



# Administering Windows Server Hybrid Core Infrastructure

Exam Ref AZ-800

Orin Thomas

FREE SAMPLE CHAPTER |



# Exam Ref AZ-800

## Administering Windows Server Hybrid Core Infrastructure

Orin Thomas

# Exam Ref AZ-800 Administering Windows Server Hybrid Core Infrastructure

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

Copyright © 2023 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](http://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: 978-0-13-772926-5

ISBN-10: 0-13-772926-X

Library of Congress Control Number: 2022938820

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](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

EDITOR-IN-CHIEF  
Brett Bartow

EXECUTIVE EDITOR  
Loretta Yates

SPONSORING EDITOR  
Charvi Arora

DEVELOPMENT EDITOR  
Songlin Qiu

TECHNICAL EDITOR  
Andrew Warren

MANAGING EDITOR  
Sandra Schroeder

SENIOR PROJECT EDITOR  
Tracey Croom

COPY EDITOR  
Elizabeth Welch

INDEXER  
Tim Wright

PROOFREADER  
Barbara Mack

EDITORIAL ASSISTANT  
Cindy Teeters

COVER DESIGNER  
Twist Creative, Seattle

COMPOSITOR  
codeMantra

## **Pearson's Commitment to Diversity, Equity, and Inclusion**

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

*This page intentionally left blank*

# Contents at a glance

	<i>Introduction</i>	<i>xiii</i>
<b>CHAPTER 1</b>	<b>Deploy and manage Active Directory Domain Services in on-premises and cloud environments</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Manage Windows Servers and workloads in a hybrid environment</b>	<b>99</b>
<b>CHAPTER 3</b>	<b>Manage virtual machines and containers</b>	<b>127</b>
<b>CHAPTER 4</b>	<b>Implement and manage an on-premises and hybrid networking infrastructure</b>	<b>185</b>
<b>CHAPTER 5</b>	<b>Manage storage and file services</b>	<b>233</b>
	<i>Index</i>	<i>269</i>

*This page intentionally left blank*

# Contents

<b>Introduction</b>	<b>xiii</b>
<i>Organization of this book</i>	<i>xiii</i>
<i>Microsoft certifications</i>	<i>xiv</i>
<i>Quick access to online references</i>	<i>xiv</i>
<i>Errata, updates, &amp; book support</i>	<i>xiv</i>
<i>Stay in touch</i>	<i>xv</i>

<b>Chapter 1</b>	<b>Deploy and manage Active Directory Domain Services in on-premises and cloud environments</b>	<b>1</b>
	Skill 1.1: Deploy and manage AD DS domain controllers . . . . .	1
	Deploy and manage domain controllers on-premises	2
	Deploy and manage domain controllers in Azure	23
	Deploy read-only domain controllers (RODCs)	24
	Troubleshoot flexible single master operations (FSMO) roles	26
	Skill 1.2: Configure and manage multi-site, multi-domain, and multi-forest environments . . . . .	29
	Configure and manage forest and domain trusts	29
	Configure and manage AD DS sites	35
	Configure and manage AD DS replication	41
	Skill 1.3: Create and manage AD DS security principals . . . . .	45
	Create and manage AD DS users and groups	45
	Manage users and groups in multi-domain and multi-forest scenarios	47
	Implement group managed service accounts (GMSAs)	48
	Join Windows Servers to AD DS, Azure AD DS, and Azure AD	52
	Skill 1.4: Implement and manage hybrid identities . . . . .	54
	Implement Azure AD Connect	54
	Manage Azure AD Connect Synchronization	65
	Implement Azure AD Connect cloud sync	67
	Manage Azure AD DS	68



Integrate Azure AD, AD DS, and Azure AD DS	71
Manage Azure AD Connect Health	72
Manage authentication in on-premises and hybrid environments	73
Configure and manage AD DS passwords	74
Skill 1.5: Manage Windows Server by using domain-based Group Policies	83
Implement Group Policy in AD DS	83
Implement Group Policy preferences in AD DS	93
Implement Group Policy in Azure AD DS	95
Chapter summary	95
Thought experiment	96
Thought experiment answers	97

## **Chapter 2 Manage Windows Servers and workloads in a hybrid environment 99**

Skill 2.1: Manage Windows Servers in a hybrid environment	99
Choose administration tools	100
Deploy a WAC gateway server	102
Configure a target machine for WAC	105
Manage Azure hybrid services with WAC	105
Configure PowerShell remoting	105
Configure CredSSP or Kerberos Delegation for second hop remoting	108
Configure Just Enough Administration for PowerShell remoting	109
Skill 2.2: Manage Windows Servers and workloads by using Azure Services	113
Manage Windows Servers by using Azure Arc	114
Assign Azure Policy guest configuration	116
Deploy Azure services using the Azure VM extensions on non-Azure machines	117
Manage updates for Windows machines	118
Integrate Windows Servers with Log Analytics	120
Integrate Windows Servers with Microsoft Defender for Cloud	121

Manage IaaS VMs in Azure that run Windows Server	122
Create runbooks to automate tasks on target VMs	123
Implement Azure Automation for hybrid workloads	123
Implement Desired State Configuration to prevent configuration drift in IaaS machines	124
Chapter summary .....	125
Thought experiment .....	125
Thought experiment answers .....	126
<b>Chapter 3 Manage virtual machines and containers</b>	<b>127</b>
Skill 3.1: Manage Hyper-V and guest virtual machines .....	127
Virtual machine types	128
Manage VM using PowerShell remoting, PowerShell Direct, and HVC.exe	129
Enable VM Enhanced Session Mode	130
Configure nested virtualization	130
Configure VM memory	131
Configure integration services	133
Configure Discrete Device Assignment	133
Configure VM resource groups	134
Configure VM CPU groups	135
Configure hypervisor scheduling types	135
Manage VM checkpoints	136
Implement high availability for virtual machines	137
Manage VHD and VHDX files	148
Configure Hyper-V network adapter	153
Configure NIC teaming	156
Configure Hyper-V switch	156
Skill 3.2: Create and manage containers .....	158
Understand container concepts	158
Manage Windows Server container images	163
Manage container instances	167
Configure container networking	168
Create Windows Server container images	171

Skill 3.3: Manage Azure Virtual Machines that run Windows Server . . . .	173
Administer IaaS VMs	173
Manage data disks	174
Resize Azure VM	175
Configure continuous delivery for an Azure VM	176
Configure connections to VMs	176
Manage Azure VM network configuration	179
Chapter summary . . . . .	182
Thought experiment . . . . .	183
Thought experiment answers . . . . .	183

## **Chapter 4 Implement and manage an on-premises and hybrid networking infrastructure 185**

Skill 4.1: Implement on-premises and hybrid name resolution . . . . .	185
Integrate DNS with AD DS	186
Create and manage zones and records	188
Configure DNS forwarding/conditional forwarding	192
Integrate Windows Server DNS with Azure DNS private zones	193
Implement DNSSEC	194
Manage Windows Server DNS	195
Skill 4.2: Manage IP addressing in on-premises and hybrid scenarios . . . . .	200
Implement and manage IPAM	200
Implement and configure the DHCP server role	203
Resolve IP address issues in hybrid environments	204
Create and manage scopes	204
Create and manage IP reservations	208
Implement DHCP high availability	209
Skill 4.3: Implement on-premises and hybrid network connectivity . . . .	210
Implement and manage the Remote Access role	210
Implement and manage Azure Network Adapter	219
Implement and manage Azure Extended Network	219
Implement and manage Network Policy Server role	220
Implement Web Application Proxy	227

Implement Azure Relay	227
Implement site-to-site VPN	228
Azure ExpressRoute	228
Implement Azure Virtual WAN	229
Implement Azure AD Application Proxy	229
Use Azure App Service Hybrid Connections	230
Chapter summary .....	231
Thought experiment.....	232
Thought experiment answers .....	232
<b>Chapter 5   Manage storage and file services</b>	<b>233</b>
Skill 5.1: Configure and manage Azure File Sync .....	233
Create Azure File Sync Service	234
Create sync groups	235
Create cloud endpoints	235
Register servers	235
Create server endpoints	236
Configure cloud tiering	237
Monitor File Sync	237
Migrate DFS to Azure File Sync	238
Skill 5.2: Configure and manage Windows Server File Shares .....	239
Configure Windows Server File Share access	239
Configure file screens	241
Configure File Server Resource Manager quotas	243
Use additional FSRM functionality	244
Configure BranchCache	247
Implement and configure Distributed File System	248
Skill 5.3: Configure Windows Server Storage .....	251
Configure disks and volumes	251
Configure and manage storage spaces	252
Configure and manage Storage Replica	257
Configure data deduplication	260
Configure SMB Direct	261

Configure Storage QoS	262
Configure filesystems	263
Chapter summary .....	266
Thought experiment.....	266
Thought experiment answers .....	267
<i>Index</i>	269

# Introduction

---

The AZ-800 exam deals with advanced topics that require candidates to have an excellent working knowledge of Windows Server and Azure Hybrid functionality. Some of the exam comprises topics that even experienced Windows Server Hybrid administrators may rarely encounter unless they are consultants who manage hybrid cloud workloads on a regular basis. To be successful in taking this exam, not only do candidates need to understand how to deploy and manage AD DS, hybrid identity, Windows Servers, virtual machines, containers, hybrid networks, and storage services, but they also need to know how to perform these tasks with on-premises and Azure IaaS instances of Windows Server.

Candidates for this exam are information technology (IT) professionals who want to validate their advanced Windows Server Hybrid administration skills and knowledge. To pass, candidates require a thorough theoretical understanding as well as meaningful practical experience implementing the technologies involved.

This edition of this book covers Windows Server and the AZ-800 exam objectives as of mid-2022. As Windows Server hybrid technologies evolve, so do the AZ-800 exam objectives, so you should check carefully if any changes have occurred since this edition of the book was authored and study accordingly.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the “Need more review?” links you’ll find in the text to find more information and take the time to research and study the topic. Great information is available on Microsoft Docs, Microsoft Learn, and in blogs and forums.

## Organization of this book

---

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list is available for each exam on Microsoft Learn: <https://microsoft.com/learn>. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter’s organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

## Microsoft certifications

---

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

### **NEED MORE REVIEW ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learn.com/learn>.

Check back often to see what is new!

## Quick access to online references

---

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these addresses (also known as URLs) can be painstaking to type into a web browser, so we've compiled all of them into a single list that readers of the print edition can refer to while they read.

Download the list at

*[MicrosoftPressStore.com/ExamRefAZ800/downloads](http://MicrosoftPressStore.com/ExamRefAZ800/downloads)*

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

## Errata, updates, & 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/ExamRefAZ800/errata](http://MicrosoftPressStore.com/ExamRefAZ800/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 <http://www.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>.

## Stay in touch

---

Let's keep the conversation going! We're on Twitter: <http://twitter.com/MicrosoftPress>.



*This page intentionally left blank*

# About the author

**ORIN THOMAS** is a Principal Cloud Advocate at Microsoft and has written more than 3 dozen books for Microsoft Press on such topics as Windows Server, Windows Client, Azure, Office 365, System Center, Exchange Server, Security, and SQL Server. He has authored Azure Architecture courses at Pluralsight and has authored multiple Microsoft Official Curriculum and EdX courses on a variety of IT Pro topics. You can follow him on Twitter at <http://twitter.com/orinthomas>.

*This page intentionally left blank*

# Manage Windows Servers and workloads in a hybrid environment

A critical element in any complex hybrid cloud deployment is the set of tools used to manage, maintain, and monitor workloads. Windows Server hybrid administrators have several options when it comes to choosing which tools they will use to manage the Windows Server instances that they are responsible for. Some tools allow you to manage up to the cloud from an on-premises administrative workstation; other tools allow you to manage down from the cloud from the Azure portal or Azure CLI.

## Skills covered in this chapter:

- Skill 2.1: Manage Windows Servers in a hybrid environment
- Skill 2.2: Manage Windows Servers and workloads by using Azure Services

## Skill 2.1: Manage Windows Servers in a hybrid environment

---

This objective deals with the technologies and techniques that you can use to manage Windows Server instances in on-premises and cloud environments. You'll learn about choosing and configuring administration tools as well as constrained delegation and Just Enough Administration.

### This skill covers how to:

- Choose administration tools
- Deploy a WAC gateway server
- Configure a target machine for WAC
- Manage Azure hybrid services with WAC
- Configure PowerShell remoting
- Configure CredSSP or Kerberos Delegation for second hop remoting
- Configure Just Enough Administration for PowerShell remoting

## Choose administration tools

You can use a variety of tools to manage Windows Server 2019. Some, such as PowerShell, the Microsoft Management Console, and Server Manager, are built into the operating systems. You'll need to download others, such as Windows Admin Center, for free from the Microsoft website.

The company's general systems administration philosophy is that while you can do almost everything with a graphical console such as Windows Admin Center, Active Directory Administrative Center, or the Server Manager console, any task that you do repeatedly should be automated using PowerShell. Microsoft best practice is that almost all administration tasks should be performed remotely rather than by signing in directly to the server and performing them locally.

### Remote not local

Windows Server is designed to be administered remotely rather than locally. This "remote first" philosophy shouldn't come as a surprise to experienced administrators. The vast majority of Windows Server instances are running as virtual machines, either in datacenters or in the cloud, and we are long past the days where your primary method of switching between different servers that you were working on was by selecting different options on a KVM switch.

You need to be familiar with how to use your tools remotely. You should avoid signing in to each server individually using Remote Desktop and firing up the console that is relevant to the role or feature that you want to manage. You should also avoid using Remote Desktop to connect to a server just to run a PowerShell script because this is a task more appropriately performed using PowerShell remoting.

### Privileged Access Workstations

Servers are only as secure as the computers that you use to manage them. An increasing number of security incidents have occurred because a privileged user's computer was infected with malware and that computer was then used to perform server administration tasks. Privileged Access Workstations (PAWs) are specially configured computers that you use to perform remote administration tasks. The idea of a PAW is that you have a computer with a locked-down configuration that you only use to perform server administration tasks. You don't use this computer to read your email or browse the internet; you just use it to perform server administration tasks.

Consider configuring a PAW in the following way:

- Configure Windows Defender Application Control to allow only specifically authorized and digitally signed software to run on the computer.
- Configure Credential Guard to protect credentials stored on the computer.
- Use BitLocker to encrypt the computer's storage and protect the boot environment.
- The computer should not be used to browse the internet or to check email. Server administrators should have completely separate computers to perform their other

daily job tasks. Block internet browsing on the PAW both locally and on the perimeter network firewall.

- Block the PAW from accessing the internet. Software updates should be obtained from a dedicated secure update server on the local network. External tools should be obtained from another computer and transferred to the PAW.
- Server administrators should not sign in to the PAW using an account that has administrative privileges on the PAW.
- Only specific user accounts used by server administrators should be able to sign on to the PAW. Consider additional restrictions such as sign-in hours. Block privileged accounts from signing in to computers that are not PAWs or servers to be managed, such as the IT staff's everyday work computers.
- Configure servers to only accept administrator connections from PAWs. This can be done through Windows Defender Firewall with Advanced Security.
- Use configuration-management tools to monitor the configuration of the PAW. Some organizations rebuild PAWs entirely every 24 hours to ensure that configurations are not altered. Use these tools to restrict local group membership and ensure that the PAW has all appropriate recent software updates applied.
- Ensure that audit logs from PAWs are forwarded to a separate secure location.
- Disable the use of unauthorized storage devices. For example, you can configure policies so that only USB storage devices that have a specific BitLocker organizational ID can be used with the computer.
- Block unsolicited inbound network traffic to the PAW using Windows Defender Firewall.

## Jump servers

Jump servers are another security procedure that can be used in conjunction with privileged-access workstations. Jump servers allow servers to accept administrative connections only from specific hosts. For example, you only allow domain controllers to be administered from computers that have a specific IP address and a computer certificate issued by a specific certification authority. You can configure jump servers to only accept connections from PAWs and servers to be administered to only accept connections from jump servers. As mentioned earlier, some organizations that use jump servers have them rebuilt and redeployed every 24 hours to ensure that their configuration does not drift from the approved configuration. Azure provides a service, Azure Bastion, that functions as a managed jump server. You'll learn more about using Azure Bastion to access Windows Server IaaS VMs in Chapter 3.

## Remote Desktop

Remote Desktop is the way that many administrators are likely to remotely perform one-off tasks on servers running the GUI version of Windows Server. While best practice is to use PowerShell or Windows Admin Center for remote administration, sometimes it's quicker to just establish a Remote Desktop session. This is because using Remote Desktop allows you to

perform tasks on the remote server in a manner that appears similar to being directly signed in at the console.

By default, Remote Desktop is disabled on newly deployed computers running Windows Server (though this is not the case for new Azure IaaS instances of Windows Server). You enable Remote Desktop either through the Remote tab of the System Properties dialog box or by running the following PowerShell command:

```
Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" -Value 0
```

You can make Remote Desktop connections to computers running the Server Core installation option if Remote Desktop is enabled.

By default, Remote Desktop Connection connects to Remote Desktop services on port 3389. When you enable Remote Desktop using the GUI, a remote desktop related firewall is automatically enabled. If you enable Remote Desktop using PowerShell, you also need to manually enable a firewall rule to allow connections. You can do this using the following PowerShell command:

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

By default, the **Allow connections only from computers running Remote Desktop with Network Level Authentication** option is selected. Network Level Authentication requires that a user be authenticated prior to the Remote Desktop session being established. Network Level Authentication is supported by the Remote Desktop Connection client, which is available on all Windows operating systems, but it might not be supported by third-party Remote Desktop clients.

Only users who are members of the local Administrators group and members of the local Remote Desktop Users group can make connections via Remote Desktop. If you want to grant a user account permission to access the server without the account full administrative privileges, add the account to the local Remote Desktop Users group.

You can map local volumes to a remote host in an active Remote Desktop Connection session by configuring the **Local Resources and Devices** setting on the **Local Resources** tab of the **Remote Desktop Connection** dialog box. While it is less effective over low-bandwidth connections, it can provide a simple way to transfer files from your client computer to a remote server instead of setting up FTP or another file transfer method.

## Deploy a WAC gateway server

Windows Admin Center (WAC) is a web-based console that allows you to remotely manage Windows Server through a web browser. You can connect to and use Windows Admin Center using Edge, Chrome, or any standards-compliant browser. You can use WAC to manage computers running Windows Server 2012 and later and Windows 10 or later client computers.

You can install WAC on computers running Windows 10 and later and Windows Server 2016 and later. You can install WAC on a Windows Server instance deployed using the Server Core installation option.

When you deploy WAC on a Windows Server instance, it functions as a *gateway server*. Gateway servers allow any client on the network to connect to the Windows Admin Center instance using their standards-compliant web browser without requiring Windows Admin Center be installed locally. A WAC gateway server can function as an administration connection point for multiple administrative sessions from different administrative users. Some organizations only deploy a single highly available gateway server and have all WAC administration tasks performed using that single WAC gateway instance. You should not deploy Windows Admin Center on a Windows Server instance that hosts the AD DS role.

## Installing WAC

Windows Admin Center isn't included in Windows Server. You have to download the installation files from the Microsoft website. There are four Windows Admin Center deployment options:

- **Local client** When you choose this installation option, you install Windows Admin Center on your workstation. You connect to the WAC instance locally, which is similar to installing the Remote Server Administration Tools (RSAT) on a local workstation. When you install WAC locally, a shortcut to the WAC console is placed on your desktop.
- **Gateway server** When you install WAC in the gateway server configuration, you install it on a computer running Windows Server 2016 or later and then make remote connections to the WAC instance hosted on that computer through your preferred browser. Once connected to the WAC instance, you can add servers that you want to manage to the web-based console. When you perform an administrative task, the instructions to perform that task are issued from the gateway server and are run against the target server.
- **Managed server** The managed server deployment is a version of WAC in a gateway server configuration deployed on a cluster node to manage the cluster.
- **Failover cluster** The gateway server is deployed as a highly available service. This requires the configuration of a Cluster Shared Volume to store persistent data used by WAC. A script is available from the Microsoft website that simplifies the process of performing a high availability deployment.

When you install WAC on a Windows Server instance, you get the option of configuring which port will be used. You can choose between using a self-signed SSL (TLS) certificate or an SSL (TLS) certificate that is already installed on the computer. If you're deploying a gateway server, things will be a lot simpler if you deploy a TLS certificate from a trusted CA because it won't be necessary to go through the hassle of responding to dialog boxes about whether to trust the self-signed certificate when connecting to the gateway server from a variety of different administrative systems.

You can install Windows Admin Center on a Server Core instance of Windows Server using `msiexec` and by specifying the management port and SSL certificate option. (It should be the TLS certificate since the SSL protocol has been phased out, but most of the world still uses the



legacy terminology.) The syntax of the command-line installation where a trusted certificate is used is as follows:

```
msiexec /i <WACInstallerName>.msi /qn /L*v log.txt SME_PORT=<port> SME_THUMBPRINT=<thumbprint> SSL_CERTIFICATE_OPTION=installed
```

SME\_PORT is the port you want to use, and SME\_THUMBPRINT is the thumbprint of the installed SSL (TLS) certificate. By default, installing WAC updates the computer's trusted host files. When you deploy WAC, you can configure it to update automatically or manually. When you configure WAC to update automatically, new versions will be installed as they become available through Microsoft Update. If you don't configure this option, you'll need to manually install newer versions of WAC as they become available.

To update an expired certificate on a WAC gateway server, you need to obtain and install the new certificate, obtain the certificate's thumbprint, and then rerun Setup and change the certificate used by WAC by specifying the new thumbprint.

#### **NEED MORE REVIEW? DEPLOY WAC GATEWAY**

You can learn more about deploying a WAC gateway at <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/deploy/install>.

## Windows Admin Center extensions

Windows Admin Center extensions allow for the extension of WAC functionality. Windows Admin Center includes extensions for roles built into Windows Server such as Storage Migration Services and third-party extensions. Microsoft encourages third-party partners to add extensions to Windows Admin Center as an alternative to requiring systems administrators to use product-specific consoles.

By default, Windows Admin Center will display extensions published to the Microsoft official NuGet feed. This feed includes extensions published and updated by Microsoft as well as those published by trusted third-party vendors. Also, you can configure Windows Admin Center to display extensions or installations from any NuGet feed that supports the NuGet V2 APIs or a specially configured file share accessible to the computer hosting Windows Admin Center.

Extensions are available in Windows Admin Center by selecting the **Settings** icon and then selecting **Extensions**. The **Available Extension** pane displays all extensions that are available but not installed from the currently configured feed. You can update currently installed extensions if new versions of those extensions are available through the **Installed Extensions** pane. You can also configure Windows Admin Center to automatically update extensions.

## Show script

When you perform a task in Windows Admin Center, you can select the PowerShell icon in the Windows Admin Center title bar to view PowerShell source code relevant to the tasks.

This allows you to copy and save useful PowerShell code for reuse later rather than having to perform all tasks through WAC.

## Configure a target machine for WAC

Just like you need to configure a Windows Server instance so that you can connect to it using Remote Desktop, a Microsoft Management Console, or a remote PowerShell session, you will also have to configure a Windows Server instance so that it can be managed from a remote WAC instance.

To allow administration from a WAC instance, Remote Management must be enabled on a Windows Server instance you intend to manage. WAC traffic from the WAC instance to target servers uses PowerShell and WMI over WinRM. WinRM connections over HTTP use port 5985 and WinRM connections over HTTPS uses port 5986. If WinRM over HTTPS is not configured, you can configure a WinRM HTTPS listener using the following command:

```
winrm quickconfig -transport:https
```

In addition to the WinRM ports, WAC uses the SMB file sharing protocol for some file copying tasks. To configure a target machine for remote management by WAC, you will need to ensure any firewalls between the WAC instance and the target computer allow inbound connections on ports 445, 5985, and 4986.

To use Windows Admin Center from the Azure portal to manage Windows Server instances in Azure, it's necessary to deploy Windows Admin Center to each Windows Server Azure IaaS instance.

### **NEED MORE REVIEW? CONFIGURE TARGET MACHINE**

You can learn more about configuring a target machine at <https://docs.microsoft.com/windows-server/manage/windows-admin-center/azure/manage-vm>.

## Manage Azure hybrid services with WAC

Windows Admin Center can also be used to manage Azure hybrid services, such as Azure Backup, Azure Software Update, Azure Site Recovery, Azure Network Adapter, and Azure Monitor. Before you can integrate Azure hybrid services with WAC, you need to register the Windows Admin Center gateway with your Azure subscription. This process requires that you have access to an Azure AD account with the necessary permissions to configure an Azure AD application that has access to the Azure AD tenancy associated with your Azure subscription.

## Configure PowerShell remoting

PowerShell is the primary scripting, automation, and management tool from Microsoft. In almost all cases, you can access greater functionality and settings through PowerShell than you can through WAC or the Azure console.

PowerShell includes a substantial amount of documentation explaining what each cmdlet can do and how you can do it. Once you know the name of the command you want to use to perform a task, you can use the PowerShell built-in help to learn the precise details of how to use that cmdlet to perform that task. You can get help for each cmdlet by typing **help cmdletname**. For example, to get help with the `get-service` cmdlet, type **help get-service** into a PowerShell session.

## Modules

Modules are collections of PowerShell cmdlets. In older versions of PowerShell, you needed to manually load a module each time you wanted to use one of its associated cmdlets. In Windows Server 2016 and later, any module that is installed will load automatically when you try to run an associated cmdlet. Viewing cmdlets by module using the `Get-Command-Module <module name>` cmdlet allows you to view just those cmdlets associated with a specific role or feature.

## PowerShell Gallery

The PowerShell Gallery is a collection of modules published by the community that extend the functionality of PowerShell beyond what is available with a default installation of Windows Server. Table 2-1 lists the commands that you can use to get started with the PowerShell Gallery.

**TABLE 2-1** PowerShell Gallery basics

Command	Functionality
<code>Find-Module -Repository PSGallery   out-host -paging</code>	This will list the available modules in the PowerShell Gallery in a paged format. You'll be prompted to install the NuGetProvider to interact with the PowerShell Gallery.
<code>Find-Module -Repository PSGallery -Name &lt;ModuleName&gt;</code>	This will list the modules with a specific name. You can use wildcards. For example, to view all modules that start with the name AzureRM, run the command <code>Find-Module -Repository PSGallery -Name AzureRM*</code> .
<code>Install-Module -Repository PSGallery -Name &lt;ModuleName&gt;</code>	This will install the ModuleName module. For example, to install the AzureRM module, run the command <code>Install-Module -Repository PSGallery -Name AzureRM</code> .
<code>Update-Module</code>	This will update any module that you've installed using <code>Install-Module</code> .
<code>Get-InstalledModule</code>	Use this command to view all modules installed from the PowerShell Gallery.

## PowerShell remoting

PowerShell remoting allows you to establish a remote interactive PowerShell session from a local PowerShell session on an administrative workstation or Cloud Shell. By default, PowerShell remoting is enabled on Windows Server instances but also requires a connection from a

private network and an account that is a member of the local Administrators group. PowerShell uses WMI over WinRM. WinRM connections over HTTP use port 5985, and WinRM connections over HTTPS uses port 5986. If PowerShell remoting has been disabled, you can enable it using the `Enable-PSRemoting` cmdlet. If WinRM over HTTPS is not configured, you can configure a WinRM HTTPS listener using the following command:

```
winrm quickconfig -transport:https
```

You initiate a remote PowerShell session using the `enter-psession` command. If you do not specify alternate credentials, the credentials of the currently signed-on user will be used. If you want to use alternate credentials, one method to do so securely is by using the `get-credential` command and assigning it to a PowerShell variable, and then using the variable with the `enter-psession` command. When you use `get-credential`, you will be prompted to enter a set of credentials. For example, to enter a set of credentials and then to use those credentials to establish a remote PowerShell session to a host named `dc1.tailwindtraders.com`, use the following commands:

```
$creds = get-credential  
Enter-PSession -Computername dc1.tailwindtraders.com -credential $creds
```

To enable PowerShell remoting to computers that are not domain-joined, you must configure the trusted hosts list on the client computer from which you want to establish the remote session. You do this on the client computer using the `set-item` cmdlet. For example, to trust the computer at IP address `192.168.3.200`, run this command:

```
Set-Item wsman:\localhost\Client\TrustedHosts -Value 192.168.3.200 -Concatenate
```

Once you've run the command to configure the client, you'll be able to establish a PowerShell remote session using the `Enter-PSession` cmdlet. If you want more information about remoting, run the following command to bring up help text on the subject:

```
Help about_Remote_faq -ShowWindow
```

PowerShell allows you to run one command against many machines, which is known as *one-to-many remoting* or *fan-out administration*. You can use one-to-many remoting to run the same command against any number of computers. Rather than signing in to each computer to check whether a particular service is running, you can use PowerShell remoting to run the same command that checks the status of the service against each computer within the scope of the command.

For example, you could use the following command to read a list of computers from a text file named `computers.txt`:

```
$Computers = Get-Content c:\Computers.txt
```

You could then use the following command to get the properties of the Windows Update service:

```
Invoke-Command -ScriptBlock { get-service wuauerv } -computername $Computers
```

You can also use the `Invoke-Command` cmdlet to run a script from the local computer against a number of remote computers. For example, to run the script `FixStuff.ps1` against the computers in the file `computers.txt`, run this command:

```
$Computers = Get-Content c:\Computers.txt
Invoke-Command -FilePath c:\FixStuff.ps1
```

#### **NEED MORE REVIEW? POWERSHELL REMOTING**

You can learn more about PowerShell remoting at <https://docs.microsoft.com/powershell/scripting/learn/remoting/powershell-remoting-faq>.

## Configure CredSSP or Kerberos Delegation for second hop remoting

Second hop remoting is when you are signed in to one host, make a remote PowerShell connection to a second host, and perform a task that requires resource access to a third host that requires your account credentials. Unless the second host has a way of forwarding your credentials to the third host, the task may not complete because your credentials can't be used for that task. The process of a server acting on behalf of a signed-on user is termed *delegation*.

Kerberos delegation allows a computer to interact with the Kerberos Key Distribution Center to obtain a service ticket derived from the user's permissions that is used to access resources on the network.

For example, say you need to allow users with accounts in the `tailwindtraders.com` domain to use a WAC to manage a server named `app1.adatum.com` in the `adatum.com` domain. The following conditions exist:

- You have deployed a WAC gateway server on host `wac.tailwindtraders.com`.
- There is a two-way forest trust between the `adatum.com` and the `tailwindtraders.com` single-domain forests.

You can configure constrained delegation in this scenario by running the following PowerShell command:

```
Set-ADComputer -Identity (Get-ADComputer wac.tailwindtraders.com) -PrincipalsAllowedToDelegateToAccount (Get-ADComputer app1.adatum.com)
```

Kerberos constrained delegation allows you to limit which of a computer's services can interact with the KDC to obtain the appropriate ticket on the user's behalf. You can configure constrained delegation on the **Delegation** tab of a computer account's properties in Active Directory Users and Computers. When you do this, you specify the service type, the user or computer account that can leverage delegated credentials, the port, and the service principal name of the service that can perform the action.

### **NEED MORE REVIEW? SECOND HOP REMOTING**

You can learn more about second hop remoting at <https://docs.microsoft.com/powershell/scripting/learn/remoting/ps-remoting-second-hop>.

## **Configure Just Enough Administration for PowerShell remoting**

Just Enough Administration (JEA) allows you to implement role-based access control (RBAC) functionality through Windows PowerShell remoting. JEA allows you to specify which PowerShell cmdlets and functions can be used when connected to a specific endpoint. You can go further and specify which parameters within those cmdlets and functions are authorized and even specify which values can be used with those parameters.

For example, you could create a JEA endpoint where a user is able to run the `Restart-Service` command, but only where the `Name` parameter is set to `DHCPService`. This would allow the user to restart the `DHCPService` on the computer they connected to, but it would not restart any other service on the computer.

You can also configure a JEA endpoint to allow other command-line commands such as `whoami` to be run, though the drawback of this is that you don't have the same level of control when restricting how that command can be run.

JEA endpoints can leverage virtual accounts. This means that activities performed on the computer through the endpoint use a special temporary virtual account rather than the user's account. This temporary virtual account has local administrator privileges but is constrained to only using the cmdlets, functions, parameters, and values defined by JEA. The benefits of this include:

- The user's credentials are not stored on the remote system. If the remote system is compromised, the user's credentials are not subject to credential theft and cannot be used to traverse the network to gain access to other hosts.
- The user account used to connect to the endpoint does not need to be privileged. The endpoint simply needs to be configured to allow connections from specified user accounts.
- The virtual account is limited to the system on which it is hosted. The virtual account cannot be used to connect to remote systems. Attackers cannot use a compromised virtual account to access other protected servers.
- The virtual account has local administrator privileges but is limited to performing only the activities defined by JEA. You have the option of configuring the virtual account with the membership of a group other than the local administrators group, to further reduce privileges.

## Role-capability files

A role-capability file is a special file that allows you to specify what tasks can be performed when connected to a JEA endpoint. Only tasks that are explicitly allowed in the role-capability file can be performed.

You can create a new blank role-capability file by using the `New-PSRoleCapabilityFile` cmdlet. Role-capability files use the `.psrc` extension. For example, run this command to create a new role-capability file for a role that allows someone to manage a DNS server:

```
New-PSRoleCapabilityFile -Path .\DNSOps.psrc
```

Once the PSRC file is created, you edit the role-capability file and add the cmdlets, functions, and external commands that are available when a user is connected to the endpoint. You can allow entire Windows PowerShell cmdlets or functions or list which parameters and parameter values can be used.

You can edit a role-capability file in PowerShell ISE, Visual Studio Code (though only the first is available on Windows Server), or any capable text editor. Editing the file involves commenting out the appropriate sections and filling them in with the configuration items that you want to set.

Authoring role-capability files is one of those few times when you need to know whether something in PowerShell is a cmdlet or a function. Mostly, people refer to commands in PowerShell as cmdlets, but some are actually functions and others are aliases. You need to know the appropriate type when configuring a role-capability file because if you put a function in as an allowed cmdlet, you won't get the expected result. You can figure out which designation is appropriate by using the `Get-Command` cmdlet.

Table 2-2 describes the different options that you can configure in a role-capability file.

**TABLE 2-2** Role-capability files

Capability	Description
<i>ModulesToImport</i>	JEA auto-loads standard modules, so you probably don't need to use this unless you need to import custom modules.
<i>VisibleAliases</i>	Specifies which aliases to make available in the JEA session. Even if an aliased cmdlet is available, the alias won't be available unless it's here.
<i>VisibleCmdlets</i>	Lists which Windows PowerShell cmdlets are available in the session. You can extend this by allowing all parameters and parameter values to be used or you can limit cmdlets to particular parameters and parameter values. For example, use the following syntax, if you wanted to allow the <code>Restart-Service</code> cmdlet to only be used to restart the DNS service: <pre>VisibleCmdlets = @{ Name = 'Restart-Service'; Parameters = @{ Name='Name'; ValidateSet = 'DNS'}}</pre>

Capability	Description
<i>VisibleFunctions</i>	This field lists which Windows PowerShell functions are available in the session. You can choose to list functions, allowing all parameters and parameter values to be used, or you can limit functions to particular parameters and parameter values. For example, if you wanted to allow the <code>Add-DNSServerResourceRecord</code> , <code>Get-DNSServerResourceRecord</code> , and <code>Remove-DNSServerResourceRecord</code> functions to be used, you would use the following syntax: <pre>VisibleFunctions = 'Add-DNSServerResourceRecord', 'Get-DNSServerResourceRecord', 'Remove-DNSServerResourceRecord'</pre>
<i>VisibleExternalCommands</i>	This field allows users who are connected to the session to run external commands. For example, you can use this field to allow access to <code>c:\windows\system32\whoami.exe</code> so that users connected to the JEA session can identify their security context by using the following syntax: <pre>VisibleExternalCommands = 'C:\Windows\System32\whoami.exe'</pre>
<i>VisibleProviders</i>	This field lists Windows PowerShell providers that are visible to the session.
<i>ScriptsToProcess</i>	This field allows you to configure Windows PowerShell scripts to run automatically when the session is started.
<i>AliasDefinitions</i>	This field allows you to define Windows PowerShell aliases for the JEA session.
<i>FunctionDefinitions</i>	This field allows you to define Windows PowerShell functions for the JEA session.
<i>VariableDefinitions</i>	This field allows you to define Windows PowerShell variables for the JEA session.
<i>EnvironmentVariables</i>	This field allows you to specify environment variables for the JEA session.
<i>TypesToProcess</i>	This field allows you to configure Windows PowerShell type files to load for the JEA session.
<i>FormatsToProcess</i>	This field allows you to configure Windows PowerShell formats to load for the JEA session.
<i>AssembliesToLoad</i>	This field allows you to specify which assemblies to load for the JEA session.

## Session-configuration files

Session-configuration files determine which role capabilities are mapped to specific security groups. For example, if you wanted to allow only members of the `CONTOS\DNSOps` security group to connect to the JEA endpoint that is defined by the `DNSOps` role-capability file, you would configure this security group in the session-configuration file.

You use the `New-PSSessionConfigurationFile` cmdlet to create a session-configuration file. These files use the `.pssc` extension. For example, to create a new session-configuration file for the `DNSOps` role, run the following command:

```
New-PSSessionConfigurationFile -Path .\DNSOps.pssc -Full
```

Session-configuration files have elements described in Table 2-3.



**TABLE 2-3** Session-configuration files

Field	Explanation
<i>SessionType</i>	This field allows you to configure the session's default settings. If you set this to <i>RestrictedRemoteServer</i> , you can use the <code>Get-Command</code> , <code>Get-FormatData</code> , <code>Select-Object</code> , <code>Get-Help</code> , <code>Measure-Object</code> , <code>Exit-PSSession</code> , <code>Clear-Host</code> , and <code>Out-Default</code> cmdlets. The session execution policy is set to <i>RemoteSigned</i> . Example: <code>SessionType = 'RestrictedRemoteServer'</code>
<i>RoleDefinitions</i>	You use the <i>RoleDefinitions</i> entry to assign role capabilities to specific security groups. These groups do not need to have any privileges and can be standard security groups. Example: <code>RoleDefinitions = @{ 'CONTOSO\DNSOps' = @{ RoleCapabilities = 'DNSOps' } }</code>
<i>RunAsVirtualAccount</i>	When enabled, this field allows JEA to use a privileged virtual account created just for the JEA session. This virtual account has local administrator privileges on member servers and is a member of the Domain Admins group on a domain controller. Use this option to ensure that credentials are not cached on the server that hosts the endpoint. Remember that you can configure the virtual account to be a member of groups other than the local administrators group.
<i>TranscriptDirectory</i>	This field allows you to specify the location where JEA activity transcripts are stored.
<i>RunAsVirtualAccountGroups</i>	If you do not want the virtual account to be a member of the local administrators group (or Domain Admins on a domain controller), you can instead use this field to specify the groups in which the virtual account is a member.

## JEA endpoints

A JEA endpoint is a Windows PowerShell endpoint that you configure so that only specific authenticated users can connect to it. When those users do connect, they only have access to the Windows PowerShell cmdlets, parameters, and values defined by the appropriate session-configuration file that links security groups and role capabilities. When you use endpoints with virtual accounts, the actual activity that a user performs on the server that hosts the endpoint occurs using the virtual account. This means that no domain-based administrative credentials are stored on the server that hosts the endpoint.

A server can have multiple JEA endpoints, and each JEA endpoint can be used for a different administrative task. For example, you could have a DNSOps endpoint to perform DNS administrative tasks and an IISOps endpoint to perform Internet Information Server–related administrative tasks. Users are not required to have privileged accounts that are members of groups, such as the local administrators group, to connect to an endpoint. Once connected, users have the privileges assigned to the virtual account configured in the session-configuration file.

You create JEA endpoints by using the `Register-PSSessionConfiguration` cmdlet. When using this cmdlet, you specify an endpoint name and a session-configuration file hosted on the local machine.

For example, to create the endpoint `DNSOps` using the `DNSOps.pssc` session-configuration file, issue the following command and then restart the WinRM service:

```
Register-PSSessionConfiguration -Name DNSOps -Path .\DNSOps.pssc
```

You can use the `Get-PSSessionConfigurationFile` cmdlet to determine which endpoints are present on a computer. A user wanting to connect to a JEA session endpoint uses the `Enter-PSSession` cmdlet with the `ConfigurationName` parameter. For example, to connect to the `DNSOps` JEA endpoint on server `MEL-DNS1`, you would use this command:

```
Enter-PSSession -ComputerName MEL-DNS1 -ConfigurationName DNSOps
```

Once you've verified that JEA works, you'll need to lock down the default PowerShell endpoint. By default, only members of the local administrators group can connect to this default endpoint, and if you've implemented JEA properly, this group shouldn't need to have very many members anyway.

#### **NEED MORE REVIEW? JUST ENOUGH ADMINISTRATION**

You can learn more about Just Enough Administration at <https://docs.microsoft.com/powershell/scripting/learn/remoting/jea/overview>.



#### **EXAM TIP**

Remember which PowerShell cmdlets are relevant to specific JEA tasks.

## **Skill 2.2: Manage Windows Servers and workloads by using Azure Services**

This objective deals with managing Windows Server instances in hybrid environments using Azure services, including Azure Arc, Microsoft Defender for Cloud, Microsoft Update, and Desired State Configuration.

# Index

## A

- access-denied assistance, 247
- Active Directory Domains and Trusts, 6
- Active Directory Federation Services, 74
- Active Directory Recycle Bin, 12–13
- Active Directory Sites and Services, 6
- Active Directory Users and Computers, 5
  - Delegation of Control Wizard, 5
  - tasks, 5
  - View Advanced Features function, 5
- Active Directory-integrated zones, 186–187
- AD DS (Active Directory Domain Services), 1, 9. *See also* Azure AD; domain(s)
  - backup, 10
  - database optimization, 20–21
  - DNS integration, 186, 188, 192
    - Active Directory-integrated zones, 186–187
    - alias (CNAME) records, 191
    - conditional forwarders, 193
    - forwarders, 192–193
    - GlobalNames zones, 189–190
    - host records, 190
    - MX (mail exchanger) records, 191
    - pointer records, 191
    - resource records, 190, 194–195
    - reverse lookup zones, 188–189
    - scavenging, 192
    - secondary zones, 188
    - stub zones, 193
    - unknown records, 191
    - zone aging, 191–192
    - zone delegation, 190
  - domain(s), 16–17
    - authentication and, 18
    - controllers, 1–2, 6–7
    - forests and, 19–20
    - functional levels, 19
    - trees and, 18
  - DSRM (Directory Services Restore Mode), 7–8
  - forests, 16
  - Group Policy, 83. *See also* AGPM (Advanced Group Policy Management); Group Policy
    - Administrative template, 92–93
    - caching, 91
    - fixing GPO problems, 85–86
    - forced update, 91–92
    - GPO backup, 84–85
    - GPO management, 83–85, 86
    - implementing, 95
    - import and copy GPOs, 85
    - loopback processing, 90–91
    - preferences, 93–94
    - security filtering, 89–90
    - WMI filters, 90
  - groups, 47
  - integration with other AD instances, 71
  - metadata cleanup, 21
  - multi-domain forests, 17–18
  - partitions, 41
  - password(s)
    - managing, 74–75
    - policy items, 75
    - replication, 24–25
    - settings permissions, 76
  - replication, 41
    - conflict resolution, 43
    - KCC (Knowledge Consistency Checker), 42
    - managing and monitoring, 44
    - multi-master, 42
    - RODC, 43–44
    - store and forward, 42
    - triggering, 44
  - security, 45
  - site(s), 35–37
    - creating, 37–38
    - link bridges, 40

## Azure AD; domain(s)

- links, 39–40
- subnets, 38
- snapshots, 22
- tombstone lifetime, 10–12
- trust(s), 29, 30
  - direction, 30–31
  - external, 32
  - forest, 31–32
  - name suffix routing, 35
  - netdom.exe and, 34
  - realm, 33
  - shortcut, 32
  - SID filtering, 34–35
  - transitivity, 30
- ADAC (Active Directory Administrative Center), 3
  - Powershell and, 3
  - search functionality, 3–4
- Add-Clusternode cmdlet, 257
- Add-Computer cmdlet, 52
- Add-DhcpServer4Filter cmdlet, 209
- Add-DHCPsServer4Scope cmdlet, 205
- Add-DHCPsServer6Scope cmdlet, 205
- Add-DhcpServerv4SuperScope cmdlet, 206
- Add-DNSPrimaryZone cmdlet, 189
- Add-DnsServerConditionalForwarderZone cmdlet, 193
- Add-DNSServerDirectoryPartition cmdlet, 187
- Add-DnsServerPrimaryZone cmdlet, 187
- Add-DNSServerQueryResolutionPolicy cmdlet, 199
- Add-DNSServerSecondaryZone cmdlet, 188
- Add-DnsServerStubZone cmdlet, 193
- Add-DnsServerZoneDelegation cmdlet, 190
- ADDomainMode cmdlet, 19
- Add-VMAssignableDevice cmdlet, 134
- administration tools, Windows Server, 100
  - jump servers, 101
  - PAWs (Privileged Access Workstations), 100–101
  - remote access and, 100
  - Remote Desktop, 101–102
  - WAC (Windows Admin Center), 102–105
- AGPM (Advanced Group Policy Management), 88–89
- alias (CNAME) records, 191
- ARM (Azure Resource Manager), templates, 53
- assessment, Windows update compliance, 119
- authentication
  - intra-forest, 18
  - NPS and, 223
  - pass-through, 74
  - on-premises environments and, 73
  - VPN, 213–214
  - authoritative restore, 13–15
- Azure AD, 1, 2. *See also* domain controllers
  - Application Proxy, 229–230
  - Connect Health, 72
  - deleted items, restoring, 15
    - Active Directory Recycle Bin, 12–13
  - AD DS (Active Directory Domain Services), 10
    - authoritative restore, 13–15
    - non-authoritative restore, 15
  - integration with other AD instances, 71
  - managing, 2–3
    - using Active Directory Domains and Trusts, 6
    - using AD sites and Services, 6
    - using AD Users and Computers, 5
    - using ADAC (Active Directory Administrative Center), 3–4
  - Password Protection, 82
- Azure AD Connect, 54–55
  - cloud sync, 67
  - installing, 58–63
  - requirements, 56–57
    - deployment account, 57–58
    - SQL Server, 57
  - synchronization, 65–67
- Azure AD DS
  - deploying, 68–70
  - domain join, 70
  - integration with other AD instances, 71
  - managing, 68
- Azure App Service Hybrid Connections, 230–231
- Azure Arc, 114
  - connecting to Windows Server instances, 115–116
  - deployment, 115–116
  - functionality, 114–115
- Azure Automation
  - Hybrid Runbook Worker, 123–124
  - runbooks, 123
  - State Configuration, 124
- Azure Bastion, connecting to IaaS VMs, 178
- Azure DNS, integrating with Windows Servers DNS, 193–194
- Azure ExpressRoute, 228–229
- Azure Extended Network, 219–220
- Azure File Sync, 233
  - cloud endpoints, creating, 235
  - cloud tiering, 237
  - migrating DFS to, 234–239
  - monitoring, 234–238
  - server endpoints, creating, 236

- server registration, 235–236
- storage sync service, deploying, 234
- sync groups, creating, 234–235
- Azure Monitor, 120
  - agent, 121
  - Azure File Sync and, 234–238
  - data collection, 120
  - installing, 121
  - Log Analytics workspace, 120
- Azure Network Adapter, 219
- Azure Policy guest configuration, 116–117
- Azure Relay, 227–228
- Azure Serial Console, connecting to IaaS VMs, 179
- Azure Virtual WAN, 229

## B

- backup and restore, 10–12
  - Active Directory Recycle Bin, 12–13
  - AD DS (Active Directory Domain Services), 10
  - authoritative restore, 13–15
  - checkpoints and, 137
  - GPOs, 84–85
  - non-authoritative restore, 15
- bandwidth management, Hyper-V, 155
- basic disks, 252
- BranchCache, 247–248

## C

- checkpoints, 136–137, 153
- cloning, virtual domain controllers, 16
- cloud endpoints, creating, 235
- Cloud Shell, 122
- cloud sync, 67
- cloud tiering, 237
- cmdlets, 3
  - Add-Clusternode, 257
  - Add-Computer, 52
  - Add-DhcpServer4Filter, 209
  - Add-DHCPsServer4Scope, 205
  - Add-DHCPsServer6Scope, 205
  - Add-DhcpServerv4SuperScope, 206
  - Add-DNSPrimaryZone, 189
  - Add-DnsServerConditionalForwarderZone, 193
  - Add-DNSServerDirectoryPartition, 187
  - Add-DnsServerPrimaryZone, 187

- Add-DNSServerQueryResolutionPolicy, 199
- Add-DNSServerSecondaryZone, 188
- Add-DnsServerStubZone, 193
- Add-DnsServerZoneDelegation, 190
- ADDomainMode, 19
- Add-VMAssignableDevice, 134
- checkpoint-related, 136–137
- DNSServerCache, 197
- Enable-PSRemoting, 106–107, 129
- Enter-PSSession, 107, 129, 130
- Get-ADTrust, 34
- Get-Command-Module <modulename>, 106
- Get-NetAdapter, 131
- Get-PSSessionConfigurationFile, 113
- Get-SRPartnership, 260
- Get-StoragePool, 254
- getting help with, 106
- GPO management, 84
- Install-ADDSForest, 9
- Install-ADServiceAccount, 49
- Invoke-Command, 108
- Move-ADDirectoryServer, 40
- New-ADDCCloneConfig, 16
- New-ADReplicationSiteLink, 40
- New-ADReplicationSubnet, 38
- New-AzADServicePrincipal, 115–116
- New-NetNAT, 131
- New-StorageQosPolicy, 262
- New-VMSSwitch, 131
- Register-PSSessionConfiguration, 113
- Set-ADComputer, 50
- Set-ADForestMode, 20
- Set-ADObject, 9
- Set-DhcpServerv4DnsSetting, 207
- Set-PhysicalDisk, 254
- Set-SRPartnership, 260
- Test-SRTopology, 259
- Uninstall-ADDSDomainController, 21
- commands
  - Docker, 160
  - docker load, 166
  - docker rmi, 166
  - docker run, 167, 169
  - docker save, 166
  - docker tag, 166
  - get-credential, 107
  - netdom trust, 34
- compliance, Windows update, 119
- computer accounts, 47

## conditional forwarders

- conditional forwarders, 193
- conflict resolution, 43
- connection request policies, 220
  - creating, 224
  - default, 223–224
  - Realm and RADIUS attributes, 223
- consoles, 2–3
  - Active Directory Domains and Trusts, 6
  - Active Directory Sites and Services, 6
  - Active Directory Users and Computers, 5
    - Delegation of Control Wizard, 5
    - tasks, 5
    - View Advanced Features function, 5
  - ADAC (Active Directory Administrative Center), 3
    - Powershell and, 3
    - search functionality, 3–4
- constrained delegation, 108
- container(s), 158. *See also* Docker
  - host, 159
  - Hyper-V isolation, 160
  - image dependency, 159
  - images, 158–159
    - creating, 171–172
    - managing, 166
    - updating, 165–166
    - Windows Server, 163–164
  - instance, 159, 167–168
  - modifying, 168
  - networking, 168–169
    - Layer 2 Bridge mode, 171
    - NAT, 169–170
    - transparent mode, 170
  - process isolation, 160
  - registries, 159, 163
  - sandbox, 159
  - Windows, service accounts, 164–165
- continuous delivery, IaaS VMs and, 176
- copying, VMs, 153
- core scheduler, Hyper-V, 135–136
- CPU groups, 135
- creating
  - Azure File Sync endpoints, 236
  - cloud endpoints, 235
  - connection request policies, 224
  - container images
    - from a container, 171
    - using Dockerfiles, 171–172
  - container instance, 167–168
  - GPOs, 86–87

- network policies, 225–227
- shared folders, 240
- site links, 39–40
- sites, 37–38
- sync groups, 234–235
- CSVs (Cluster Shared Volumes), 143

## D

- DANE (DNS-based Authentication of Named Entities), 198
- data disks, 174
- DDA (Discrete Device Assignment), 133–134
- decommissioning RODCs, 26–27
- deduplication, 152, 260–261
- defragmentation, Active Directory database, 20–21
- delegation, 108
- Delegation of Control Wizard, Active Directory Users and Computers, 5
- deployment
  - Azure Arc, 115–116
  - domain controller, 6–7
    - global catalog servers, 9–10
    - Server Core, 8–9
    - virtualized, 9
  - IPAM, 200
  - Windows updates, 118–119
- detached clusters, 143–144
- DFS (Distributed File System), 248
  - namespace, 249–250
  - replication, 234–239, 250
    - groups, 250–251
    - replicated folders and targets, 250
    - schedules, 251
- DHCP (Dynamic Host Configuration Protocol)
  - failover, 209
  - filtering, 208–209
  - name protection, 207
  - policies, 208
  - relay, 207–208
  - scopes, 204–206
    - multicast, 206
    - split, 207
    - super, 206
  - server options, 205–206
  - server role, deploying, 203–204
- differencing disks, 149
- DirectAccess, 216

- NLS (Network Location Server), 218–219
  - server, 217–218
  - topologies, 216–217
- Directory Services Restore Mode, authoritative restore, 14–15
- disks. *See also* storage
  - basic, 252
  - dynamic, 252
  - partitions, 252
  - thin-provisioned, 254–255
- DNS (Domain Name System), 186, 188, 192. *See also* IPAM
  - cache locking, 197
  - conditional forwarders, 193
  - DANE (DNS-based Authentication of Named Entities), 198
  - forwarders, 192–193
  - netmask ordering, 197
  - policies, 199
  - records
    - alias (CNAME), 191
    - host, 190
    - MX (mail exchanger), 191
    - pointer, 191
    - resource, 190, 194–195
    - unknown, 191
  - recursion, 197
  - response rate limiting, 198
  - scavenging, 192
  - socket pool, 196
  - spoofing, 196
  - Windows Server, event logs, 196
  - zone(s)
    - Active Directory-integrated, 186–187
    - aging, 191–192
    - delegation, 190
    - GlobalNames, 189–190
    - reverse lookup, 188–189
    - secondary, 188
    - stub, 193
- DNSSEC (Domain Name System Security Extensions), 194–195
- DNSServerCache cmdlet, 197
- Docker, 160
  - commands, 160
  - daemon.json file, 161–163
  - installing, 160–161
- docker load command, 166
- docker rmi command, 166
- docker run command, 167, 169
- docker save command, 166
- docker tag command, 166
- Dockerfiles, 171–172
- domain controllers, 1–2
  - deploying, 6–7
  - domain names and, 6–7
  - FMSO roles, 26–27
    - domain naming master, 27
    - infrastructure master, 28
    - PDC emulator, 28
    - RID master, 28
    - schema master, 27
    - seizing, 29
  - global catalog servers, 9–10
  - installing, from media, 8
  - KCC (Knowledge Consistency Checker), 42
  - moving, 40
  - physical security, 24
  - read-only, 24
    - decommissioning, 26–27
    - local administrators, 26
    - password replication, 24–25
    - replication, 43–44
  - Server Core deployment, 8–9
  - USNs (update sequence numbers), 43
  - virtual, 9, 16, 23
- domain local groups, 48
- domain(s), 16–17
  - computer accounts and, 47
  - forests, 17–18, 19–20
  - functional levels, 19
  - joining, 70
  - trees, 17, 18
  - trust(s), 30
    - direction, 30–31
    - external, 32
    - forest, 31–32
    - name suffix routing, 35
    - netdom.exe and, 34
    - realm, 33
    - shortcut, 32
    - SID filtering, 34–35
    - transitivity, 29
- DSC (Desired State Configuration), 124
- dynamic
  - disks, 252
  - memory, 131, 132
  - quorum, 142
- Dynamic Virtual Machine Queue, 156

## E

- editing, GPOs, 87
- Enable-PSRemoting cmdlet, 106–107, 129
- encryption
  - laaS VMs, 175
  - NPS and, 224–225
- endpoints
  - Azure File Sync, creating, 236
  - cloud, 235
  - JEA, 109, 112–113
- Enhanced Session Mode, 130
- Enter-PSSession cmdlet, 107, 129, 130
- ESAE (Enhanced Security Administrative Environment), forests, 20
- event logs, DNS, 196
- exporting, VMs, 153
- extensions
  - Azure VM, 117–118
  - Extended Network, 220
  - WAC (Windows Admin Center), 104
- external switches, 157
- external trusts, 32

## F

- failover
  - clustering, 140
    - Active Directory detached clusters, 143–144
    - cluster networking, 142–143
    - cluster node weight, 142
    - cluster quorum, 141
    - Cluster Shared Volumes, 143
    - dynamic quorum, 142
    - Force Quorum Resiliency, 143
    - guest clusters, 145–147
    - host cluster storage, 140
    - preferred owner and failover settings, 144
    - VM drain on shutdown, 144–145
    - VM Network Health Detection, 144
  - DHCP, 209
  - replica, 139–140
- fan-out administration, 107
- FAT/FAT32, 265
- file classification, 245–246
- file screen(s), 241
  - file groups and, 241–242
  - templates, 243

- filesystems
  - FAT/FAT32, 265
  - NTFS, 263–264
  - ReFS, 264–265
- fine-grained password policies, 76–77
- FMSO roles, 26–27
  - domain naming master, 27
  - infrastructure master, 28
  - PDC emulator, 28
  - RID master, 28
  - seizing, 29
- forests, 16, 19–20
  - authentication and, 18
  - ESAE (Enhanced Security Administrative Environment), 20
  - multi-domain, 17–18
  - trusts and, 31–32
- forwarders, 192–193
- FSRM (File Server Resource Manager)
  - access-denied assistance, 247
  - file classification, 245–246
  - file management tasks, 246
  - quotas, 243–244
  - storage reports, 244–245

## G

- gateway server, 103
- Generation 2 VMs, 128–129
- Get-ADTrust cmdlet, 34
- Get-Command-Module <modulename> cmdlet, 106
- get-credential command, 107
- Get-NetAdapter cmdlet, 131
- Get-PSSessionConfigurationFile cmdlet, 113
- Get-SRPartnership cmdlet, 260
- Get-StoragePool cmdlet, 254
- global catalog servers, 9–10
- global groups, 48
- GlobalNames zones, 189–190
- GMSAs (group managed service accounts), 48, 49–50, 164–165
- GPMC (Group Policy Management Console), 83–85
- Group Policy, 83, 95, 247. *See also* AGPM (Advanced Group Policy Management)
  - Administrative template, 92–93
  - caching, 91
  - DNSSEC and, 195
  - forced update, 91–92



- GPOs
    - backing up, 84–85
    - creating, 86–87
    - editing, 87
    - import and copy, 85
    - linking, 87
    - managing, 83–85, 86
    - troubleshooting, 85–86
  - loopback processing, 90–91
  - Modeling Wizard, 87
  - policy enforcement and blocking, 88–89
  - preferences, 93–94
  - Results, 88
  - security filtering, 89–90
  - WMI filters, 88, 90
  - groups, 47
    - domain local, 48
    - global, 48
    - universal, 47
  - guest clusters, 145
    - shared virtual hard disk, 146
    - storage, 145–146
    - VHD Sets, 147
- ## H
- high availability
    - DHCP, 209
    - Hyper-V failover clusters, 140
      - Active Directory detached clusters, 143–144
      - cluster networking, 142–143
      - cluster node weight, 142
      - cluster quorum, 141
      - Cluster Shared Volumes, 143
      - dynamic quorum, 142
      - Force Quorum Resiliency, 143
      - host cluster storage, 140
      - preferred owner and failover settings, 144
      - VM drain on shutdown, 144–145
      - VM Network Health Detection, 144
    - Hyper-V guest clusters, 145
      - shared virtual hard disk, 146
      - storage, 145–146
      - VHD Sets, 147
    - Hyper-V live migration, 147–148
    - Hyper-V Replica, 137–138
      - Broker, 139–140
      - configuring replica servers, 138
      - configuring VM replicas, 138–139
      - replica failover, 139–140
      - configuring VM replicas, 138–139
      - replica failover, 139–140
  - host records, 190
  - HVC.exe, VM management, 130
  - hybrid workloads, Azure Automation and, 123–124
  - Hyper-V, 127, 128
    - checkpoints, 136–137
    - CPU groups, 135
    - Enhanced Session Mode, 130
    - failover clusters, 140
      - Active Directory detached clusters, 143–144
      - cluster networking, 142–143
      - cluster node weight, 142
      - cluster quorum, 141
      - Cluster Shared Volumes, 143
      - dynamic quorum, 142
      - Force Quorum Resiliency, 143
      - host cluster storage, 140
      - preferred owner and failover settings, 144
      - VM drain on shutdown, 144–145
      - VM Network Health Detection, 144
    - guest clusters, 145
      - shared virtual hard disk, 146
      - storage, 145–146
      - VHD Sets, 147
    - integration services, 133
    - isolation, 160
    - live migration, 147–148
    - nested virtualization, 130–131
      - dynamic memory, 131
      - networking, 131
    - network adapter
      - network isolation, 155
      - NIC teaming, 156
      - VM MAC address and, 154–155
    - optimizing network performance, 155
      - bandwidth management, 155
      - Dynamic Virtual Machine Queue, 156
      - SR-IOV, 155–156
    - Replica, 137–138
      - Broker, 139–140
      - configuring replica servers, 138
      - configuring VM replicas, 138–139
      - failover, 139–140
    - scheduling types, 135–136
    - smart paging, 132–133
    - storage optimization
      - deduplication, 152
      - storage migration, 152–153
      - storage tiering, 152

## Hyper-V

- virtual hard disks
  - differencing disks, 149
  - dynamically expanding disks, 149
  - fixed-size disks, 149
  - formats, 148
  - modifying, 150
  - pass-through disks, 150–151
  - Storage QoS, 151
  - Virtual Fibre Channel adapters, 151
- virtual switches, 156
  - external, 157
  - internal, 157
  - private, 157

## I

- laaS VMs, 173
  - configuring continuous delivery, 176
  - connecting
    - with Azure AD account, 176–177
    - JIT access, 178
    - with Remote PowerShell, 177–178
    - using Azure Bastion, 178
    - using Azure Serial Console, 179
    - using Windows Admin Center, 178
  - data disks, 174
  - encryption, 175
  - images, 174
  - IP addressing, 180–181
  - managing, 122–123
  - NSGs and, 181
  - RBAC roles, 173–174
  - resizing, 175–176
  - shared disks, 174
  - snapshots, 175
  - virtual networks, 179–180, 181
- identities, hybrid, 54
- IKEv2, 214–215
- importing, VMs, 153
- inactive accounts, 82
- infrastructure master, 28
- Install-ADDSForest cmdlet, 9
- Install-ADServiceAccount cmdlet, 49
- installing
  - Azure AD Connect, 58–63
  - Azure Monitor, 121
  - BranchCache, 247
  - Docker, 160–161
  - domain controllers, 8
  - WAC (Windows Admin Center), 103–104
- integration services, 133
- internal switches, 157
- intra-forest authentication, 18
- Invoke-Command cmdlet, 108
- IP addressing
  - laaS VMs and, 180–181
  - reservations, 208
  - troubleshooting, 204
- IPAM, 200
  - administration, 201–202
  - deployment, 200
  - IP address
    - space management, 202
    - tracking, 202–203
  - server discovery, 201
- IPsec, 215

## J

- JEA (Just Enough Administration), 109
  - endpoints, 112–113
  - role-capability files, 110–111
  - session-configuration files, 111–112
- JIT (Just-in-Time) VM access, 178
- joining
  - domains, 70
  - Windows Server to an Active Directory instance, 52–53
- jump servers, 101

## K

- KCC (Knowledge Consistency Checker), 42
- Kerberos
  - delegation, 50, 108
  - policies, 51–52
  - SPNs (service principal names), 52

## L

- L2TP, 215
- LAN routing, 215
- Layer 2 Bridge networks, 171

linking GPOs, 87  
 Linux  
   integration services, 133  
   VMs (virtual machines), HVC.exe and, 130  
 live migration, 147–148  
 local administrators, RODC, 26  
 Local Service (NT AUTHORITY\LocalService) account, 48  
 Local System (NT AUTHORITY\SYSTEM) account, 48  
 lockout policies, 79, 81  
 Log Analytics, integrating with Windows Servers, 120–121

## M

MAC address, VM, 153–154  
 managing. *See also* administration tools  
   AD DS passwords, 74–75  
   Azure AD, 2–3  
     using Active Directory Domains and Trusts, 6  
     using AD sites and Services, 6  
     using AD Users and Computers, 5  
     using ADAC (Active Directory Administrative Center), 3–4  
   container images, 166  
   GMSAs (group managed service accounts), 49  
   IaaS VMs, 122–123  
   VMs  
     using HVC.exe, 130  
     using PowerShell Direct, 130  
     using PowerShell remoting, 129  
   Windows Server instances, 113–116  
   Windows updates, 119  
 memory  
   dynamic, 132  
   nested virtualization and, 131  
   smart paging and, 132–133  
   Startup, 132–133  
 Microsoft Defender for Cloud, integrating with Windows Servers, 121–122  
 Microsoft Exchange Server, 2  
 modifying  
   containers, 168  
   virtual hard disks, 150  
 modules, PowerShell, 106  
 monitoring  
   Azure File Sync, 234–238  
   replication, 44  
 Move-ADDirectoryServer cmdlet, 40  
 moving, domain controllers, 40  
 multi-domain forests, 17–18  
 multi-master replication, 42  
 MX (mail exchanger) records, 191

## N

name suffix routing, 35  
 NAT (network address translation), 169–170, 216  
 nested resiliency, 256  
 nested virtualization, 130–131  
   dynamic memory, 131  
   networking, 131  
 netdom trust command, 34  
 netdom.exe, 34  
 network adapters, Hyper-V  
   network isolation, 155  
   NIC teaming, 156  
   VM MAC address and, 153–154  
 Network Service (NT AUTHORITY\NetworkService) account, 49  
 networking, containers, 168–169  
   Layer 2 Bridge mode, 171  
   NAT, 169–170  
   transparent mode, 170  
 New-ADDCCloneConfig cmdlet, 16  
 New-ADReplicationSiteLink cmdlet, 40  
 New-ADReplicationSubnet cmdlet, 38  
 New-AzADServicePrincipal cmdlet, 115–116  
 New-NetNAT cmdlet, 131  
 New-StorageQosPolicy cmdlet, 262  
 New-VMSwitch cmdlet, 131  
 NIC teaming, 156  
 NLS (Network Location Server), 218–219  
 non-authoritative restore, 15  
 non-Azure machines, deploying Azure services on, 117–118  
 nonexpiring passwords, 80–81  
 NPS (Network Policy Server), 211, 220, 221. *See also*  
 RADIUS servers  
   authentication, 223  
   connection request forwarding, 222  
   connection request policies, 220  
     default, 223–224  
     Realm and RADIUS attributes, 223  
   encryption, 224–225  
   IP filters, 224  
   IP settings, 225

## NPS (Network Policy Server)

- network policies, creating, 225–227
- policy conditions, 221–222
- templates, 227
- NSGs (network security groups), IaaS VMs and, 181
- ntdsutil.exe, 21
  - metadata cleanup, 21
  - snapshots, 22
- NTFS, 263–264

## O-P

- one-to-many remoting, 107
- one-way trust, 6
- partitions, 41, 252
- pass-through authentication, 74
- disks, 150–151
- password(s)
  - DSRM (Directory Services Restore Mode), 7–8
  - lockout settings, 79
  - managing, 74–75
  - nonexpiring, 80–81
  - policies, 75, 76, 78–79
  - protection, 82
  - replication, 24–25
  - settings permissions, 76
  - synchronization, 73–74
- PAWs (Privileged Access Workstations), 100–101
- PDC emulator, 28
- permissions, 201–202
  - NTFS, 263–264
  - password, 76
  - Windows update deployment, 119
- physical security, domain controllers and, 24
- pointer records, 191
- policy(ies). *See also* Group Policy
  - BranchCache, 247–248
  - conditions, 221–222
  - connection request, 220
    - creating, 224
    - default, 223–224
    - Realm and RADIUS attributes, 223
  - DHCP, 208
  - DNS, 199
  - Kerberos, 51–52
  - lockout, 79, 81
  - network, creating, 225–227
  - password, 75, 76, 78–79

## PowerShell

- cmdlets, 3
  - Add-Clusternode, 257
  - Add-Computer, 52
  - Add-DhcpServer4Filter, 209
  - Add-DHCPServer4Scope, 205
  - Add-DHCPServer6Scope, 205
  - Add-DhcpServerv4SuperScope, 206
  - Add-DNSPrimaryZone, 189
  - Add-DnsServerConditionalForwarderZone, 193
  - Add-DNSServerDirectoryPartition, 187
  - Add-DnsServerPrimaryZone, 187
  - Add-DNSServerQueryResolutionPolicy, 199
  - Add-DNSServerSecondaryZone, 188
  - Add-DnsServerStubZone, 193
  - Add-DnsServerZoneDelegation, 190
  - ADDomainMode, 19
  - Add-VMAssignableDevice, 134
  - checkpoint-related, 136–137
  - DNSServerCache, 197
  - Enable-PSRemoting, 106–107, 129
  - Enter-PSSession, 107, 129, 130
  - Get-ADTrust, 34
  - Get-Command-Module <modulename>, 106
  - Get-NetAdapter, 131
  - Get-PSSessionConfigurationFile, 113
  - Get-SRPartnership, 260
  - Get-StoragePool, 254
  - getting help with, 106
  - GPO management, 84
  - Install-ADDSForest, 9
  - Install-ADServiceAccount, 49
  - Invoke-Command, 108
  - Move-ADDirectoryServer, 40
  - New-ADDCCloneConfig, 16
  - New-ADReplicationSiteLink, 40
  - New-ADReplicationSubnet, 38
  - New-AzADServicePrincipal, 115–116
  - New-NetNAT, 131
  - New-StorageQosPolicy, 262
  - New-VMSwitch, 131
  - Register-PSSessionConfiguration, 113
  - Set-ADComputer, 50
  - Set-ADForestMode, 20
  - Set-ADObject, 9
  - Set-DhcpServerv4DnsSetting, 207
  - Set-PhysicalDisk, 254
  - Set-SRPartnership, 260

- Test-SRTopology, 259
- Uninstall-ADDSDomainController, 21
- Direct, VM management, 130
- Gallery, 106
- GMSA management, 49
- JEA (Just Enough Administration), 109
  - endpoints, 112–113
  - role-capability files, 110–111
  - session-configuration files, 111–112
- modules, 106
- remoting, 106–108
  - laaS VMs and, 177–178
  - VM management, 129
- WAC (Windows Admin Center) and, 104–105
- PPTP (Point-to-Point Tunneling Protocol), 215
- private switches, 157
- Process Automation, 123
- process isolation, 160
- protocols, VPN, 214
  - IKEv2, 214–215
  - L2TP/IPsec, 215
  - PPTP, 215
  - SSTP, 215
- PSOs (Password Settings Object), 77–78
- replicated folders and targets, 250
- schedules, 251
  - managing and monitoring, 44
  - RODC, 43–44
  - triggering, 44
- reservations, 208
- resiliency
  - nested, 256
  - storage space, 253
  - Storage Spaces Direct, 256–257
- resizing, laaS VMs, 175–176
- resource
  - groups, 134–135
  - records, 190, 194–195
- restoring. *See* backup and restore
- Resultant Set of Policy tool, 92
- RID (Relative ID) master, 28
- RODCs (read-only domain controllers), 24, 187
  - decommissioning, 26–27
  - local administrators, 26
  - password replication, 24–25
  - replication, 43–44
- role-capability files, 110–111
- RSO (replicate-single-object) operation, 43–44
- runbooks, 123

## Q-R

- quotas, FSRM (File Server Resource Manager), 243–244
- RADIUS servers, 211
  - accounting, 212–213
  - clients, 211–212
  - proxies, 211
- RBAC (remote-based access control), 109, 173–174
- realm trusts, 33
- ReFS (Resilient File System), 264–265
- Register-PSSessionConfiguration cmdlet, 113
- registration, Azure File Sync server, 235–236
- Remote Access role service, 210
- Remote Desktop, 2, 101–102, 130
- RemoteFX, 134
- repadmin tool, 44
- replication
  - AD DS, 41
    - KCC (Knowledge Consistency Checker), 42
    - multi-master, 42
  - conflict resolution, 43
  - DFS, 250
    - groups, 250–251

## S

- sandbox, 159
- scavenging, 192
- scheduling, Hyper-V, 135–136
- schema master, 27
- search functionality, ADAC (Active Directory Administrative Center), 3–4
- secondary zones, 188
- second-hop remoting, 108
- security
  - DNS (Domain Name System), 196
    - cache locking, 197
    - DANE (DNS-based Authentication of Named Entities), 198
    - netmask ordering, 197
    - policies, 199
    - recursion, 197
    - response rate limiting, 198
    - socket pool, 196
  - DNSSEC (Domain Name System Security Extensions), 194–195

## security

- Group Policy and, 89–90
  - physical, domain controllers, 24
- seizing FMSO roles, 29
- Server Core deployment, 8–9
- service accounts, 48, 164–165
- session-configuration files, 111–112
- Set-ADComputer cmdlet, 50
- Set-ADForestMode cmdlet, 20
- Set-ADObject cmdlet, 9
- Set-DhcpServerv4DnsSetting cmdlet, 207
- Set-PhysicalDisk cmdlet, 254
- SetSPN utility, 52
- Set-SRPartnership cmdlet, 260
- shared disks, 174
- shared folders, 239–241. *See also* BranchCache
- shortcut trusts, 32
- SID filtering, 34–35
- site(s), 35–37, 39–40
  - creating, 37–38
  - link bridges, 40
  - subnets, creating, 38
- site-to-site VPN, 228
- smart paging, 132–133
- SMB Direct, 261–262
- SMTP (Simple Mail Transfer Protocol), reverse lookup zones and, 189
- snapshots, 22, 175
- SPNs (service principal names), 52
- spoofing, 196
- SR-IOV (Single-Root I/O Virtualization), 155–156
- SSTP (Secure Socket Tunneling Protocol), 214–215
- State Configuration, 124
- storage
  - disks
    - basic, 252
    - dynamic, 252
    - partitions, 252
    - thin-provisioned, 254–255
  - guest cluster, 145–146
  - Hyper-V
    - deduplication, 152
    - tiering, 152
  - migration, 152–153
  - pools, 253
  - reports, 244–245
  - space, 253
    - resiliency, 253
    - tiering, 254
  - trim, 255

- Storage QoS, 151, 262–263
- Storage Replica, 257–258
  - requirements, 259–260
  - supported configurations, 258–259
- Storage Spaces Direct, 255
  - cluster nodes, 257
  - deployment options, 256
  - nested resiliency, 256
  - properties, 255–256
  - resiliency types, 256–257
- store and forward replication, 42
- stub zones, 193
- subnets, 38
- synchronization, password, 73–74

## T

- tasks, Active Directory Users and Computers, 5
- templates
  - Administrative, 92–93
  - ARM (Azure Resource Manager), 53
  - file screen, 243
  - NPS, 227
  - quota, 244
- Test-SRTopology cmdlet, 259
- thin provisioning, 254–255
- tombstone lifetime, 10–12
- tombstone reanimation, 15
- tools. *See also* PowerShell
  - Azure AD Connect, 54–55
    - deployment account requirements, 57–58
    - Health, 72
    - installing, 58–63
    - requirements, 56–57
    - SQL Server requirements, 57
    - synchronization, 65–67
  - Cloud Shell, 122
  - repadmin, 44
  - Resultant Set of Policy, 92
  - SetSPN, 52
  - Validate-DCB, 143
  - Windows Server administration, 100
    - jump servers, 101
    - PAWs (Privileged Access Workstations), 100–101
    - remote access and, 100
    - Remote Desktop, 101–102
    - WAC (Windows Admin Center), 102–105

- topologies, DirectAccess, 216–217
- transitivity, trust, 30
- transparent networks, 170
- triggering, replication, 44
- trim, 255
- troubleshooting
  - GPOs, 85–86
  - IP address issues, 204
- Trust Anchor, 195
- trust(s), 6, 29, 30
  - direction, 30–31
  - external, 32
  - forest, 31–32
  - name suffix routing, 35
  - netdom.exe and, 34
  - realm, 33
  - shortcut, 32
  - SID filtering, 34–35
  - transitivity, 30
- two-way trust, 6

## U

- UGMC (universal group membership caching), 10
- Uninstall-ADDSDomainController cmdlet, 21
- universal groups, 47
- unknown records, 191
- updates, Windows, 118
  - compliance, 119
  - deploying, 118–119
  - managing permissions, 119
- UPN (user principal name) suffixes, 63–65
- user accounts, 45–46. *See also* password(s)
  - inactive, 82
  - locked-out, 81
  - lockout settings, 79
  - nonexpiring passwords, 80–81
  - UPN (user principal name) suffixes, 63–65
- USNs (update sequence numbers), 43

## V

- Validate-DCB tool, 143
- VHD Sets, 147
- virtual accounts, 50
- virtual domain controllers, 9, 16, 23

- virtual hard disks
  - differencing disks, 149
  - dynamically expanding disks, 149
  - fixed-size disks, 149
  - formats, 148
  - modifying, 150
  - pass-through disks, 150–151
  - Virtual Fibre Channel adapters, 151
- virtual switches, 156
  - external, 157
  - internal, 157
  - private, 157
- virtualization
  - Hyper-V, 127. *See also* Hyper-V
    - nested, 130–131
      - dynamic memory, 131
      - networking, 131
  - VLAN tagging, 155
- VMs (virtual machines). *See also* Hyper-V
  - checkpoints, 136–137
  - configuring replicas, 138–139
  - CPU groups, 135
  - DDA (Discrete Device Assignment), 133–134
  - dynamic memory, 132
  - Enhanced Session Mode, 130
  - exporting, 153
  - extensions, 117–118
  - Generation 2, 128–129
  - high availability, Hyper-V Replica, 137–140
  - laaS, 173
    - configuring continuous delivery, 176
    - connections to, 176–179
    - data disks, 174
    - encryption, 175
    - images, 174
    - IP addressing, 180–181
    - managing, 122–123
    - NSGs and, 181
    - RBAC roles, 173–174
    - resizing, 175–176
    - shared disks, 174
    - snapshots, 175
    - virtual networks, 179–180, 181
  - importing, 153
  - integration services, 133
  - live migration, 147–148
  - MAC address, 153–154
  - managing
    - using HVC.exe, 130

## VMs (virtual machines)

- using PowerShell Direct, 130
- using PowerShell remoting, 129
- nested virtualization, 130–131
  - dynamic memory, 131
  - networking, 131
- optimizing network performance, 155
  - bandwidth management, 155
  - Dynamic Virtual Machine Queue, 156
  - SR-IOV, 155–156
- resource groups, 134–135
- smart paging, 132–133

## VPN

- authentication, 213–214
- Docker, 1
- IaaS virtual networks and, 181
- protocols, 214
  - IKEv2, 214–215
  - L2TP/IPsec, 215
  - PPTP, 215
  - SSTP, 215
- server configuration, 213
- site-to-site, 228

## W

- WAC (Windows Admin Center), 102–103
  - configuring a target machine, 105
  - extensions, 104
  - installing, 103–104
  - managing Azure hybrid services, 105
  - showing PowerShell source code, 104–105
- Web Application Proxy, 227
- Windows Admin Center, 2, 3, 178
- Windows Server, 124
  - administration tools, 100
    - jump servers, 101
  - PAWs (Privileged Access Workstations), 100–101
  - remote access and, 100
  - Remote Desktop, 101–102
  - WAC (Windows Admin Center), 102–105
- Azure VM extensions, 117–118
- Backup, 10
- checkpoints, 136
- container(s)
  - images, 163–164
  - service accounts, 164–165

DHCP (Dynamic Host Configuration Protocol) server role, deploying, 203–204

- DNS, 196
  - cache locking, 197
  - DANE (DNS-based Authentication of Named Entities), 198
  - event logs, 196
  - netmask ordering, 197
  - policies, 199
  - recursion, 197
  - response rate limiting, 198
  - socket pool, 196
- IaaS VMs, managing, 122–123
- integration
  - with Azure DNS private zones, 193–194
  - with Log Analytics, 120–121
  - with Microsoft Defender for Cloud, 121–122
- joining to an Active Directory instance, 52–53
- LAN routing, 215
- managing, 113–116
- NPS, 220, 221

- authentication, 223
- connection request forwarding, 222
- connection request policies, 220, 223–224
- encryption, 224–225
- IP settings, 225
- network policies, creating, 225–227
- policy conditions, 221–222
- templates, 227
- RemoteFX, 134
- shared folders, 239–241
- updates, 118
  - compliance, 119
  - deploying, 118–119
  - managing permissions, 119

## X-Y-Z

- zone(s)
  - Active Directory-integrated, 186–187
  - aging, 191–192
  - delegation, 190
  - GlobalNames, 189–190
  - reverse lookup, 188–189
  - secondary zones, 188
  - Trust Anchor, 195