



Inside **OUT**

The ultimate in-depth reference
Hundreds of timesaving solutions
Supremely organized, packed
with expert advice

Windows Server 2019

Orin Thomas

Microsoft Cloud Operations Advocate, Cloud and Datacenter expert, and leading Windows author

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Windows Server 2019 Inside Out

Orin Thomas

Windows Server 2019 Inside Out

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

Copyright © 2020 by Orin Thomas

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/permissions

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: 978-0-13-549227-7

ISBN-10: 0-13-549227-0

Library of Congress Control Number: 2020935953

ScoutAutomatedPrintCode

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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief: Brett Bartow

Executive Editor: Loretta Yates

Sponsoring Editor: Charvi Arora

Development Editor: Rick Kughen

Managing Editor: Sandra Schroeder

Senior Project Editor: Tracey Croom

Copy Editor: Charlotte Kughen

Indexer: Valerie Haynes Perry

Proofreader: Dan Foster

Technical Editor: Vince Averello

Editorial Assistant: Cindy Teeters

Cover Designer: Twist Creative, Seattle

Compositor: Danielle Foster

Graphics: Vived Graphics



Contents at a glance

Chapter 1		Chapter 13	
Administration tools	1	Active Directory Federation Services	437
Chapter 2		Chapter 14	
Installation options	31	Dynamic Access Control and Active	
Chapter 3		Directory Rights Management Services	455
Deployment and configuration	47	Chapter 15	
Chapter 4		Routing and Remote Access	475
Active Directory	109	Chapter 16	
Chapter 5		Remote Desktop Services	499
DNS, DHCP, and IPAM	159	Chapter 17	
Chapter 6		Azure IaaS and hybrid services	519
Hyper-V	191	Chapter 18	
Chapter 7		Windows Subsystem for Linux	575
Storage	229	Chapter 19	
Chapter 8		Hardening Windows Server and	
File servers	273	Active Directory	581
Chapter 9		Chapter 20	
Internet Information Services	309	Security systems and services	635
Chapter 10		Chapter 21	
Containers	337	Maintenance and monitoring	653
Chapter 11		Chapter 22	
Clustering and high availability	369	Upgrade and migration	685
Chapter 12		Chapter 23	
Active Directory Certificate Services	391	Troubleshooting	723
		Index	755



Table of contents

	Introduction	xxi
	Changes since <i>Windows Server 2016 Inside Out</i>	<i>xxi</i>
	Acknowledgments	xxii
	Errata, updates, and book support	xxii
Chapter 1	Administration tools	1
	Remote not local	1
	Privileged Access Workstations	2
	Windows Admin Center	4
	Installing Windows Admin Center	6
	Windows Admin Center extensions	9
	Show script	10
	Remote Server Administration Tools	11
	RSAT consoles	11
	Server Manager console	14
	PowerShell	17
	Modules	18
	PowerShell Gallery	19
	Remoting	19
	One-to-many remoting	21
	PowerShell ISE	21
	PowerShell Direct	24
	Remote Desktop	25
	SSH	27
Chapter 2	Installation options	31
	Windows Server 2019 editions	31
	Windows Server servicing branches	33
	Long Term Servicing Channel	33
	Semi Annual Channel	33
	Insider Preview Builds	34
	Server Core	35
	Server Core interface	36
	Server Core roles	37
	Server Core App Compatibility Features on Demand	42
	When to deploy Server Core	43

	Server with Desktop Experience	44
	Roles and features	45
Chapter 3	Deployment and configuration	47
	Bare metal versus virtualized	47
	Windows images	48
	Modifying Windows images	49
	Servicing Windows images	50
	Mounting images	50
	Adding drivers and updates to images	53
	Adding roles and features	54
	Committing an image	56
	Build and capture	56
	Answer files	57
	Windows Deployment Services	59
	WDS requirements	60
	Managing images	62
	Configuring WDS	62
	Configuring transmissions	67
	Driver groups and packages	68
	Virtual Machine Manager	68
	Virtual machine templates	68
	VMM storage	69
	VMM networking	71
	Adding a WDS to VMM	75
	VMM host groups	76
	Infrastructure configuration as code	79
	Desired State Configuration	81
	DSC configuration files	82
	Local Configuration Manager	83
	DSC resources	83
	DSC push model	84
	DSC pull server	84
	Chef Infra Server	85
	Chef servers	85
	Chef Development Kit	89
	Deploying Chef agents	94
	Deploying Chef cookbooks and recipes	95
	Puppet	96
	Puppet Master Server	96
	Deploying Puppet agent to Windows Server	99
	Managing Windows Server configuration	101
	Puppet Windows Module Pack	102
	Package-management utilities	103
	PowerShell Gallery	104
	Chocolatey	105

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	114
	Active Directory Domains and Trusts console	117
	Domain controllers	118
	Deployment	118
	Server Core	120
	Global catalog servers	121
	Read only domain controllers	121
	Virtual domain controller cloning	124
	AD DS structure	125
	Domains	125
	Domain functional levels	125
	Forests	126
	Account and resource forests	127
	Organizational units	127
	Flexible Single Master Operations roles	128
	Accounts	130
	User accounts	130
	Computer accounts	132
	Group accounts	133
	Default groups	134
	Service accounts	136
	Group policy	138
	GPO management	139
	Policy processing	141
	Group Policy preferences	143
	Administrative templates	145
	Restoring deleted items	146
	Active Directory Recycle Bin	147
	Authoritative restore	149
	Active Directory snapshots	151
	Managing AD DS with PowerShell	152
	Active Directory module	152
	Group Policy module	156
	ADDSDeployment module	157
Chapter 5	DNS, DHCP, and IPAM	159
	DNS	159
	DNS zone types	159
	Zone delegation	162
	Forwarders and conditional forwarders	163
	Stub zones	164

GlobalNames zones	164
Peer Name Resolution Protocol	165
Resource records	166
Zone aging and scavenging	167
DNSSEC	168
DNS event logs	169
DNS options	170
Delegated administration	174
Managing DNS with PowerShell	174
DHCP	177
Scopes	177
Server and scope options	178
Reservations	178
DHCP filtering	179
Superscopes	179
Multicast scopes	180
Split scopes	180
Name protection	180
DHCP failover	181
Administration	182
IPAM	185
Deploy IPAM	185
Configure server discovery	185
IPAM Administration	186
Managing IPAM with PowerShell	188
Chapter 6 Hyper-V	191
Dynamic memory	191
Smart paging	192
Resource metering	193
Guest integration services	193
Generation 2 VMs	194
Enhanced Session Mode	195
Discrete Device Assignment	195
Nested virtualization	197
Nested virtualization dynamic memory	197
Nested virtualization networking	197
PowerShell Direct	198
HVC for Linux	198
Virtual hard disks	199
Fixed-sized disks	199
Dynamically expanding disks	199
Differencing disks	200
Modifying virtual hard disks	200
Pass-through disks	201
Managing checkpoints	202
Virtual Fibre Channel adapters	203
Storage QoS	204

Hyper-V storage optimization	204
Deduplication	204
Storage tiering	204
Hyper-V virtual switches	205
External switches	205
Internal switches	205
Private switches	206
Virtual machine network adapters	206
Optimizing network performance	206
Bandwidth management	207
SR-IOV	207
Dynamic virtual machine queue	207
Virtual machine NIC teaming	208
Virtual machine MAC addresses	208
Network isolation	209
Hyper-V replica	209
Configuring Hyper-V replica servers	210
Configuring VM replicas	210
Replica failover	211
Hyper-V replica broker	211
Hyper-V failover clusters	212
Hyper-V host cluster storage	212
Cluster quorum	213
Cluster networking	214
Force Quorum Resiliency	215
Cluster Shared Volumes	215
Active Directory detached clusters	216
Preferred owner and failover settings	216
Hyper-V guest clusters	217
Hyper-V guest cluster storage	218
Shared virtual hard disk	218
Hyper-V VHD Sets	219
Live migration	219
Storage migration	221
Exporting, importing, and copying VMs	221
VM Network Health Detection	222
VM drain on shutdown	222
Domain controller cloning	223
Shielded virtual machines	223
Managing Hyper-V using PowerShell	224
Chapter 7 Storage	229
Storage spaces and storage pools	229
Storage pools	230
Storage space resiliency	234
Storage space tiering	235
Thin provisioning and trim	237
Creating virtual disks	239
Storage Spaces Direct	240

- Storage Replica 247
 - Supported configurations 248
 - Configuring replication 249
- SMB 3.1.1 251
- iSCSI 252
- iSNS server 256
- Scale-Out File Servers 258
- Server for NFS 259
- Deduplication 260
- Storage Quality of Service 263
- ReFS 264
- Storage-related PowerShell cmdlets 266
 - Deduplication 266
 - iSCSI 266
 - iSCSITarget 267
 - NFS 267
 - Storage 268
 - Storage Replica 271

Chapter 8 File servers 273

- Shared folder permissions 274
 - Using File Explorer 275
 - Windows Admin Center 276
 - Server Manager 277
- File Server Resource Manager 280
 - Folder level quotas 280
 - File screens 282
 - Storage reports 286
 - File classification 288
 - File management tasks 290
 - Access-Denied Assistance 292
- Distributed File System 293
 - DFS namespace 293
 - DFS replication 296
- BranchCache 299
- PowerShell commands 302
 - Shared Folder cmdlets 302
 - File Server Resource Manager cmdlets 303
 - BranchCache Cmdlets 305
 - DFS Cmdlets 306

Chapter 9 Internet Information Services 309

- Managing sites 309
 - Adding websites 310
 - Virtual directories 313
 - Modifying site settings 314
 - Adding web applications 314
 - Configuring TLS certificates 315

	Site authentication	318
	Modifying custom error response	319
	Adding or disabling the default document	320
	Directory browsing	321
	IP address and domain name filtering	322
	URL authorization rules	323
	Request filters	324
	Application pools	326
	Creating application pools	327
	Configuring application pool recycling settings	328
	IIS users and delegation	329
	IIS user accounts	330
	Delegating administrative permissions	331
	Managing FTP	332
	Managing IIS using PowerShell	334
Chapter 10	Containers	337
	Container concepts	337
	Isolation modes	339
	Process Isolation mode	339
	Hyper-V Isolation mode	340
	Managing containers with Docker	340
	Installing Docker	341
	Dockerfile	342
	Retrieving container OS image	344
	Container registries and images	345
	Managing containers	347
	Starting a container	347
	Modifying a running container	350
	Creating a new image from a container	351
	Using Dockerfiles	351
	Managing container images	353
	Service accounts for Windows containers	355
	Applying updates	356
	Container networking	357
	NAT	359
	Transparent	360
	Overlay	362
	Layer 2 Bridge	362
	Linux containers on Windows	363
	Container orchestration	364
	Kubernetes	365
	Docker Swarm	365
Chapter 11	Clustering and high availability	369
	Failover clustering	369
	Cluster quorum modes	370
	Cluster storage and cluster shared volumes	372

	Cluster networks	372
	MPIO	373
	Cluster Aware Updating	373
	Failover and preference settings	374
	Multisite clusters	375
	Cloud witness	376
	Virtual machine failover clustering	377
	Rolling upgrades	379
	Workgroup clusters	381
	Cluster sets	382
	Managing failover clustering with PowerShell	383
	Network Load Balancing	385
	Network Load Balancing prerequisites	386
	NLB cluster operation modes	386
	Managing cluster hosts	387
	Port rules	388
	Filtering and affinity	388
	Managing NLB with PowerShell	389
Chapter 12	Active Directory Certificate Services	391
	CA types	391
	Enterprise CA	393
	Standalone CAs	403
	Certificate revocation lists	406
	CRL distribution points	406
	Authority Information Access	407
	Revoking a certificate	408
	Publishing CRLs and delta CRLs	410
	Certificate Services role services	412
	Certificate templates	413
	Template properties	414
	Adding and editing templates	420
	Certificate autoenrollment and renewal	420
	CA management	422
	Handling certificate requests	424
	CA backup and recovery	425
	Key archiving and recovery	427
	CAPolicy.inf	432
	Managing Certificate Services using PowerShell	433
	Managing Certificate Services using Certutil.exe and Certreq.exe	435
Chapter 13	Active Directory Federation Services	437
	AD FS components	437
	Claims, claim rules, and attribute stores	438
	Claims provider	439
	Relying party	439
	Relying party trust	439
	Claims provider trust	440

	Configuring certificate relationship	441
	Attribute stores	442
	Claim rules	443
	Relying party trust claim rules	443
	Claims provider trust claim rules	444
	Configure Web Application Proxy	445
	Workplace Join	447
	Multifactor authentication	449
	Managing AD FS with PowerShell	450
	Managing Web Application Proxy with PowerShell	453
Chapter 14	Dynamic Access Control and Active Directory Rights Management Services	455
	Dynamic Access Control	455
	Configuring Group Policy to support DAC	456
	Configuring User and Device Claims	456
	Configuring Resource Properties	457
	Central access rules	459
	Central access policies	461
	Staging	463
	Access Denied Assistance	463
	Installing AD RMS	464
	AD RMS certificates and licenses	465
	AD RMS Templates	466
	AD RMS Administrators and Super Users	469
	Trusted User and Publishing Domains	470
	Exclusion policies	471
	Apply AD RMS templates automatically	471
	Managing AD RMS with Windows PowerShell	473
	Dynamic Access Control cmdlets	474
Chapter 15	Routing and Remote Access	475
	Remote Desktop Gateway	475
	RD Gateway connection and resource policies	476
	Configuring server settings	477
	Configuring clients to use RD Gateway	477
	Virtual private networks	479
	IKEv2 Always On VPN protocol	479
	SSTP VPN protocol	481
	L2TP/IPsec protocols	481
	PPTP VPN protocol	481
	VPN authentication	482
	Deploying a VPN server	482
	Disable VPN protocols	483
	Granting access to a VPN server	483
	LAN routing	487
	Network Address Translation (NAT)	487

DirectAccess	489
DirectAccess topologies	490
DirectAccess server	490
Network Location Server	492
Configuring DirectAccess	493
Managing Remote Access using PowerShell	496
Chapter 16 Remote Desktop Services	499
Deployment	499
Remote Desktop Connection Broker	502
Deployment properties	502
Remote Desktop Session Host	503
Session collection settings	504
Personal session desktops	506
RemoteApp	506
Group Policy configuration	507
Remote Desktop Virtualization Host	509
Virtual machine preparation	510
Virtual desktop collections	511
Pooled virtual desktops	512
Personal virtual desktops	512
DDA and RemoteFX	512
Remote Desktop Web Access	513
Remote Desktop licensing	513
Installing RDS CALs	514
Activating a License Server	515
Managing Remote Desktop Services using PowerShell	515
Chapter 17 Azure IaaS and hybrid services	519
Windows Server IaaS VMs	519
Creating Azure IaaS VMs	520
IaaS VM networking	524
IaaS VM administration	532
Azure Active Directory	538
Azure Active Directory Connect	540
Azure AD Connect server requirements	541
Installing Azure AD Connect	544
Using UPN suffixes and non-routable domains	551
Monitor Azure AD Connect Health	554
Forcing synchronization	555
Configure object filters	557
Implement and manage Azure AD self-service password reset	560
Azure AD Password Protection	562
Azure AD DS	563
Azure hybrid cloud services	564
Connect Windows Admin Center	565
Creating Azure IaaS VMs from Windows Admin Center	567
Azure File Sync	569

	Azure Arc	572
	Azure Site Recovery	572
	Azure Network Adapter	573
Chapter 18	Windows Subsystem for Linux	575
	Linux on Windows Server	575
	Installing WSL	576
	WSL 2.0	579
Chapter 19	Hardening Windows Server and Active Directory	581
	Hardening Active Directory	582
	Hardening domain controllers	582
	Least privilege	583
	Role-Based Access Control	584
	Password policies	585
	Account security options	586
	Protected accounts	588
	Authentication policies silos	589
	Disable NTLM	591
	Block server operators from scheduling tasks	592
	Enable Local Security Authority protection	592
	KRBTGT account password	593
	Enhanced Security Administrative Environment forest	594
	Hardening Windows Server	596
	User rights	596
	Service accounts	600
	Just Enough Administration	603
	Privileged Access Management	609
	Local Administrator Password Solution	613
	Advanced auditing	615
	Windows Firewall with Advanced Security	618
	Shielded VMs	628
	Guarded fabric	631
Chapter 20	Security systems and services	635
	Security Compliance Toolkit	636
	Policy Analyzer tool	636
	Local Group Policy Object tool	638
	Attack Surface Analyzer	638
	Credential Guard	640
	Windows Defender Application Control	642
	Virtualization-based security	644
	Controlled Folder Access	645
	Exploit Protection	647
	Windows Defender	650
	Windows Defender SmartScreen	651

Chapter 21	Maintenance and monitoring	653
	Data collector sets	653
	Alerts	655
	Event Viewer	655
	Event log filters	655
	Event log views	656
	Event subscriptions	657
	Event-driven tasks	658
	Network monitoring	659
	Resource Monitor	659
	Message Analyzer	660
	Azure Monitor	661
	Windows Server Backup	662
	Backup locations	664
	Backing up data	664
	Role- and application-specific backups	665
	Restore from backups	665
	Restore to an alternative location	666
	Azure Backup	666
	Preparing Azure Backup	667
	Backing up data to Azure Backup Agent	669
	Restore from Azure Backup	669
	Vssadmin	670
	Windows Server Update Services	672
	Products, security classifications, and languages	672
	Autonomous and replica modes	673
	Update files	673
	WSUS security roles	674
	WSUS groups	675
	WSUS policies	675
	Deploying updates	677
	Automatic approval rules	677
	Azure Update Management	679
	Monitoring and maintenance related PowerShell cmdlets	683
	WSUS related PowerShell cmdlets	684
Chapter 22	Upgrade and migration	685
	Supported upgrade and migration paths	685
	Upgrading roles and features	687
	Converting evaluation version to licensed version	688
	Upgrading editions	689
	Windows Server Migration Tools	689
	Active Directory	693
	FRS to DFSR migration	695
	Migrating to a new forest	696

Active Directory Certificate Services	699
Preparation	700
Migration	702
Verification and post migration tasks	703
DNS	704
DHCP	705
Preparing to migrate DHCP	706
Migration	708
Verification and post migration tasks	709
File and storage servers	709
Migrate file servers using Storage Migration Service	710
Migrate file and storage servers using WSMT	718
Chapter 23 Troubleshooting	723
Troubleshooting methodology	723
Redeployment	724
Symptoms and diagnosis	725
Dependencies	726
Ranking hypothetical solutions	727
Applying solutions	728
Command-line tools	729
Sysinternals tools	733
Process Explorer	734
Process Monitor	735
ProcDump	736
PsTools	737
VMMap	738
SigCheck	739
AccessChk	740
Sysmon	741
AccessEnum	744
ShellRunAs	745
LogonSessions	746
Active Directory Explorer	746
Insight for Active Directory	749
PsPing	750
RAMMap	751
Index	761

About the author



Orin Thomas is a principal cloud operations advocate at Microsoft and has written more than three dozen books for Microsoft Press on topics including Windows Server, Windows Client, Azure, Office 365, System Center, Exchange Server, Security, and SQL Server. He has authored Azure Architecture courses at Pluralsight, has authored multiple Microsoft Official Curriculum and EdX courses on a variety of IT Pro topics, and is completing his Doctorate in Information Technology on cloud computing security and compliance at Charles Sturt University. You can follow him on twitter at <http://twitter.com/orinthomas>.

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 2019 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. With that in mind, this book doesn't spend a great amount of time on introductory concepts or techniques; instead, it aims to provide intermediate to advanced coverage of the most important roles and features available with Windows Server 2019, including its hybrid cloud capabilities.

This book is also written under the assumption that as an experienced IT professional, you know how to use a search engine to find relevant technical information. This leads to an obvious question, "Why would I buy a book if I can find relevant technical information with a search engine?" 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 search for something if you have an idea about it in the first place.

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 is because Windows Server 2019 includes so many roles, features, and moving parts, you are simply unlikely to know everything about the operating system. My aim in writing this book is to give you comprehensive coverage so that you'll learn things that you didn't know or simply missed, 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.

Changes since *Windows Server 2016 Inside Out*

This book includes several new chapters as well as revisions and updates—from moderate to substantive—of chapters that were present in the Windows Server 2016 version of this book. Some of the substantive changes include removing content related to the Nano Server deployment option, which is no longer supported; coverage of Windows Admin Center; a new chapter on Azure IaaS and hybrid services, as well as Windows Subsystem for Linux; and splitting an extension of the security chapter from the 2016 edition into two separate chapters in this text. There is also coverage of new roles and features including Storage Migration Services, Azure File Sync, and Azure Update Management. While there are some chapters where only cosmetic changes were made, from the perspective of total word count, this book is about 15 percent longer than its predecessor, *Windows Server 2016 Inside Out*.

Acknowledgments

I'd like to thank Rick Kughen, Vince Averello, Dan Foster, Charvi Arora, and Loretta Yates for the assistance they provided in bringing this text to print. I would also like to thank Thomas Maurer for his advice on revisions for this new edition of the text.

Figure Credits

Figure number	Credit
FIG03-17	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-18	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-19	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-20	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-21	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-22	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-23	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-24	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-25	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-26	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-27	Copyright © 2020 Chef Software, Inc. All Rights Reserved.
FIG03-28	© 2020 Puppet
FIG03-29	© 2020 Puppet
FIG03-30	© 2020 Puppet
FIG03-31	© 2020 Puppet
FIG03-32	© 2020 Puppet
FIG11-01	Courtesy of Pearson Education

Errata, updates, and book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/WindowsServer2019InsideOut/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 <http://support.microsoft.com>.



Bare metal versus virtualized	47	Infrastructure configuration as code	79
Windows images	48	Desired State Configuration	81
Answer files	57	Chef Infra Server	85
Windows Deployment Services	59	Puppet	96
Virtual Machine Manager	68	Package-management utilities	103

Depending on the size of your organization, you might deploy a couple of servers and then leave them in production for years, or, as we saw when it came to the (ongoing) retirement of Windows Server 2008 R2, well over a decade. Other organizations deploy servers on a more frequent basis. Some even use a process where rather than applying software updates to a production server and incurring downtime as the update is applied and the server rebooted, they find it faster to deploy a newly patched computer, to migrate the existing workload to the new host, and then to decommission the original server.

This type of iterative deployment is possible because the tools around managing the configuration of servers have evolved. Today, deploying and configuring a new server is no more bothersome than deploying an application would have been a decade ago. In this chapter, you'll learn about how you can use Windows Server images, Windows Deployment Services, Virtual Machine Manager, Desired State Configuration, Puppet, and Chef to deploy and manage the configuration of computers and virtual machines running the Windows Server 2019 operating system.

Bare metal versus virtualized

Today, almost all new workloads are virtualized. For most organizations, virtualization hosts are the primary remaining physically deployed server, with almost all other workloads running as virtual machines. Unless you have specific reasons not to virtualize a workload, you should run Windows Server 2019 as a virtual machine (VM) rather than as a physically deployed server.

The security available with shielded VMs addresses one of the final objections that many organizations have had around deploying servers virtually rather than physically. With shielded VMs, you can provide the same level of security to a workload that you can to a physically deployed server sitting in a locked cage in a datacenter.

At present, your best bet when deploying virtualization hosts is to choose the Server Core installation option because this has a smaller installation footprint and a reduced attack surface compared to the Server with Desktop Experience option. When you deploy a Server Core virtualization host, you manage Hyper-V remotely from a privileged access workstation or a tool such as Windows Admin Center or Virtual Machine Manager.

Windows images

With Windows *images*, the entire operating system, as well as associated drivers, updates, and applications, is stored within a single file known as an image file. During installation, this image is applied to the target volume. Windows images use the Windows Imaging (WIM) file format, which has the following benefits:

- **Multiple deployment methods.** You can use a variety of ways to deploy Windows images. While unusual these days, you can deploy *.wim* files using a traditional DVD-ROM, from a bootable USB drive, from a network share, or through specialized deployment technologies such as Windows Deployment Services (WDS) or System Center Virtual Machine Manager. While it is possible to use System Center Configuration Manager to deploy Windows Server, Configuration Manager is primarily used with client operating systems rather than server operating systems.
- **Editable.** You can mount an image and edit it, enabling, disabling, or removing operating system roles and features as necessary.
- **Updatable.** You can update an image without having to perform an operating system image capture.

The Windows Server 2019 installation media contain two *.wim* files in the Sources folder: *Boot.wim* and *Install.wim*. The installation media uses *Boot.wim* to load the preinstallation environment that you use to deploy Windows Server 2019. *Install.wim* stores one or more operating system images. For example, as Figure 3-1 shows, the *Install.wim* file available with the evaluation version of Windows Server 2019 contains four different editions of Windows Server 2019. Depending on the specifics of the hardware on which you are attempting to install Windows Server, you might need to add extra drivers to the *boot.wim* file. For example, you will need to add extra drivers if the Windows Server installation routine cannot access the storage device on which you want to install Windows Server because that device's driver is included in the default boot image.

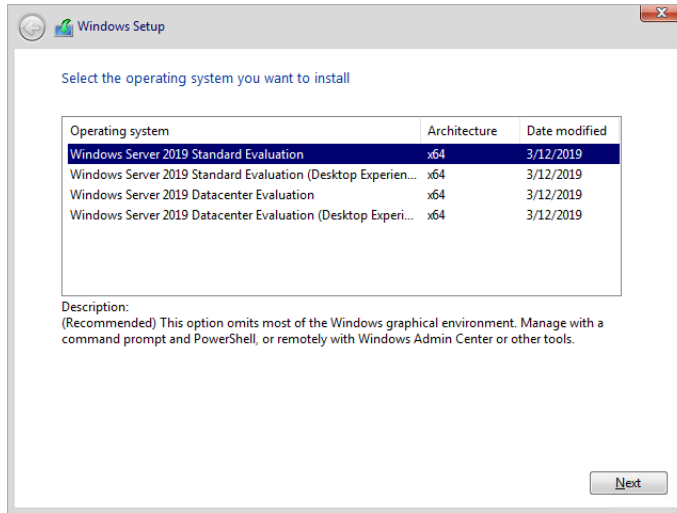


FIGURE 3-1 Windows Server 2019 editions

Modifying Windows images

The Deployment Image Servicing and Management (DISM) tool is a command-line tool that you can use to manage images in an offline state. You can use *Dism.exe* to perform the following tasks:

- Enable or disable roles and features
- List roles and features
- Add, remove, and list software updates
- Add, remove, and list software drivers
- Add, remove, and list software packages in .appx format to a Windows image

For example, you can take the *Install.wim* file from the Windows Server installation media and use *Dism.exe* to mount that image, add new drivers and recent software updates to that image, and save those changes to an image all without having to perform an actual deployment. The advantage is that when you do use this updated image for deployment, the drivers and updates that you added are already applied to the image and you won't have to install them as part of your post-installation configuration routine.

You can use the Microsoft Update Catalog (<https://catalog.update.microsoft.com>) to search for drivers for images that you use with physically deployed servers. This site stores all the certified hardware drivers, software updates, and hotfixes published by Microsoft. Once you download

drivers and software updates, you can add them to your existing installation images by using *Dism.exe* or the appropriate PowerShell cmdlets in the *DISM* PowerShell module.

Servicing Windows images

As an IT professional responsible for deploying Windows Server, you need to ensure that your deployment images are kept up to date. The latest software updates should be applied to the image, and any new device drivers for commonly used server hardware should be included.

The main goals of an image servicing strategy are the following:

- Ensure that the latest software updates and hotfixes are applied to the image before the image is deployed to new servers.
- Ensure that the latest drivers are applied to the image before the image is deployed to new servers.

If you don't take these steps, you'll have to wait until after you've deployed the operating system before you can apply updates and drivers. While Windows Server updates are cumulative now, and you won't need to spend hours updating an image from RTM, it's quicker to have the most recent update already applied to the image than it is to wait for the server to deploy, retrieve the latest update, and then wait for it to download and then install. Having updates apply after deployment has occurred consumes a significant amount of time and also substantively increases network traffic. One of your aims when performing a deployment should be to get the server operational and hosting workloads as quickly as possible.

You can use the DISM (Deployment Image Servicing and Management) utility or the associated PowerShell cmdlets in the *DISM* PowerShell module to service the current operating system in an online state or perform offline servicing of a Windows image.

Servicing images involves performing the following general steps:

1. Mount the image so that it can be modified.
2. Service the image.
3. Commit or discard the changes made to the image.

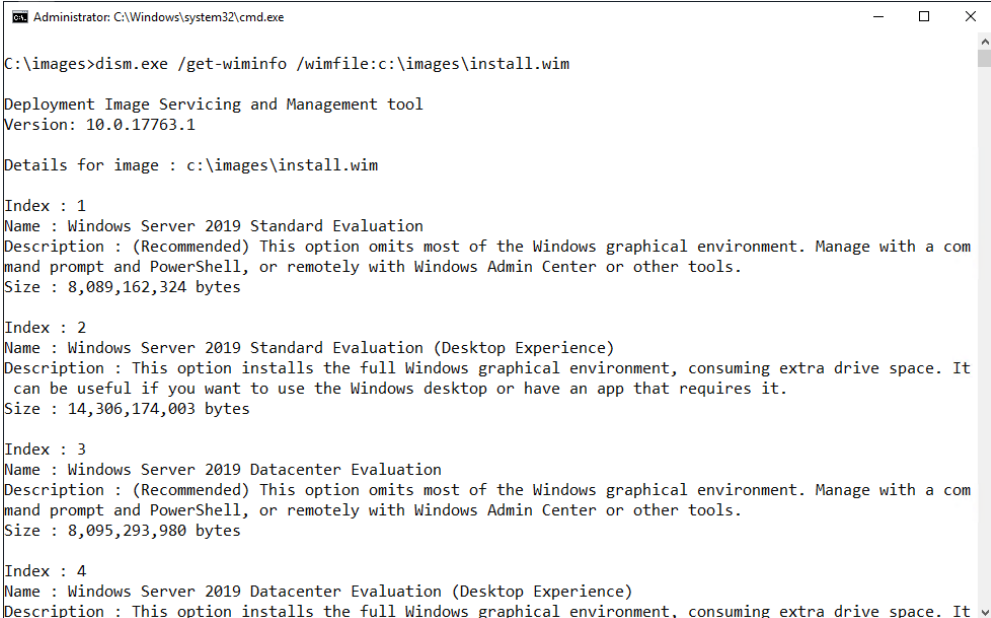
Mounting images

By mounting an image, you can make changes to that image. When you mount an image, you link it to a folder. You can use File Explorer, Windows PowerShell, or *Cmd.exe* to navigate the structure of this folder and interact with it as you would any other folder located on the file system. Once the image is mounted, you can also use *Dism.exe* or PowerShell to perform servicing tasks, such as adding and removing drivers and updates.

A single WIM file can contain multiple operating system images. Each operating system image is assigned an index number, which you need to know before you can mount the image. You can determine the index number using *Dism.exe* with the */Get-wiminfo* switch. For example, if you have an image named *Install.wim* located in the *C:\Images* folder, you can use the following command to get a list of the operating system images it contains.

```
Dism.exe /get-wiminfo /wimfile:c:\images\install.wim
```

Figure 3-2 shows the result of this command and lists the images contained in Windows Server 2019. The Standard Evaluation Edition of Windows Server 2019 with the Server Core installation option is assigned index identity 1, the Standard Evaluation with Desktop Experience is assigned index identity 2, the Datacenter Evaluation with the Server Core installation option is assigned index identity 3, and the Datacenter Evaluation with Desktop Experience is assigned index identity 4.



```
Administrator: C:\Windows\system32\cmd.exe

C:\images>dism.exe /get-wiminfo /wimfile:c:\images\install.wim

Deployment Image Servicing and Management tool
Version: 10.0.17763.1

Details for image : c:\images\install.wim

Index : 1
Name : Windows Server 2019 Standard Evaluation
Description : (Recommended) This option omits most of the Windows graphical environment. Manage with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.
Size : 8,089,162,324 bytes

Index : 2
Name : Windows Server 2019 Standard Evaluation (Desktop Experience)
Description : This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.
Size : 14,306,174,003 bytes

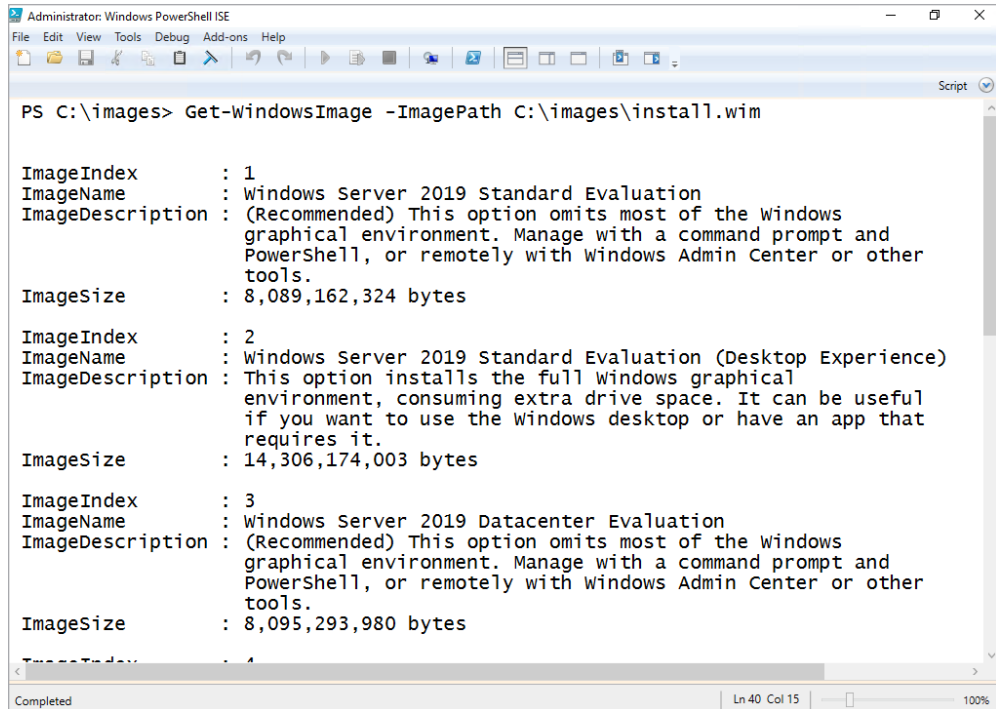
Index : 3
Name : Windows Server 2019 Datacenter Evaluation
Description : (Recommended) This option omits most of the Windows graphical environment. Manage with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.
Size : 8,095,293,980 bytes

Index : 4
Name : Windows Server 2019 Datacenter Evaluation (Desktop Experience)
Description : This option installs the full Windows graphical environment, consuming extra drive space. It
```

FIGURE 3-2 Details of an operating system image

You can accomplish the same task using the *Get-WindowsImage* PowerShell cmdlet. For example, to view the contents of the image *Install.wim* in the *C:\Images* folder, run the following command, as shown in Figure 3-3.

```
Get-WindowsImage -ImagePath c:\images\install.wim
```



```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\images> Get-WindowsImage -ImagePath C:\images\install.wim

ImageIndex      : 1
ImageName       : Windows Server 2019 Standard Evaluation
ImageDescription : (Recommended) This option omits most of the Windows
                  graphical environment. Manage with a command prompt and
                  PowerShell, or remotely with Windows Admin Center or other
                  tools.
ImageSize       : 8,089,162,324 bytes

ImageIndex      : 2
ImageName       : Windows Server 2019 Standard Evaluation (Desktop Experience)
ImageDescription : This option installs the full Windows graphical
                  environment, consuming extra drive space. It can be useful
                  if you want to use the Windows desktop or have an app that
                  requires it.
ImageSize       : 14,306,174,003 bytes

ImageIndex      : 3
ImageName       : Windows Server 2019 Datacenter Evaluation
ImageDescription : (Recommended) This option omits most of the Windows
                  graphical environment. Manage with a command prompt and
                  PowerShell, or remotely with Windows Admin Center or other
                  tools.
ImageSize       : 8,095,293,980 bytes

ImageIndex      : 4
ImageName       : Windows Server 2019 Datacenter Evaluation (Desktop Experience)
ImageDescription : This option installs the full Windows graphical
                  environment, consuming extra drive space. It can be useful
                  if you want to use the Windows desktop or have an app that
                  requires it.
ImageSize       : 14,306,174,003 bytes

Completed | Ln 40 Col 15 | 100%

```

FIGURE 3-3 Windows image details

Inside OUT

DISM and PowerShell

Image management coverage is provided for both DISM and PowerShell because a large number of IT professionals are accustomed to the former and may still use DISM in scripts. In the long run, it's probably a good idea to use PowerShell, but it's also fair to say that DISM will be around for some time yet.

Once you have determined which operating system image you want to service, you can use the */Mount-image* switch with the *Dism.exe* command to mount that image. For example, to mount the Standard Edition of Windows Server 2019 from the *Install.wim* file that is available with the Evaluation Edition in the *C:\Mount* folder, issue this command:

```
Dism.exe /mount-image /imagefile:c:\images\install.wim /index:2 /mountdir:c:\mount
```

Alternatively, you can accomplish the same goal using the following *Mount-WindowsImage* command:

```
Mount-WindowsImage -ImagePath c:\images\install.wim -index 2 -path c:\mount
```

Adding drivers and updates to images

Once you have mounted an image, you can start to service that image. When servicing images used to deploy Windows Server, the most common tasks are adding device drivers and software updates to the image. You can use the */Add-Driver* switch with the *Dism.exe* command to add a driver to a mounted image. When using the switch by itself, you need to specify the location the driver's *.inf* file. Rather than adding a driver at a time, you can use the */Recurse* option to have all drivers located in a folder and its subfolders added to an image. For example, to add all of the drivers located in and under the *C:\Drivers* folder to the image mounted in the *C:\Mount* folder, use the following command.

```
Dism.exe /image:c:\mount /Add-Driver /driver:c:\drivers\ /recurse
```

Similarly, you could use the *Add-WindowsDriver* cmdlet to accomplish the same objective by issuing the command:

```
Add-WindowsDriver -Path c:\mount -Driver c:\drivers -Recurse
```

You can use the */Get-Driver* option to list all drivers that have been added to the image and the */Remove-Driver* option to remove a driver from an image. In PowerShell, you use the *Get-WindowsDriver* cmdlet and the *Remove-WindowsDriver* cmdlets. You can remove only the drivers that you or someone else has added to an image. You can't remove any of the drivers that were present in the image when Microsoft published it. You might choose to remove an existing driver if the driver you added in the past has since been updated.

You can use *Dism.exe* with the */Add-Package* switch to add packages that contain updates or packages in *.cab* or *.msu* format. Software updates are available from the Microsoft Update Catalog website in *.msu* format. For example, you can download an update from the Microsoft Update Catalog website named *Cumulative Update For Windows Server 2019 for x64-based Systems (KB4505056)* to the *C:\Updates* folder on a computer, as shown in Figure 3-4.

If you mounted a WIM image of the Windows Server 2019 operating system in the *C:\Mount* folder, you could apply the update to the image by using the command:

```
Dism.exe /image:c:\mount /Add-Package /PackagePath:"c:\updates\windows10.0-kb4505056-x64_09c6216e684ce667fc0c07cc30e84ef21f04c6f1.msu"
```

You can accomplish the same thing with the following *Add-WindowsPackage* command:

```
Add-WindowsPackage -path c:\mount -packagepath "c:\updates\AMD64-all-windows10.0-kb4505056-x64_09c6216e684ce667fc0c07cc30e84ef21f04c6f1.msu"
```

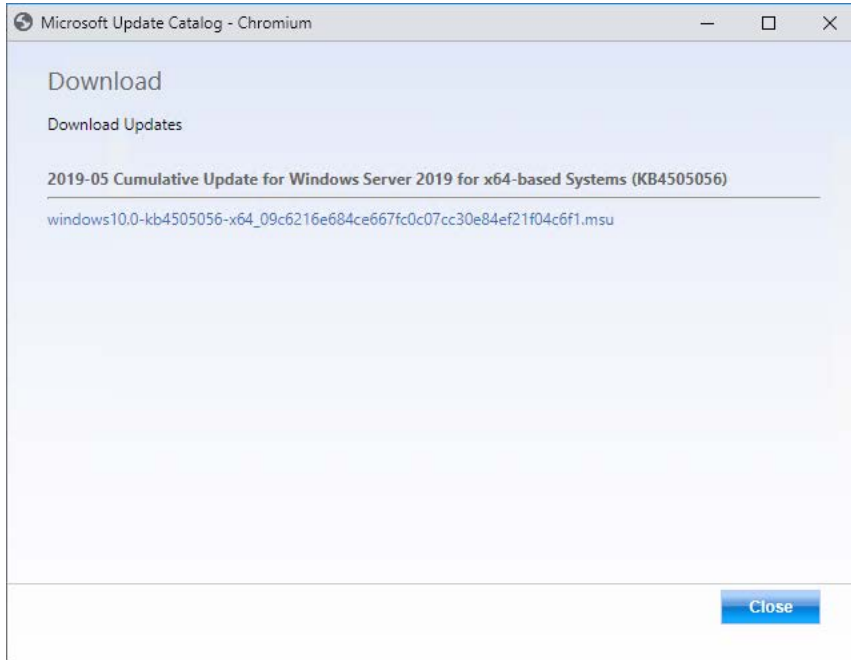


FIGURE 3-4 Downloading a cumulative update

Adding roles and features

You can determine which features are available in a mounted operating system image by using the `/Get-Features` switch. Features include both Windows Server 2019 roles and features. For example, to learn which features are available in the image mounted in the `C:\Mount` folder, use this command, as shown in Figure 3-5:

```
Dism.exe /image:c:\mount /Get-Features
```

You can enable or disable a specific feature using the `/Enable-Feature` switch. For example, to enable the `NetFx3ServerFeatures` feature, which enables the .NET Framework 3.5 server features in an image, use this command.

```
Dism.exe /image:c:\mount /Enable-Feature /all /FeatureName:NetFx3ServerFeatures
```

Some features in the Windows Server image are in a state in which they are listed as having their payload removed, which means that the installation files for that feature are not included in the image. If you install a feature that had its payload removed when the operating system was deployed, the operating system can download the files from the Microsoft update servers on the Internet. You can also specify the location of the installation files. The installation files for the features that have had their payload removed in Windows Server are located in the `\Sources\sxs` folder of the volume in which the installation media is located.

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\> dism.exe /image:c:\mount /Get-Features

Deployment Image Servicing and Management tool
Version: 10.0.17763.1

Image Version: 10.0.17763.379

Features listing for package : Microsoft-Windows-Foundation-Package~31bf3856ad364e35-amd64~10.0.17763.1

Feature Name : Server-Core
State : Enabled

Feature Name : NetFx4ServerFeatures
State : Enabled

Feature Name : NetFx4
State : Enabled

Feature Name : NetFx4Extended-ASPNET45
State : Disabled

Feature Name : MicrosoftWindowsPowerShellRoot
State : Enabled

Feature Name : MicrosoftWindowsPowerShell
State : Enabled

Completed | Ln 949 Col 9 | 100%

```

FIGURE 3-5 View features

You can add these payload-removed features to an image by using *Dism.exe* and specifying the source directory. For example, to modify an image mounted in the *C:\Mount* folder so that the Microsoft .NET Framework 3.5 features are installed and available, issue this command when the installation media is located on volume D, as shown in Figure 3-6:

```
Dism.exe /image:c:\mount /Enable-Feature /all /FeatureName:NetFx3 /Source:d:\sources\sxs
```

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\> Dism.exe /image:c:\mount /Enable-Feature /all /FeatureName:NetFx3 /Source:d:\sources\sxs

Deployment Image Servicing and Management tool
Version: 10.0.17763.1

Image Version: 10.0.17763.379

Enabling feature(s)

[=====100.0%=====]
The operation completed successfully.

PS C:\> |

```

FIGURE 3-6 Enabling a feature

Inside OUT

.NET Framework 3.5

While features like WINS remain available within Windows Server 2019, the .NET Framework 3.5 is not only not installed by default, but it has been quarantined into its own separate installation folder. One might suspect that Microsoft wants it to be difficult to install. The problem is that such a huge variety of software depends on .NET Framework 3.5, which makes installing it more of a hassle than it needs to be.

Committing an image

When you finish servicing an image, you can save your changes using the `/Unmount-Wim` switch with the `/Commit` option. You can discard changes using the `/Discard` option. For example, to make changes and then commit the image mounted in the `C:\Mount` folder, use this command.

```
Dism.exe /Unmount-Wim /MountDir:c:\mount /commit
```

You can use the `Save-WindowsImage` PowerShell cmdlet to save changes to an image without dismounting the image. You use the `Dismount-WimImage` cmdlet with the `Save` parameter to save the modifications that you've made to an image and then dismount it. For example, to dismount and save the image mounted in the `C:\Mount` folder, run the command:

```
Dismount-WimImage -Path c:\mount -Save
```

Once you have committed the changes, the `.wim` file that you originally mounted is updated with these modifications. You can then import this `.wim` file into WDS, use it to build a virtual hard disk, or use it with bootable USB installation media to deploy Windows Server 2019 with these updates and modifications already applied.

Build and capture

When you perform a build and capture, you deploy an operating system; provision that operating system with updates, applications, and drivers; and then capture that operating system for deployment. Build and capture is used less often with server operating systems because they rarely require the same sort of application deployment that is required for client operating systems. If you can just pull a container with an updated application down onto an operating system after deployment, there is little reason to include it in the image. Additionally, with tools such as Desired State Configuration, Chef, and Puppet, many post-installation and configuration tasks can be completely automated, reducing the hassle of post-installation configuration.

If your deployment strategy does involve the deployment and capture of Windows Server 2019, you need to remember that you'll need to generalize the image prior to capture, removing any

configuration information that is specific to the installation. You can perform this task using the Sysprep.exe utility. Sysprep.exe is included with Windows Server 2019 and is located in the `C:\Windows\System32\Sysprep` folder. When you use Sysprep.exe to prepare the image, you can configure the image to return to the system Out-of-Box Experience (OOBE), as shown in Figure 3-7. This is the same experience you get when Windows Server boots for the first time, though in this case all the updates, applications, and drivers included in the captured image are included in the newly deployed image.

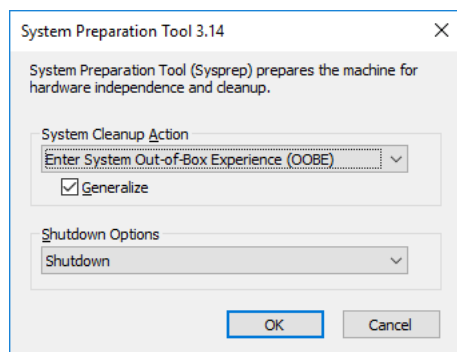


FIGURE 3-7 Sysprep

You can use Dism.exe with the `/Capture-Image` switch or the `New-WindowsImage` PowerShell cmdlet to capture an image.

Answer files

Answer files present a traditional method of performing operating system deployment and configuration. While not as comprehensive as newer technologies such as Desired State Configuration (DSC) that assist not only in deployment but in ongoing configuration, answer files allow you to automate the process of deploying Windows Server.

Instead of having to manually select specific installation options and perform post-installation configuration actions such as joining a newly deployed server to an AD DS domain, you can automate the process with answer files. During setup, the Windows Server looks for a file on local and attached media named `Autounattend.xml`. If this file is present, Windows Server automatically uses the settings contained in the file to configure the new server deployment.

As its name suggests, `Autounattend.xml` uses the XML file format. Although it is certainly possible for you to manually edit this XML file using a text editor such as Notepad, this process is complicated, and you are likely to make errors that cause the file to not work. The Windows System Image Manager (known as Windows SIM) is a GUI-based tool that you can use to create an answer file. When using the tool, you must specify the image for which you want to create

an answer file. Windows SIM then creates a catalog file for all the options that you can configure. After you configure all the settings that you want automated during installation and post-installation configuration, you can have the tool output an answer file using correct XML syntax. Windows SIM is included with the Windows Assessment and Deployment Kit (Windows ADK), which you can download from the Microsoft website.

To create an answer file using Windows SIM, perform the following steps:

1. Download and install Windows ADK from the Microsoft website using the installation defaults. You can do this with Chocolatey, covered later in this chapter, by running the following command:


```
Choco install -y windows-adk-all
```
2. Copy the `\Sources\install.wim` file from the Windows Server installation media to a temporary directory on the computer on which you have installed Windows ADK.
3. Open Windows SIM from the Start screen.
4. In the Windows SIM interface, click File, and then choose Select Windows Image. Open the *Install.wim* file.
5. Select an operating system image in the install image for which you wish to create an answer file. For example, Figure 3-8 shows the selection of the Standard edition with Desktop Experience operating system.

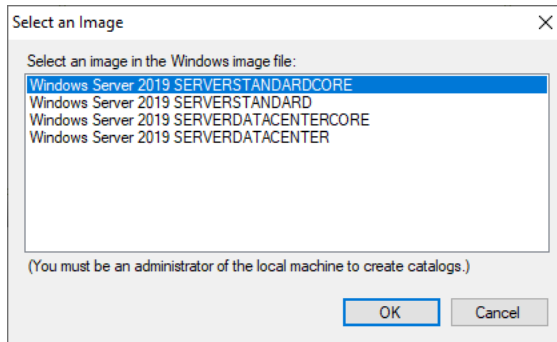


FIGURE 3-8 Select an image

6. When prompted to create a catalog file, click Yes.
7. Click File, New Answer File.

- Use Windows SIM to select each component that you want to configure. Figure 3-9 shows how you can configure installation to join the *adatum.com* domain.

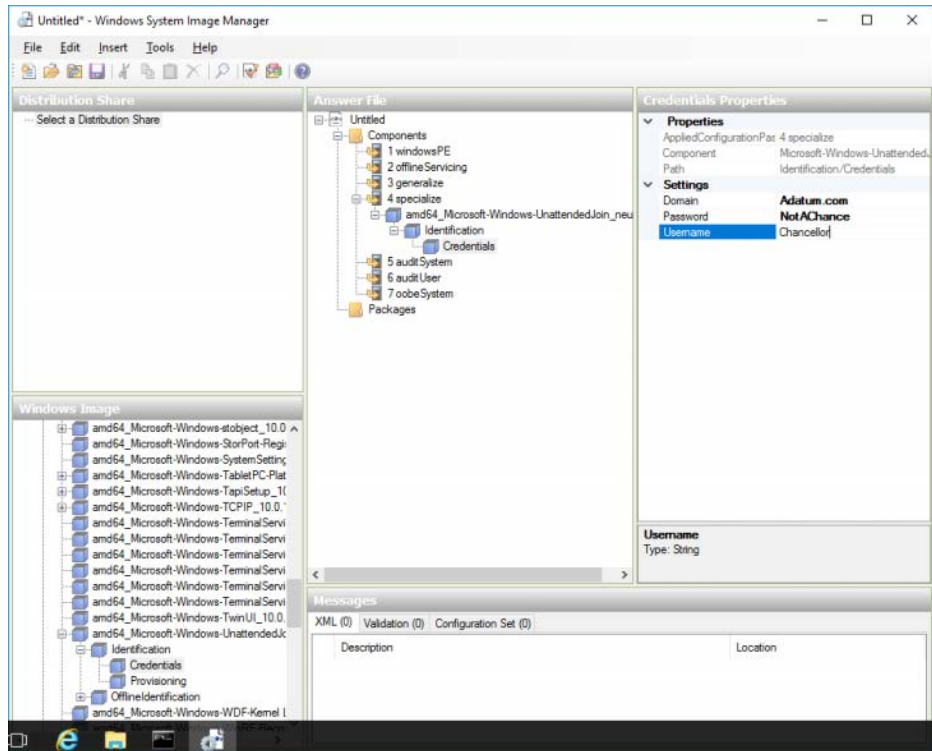


FIGURE 3-9 Windows System Image Manager

Windows Deployment Services

Windows Deployment Services (WDS) is a server role that you can deploy on computers running Windows Server. WDS enables you to deploy operating systems, including Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, to computers over the network. WDS can send these operating systems across the network using multicast transmissions, which means that multiple computers receive the same operating system image while minimizing the use of network bandwidth. When you use multicast transmissions, the same amount of traffic crosses the network independently of whether you are deploying an operating system to 1 computer or to 50. WDS also can use unicast transmissions.

Deploying Windows Server through WDS involves performing the following steps:

- An operating system deployment transmission is prepared on the WDS server.

2. The media access control (MAC) addresses of Pre-boot Execution Environment (PXE)-compliant network adapters are made available to the WDS server.
3. The computers that are targets of the transmission boot using their PXE-compliant network adapters.
4. These computers locate the WDS server and begin the operating system setup process. If the WDS server has been provisioned with an answer file, the setup completes automatically. If the WDS server has not been provisioned with an answer file, an administrator must enter setup configuration information.

Each WDS server can have only one unattended installation file for each processor architecture. Because unattended installation files differ between server and client, you either need to swap unattended files when you are switching between client and server or have multiple WDS servers. WDS can be used in conjunction with other technologies such as Desired State Configuration where an answer file only performs basic configuration tasks, with the substantial tasks completed by an advanced configuration technology.

WDS requirements

WDS clients need a PXE-compliant network adapter, which is rarely a problem because almost all modern network adapters are PXE-compliant. You can also use WDS to deploy Windows Server 2012 and later to virtual machines running under Hyper-V. The trick to doing this is to use a legacy rather than a synthetic network adapter when creating the virtual machine as a Generation 1 virtual machine. This isn't necessary when using Generation 2 virtual machines because the Generation 2 virtual machine network adapters support PXE booting.

If you have a computer that does not have a PXE-compliant network adapter, you can configure a special type of boot image known as a discover image. A discover image boots an environment, loading special drivers to enable the network adapter to interact with the WDS server. You create the boot image by adding the appropriate network adapter drivers associated with the computer that can't PXE boot to the *Boot.wim* file from the Windows Server installation media.

WDS has the following requirements:

- A Windows Server DNS server must be present on the local area network (LAN).
- Prior to Windows Server 1810, an authorized Dynamic Host Configuration Protocol (DHCP) server must be present on the network. You can host WDS and DHCP on the same computer as long as you configure the options shown in Figure 3-10. Versions of Windows Server after 1810—including Windows Server 2019—can be used with third-party DHCP

servers. Because this limits your ability to use IP address tracking through IPAM, using a third-party DHCP server if you are using WDS is not a recommended strategy.

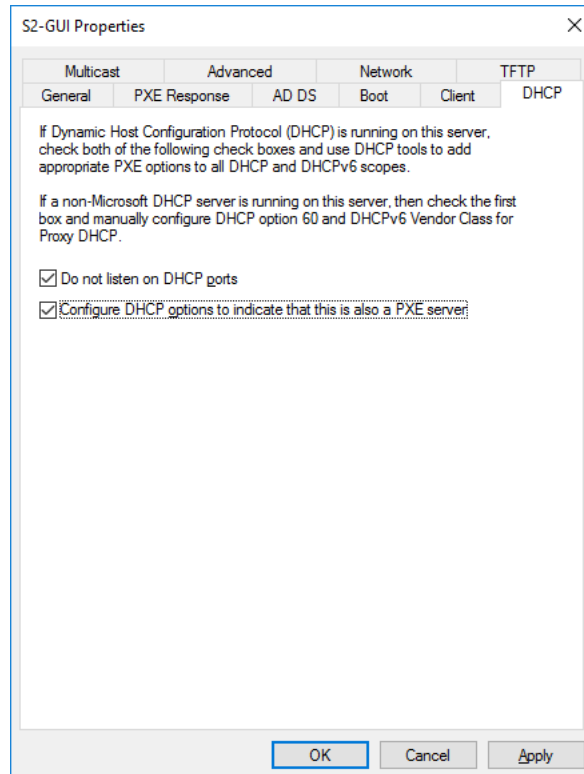


FIGURE 3-10 WDS DHCP settings

If you install WDS from the Add Roles And Features Wizard, you can configure these settings automatically. Although the WDS server does not require a static IP address, it is good practice to ensure that infrastructure roles such as WDS always use a consistent network address. You can install WDS on computers running the Server Core version of Windows Server.

When installing WDS on Server Core, you have to specify the location of the source files or ensure that the server has a connection to the Internet, which enables them to be downloaded automatically. Although it is possible to manage WDS from Windows PowerShell, most administrators use the graphical WDS Remote Server Administration Tools (RSAT) from a computer running Windows 10, Windows Server 2016, or Windows Server 2019 with Desktop Experience.

Managing images

Images contain either entire operating systems or a version of a special stripped-down operating system known as Windows PE. Windows PE functions as a type of boot disk, enabling a basic environment to be loaded from which more complex maintenance and installation tasks can be performed. WDS uses four image types: boot image, install image, discover image, and capture image.

- **Boot Image.** A special image that enables the computer to boot and begin installing the operating system using the install image. A default boot image, named *Boot.wim*, is located in the *sources* folder of the Windows Server installation media.
- **Install Image.** The main type of image discussed in this chapter. Contains the operating system as well as any other included components, such as software updates and additional applications. A default install image, named *Install.wim*, is present in the *sources* folder of the Windows Server installation media. Install images can be in *.vhd* or *.vhdx* format, though you can only manage install images using the WDS console in Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019.
- **Discover Image.** This special image is for computers that cannot PXE boot to load appropriate network drivers to begin a session with a WDS server.
- **Capture Image.** A special image type that enables a prepared computer to be booted so that its operating system state can be captured as an install image. You add capture images as boot images in WDS.

To import an image into WDS, perform the following steps:

1. Open the Windows Deployment Services console.
2. Click Install Images. From the Action menu, click Add Install Image.
3. Choose whether to create a new image group or to use an existing image group.
4. Specify the location of the image file.
5. In the Available Images page of the Add Image Wizard, select the operating system images that you want to add. When the image or images are added, click Next, Finish.

Configuring WDS

The installation defaults for WDS are suitable when you deploy the role in small environments. If you are deploying WDS in larger environments and do not choose to implement System Center Virtual Machine Manager for server operating system deployments, you might want to configure the options discussed in the following sections, which are available by editing the properties of the WDS server in the Windows Deployment Services console.

PXE response settings

With PXE response settings, you can configure how the WDS server responds to computers. As Figure 3-11 shows, you can configure WDS not to respond to any client computers (this effectively disables WDS), to respond to known client computers, or to respond to all computers but require an administrator to manually approve an unknown computer. Known computers are those that have prestaged accounts in Active Directory. You can prestage computers if you know the MAC address of the network interface card (NIC) that the computer uses. Vendors often supply a list of MAC addresses associated with computers when you purchase those computers, and you can use this list to prestage computer accounts.

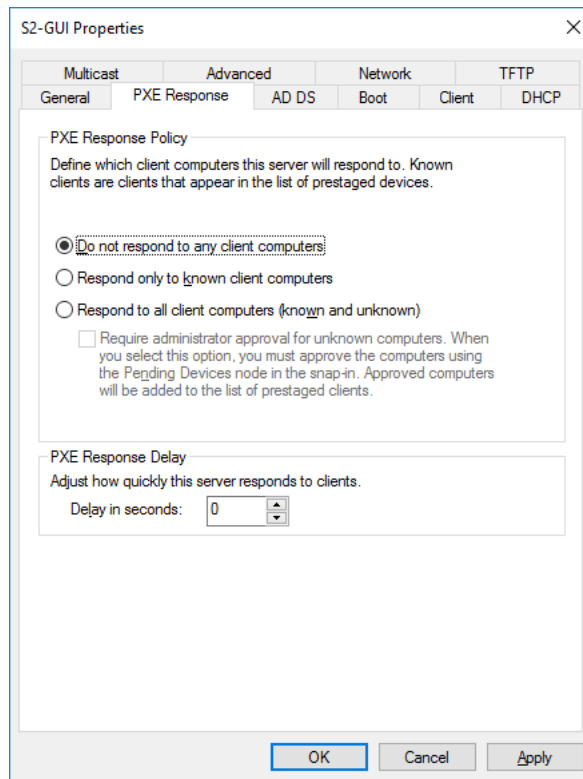


FIGURE 3-11 PXE Response settings

You use the PXE Response Delay setting when you have more than one WDS server in an environment. You can use this setting to ensure that clients receive transmissions from one WDS server over another, with the server configured with the lowest PXE response delay having priority over other WDS servers with higher delay settings.

Client Naming Policy

The Client Naming Policy enables you to configure how computers installed from WDS are named if you aren't using deployment options that perform the action. You can also use the settings on the AD DS tab, shown in Figure 3-12, to configure domain membership and organizational unit (OU) options for the computer account.

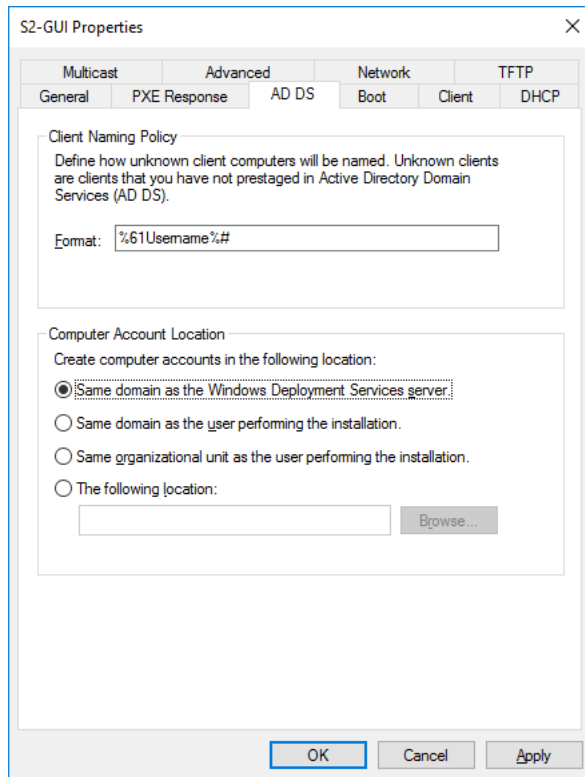


FIGURE 3-12 Client Naming Policy

WDS boot options

In the Boot options tab of the WDS server's Properties dialog box, shown in Figure 3-13, you can configure how clients that PXE boot interact with the WDS server. You can also configure a default boot image for each architecture supported by WDS. By default, once a client has connected to a WDS server, someone must press the F12 key to continue deploying the operating system. In environments in which you are performing a large number of simultaneous deployments, requiring this level of manual intervention might substantially delay the deployment.

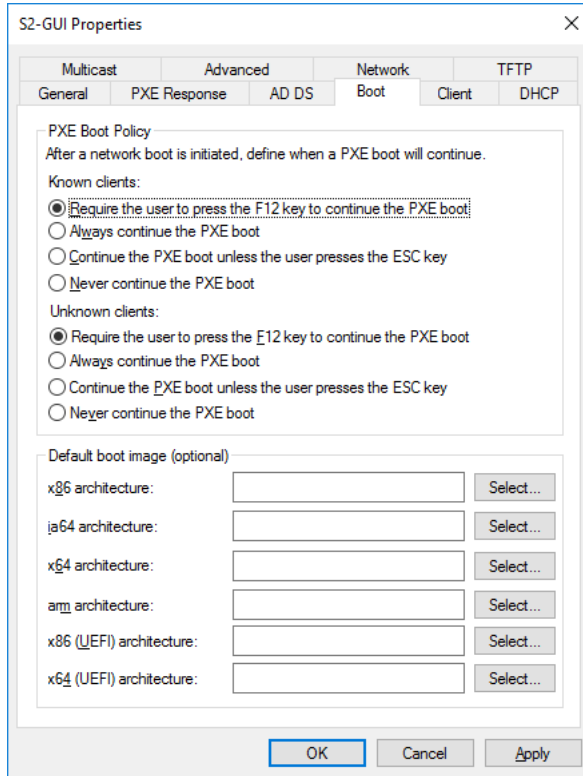


Figure 3-13 Boot options

Multicast options

The default settings of WDS have all computers that join the multicast transmission receiving the installation image at the same speed. If you frequently deploy operating systems, you are aware that sometimes there are one or two computers that have network adapters that slow transmission; transmissions that should take only 15 minutes now take half a day. You can configure the transfer settings on the Multicast tab, shown in Figure 3-14, so that clients are partitioned into separate sessions depending on how fast they can consume the multicast transmission. You still have those slow computers taking a long time to receive the image, but the other computers connected to the transmission can complete the deployment quicker.

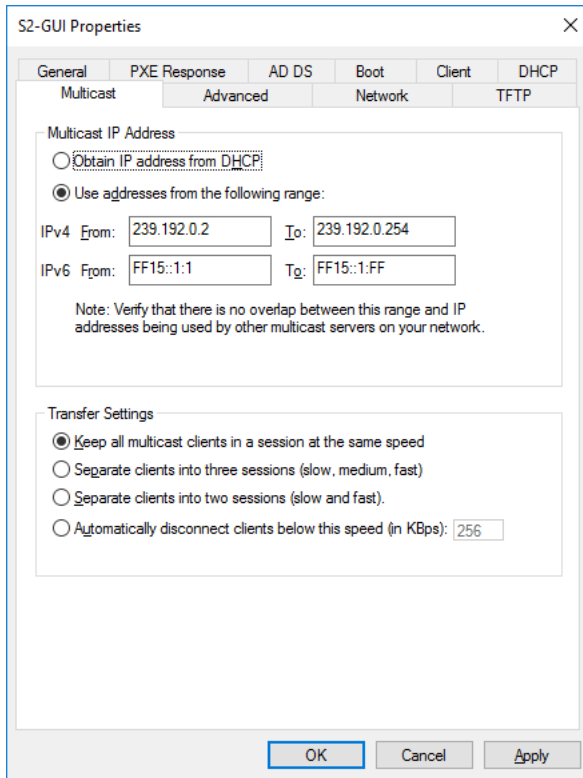


Figure 3-14 WDS Multicast tab

Other options

Although you are less likely to need them, you can configure other options on the following tabs:

- Advanced tab.** You can configure WDS to use a specific domain controller and global catalog (GC) server. You can also configure whether WDS is authorized in DHCP. DHCP authorization occurs automatically when you install the WDS role.
- Network tab.** You can specify a User Datagram Protocol (UDP) port policy to limit when UDP ports are used with transmissions. You can also configure a network profile to specify the speed of the network, minimizing the chance that WDS transmissions slow the network down.
- TFTP tab.** You can specify maximum block size and Trivial File Transfer Protocol (TFTP) window size.

Configuring transmissions

You use WDS transmissions to set WDS to transfer the operating system image to PXE clients. When configuring a WDS transmission, you need to decide what type of multicast transmission you are going to perform in the Multicast Type page of the Create Multicast Transmission Wizard, as shown in Figure 3-15.

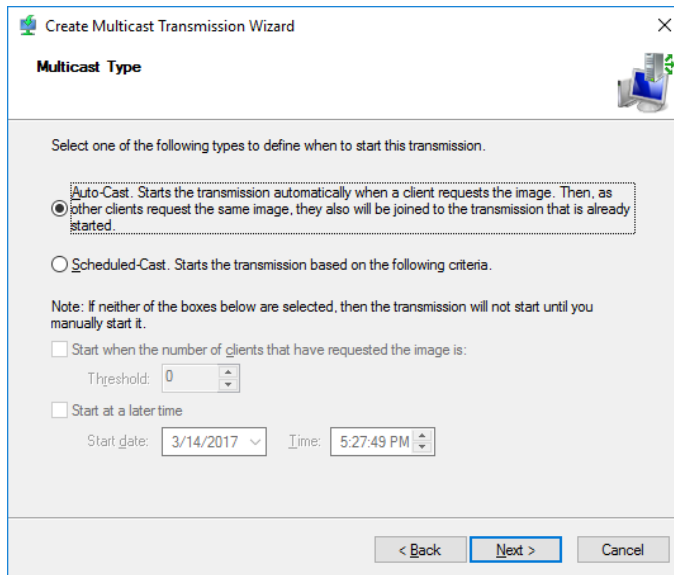


Figure 3-15 Multicast type

The difference between these options is as follows:

- **Auto-Cast.** A transmission starts when a client requests the image. If another client requests the same image, the client joins the existing transmission, caching data from the current transfer and then retrieving data that was transmitted before the client joined the transmission. This is the best option to use when you are performing one-off deployments.
- **Scheduled-Cast.** You choose either to start the transmission when a specified number of clients have joined, or you start the transmission at a particular date and time. Scheduled-Cast is the best option to use when you are deploying the same operating system image to a large number of computers.

To configure a WDS transmission, perform the following steps:

1. Open the Windows Deployment Services console, expand the WDS server from which you want to perform the deployment, and click Multicast Transmissions. In the Action menu, click Create Multicast Transmission.

2. Provide a name for the multicast transmission.
3. On the Image Selection page, specify which operating system image you want to deploy using the transmission.
4. On the Multicast Type page, specify whether you use Auto-Cast or Scheduled-Cast. If you choose Scheduled-Cast, select the number of clients or the transmission start time.

Driver groups and packages

You can stage device drivers on a WDS server by importing the device driver as a package. A driver package contains the extracted driver files. You can import the driver package into WDS by locating the driver's *.inf* file. When using the WDS console, you can either import individual driver packages or all the drivers in a set of folders.

In the WDS console, you can organize drivers into driver groups. A driver package can be a member of more than one group, and deleting a driver group does not delete the associated driver packages. You can use driver groups with filters to limit which driver packages are available to WDS clients.

Virtual Machine Manager

For most organizations, the majority of their server deployments involve virtual machines rather than deploying to bare metal physical hardware. While tools such as the Hyper-V console and WDS are adequate for smaller environments, if you need to deploy hundreds or thousands of virtual machines each year, you need a more comprehensive set of tools than those that are included with the Windows Server operating system.

System Center Virtual Machine Manager is one tool that you can use to manage your organization's entire virtualization infrastructure, from virtualization hosts, clusters, and VMs, to managing the entire networking and storage stack. In this section, you'll learn about VMM templates, storage, networking, and host groups.

Virtual machine templates

A Virtual Machine Manager VM template allows you to rapidly deploy virtual machines with a consistent set of settings. A VMM VM template is an XML object that is stored with a VMM library, and it includes one or more of the following components:

- **Guest Operating System Profile.** A guest operating system profile that includes operating system settings.
- **Hardware Profile.** A hardware profile that includes VM hardware settings.

- **Virtual Hard Disk.** This can be a blank hard disk or a virtual hard disk that hosts a specially prepared—sysprepped, in the case of Windows-based operating systems— version of an operating system.

You can create VM templates based on existing virtual machines deployed on a virtualization host managed by VMM, based on virtual hard disks stored in a VMM library, or by using an existing VM template.

VM templates have the following limitations:

- A VM template allows you to customize IP address settings, but you can only configure a static IP address for a specific VM from a pool when deploying that VM from the template.
- Application and SQL Server deployment are only used when you deploy a VM as part of a service.
- When creating a template from an existing VM, ensure that the VM is a member of a workgroup and is not joined to a domain.
- You should create a separate local administrator account on a VM before using it as the basis of a template. Using the built-in administrator account causes the sysprep operation to fail.

More Info

Virtual machine templates

You can learn more about virtual machine templates at <https://docs.microsoft.com/en-us/system-center/vmm/vm-template?view=sc-vmm-2019>.

VMM storage

VMM can use local and remote storage, with local storage being storage devices that are directly attached to the server and remote storage being storage available through a storage area network. VMM can use:

- **File storage.** VMM can use file shares that support the SMB 3.0 protocol. This protocol is supported by file shares on computers running Windows Server 2012 and later. SMB 3.0 is also supported by third-party vendors of network-attached storage (NAS) devices.
- **Block storage.** VMM can use block-level storage devices that host LUNs (Logical Unit Numbers) for storage using either the iSCSI, Serial Attached SCSI (SAS), or Fibre Channel protocols.

VMM supports automatically discovering local and remote storage. This includes automatic discovery of:

- Storage arrays
- Storage pools
- Storage volumes
- LUNs
- Disks
- Virtual disks

Using VMM, you can create new storage from storage capacity discovered by VMM and assign that storage to a Hyper-V virtualization host or host cluster. You can use VMM to provision storage to Hyper-V virtualization hosts or host clusters using the following methods:

- **From available capacity.** Allows you to create storage volumes or LUNs from an existing storage pool.
- **From writable snapshot of a virtual disk.** VMM supports creating storage from writable snapshots of existing virtual disks.
- **From a clone of a virtual disk.** You can provision storage by creating a copy of a virtual disk. This uses storage space less efficiently than creating storage from snapshots.
- **From SMB 3.0 file shares.** You can provision storage from SMB 3.0 file shares.

VMM supports the creation of a thin provisioned logical unit on a storage pool. This allows you to allocate a greater amount of capacity than is currently available in the pool, and it is only possible when:

- The storage array supports thin provisioning
- The storage administrator has enabled thin provisioning for the storage pool

VMM 2019 supports balancing of virtual disks across cluster-shared volumes to ensure that no single cluster shared volume is over-committed.

More Info

Storage in VMM

You can learn more about storage in VMM at <https://docs.microsoft.com/en-us/system-center/vmm/manage-storage?view=sc-vmm-2019>.

Inside OUT

Storage classifications

Storage classifications allow you to assign a metadata label to a type of storage. For example, you might name a classification used with a storage pool that consists of high-speed solid-state disks as Alpha, a classification used with Fibre Channel RAID 5 SAS storage as Beta, and iSCSI SATA RAID 5 as Gamma. The labels that you use should be appropriate to your environment.

VMM networking

A VMM logical network is a collection of network sites, VLAN information, and IP subnet information. A VMM deployment needs to have at least one logical network before you can use it to deploy VMs or services. When you add a Hyper-V based virtualization host to VMM, one of the following happens:

- If the physical adapter is associated with an existing logical network, it remains associated with that network once added to VMM.
- If the physical adapter is not already associated with a logical network, VMM creates a new logical network, associating it with the physical adapter's DNS suffix.

You can create logical networks with the following properties:

- **One Connected Network.** Choose this option when network sites that compose this network can route traffic to each other, and you can use this logical network as a single connected network. You have the additional option of allowing VM networks created on this logical network to use network virtualization.
- **VLAN-Based Independent Networks.** The sites in this logical network are independent networks. The network sites that compose this network can route traffic to each other, though this is not required.
- **Private VLAN (PVLAN) Networks.** Choose this option when you want network sites within the logical network to be isolated independent networks.

You create network sites after you have created a VMM logical network. You use network sites to associate IP subnets, VLANs, and PVLANS with a VMM logical network.

More Info

VMM logical network

You can learn more about VMM logical networks at <https://docs.microsoft.com/en-us/system-center/vmm/plan-network?view=sc-vmm-2019>.

Logical switches

VMM logical switches store network adapter configuration settings for use with VMM-managed virtualization hosts. You configure the properties of one or more virtualization host's network adapters by applying the logical switch configuration information.

You should perform the following tasks before creating a logical switch:

- Create logical networks and define network sites.
- Install the providers for any Hyper-V extensible virtual switch extensions.
- Create any required native port profiles for virtual adapters that you use to define port settings for the native Hyper-V virtual switch.

When you configure a VMM logical switch, you configure the following:

- Extensions
- Uplinks
- Virtual Ports

Extensions

You use logical switch extensions to configure how the logical switch interacts with network traffic. VMM includes the following switch extensions:

- **Monitoring.** Allows the logical switch to monitor but not modify network traffic.
- **Capturing.** Allows the logical switch to inspect but not modify network traffic.
- **Filtering.** Allows the logical switch to modify, defragment, or block packets.
- **Forwarding.** Allows the logical switch to alter the destination of network traffic based on the properties of that traffic.

Uplink port profiles

Uplink port profiles specify which set of logical networks should be associated with physical network adapters. In the event that there are multiple network adapters on a virtualization host,

an uplink port profile specifies whether and how those adapters should participate in teaming. Teaming allows network adapters to aggregate bandwidth and provide redundancy for network connections.

Virtual port profiles

You use port classifications to apply configurations based on functionality. The following port profiles are available:

- **SR-IOV.** Allows a virtual network adapter to use SR-IOV (Single Root Input Output Virtualization)
- **Host Management.** For network adapters used to manage the virtualization host using RDP, PowerShell, or another management technology
- **Network Load Balancing.** To be used with network adapters that participate in Microsoft Network Load Balancing
- **Guest Dynamic IP.** Used with network adapters that require guest dynamic IP addresses, such as those provided by DHCP
- **Live Migration Workload.** Used with network adapters that support VM live migration workloads between virtualization hosts
- **Medium Bandwidth.** Assign to network adapters that need to support medium-bandwidth workloads
- **Host Cluster Workload.** Assign to network adapters that are used to support host clusters
- **Low Bandwidth.** Assign to network adapters that need to support low-bandwidth workloads
- **High Bandwidth.** Assign to network adapters that are used to support high-bandwidth workloads
- **iSCSI Workload.** Assign to network adapters that are used to connect to SAN resources using the iSCSI protocol

More Info

Port profiles and logical switches

You can learn more about port profiles at <https://docs.microsoft.com/en-us/system-center/vmm/network-port-profile?view=sc-vmm-2019>.

Virtual machine networks

In VMM, virtual machines connect to a VMM logical network through a VMM virtual machine network. You connect a virtual machine's network adapter to the virtual machine network rather than the logical network. You can have VMM automatically create an associated virtual machine network when you create a logical network. If you have configured a logical network to support network virtualization, you can connect multiple VM networks to the logical network, and they will be isolated from each other. Also, you can configure virtual networks to support encryption.

You can use network virtualization to configure logical networks in such a manner that different VM tenants can utilize the same IP address space on the same virtualization host without collisions occurring. For example, tenant alpha and tenant beta use the 172.16.10.x address space when their workloads are hosted on the same virtualization host cluster. Even though tenant alpha and tenant beta have virtual machines that use the same IPv4 address, network virtualization ensures that conflicts do not occur.

When you configure network virtualization, each network adapter is assigned two IP addresses:

- **Customer IP address.** This IP address is the one used by the customer. The customer IP address is the address visible within the VM when you run a command such as *ipconfig* or *Get-NetIPConfiguration*.
- **Provider IP address.** This IP address is used by and is visible to VMM. It is not visible within the VM operating system.

MAC address pools

A MAC address pool gives you a pool of MAC addresses that can be assigned to virtual machine network adapters across a group of virtualization hosts. Without MAC address pools, virtual machines are assigned MAC addresses on a per-virtualization host basis. While unlikely, it is possible the same MAC address may be assigned by separate virtualization hosts in environments with a very large number of virtualization hosts. Using a central MAC address pool ensures that doesn't happen. When creating a MAC address pool, you specify a starting and an ending MAC address range.

More Info

MAC address pools

You can learn more about MAC address pools at <https://docs.microsoft.com/en-us/system-center/vmm/network-mac?view=sc-vmm-2019>.

Static IP address pools

An IP address pool is a collection of IP addresses that, through an IP subnet, is associated with a network site. VMM can assign IP addresses from the static IP address pool to virtual machines running Windows operating systems if those virtual machines use the logical network associated with the pool. Static IP address pools can contain default gateway, DNS server, and WINS server information. Static IP address pools aren't necessary because VMs can be assigned IP address information from DHCP servers running on the network.

More Info

IP address pools

You can learn more about IP address pools at <https://docs.microsoft.com/en-us/system-center/vmm/network-pool?view=sc-vmm-2019>.

Private VLANs

VLANs segment network traffic by adding tags to packets. A VLAN ID is a 12-bit number, allowing you to configure VLAN IDs between the numbers 1 and 4095. While this is more than adequate for the majority of on-premises deployments, large hosting providers often have more than 5,000 clients, so they must use an alternate method to segment network traffic. A PVLAN is an extension to VLANs that uses a secondary VLAN ID with the original VLAN ID to segment a VLAN into isolated sub networks.

You can implement VLANs and PVLANS in VMM by creating a Private VLAN logical network. Private VLAN logical networks allow you to specify the VLAN and/or PVLAN ID, as well as the IPv4 or IPv6 network.

Adding a WDS to VMM

In a scalable environment, you'll need to add additional Hyper-V host servers on a frequent basis as either a standalone server or as part of a failover cluster to increase your capacity. While it's possible to use another technology to deploy new Hyper-V host servers to bare metal, the advantage of integrating virtualization host deployment with VMM is that you can fully automate the process. The process works in the following general manner:

1. Discovery of the chassis occurs. This may be through providing the chassis network adapter's MAC address to VMM.
2. The chassis performs a PXE boot and locates the Windows Deployment Services (WDS) server that you have integrated with VMM as a managed server role. When you integrate WDS with VMM, the WDS server hosts a VMM provider that handles PXE traffic from the bare metal chassis started using the VMM provisioning tool.

3. The VMM provider on the WDS server queries the VMM server to verify that the bare metal chassis is an authorized target for managed virtualization host deployment. In the event that the bare metal chassis isn't authorized, WDS attempts to deploy another operating system to the chassis. If that isn't possible, PXE deployment fails.
4. If the bare metal chassis is authorized, a special Windows PE (Preinstallation Environment) image is transmitted to the bare metal chassis. This special Windows PE image includes a VMM agent that manages the operating system deployment.
5. Depending on how you configure it, the VMM agent in the Windows PE image can run scripts to update firmware on the bare metal chassis, configure RAID volumes, and prepare local storage.
6. A specially prepared virtual hard disk (in either *.vhdx* or *.vhd* format) containing the virtualization host operating system is copied to the bare metal chassis from a VMM library server.
7. The VMM agent in the Windows PE image configures the bare metal chassis to boot from the newly placed virtual hard disk.
8. The bare metal chassis boots into the virtual hard disk. If necessary, the newly deployed operating system can obtain additional drivers not included in the virtual hard disk from a VMM library server.
9. Post-deployment customization of the newly deployed operating system occurs. This includes setting a name for the new host and joining an Active Directory Domain Services domain.
10. The Hyper-V server role is deployed, and the newly deployed virtualization host is connected to VMM and placed in a host group.

The PXE server needs to provide the PXE service through Windows Deployment Services. When you add the VMM agent to an existing Windows Deployment Services server, VMM only manages the deployment process if the computer making the request is designated as a new virtualization host by VMM.

To integrate the WDS server with VMM to function as the VMM PXE server, you need to use an account on the VMM server that is a member of the local Administrators group on the WDS server. PXE servers need to be on the same subnet as the bare metal chassis to which they deploy the virtualization host operating system.

VMM host groups

Host groups allow you to simplify the management of virtualization hosts by allowing you to apply the same settings across multiple hosts. VMM includes the All Hosts group by default.

You can create additional host groups as required in a hierarchical structure. Child host groups inherit settings from the parent host group. However, if you move a child host group to a new host group, the child host group retains its original settings, except for any PRO configuration. When you configure changes to a parent host group, VMM provides a dialog box asking if you would like to apply the changed settings to child host groups.

You can assign network and storage to host groups. Host group networks are the networks that are assigned to the host group. These resources include IP address pools, load balances, logical networks, and MAC address pools. Host group storage allows you to allocate logical units or storage pools that are accessible to the VMM server for a specific host group.

More Info

VMM host groups

You can learn more about VMM host groups at <https://docs.microsoft.com/en-us/system-center/vmm/host-groups?view=sc-vmm-2019>.

VMM virtualization host requirements

To be able to configure a bare metal hardware chassis so that it can function as a VMM managed Hyper-V virtualization host, the hardware chassis needs to meet the following requirements:

- **X64 processor.** This needs to support hardware-assisted virtualization and hardware-enforced Data Execution Prevention (DEP). In some cases, it may be necessary to enable this support in BIOS.
- **PXE boot support.** The hardware chassis must be able to PXE boot from a PXE-enabled network adapter. The PXE-enabled network adapter must be configured as a boot device.
- **Out-of-band (OOB) management support.** System Center VMM can discover and manage the power states of hardware chassis that support BMC (Baseboard Management Controller). VMM supports the following protocols:
 - SMASH (Systems Management Architecture for Server Hardware) version 1 over WS-Management
 - DCMI (Datacenter Management Interface) version 1.0
 - IPMI (Microsoft Intelligent Platform Management Interface) version 1.5 or version 2.0



Index

A

- access rights, 597. *See also* file access
- access rules, DAC, 459–460
- AccessChk tool, 740
- Access-Denied Assistance, DAC, 292–293, 463–464
- AccessEnum tool, 744–745
- account security options, 586–587
- accounts
 - AD environment, 130–138
 - creating in containers, 587
 - rights assignments, 598
 - types, 130–138
- ACLs (access control lists), command-line tool, 730
- AD (Active Directory). *See also* Azure Active Directory
 - accounts, 130–138
 - authoritative restore, 149–151
 - consoles, 12
 - Container Service Accounts, 326
 - Domains And Trusts console, 117
 - editing objects, 746–748
 - Enterprise CA, 393
 - Enterprise Subordinate CA, 402–403
 - FRS to DFSR migration, 695–696
 - migration to forest, 696–698
 - Migration Tool, 697–698
 - module cmdlets, 152–155
 - overview, 109
 - Recycle Bin, 147–149
 - remote administration, 110
 - Sites And Services Console, 114–117
 - snapshots, 151–152
 - Standalone CAs, 403–406
 - upgrade and migration paths, 693–695
 - upgrading domain controllers, 693–695
 - Users And Computers console, 113–114
- AD CS (Active Directory Certificate Services).
 - See also* CAs (Certificate Authorities)
 - Certutil.exe* and *Certreq.exe*, 435–436
 - migration, 699–704
 - overview, 391
 - PowerShell cmdlets, 433–434
 - role services, 412
 - roles, 412
- AD DS structure, 125–130, 152–157
- AD Explorer, 746–749
- AD FS (Federation Services)
 - attribute stores, 438, 442
 - certificate relationship, 441–442
 - claim rules, 443–444
 - claims and claim rules, 438
 - claims provider, 439
 - claims provider trust, 440–441
 - components, 437
 - multifactor authentication, 449
 - overview, 437
 - PowerShell cmdlets, 450–453
 - relying party, 439–440
 - web application proxy servers, 445–447
 - WebApplicationProxy module, 453
 - Workplace Join, 447–449
- AD RMS. *See also* DAC (Dynamic Access Control)
 - administrators and super users, 469–470
 - certificates and licenses, 465–466
 - exclusion policies, 471–472
 - installing, 464–465

AD RMS (continued)

- PowerShell cmdlets, 473–474
- publishing domains, 469–470
- templates, 466–469, 471–472
- TPDs (Trusted Publishing Domains), 471
- TUDs (Trusted User Domains), 470–471
- ADAC (Active Directory Administrative Center), 110–113**
- ADCSAdministration PowerShell module cmdlets, 433–434**
- address resolution protocol cache, managing, 729
- ADDSDeployment module cmdlets, 157**
- ADInsight tool, 749**
- administrative permissions, IIS, 331. *See also* permissions
- admin-trusted attestation, shielded VMs, 631–633
- ADModify.Net tool, 553**
- ADMX file format, 145**
- ADSI Edit console, 12**
- advanced auditing, 615–617
- AGPM (Advanced Group Policy Management), 139–140**
- alerts, performance counter, 655
- alias records, 166
- AliasDefinitions role-capability file, 606**
- answer files, 57–59
- antimalware solution, 650. *See also* malware toolchains
- appcmd.exe utility, 312–313**
- application pools, IIS, 326–329
- applications, launching with ShellRunAs, 745
- application-specific backups, 665
- archived certificate, recovering, 431
- arp.exe command-line tool, 729**
- ASP.NET Core Runtime, 346**
- AssembliesToLoad role-capability file, 607**
- assume breach, 635
- at.exe command-line tool, 729**
- Attack Surface Analyzer, 638–639**
- attestation types, shielded VMs, 632
- attrib.exe command-line tool, 729**
- attribute stores, AD FS, 438, 442

- attributes, managing, 729

- audit policies, command-line tool, 729

- auditing and security, rights assignment, 599

- auditing policies, GPOs, 615–617

- auditpol.exe command-line tool, 617, 729**

authentication

- Azure AD Connect, 540

- IPsec connections, 622

- Kerberos V5, 622

- NTLMv2, 622

- policy silos, 589–590

- rights assignment, 598

- VPNs (virtual private networks), 482

- websites, 318–319

- authoritative restore, AD (Active Directory), 149–151**

- authorization rules, URLs, 323–324**

- automating tasks, 2**

- Autounattend.xml file, 57–58**

Azure

- Chef Infra Server, 85

- and Remote Desktop, 25

- Azure Active Directory. *See also* AD (Active Directory)**

- overview, 538–539

- password protection, 562–563

- self-service password reset, 560–561

Azure AD Connect

- connectivity requirements, 542

- deployment accounts, 543–544

- Directory Federation, 541

- Health tool, 554

- installing, 544–551

- non-routable domains, 551–553

- object filters, 557–559

- overview, 540–541

- pass-through authentication, 540

- passwords, 540

- server requirements, 541–544

- SQL Server requirements, 543

- synchronization, 555–559

- UPN suffixes, 551–553

- User sign-in, 546

Azure AD DS (Active Directory Domain Services), 563–564

Azure Arc, 572

Azure Backup, 666–670. *See also* backup;
Windows Server Backup

Azure Bastion, 533–534

Azure Cli, 346

Azure File Sync, 569–571

Azure Hybrid services, 6, 564–567, 681

Azure Iaas VMs

creating, 520–524

WAC (Windows Admin Center), 567–569

Azure Monitor, 661–662

Azure Network Adapter, 573

Azure Site Recovery, 572–573

Azure Update Management, 679–682.

See also updates

Azure VPN gateways, 531

B

backup. *See also* Azure Backup; Windows Server Backup

command-line tool, 733

and restore, 140–141

rights, 597

security, 663

using with WAC (Windows Admin Center), 5

bandwidth management, 207

bare metal chassis, 47, 68, 75–77

base images, containers, 345–347

batch job, rights assignment, 599

bcdboot.exe command-line tool, 729

bcdedit.exe command-line tool, 729

BitLocker, 2, 731–732

blocking writing files, 282

boot environment, command-line tool, 729

boot.wim file, 48

brace matching, PowerShell, 22

BranchCache, 299–302, 305–306

C

CA management

backup and recovery, 425–427

certificate requests, 424–425

key archiving and recovery, 427–431

overview, 422–424

CAL licenses, RDS, 514

CAPolicy.inf file, 432

CAs (Certificate Authorities). *See also* AD CS (Active Directory Certificate Services)

autoenrollment and renewal, 420–422

backup and recovery, 425–427

certificates, 391–393

command-line tools, 729

CRLs (certificate revocation lists), 406–412

customizing settings, 432

deployments, 394

Enterprise CAs, 393–403

hash algorithms, 399–400

hierarchies, 392

key archiving and recovery, 427–431

KRA key, 431

management, 422–424

PKIview, 392

private key cryptography, 399–400

renewing, 392

requests, 424–425

Standalone CAs, 403–406

templates, 413–420

types, 391–392

CAU (Cluster Aware Updating), clusters, 373–374

CCI (Configurable Code Integrity) policy, 642

Center for Internet Security, 596

central access policies, DAC, 461–462

central access rules, DAC, 459–460

certificate chains, viewing, 739–740

certificate relationship, AD FS, 441–442

Certificate Services, managing, 435–436

Certificates, using with WAC (Windows Admin Center), 5

Certification Authority console, 12

certreq.exe command-line tool, 436, 729

certutil.exe command-line tool, 435, 729

CFG (Control Flow Guard), 647

checkpoints, Hyper-V virtualization platform, 202–203

checkpoints, managing, 202–203

Chef Infra Server

agents, 94–95

cookbooks and recipes, 95

desired state, 46

vs. DSC, and Puppet, 103

servers, 85–88

ChefDK (Development Kit), 89–94

chkdsk.exe command-line tool, 729

chkntfs.exe command-line tool, 729

Chocolatey package manager, 11, 105–107

cipher.exe command-line tool, 729

claims and claim rules, AD FS, 438, 443–444. *See also* user and device claims

claims provider, AD FS, 439

claims provider trust, AD FS, 440–441, 444

Client Naming Policy, WDS, 64

clip.exe command-line tool, 729

cloud witness and clusters, 376–377

cluster networking, Hyper-V, 214–215

cluster quorum, Hyper-V, 213–214, 370–371

cluster storage, Hyper-V, 212

Cluster-Aware Updating console, 12

clusterng, future of, 370

clusters

CAU (Cluster Aware Updating), 373–374

host management, 387–388

MPIO (multipath I/O), 373

networks, 372–373

NLB operation modes, 386–387

Rolling Upgrades, 379–380

sets, 382

storage and shared volumes, 372

workgroups, 381

cmd.exe, using with containers, 347

CNAME records, 166

color coding, PowerShell, 21

command prompt, 36

command-line tools, 729–733. *See also* troubleshooting methodology

command-line output, redirecting, 729

compact.exe command-line tool, 729

comp.exe command-line tool, 729

Component Services console, 12

compression of files, command-line tool, 729

computer access rights, 597

computer accounts, 132–133, 587

Computer Management console, 12

computer name, viewing, 730

Connection Manager Administration Kit console, 12

connection security rules, WFAS, 623–627.

See also security

consoles, 11–17

container images, 353–354. *See also* images; OS images

containers. *See also* Docker engine; LCOW (Linux Containers on Windows)

applying updates, 356–357

and Chocolatey, 351

concepts, 337–339

creating accounts in, 587

creating images from, 351

and data, 339

Dockerfiles, 351–352

images, 353–354

isolation modes, 339–340

listing, 348–349

modifying running, 350

networking, 357–363

orchestration, 364–368

registries and images, 345–347

retrieving OS images, 344–345

service accounts, 355–356

starting, 347–350

using with WAC (Windows Admin Center), 5

context-sensitive help, PowerShell, 22

control panels, 37

Controlled Folder Access, 645–647

CPU utilization spikes, monitoring, 736

Credential Guard, 2, 640–642
 CRLs (certificate revocation lists), 406–412
cscript.exe command-line tool, 729
 CSP (Cryptographic Service Provider),
 465, 700–701
 CSVs (Cluster Shared Volumes), Hyper-V, 215–216

D

DAC (Dynamic Access Control). *See also* AD RMS

Access-Denied Assistance, 463–464
 central access policies, 461–462
 central access rules, 459–460
 group policy, 456
 overview, 455–456
 PowerShell cmdlets, 474
 resource properties, 457–459
 staging, 463
 user and device claims, 456–457

DANE (DNS-based Authentication of Named Entities), 172–173

data, backing up, 664

data collector sets, 653–654

Datacenter edition, 31–32, 687

date panel, 37

***date.exe* command-line tool,** 729

***dcgppofix.exe* command-line tool,** 730

DCs (domain controllers)

and Credential Guard, 642
 deployment, 118–120
 evaluation, 689
 global catalog servers, 121
 hardening, 582–583
 installation options, 120
 Server Core, 120–121
 as targets, 109
 upgrading, 693–695
 virtual domain controller cloning, 124
 virtualization platforms, 121

DDA (Discrete Device Assignment), 195–196, 512

debug programs, rights assignment, 598

debugging, PowerShell, 21

deduplication

enabling, 273
 PowerShell cmdlets, 266
 process, 260–263
 support, 204

default groups, 134–136

Defragment and Optimize Drives console, 12

deleted items, restoring, 119–120, 146–152

***Demon.json* file, Docker,** 342–344

deny access, rights assignment, 598

DEP (Data Execution Prevention), 647

dependencies, 338, 726–727

Desired State Configuration (DSC), 46, 57,
 81–85, 103

Desktop Experience installation options, 42

detached clusters, 216

device and user claims, configuring for DAC,
 456–457

device drivers

command-line tool, 730
 rights assignment, 599

Device Guard policy, 642

Devices, using with WAC (Windows Admin Center), 5

DFS (Distributed File System)

migration from FRS (File Replication Service),
 695–696
 namespace, 293–295
 PowerShell cmdlets, 306–308
 replication, 296–299
 witnesses, 370

DFS Management console, 12

DFSR (distributed file system replication), 730

***dfsrmig.exe* command-line tool,** 730

DHCP (Dynamic Host Configuration Protocol)

administration, 182–184
 console, 12
 failover, 181
 filtering, 179
 migration, 705–709
 multicast scopes, 180
 name protection, 180–181

DHCP (continued)

- reservations, 178–179
- scopes, 177
- server and scope options, 178
- split scopes, 180
- superscopes, 179–180
- using with WAC (Windows Admin Center), 5

diagnostic hypothesis, 726**digital signature details, viewing, 739–740****DirectAccess**

- configuring, 493–496
- overview, 489–490
- server, 490–492
- topologies, 490

directories, rights assignment, 600. See also mounted directories**directory browsing, website management, 321–322****directory service data, rights assignment, 600****directory structure, command-line tool, 732****DISA (Defense Information Systems Agency), 596****disk checking, command-line tool, 729****Disk Cleanup console, 12*****diskshadow.exe* command-line tool, 730****DISM (Deployment Image Servicing and Management) tool, 49–50, 52****DNS (Domain Name Service)**

- cache locking, 170–171
- conditional forwarders, 163–164
- console, 12
- delegated administration, 174
- event logs, 169–170
- forwarders, 163
- GlobalNames zones, 164–165
- managing with PowerShell, 174–176
- migration, 704–705
- netmask ordering, 171
- PNRP (Peer Name Resolution Protocol), 165–166
- policies, 173
- recursion, 171
- resource records, 166–167
- response rate limiting, 171–172
- reverse lookup zones, 162

- scavenging, 167–168
- socket pool, 170
- stub zones, 164
- using with WAC (Windows Admin Center), 5
- zone aging, 167–168
- zone delegation, 162–163
- zone types, 159

DNS information, command-line tool, 731**DNS servers, command-line tool, 730*****dnscmd* command-line tool, 170*****dnscmd.exe* command-line tool, 730****DNSSEC (Domain Name System Security Extensions), 168–169****Docker engine. See also containers**

- Demon.json* file, 342–344
- Experimental mode, 363
- installing, 341–342
- Linux containers on Windows, 363–364
- overview, 340
- registries and images, 345–347
- retrieving container OS image, 344–345

docker ps* command, 360*Docker Swarm orchestration, 365–368****Dockerfiles, using, 351–352****docking station, rights assignment, 599****domain controller cloning, Hyper-V virtualization platform, 223****domain dominance, 109****domain local groups, 133****domain name filtering and IP addresses, 322–323****domain names, repairing dependencies, 730****domain naming master, 129****domains, AD DS structure, 125–126****downloading files, 44****driver verification, command-line tool, 732*****driverquery.exe* command-line tool, 730****drivers and updates**

- adding to images, 53–54
- command-line tool, 731

DSC (Desired State Configuration), 46, 57, 81–85, 103**DSRM (Directory Services Restore Mode), 119–120**

dynamic memory, Hyper-V virtualization platform, 191–192
dynamic virtual machine queue, 207

E

editions of Windows Server, upgrading, 31–33, 687, 689
EMET (Enhanced Mitigation Experience Toolkit), 647
encryption
command-line tool, 729
IPsec, 622
encryption-supported VMs, 633. *See also* VMs (Virtual Machines)
Enhanced Session Mode, Hyper-V virtualization platform, 195
Enterprise CA, 393
Enterprise Root CA, 394–402
Enterprise Subordinate CA, 402–403
EnvironmentVariables role-capability file, 607
error response, modifying in IIS, 319
ESAE (Enhanced Security Administrative Environment), 127, 594–596. *See also* security
Essentials edition, 31, 687
evaluation version, converting to licensed version, 688–689
event logs
DNS, 169–170
event customization, 730
PowerShell cmdlets, 683–684
and publishers, 733
system activity, 741–744
event subscriptions, command-line tool, 733
Event Trace Logs, command-line tool, 732
Event Trace Sessions, command-line tool, 731
Event Viewer, 12, 655–659
eventcreate.exe command-line tool, 730
events, using with WAC (Windows Admin Center), 5
exclusion policies, AD RMS, 471–472
Exploit Protection, 647–649

F

Failover Cluster Manager console, 12
failover clustering
CAU (Cluster Aware Updating), 373–374
cloud witness, 376–377
cluster quorum modes, 370–371
cluster sets, 382
Hyper-V, 212–217
MPIO (multipath I/O), 373
multisite clusters, 375–376
networks, 372–373
NLB (Network Load Balancing), 385–389
overview, 369–370
PowerShell cmdlets, 383–385
preference settings, 374–375
rolling upgrades, 379–380
shared volumes, 372
storage spaces, 372
VMs (Virtual Machines), 377–379
workgroup clusters, 381
Fax Service Manager console, 12
features and roles, adding, 45–46, 54–56
Federation Server, 437
file access
recovering, 732
speeding up, 299–302
file and storage servers. *See also* file and storage servers
Storage Migration Service, 710–718
WSMT (Windows Server Migration Tools), 718–722
File Explorer, shared folder permissions, 275–276
file management, command-line tool, 729
file screens, FSRM, 282–286
File Server Resource Manager console, 13
file servers
BranchCache, 299–302
BranchCache cmdlets, 305–306
cleaning up, 292
DFS (Distributed File System), 293–299
DFS cmdlets, 306–308
FSRM cmdlets, 303–305
overview, 273

file servers (continued)

- protecting from ransomware, 645
- Shared Folder cmdlets, 302–303
- shared folder permissions, 274–279
- Storage Migration Service, 710–718
- workgroup clusters, 381
- WSMT (Windows Server Migration Tools), 718–722

file systems command-line tool, 729**file version number, viewing, 739–740****files. See also *Openfiles.exe* command-line tool;****protected system files; system files**

- auditing, 616–617
- comparing, 729
- compression, 729
- downloading, 44
- locating, 733
- rights assignment, 600
- updating, 673–674
- using with WAC (Windows Admin Center), 5

find.exe* command-line tool, 730**findstr.exe* command-line tool, 730****firewall**

- profiles, 619–620
- using with WAC (Windows Admin Center), 683–683

firmware environment values, rights assignment, 599**folder level quotas, FSRM, 280–282****folders**

- access control, 645–647
- auditing, 616–617
- sharing, 258–259, 274–279

force shutdown, rights assignment, 598**forests**

- AD DS structure, 126–127
- migration to, 696–698
- policy in, 142

format.exe* command-line tool, 730**FormatsToProcess* role-capability file, 607****FRS (File Replication Service), to DFS (Distributed File System) migration, 695–696****FSMO (Flexible Single Master Operations), 128–130****FSRM (File Server Resource Manager)**

- Access-Denied Assistance, 292–293
- file classification, 288–290
- file management tasks, 290–292
- file screens, 282–286
- folder level quotas, 280–282
- PowerShell cmdlets, 303–305
- storage reports, 286–287

fsutil.exe* command-line tool, 730*FTP protocol, managing, 332–334*****FunctionDefinitions* role-capability file, 606****G****garbage collection, 262****Generation 2 VMs, Hyper-V virtualization platform, 194–195****Get-Credential command, PowerShell, 20*****getmac.exe* command-line tool, 730****global catalog servers, 121****global groups, 133****global objects, rights assignment, 598****Global Resource Property list, DAC, 458****gMSA (group-managed service account), 137–138, 355–356, 601–603*****gpfixup.exe* command-line tool, 730****GPOs (Group Policy Objects)**

- AD DS structure, 127–128
- audit policies, 615
- command-line tools, 730
- comparing, 636
- DAC (Dynamic Access Control), 456
- management, 139–141
- preferences, 143
- RDS (Remote Desktop Services), 507–509

gpresult.exe* command-line tool, 730**gpupdate.exe* command-line tool, 730****group accounts, 133–136****group policy**

- administrative templates, 145–146
- management, 139–141
- policy processing, 141–142
- preferences, 143–145

Group Policy Management console, 13
guarded fabric, shielded VMs, 631–633

H

hardening, process, 581

hardening Active Directory

- account security option, 586–587
- authentication policies silos, 589–590
- block server operations, 592
- disable NTLM, 591
- domain controllers, 582–583
- ESAE (Enhanced Security Administrative Environment), 594–596
- KRBTGT account password, 593–594
- least privilege, 583–584
- LSA (Local Security Authority) protection, 592–593
- password policies, 585–586
- protected accounts, 588–589
- RBAC (Role-Based Access Control), 584
- scheduling tasks, 592

hardening Windows Server

- advanced auditing, 615–617
- JEA (Just Enough Administration), 603–609, 613
- LAPS (Local Administrator Password Solution), 613–615
- PAM (Privileged Access Management), 609–613
- service accounts, 600–603
- user rights, 596–600

hash algorithms, CAs (Certificate Authorities), 399–400

HGS (Host Guardian Service), 631

host records, 166

***hostname.exe* command-line tool, 730**

HVC for Linux, Hyper-V virtualization platform, 198

Hyper-V Manager console, 13

Hyper-V virtualization platform

- checkpoints, 202–203
- and containers, 340
- copying VMs, 221–222
- DDA (Discrete Device Assignment), 195–196
- domain controller cloning, 223

- dynamic memory, 191–192
 - Enhanced Session Mode, 195
 - exporting VMs, 221–222
 - failover clusters, 212–217
 - Generation 2 VMs, 194–195
 - guest clusters, 217–219
 - guest integration services, 193–194
 - host validation, 631
 - HVC for Linux, 198
 - importing VMs, 221–222
 - live migration, 219–221
 - nested virtualization, 197–198
 - network isolation, 209
 - optimizing network performance, 206–208
 - PowerShell cmdlets, 224–227
 - PowerShell Direct, 198
 - private switches, 206
 - replica, 209–212
 - resource metering, 193
 - shielded virtual machines, 223
 - smart paging, 192–193
 - storage migration, 221
 - storage optimization, 204–205
 - Storage QoS (Quality of Service), 204
 - V VHD Sets, 219
 - Virtual Fibre Channel adapters, 203
 - virtual hard disks, 199–202
 - virtual machine network adapters, 206
 - virtual switches, 205–206
 - VM drain on shutdown, 222
 - VM MAC addresses, 208
 - VM network adapters, 206
 - workgroup clusters, 381
- hypothetical solutions, ranking, 727–728**
- laas (Azure Infrastructure as a Service) VMs.**
See also VMs (Virtual Machines)
- administration, 532–538
 - Azure Bastion, 533–534
 - backup, 536–537
 - creating from WAC, 567–569
 - encryption, 537–538
 - networking, 524–531

IaaS (continued)

- NSGs (Network Security Groups), 530–531
- overview, 519–524
- ICMP (Internet Control Message Protocol), 621, 731
- IDE (Integrated Development Environment), 23
- idempotency, 80
- IIS (Internet Information Services). *See also* website management
 - administrative permissions, 331
 - application pools, 326–329
 - container operating system, 346
 - FTP management, 332–334
 - Management console, 332–334
 - missing items, 310
 - overview, 309–310
 - PowerShell cmdlets, 334–336
 - test certificates, 312
 - users and delegation, 329–331
- IKEv2 (Internet Key Exchange version 2), VPNs, 479–480
- images. *See also* container images; OS images
 - benefits, 48
 - build and capture, 56–57
 - committing, 56
 - configuring WDS, 62–66
 - creating from containers, 351
 - drivers and updates, 53–54
 - listing, 349
 - managing with WDS, 62
 - modifying, 49–50
 - mounting, 50–53
 - roles and features, 54–55
 - servicing, 50
- infrastructure configuration as code, 79–80
- Infrastructure Developer, 80
- infrastructure master, 130
- in-place upgrade, 686
- Insider Preview builds, 34–35
- installation options, 35–36
- Installed Apps, using with WAC (Windows Admin Center), 5

- install.wim* file, 44, 48
- integrity scrubbing, 262
- IntelliSense, PowerShell, 21
- Intl.cpl, 37
- IoT Core base image, 346
- IP addresses. *See also* NAT (Network Address Translation)
 - and domain name filtering, 322–323
 - IaaS VMs, 527–530
- IPAM (IP Address Management), 185–190
- ipconfig.exe* command-line tool, 730
- IPsec, configuring for WFAS, 621–622
- IPv6
 - DHCP, 178
 - PNRP (Peer Name Resolution Protocol), 165–166
- iSCSI
 - PowerShell cmdlets, 266–267
 - and storage devices, 252–255, 266–267
- iSCSI Initiator consoles, 13, 37
- iSNS (Internet Storage Name Service) server, 256–257
- isolation modes, containers, 339–340

J

- JEA (Just Enough Administration), 26, 603–609, 613
- JIT (Just In Time). *See also* VMs (Virtual Machines)
 - Administration, 609–613
 - VM Access, 534–536
- jump servers, using with PAW, 3

K

- Kerberos protocol, command-line tool, 730
- Kerberos V5 authentication, 622
- kernel transaction manager utility, 731
- klist.exe* command-line tool, 730
- KPS (Key Protection Service), 631
- KRA key, CAs (Certificate Authorities), 431
- KRBtgt account password, 593–594
- ksetup.exe* command-line tool, 730
- ktutil.exe* command-line tool, 731
- ktpass.exe* command-line tool, 731
- Kubernetes orchestration, 365

L

L2 (Layer 2) Bridge networks, 362
 L2TP/IPsec protocols, VPNs, 481
 LAN routing, 487
 languages, updating, 672
 LAPS (Local Administrator Password Solution), 613–615. *See also* passwords
lcacls.exe command-line tool, 730
 LCM (Local Configuration Manager), DSC, 83
 LCOW (Linux Containers on Windows), 346, 363, 575, 578. *See also* containers
 LDAP traffic, monitoring, 749
 least privilege, 583–584. *See also* privileged access
 licensed version, converting to, 688–689
 licensing
 laas VMs, 519
 RDS (Remote Desktop Services), 513–515
 Linux containers on Windows, 363–364
 Linux distro selection, Chef and Puppet, 96–97
 Linux on Windows Server. *See* WSL (Windows Subsystem for Linux)
 Local Security Policy console, 13
 Local Service account, 136
 Local System account, 136
 Local Users and Groups, using with WAC (Windows Admin Center), 5
 local vs. remote administration, 1
locctr.exe command-line tool, 731
 lock pages in memory rights assignment, 599
logman.exe command-line tool, 731
logoff.exe command-line tool, 731
 logon rights, 586, 597–599
 LogonSessions tool, 746
 LSA (Local Security Authority) protection, 592–593
 LTSC (Long Term Servicing Channel), 6, 33

M

MAC addresses
 command-line tool, 730
 enabling spoofing, 361
 VMs, 208

malware toolchains, 737. *See also* antimalware solution
manage-bde.exe command-line tool, 731
 MD hash algorithms, CAs, 399–400
 Message Analyzer, 660
 Microsoft Update Catalog, 49
 migration. *See also* upgrade and migration paths
 AD CS (Active Directory Certificate Services), 699–704
 DHCP, 705–709
 DNS, 704–705
 to forest, 696–698
 FRS to DFSR, 695–696
 vs. upgrade, 685
 Migration Tool, Active Directory, 697–698
 MIM (Microsoft Identity Manager), 610–611
 mirroring and storage spaces, 234
mklink.exe command-line tool, 731
ModulesToImport role-capability file, 606
 MOF file, DSC configuration script, 82–84
 monitoring and maintenance, PowerShell cmdlets, 683–684
 monitoring tool, Process Monitor, 735–736
 mounted directories, command-line tool, 732.
 See also directories
 mounting images, 50–53
mountvol.exe command-line tool, 731
 MPIO (multipath I/O), clusters, 373
msiexec.exe command-line tool, 731
 MSInfo32.exe, 37
 multicast options, WDS, 65–66
 multifactor authentication, AD FS, 449–450
 MX (mail exchanger) records, 166–167

N

name of computer, viewing, 730
 Nano Server, 44, 345
 NAT (Network Address Translation), 359–360, 487–488. *See also* IP addresses
nbstat.exe command-line tool, 731
 nested virtualization, Hyper-V virtualization platform, 197–198

.NET Framework 3.5, 56
Net print command-line tool, 731
 NetBIOS over TCP/IP command-line tool, 731. *See also* TCP/IP (Transmission Control Protocol/Internet Protocol)
netcfg.exe command-line tool, 731
netsh.exe command-line tool, 731
netstat.exe command-line tool, 731
 network configuration, command-line tool, 731
 network isolation, Hyper-V virtualization platform, 209
 Network Load Balancing Manager console, 13
 network monitoring, 659–660
 network performance, optimizing, 206–208
 Network Policy Server console, 13
 Network Service account, 136
 Network tool, using with WAC (Windows Admin Center), 5
 networking IaaS VMs, 524–531
 NFS (Network File System), 259–260, 267–268
 NIC teaming, VMs, 208
 NLB (Network Load Balancing), 385–389
nlbmgr.exe command-line tool, 731
 NLS (Network Location Server), 492
 Notepad, 37
 NSGs (Network Security Groups), IaaS VMs, 530–531
nslookup.exe command-line tool, 726, 731
 NTLM (NT Lan Manager), disabling, 591
 NTLMv2 authentication, 622

O

object label, rights assignment, 599
 ODBC Data Sources consoles, 13
 Offline Root CAs, 406
 Online Responder Management console, 13
 OOBE (Out-of-Box Experience), 57
openfiles.exe command-line tool, 731.
See also files
 OpenSSH on Windows Server, 29
 operating system, rights assignment, 597
 orchestration of containers, 364–368
 OS container image, retrieving, 344–345

OS images, keeping, 327. *See also* images
 OS Rolling Upgrade, clusters, 380
 OU (organizational unit) structure, 127–128, 132–133
 overlay networks, creating, 362, 367
 Overview tool, using with WAC (Windows Admin Center), 5

P

package-management utilities, 103–107
 pagefile, rights assignment, 597
 PAM (Privileged Access Management), 609–613
 parity data, storage, 234
 passwords. *See also* LAPS (Local Administrator Password Solution)
 Azure Active Directory, 562–563
 KRBTGT account, 593–594
 policies, 585–586
 resetting, 585
 RODC replication, 122–123
 security options, 586
pathping.exe command-line tool, 731
 paths, associating with volume letters, 732
 paths, command-line tools, 732
 PAW (Privileged Access Workstations), 2–3
 PDC emulator, 129
 PDK file, 634
 performance counters, 655, 731
 Performance logs, command-line tool, 731
 Performance Monitor console, 13
 permissions. *See also* administrative permissions
 AccessEnum tool, 744–745
 CA autoenrollment, 420
 shared folders, 274
 staging, 463
 persistent memory, 229
ping.exe utility, 731, 750
 PKIview, CAs (Certificate Authorities), 392
pnputil.exe command-line tool, 731
 PNRP (Peer Name Resolution Protocol), 165–166
pnunattend.exe command-line tool, 731
 Policy Analyzer tool, 636–638
 policy processing, 141–142

port rules, NLB, 388**PowerShell**

- DHCP management, 182–184
- direct connection, 24–25
- and DISM (Deployment Image Servicing and Management) tool, 52
- DNS management, 174–176
- documentation, 17–18
- features, 17
- Gallery, 19, 104–105
- Get-Credential command, 20
- help commands, 18
- IPAM management, 188–190
- ISE (Integrated Scripting Environment), 21–24
- modules, 18
- remote tabs, 22–23
- remoting, 19–21
- snippets, 23–24
- storage-related cmdlets, 266–271
- using with WAC (Windows Admin Center), 5, 10
- wget* command, 44

PowerShell cmdlets

- AD (Active Directory) module, 152–155
- AD Deployment module, 157
- AD FS, 450–453
- AD RMS, 473–474
- ADCSAdministration, 433–434
- BranchCache, 305–306
- container images, 346
- DAC (Dynamic Access Control), 474
- deduplication module, 266
- DFS (Distributed File System), 306–308
- DHCP, 182–184
- DNS, 174–176
- Event Logs, 683–684
- event logs, 683–684
- failover clustering, 383–385
- FSRM (File Server Resource Manager), 303–305
- vs. functions and aliases, 605
- Group Policy module, 156
- Hyper-V virtualization platform, 224–227
- IIS (Internet Information Services), 334–335
- IPAM, 188–190

- iSCSI module, 266
- iSCSI Target module, 267
- monitoring and maintenance, 683–684
- NFS module, 267
- NLB (Network Load Balancing), 389
- Remote Access, 224–227, 496–498, 515–517
- shared folder, 302–303
- Storage module, 268
- Storage Replica, 271
- web administration, 335–336
- Web Application Proxy, 453
- Windows Server Backup, 683–684
- WSUS (Windows Server Update Services), 684

PowerShell Direct, Hyper-V virtualization platform, 198**PowerShell session**

- entering, 37
- initiating remotely, 532–533

PowerShell.exe*, 347*PPTP VPN protocol, 481–482****print jobs and queues, command-line tools, 731****Print Management console, 13****printer drivers, command-line tool, 731****printer queues, command-line tool, 732****printers, command-line tool, 732****privileges. *See also* least privilege**

- delegating, 584–585
- securing, 596

prndrvr.exe* command-line tool, 731**prnjobs.exe* command-line tool, 731*****prnmngr.exe* command-line tool, 732*****prnqctl.exe* command-line tool, 732****ProcDump tool, 736****Process Explorer tool, 734–735****process level token, rights assignment, 600****Process Monitor tool, 735–736****process working set, rights assignment, 599****processes**

- command-line tools, 732
- rights assignment, 599
- using with WAC (Windows Admin Center), 5

Production Checkpoints feature, 121**products, updating, 672**

programs, managing and executing remotely, 733
 protected accounts, 588–589
 protected system files, command-line tool, 732.

See also files; system files

provisioning data file, 634

PsPing tool, 750

.psrc extension, 604–605

PsTools Suite, 737–738

PTR (pointer) records, 167

pubprn.exe command-line tool, 732

Puppet environment, 96–103

PXE (Pre-boot Execution Environment), 60, 63

R

RAC (rights account certificate), 466

RAMMap tool, 751–753

ransomware, protecting file servers from, 645

RBAC (Role-Based Access Control), 584–585

RD (Remote Desktop) Gateway, 475–479

RD (Remote Desktop) Session Host

Group Policy configuration, 507–509

overview, 503–504

personal session desktops, 506

RemoteApp, 506–507

session collections, 504–506

RD (Remote Desktop) Virtualization Host, 509–512

RD (Remote Desktop) Web Access, 513

RDS (Remote Desktop Services)

CAL licenses, 514

Connection Broker, 502

deployment, 499–501

deployment properties, 502–503

licensing, 513–515

PowerShell cmdlets, 515–517

Session Host, 503–509, 731

Virtualization Host, 509–512

recover.exe command-line tool, 732

Recovery Vault, Azure Backup, 668. *See also* Windows Server Backup

Recycle Bin, AD (Active Directory), 147–149

redeployment, 724–725

ReFS (Resilient File System), 264–265

Regedit.exe/Regedt32.exe, 37

reg.exe command-line tool, 732

Regional Settings control panel, 37

Registry, using with WAC (Windows Admin Center), 5

registry entries, command-line tool, 732

regsvr32.exe command-line tool, 732

relying party, AD FS, 439–440

relying party trust, AD FS, 439, 443

Remote Access Management console, 13.

See also routing and remote access

Remote Access PowerShell cmdlets, 224–227

remote administration, 1

Remote Desktop, 1–2, 5, 13, 25–27

Remote FX, 196

RemoteApp, 506–507

RemoteFX, 512

repair-bde.exe command-line tool, 732

replication, DFS, 296–299

request filters, website management, 324–326

reset password right, delegating, 585

resource metering, Hyper-V virtualization platform, 193

Resource Monitor, 13, 659

Resource Properties, configuring for DAC, 457–459

resource records, DNS, 166–167

restore files and directories, rights assignment, 600

restoring

from Azure Backup, 669–670

from backups, 665–666

deleted items, 119–120, 146–152

to locations, 666

revoking certificates, 408–410

RID (relative identifier) master, 130

RODC (Read Only Domain Controllers), 121–124

role-capability files, JEA, 604–607

RoleDefinitions session configuration file, 607

roles and features

adding, 45–46

adding to images, 54–56

- upgrading, 687–688
- using with WAC (Windows Admin Center), 5
- role-specific backups, 665
- Rolling Upgrades, clusters, 379–380. *See also* upgrade and migration paths
- root certificates, deploying, 405
- routing and remote access, 493–496. *See also* Remote Access Management console; VPNs (virtual private networks)
 - DirectAccess, 489–496
 - LAN routing, 487
 - NAT (Network Address Translation), 487–488
 - PowerShell cmdlets, 496–498
 - RD (Remote Desktop) Gateway, 475–479
- Routing and Remote Access console, 13
- RSAT (Remote Server Administration Tools) tools, 6, 11–17, 61
- RunAsVirtualAccount* session configuration file, 608
- RunAsVirtualAccountGroups* session configuration file, 608

S

- S2D, Storage Spaces Direct, 240–246
- SAC (Semi Annual Channel), 33–34
- sandbox, using with containers, 338
- scheduled tasks
 - blocking, 592
 - command-line tool, 729, 732
 - using with WAC (Windows Admin Center), 729–723
- scheduling priority, rights assignment, 599
- schema master, 129
- schtasks.exe* command-line tool, 732
- scripts, command-line tool, 729
- ScriptsToProcess* role-capability file, 606
- SCT (Security Compliance Toolkit)
 - Attack Surface Analyzer, 638–639
 - Credential Guard, 640–642
 - Policy Analyzer tool, 636–638
- searching files, 730, 733
- secedit.exe* command-line tool, 732

- secrets, isolating, 640–642
- security. *See also* connection security rules; ESAE (Enhanced Security Administrative Environment)
 - of backups, 663
 - connection security rules, 623
 - Controlled Folder Access, 645–647
 - Exploit Protection, 647–649
 - virtualization-based, 644–645
- security audits, rights assignment, 598
- security classifications, updating, 672
- security configuration, command-line tool, 732
- security options, accounts, 586–587
- security roles, WSUS, 674–675
- security settings, Exploit Protection, 647–649
- security vulnerabilities, locating, 638–639
- server configuration, command-line tool, 732
- Server Core
 - App Compatibility Features on Demand, 42–43
 - base image, 346
 - containers, 338
 - DCs (domain controllers), 120–121
 - deployment, 43–44
 - interface, 36–37
 - and migration, 691
 - overview, 34–35
 - roles, 37–42
- Server for NFS (Network File System), 259–260
- Server Manager console, 14–17, 277–279
- server operators, blocking from scheduling tasks, 592
- Server with Desktop Experience, 44–45
- servermanagercmd.exe* command-line tool, 732
- service accounts
 - containers, 355–356
 - hardening, 600–603
 - types, 136
- service dependencies, 726–727
- Service Principal Name, command-line tool, 731
- Services, using with WAC (Windows Admin Center), 5
- Services console, 13

Services for NFS (Network File System) console, 13
 servicing branches, 33–35
 session activity, viewing, 746
 session-configuration files, JEA, 607–608
SessionType configuration file, 607
sfc.exe command-line tool, 732
 SHA hash algorithm, CAs, 399–400
 shared folder cmdlets, 302–303
 shared objects, rights assignment, 598
 sharing folders, 258–259, 274–279
 ShellRunAs tool, 745
 shielded VMs. *See also* VMs (Virtual Machines)
 vs. encryption-supported VMs, 633
 guarded fabric, 631–634
 Hyper-V virtualization platform, 223
 overview, 628–630
 shielding data file, 13, 634
showmount.exe command-line tool, 732
 shutdown, rights assignment, 598, 600
 SigCheck tool, 739–740
 signed-on user identity, command-line tool, 733
 sites. *See* website management; websites
 SLC (server licensor certificate), 465–466
 smart card security option, 587
 smart paging, Hyper-V virtualization platform,
 192–193
 SmartScreen, Windows Defender, 651
 SMB (Server Message Block) 3.1.1, 251–252
 snapshots, AD (Active Directory), 151–152
 snippets, PowerShell, 23–24
 SoFS (Scale-Out File Server), 258–259
 solutions, applying, 728
 SQL Server
 base image, 346
 workgroup clusters, 381
 SSD (Storage Spaces Direct), 240–246
 SSDs (solid-state disks), 204
 SSH client and server, 27–29
 SSTP VPN protocol, 481
 staging, DAC, 463
 Standalone CAs, 403–406
 Standard edition, 31–32, 687

storage
 adding to storage pools, 230–233
 using with WAC (Windows Admin Center), 5
 storage devices, iSCSI, 252–255
 storage migration, Hyper-V virtualization
 platform, 221
 Storage Migration Service, 5, 710–718. *See also* file
 and storage servers
 Storage module, PowerShell cmdlets, 268–270
 storage optimization, Hyper-V virtualization
 platform, 204–205
 storage pools
 features, 229–233
 thin provisioning and trim, 237–239
Storage QoS (Quality of Service), 204, 263–264
Storage Replica
 configuration replication, 249–251
 configurations, 248–249
 features, 247–248
 PowerShell cmdlets, 271
 using with WAC (Windows Admin Center), 5
Storage Reports, FSRM, 286–287
 storage servers, WSMT (Windows Server
 Migration Tools), 718–722
 storage spaces
 resiliency, 234–235
 and storage pools, 229
 tiering, 235–236
 virtual disks, 239–240
Storage Spaces Direct, 240–241
 storage tiering, 204–205
 storage-related PowerShell cmdlets, 266–271
 subnets, adding in Active Directory, 116
subst.exe command-line tool, 732
 support calls, 753
 Swarm mode, Docker, 365–368
 symbolic links
 command-line tool, 731
 rights assignment, 598
 symptoms and diagnosis, documenting, 725–726

Sysinternals tools

- AccessChk, 740
- AccessEnum, 744–745
- AD Explorer, 746–749
- ADInsight, 749
- LogonSessions, 746
- overview, 733
- ProcDump, 736
- Process Explorer, 734–735
- Process Monitor, 735–736
- PsPing, 750
- PsTools Suite, 737–738
- RAMMap, 751–753
- ShellRunAs, 745
- SigCheck, 739–740
- Sysmon, 741–744
- VMMMap, 738–739
- Sysmon tool, 741–744**
- Sysprep.exe utility, 57**
- system activity, logging to event logs, 741–744**
- System Configuration console, 13**
- system date, command-line tool, 729**
- system files, blocking extensions, 283. *See also* files; protected files**
- system information**
 - command-line tool, 732
 - console, 14
- System Insights, using with WAC (Windows Admin Center), 5**
- system performance, rights assignment, 599**
- system time, rights assignment, 597**
- systeminfo.exe* command-line tool, 732**
- SYSVOL replication**
 - migrating, 730
 - upgrading, 695–696

T

- takeown.exe* command-line tool, 732**
- Task Manager, 37**
- Task Scheduler console, 14**
- task scheduling, blocking, 592**
- taskkill.exe* command-line tool, 732**
- tasklist.exe* command-line tool, 732**
- tasks, automating, 2**
- TCP/IP (Transmission Control Protocol/Internet Protocol). *See also* NetBIOS over TCP/IP command-line tool**
 - command-line tool, 730
 - networks, 252–255
 - subnets, 115
- Template Disk Wizard console, 14**
- test certificates, IIS (Internet Information Services), 312**
- text files, searching, 730**
- thin provisioning and trim storage, 237–238**
- time stamp, viewing, 739–740**
- time zone settings, command-line tool, 732**
- TimeDate.cpl, 37**
- time.exe* command-line tool, 732**
- TLS certificates**
 - configuring, 315–317
 - DirectAccess, 491
- token object, rights assignment, 597**
- token-signing certificates, AD FS, 442**
- TPDs (Trusted Publishing Domains), AD RMS, 471**
- TPM (Trusted Platform Module), 223, 631–633**
- tracert.exe*, command-line tool, 731**
- tracert.exe* command-line tool, 732**
- tracert.exe* command-line tool, 732**
- traffic, distribution, 385–389**
- TranscriptDirectory* session configuration file, 608**
- transparent networks, 360–362**
- traverse checking, rights assignment, 597**
- tree.exe* command-line tool, 732**
- trim storage, 238**
- troubleshooting methodology. *See also* command-line tools**
 - applying solutions, 728
 - dependencies, 726–727
 - overview, 723–724
 - ranking hypothetical solutions, 727–728
 - redeployment, 724–725
 - symptoms and diagnosis, 725–726
- trustlets, 640**

TTL (Time to Live) value, DNS, 170–171
 TUDs (Trusted User Domains), AD RMS, 470–471
 tunnel rules, firewalls, 627
TypesToProcess role-capability file, 607
tzutil.exe command-line tool, 732

U

universal groups, 133
 “unknown records,” 167
 unoptimization, 262
 updates. *See also* Azure Update Management;
 WSUS (Windows Server Update Services)
 applying, 356–357
 and drivers added to images, 53–54
 using with WAC (Windows Admin Center), 5
 upgrade and migration paths. *See also* migration;
 Rolling Upgrades
 AD CS (Active Directory Certificate Services),
 699–704
 DHCP, 705–709
 DNS, 704–705
 editions, 689
 evaluation to licensed version, 688–689
 overview, 685–688
 support, 685–693
 upgrading
 DCs (domain controllers), 693–695
 editions, 689
 roles and features, 687–688
 URL authorization rules, 323–324
 user accounts, 130–132
 user and device claims, configuring for DAC,
 456–457. *See also* claims and claim rules
 user identity, getting information about, 733
 user rights, assignment policies, 596–600

V

V VHD Sets, Hyper-V virtualization platform, 219
VariableDefinitions role-capability file, 606
verifier.exe command-line tool, 732
 virtual account, 602
 virtual directories, IIS, 313

virtual disks, creating, 239–240
 Virtual Fibre Channel adapters, Hyper-V
 virtualization platform, 203
 virtual hard disks, Hyper-V virtualization
 platform, 199–202
 virtual switches, Hyper-V virtualization platform,
 205–206
 Virtual Switches, using with WAC (Windows
 Admin Center), 5
 Virtualization Host, RDS, 509–512
 virtualization-based security, 640–642, 644–645
 virtualized domain controllers, 121, 124
 virtualized workloads, 47–48
VisibleAliases role-capability file, 606
VisibleCmdlets role-capability file, 606
VisibleExternalCommands role-capability file, 606
VisibleFunctions role-capability file, 606
VisibleProviders role-capability file, 606
 visual debugging, PowerShell, 21
 VM MAC addresses, Hyper-V virtualization
 platform, 208
 VM network adapters, Hyper-V virtualization
 platform, 206
 VM Network Health Detection, 222
 VMM (Virtual Machine Manager)
 adding WDS, 75–79
 host groups, 77
 multitier VM service, 80
 networking, 71–75
 storage, 69–71
 templates, 68–69
 VMMap tool, 738–739
 VMs (Virtual Machines). *See also* encryption-
 supported VMs; IaaS (Azure Infrastructure as
 a Service) VMs; JIT (Just In Time) VM Access;
 shielded VMs
 copying with Hyper-V, 221–222
 drain on shutdown, 222
 exporting with Hyper-V, 221–222
 failover clustering, 377–379
 Generation 2, 194–195
 importing with Hyper-V, 221–222

load balancing, 378–379

MAC addresses, 208

Network adapters, 206

NIC teaming, 208

resizing, 536

WAC (Windows Admin Center), 5

Volume Activation Tools console, 14

volumes

command-line tools, 730–732

formatting and managing, 730

maintenance task rights, 599

recovering readable information, 732

VPNs (virtual private networks). *See also* routing and remote access

authentication, 482

certificates, 479

default conditions and settings, 485

disabling protocols, 483

IKEv2 (Internet Key Exchange version 2) VPN protocol, 479–480

L2TP/IPsec protocols, 481

PPTP VPN protocol, 481–482

server access, 483–486

server deployment, 482–483

SSTP VPN protocol, 481

VSCoDe (Visual Studio Code), 23

VSS (Volume Shadow Copy Services), 670–671

Vssadmin, 670–671

W

WAC (Windows Admin Center)

AD DS feature, 120–121

Azure hybrid cloud services, 565–567

Azure IaaS VMs, 567–569

extensions, 9–10

features, 4–6

installing, 6–8

shared folder permissions, 276–277

show script, 10

tools and functionality, 5

WDAC (Windows Defender Application Control), 642–644

WDS (Windows Deployment Services)

adding to VMM, 75–76

boot options for images, 64–65

configuring, 62–66

configuring for images, 62–66

driver groups and packages, 68

managing images, 62

requirements, 60–61

transmissions, 67–68

using, 59–60

wdsutil.exe command-line tool, 733

Web Access, RDS (Remote Desktop Services), 513

Web Application Proxy, AD FS, 437, 445–447

web applications, adding, 314–315

webadmin.exe command-line tool, 733

website management. *See also* IIS (Internet Information Services)

adding sites, 310–313

default document, 320–321

directory browsing, 321–322

domain name filtering, 322–323

error response, 319–320

IP address restrictions, 322–323

modifying settings, 314

overview, 309–310

request filters, 324–326

site authentication, 318–319

test certificates, 312

TLS certificates, 315–317

URL authorization rules, 323–324

virtual directories, 313

websites, creating, 115

wecutil.exe command-line tool, 733

wevutil.exe command-line tool, 733

WFAS (Windows Firewall with Advanced Security)

connection security rules, 623–628

firewall profiles, 618–619

inbound rules, 619–620

IPsec configuration, 621–622

outbound rules, 620–621

overview, 618

wget command, PowerShell, 44

where.exe command-line tool, 733
whoami.exe command-line tool, 733
 WIM (Windows Imaging) file format, 48
.wim files, 48
 Windows 10 for Server 2019, 11
 Windows clipboard, redirecting output to, 729
 Windows Defender, 2, 650–651
 Windows Deployment Services, 14, 733
 Windows Firewall with Advanced Security console, 14
 Windows Installer files, command-line tool, 731
 Windows Memory Diagnostics console, 14
 Windows Script Host, command-line tool, 733
 Windows Server
 editions, 31–33
 servicing branches, 33–35
 Windows Server 2003, end of support, 686
 Windows Server 2008 mode, 295
 Windows Server Backup, 14, 662–666,
 683–684. *See also* Azure Backup; backup;
 Recovery Vault
 Windows Server Update Services console, 14
 Windows SIM, 58
 WinPE (Windows Preinstallation Environment),
 command-line tool, 731
winrs.exe command-line tool, 733
 WINS console, 14
wmic.exe command-line tool, 733
 workgroup clusters, 381
 Workplace Join, 447–449

writing files, blocking, 282
wscript.exe command-line tool, 733
 WSL (Windows Subsystem for Linux)
 installing, 576–579
 overview, 575–576
 updating, 579
 version 2.0, 579–580
 WSLab project, 79–80
 WSMT (Windows Server Migration Tools)
 DHCP server, 705–709
 file servers, 718–722
 storage servers, 718–722
 using, 689–693
 WSUS (Windows Server Update Services). *See also*
 updates
 automatic approval rules, 679
 autonomous and replica modes, 673
 groups, 675
 languages, 672
 policies, 675–676
 PowerShell cmdlets, 684
 products, 672
 security classifications, 672
 security roles, 674–675
 update deployment, 677–679
 update files, 673–674

Z

zone aging and scavenging, 167–168