506-508

WDS (Windows Deployment Services), 90-98
adding to VMM, 105-106
configuring options, 92-96
configuring transmissions, 96-97
driver groups/packages, 98
image management, 92
requirements, 90-91
steps in Windows Server deployment, 90

web application pools, 541-543
configuring recycling settings, 542-543
creating, 541-542

web application proxy, 643
configuring, 650-653
PowerShell cmdlets for, 659

web applications, 529

Web servers. *See* IIS (Internet Information Services)

website management, 523-541
adding websites to server, 524-527
authentication methods, 532-534
changing website settings, 528
configuring remote management, 544
configuring TLS certificates, 529-531
custom error messages, 534-535
default documents, 535-536
delegating administrative permissions, 545-546
directory browsing, 536
enabling HTTP/3, 532
enabling TLS 1.3, 531
IP address and domain name filtering, 536-538
PowerShell cmdlets, 550
request filters, 539-541
self-signed TLS certificates, 527
URL authorization rules, 538-539
virtual directories, 527-528
web applications, 529

WFAS (Windows Firewall with Advanced Security), 455-465
connection security rules, 460-465
firewall profiles, 456-457
inbound rules, 457-458
IPsec configuration, 458-460
outbound rules, 458

wget command, 70

WIM (Windows Imaging) file format, 74
WinDbg (Windows Debugger), 793-795
Windows Admin Center (WAC), 5-10
Azure IaaS VM administration, 407-408
certificate trust and, 8
configuring Azure Backup, 744-745
default tools, 6
extensions, 9
installing, 7-8
shared folder permissions, 320-321
viewing PowerShell source code, 10
Windows container image, 554
Windows Debugger (WinDbg), 793-795
Windows Defender, 517-518
Windows Defender Application Control (WDAC), 506-508
Windows Deployment Services. *See* WDS (Windows Deployment Services)
Windows Event Collector, 734
Windows Firewall, 405
Windows Firewall with Advanced Security. *See* WFAS (Windows Firewall with Advanced Security)
Windows IIS container image, 561
Windows images, 74-79
build-and-capture, 79
committing, 78
modifying, 74-75
mounting, 76
servicing, 75-78
Windows Imaging (WIM) file format, 74
Windows LAPS (Local Administrator Password Solution), 451-453
group policies, 452
installing, 451-452
password management, 452
requirements, 451
Windows Memory Diagnostic, 796-797
Windows PE, 92
Windows Remote Management (WinRM), 734
Windows Server 2008 mode, 339
Windows Server 2022, SSH Server in, 28-29
Windows Server 2025
editions of, 57
end of support, 758
hardening. *See* hardening Windows Server
hardware limitations, 58
installation options
Nano Server, 70
Server Core, 60, 70
Server with Desktop Experience, 60, 68-70
switching between, 68
licensing options, 58
Linux on, 427
onboarding to Azure Arc, 385
roles and features, adding, 71-72
servicing branches, 59-60
SSH Server in, 26-27
Windows Server Backup, 739-743
installing, 175
locations for backups, 740-741
methods for backups, 741
PowerShell cmdlets, 754
restoring from backups, 742-743
role- and application-specific backups, 742
Windows Server container image, 554, 561
Windows Server Core container image, 553, 561
Windows Server Migration Tools (WSMT), 760-762, 783-786
Windows Server Update Services. *See* WSUS (Windows Server Update Services)
Windows SIM (Windows System Image Manager), 80
Windows Subsystem for Linux. *See* WSL (Windows Subsystem for Linux)
WinGet, 83-84
WinRM (Windows Remote Management), 734
WINS (Windows Internet Name Service) servers, 195
witnesses in failover clustering, 574
workgroup clusters, 586-587
Workplace Join, 653-655
WSL (Windows Subsystem for Linux), 427-431
installing, 427-429
networking, 430-431
updating, 429
versions, 429-430
WSMT (Windows Server Migration Tools), 760-762, 783-786
WSUS (Windows Server Update Services), 747-753
automatic approval rules, 751-752
autonomous and replica modes, 748
deploying updates, 751
Group Policy options, 750-751
groups, 749
locations of update files, 748
PowerShell cmdlets, 755
product, classification, language settings, 748
security roles, 749

X–Y–Z

zone delegations (DNS servers), 193
zone scopes (DNS), 203
zones (DNS servers), 189, 196
Active Directory–integrated zones, 189-191
aging and scavenging, 197-198
GlobalNames zones, 195-196
primary zones, 191-192
reverse lookup zones, 192-193
secondary zones, 192
stub zones, 195
ZSK (Zone Signing Key), 199