

Microsoft[®] Official Academic Course

Mobility and Devices Fundamentals

Microsoft Technology Associate EXAM 98-368



Microsoft® Official Academic Course

Mobility and Devices Fundamentals, Exam 98-368



VP & DIRECTOR SENIOR DIRECTOR EXECUTIVE EDITOR DEVELOPMENT EDITOR ASSISTANT PROJECT MANAGER PROJECT SPECIALIST PROJECT ASSISTANT MARKETING MANAGER ASSISTANT MARKETING MANAGER ASSOCIATE DIRECTOR, PRODUCTION SENIOR CONTENT SPECIALIST PRODUCTION EDITOR COVER PHOTO CREDIT Laurie Rosatone Don Fowley Bryan Gambrel Jennifer Lartz Jessy Moor Gladys Soto Nichole Urban Anna Melhorn Dan Sayre Puja Katariwala Kevin Holm Nicole Repasky Arun Surendar © Captain Yeo/Shutterstock

This book was set in Garamond by SPi Global and printed and bound by Strategic Content Imaging.

Copyright © 2016 by John Wiley & Sons, Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc. 222 Rosewood Drive, Danvers, MA 01923, website www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, (201)748-6011, fax (201)748-6008, website http://www.wiley.com/go/permissions.

Microsoft, ActiveX, Excel, InfoPath, Microsoft Press, MSDN, OneNote, Outlook, PivotChart, PivotTable, PowerPoint, SharePoint, SQL Server, Visio, Visual Basic, Visual C#, Visual Studio, Windows, Windows 8.1, Windows Mobile, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/ or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

The book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, John Wiley & Sons, Inc., Microsoft Corporation, nor their resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

All photos in this book were printed with permission of the copyright owner. For all other third party photo provisions in the text, the copyright holders are indicated near the photo. The remaining photos were created by the authors of this textbook and printed with their permission.

ISBN 978-1-119-23955-0

Printed in the United States of America

www.wiley.com/college/microsoft

Preface

Welcome to the Microsoft Official Academic Course (MOAC) program for Mobility and Devices Fundamentals. MOAC represents the collaboration between Microsoft Learning and John Wiley & Sons, Inc. Microsoft and Wiley teamed up to produce a series of textbooks that deliver compelling and innovative teaching solutions to instructors and superior learning experiences for students. Infused and informed by in-depth knowledge from the creators of Microsoft products, and crafted by a publisher known worldwide for the pedagogical quality of its products, these textbooks maximize skills transfer in minimum time. Students are challenged to reach their potential by using their new technical skills as highly productive members of the workforce.

Because this knowledgebase comes directly from Microsoft, creator of the Microsoft Technology Associate (MTA) exams (www.microsoft.com/learning/certification), you are sure to receive the topical coverage that is most relevant to students' personal and professional success. Microsoft's direct participation not only assures you that MOAC textbook content is accurate and current; it also means that students will receive the best instruction possible to enable their success on certification exams and in the workplace.

The Microsoft Official Academic Course Program

The *Microsoft Official Academic Course* series is a complete program for instructors and institutions to prepare and deliver great courses on Microsoft software technologies. With MOAC, we recognize that, because of the rapid pace of change in the technology and curriculum developed by Microsoft, there is an ongoing set of needs beyond classroom instruction tools for an instructor to be ready to teach the course. The MOAC program endeavors to provide solutions for all these needs in a systematic manner in order to ensure a successful and rewarding course experience for both instructor and student—technical and curriculum training for instructor readiness with new software releases; the software itself for student use at home for building hands-on skills, assessment, and validation of skill development; and a great set of tools for delivering instruction in the classroom and lab. All are important to the smooth delivery of an interesting course on Microsoft software, and all are provided with the MOAC program. We think about the model below as a gauge for ensuring that we completely support you in your goal of teaching a great course. As you evaluate your instructional materials options, you may wish to use the model for comparison purposes with available products.



www.wiley.com/college/microsoft

Pedagogical Features

The MOAC textbook for Mobility and Devices Fundamentals is designed to cover all the learning objectives for MTA Exam 98-368, which are referred to as its "objective domains." The Microsoft Technology Associate (MTA) exam objectives are highlighted throughout the textbook. Many pedagogical features have been developed specifically for *Microsoft Official Academic Course* programs.

Presenting the extensive procedural information and technical concepts woven throughout the textbook raises challenges for the student and instructor alike. The Illustrated Book Tour that follows provides a guide to the rich features contributing to the *Microsoft Official Academic Course* program's pedagogical plan. Following is a list of key features in each lesson designed to prepare students for success as they continue in their IT education, on the certification exams, and in the workplace:

- Each lesson begins with an **Exam Objective Matrix**. More than a standard list of learning objectives, the Exam Objective Matrix correlates each software skill covered in the lesson to the specific exam objective domain.
- Concise and frequent **Step-by-Step** instructions teach students new features and provide an opportunity for hands-on practice. Numbered steps give detailed, step-by-step instructions to help students learn software skills.
- **Illustrations:** Screen images provide visual feedback as students work through the exercises. The images reinforce key concepts, provide visual clues about the steps, and allow students to check their progress.
- **Key Terms:** Important technical vocabulary is listed with definitions at the beginning of the lesson. When these terms are used later in the lesson, they appear in bold italic type and are defined. The Glossary contains all of the key terms and their definitions.
- Engaging point-of-use **Reader Aids**, located throughout the lessons, tell students why this topic is relevant (*The Bottom Line*), and provide students with helpful hints (*Take Note*). Reader Aids also provide additional relevant or background information that adds value to the lesson.
- **Certification Ready** features throughout the text signal students where a specific certification objective is covered. They provide students with a chance to check their understanding of that particular MTA objective and, if necessary, review the section of the lesson where it is covered. MOAC offers complete preparation for MTA certification.
- End-of-Lesson Questions: The Knowledge Assessment section provides a variety of multiple-choice, true-false, matching, and fill-in-the-blank questions.
- End-of-Lesson Exercises are projects that test students' ability to apply what they've learned in the lesson.

Conventions and Features Used in This Book

This book uses particular fonts, symbols, and heading conventions to highlight important information or to call your attention to special steps. For more information about the features in each lesson, refer to the Illustrated Book Tour section.

CONVENTION	Meaning
THE BOTTOM LINE	This feature provides a brief summary of the material to be covered in the section that follows.
CLOSE	Words in all capital letters indicate instructions for opening, saving, or closing files or programs. They also point out items you should check or actions you should take.
CERTIFICATION READY	This feature signals the point in the text where a specific certification objective is covered. It provides you with a chance to check your understanding of that particular MTA objective and, if necessary, review the section of the lesson where it is covered.
TAKE NOTE*	Reader aids appear in shaded boxes found in your text. <i>Take Note</i> provides helpful hints related to particular tasks or topics.
Xref	These notes provide pointers to information discussed elsewhere in the textbook or describe interesting gaming development features that are not directly addressed in the current topic or exercise.
Alt + Tab	A plus sign (+) between two key names means that you must press both keys at the same time. Keys that you are instructed to press in an exercise will appear in the font shown here.
Example	Key terms appear in bold italic.

Instructor Support Program

	The <i>Microsoft Official Academic Course</i> programs are accompanied by a rich array of resources that incorporate the extensive textbook visuals to form a pedagogically cohesive package. These resources provide all the materials instructors need to deploy and deliver their courses. Resources available online for download include:
	• DreamSpark Premium is designed to provide the easiest and most inexpensive developer tools, products, and technologies available to faculty and students in labs, classrooms, and on student PCs. A free 3-year membership is available to qualified MOAC adopters.
	<i>Note:</i> Microsoft Visual Studio, Windows Server, and Windows Operating Systems can be downloaded from DreamSpark Premium for use by students in this course.
	• The Instructor Guide contains Solutions to all the textbook exercises and Syllabi for various term lengths. The Instructor Guide also includes chapter summaries and lecture notes. The Instructor's Guide is available from the Book Companion site (http://www.wiley.com/college/microsoft).
	• The Test Bank contains hundreds of questions in multiple-choice, true-false, short answer, and essay formats, and is available to download from the Instructor's Book Companion site (www.wiley.com/college/microsoft). A complete answer key is provided.
	• A complete set of PowerPoint presentations and images is available on the Instructor's Book Companion site (http://www.wiley.com/college/microsoft) to enhance classroom presentations. Approximately 50 PowerPoint slides are provided for each lesson. Tailored to the text's topical coverage and Skills Matrix, these presentations are designed to convey key concepts addressed in the text. All images from the text are on the Instructor's Book Companion site (http://www.wiley.com/college/microsoft). You can incorporate them into your PowerPoint presentations, or create your own overhead transparencies and handouts. By using these visuals in class discussions, you can help focus students' attention on key elements of technologies covered and help them understand how to use it effectively in the workplace.
Wiley Faculty Network	• When it comes to improving the classroom experience, there is no better source of ideas and inspiration than your fellow colleagues. The Wiley Faculty Network connects teachers with technology, facilitates the exchange of best practices, and helps to enhance instructional efficiency and effectiveness. Faculty Network activities include technology training and tutorials, virtual seminars, peer-to-peer exchanges of experiences and ideas, personal consulting, and sharing of resources. For details visit www.WhereFacultyConnect.com.

DREAMSPARK PREMIUM—FREE 3-YEAR MEMBERSHIP AVAILABLE TO QUALIFIED ADOPTERS!

DreamSpark Premium is designed to provide the easiest and most inexpensive way for universities to make the latest Microsoft developer tools, products, and technologies available in labs, classrooms, and on student PCs. DreamSpark Premium is an annual membership program for departments teaching Science, Technology, Engineering, and Mathematics (STEM) courses. The membership provides a complete solution to keep academic labs, faculty, and students on the leading edge of technology.

Software available in the DreamSpark Premium program is provided at no charge to adopting departments through the Wiley and Microsoft publishing partnership.

Contact your Wiley rep for details.

For more information about the DreamSpark Premium program, go to:

https://www.dreamspark.com/

Note: Microsoft Visual Studio, XNA Game Studio, and Windows Operating Systems can be downloaded from DreamSpark Premium for use by students in this course.

Important Web Addresses and Phone Numbers

To locate the Wiley Higher Education Rep in your area, go to http://www.wiley.com/ college and click on the "*Who's My Rep?*" link at the top of the page.

To learn more about becoming certified and exam availability, visit www.microsoft.com/ learning/mcp/mcp.

Student Support Program

Additional Resources

Book Companion Website (www.wiley.com/college/microsoft)

The students' book companion site for the MOAC series includes any resources, exercise files, and Web links that will be used in conjunction with this course.

Wiley E-Text

Wiley MOAC E-Texts are innovative, electronic versions of printed textbooks. Students buy the e-text version for up to 40% off the U.S. price of the printed text, and get the added value of permanence and portability. Wiley E-Texts provide students with numerous additional benefits that are not available with other e-text solutions.

Wiley E-Texts are NOT subscriptions; students download the Wiley E-Text to their computer desktops. Students own the content they buy to keep for as long as they want. Once a Wiley E-Text is downloaded to the computer desktop, students have instant access to all of the content without being online. Students can also print out the sections they prefer to read in hard copy. Students also have access to fully integrated resources within their Wiley E-Text. From highlighting their e-text to taking and sharing notes, students can easily personalize their Wiley E-Text as they are reading or following along in class.

About the Microsoft Technology Associate (MTA) Certification

Preparing Tomorrow's Technology Workforce

Technology plays a role in virtually every business around the world. Possessing the fundamental knowledge of how technology works and understanding its impact on today's academic and workplace environment is increasingly important—particularly for students interested in exploring professions involving technology. That's why Microsoft created the Microsoft Technology Associate (MTA) certification—a new entry-level credential that validates fundamental technology knowledge among students seeking to build a career in technology.

The Microsoft Technology Associate (MTA) certification is the ideal and preferred path to Microsoft's world-renowned technology certification programs. MTA is positioned to become the premier credential for individuals seeking to explore and pursue a career in technology, or augment related pursuits such as business or any other field where technology is pervasive.

MTA Candidate Profile

The MTA certification program is designed specifically for secondary and post-secondary students interested in exploring academic and career options in a technology field. It offers

students a certification in basic IT and development. As the new recommended entry point for Microsoft technology certifications, MTA is designed especially for students new to IT and software development. It is available exclusively in educational settings and easily integrates into the curricula of existing computer classes.

MTA Empowers Educators and Motivates Students

MTA provides a new standard for measuring and validating fundamental technology knowledge right in the classroom while keeping your budget and teaching resources intact. MTA helps institutions stand out as innovative providers of high-demand industry credentials and is easily deployed with a simple, convenient, and affordable suite of entry-level technology certification exams. MTA enables students to explore career paths in technology without requiring a big investment of time and resources, while providing a career foundation and the confidence to succeed in advanced studies and future vocational endeavors.

In addition to giving students an entry-level Microsoft certification, MTA is designed to be a stepping stone to other, more advanced Microsoft technology certifications.

To learn more about becoming a Microsoft Technology Associate and exam availability, visit www.microsoft.com/learning/mta.

MOAC MTA Technology Fundamentals Reviewers

We'd like to thank the many reviewers who pored over the manuscript and provided invaluable feedback in the service of quality instructional materials:

Yuke Wang, University of Texas at Dallas Palaniappan Vairavan, Bellevue College Harold "Buz" Lamson, ITT Technical Institute Colin Archibald, Valencia Community College Catherine Bradfield, DeVry University Online Robert Nelson, Blinn College Kalpana Viswanathan, Bellevue College Bob Becker, Vatterott College Carol Torkko, Bellevue College Bharat Kandel, Missouri Tech Linda Cohen, Forsyth Technical Community College Candice Lambert, Metro Technology Centers Susan Mahon, Collin College Mark Aruda, Hillsborough Community College Claude Russo, Brevard Community College Heith Hennel, Valencia College Adrian Genesir, Western Governors University Zeshan Sattar, Zenos Douglas Tabbutt, Blackhawk Technical College

David Koppy, Baker College Sharon Moran, Hillsborough Community College Keith Hoell, Briarcliffe College and Queens College—CUNY Mark Hufnagel, Lee County School District Rachelle Hall, Glendale Community College Scott Elliott, Christie Digital Systems, Inc. Gralan Gilliam, Kaplan Steve Strom, Butler Community College John Crowley, Bucks County Community College Margaret Leary, Northern Virginia Community College Sue Miner, Lehigh Carbon Community College Gary Rollinson, Cabrillo College Al Kelly, University of Advancing Technology Katherine James, Seneca College David Kidd, Western Governors University Bob Treichel, Lake Havasu Unified School District & Mohave Community College

Brief Contents

- Lesson 1: Understanding Device Configurations 1
- **Lesson 2:** Understanding Data Access and Management 44
- **Lesson 3:** Understanding Device Security 95
- Lesson 4: Understanding Cloud Services 120
- Lesson 5: Understanding Enterprise Mobility 145

Appendix 185

Index 187

Contents

Lesson 1: Understanding Device Configurations 1

Objective Domain Matrix 1 Key Terms 1 Configuring Device Options 2 Understanding Microsoft Accounts 6 Configuring Control Panel 9 Configuring System Options 10 Changing Date and Time 12 Managing Devices 13 Using the Devices and Printers Folder 14 Using Device Manager 15 Troubleshooting Problem Devices 18 **Configuring Desktop Settings** 20 Configuring the Start Menu 22 **Configuring User Profiles** 22 Using Roaming Profiles 23 Using Mandatory User Profiles 24 Migrating User Profiles 25 Configuring Display Settings 25 Configuring Shortcuts 27 Understanding Group Policy 27 Applying Group Policy 28 Configuring Group Policy Settings 29 Using Administrative Templates 30 Configuring Drive Encryption 31 Preparing for File Encryption 31 Configuring EFS 32 Configuring BitLocker 33 Configuring Updates 37 Understanding Windows Update 38 Understanding App Updates 40 Understanding Device System Updates 40 Summary Skill Matrix 40 Knowledge Assessment 41 Case Projects 43

Lesson 2: Understanding Data Access and Management 44

Objective Domain Matrix 44 Key Terms 44 **Understanding Cloud Storage Services** 45 Understanding OneDrive 46 Accessing OneDrive and OneDrive for Business from a Browser 46 Creating a File Within OneDrive and OneDrive For Business 48 Uploading Files to OneDrive and OneDrive for Business 49 Sharing a Document in OneDrive and OneDrive for Business 49 Accessing OneDrive from the OneDrive Desktop App for Windows 50 Understanding OneNote 51 Understanding Outlook 51 Understanding Microsoft Office 365 52 Understanding Microsoft Office 365 Features 52 Managing Office 365 53 Installing and Managing Software by Using Microsoft Office 365 54 Using Azure Storage 55 Understanding Local Storage 56 Creating Storage Pools 56 Creating Storage Spaces 57 **Understanding File Systems** 59 Understanding File and Print Sharing 62 Setting NTFS Permissions 62 Creating Effective NTFS Permissions 65 Sharing Drives and Folders 67 Using Public Folders 70 Using HomeGroup 72 Mapping Drives 73 Sharing Printers 75 Installing Printers 75 Understanding Printer Properties 77 Setting Printer Permissions 78 Managing Print Jobs 79

www.wiley.com/college/microsoft

Understanding Data Encryption 80

Understanding Certificates and Their Use 81 Understanding Secure Sockets Layer (SSL) 81 Using Digital Certificates to Encrypt Data 82 Digital Certificates used in Wireless Communications 83 Digital Signature 83 Using a Smart Card 83 Using Software Code Signing 84 Managing Certificates 84 Understanding Certificate Services 87 Moving and Copying EFS-Encrypted Folders 87 Using BitLocker To Go 88 Using a Virtual Private Network (VPN) 88 Summary Skill Matrix 91 Knowledge Assessment 92 Case Projects 94

Lesson 3: Understanding Device Security 95

Objective Domain Matrix 95 Key Terms 95 Understanding the Differences Between the Internet, an Intranet, and an Extranet 96 Defining LANs, MANs, and WANs 96 Defining Private and Public Networks 97 Defining the Different Types of Networks 97 Understanding Firewalls 100 Understanding the Cloud 102 Understanding User Authentication 102 Authenticating with What You Know 103 Using Passwords 103 Using a Personal Identification Number (PIN) 104 Authenticating with What You Own or Possess 104 Authenticating with What You Are 104 Using Windows Rights Management Services (Windows RMS) 105 Understanding Permissions 106 Configuring NTFS Permissions 108 Configuring Basic NTFS Permissions 108 Configuring Advanced NTFS Permissions 109 Copying and Moving Files and Folders on an NTFS Volume 110 Taking Ownership, Delegating, and Viewing Resultant Permissions 110

Setting Share Permissions 112 Understanding Malware 112 Understanding Malware 112 Identifying Malware 114 Developing Antivirus and Antimalware Strategies 115 Summary Skill Matrix 116 Knowledge Assessment 117 Case Projects 119

Lesson 4: Understanding Cloud Services 120

Objective Domain Matrix 120 Key Terms 120 Understanding the Types of Cloud Services 121 Understanding Microsoft Intune 122 **Understanding Microsoft Intune** Capabilities 123 Deploying the Microsoft Intune Client 125 Reviewing Microsoft Intune Administrator Roles 128 Managing User and Computer Groups 129 Managing Microsoft Intune Policies 131 Supporting Mobile Device Management Using Microsoft Intune 132 Understanding Selective Wipe 135 Understanding Location Settings 136 Understanding Microsoft Azure 137 Understanding Virtual Machines 138 Understanding Azure Services 138 Understanding Disaster Recovery, High Availability, Redundancy, and Fault Tolerance 140 Summary Skill Matrix 142 Knowledge Assessment 142 Multiple Choice 143 True / False 144 Case Projects 144

Lesson 5: Understanding Enterprise Mobility 145

Objective Domain Matrix 145 Key Terms 145 Understanding Identity Services 146

www.wiley.com/college/microsoft

Understanding Windows Server Active Directory 147 Introducing Domains, Trees, and Forests 147 Introducing Sites and Domain Controllers 148 Introducing Organizational Units 150 Looking at Objects 151 Understanding User Accounts 152 Understanding Computer Accounts 154 Understanding Groups 154 Understanding Azure Active Directory 155 Understanding Microsoft Accounts 156 Understanding Federation Services 156 **Understanding Business Data Access** 158 Configuring the Company Portal 159 Customizing the Company Portal 160 Using Work Folders 161 Creating a Work Folder 161 Connecting to a Work Folder 163 Understanding Azure RemoteApp 165 Understanding Bring Your Own Device (BYOD) 166 Deploying and Managing Applications by Using Microsoft Intune 166

Installing Windows Installer and Executable Programs 167 Sideloading WINDOWS APPLICATIONS by Using Microsoft Intune 168 Deeplinking WINDOWS APPLICATIONS by Using Microsoft Intune 170 Configuring Application Deployment Policies 171 Managing Outlook Apps 171 Understanding Device-Centric to People-Centric IT 172 Understanding Desktop Virtualization 173 Understanding Dynamic Access Control (DAC) Policies 175 Configuring User and Device Claim Types 176 Configuring File Classification 177 Implementing a Central Access Policy 178 Understanding Windows Rights Management (RMS) 180 Summary Skill Matrix 180 Knowledge Assessment 181 Case Projects 184

Appendix 185 Index 187

Understanding Device Configurations



OBJECTIVE DOMAIN MATRIX

Technology Skill	OBJECTIVE DOMAIN DESCRIPTION	Objective Domain Number
Configuring Device Options Understanding Microsoft Accounts Configuring Control Panel Configuring System Options Changing Date and Time Managing Devices 	Configure device options	1.1
Configuring Desktop Settings Configuring the Start Menu Configuring User Profiles Configuring Display Settings Configuring Shortcuts Understanding Group Policy 	Configure desktop settings	1.2
Configuring Drive Encryption Preparing for File Encryption Configuring BitLocker 	Configure drive encryption	1.3
 Configuring Updates Understanding Windows Update Understanding App Updates Understanding Device System Updates 	Configure updates	1.4

KEY TERMS		
Action Center	Computer Configuration node	encryption
Active Directory accounts	decryption	Group Policy
Administrative Tools	device driver	Group Policy objects (GPOs)
BitLocker Drive Encryption (BDE)	Device Manager Devices and Printers folder	Internet Protocol Security (IPsec)
Cortana	domain-based accounts	Jump List
Control Panel	Encrypting File System (EFS)	live previews

2 | Lesson 1

live tiles	Recycle Bin	user account
local user accounts	resolution	user profile
local user profile	roaming user profile	User State Migration Tool
mandatory user profile	shortcut	Windows Easy Transfer
Microsoft accounts	Secure Sockets Layer (SSL)	Windows Server Update
Microsoft Management Console (MMC) Patch Tuesday	Transport Layer Security (TLS) Trusted Platform Module (TPM)	Windows Update
pin	User Configuration node	

You work as an IT technician for the Contoso Corporation, which has hundreds of computers with a good mix between desktop computers and laptop computers. In addition, several users use smartphones and tablets to access their emails and documents. As an administrator, you need to ensure that your computers are fully functional and secure. You also need to make the machines similar to each other so that the helpdesk can support those machines.

Configuring Device Options

THE BOTTOM LINE

Windows 10 is a robust and flexible system that is made to work on and support a wide range of hardware. For example, Windows 10 can work on a tablet, a laptop, or a desktop computer. Windows 10 also supports mobile devices so that you can take your computer or device with you while accessing your files and programs.

The desktop (as shown in Figure 1-1) is the main screen area that you see when you first start the computer and log on to Windows. Like the top of an actual desktop, it is where you perform your work by opening and running one or more applications. It also includes the *Recycle Bin*, which is used to recover files that have been previously deleted.

At the bottom of the desktop, you will find the Taskbar, which shows you the programs that are running and allows you to navigate between those programs. On the taskbar, you will see the Start button, which is located at the bottom-left corner.

When you click the Start button, the Windows 10 Start menu opens, as shown in Figure 1-2); the Windows 10 Start menu is a blend of the Windows 7 Start menu and the Windows 8 Start screen.

The left side of the Windows 10 Start menu displays the programs, which are used most often, and also provides access to File Explorer, Settings, Power, and All apps. When you click All Apps, all of the installed programs are shown in alphabetical order (see Figure 1-3). When you right-click an installed application, you can select Pin to Start or Pin to taskbar.

On the right side of the Windows 10 Start menu, tiles are displayed. Tiles are larger than the icons found on the Windows desktop and, unlike the static icons, they can contain dynamic content provided by the software they represent. For example, the tile for a Web browser can contain a thumbnail of the currently open Web site, while the Messaging tile can display part of your latest incoming email. Tiles in Windows 10 that contain this type of dynamic content are called *live tiles*.





Figure 1-1

The Windows 10 Desktop



The tiles on the Start menu are configurable in a number of ways. Users can move the tiles around, change their size, change their groupings, and control whether they display live content. It is also possible to remove seldom-used tiles and add new tiles for applications, files, and shortcuts on the computer.

Figure 1-3

Accessing all Windows 10 programs



Clicking the Settings option displays the Settings application, which is based on the Modern UI interface to access common settings, as shown in Figure 1-4. These settings are organized according to the following icons:

- **System**: Allows you to configure the display, notifications and actions, Apps and features, multitasking, table mode, power and sleep options, and default apps.
- Devices: Provides quick access to hardware devices, such as printers.
- **Network & Internet**: Keeps track of Wi-Fi connections and allows you to configure VPN, dial-up connections, Ethernet connections, and proxy settings.
- **Personalization**: Provides settings for the background, colors, lock screen, themes, and the Start menu.
- Accounts: Allows you to change the profile picture and add accounts.
- **Time & language**: Allows you to configure date and time, Region and language, and Speech.
- **Ease of Access**: Provides settings for Narrator, Magnifier, high contrast, closed captions, the keyboard, and the mouse.
- **Privacy**: Allows you to configure the camera, the microphone, speech, account information, contacts, calendar, messaging, and application radio controls for Wi-Fi/Bluetooth connections.
- Update & security: Allows you to configure Windows Update, activate Windows, perform backups and recoveries, and configure Windows Defender.

Cortana is Microsoft's new personal assistant that will help you find things on your PC, manage your calendar, find files, chat with users, and search the Internet. To see the search results, just type the desired text in the Search the web and Windows box option. For example, Figure 1-5 shows the results for a search for "keyboard settings."



USING A TOUCH SCREEN

Windows 10 can be navigated by using a pointing device (such as a mouse) or by using a touch screen. Operating a touch screen requires familiarity with certain finger gestures, such as the following:

Tap: Press a fingertip to the screen and release it. The function is identical to that of a mouse click.

Double-tap: Press a fingertip to the screen twice in quick succession on the same spot. The function is identical to that of a double mouse click.

Press and hold: Tap a location on the screen and press down for approximately two seconds. The function is the same as that of mousing over a designated spot and hovering.

Slide: Press a point on the screen and draw your finger across it without pausing. The function is the same as clicking and dragging a mouse.

Swipe: Draw a finger across the screen in the indicated direction.

Understanding Microsoft Accounts

A *user account* is used to identify a user or other identity on a system, which can be used in authentication, authorization, and auditing. In Windows, user accounts provide different levels of control over an organization's computers and resources.

When working with Windows 10, there are three types of accounts:

- *Microsoft accounts* enable you to synchronize your desktop across multiple Windows 10 devices.
- *Local user accounts* are created on individual computers that are members of a workgroup to provide access to resources on that computer.
- *Domain-based accounts*, also called *Active Directory accounts*, are stored as objects on a domain controller and are used by the operating system to identify and authenticate the user and to grant her authorization to access specific domain resources.

When you set up a computer running Windows 10 for the first time, you have the option of creating a Microsoft account using an email address that you provide. The email address you use can come from any provider. After the account is set up, Microsoft will use it along with your password to help manage your settings across all your PCs running Windows 10. After organizing your system the way you want it (your preferred desktop background, user tiles, favorite websites in your browser, explorer settings, and so on), the information will be associated with your Microsoft account and will be stored in the cloud. Every time you log into a Windows 10 device using the account, your settings are synched from the cloud, and any changes you make are updated and available to you on the next device.

Using a Microsoft account provides a consistent experience when working with Windows Store apps. Purchased apps will be available from each device, feeds you add will be synched across all devices, and state information will be maintained, so you can start a game or read a book and pick it up later on another device.

Microsoft accounts can be synced with a domain account, but the capability to do so depends upon Group Policy settings. Using Group Policy—covered later in this lesson—you can determine whether you want to allow the syncing of the two accounts and what information can be synced.

You can create a Microsoft account during the initial installation of the operating system or after the system is running. The following steps outline the process you can use to create the account.

CREATE A MICROSOFT USER ACCOUNT USING THE SETTINGS PROGRAM

GET READY. To create the account after Windows 10 is installed using the Settings program, perform the following steps.

- 1. Log into the Windows 10 client computer.
- 2. Click the Start button to open the Start menu.
- 3. Click Settings.

CERTIFICATION READY Configure device options 1.1

- 4. Click Accounts.
- 5. Click the Family & other users option.
- 6. Click Add someone else to this PC.
- 7. On the How will this person sign in? page, to use an existing Microsoft Account, in the Email or phone text box (see Figure 1-6), type the email address you want to use. Click Next and then click Finish. If you want sign up for a new Microsoft account, click The person I want to add doesn't have an email address.

Figure 1-6		×
Adding a user		
	How will this person sign in?	
	Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.	
	Email or phone	
	The person I want to add doesn't have an email address Privacy statement	
	Next Cancel	

8. On the Let's create your account page (as shown in Figure 1-7), in the First name text box and Last name text box, type your first name and last name. In the someone@ example.com text box, type the desired email address.

Figure 1-7	_	×
Creating a new account		
	Let's create your account Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more	
	personal when you sign in with your Microsoft account.* Learn more	
	Last name	
	someone@example.com	
	Get a new email address	
	Password	
	United States ~	
	Birth month \checkmark Day \checkmark Year \checkmark	
	*If you already use a Microsoft service, go Back to sign in with that account. Add a user without a Microsoft account	
	Next Back	

- 9. In the Password text box, type the desired password.
- In the Country text box, type the name of your country. In the remaining text boxes, type your Birth month, Day, and Year. Click Next.
- **11.** On the Add security info page, in the Phone number text box, type a phone number that can receive text messages. Click **Next**.
- On the See what's most relevant to you option, deselect one or both options, if desired:
- **13.** Enhance my online experience by letting Microsoft Advertising use my account information
 - Send me promotional offers from Microsoft
 - By default, the account will be a standard user account. If you want to upgrade the account to an administrator, click the new account, and then click **Change account type**.
- 14. Change the Account type to Administrator and then click OK.
- 15. On the Add a user page, Click Finish.

When using a logon with a Microsoft or work account in Windows 10, you can sync your PC settings—even between multiple Windows 10 machines—as long as they are connected with the same Microsoft account. Therefore, if you change the wallpaper or add a favorite shortcut in Internet Explorer, those changes will be replicated to the other machines.

The Sync feature (located under OneDrive settings, as shown in Figure 1-8) can sync many of your settings between PCs, including the following:

- Personalization settings, such as Start screen colors, background, and lock screen image
- Themes, such as the desktop background and sounds
- Ease of Access settings, such as Speech Recognition, Magnifier, On-screen Keyboard, and Narrator

← Settings	- 0
र्ेंडे ACCOUNTS	Find a setting
Your account	Sync your settings
Sign-in options	Sync Windows settings to other devices using patrick_regan123456@hotmail.com.
Work access	How does syncing work?
Family & other users	Sync settings
Sync your settings	On On
	Individual sync settings
	Theme
	On
	Web browser settings
	On On
	Passwords
	On
	Language preferences
	On
	Ease of Access
	On On
	Other Windows estings

Figure 1-8

Managing Sync settings in Windows 10

- Language preferences, such as keyboard settings, other input methods, and display language
- Web browser settings, such as history, pinned sites, and favorites for both versions of the browser
- Taskbar settings, such as pinned items and which side of the monitor the Taskbar is attached to
- Folder and Search settings for File Explorer
- Mouse settings
- Your accounts picture (user tile)
- Per-app notification state
- Settings for Windows Store apps, including third-party apps
- HomeGroup password

Configuring Control Panel

As with previous versions of Windows, the main graphical utility to configure the Windows environment and hardware devices is the *Control Panel*. It can be accessed by right-clicking the Start button and choosing Control Panel. See Figure 1-9. Of the eight categories that are listed, each category includes a top-level link, and under this link are several of the most frequently performed tasks for the category.

Clicking a category link provides a list of utilities in that category. Each utility listed within a category includes a link to open the utility, and under this link are several of the most frequently performed tasks for the utility.

As with current and previous versions of Windows, you can change from the default category view to classic view (large icon view or small icon view). Icon view is an alternative view that provides the look and functionality of Control Panel in Windows 2000 and earlier versions of Windows where all options are displayed as applets or icons.

The *Microsoft Management Console (MMC)* is one of the primary administrative tools used to manage Windows and many of the network services provided by Windows. It provides a standard method to create, save, and open the various administrative tools provided by Windows. When you open Administrative Tools, most of these programs are MMC.



Administrative Tools is a folder in the Control Panel that contains tools for system administrators and advanced users. To access the Administrative Tools, open the Control Panel, open Administrative Tools by clicking Start, Control Panel, System and Security while in category view or double-click the Administrative Tools applet while in icon view. There is also a quick link on Windows that can be accessed by clicking the Start button.

Some common administrative tools in this folder include:

- **Component Services**: Configures and administers Component Object Model (COM) components. Component Services is designed for use by developers and administrators.
- **Computer Management**: Manages local or remote computers by using a single, consolidated desktop tool. Using Computer Management, you can perform many tasks, such as monitoring system events, configuring hard disks, and managing system performance.
- **ODBC Data Sources**: Uses Open Database Connectivity (ODBC) to move data from one type of database (a data source) to another.
- **Event Viewer**: Views information about significant events, such as programs starting or stopping or security errors that are recorded in event logs.
- iSCSI Initiator: Configures advanced connections between storage devices on a network.
- Local Security Policy: Views and edits Group Policy security settings.
- **Performance Monitor**: Views Advanced system information about the processor, memory, hard disk, and network performance.
- **Print Management**: Manages printers and print servers on a network and perform other administrative tasks.
- Services: Manages the different services that run in the background on your computer.
- **System Configuration**: Identifies problems that might be preventing Windows from running correctly.
- **System Information**: Shows details about your computer's hardware configuration, computer components, and software, including drivers.
- Task Scheduler: Schedules programs or other tasks to run automatically.
- Windows Memory Diagnostics: Checks your computer's memory to see whether it is functioning properly.
- Windows PowerShell: A task-based command-line shell and scripting language designed especially for system administration.

When you use these tools, you might assume that they are used only to manage the local computer. However, many of them can be used to manage remote computers as well. For example, you can use the Computer Management console to connect to and manage other computers, assuming you have administrative rights to the computer.

Configuring System Options

Some of the most important configuration settings for a user are the system settings within the Control Panel. These include gathering generation information about your system, changing the computer name, adding the computer to a domain, accessing the device manager, configuring remote settings, configuring startup and recovery options, and configuring overall performance settings.

To access the system settings, you can do one of the following:

- In the Control Panel, if you are in Category view, click System and Security, and then click System or click View amount of RAM and processor speed.
- In the Control Panel, if in classic view, double-click the System applet.

- Right-click Computer and choose Properties.
- Right-click the Start button and choose System.

In Windows, there are often several ways to do the same thing.

At the top of the screen, you see the Windows edition you have and the system type. If Windows comes in 64-bit, it will show 64-bit Operating System in the middle of the screen. Toward the bottom of the screen you will see the computer name and domain (if any) if Windows is activated and the Product ID. See Figure 1-10.

To help identify computers, you should name a computer with a meaningful name. This can be done within the System settings within the Control Panel. You can also add a computer to a domain or workgroup.

Every computer must have a unique computer name assigned to a network. If two computers have the same name, one or both of the computers will have trouble communicating on the network. To change the computer name, open System from the Control Panel. Then click the Change Settings option in the Computer name, domain, and workgroup settings. When the System Properties box appears with the Computer Name tab selected, click the Change button. See Figure 1-11. Any changes to the computer name or workgroup/domain name will require a reboot.





Figure 1-11

Displaying System Properties

By default, a computer is part of a workgroup. A workgroup is usually associated with a peerto-peer network in which user accounts are decentralized and stored on each individual computer. If several users need to access the computer (while requiring unique usernames and passwords), you will need to create a user account for each user. If you want those users to access another stand-alone computer, you will have to create the same computer accounts and password on that computer as well. As you can imagine, with several computers, this can become a lot of work as you keep creating and managing accounts on each individual computer.

A domain is a logical unit of computers that define a security boundary, and it is usually associated with Microsoft's Active Directory Domain Services (AD DS). The security of the domain is generally centralized and controlled by Windows servers acting as domain controllers. As a result, you can manage the security much easier for multiple computers while providing better security.

When a computer is added to a domain, a computer account is created to represent the computer. In addition, information stored on the computer is used to uniquely identify the computer. When these items match, it shows that a computer is who it says is, which contributes to a more secure work environment.

To add the computer to the domain, open System Properties and click the Change button. You will then select the Domain option and type the name of the domain. Next, click OK. It will prompt you to log in with a domain account that has the ability to add computers to the domain. This is typically a domain administrator or account administrator. After you enter the credentials (username and password), a Welcome dialog box appears. Click OK to close the Welcome dialog box. When you close the System Properties dialog box, it will prompt you to reboot the computer.

To remove a computer from a domain, join an existing workgroup, or create a new workgroup, you select the workgroup option and type in the name of the workgroup and click OK. If you are removing yourself from the domain, you will be asked for administrative credentials so that it can delete the account from Active Directory. If you don't specify administrative credentials, it will still remove the computer from the domain, but the computer account will still remain within Active Directory.

Changing Date and Time

One of your easiest but most essential tasks is making sure that the computer has the correct date and time, which is essential for logging purposes and for security. If a secure packet is sent with the wrong date or time, the packet may be automatically denied because the date and time is used to determine if the packet is legit.

To access the date and time settings, perform one of the following steps:

- Click Clock, Language, and Region in the Control Panel while in Category view and click Set the time and date.
- Double-click Date and Time while in Icon view.
- If the date and time show in the Notification area, double-click the date and time.

To set the clock:

- 1. Click the Date and Time tab and then click Change date and Time.
- 2. Double-click the hour, minutes, or seconds, and then click the arrows to increase or decrease the value.
- 3. When you are finished changing the time settings, click OK.

To change the time zone, click Change time zone and click your current time zone in the drop-down list. Then click OK.

If you are part of a domain, the computer should be synchronized with the domain controllers. If you have a computer that is not part of a domain, you can synchronize with an Internet time server by clicking the Internet Time tab and selecting the checkbox next to Synchronize with an Internet time server. Then select a time server and click OK.

Managing Devices

A computer is a collection of hardware devices, each of which requires a piece of software called a device driver in order to function. Windows 10 includes a large library of device drivers, but it is still sometimes necessary to obtain them yourself.

As most people know, a PC is a collection of hardware devices, all of which are connected together and installed in a single case. Disk drives, keyboards, mice, modems, and printers are all types of devices. To communicate with the operating system running on the computer, each device also requires a software element called a *device driver*. The device driver provides the operating system with information about a specific device.

For example, when you use a word processing application to save a file to a hard disk, the application issues a generic WriteFile function call to the operating system. The application knows nothing specific about the disk drive hardware; it just issues an instruction to store a particular file there. When the operating system processes the function call, it accesses the device driver for the hard disk drive, which provides detailed information about how to communicate with the drive. If the user selects a different target location for the file, the operating system accesses the device driver for that location, whether it's a hard drive, a floppy drive, or USB flash drive.

In most cases the information the device driver provides is integrated into the Windows interface. For example, the Properties sheet for a printer includes generic system information (see Figure 1-12), such as which port the printer is connected to and who is permitted to use it. Other tabs, and particularly the Device Settings tab, as shown in Figure 1-13, are based on hardware-specific information provided by the device driver.

re 1-12	🐻 Hewlett-Pa	ckard HP Lase	erJet 400 colo	or M451dn on pat8	Properties
General Settings tab of a	Securi	ty	Devic	e Settings	About
er's Properties sheet	General	Sharing	Ports	Advanced	Color Management
	8	Hewlett-Pa	ackard HP La	aserJet 400 color M	451dn
	Location:				
	Comment:				
	Model:	HP LJ300-4	00 color M3	51-M451 PCL 6	
	Features				
	Color: Yes			Paper available:	
	Double-si	ded: Yes		Letter	^
	Staple: No	6			
	Speed: 18	ppm			
	Maximum	resolution: 60	00 dpi		¥ .
			Prefe	rences	Print Test Page
			Г	OK (Cancel Apply

Figu

The print

Figure 1-13

The Device Settings tab of a printer's Properties sheet

General	Sharing	Ports	Advanced	Color Managemer
Secu	rity	Device	Settings	About
HP LJ3	00-400 color M	351-M451 PC	L 6 Device Setting	ąs
- For	rm To Tray Assi	ignment		
	Printer auto se	lect: Letter		~
	Manual Feed i	n Tray 1: Lett	er	
	Tray 1: Letter			
	Tray 2: Letter			
	Tray 3: Not Av	ailable		
🕀 👌 For	nt Substitution	Table		
Ext	ernal Fonts			
🖻 🎼 Ins	tallable Option	s		
	Automatic Co	nfiguration: (Dff	
	Printer Status	Notification:	Enabled	
	Tray 3: Not Ins	talled		
	Duplex Unit (fo	or 2-Sided Pri	nting): <u>Installed</u>	
	Allow Manual	Duplexing: El	napled	
	Ich Separator	Dicabled		
	Job Separator.	Disableu		

In addition to providing information about a device, drivers also permit the operating system to modify the hardware configuration settings of the device. For example, when you configure a printer to print a document in landscape mode instead of portrait mode, the printer device driver generates the appropriate commend and sends it to the hardware.

The process of installing a hardware device consists primarily of identifying the device and installing a device driver for it. This process can occur during the operating system installation or at a later time, but the steps are fundamentally the same.

A major part of the Windows 10 installation process consists of identifying the devices in the computer and installing the appropriate drivers for them. The Windows 10 installation package includes hundreds of drivers for many different devices, which is why many installations finish without any user intervention. Sometimes, however, you might have to supply device drivers yourself.

USING THE DEVICES AND PRINTERS FOLDER

Windows 10, Windows includes the *Devices and Printers folder* to quickly allow users to see all the devices connected to the computer and to configure and troubleshoot these devices. It will also allow you to view information about the make, model, and manufacturer and give you detailed information about the sync capabilities of a mobile phone or other mobile devices.

The Devices and Printers folder gives you a quick view of devices connected to your computer that you can connect or disconnect from your computer through a port or network connection. This includes mobile devices such as music players and digital cameras, USB (Universal Serial Bus) devices, and network devices. See Figure 1-14. It does not include items installed inside your computer such as internal disk drives, expansion cards, RAM and it will not display legacy devices such as keyboards and mice connected through a PS/2 or serial port.

To open the Devices and Printers folder, open the Control Panel and, under Hardware and Sound, click View devices and printers while in Category view or double-click Devices and Printers in Icon view.

When you right-click a device icon in the Devices and Printers folder, you can choose from a list of tasks that vary depending on the capabilities of the device. For example, you might be able to see what's printing on a network printer, view files stored on a USB flash drive, or open a program from the device manufacturer. For mobile devices that support the new Device Stage feature in Windows, you can also open advanced, device-specific features in Windows from the right-click menu, such as the ability to sync with a mobile phone or change ringtones.



Most PCs use USB connections for peripheral devices, and Plug and Play is an integral part of the USB standard. When you connect a printer, a camera, a scanner, or another type of device to a computer running Windows 10 using a USB port, the system usually detects it, adds it to the Devices and Printers folder and installs the appropriate device driver for it.

You can also manually install a device by selecting Add a device, which displays the Choose a device or a printer to add to this PC page.

USING DEVICE MANAGER

The Windows 10 tool for managing devices and their drivers is called *Device Manager*. You can use Device Manager to get information about the devices installed in the computer, as well as install, update, and troubleshoot device drivers.

Although it is not immediately apparent, Device Manager is a snap-in for the Microsoft Management Console (MMC). This means that there are many ways that you can access Device Manager, including the following:

- Open the Hardware and Sound control panel and click the Device Manager link.
- Open the Computer Management console from the Administrative Tools program group in the System and Security control panel and click Device Manager in the scope (left) pane.
- Run the Microsoft Management Console shell application (Mmc.exe), select File > Add/Remove Snap-in, and select Device Manager from the list of snap-ins provided.
- Open the Start menu, type Device Manager or the file name of the Device Manager snap-in (Devmgmt.msc), and then execute the resulting file.
- Using Cortana, search for Device Manager and then execute the resulting file.

Each of these procedures launches the Device Manager and displays a window with an interface like that shown in Figure 1-15.

16 | Lesson 1

Figure 1-15

The Windows 10 Device Manager

🚔 Device Manager	-	
File Action View Help		
V 📇 Win10A		
V 🛄 Computer		
ACPI x64-based PC		
🗸 👝 Disk drives		
👝 Virtual HD ATA Device		
> 💵 Display adapters		
> 🔐 DVD/CD-ROM drives		
> 📲 Floppy disk drives		
> 🖷 Floppy drive controllers		
> 🕼 Human Interface Devices		
> 🥁 IDE ATA/ATAPI controllers		
> 📖 Keyboards		
> 🖞 Mice and other pointing devices		
> 🛄 Monitors		
> 📃 Network adapters		
> 👳 Network Infrastructure Devices		
> 🚏 Ports (COM & LPT)		
> 🛱 Print queues		
> 🛱 Printers		
V Processors		
Intel(R) Xeon(R) CPU E5345 @ 2.33GHz		
> 🗋 Software devices		
> 🗲 Storage controllers		
> 💻 System devices		

Device Manager is capable of displaying information in the following four modes:

- **Devices by type**: Displays a list of device categories, which you can expand to show the devices in each category. This is the default Device Manager view.
- **Devices by connection**: Displays a list of the interfaces that hardware devices use to communicate with the computer. Expanding a connection shows the devices using that connection.
- **Resources by type**: Displays a list of resource types, including Direct Memory Access (DMA), Input/Output (I/O), Interrupt Request (IRQ), and Memory, which you can expand to show the resources of each type and the devices that are using them.
- **Resources by connection**: Displays a list of resource types, including Direct Memory Access (DMA), Input/Output (I/O), Interrupt Request (IRQ), and Memory, which you can expand to show the connection associated with each individual resource and the device using each connection.

To examine the properties of a device, simply locate it in the tree display and double-click it to open its Properties sheet.

The tabs on the Properties sheet vary depending on the nature of the device you select, but virtually all devices have the following four tabs:

- **General**: Displays the name of the device, its type, manufacturer, and location in the system. The Device Status box indicates whether the device is functioning and, if not, provides troubleshooting help.
- **Driver**: Displays the device driver's provider, date, version, and digital signer. The tab also provides buttons you can use to display driver details, update, roll back (used when an upgrade of a device driver fails or causes problems with a system), or uninstall the driver, and enable or disable the device.
- Detail: Displays extensive information about the driver and its properties.
- **Resources**: Displays the hardware resources being used by the device and indicates whether there are any conflicts with other devices in the computer.

With Device Manager, you can disable any device in the computer, using any of the following procedures:

- Select the device and choose Disable from the Action menu.
- Right-click the device and choose Disable from the context menu.
- Open the device's Properties sheet and click the Disable button on the Driver tab.

Disabling a device does not affect the hardware in any way or uninstall the device driver; it simply renders the device inoperative until you enable it again. Obviously, you cannot disable devices that are necessary for the system to function, such as the processor, and some devices that are in use require you to restart the system before they can be disabled.

TAKE NOTE*Disabling a device releases the hardware resources it was using back to the operating system.
If you restart the computer with the device disabled, Windows might reassign those hard-
ware resources to other devices. If you re-enable the device, the computer might allocate
different hardware resources to it than it had originally.

When you update a driver using Device Manager, you can point to a location on your computer where you have already saved the new driver, or you can run a search of your computer and the Internet. To update a device driver, use the following procedure.

UPDATE A DEVICE DRIVER

GET READY. Log on to Windows 10 using an account with Administrator privileges.

- 1. Open Device Manager and locate the device that you want to update.
- **2.** Double-click the device you want to update, so that its Properties sheet appears.
- Click the Driver tab and then click the Update Driver button. The How Do You Want To Search For Driver Software? page appears, as shown in Figure 1-16.

u Want To er Software?	 Update Driver Software - Microsoft Hyper-V Video How do you want to search for driver software?
	→ Search automatically for updated driver software Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.
	→ Browse my computer for driver software Locate and install driver software manually.
	Cancel

- **4.** Click **Browse My Computer For Driver Software** to specify a location for the driver or to select from a list of installed drivers. Click **Search Automatically For Updated Driver Software** to initiate a search for a driver.
- **5.** Click **Next** when you locate the driver you want to install. The Windows Has Successfully Update Your Driver Software page appears.
- 6. Click Close.
- 7. Close the Device Manager window.

Figure 1-16

The How Do You Want To Search For Driver Software? page When you update a device driver in Windows 10, the operating system does not discard the old driver completely. It is not uncommon for new drivers to cause more problems than they solve, and many users find that they would prefer to go back to the old version. Windows 10 makes this possible with the Roll Back feature, which you initiate by clicking the Roll Back Driver button on the Driver tab of the device's Properties sheet. This procedure uninstalls the current driver and reinstalls the previous version, returning the device to its state before you performed the most recent driver update.

Installing a new hardware device or a new device driver is a risky undertaking. There is always the possibility of a problem that, depending on the devices involved, could be trivial or catastrophic. For a peripheral device, such as a printer, a hardware misconfiguration or faulty driver would probably just cause the new device to malfunction. However, if the device involved is a graphics adapter, a bad driver could prevent the system from functioning.

TROUBLESHOOTING PROBLEM DEVICES

The *Action Center* (as shown in Figure 1-17) shows important notifications related to the security and maintenance of your computer. When problems occur, you will be alerted to investigate them further.

To troubleshoot hardware or driver problems, consider some of the following techniques:

- Open the Properties sheet for the device and check the Device Status box on the General tab. If the device is malfunctioning, this tab informs you of its status and enables you to launch a troubleshooter.
- Open the Device Manager and delete the device entirely. Then restart the system and allow Windows 10 to detect and install the device over again. This process will cause





Windows to re-allocate hardware resources to the device, which could resolve the problem if it was caused by a hardware resource conflict.

• If the device or driver malfunction prevents the system from running properly, as in the case of a bad graphics driver that prevents an image from appearing on the screen, you can start the computer in Safe Mode by pressing the F8 key as the system starts. Safe Mode loads the operating system with a minimal set of generic device drivers, bypassing the troublesome ones, so you can uninstall or troubleshoot them.

Device Manager also displays all of the devices installed on your computer. When a device is experiencing problems, Device Manager uses symbols to provide information about the particular error condition.

When there is an issue with a device, you will see one of the following symbols (each symbol represents a specific type of problem):

- **Blue question mark inside white circle**: Driver installed; may not provide full functionality.
- **Red "X"**: device is installed in computer and is consuming resources; protected mode driver not loaded; device installed improperly.
- **Black exclamation point on yellow field**: Device in problem state; the device might be functioning; problem code will be displayed with device.
- Blue "I" on white field: Use automatic settings not selected for device; resource was manually selected; does not indicate a problem or disabled state.
- **Problem code**: Code explaining the problem with the device.
- White circle with down arrow: Device was disabled by an administrator or user.
- **Yellow warning symbol with exclamation point**: There is a problem with the device.

Windows 10 uses built-in hardware diagnostics to detect hardware problems on your computer. When problems are identified, a message appears that lets you know about the problem. If you select the message, you will be taken to the Action Center, which provides a central location to view any problems with your hardware or software.

When there is a problem, you will see two types of messages in the notification area (the bottom-right corner of your desktop):

- **Red items (white flag, red circle with white x)**: These are important messages that indicate a significant problem that needs to be addressed. For example, your firewall is turned off, or spyware or antivirus applications need to be updated.
- Yellow items: These are messages that suggest tasks that can make your computer run better. For example, updating an application or configuring Windows Update to automatically download and install updates rather than checking with you beforehand.

How you troubleshoot a device depends upon the type of problem you encounter. For example, when you notice a device with the black exclamation point in a yellow triangle, you can double-click the device to investigate the problem further. Figure 1-18 shows that the device cannot start and the specified request is not a valid operation for the target device.

Another item of interest when troubleshooting device problems is to look for an Other Devices folder. This folder contains devices detected by Windows but lacks a driver for the device.



Figure 1-18

Troubleshooting a device

USB Keyboard Properties Driver Details Events Key Tronic USB Keyboard Device type: Keyboards Manufacture: Key Tronic Location: on Microsoft Hyper-V Virtual Machine Bus	>
status evice cannot start. (Code 10) oecified request is not a valid operation for the target device.	
st	operation of the target device.

Configuring Desktop Settings

THE BOTTOM LINE

Windows desktop settings is a broad term that refers to many different settings you can configure to personalize Windows, such as the Windows theme, the desktop background, mouse clicks and pointer speeds, gadgets, shortcuts, and more. All settings are customizable—choosing the right mix will make your Windows experience more enjoyable and more productive.

CERTIFICATION READY Configure desktop settings The Windows desktop is a flexible, configurable part of the Windows environment. You can grab the Taskbar and move it to either side of the screen, to the top, or back to its default location at the bottom (the Taskbar must be unlocked to move it—right-click the Taskbar and, if Lock the taskbar is checked, select the box to deselect it). You can also choose which items appear in the notification area on the right side of the Taskbar by configuring the Taskbar Properties dialog box. To access this dialog box, right-click the Taskbar and choose Properties, as shown in Figure 1-19.

Figure 1-19	Taskbar and Start Menu Properties X
Menu Properties dialog box	Taskbar Navigation Toolbars
	How do I customize taskbars? OK Cancel Apply
Windows 10 has the ability to *pin* program shortcuts directly to the Taskbar; when you pin a program, the icon for that program displays on the Taskbar even when the program isn't running. This provides you with quick access to your frequently used programs. Shortcuts for Task View, Microsoft Edge, File Explorer, and Store appear there by default. You can unpin programs from the Taskbar as well. You'll learn about shortcuts later in the lesson.

When you open a program in Windows 10, an icon for that program displays on the Taskbar. To activate a program, just click its icon on the Taskbar. If you have several programs open at once, Windows allows you to hover the mouse pointer over an icon in the Taskbar to see a thumbnail preview of the window. This thumbnail preview is called a *Jump List*. You can also press and hold the Alt key and then press the Tab key repeatedly to switch between windows and see *live previews* of the window for each open program.

Many Windows 10 desktop settings are available when you right-click a blank area of the desktop and choose Personalize. The Personalization window is shown in Figure 1-20. The main part of the window displays various themes you can use. Just click the theme of your choice and see the changes take effect immediately.

You can also change the background of any theme. Just click Background. In the Background window, open the Picture location drop-down list, and then select a picture, a solid color, or a slideshow.

When you click the Themes > Advanced sound settings, the Sound dialog box opens (see Figure 1-21). From here, you can choose different sounds to accompany Windows events, such as when you connect a device or when you close Windows. The computer's sound volume must be set at an appropriate level to actually hear the sound.

When you click the Lock screen option, you can click the Screen saver settings option to open the Screen Saver Settings dialog box (as shown in Figure 1-22). Then open the Screen saver drop-down list, select a screen saver, and click OK.



Figure 1-20

The Windows 10 Personalization window



(None)



reen Saver			
	1 · ···		
	Napar Ini Ini Napar		
	E Contraction de la contractio		
		20 June 22	
		.0	
Screen saver			
Screen saver (None)	~	Settings	Preview
Screen saver (None)	×	Settings	Preview
Screen saver (None) Wait: 1	minutes On result	Settings	Preview
Screen saver (None) Wait: 1	minutes □ On resument	Settings me, display logon	Preview
Screen saver (None) Wait: 1	minutes On resu ment ay or maximize perform.	Settings Ime, display logon ance by adjusting o	Preview screen lisplay
Screen saver (None) Wait: 1 Power manage Conserve energ brightness and	minutes On resument ay or maximize perform other power settings.	Settings Ime, display logon ance by adjusting o	Preview screen lisplay
Screen saver (None) Wait: 1 Power manage Conserve energ brightness and Change power	minutes On resument ay or maximize perform, other power settings.	Settings Ime, display logon ance by adjusting o	Preview screen lisplay

×

► Test Browse...

OK Cancel Apply

Configuring the Start Menu

Windows 10 uses the Modern UI/Metro style that utilizes the Start menu. The Start menu contains a list of applications and Desktop programs via pinned tiles. The pinned tiles have different sizes and colors. In addition, you can pin folders to the new Start screen.

To pin an item to the Start screen, find a program or file by using the All apps option, by using Cortana, or by using File Explorer. Then right-click the program, application or folder and choose Pin to Start in App bar or popup menu. Some tiles allow for additional actions. For example, when you pin This PC to the Start menu, you can quickly open Computer Management or System Properties or you can connect/disconnect network drives.

Configuring User Profiles

A user profile is a series of folders, associated with a specific user account that contain personal documents, user-specific registry settings, Internet favorites, and other personalized information—everything that provides a user's familiar working environment. On a Windows 10 computer, user profiles are stored in the Users folder, within subfolders named for the user accounts.

On computers running Windows 10, user profiles automatically create and maintain the desktop settings for each user's work environment on the local computer in a folder beneath C:\Users. The system creates a new user profile for each user logging on at the computer for the first time.

Each user folder contains a separate user profile for that person. A typical user profile consists of the following folders, some of which are hidden, plus a hidden registry file:

- AppData
- Contacts
- Desktop
- Downloads
- Favorites
- Links
- My Documents
- My Music
- My Pictures
- My Videos
- Saved Games
- Searches

When a user logs on at the workstation using a local or domain account, the system loads that individual's profile and uses it throughout the session until the user logs off. During the session, the My Documents folder in the user's profile becomes the operative My Documents folder for the system, as do all the other folders in the profile.

There are three main types of user profiles, as follows:

- *Local user profile*: A profile that Windows automatically creates when each user logs on at the computer for the first time. The local user profile is stored on the computer's local hard disk.
- *Roaming user profile*: A copy of a local user profile that is stored on a shared server drive, making it accessible from anywhere on the network.
- *Mandatory user profile*: A roaming profile that users cannot change. Administrators use mandatory user profiles to enforce particular desktop settings for individuals or for a group of users. A fourth variation, called a super-mandatory profile, requires the user to access the server-based profile or the logon fails.

USING ROAMING PROFILES

To support users who work at multiple computers on the same network, administrators can create roaming user profiles.

A roaming user profile is simply a copy of a local user profile that is stored on a network share (to which the user has appropriate permissions), so that the user can access it from any computer on the network. No matter which computer a user logs on from, he or she always receives the files and desktop settings from the profile stored on the server.

To enable a user to access a roaming user profile, rather than a local profile, you must open the user's Properties sheet to the Profile tab, as shown in Figure 1-23, and type the location of the roaming profile in the Profile Path field.

24 | Lesson 1

Figure 1-23

The Profile tab of a user's Properties sheet

patri Properties		?
General Membe	r Of Profile	
User profile		
Profile path:	I	
Logon script:		
Home folder		
Local path	1:	
O Connect:	Z: ~ To:	
_		
	01/ 0 1	

Then, the next time the user logs on, Windows 10 accesses the roaming user profile in the following manner:

- 1. During the user's first logon, the computer copies the entire contents of the roaming profile to the appropriate subfolder in the Users folder on the local drive. Having the roaming user profile contents stored on the local drive enables the user access to the profile during later logons, even if the server containing the roaming profile is unavailable.
- 2. The computer applies the roaming user profile settings to the computer, making it the active profile.
- 3. As the user works, the system saves any changes he or she makes to the user profile to the copy on the local drive.
- 4. When the user logs off, the computer replicates any changes made to the local copy of the user profile back to the server where the roaming profile is stored.
- 5. The next time the user logs on at the same computer, the system compares the contents of the locally stored profile with the roaming profile stored on the server. The computer copies only the roaming profile components that have changed to the copy on the local drive, which makes the logon process shorter and more efficient.

You should create roaming user profiles on a file server that you back up frequently, so that you always have copies of your users' most recent profiles. To improve logon performance for a busy network, place the users' roaming profiles folder on a member server instead of a domain controller.

USING MANDATORY USER PROFILES

A mandatory user profile is simply a read-only roaming user profile. Users receive files and desktop settings from a server-based profile, just as they would with any roaming profile, and they can modify their desktop environments while they are logged on. However, because the profile is read-only, the system cannot save any profile changes back to the server when the users log off. The next time the user logs on, the server-based profile will be the same as during the previous logon.

Windows 10 downloads the mandatory profile settings to the local computer each time the user logs on. You can assign one mandatory profile to multiple users who require the same desktop settings, such as a group of users who all do the same job. Because the profile never changes, you do not have to worry about one user making changes that affect all of the other users. Also, a mandatory profile makes it possible to modify the desktop environment for multiple users by changing only one profile.

To create a mandatory user profile, rename the Ntuser.dat file in the folder containing the roaming profile to Ntuser.man. The Ntuser.dat file consists of the Windows 10 system registry settings that apply to the individual user account and contains the user environment settings, such as those controlling the appearance of the desktop. Renaming this file with a .man extension makes it read-only, preventing the client computers from saving changes to the profile when a user logs off.

MIGRATING USER PROFILES

There are two basic methods for deploying Windows 10 to a client while retaining the user profile settings: upgrade and migration. In an upgrade, you install Windows 10 on the computer running an earlier operating system. Windows 10 overwrites the old OS, but all of the user profiles already on the computer remain in place. In a migration, you copy the user profile information from the old operating system to some temporary medium and transfer it to a new, clean installation of Windows 10.

Microsoft provides the following two tools for migrating files and settings to new computers:

- *Windows Easy Transfer*: Designed for the migration of a single computer, Easy Transfer is a wizard-based utility that makes it possible to migrate user profile information for multiple users from one computer to another.
- *User State Migration Tool*: Designed for large-scale enterprise deployments, the User State Migration Tool is a command-line utility that can migrate profile information for multiple users on multiple computers.

In the following sections, you will learn the procedure for using Windows Easy Transfer to migrate user profile settings from a Windows 7 workstation, a Windows 8/8.1 workstation, or a Windows 10 workstation to a new Windows 10 workstation. You will also learn some basic facts about using the User State Migration Tool.

Configuring Display Settings

Windows 10 has several display settings, but you're most likely to modify the resolution, color depth, and font size most often. You can modify each setting to suit a particular application.

When you right-click the desktop and choose Display Settings, the Display page opens. This is where you can change the orientation and the size of the text and apps, as shown in Figure 1-24.

To open the screen resolution window (as shown in Figure 1-25), click the Advanced display settings option. This is where you choose which monitor to use (if your computer is connected to two or more monitors) and whether to display content in a landscape orientation or a portrait orientation. You can also configure settings to connect a projector to your computer. Three other important display settings you might want to adjust for specific purposes are resolution, color depth, and font size.

Resolution refers to the number of pixels that create the "image," that is, everything you see on the screen. *Resolution* has a horizontal value and a vertical value, such as 1200 x 768 or 1600 x 900. The Windows desktop expands itself to fit whatever resolution you select, so you always have a full background. Similarly, the Taskbar stretches across the bottom of the screen, regardless of the resolution you choose.

You might need to change a computer's screen resolution for a variety of reasons, such as when you're accommodating a visually impaired user or when you're using an external projector.

26 | Lesson 1

Figure 1-24

Opening the Display Settings page



Figure 1-25

The Advanced Display Settings page

← Settings	– 🗆 X
ई्रें ADVANCED DISPLAY SETTINGS	
Customize your display	
1	
Identify Detect	
Resolution	
1024 × 768 (Recommended) ~	
Apply Cancel	
Related settings	

Your computer's monitor has a minimum and a maximum resolution it can display, so Windows 7 gives you a range of resolutions to choose from.

Screen fonts are usually measured in dots per inch (dpi). You can enhance the appearance of your desktop by adjusting font size dpi to improve the readability of pixelated or illegible fonts.

Configuring Shortcuts

Shortcuts are icons you can click to start a program or go to a location without requiring any extra steps. Shortcuts save time because you don't have to use several keystrokes or click several menus or commands.

An icon is a small, visual symbol of a computer resource, such as a program, folder, file, or drive. To access an actual computer resource, click or double-click its icon. Some icons are located on the desktop, others are in the Start menu, and still others might appear in the list of files and folders in Windows Explorer.

A *shortcut* (see Figure 1-26) is an icon or link that gives you quick access to an original resource. The links you see in Control Panel are also considered shortcuts. Because a shortcut only points to a resource, deleting a shortcut does not delete the actual item. You can usually distinguish a shortcut icon from the original item it refers to because the shortcut has a small arrow in the shortcut icon's lower-left corner.

Figure 1-26

Shortcut icons



If you regularly access a particular folder, for example, you can create a shortcut to that folder on the desktop. Whenever you want to open that folder, double-click the icon instead of launching Windows Explorer and navigating to the folder to open it.

Ð

CREATE AND DELETE A SHORTCUT

GET READY. To create a folder shortcut on the desktop, perform the following steps.

- **1.** In File Explorer, point to the folder for which you want to create a shortcut.
- 2. Right-click the folder and choose Send To > Desktop (create shortcut).
- **3.** To delete a shortcut icon:
- **4.** Right-click it, choose **Delete**, and then click **OK**. The shortcut is removed and sent to the Recycle Bin.

Understanding Group Policy

Group Policy is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment. For example, you can use Group Policy to specify how often a user must change his password, set the desktop background image and screensaver on a person's computer, or configure spell-checking so that it is required before a user can send an email.

There are literally thousands of settings that can be used to restrict certain actions, make a system more secure, or standardize a working environment. A setting can control a computer registry, NTFS security, an audit and security policy, software installation, folder redirection, offline folders, or log on and log off scripts. Group Policy is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy (see Figure 1-27) provides the centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment. As each server version is released, Microsoft usually adds additional parameters.

Group Policy objects (GPOs) are collections of user and computer settings, including the following:

- System settings: Application settings, desktop appearance, and behavior of system services.
- Security settings: Local computer, domain, and network security settings.
- Software installation settings: Management of software installation, updates, and removal.
- Scripts settings: Scripts for when a computer starts or shuts down and for when a user logs on and off.
- **Folder redirection settings**: Storage for users' folders on the network. For example, the *Redirect to the local user profile location* option will move the location of the folder to the local user profile under the Users folder.

APPLYING GROUP POLICY

Group Policy can be set locally on a workstation or set at different levels (site, domain, or organizational unit) within Active Directory. Generally speaking, you will not find as many settings locally as you will at the site, domain, or OU level. When group policies are applied, they are applied in the following order:

- 1. Local
- 2. Site
- 3. Domain
- 4. OU



Group Policy Editor

	Thep					
Console Root	Setting			State	Comment	Actions
Local Computer Policy	E Force a specific default lock screen image			Not configured	No	Personalization
Computer Configuration	📔 Prevent changi	ing lock screen image	Not configured	No	More Actions	
Windows Settings	Prevent changi	ing start menu backgrou	und	Not configured	No	
Windows Settings	📄 🗈 Do not display	the lock screen		Not configured	No	Prevent changin
Scripts (Startup/Shutdown)	📄 Prevent enablir	ng lock screen camera		Not configured	No	More Actions
E Denloved Printers	📔 Prevent enablir	ng lock screen slide sho	N	Not configured	No	
B Security Settings	Force a specific	c background and accer	nt color	Not configured	No	
Policy-based OoS	Force a specific	c Start background		Not configured	No	
Administrative Templates						
Control Panel						
Personalization		Р	revent chance	ging start menu background	ł	_ 🗆 🗙
Regional and Language Op			-	, , , , , , , , , , , , , , , , , , , ,		
🔛 User Accounts	Prevent cha	anging start menu back	ground	Draviour Satting	Novt Sotting	
Detwork	L.C.			Previous setting	Next Setting	
Printers		. Comment				
Server	Not Configu	ured				^
Start Menu and Taskbar	🔘 Enabled					
System	0.05.11.1					~
Windows Components	Disabled	Supported on				
All Settings		supported on.	At least Wind	ows Server 2012, Windows 8 or Wir	ndows RT	^
▲ 10 User Configuration						~
Software Settings						
Windows Settings	Options:			Help:		
Administrative remplates				7		
Desisten				Prevents users from changing	the look of their sta	art menu
Desktop				background, such as its color o	or accent.	
Shared Folders				By default, users can change the	he look of their star	t menu
Start Menu and Taskhar				background, such as its color o	or accent.	
Start Mend and Taskbar				Kanan anakirahirahirahi		d also al a 6 a
Windows Components				start menu background and co	iser will be assigned	a the default
All Settings	-			change them.	sions and will not b	c anowed to
>	7					
etting(s)				If the "Force a specific backgro	ound and accent co	olor" policy is

Path

- 0 - 5

Figure 1-28		Group Policy Management
Figure 1-28 The Group Policy Management Console	Image: Second system Image: Second system <td>Group Policy Management Default Domain Policy Scope Details Settings Delegation Status Links Display links in this location: The following sites, domains, and OUs are linked to this GPO: Location Control Control Control Context Cont</td>	Group Policy Management Default Domain Policy Scope Details Settings Delegation Status Links Display links in this location: The following sites, domains, and OUs are linked to this GPO: Location Control Control Control Context Cont
	 ▶ ∰ VMI Fitters ▶ ∰ Starter GPOs ▶ ∰ Stes ₩ Group Policy Modeling ₩ Group Policy Results 	Security Filtering The settings in this GPO can only apply to the following groups, users, and computer Name Authenticated Users

If you configure a Group Policy setting at the site, domain, or OU level and that setting contradicts a setting configured at the local policy level; the local policy setting will be overridden. Generally speaking, if you have a policy setting that conflicts with a previous executed setting, the more recent executed setting remains in effect (see Figure 1-28).

Properties

✓ Open

ACCESS THE LOCAL GROUP POLICY EDITOR

GET READY. You can open the Local Group Policy Editor by using gpedit.msc at a command line or by using the Microsoft Management Console (MMC). To open the Local Group Policy Editor from the command line, perform the following steps.

- 1. Open MMC by clicking **Start**, clicking in the Start Search box, typing mmc, and then pressing Enter.)
- 2. On the File menu, click Add/Remove Snap-in.
- 3. In the Add or Remove Snap-in dialog box, click Group Policy Object Editor, and then click Add.
- **4.** In the Select Group Policy Object dialog box, click **Browse**.

Add.

This GPO is linked to the following WMI filter

WMI Filterin

<none>

- 5. Click This computer to edit the Local Group Policy object, or click Users to edit Administrator, Non-Administrator, or per-user Local Group Policy objects.
- 6. Click Finish.

Most times, you only need to access the security settings that you found in the local policy. This can be done by opening the Local Security Policy from Administrative Tools.

CONFIGURING GROUP POLICY SETTINGS

There are thousands of settings available with group policies. In addition, as each version of Windows is released, new settings are added to allow administrators to configure new technology that has been added to Windows, provide control that was not available previously, or provide more granular control.

As discussed, group policies are organized according to computer settings (contained in the Computer Configuration node) and user settings (contained in the User Configuration node). The *Computer Configuration* node contains settings that are applied to the computer regardless of who logs on to the computer. By default, computer settings are applied when the computer is started. The *User Configuration* node contains settings that are applied when the user logs on. Group policy settings are refreshed every 90 minutes with a random delay of 30 minutes (giving a random range between 90 minutes and 120 minutes). On domain controllers, group policies get refreshed every five minutes.

Starting with Windows Server 2008, the Computer Configuration and User Configuration nodes are divided into Policies and Preferences nodes. Policies include the traditional settings that were available with earlier versions of Windows, but also have many new settings that were not available previously. Preferences allow you to configure additional Windows settings that were not available previously and they allow more control on how the settings are applied to the clients.

Computer Configuration\Policies can be organized according to the following nodes:

- **Software Settings**: Contains only one node, Software installation, which allows you to install and maintain software within your organization.
- Windows Settings: Allows you to configure Windows settings, including Name Resolution Policy, Scripts (Startup/Shutdown), Security Settings, and Policy-Based QoS nodes.
- Administrative Templates: Contains registry-based Group Policy settings that are used to configure the computer environment, such as the Control Panel, Printers, System, and Windows components.

Software Configuration\Policies can be divided into the following nodes:

- **Software Settings**: Contains only one node, Software installation, which allows you to install and maintain software within your organization.
- Windows Settings: Allows you to configure Windows settings, including Scripts (Logon/Logoff), Security Settings, Folder Redirection, and Policy-Based QoS nodes.
- Administrative Templates: Contains registry-based Group Policy settings that are used to configure the user environment, such as the Control Panel, Printers, System, and Windows components.

USING ADMINISTRATIVE TEMPLATES

Windows 10 includes thousands of Administrative Template policies, which contain registrybased policy settings that are used to configure the user and computer environment. For example, to configure the user's desktop image or a default screen saver, you would use an Administrative Template policy.

Administrative Templates can be located under both Computer Configuration and User Configuration. The requirements for an Administrative Template setting, such as which operating system supports the setting and the description of the feature, are displayed:

- On the Extended tab when you click to select an Administrative Template setting
- When you double-click an Administrative Template setting

When configuring Administrative Templates, there are three states:

- Not Configured: The registry key is not modified or overwritten.
- **Enabled**: The registry key is modified by this setting.
- **Disabled**: The Disabled settings undo a change made by a prior Enabled setting.

If you want to undo the group policy, removing the group policy does not necessarily remove the setting from a computer that has the setting configured with a GPO. In these cases, you need to change the policy to Disabled (or create a second policy) and is applied to the computer and/or user. After the policy is applied, the policy can be removed. The policy can also be manually removed using the registry editor (HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies and HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Policies).

Some Administrative Templates will be used to configure a setting such as specifying a desktop image or specifying a screen saver. Although these settings are configured with group policies, some of these settings can be changed while the computer is running. However, when the group policy is reapplied, the setting will revert back to the setting defined with the GPO. Other settings will used to lock down a computer so that users cannot modify a setting or hide the setting from the user.



CONFIGURE THE DESKTOP BACKGROUND IMAGE WITH GROUP POLICIES

GET READY. To configure the desktop background image with group policies, perform the following steps.

- 1. Open the Group Policy Management Editor for the GPO you want to configure.
- Navigate to User Configuration\Policies\Administrative Templates\Desktop\ Desktop.
- 3. Double-click Desktop Wallpaper. The Desktop Wallpaper dialog box opens.
- 4. Click Enabled.
- 5. In the Wallpaper Name text box, type the path and name of an image file.
- 6. Click **OK** to close the Desktop Wallpaper dialog box. The Desktop Wallpaper shows as Enabled.
- 7. Close the Group Policy Management Editor window.

Configuring Drive Encryption

THE BOTTOM LINE

Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, that file remains encrypted when the file is stored on disk. *Decryption* is the process of converting data from encrypted format back to its original format. You can use encryption to help protect files on a computer.

CERTIFICATION READY Configure drive encryption 1.3 Today, newer versions of Windows offer two file encrypting technologies: Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders; BitLocker protects entire volumes.

Preparing for File Encryption

Encrypting File System (EFS) can encrypt files on an NTFS volume and those files cannot be used unless the user has access to the keys required to decrypt the information. By default, when you encrypt a file with EFS, the file or folder turns green to show that the file is encrypted.

After a file has been encrypted, you do not have to manually decrypt an encrypted file before you can use it. Instead, you work with the file or folder just like any other file that is not encrypted. When you open a file that is encrypted with EFS, the file is automatically

decrypted as needed. When you save the file, it is automatically decrypted. However, if another user tries to access the same file, he cannot open it because he does not have the proper key to open the file.

EFS uses an encryption key to encrypt the data, which is stored in a digital certificate. The first time a user encrypts a file or folder, an encryption certificate and key are created and bound to the user account. The user who creates the file is the only person who can read it. As the user works, EFS encrypts the files using a key generated from the user's public key. Data encrypted with this key can be decrypted only by the user's personal encryption certificate, which is generated using a private key.

CONFIGURING EFS

To encrypt or decrypt a folder or file, enable or disable the encryption attribute just as you set any other attribute, such as read-only, compressed, or hidden. If you encrypt a folder, all files and subfolders created in the encrypted folder are automatically encrypted. Microsoft recommends that you encrypt at the folder level. You can also encrypt or decrypt a file or folder using the Cipher command.



ENCRYPT A FOLDER OR FILE USING EFS

GET READY. To encrypt a folder or file, perform the following steps.

- 1. Right-click the folder or file you want to encrypt and choose **Properties**. The Properties dialog box opens.
- 2. Click the **General** tab, and then click **Advanced**. The Advanced Attributes dialog box appears (see Figure 1-29).

/ turui			no acc.								
*	1	Choo	se the :	settings	s you wa	nt for t	this	folder			
¥		When asked as we	i you d l if you ll.	ick OK d want ti	or Apply ne chang	on the jes to a	Pro	bertie t all s	s diale ubfol	og, you ders ar	u will be nd files
Arch	hive	e and	Index a	attribut	es						
	Fol	der is	ready f	for arch	ivina						
	1 01	10110	cuuy i	or arch	iving .						
	Allo	w file pertie	s in this	folder	to have	conter	nts ir	dexe	d in a	ddition	to file
Com	Alla	w file pertie	s in this s Encryp	folder ot attrib	to have	conter	nts ir	ndexe	d in a	ddition	to file
Com	Alla pro	w file pertie ess or mpres	s in this s Encryp s conte	of alter of attrib	to have utes ave disk	conter	nts ir	ndexe	d in a	ddition	to file

- **3.** Select the **Encrypt contents to secure data** checkbox.
- **4.** Click **OK** to close the Advanced Attributes dialog box.
- 5. Click **OK** to close the Properties dialog box.
- 6. If you encrypt a file in an unencrypted folder, a warning appears. If you want to encrypt only the file, select **Encrypt the file only** and then click **OK**. If you want to encrypt the folder and all content in the folder, select the **Encrypt the file and its parent folder (recommended)** option. Click **OK**.
- 7. If you encrypt a folder, a message prompts you to confirm the changes. If you want to encrypt only the folder, select Apply changes to this folder only. If you want to apply to all folders, select Apply changes to this folder, subfolders and files. Click OK to close the Confirm Attribute Changes dialog box.

Figure 1-29 The Advanced Attributes dialog box

DECRYPT A FOLDER OR FILE

GET READY. To decrypt a folder or file, perform the following steps.

- 1. Right-click the folder or file you want to decrypt and choose **Properties**. The Properties dialog box opens.
- 2. Click the **General** tab and then click **Advanced**. The Advanced Attributes dialog box opens.
- 3. Clear the Encrypt contents to secure data checkbox.
- 4. Click OK to close the Advanced Attributes dialog box.
- 5. Click **OK** to close the Properties dialog box.
- 6. When you are prompted to confirm the changes, click OK. When you want to decrypt only the folders, select Apply changes to this folder only. When you want to apply to all folders, select Apply changes to this folder, subfolders and files.

When working with EFS, keep the following in mind:

- You can encrypt or compress NTFS files only when using EFS; you can't do both. If the user marks a file or folder for encryption, that file or folder is uncompressed.
- If you encrypt a file, it is automatically decrypted if you copy or move the file to a volume that is not an NTFS volume.
- Moving unencrypted files into an encrypted folder automatically causes those files to be encrypted in the new folder.
- Moving an encrypted file from an EFS-encrypted folder does not automatically decrypt files. Instead, you must explicitly decrypt the file.
- Files marked with the System attribute or that are in the root directory cannot be encrypted.
- Remember that an encrypted folder or file does not protect against the deletion of the file, listing the files or directories. To prevent deletion or listing of files, use NTFS permissions.
- Although you can use EFS on remote systems, data that is transmitted over the network is not encrypted. If encryption is needed over the network, use *SSL/TLS (Secure Sockets Layer/Transport Layer Security)* or IPsec. SSL/TLS uses a digital certificate to encrypt a web page such as when you access an https:// website using a browser. *Internet Protocol Security (IPsec)* is a protocol suite that secures IP communications by authenticating and encryption each IP packet of a communication session.

Configuring BitLocker

Unlike EFS, BitLocker allows you to encrypt the entire volume. Therefore, if a drive or laptop is stolen, the data is still encrypted even if the thief installs it in another system for which he is an administrator.

BitLocker Drive Encryption (BDE) is the feature in Windows since Windows Vista and Windows Server 2008 that can use a computer's **Trusted Platform Module (TPM)**, which is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft. BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at startup, and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. BitLocker Drive Encryption also stores measurements of core operating system files in the TPM.



- **TPM + startup PIN + startup key**: The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a personal identification number (PIN) and insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup key**: The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup PIN**: The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a PIN before the system can unlock the BitLocker volume and complete the system boot sequence.
- **Startup key only**: The BitLocker configuration process stores a startup key on a USB flash drive, which the administrator must insert each time the system boots. This mode

does not require the server to have a TPM chip, but it must have a system BIOS that supports access to the USB flash drive before the operating system loads.

• **TPM only**: The system stores the BitLocker volume encryption key on the TPM chip, and accesses it automatically when the chip has determined that the boot environment is unmodified. This unlocks the protected volume and the computer continues to boot. No administrative interaction is required during the system boot sequence.

When you use BitLocker on fixed and removable data drives that are not the OS volume, you can use one of the following:

- Password
- Smart card

Figure 1-30

Automatic Unlock

When you enable BitLocker using the BitLocker Drive Encryption control panel, you can select the TPM + startup key, TPM + startup PIN, or TPM only option. To use the TPM + startup PIN + startup key option, you must first configure the Require additional authentication at startup Group Policy setting, found in the Computer Configuration\Policies\ Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives container.

DETERMINE WHETHER YOU HAVE TPM

GET READY. To find out whether your computer has TPM security hardware, perform the following steps.

- 1. Open the Control Panel.
- 2. Click System and Security and click BitLocker Drive Encryption. The BitLocker Drive Encryption window opens (see Figure 1-30).

Figure 1-30	Real BitLocker Drive Encryption					×
The BitLocker Drive Encryption window	← → ▼ ↑ 🏘 « All Control Panel Items > BitLocker Drive Encryption V 🖏 Search Com					٩
	Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorize	d access by prot	tecting your drives with Bi	itLocker.	0
		Operating system drive				
		C: BitLocker off		6)	
		•	Turn on BitLock	ter		
		Fixed data drives				
		Removable data drives - BitLocker To Go Insert a removable USB flash drive to use BitLocke) r To Go.			
	See also					
	TPM Administration Disk Management					
	Privacy statement					

3. In the left pane, click TPM Administration. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

The TPM Management on Local Computer snap-in tells you whether your computer has the TPM security hardware. If your computer doesn't have it, you'll need a removable USB memory device to turn on BitLocker and store the BitLocker startup key that you need whenever you start your computer.

If your computer does not have TPM and you need to encrypt the C drive with BitLocker, you will have to set the Allow BitLocker without a compatible TPM option to Require additional authentication at startup using a GPO. This setting is located at Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives. Doubleclick the Require additional authentication at startup setting, select Enabled, and select the Allow BitLocker without a compatible TPM option. Click OK to save the new setting.

TURN ON BITLOCKER

GET READY. To turn on BitLocker for the C drive on a computer running Windows 10, perform the following steps.

- 1. Click Start and then click the Control Panel.
- Click System and Security and then click BitLocker Drive Encryption. The BitLocker Drive Encryption window opens.
- **3.** Click **Turn on BitLocker** for the volume that you want to encrypt. A BitLocker Drive Encryption (X:) window opens.

MORE INFORMATION

If your computer has a TPM chip, Windows provides a TPM Management console that you can use to change the chip's password and modify its properties.

- **4.** On the Choose how you want to unlock this drive page, select **Enter a password**. Type a password in the Enter your password text box and the Reenter your password text box. Click **Next**.
- 5. On the How do you want to back up your recovery key? page, click Save to a file.
- 6. In the Save BitLocker recovery key as dialog box, click Save.
- 7. After the file is saved, make sure the key is stored in a safe place. Then click Next.
- 8. On the Are you ready to encrypt this drive page, the *Run BitLocker system check* option is already selected. Click **Continue**.
- 9. When a message indicates the computer must be restarted, click Restart now.

When the encryption process is complete, you can open the BitLocker Drive Encryption Control Panel to ensure that the volume is encrypted or to turn off BitLocker, such as when you want to perform a BIOS upgrade or other system maintenance.

The BitLocker Control Panel applet enables you to recover the encryption key and recovery password at will. Figure 1-31 shows the following options available after you use BitLocker to encrypt a drive:

- Back up your recovery key
- Change password
- Remove password
- Add smart card
- Turn on auto-unlock
- Turn off BitLocker

You should consider carefully how to store this information, because it allows access to the encrypted data. It is also possible to escrow this information into Active Directory.

Figure 1-31

The BitLocker applet options for a BitLocker-encrypted volume

# BitLocker Drive Encryption			- U
All Co	ontrol Panel Items > BitLocker Drive Encryption	✓ ບ້ Search Co	ntrol Panel
Control Panel Home	Bitl ocker Drive Encryption		
	Hole protect your files and folders from up	aputhorized access by protecting your a	lrives with Ritl ocks
	Help protect your files and folders from ur	nautriorized access by protecting your o	INVES WITH DILLOCKE
	Operating system drive		
	C: BitLocker off		\bigcirc
		🗣 Turn on BitLocker	
	Fixed data drives		
	New Volume (E:) BitLocker on		\bigcirc
	6	Back up your recovery key	
		Change password	
		Add smart card	
		Turn on auto-unlock	
		Turn off BitLocker	
	Removable data drives - BitLock	er To Go	
See also	Insert a removable USB flash drive to us	e BitLocker To Go.	
TPM Administration			
Disk Management			
Privacy statement			

Standard users can change the password or PIN if they know the current PIN or password. By default, a user has five attempts to type the current PIN or password. When this happens, the administrator has to reset the volume PIN or password or the system needs to be rebooted. To make sure that password or PIN is not too easy to guess, you can define how complex the password is by using a group policy. To define the complexity, enable and configure the Configure use of passwords for fixed data drives settings found in Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\.

Configuring Updates



Intruders and some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or other software applications. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes.

Microsoft routinely releases security updates on the second Tuesday of each month, commonly known as *Patch Tuesday*. However, in the future, Microsoft might release patches as soon as they become available.

Because computers are often used as production systems, you should test any updates to make sure they do not cause problems for you. Although Microsoft performs intensive testing, occasionally problems do occur, either as a bug or as a compatibility issue with third-party software. Therefore, always be sure you have a good backup of your system and data files before you install patches so that you have a back-out plan if necessary. Figure 1-32

CERTIFICATION READY Configure updates	
1.4	
	_

Understanding Windows Update

Windows Update provides your Windows 10 users with a way to keep their computers current by checking a designated server. The server provides software that patches security issues, installs updates that make Windows and your applications more stable, fixes issues with existing Windows programs, and provides new features. The server can be hosted by Microsoft or it can be set up and managed in your organization by running the Windows Server Update Services (WSUS) or Configuration Manager.

When you first install Windows 10, you can choose how you want Windows Update to function. On a Windows 10 computer, you can open Settings and click Update & security to open the Windows Update page (see Figure 1-32).



By clicking Advanced options, you can configure for Automatic updates, give updates for other Microsoft products when Windows is updated, defer upgrades, and view your update history (as shown in Figure 1-33).

If your computer is part of an enterprise infrastructure, the enterprise organization might automatically configure the update settings via a local Group Policy or a domain-based Group Policy for your user and/or computer account. Group Policy settings related to Windows Update can be found in the following locations:

- Computer Configuration > Policies\Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates
- User Configuration > Policies > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates

For corporations, you can also use Windows Server Update Service (WSUS) or System Center Configuration Manager to keep your systems updated. Smaller organizations might use WSUS or cloud-based services such as Microsoft Intune to keep systems up-to-date. The advantage of using one of these systems is that it allows you to test the patch, schedule the



updates, and prioritize client updates. Once you determine a patch is safe, you can enable it for deployment.

If you click the Choose how updates are delivered option, the Updates from more than one place page displays (see Figure 1-34). Unless you are part of a corporation that is using WSUS or Configuration Manager, you must use your Internet connection to retrieve updates from Microsoft. Starting with Windows 10, you can enable the Updates from more than one place option, which also allows you to get updates from other computers on the same network as your local computer and from computers on the Internet.



Figure 1-34

The Updates from more than one place page

Understanding App Updates

As applications became more sophisticated, they were provided more access so that they could do more on a system. Unfortunately, it was not long before these apps became targets of intruders and malware. To fix problems with applications and to keep a system or device secure, you need to keep applications current with the latest updates.

For Microsoft applications, you can find Microsoft updates using Windows Update, WSUS, Configuration Manager, or Microsoft Intune. To enable updates for Microsoft applications, you can click Change settings and then select the Give me updates for other Microsoft products when I update Windows option.

Some non-Microsoft products also release regular updates. Some of these applications (such as Adobe products, and Java) have mechanisms that will automatically check for updates and notify you that updates are available or they will automatically install those updates.

Understanding Device System Updates

For all intents and purposes, mobile devices (including smart phones and tablets) are computers that can run a wide range of applications. Since these devices usually contain personal and corporate information, these devices are also targets of intruders and malware. Therefore, you need to keep the operating system and the applications up-to-date so that security patches can be applied as they are released.

Applications on smart phones and tablets are usually updated through stores such as Microsoft Store, Google Play, and iTunes. Fortunately, these stores offer mechanisms to notify you when updates are available and to automatically install these updates as they become available. For example, for Windows 10 store the live tile for the Store app change to indicate the number of app updates that were available, launch the Store app, click the updates link, select all the updates, click Install. By default, Windows 10 has been automated, whereas these updates are automatically downloaded and installed as soon as they are available with no user interaction.

SUMMARY SKILL MATRIX

IN THIS LESSON YOU LEARNED:

- Windows 10 is a robust and flexible system that is made to work on and support a wide range of hardware. For example, Windows 10 can work on a tablet, a laptop, or a desktop computer. Windows 10 also supports mobile devices so that you can take your computer or device with you while accessing your files and programs.
- Microsoft accounts enable you to synchronize your desktop across multiple Windows 10 devices.
- A user account is used to identify a user or other identity on a system, which can be used in authentication, authorization, and auditing. In Windows, user accounts provides different levels of control over the organization's computers and resources. Microsoft accounts enable you to synchronize your desktop across multiple Windows 10 devices.
- A computer is a collection of hardware devices, each of which requires a piece of software called a device driver in order to function. Windows 10 includes a large library of device drivers, but it is still sometimes necessary to obtain them yourself. Device Drivers are managed by the Devices and Printers folder and Device Manager.

- Group Policy is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.
- Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. Decryption is the process of converting data from encrypted format back to its original format. To help protect files on a computer, you can use encryption.
- Today, newer versions of Windows offer two file encrypting technologies: Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders; BitLocker protects entire volumes.
- Intruders and some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or other software applications. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes.

Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

- 1. ______ enable you to synchronize your desktop across multiple Windows 10 devices.
- **2.** A ______ is a series of folders, associated with a specific user account that contains personal documents and settings.
- **3.** The ______ is a microchip that is built into a computer.
- 4. To protect computers against intruders and malware, you must _____
- 5. A Windows application that has dynamic content can be viewed at any time from
- 6. The primary configuration tool for Windows is the _____.
- 7. Computer Management, Event Viewer, and GPO Editor are based on the _
- 8. For a device to operate in Windows, you must install a _____
- 9. ______ is the process of converting data into a format that cannot be read by another user.
- **10.** The ______ shows important notifications related to the security and maintenance of your computer.

Multiple Choice

Circle the letter that corresponds to the best answer.

- 1. Which of the following are types of user accounts used in Windows 10? (Choose all that apply)
 - a. Domain-based accounts
 - b. Local user accounts
 - c. Microsoft accounts
 - d. Computer centric accounts

- 2. In Windows 10, how can you minimize network traffic when downloading Windows updates?
 - **a.** You can enable file caching.
 - **b.** You can enable the WriteFile function.
 - c. You can enable the Updates from more than one place option.
 - d. You can enable Internet Sharing.
- 3. Which of the following is the best place to manage printers and print drivers?
 - a. Device Manager
 - b. Devices and Printers folder
 - c. Print Manager
 - d. Print Configuration Tool
- 4. In Device Manager, which of the following indicates that a device is not functioning properly?
 - **a.** A red "X
 - **b.** A blue question mark inside white circle
 - c. A black exclamation point on yellow field
 - d. A white circle with down arrow
 - e. A yellow warning symbol with exclamation point
- 5. Which type of profile allows a user within a corporation to use the same user profile no matter what computer that user accesses?
 - a. Local user profile
 - **b.** Persistent user profile
 - c. Roaming user profile
 - **d.** Mandatory user profile
- 6. Which of the following allows you to encrypt an entire volume on a mobile computer?
 - **a.** EFS
 - **b.** DFS
 - c. SSL
 - **d.** BitLocker
- 7. You have updated the device driver for a network adapter, but now the adapter is not being recognized. What should you do?
 - a. Check to see if there is a newer driver
 - **b.** Roll back the driver
 - c. Reinstall Windows
 - d. Run Windows update
- **8.** You want to configure several computers to use the same desktop background and screensaver settings. What is the best way to ensure that all systems are compliant with these settings?
 - a. Use Group Policy
 - **b.** Manually configure the systems
 - c. Modify the registry
 - d. Generate roaming profiles
- **9.** What is the easiest way to ensure all of your computers include the newest Windows updates while still ensuring that those updates do not cause any problems for the users?
 - a. Use Task Scheduler
 - **b.** Use WSUS
 - c. Use Windows updates
 - **d.** Use GPOs
- 10. You install an application and now the system does not boot properly. What should you do?
 - **a.** Roll back the application
 - **b.** Reinstall the application
 - c. Run Windows Update
 - d. Boot the system into safe mode

True / False

Circle T if the statement is true or F if the statement is false.

- **T** | **F** 1. To see the version of Windows, the name of the computer, and the amount of memory, you can open System Properties.
- $\mathbf{T} \mid \mathbf{F} \mid \mathbf{2}$. To keep a computer secure, you need only to install all new Windows updates.
- T F 3. You have applications on your Windows phone that you downloaded from the Microsoft Store. The best way to keep these applications up-to-date is to visit the Windows Update website.
- $\mathbf{T} \mid \mathbf{F} \mid \mathbf{4}$. The most effective way to protect a document is to use NTFS permissions.
- **T** | **F** 5. For a large organization, you should use Microsoft accounts to manage rights and permissions.

Case Projects

Scenario 1-1: Syncing Settings

You own a small business, and to make it easier for you to work whenever needed, you have a desktop computer at home, a desktop computer at your office location, and a laptop—and all machines are running Windows 10. Describe how to ensure that all of the settings are the same for all machines.

Scenario 1-2: Distributing Windows Updates Across a Network

You support Richman Investments, a brokerage firm that employs 20 brokers. Each broker has his own client computer, and the firm has a server running Windows Server. All of the client computers are configured identically.

Over the past six months, some Windows updates have caused the computers to hang, leaving the brokers without computers to conduct business. How can you ensure that the Windows updates that install on client computers will not cause usability issues?

Scenario 1-3: Protecting Laptop Computers

Henry, a traveling salesperson at your company, left his laptop at the airport on his last trip. The laptop was never recovered. His new laptop arrived yesterday and you installed Windows 10 Enterprise and productivity applications and restored data from a backup. What should you do to the laptop to protect all programs and data on the computer in the event of loss or theft?

Scenario 1-4: Standardizing a User's Work Environment

You administer a network in which many of the computers are shared among users and people often use different computers based on where they work. Therefore, you need to configure the following:

- Users must be able to access all documents that they store in their Documents and Desktop folders.
- Users should also have an application installed so that they can clock in and out.

How can you accomplish this?



LESSON

Understanding Data Access and Management

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	OBJECTIVE DOMAIN NUMBER
Understanding Cloud Storage Services Understanding OneDrive Understanding OneNote Understanding Outlook Understanding Microsoft Office 365 Using Azure Storage 	Describe cloud storage services	2.1
 Understanding Local Storage Creating Storage Pools Creating Storage Spaces 	Describe local storage	2.2
Understanding File Systems	Describe file systems	2.3
Understanding File and Print Sharing Setting NTFS Permissions Creating Effective NTFS Permissions Sharing Drives and Folders Using HomeGroup Mapping Drives Sharing Printers 	Describe file and print sharing	2.4
 Understanding Data Encryption Understanding Certificates and Their Use Managing Certificates Understanding Certificate Services Moving and Copying EFS-Encrypted Folders Using BitLocker to Go Using a Virtual Private Network (VPN) 	Describe data encryption	2.5

KEY TERMS

access control entry (ACE) Access Control List (ACL) Active Directory Certificate Services (AD CS) advanced sharing asymmetric key Azure Storage Billing Administrator

BitLocker To Go certification path	Microsoft CHAP version 2 (MS-CHAP v2)	public key infrastructure (PKI) remote access server (RAS)
certificate authority (CA)	Microsoft Office 2016	Resilient File System (ReFS)
certificate chain	Microsoft Office 365	root CA
Challenge Handshake	Microsoft Outlook	Secure multipurpose Internet
Authentication Protocol	Outlook Web App (OWA)	Mail Extension (S/MIME)
(CHAP)	multi-booting	Secure Socket Layer (SSL)
digital certificates	NTFS permissions	Secure Socket Tunneling
digital signature	OneDrive	Protocol (SSTP)
effective permissions	OneDrive desktop app for	Service Administrator
enterprise CA	Windows	shared folder
explicit permissions	OneNote	simple (no resiliency)
Extensible Authentication	parity	smart card
Protocol (EAP-MS-CHAPv2)	Password Administrator	standalone CA
FAT	Password Authentication	storage pool
FAT32	Protocol (PAP)	Storage Spaces
fetching	permission	subordinate CA
file system	Point-to-Point Tunneling	symmetric encryption
Global Administrator	Protocol (PPTP)	thin provisioning
hash function	Pretty Good Privacy (PGP)	three-way mirror
HomeGroup	print device	Transport Laver Security (TLS)
inherited permissions	printer	two-way mirror
Internet Key Exchange Version	printer permissions	universal naming convention
2 (IKEv2)	private key	(UNC)
Layer 2 Tunneling Protocol	public cloud	User Management
(L2TP)	public cloud services	Administrator
locally redundant storage	public folders	Virtual Private Network (VPN)
(LRS)	public key	VPN Reconnect
mapped drive	nublic kov cryptography	zono rodundant storago (7PC)

As an administrator at the Contoso Corporation, you are responsible for many of the resources and services that the users of the corporation use. You need to ensure that those users can access necessary resources and services so that they can perform the duties of their jobs. You also need to ensure that unauthorized users do not have access to those resources and services.

Understanding Cloud Storage Services

THE BOTTOM LINE

Using public cloud services such as OneDrive and Office 365 enable you to take advantage of hosted solutions. This means users have the ability to access their information from anywhere at any time across multiple devices. By using cloud-based services, users can collaborate via calendars, email, and through document sharing. From an administrative perspective, it means you gain access to services and programs without the additional overhead of main-tenance and software upgrades.

CERTIFICATION READY Describe cloud storage services 2.1

Public cloud services provide a way to access information from anywhere at any time. There are many definitions for the cloud. Microsoft defines a *public cloud* as a web-based service that is hosted outside of your organization. This means the information technology infrastructure (hardware, servers, software, and so on) is located somewhere other than your office and is managed by a third party (such as hosted). If you use mobile banking—accessing web-based email or storing your photos online in one of the many services provided—you are interacting with "the cloud."

Understanding OneDrive

OneDrive, formerly named SkyDrive, is a file-hosting service that allows you to store and create files and folders and share them with other users and groups.

OneDrive is a free, secure file-hosting service that enables your users to store, synch, and share files across devices using the cloud. Using OneDrive, you can create folders, create or upload files, and share your documents with others. You can also use it to synchronize files and folders that you select across multiple devices. If you forget to include a file within your synch folder, you can use OneDrive to connect to your remote computer, locate the file, and then upload it to your OneDrive space. This process is called *fetching*.

Microsoft offers two forms of OneDrive:

- OneDrive is free online personal storage that you get with a Microsoft account or Outlook.com. Currently, it offers 15 GB of free space. You can purchase additional storage space as you need it.
- OneDrive for Business is online storage intended for business purposes and it's built on online SharePoint. It is managed by your organization and it lets you share and collaborate work documents with coworkers. OneDrive for Business is included with Office 365.

ACCESSING ONEDRIVE AND ONEDRIVE FOR BUSINESS FROM A BROWSER

You can access OneDrive from a browser using your Microsoft account from anywhere you have an Internet connection via http://onedrive.live.com. After reaching the site, you are prompted to log in using your Microsoft account. After you are logged on, you see your OneDrive Dashboard (see Figure 2-1), in which you can upload, download, create, and share folders and files. If your computer is configured to support fetching, you can also connect to it remotely from the OneDrive Dashboard.

The following provides an overview of each of the options available with the OneDrive for Business Dashboard, as shown in Figure 2-2:

- **Documents:** Includes folders created on the OneDrive account. You can also see the number of files each folder contains by looking at the number located in the lower-right corner of each folder. Selecting any of these folders opens and displays its content.
- **Recent:** Includes a list of documents that have been recently created on the OneDrive account.
- Shared with me: Provides a list of documents or folders that have been shared with you.
- **Followed:** Allows you to bookmark a file so that you can follow the file to track updates.
- Site folders: Allows users to go directly to the document libraries within a site.
- **Groups:** Displays a list of groups that includes users with whom you frequently communicate and share documents. When you create a group, users receive emails asking them to join.



Figure 2-2

Figure 2-1

The OneDrive Dashboard

The OneDrive for Business Dashboard



After clicking the link, they are taken to the Groups page, in which they can communicate with other members via email and also view any files that have been shared to the group.

• **Recycle bin:** By default, OneDrive storages your deleted files in a Recycle bin for at least 3 days and a maximum of 30 days. If the Recycle bin gets large enough to exceed 10% of your storage, the duration will be reduced.

CREATING A FILE WITHIN ONEDRIVE AND ONEDRIVE FOR BUSINESS

OneDrive and OneDrive for Business allows you to collaborate with others users on documents (provided those users have Microsoft accounts.) Because documents are stored on the cloud, you can access these documents anytime you are connected to the Internet.

OneDrive and OneDrive for Business include a light version of Microsoft Office apps (Word, Excel, PowerPoint, and OneNote). This allows you to create and edit documents directly from your browser.

CREATE A WORD DOCUMENT WITHIN ONEDRIVE USING A WEB BROWSER

GET READY. To create a Word document within OneDrive using a web browser, log in to a Windows 10 computer with access to the Internet and then perform the following steps.

- 1. Open Internet Explorer, go to http://onedrive.live.com, and then click Sign In.
- 2. Type your Microsoft User Account and Password.
- 3. Click the Documents folder.
- **4.** From the menu at the top of the page, click **Create > Folder**.
- 5. Name the folder Project Files and then click the folder to open it.
- 6. From the menu at the top of the page, click Create > Word document.
- **7.** Type a few words in the document (see Figure 2-3).
 - As you type text, The Word document will be saved frequently.



- 8. To specify a file name, click **Document1** at the top of the window and then replace that name by typing **Project Scope**.
- 9. Click the **OneDrive** link (located at the upper-left corner, next to Word Online) to return to the main screen.

TAKE NOTE*

Figure 2-3

To access OneDrive and complete these steps, you need a Microsoft User Account.

UPLOADING FILES TO ONEDRIVE AND ONEDRIVE FOR BUSINESS

If you have existing files on your computer that you want to upload to OneDrive and OneDrive for Business, you can use either of the following two options:

- From the OneDrive Dashboard, navigate to the folder in which you want to store the file. On the menu, click Upload, browse to the file you want from your computer, and then click Open.
- From the OneDrive app installed on your local computer, you can drag and drop the files you want to upload into the OneDrive folder. This automatically syncs with OneDrive. You can also configure OneDrive for the desktop to allow you to fetch files on your PC from other devices.

SHARING A DOCUMENT IN ONEDRIVE AND ONEDRIVE FOR BUSINESS

You can also share a document with others by sending it via email, posting it, or sending others a link to it. When sharing documents in OneDrive, you have the following options:

- Send email: This option should be used if you want to give individual users or groups permission to a file or folder. You can then remove permissions for a specific group or individual if necessary. When users receive the link via email and visit OneDrive, the file or folder will appear in their list of shared files. You do not have to know their Microsoft user account address. If they do not have one, they can create one for free after clicking on the link.
- **Post to:** This option allows you to share the link on Facebook, LinkedIn, or Twitter. Anyone who views the post on your network can forward the link. If you selected the option to allow recipients to edit the document, anyone the link is forwarded to can view and edit the file or folder.
- Get a link: This option should be used if you want to share the file with a larger number of recipients. For example, you could post the link on your blog or your website. You can also include this link in an email or via an instant message. When using this option, you can choose from the following types of links:
 - View only: Anyone who receives this link can see the files you share.
 - View and edit: Anyone with this link can see and edit the files you share.
 - **Public:** Anyone can search for and view your public files, even if you don't share a link if you decide to make it public.

SHARE A ONEDRIVE DOCUMENT VIA EMAIL

GET READY. To share the Word document you created in the previous exercise with others via email, perform the following steps.

- 1. From the main screen of OneDrive, click Files > Documents > Project Files.
- Right-click the Word document you saved in the previous exercise (Project Scope. docx) and choose Share.
- **3.** Type the email address of the person you want to share it with and, if necessary, type a message.
- **4.** If you want the recipient to be able to edit the document, click the **Recipients can** edit option.
- 5. Click Share to send the email message.
- 6. Click Close.

OneDrive for Business has a Share option (accessed by rightOclicking the document and clicking Share) that allows you to share the file with other users, to email everyone about the file, and to get a link. You can also click the Advanced option to see who access to the document and to manage the site permissions, folder, or document permissions.

ACCESSING ONEDRIVE FROM THE ONEDRIVE DESKTOP APP FOR WINDOWS

With the **OneDrive desktop app for Windows** installed on your local computer, you can automatically sync files and folders with the OneDrive cloud. You can then access your resources across multiple devices, such as computers and smartphones.

The OneDrive desktop app for Windows 7 or 8 can be downloaded directly from your OneDrive account and the OneDrive for Business can be downloaded for Windows 7, 8/8.1 and 10. The OneDrive app is already built into Windows 8.1 and Windows 10. There are also OneDrive applications for Android, Mac OSX, iOS, Windows Phone, and Xbox.

When you install the app, a folder will be created on your desktop automatically. Anything that you place into this folder is synched with OneDrive.com as well as with your other computers. You can access the folder from within File Explorer, drag new files into the folder, and choose the folders you want to sync on your computer.

As part of the setup of OneDrive, the Let me use OneDrive to fetch any of my files on this PC option is enabled, allowing you to use OneDrive to fetch files from this PC. This process works well a file is in a folder outside the OneDrive folder on your PC or is a file that you did not configure to synch with OneDrive when you initially set it up. When a PC has been configured to allow fetching, you see it in your OneDrive Dashboard, under PCs, when you log on to http://onedrive.live.com.

Ð F

FETCH A FILE USING ONEDRIVE

GET READY. To fetch a file using OneDrive, log in to a Windows 10 computer with access to the Internet and then perform the following steps.

- 1. Open Internet Explorer or Microsoft Edge, go to http://onedrive.live.com, and then click Sign In.
- 2. Type your Microsoft User Account and Password.
- **3.** In the left pane, click the remote PC from which you want to fetch files. Remote PCs will appear under the *PCs* section of the left pane.
- **4.** If this is the first time you have attempted to connect to the PC, you will be presented with a security page when you first attempt to connect to it. When the page appears, click **Sign in with a security code.**

This option automatically sends a seven-digit code to the device you configured when setting up your Microsoft account. This could be your cell phone number or an email address you provided.

- **5.** After you receive the code, type it into the field provided. The folders on your remote PC will appear in OneDrive.
- **6.** Navigate to any folder and select a file that you want to upload. Notice that you have access to your entire PC. This includes all partitions as well as the DVD drive and any externally attached drives on the computer.
- 7. Right-click the file and choose Upload to OneDrive.
- 8. When the selected item will be uploaded to: dialog box appears, double-click **Documents**, choose **ProjectFiles**, and then click **Upload**.
- **9.** From the main screen of OneDrive, click **Files > Documents > Project Files** and then confirm the file you uploaded appears in the folder.

Understanding OneNote

OneNote, included with Office 2016 and Office 365, is an application that allows multiple users access to a shared set of notes all at the same time. Everyone's changes are automatically synchronized to the notebook, so the notebook is current.

OneNote saves an offline copy on each user's computer so she can edit the notes even when she's not connected to the network. When she connects, OneNote automatically merges her changes with the Notebook along with everyone else's changes. When a user adds new sections, pages, and links in OneNote, the program displays the name of the user (author) who added them.

There are four views to choose from in OneNote:

- Editing View: Allows the notebook to be edited.
- Reading View: Removes extra information like author names and dates of changes.
- Show Authors: Displays the authors of sections, pages, and notebooks.
- Page Versions: Shows various versions of a page.

Understanding Outlook

Microsoft Outlook is a personal information manager that is used to manage emails, tasks, contacts, notes, and journal. Outlook can be a stand-alone application or part of the Microsoft Office suite.

Outlook can work with Exchange Server or any other mail server to send and retrieve emails, access shared mailboxes, and access calendars. While Outlook can be executed as a local application, Outlook can be accessed using your web browser to connect to Outlook Web App (OWA), also known as Outlook Web Access, as shown in Figure 2-4.





Today, an Outlook.com inbox comes with 15 GB of free online storage on OneDrive. If you are using Office 365 options, user mailboxes can store up to 50 GB (primary mailbox and personal archive).

Understanding Microsoft Office 365

Taking advantage of cloud computing services such as Microsoft Office 365 can reduce the workload on your IT staff. It can also improve the collaboration between your team members.

Microsoft Office 365 is a Microsoft subscription–based software service that enables users to access their documents and collaborate with others from anywhere using their computers, the web, or their smart devices. Microsoft Office takes the traditional Office suite and moves it to the cloud. The service includes Office, Exchange, SharePoint, Skype for Business, and Office Web Apps. By using Office 365, you can offload many of the administrative tasks normally handled by your IT department. These tasks include managing software updates, patches, and service packs as well as purchasing additional server hardware to support company growth.

Administration is handled through a Web portal/dashboard in which you can create/manage user accounts and oversee the health of all services. Microsoft also provides tools to migrate from your existing on-premise Exchange Server to Office 365.

The service can be used in combination with the desktop version of Microsoft Office and also works if you don't have Office installed on your computers.

Office 365 is available in a number of different plans designed to meet different segments of the market. Each plan uses a per-user/month charge and provides access to either the entire service or subsets of Office 365.

MORE INFORMATION

To compare plans, go to Microsoft's website and search for "Office 365 Plans."

UNDERSTANDING MICROSOFT OFFICE 365 FEATURES

Office 365 provides the software and tools you need to manage a fully collaborated workforce while providing a centralized Web portal to oversee and manage the services.

The following are features available with Microsoft Office 365:

- Access email, calendars, and contacts using the Microsoft Exchange service. They can be delivered to Outlook or Outlook Web App.
- Create, edit, and store documents you create with the Office Web Apps (browser-based versions of the standard Office suite of Word, PowerPoint, and Excel apps). These documents are fully compatible with the desktop version of the programs created in Office.
- Set up and maintain a company website.
- Connect immediately with co-workers via instant messaging using Skype for Business.
- Set up and conduct online meetings (audio, video, and web conferencing) with the ability to share desktops, files, and presentations online.
- Share documents inside and outside of your organization and collaborate with your colleagues using Microsoft SharePoint.

From an administrative perspective, Office 365 offers several benefits:

- **Maintenance:** Microsoft performs the administrative tasks, so you do not have to worry about backups, patches, and software updates.
- Software upgrades: Office 365 includes them with the subscription price.

- **Hardware:** Because Office 365 runs in the cloud, you don't have to purchase and maintain expensive server hardware. You can migrate Exchange Server over to Office 365 while at the same time increasing the mailbox storage for users.
- **Collaboration on projects:** Using SharePoint as a document repository and collaboration workspace, you can connect and work with a geographically dispersed workforce. By using team sites, you can share a portfolio of company projects, enable employees to access project information, share documents, and collaborate on project documents.

MANAGING OFFICE 365

If you have business or enterprise versions of Office 365, Office 365 is managed by a web console that enables you to set up and manage users and their software regardless of where they connect. The person who signs up your company for Office 365 is the Global Administrator by default. This person can then grant administrator permissions to other users in the organization as needed to distribute the workload.

Business and enterprise versions of Office 365 are managed by using the Office 365 Admin Center (see Figure 2-5). From here, you can create users and groups, manage software licenses, generate reports, and purchase services.

Office 365 provides several administrator roles that can be assigned to help distribute the workload of managing Office 365. The Global Administrator is assigned to the person who sets up Office 365 initially. This is the most powerful account in the organization. The other administrator roles can be assigned to users according to your organization's specific needs.

Five administrator roles are available for Office 365 enterprises:

- *Global Administrator*: Has access to all administrative features. This is the person who signs up for Office 365. Only Global Administrators can assign other administrative roles. Only one person in the company can serve in this role.
- *Billing Administrator*: Manages purchases, support tickets, and subscriptions and monitors the overall health of the services.





The Office 365 Admin Center

- *Password Administrator*: Manages requests for services, resets passwords, and monitors the overall health of the services. Users in this role can reset passwords only for users and other Password Administrators.
- Service Administrator: Manages service requests and monitors overall health of services.
- User Management Administrator: Manages user accounts and user groups, resets passwords, and manages service requests. User Management Administrators can also monitor the overall health of services. They cannot reset passwords for Billing, Global, or Service Administrators and they cannot delete a Global Administrator or create other administrators.

MORE INFORMATION

To learn more about Office 365, visit Microsoft's website and search for "Office 365."

INSTALLING AND MANAGING SOFTWARE BY USING MICROSOFT OFFICE 365

Microsoft Office 365 is a subscription-based service that offers various services and software that enable you to collaborate and store documents online. When implemented with Office 2016, users can work either online or offline and take advantage of the full features available with the desktop applications in the Office suite.

Office 365 offers several different plans designed for small, midsize, and enterprise-level businesses. The Office 365 Small Business Premium (25 users), Office 365 Midsize Business (300 users), and Office 365 Enterprise E3 (unlimited users) plans include a subscription for Office 2016 for up to five PCs/Macs. *Microsoft Office 2016* includes desktop versions of the following applications:

- Access 2016
- OneNote 2016
- Excel 2016
- Word 2016
- Outlook 2016
- PowerPoint 2016
- Publisher 2016
- OneDrive for Business
- Skype of Business

Business and Enterprise versions of Office 365 manages the licenses for Office 2016 through an online portal by indicating which Office 365 users have the ability to install the program during the setup of the user's account. In the Office 365 portal, you can delete users to make licenses available, remove licenses from users when their job changes, or assign licenses for users after accounts are set up. You can also review which licenses are assigned to a user and purchase more if necessary.

MORE INFORMATION

To learn more about what is included and pricing for Office 365, visit Microsoft's website and search for "Office 365 plans."

There are several options available for deploying Office 2016. The option you choose depends on the infrastructure you already have in place and the level of IT support available in your organization. The options you can choose are:

• **Deploying directly from the Office 365 portal:** This option is designed for organizations that do not have IT resources; it has a self-service approach. When this option is used, you can download and install only the 32-bit version of Office 2016.

- **Deploying from a network share:** This option requires basic IT administration skills and works well in situations where you have a slow network connection. When this option is used, you have the option to deploy both 32-bit and 64-bit versions of Office 2016.
- **Deploying using Group Policy or System Center Configuration Manager:** These two methods are designed to leverage Active Directory and should be used when deploying to large groups of users.

Following is a brief overview of the steps involved to deploy Office 2016 directly from the Office 365 portal. In the exercise that follows, you will learn the following steps in more detail:

- 1. The administrator signs up for Office 365, sets a new domain name, creates user accounts, and assigns licenses to each user.
- 2. The administrator sends users their temporary passwords by email.
- 3. Users sign into the Office 365 portal and set up new passwords.
- 4. Users download and configure their desktops with Office 2016 (32-bit version).

Using Azure Storage

Azure Storage is cloud storage designed for large-scale applications including providing a storage foundation for Azure virtual machines. The cost for Azure Storage is based on the amount of data stored and the number of requests made. To allow Azure Storage to adapt to its usage, Azure Storage users auto-partitioning that automatically load balances the data based on traffic. Therefore, as the demands on your application grow, Azure Storage will automatically allocate the appropriate resources to meet those demands.

Since Azure Storage is on the cloud, it can be accessed from anywhere in the world, and from any type of application via HTTP/HTTPS. It can also be accessed on a server, desktop computer, or a mobile device such as a tablet or laptop. Azure Storage can also store a subset of data on a mobile device that is synchronized with the full set of data stored in the cloud. Lastly, Azure Storage can be accessed from Windows and Linux machines and a variety of programming languages (including .NET, Java, and C++).

To access the Azure Storage, you must have an Azure storage account. The storage account will provide the unique namespace for:

- A standard storage account includes Blob, Table, Queue, and File storage.
- A premium storage account currently supports Azure Virtual Machine disks only. Azure Premium Storage is available by request via the Azure Preview page.

To create a storage account, you must have an Azure subscription. You can then create up to 100 uniquely named storage accounts with a single subscription.

A standard storage account gives you access to Blob storage, Table storage, Queue storage, and File storage:

- **Blob storage:** Stores file data known as blobs. A blob can be any type of text or binary data, such as a document, media file, or application installer.
- **Table storage:** Stores structured datasets, which is a NoSQL key-attribute data store that allows for rapid development and fast access to large quantities of data.
- **Queue storage:** Provides reliable messaging for workflow processing and for communication between components of cloud services.
- File storage: Offers shared storage for legacy applications using the standard SMB 2.1 protocol.

Each standard storage account can contain up to 500 TB of combined blob, queue, table, and file data.

Azure Storage is deployed in 15 regions around the world and supports for replicating data between regions. To ensure high availability, you have the following options:

- *Locally redundant storage (LRS)* maintains three copies of your data within a single facility in a single region. LRS protects your data from normal hardware failures, but not from the failure of a single facility.
- For maximum durability, you need to use *zone-redundant storage (ZRS)*, which replicates data three times across two to three facilities. ZRS ensures that your data is durable within a single region.

Understanding Local Storage

THE BOTTOM LINE

Storage Spaces is a feature in Windows 10/Windows Server 2016 that allows you to combine multiple disks into a single logical volume that can be mirrored to protect against one or more drive failures.

CERTIFICATION READY Describe local storage 2.2 The Storage Spaces feature in Windows 10 allows you to combine several physical drives, which the operating system will see as one large drive. The drives can be of any capacity and can consist of a variety of different drive interfaces—Small Computer System Interface (SCSI), Universal Serial Bus (USB), and Serial ATA (SATA).

When the drives are combined, Windows places them into a *storage pool*. These storage pools can then be segmented into multiple storage spaces, which are then formatted with a file system and can be used just like any other regular disk on your computer. New disks (internal/ external) can be added to the storage pool as space requirements increase over time.

Although data can be stored on the drives, you cannot use storage spaces to host the Windows operating system files.

Storage spaces offer two key benefits:

- By spreading data across multiple disks you achieve data resiliency (fault tolerance), which can protect your data against hard disk failure.
- Volume sizes can be larger than the actual physical size of your drives in the storage pool (capacity). This is accomplished through a process called thin provisioning.

Creating Storage Pools

Creating a storage pool allows you to combine multiple smaller drives that you might not otherwise be able to use by themselves into a larger single logical volume.

To create a storage pool on a Windows 10 client, you access the Manage Storage Spaces tool found in the Control Panel. The Wizard prompts you to select the disks that you want to use and then add them to the storage pool. For example, if you have two physical disks with capacities of 200 GB and 300 GB, it creates a pool that has a total capacity of 500 GB (see Figure 2-6).




Creating Storage Spaces

After selecting the drives to include in your storage pool, you will be prompted to create the storage space. This involves entering a name, selecting a drive letter, identifying the type of resiliency you want to configure, and setting the maximum size you want to assign to the storage space.

When creating storage spaces, there are four resiliency types to select from. Only three of them provide real fault-tolerance.

- *Simple (no resiliency)*: Writes one copy of your data but doesn't protect against drive failures; requires at least one drive.
- *Two-way mirror* Writes two copies of your data to protect against a single drive failure; requires at least two drives.
- *Three-way mirror* Writes three copies of your data to protect against two simultaneous drive failures; requires at least five drives.
- *Parity* Writes data with parity information to protect against single drive failures; requires at least three drives.

You also need to decide how much of the total storage pool capacity you want to use for your new storage space. In Figure 2-6, you saw the total pool capacity is 500 GB. By using a process called *thin provisioning* (see Figure 2-7), you can create a storage space that is larger than the available capacity of the storage pool. After setting the size, the Wizard will create the storage space based on the parameters you provided.

Thin provisioning reserves the space for future use. For example, in Figure 2-7, you can see there are two physical drives being added to the storage pool to create a total capacity of 500 GB. Even though you have a total capacity of only 500 GB, you can configure the storage space that uses this pool to be 1 TB or greater capacity. When the storage pool approaches capacity, you will receive a warning and need to add more disks to the pool. This approach works well in situations in which you expect your data storage needs will grow, but you don't want to purchase additional disks immediately.

After the storage space is created, it will appear as a drive in File Explorer. The drive can be protected using BitLocker and NTFS permissions, just like any other drive in Windows 10.

Figure 2-7

An example of thin provisioning



CREATE A STORAGE POOL AND A STORAGE SPACE IN WINDOWS 10

GET READY. To create a storage pool and storage space in Windows 10, perform the following steps.

- 1. Log on with administrative credentials.
- 2. Connect the drives you want to use to your computer.
- 3. Open the Control Panel, click System and Security, and click Storage Spaces.
- 4. Click Create a new pool and storage space.
- **5.** Select the drive(s) you want to include in the new storage pool. (Warning: Any data on these drives will be deleted.)
- 6. Click Create pool.
- **7.** Once the pool is created, you will be taken automatically to the Create a storage space screen.
- 8. In the Name field, type a name for your storage space.
- **9.** In the Drive letter field, click the down arrow and then choose a driver letter for the storage space.
- In the File system field, select NTFS or REFS. NTFS is the default file system. In the Resiliency type field, click the down arrow and then choose the resiliency type, as shown in Figure 2-8.
- **11.** In the Size (maximum) field, type the maximum size that you want for your storage space.
- **12.** Click Create storage space.
- **13.** Open **File Explorer** and confirm that the new storage space appears under the drive letter you assigned in Step 8.

After completing the setup of your storage space, you can continue to monitor and manage it from the Manage Storage Space tool. You can perform the following tasks:

- View your storage pool(s)
- View the storage spaces in the pools
- View the physical drives included in the pool(s)
- · Identify how much pool capacity is currently being used
- Add more drives to the pool
- Rename the pool

Figure 2-8	E Create a storage space – 🗆 🗙
Creating a storage space	(→ → ≦ « Storage Spaces → Create a storage space v) Search Control Pa
	Enter a name, resiliency type, and size for the storage space
	Name and drive letter
	Name: Storage space
	Drive letter: I: 🗸
	Resiliency
	Resiliency type: Two-way mirror V
	A two-way mirror storage span drive failure. A two-way mirror Parity Parity Parity
	Size
	Total pool capacity: 1.20 TB
	Available pool capacity: 1.20 TB
	Size (maximum): 614 GB 🗸
	Including resiliency: 1.19 TB
	A storage space can be larger than the amount of available capacity in the storage pool. When you run low on capacity in the pool, you can add more drives.
	Create storage space Cancel

- Change the size of storage spaces
- View files stored in storage spaces
- Delete storage spaces
- Describe storage spaces and storage pools

Understanding File Systems

THE BOTTOM LINE

CERTIFICATION READY Describe file systems 2.3 A *file system* is a method of storing and organizing computer files and the data they contain to make it easy to find and access this information. A file system also maintains the physical location of the files so that you can find and access the files in the future. Windows 10 supports FAT16, FAT32, NTFS and Resilient File System (ReFS) file systems on hard drives.

The primary file system used by Windows 10 is *NTFS*. NTFS supports larger disks than FAT32 or FAT (up to 256 terabytes [TB]) and NTFS-formatted files and folders provide better security. It's also more reliable, with built-in features for recovering from disk errors automatically. Microsoft recommends NTFS for its security features: You can use encryption and permissions to restrict file access to specific users.

FAT32 and *FAT* (which is seldom used today) are file systems that were popular in earlier versions of Windows (such as Windows 95, Windows 98, Windows Millennium Edition, Windows NT, and Windows 2000). FAT is an abbreviation for File Allocation Table. The limitations of FAT32 make it less desirable than NTFS:

- A FAT32 partition is limited to a maximum size of 32 gigabytes (GB).
- The maximum size of a file that can be stored on a FAT32 volume is 4 GB.

So why use FAT32? Many universal serial bus (USB) flash drives come formatted as FAT32 to be compatible with a large variety of operating systems. If you plan to configure your computer for *multi-booting*, where you choose at startup which operating system you want to load, you might need to format a partition with FAT32 if you need to support an older operating system

Table 2-1

Comparing FAT, FAT32, and NTFS

FILE SYSTEM	MAXIMUM PARTITION SIZE	Maximum File Size
FAT	2 GB	2 GB
FAT32	32 GB	4 GB
NTFS	256 TB	Limited by size of volume on which it resides

Table 2-1 compares attributes of FAT, FAT32, and NTFS.

You can usually convert a FAT or FAT32 partition to NTFS with few to no problems. One hitch you might run into is if the disk is nearly full. The conversion process (Convert.exe) needs a certain amount of free disk space to work properly. If there is insufficient free disk space, Convert.exe will notify you.

TAKE NOTE*

Converting to NTFS is a one-way process. After you convert a drive to NTFS, you cannot convert it back to FAT or FAT32. You can reformat an NTFS drive to FAT32, but you would need to back up all of your data first and then copy it back.

You can also convert to FAT32 from a different type of file system, although you need to keep the FAT32 size limitations in mind. If the partition you want to format is larger than 32 GB, the conversion process won't be successful.

Before converting a disk from one file system to another, back up your data, if possible. If you have a relatively small number of files on a disk, and no system files or programs installed, it's better to back up the data to a different storage medium and then format the disk.

A new file system that was introduced with Windows Server 2012 is the *Resilient File System* (*ReFS*). It is designed to increase data availability, despite errors that would normally cause data loss or downtime while providing increased scalability and performance.

The features of ReFS include:

- **Integrity:** Stores data so that it is protected from many of the common errors that can cause data loss. If corruption occurs, ReFS can detect and, when configured with Storage Spaces, automatically correct the corruption.
- Availability: If corruption cannot be repaired, the online salvage process is localized to the area of corruption, requiring no volume downtime.
- **Scalability:** Designed for the data set sizes of today and the data set sizes of tomorrow; it's optimized for high scalability.
- **App Compatibility:** To maximize compatibility, ReFS supports a subset of NTFS features plus Win32 APIs that are widely adopted.
- **Proactive Error Identification:** Includes a data integrity scanner that periodically scans the volume, attempts to identify latent corruption, and then proactively triggers a repair of that corrupt data.

While Disk Management does not allow you to create a volume with ReFS, you can create a volume with REFS when you create a storage space.

The main disk management tool in Windows 10 is the MMC snap-in called Disk Management, which is also part of the Computer and Management consoles. In addition, you can use a diskpart.exe and the Format command to partition and format a drive, as well as Windows Explorer to format a drive.

Disk Management is a system utility for managing hard disks and the volumes or partitions they contain. With Disk Management, you can initialize disks, create volumes, and format volumes with the FAT16, FAT32, or NTFS file systems. See Figure 2-9.

Figure 2-9	4			Com	puter Management		- 🗇 🗡
The Disk Management snap-in	File Action View Help	1					
	Computer Management (Local Computer Management Computer M	Volume (C:) System Reserved	Layout Type Fil Simple Basic N Simple Basic N	e System TFS TFS	Status Healthy (Boot, Page File, Crash Dump, Primary Partition) Healthy (System, Active, Primary Partition)	Capacity 29.66 GB 350 MB	Actions Disk Management A More Actions
	 Bick Management Services and Applications 	< Disk 0 Basic 30.00 GB Online	System Reserved 350 MB NTFS Healthy (System, Ac	tive, Pri	(C:) 29.66 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Part	>	
		Disk 1 Basic 9.88 GB Online	9.88 GB Unallocated				
	< >>	Basic 4.88 GB Online Unallocated F	4.88 GB Unallocated Primary partition			~	

Whenever you add a new disk (either a local hard drive or a virtual drive, such as from a SAN) to a Windows 10 system, you need to open Disk Management and initialize the disk.

INITIALIZE A NEW DISK

GET READY. To initialize new disks in Windows 10, perform the following steps.

- 1. Right-click the disk you want to initialize and choose Initialize Disk.
- 2. In the Initialize Disk dialog box, select the disk(s) to initialize. You can select whether to use the Master Boot Record (MBR) or GUID Partition Table (GPT) partition style.
- 3. Click OK.

If the disk that you want to initialize does not appear, you may need to right-click Disk Management and choose Refresh or Rescan Disks. If the disk still does not appear, you need to make sure that it is connected properly and running.

CREATE OR DELETE A PARTITION OR LOGICAL DRIVE

GET READY. To create or delete a partition or logical drive in Windows 10, perform the following steps.

- 1. Open the Disk Management console.
- 2. Perform one of the following options:

Right-click an unallocated region of a basic disk and choose New Partition.

Right-click an area of free space within an extended partition and choose New Logical Drive.

Right-click a partition or logical drive and choose Delete Partition to remove that partition or logical drive. Click **Yes** to confirm the deletion.

- 3. When you choose to create a new partition or logical drive, the New Partition Wizard appears. Click Next to continue.
- 4. Specify the size of the volume and click the Next button.

- Assign a drive letter or mount the volume to an empty NTFS folder and click the Next button.
- 6. Specify the file system (such as NTFS or FAT32), allocation unit size, and volume label. You can also perform a quick format and enable file and folder compression if desired. Click Next. See Figure 2-10.
- 7. When the wizard is complete, click Finish.

Figure 2-10	New Simple Volume Wizard	×
Formatting the volume	Format Partition To store data on this partition, you must format it first.	
	Choose whether you want to format this volume, and if so, what settings you	want to use.
	O Do not format this volume	
	Format this volume with the following settings:	
	File system: NTFS V	
	Allocation unit size: Default 🗸	
	Volume label: New Volume	
	✓ Perform a quick format	
	Enable file and folder compression	
	A Back Next >	Cancel

For basic disks, you must first create an extended partition before you can create a new logical drive, if no extended partition exists already.

If you choose to delete a partition, all data on the deleted partition or logical drive will be lost unless you previously backed it up. In addition, you cannot delete the system partition, boot partition, or any partition that contains an active paging file. Windows 10 requires that you delete all logical drives and any other partitions that have not been assigned a drive letter within an extended partition before you delete the extended partition itself.

Understanding File and Print Sharing

THE BOTTOM LINE

As you learned in the previous section, NTFS is the preferred file system in part because it supports much larger hard disks and a higher level of reliability than FAT or FAT32. In addition, NTFS offers better security through permissions and encryption.

CERTIFICATION READY Describe file and print sharing 2.4

TAKE NOTE*

NTFS permissions are managed using File Explorer (explorer.exe). A *permission* is defined as the type of access that is granted to an object, such as NTFS files and folders. When files and folders are created on an NTFS volume, a security descriptor known as an *Access Control List (ACL)* is created. This descriptor includes information that controls which users and groups can access the file or folder, as well as what type of access is granted to particular users and groups. Each assignment of permissions to a user or group is represented as an *access control entry (ACE)*.

Setting NTFS Permissions

NTFS permissions allow you to control which users and groups can gain access to files and folders on an NTFS volume. The advantage of NTFS permissions is that they affect local users as well as network users.

Usually, when assigning NTFS permissions, you would assign the following standard permissions:

• **Full control:** This provides permission to read, write, modify, and execute files in a folder; change attributes and permissions; and take ownership of a folder or the files within it.

- **Modify:** This provides permission to read, write, modify, and execute files in a folder, as well as change attributes of the folder or the files within it.
- **Read & execute:** This provides permission to display a folder's contents; display the data, attributes, owner, and permissions for files within the folder; and run files within the folder.
- List folder contents: This provides permission to display a folder's contents; display the data, attributes, owner, and permissions for files within the folder; and run files within the folder.
- Read: This provides permission to display a file's data, attributes, owner, and permissions.
- Write: This provides permission to write to a file, append to the file, and read or change the file's attributes.

TAKE NOTE*While List Folder Contents and Read & Execute appear to have the same special
permissions, these permissions are inherited differently. List folder Contents is inherited by
folders but not files while Read & Execute is inherited by both files and folders.

To manage NTFS permissions, right-click a drive, folder, or file, choose Properties, and then click the Security tab. You should see the group and users who have been given NTFS permissions and their respective standard NTFS permissions. To change the permissions, click the Edit button to open the Permissions dialog box, as shown in Figure 2-11. You can then click the Add button to add additional users or groups or click the Remove button to remove a user or group.

Each of the standard permissions consists of a logical group of special permissions. The available special permissions are as follows:

- **Traverse folder/Execute file:** This permission allows or denies moving through folders to reach other files or folders, even if the user has no permissions for the traversed folders. By default, the Everyone group is granted the Bypass traverse checking user right. (This applies to folders only.) Execute file allows or denies running program files. (This applies to files only.) Setting the Traverse folder permission on a folder does not automatically set the Execute file permission on all files within that folder.
- List folder/Read data: This permission allows or denies viewing filenames and subfolder names within a folder. List folder affects the contents of that folder only and does not affect whether the folder you are setting the permission on will be listed. (This applies to folders only.) Read data allows or denies viewing data in files. (This applies to files only.)
- **Read attributes:** This permission allows or denies viewing the attributes of a file or folder, such as read-only and hidden.
- **Read extended attributes:** This permission allows or denies viewing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.

	ri\Desktop\TestFolder\	\Test.txt.txt
Group or user names:		
SASYSTEM	100450.01 + 1	
SP Administration (MINI10A)	Administratem)	
		D
	Add	Remove
Permissions for SYSTEM	Add	Remove Deny
Permissions for SYSTEM	Add Allow	Remove Deny
Permissions for SYSTEM Full control Modify	Add Allow	Remove Deny
Permissions for SYSTEM Full control Modify Read & execute	Add Allow	Remove Deny
Permissions for SYSTEM Full control Modify Read & execute Read	Add Allow	Remove
Pemissions for SYSTEM Full control Modify Read & execute Read Write	Add Allow V V	Remove Deny

Figure 2-11 NTFS permissions

- **Create files/Write data:** The Create files permission allows or denies creating files within a folder. (This applies to folders only.) The Write data permission allows or denies making changes to a file and overwriting existing content. (This applies to files only.)
- **Create folders/Append data:** The Create folders permission allows or denies creating folders within a folder. (This applies to folders only.) The Append data permission allows or denies making changes to the end of a file but not changing, deleting, or overwriting existing data. (This applies to files only.)
- Write attributes: This permission allows or denies changing the attributes of a file or folder, such as read-only or hidden. The Write attributes permission does not imply creating or deleting files or folders; it only includes the permission to make changes to the attributes of a file or folder. To allow (or deny) create or delete operations, see Create files/Write data, Create folders/Append data, Delete subfolders and files, and Delete.
- Write extended attributes: This permission allows or denies changing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program. The Write extended attributes permission does not imply creating or deleting files or folders; it only includes the permission to make changes to the attributes of a file or folder. To allow (or deny) create or delete operations, see Create folders/Append data, Delete subfolders and files, and Delete.
- **Delete subfolders and files:** This permission allows or denies deleting subfolders and files, even if the Delete permission has not been granted on the subfolder or file.
- **Delete:** This permission allows or denies deleting the file or folder. If you do not have Delete permission on a file or folder, you can still delete it if you have been granted Delete subfolders and files permission on the parent folder.
- **Read permissions:** This permission allows or denies reading the permissions of a file or folder, such as full control, read, and write.
- **Change permissions:** This permission allows or denies changing the permissions of a file or folder, such as full control, read, and write.
- **Take ownership:** This permission allows or denies taking ownership of a file or folder. The owner of a file or folder can always change permissions on it, regardless of any existing permissions on the file or folder.
- **Synchronize:** This permission allows or denies different threads to wait on the handle for a file or folder and synchronize with another thread that may signal it. This permission applies only to multithreaded, multiprocess programs.

Table 2-2 shows the special permissions assigned to each standard NTFS permission. If for some reason you need more granular control, you can assign special permissions. To assign special permissions, right-click a drive, folder, or file, choose Properties, and then click the Security tab. Then click the Advanced button to open the Advanced Security Settings, click the Change Permissions button, and click the Add, Edit, or Remove button.

Groups or users that are granted full control permission on a folder can delete any files in that folder regardless of the permissions protecting the file. In addition, the List folder contents permission is inherited by folders but not files, and it should only appear when you view folder permissions. In Windows 10, the Everyone group does not include the Anonymous Logon group by default, so permissions applied to the Everyone group do not affect the Anonymous Logon group.

To simplify administration, you can grant permissions using groups. By assigning NTFS permissions to a group, you are granting permissions to one or more users simultaneously, reducing the number of entries in each access list, as well as the amount of effort required to grant multiple users access to certain files or folders.

Table 2-2

NTFS permissions

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse folder/ Execute file	Х	Х	Х	Х		
List folder/ Read data	Х	Х	х	х	х	
Read attributes	х	Х	х	Х	х	
Read extended attributes	Х	Х	Х	Х	х	
Create files/ Write data	Х	Х				Х
Create folders/ Append data	Х	Х				х
Write attributes	х	Х				х
Write extended attributes	Х	Х				х
Delete subfolders and files	Х					
Delete	х	х				
Read permissions	Х	Х	х	х	х	х
Change permissions	Х					
Take ownership	х					
Synchronize	Х	Х	х	Х	х	х

Creating Effective NTFS Permissions

The folder/file structure on an NTFS drive can be complicated, with many folders and nested folders. In addition, because you can assign permissions to groups and at different levels on an NTFS volume, figuring out the effective permissions of a particular folder or file for a particular user can be tricky.

There are two types of permissions used in NTFS:

- Explicit permissions: These permissions are granted directly to a file or folder.
- *Inherited permissions*: These permissions are granted to a folder (parent object or container) that flows into a child objects (subfolders or files inside the parent folder).

By default, any objects within a folder inherit the permissions from that folder when they are created (see Table 2-3). However, explicit permissions take precedence over inherited permissions (see Table 2-4). So, if you grant different permissions at a lower level, the lower-level permissions take precedence.

Овјест	NTFS Permissions
Data	Allow full control (explicit)
Folder1	Allow full control (inherited)
Folder2	Allow full control (inherited)
File1	Allow full control (inherited)

Table 2-4

Table 2-3

Inherited permissions

Explicit permissions overwrite inherited permissions

Овјест	NTFS Permissions
Data	Allow full control (explicit)
Folder1	Allow read (explicit)
Folder2	Allow read (inherited)
File1	Allow read (inherited)

For example, let's say you have a folder called Data. Within the Data folder, you have Folder1, and within Folder1, you have Folder2. If you grant Allow full control to a user account, the Allow full control permission will flow to the subfolders and files within the Data folder.

In comparison, if you grant Allow full control on the Data folder to a user account and you grant Allow read permission to Folder1, the Allow read permission will overwrite the inherited permissions and will then flow to Folder2 and File1.

If a user has access to a file, he or she will still be able to gain access to the file even if he or she does not have access to the folder containing the file. Of course, because the user doesn't have access to the folder, the user cannot navigate or browse through the folder to get to the file. Therefore, the user will have to use the universal naming convention (UNC) or local path to open the file.

When you view permissions, they will be one of the following:

- Checked: Here, permissions are explicitly assigned.
- Cleared (unchecked): Here, no permissions are assigned.
- Shaded: Here, permissions are granted through inheritance from a parent folder.

Besides granting the Allow permissions, you can also grant the Deny permission. The Deny permission always overrides other permissions that have been granted, including when a user or group has been given Full control. For example, if a group has been granted Read and Write permission yet one person within the group has been denied the Write permission, that user's effective permissions would be the Read permission.

When you combine applying Deny versus Allowed with explicit versus inherited permissions, the hierarchy of precedence of permission is as follows:

- 1. Explicit Deny
- 2. Explicit Allow
- 3. Inherited Deny
- 4. Inherited Allow

Because users can be members of several groups, it is possible for them to have several sets of explicit permissions for a particular folder or file. When this occurs, the permissions are combined to form the *effective permissions*, which are the actual permissions when logging in and accessing a file or folder. These consist of explicit permissions plus any inherited permissions.

When you calculate effective permissions, you must first calculate the explicit and inherited permissions for an individual or group and then combine them. When combining user and group permissions for NTFS security, the effective permission is the cumulative permission. The only exception is that Deny permissions always apply.

For example, say you have a folder called Data. Within the Data folder, you have Folder1, and within Folder1, you have Folder2. If User 1 is a member of Group 1 and Group 2 and you assign the Allow write permission to the Data folder to User 1, the Allow read permission to Folder1 to Group 1, and the Allow modify permission to Folder2 to Group 2, then User 1's effective permissions would be as shown in Table 2-5.

Овјест	User 1 NTFS Permissions	GROUP 1 PERMISSIONS	GROUP 2 PERMISSIONS	Effective Permissions
Data	Allow write (explicit)			Allow write
Folder1	Allow write (inherited)	Allow read (explicit)		Allow read and write
Folder2	Allow write (inherited)	Allow read (inherited)	Allow modify* (explicit)	Allow modify*
File1	Allow write (inherited)	Allow read (inherited)	Allow modify [*] (inherited)	Allow modify*

*The Modify permission includes the Read and Write permissions.

As another example, let's say you have a folder called Data. Within the Data folder, you have Folder1, and within Folder1, you have Folder2. If User 1 is a member of Group 1 and Group 2 and you assign the Allow write permission to the Data folder to User 1, the Allow read permission to Folder1 to Group 1, and the Deny modify permission to Folder2 to Group 2, User 1's effective permissions would be as shown in Table 2-6.

Sharing Drives and Folders

Most users are not going to log onto a server directly to access their data files. Instead, a drive or folder will be shared (known as a *shared folder*), and they will access the data files over a network. To help protect against unauthorized drive or folder access, you should use share permissions along with NTFS permissions (assuming the shared folder is on an NTFS volume). When a user needs to access a network share, she will use the UNC, which is \\servername\sharename.

Table 2-5

Calculating effective permissions

68 | Lesson 2

Table 2-6

Figure 2-12 Sharing a folder

Effective permissions affected by Deny permissions

Овјест	User 1 NTFS Permissions	GROUP 1 PERMISSIONS	GROUP 2 Permissions	Effective Permissions
Data	Allow write (explicit)			Allow write
Folder1	Allow write (inherited)	Allow read (explicit)		Allow read and write
Folder2	Allow write (inherited)	Allow read (inherited)	Deny modify (explicit)	Deny modify
File1	Allow write (inherited)	Allow read (inherited)	Deny modify (inherited)	Deny modify

Traditional Windows file sharing allows you to restrict access to shared specific files and folders, and choose which users have access. *Basic sharing* allows you to share a file or folder with a specific user and restrict the user to Read or Read/Write actions.

The easiest way to share a folder in Windows 10 is to create a basic share by right-clicking a folder and choosing Share with. If you want to share a folder on a workgroup or domain, you then click Specific People. When the File Sharing dialog box opens, as shown in Figure 2-12, you type the name of the user, click Add, and then specify the permission level (Read or Read/Write).

Choose people to share with	
Type a name and then click Add, or click the arrow to	find someone.
	LLA I
	✓ Add
Name	Permission Level
Administrator	Read/Write 💌
🔏 Guest	Read 💌
Patrick Regan (patrick_regan123456@hotmail.co	m) Owner

Advanced sharing offers the greatest amount of control by allowing you to do the following:

- Share files, folders, or an entire drive
- · Choose users or groups with which to share files and folders
- Limit the number of users who may use a file or folder at the same time, mainly for security purposes
- Set permissions on shared files and folders, such as allowing users Read, Change, or Full Control

For more control on the share permissions, you can right-click the folder, choose Properties, and then click the Sharing tab.

SHARE A FOLDER

GET READY. To share a drive or folder in Windows 10, perform the following steps.

- 1. In Windows 10, right-click the drive or folder, choose **Properties**, click the **Sharing** tab, and then click the **Advanced Sharing** button.
- 2. When the Advanced Sharing dialog box opens, select the Share this folder option
- 3. Type the name of the shared folder.
- **4.** If necessary, specify the maximum number of users who can access the shared folder at the same time.
- 5. Click the Permissions button.
- 6. When the Permissions dialog box opens, by default, Everyone is given the Allow read shared permission. You can then remove Everyone, expand the Read shared permission, or add additional users.
- **7.** After users and groups have been added with the proper permissions, (as shown in Figure 2-13), click **OK** to close the Permissions dialog box.

Everyone		
	Add	Remove
Permissions for Everyone	Allow	Deny
Full Control Change Read		

8. Click **OK** to close the Properties dialog box.

The *share permissions* that are available are as follows:

- **Full control:** Users who are allowed this permission have Read and Change permissions, as well as additional capabilities to change file and folder permissions and take ownership of files and folders.
- **Change:** Users who are allowed this permission have Read permission and the additional capability to create files and subfolders, modify files, change attributes on files and subfolders, and delete files and subfolders.
- **Read:** Users who are allowed this permission can view file and subfolder names, access the subfolders of the share, read file data and attributes, and run program files.

As with NTFS, you can allow or deny each share permission. To simplify managing share and NTFS permissions, Microsoft recommends giving Everyone Full control at the share level, then controlling access using NTFS permissions. In addition, because a user can be member of several groups, it is possible for a particular user to have several sets of permissions to a shared drive or folder. The effective share permissions are a combination of the user's permissions and the permissions of all groups of which the user is a member.

Figure 2-13

Adding users and groups and configuring permissions

When a user logs onto the server and accesses files and folders without using the UNC, only the NTFS permissions apply, not the share permissions. When a person accesses a shared folder using the UNC, you must combine the NTFS and share permissions to see what a user can do. To figure overall access, first calculate the effective NTFS permissions. Then determine the effective shared permissions. Finally, apply the more-restrictive permissions between the NTFS and shared permissions.

USING PUBLIC FOLDERS

If you need to share files with other users who have accounts on your computer or with users on a network, Public folders is a convenient drag-and-drop method.

Perhaps the easiest way to quickly share files and folders with other users on a network is by copying or moving them into one of the Windows 10 Public folders. Each default library in Windows 10 has *public folders* (see Figure 2-14), such as Public Documents, Public Music, and so on, which can be found in C:\Users\Public. You just drag and drop items you want to share into the appropriate Public folder. Other users on your computer or on your network can use Windows Explorer to navigate to the files, and then open the files just as if the files were on their own computers.

One consideration is that if you simply copy a file to a Public folder to share with someone, you have two instances of that file on your computer. If you want to change the file, you must change it in one place and copy it to the other to keep both versions current. For example, you're working on a spreadsheet named Projects.xlsx in your My Documents folder. You copy it to the Public Documents folder so a co-worker can also view it. When you update Projects.xlsx in My Documents, you also need to save it again or copy the new version to Public Documents. For this reason, if you want to share the most current version of a file at all times using Public folders, you should move the file to the Public folder rather than try to maintain two versions.

Public folders are all about convenience, but they don't offer a lot of control. For example, you can't limit which files or folders are shared in a Public folder—everything is shared. Plus, anyone with network access can read and write files in the Public folders.

Public folder sharing in Windows 10 is turned off by default (except on a HomeGroup). When Public folder sharing is turned on, anyone on your computer or network can access



Figure 2-14

Libraries expanded to show Public folders these folders. When Public folder sharing is turned off, only users with a user account and password on your computer have access. In addition, Windows offers a password-protected sharing feature that you can use to limit Public folder access to users with a user account and password on your computer.

_	
- 62	
- 16-	- AU

TURN PUBLIC FOLDER SHARING ON OR OFF

GET READY. To turn Public folder sharing on or off in Windows 10, perform the following steps.

- 1. Click any Public folder using File Explorer, click the **Share with** menu on the Toolbar, and then click **Advanced sharing settings**.
- 2. Click the Home or Work down arrow to access the profile settings.
- **3.** Under All Networks, in the Public folder sharing section (as shown in Figure 2-15), select an option to turn sharing on or off.

Figure 2-15	• Advanced sharing settings —	×
Configuring sharing options	← → ▼ ↑ • 4 « Network and Shari > Advanced sharing settings V ⊘ Search Control Panel	٩
	All Networks	^
	Public folder sharing	
	When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.	
	① Turn on sharing so anyone with network access can read and write files in the Public folders 〇 Turn off Public folder sharing (people logged on to this computer can still access these folders)	
	Media streaming	
	When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.	
	Choose media streaming options	
	File sharing connections	~
	Save changes Cancel	

4. Click **Save changes** at the bottom of the Advanced sharing settings window. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

TURN PASSWORD-PROTECTED SHARING ON OR OFF

GET READY. To turn password-protected sharing on or off in Windows 10, perform the following steps.

- Using File Explorer, click any Public folder, click the Share with menu on the Toolbar, and then click Advanced sharing settings.
- 2. Click the Home or Work down arrow to access the profile settings.
- **3.** Under All Networks, in the **Password protected sharing** section, select an option to turn password-protected sharing on or off.
- **4.** At the bottom of the Advanced sharing settings window, click **Save changes**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

Remember, by turning on password-protected sharing in Control Panel, you can limit Public folder access to users with a user account and password on your computer.

Using HomeGroup

When you are running Windows 10 within a domain, Windows servers and clients have several tools and mechanisms to share files and printers. Today, many households have multiple computers. A *HomeGroup* is a group of computers on a home network that can share files and printers. To protect your HomeGroup, you can use a password. Similar to share permissions, other users cannot change the files that you share unless you give them permission to do so. When compared to any folder sharing, HomeGroups are relatively limited, because you can share only the contents of the libraries in the user's profile.

HomeGroup is available with Windows 7, Windows 8 (including Windows 8.1 and Windows RT 8.0/8.1) and Windows 10. You can join a HomeGroup on a PC running Windows RT 8.1, but you can't create a HomeGroup or share content with the HomeGroup. In Windows 7 Starter and Windows 7 Home Basic, you can join a HomeGroup, but you can't create one. If the system does not detect a HomeGroup, the Network and Sharing Center control panel contains a link providing access to the Create a HomeGroup Wizard.

\mathbf{E}

CREATE A HOMEGROUP

GET READY. Log in to Windows 10 using an account with Administrator privileges. Make sure that the system is configured to use the Private network location. To create a HomeGroup, perform the following steps.

- Open Control Panel and then click Network and Internet > Network and Sharing Center. The Network and Sharing Center control panel appears.
- 2. Click the HomeGroup link. The HomeGroup control panel appears (see Figure 2-16).

• & HomeGroup				_	×
$\leftarrow \rightarrow \checkmark \uparrow$	•4 « All Control Panel Items > HomeGroup >	5	Search Contr	ol Panel	م
Share	with other home computers				
•6	There is currently no homegroup on the network.				
With a also str	homegroup, you can share files and printers with other computers o eam media to devices.	n your h	iome network.	You can	
The ho	megroup is protected with a password, and you'll always be able to o	hoose v	vhat you share		
Chang	advanced sharing settings				
Start th	e HomeGroup troubleshooter				
	Crea	te a hor	negroup	Close	

- 3. Click the Create a homegroup button. The Create a HomeGroup Wizard appears.
- 4. Click Next. The Share with other homegroup members page appears.
- 5. Select the libraries that you want to share and then click Next.
- 6. The wizard creates the HomeGroup and assigns it a password. The Use this password to add other computers to your homegroup page appears.
- **7.** Click **Finish**. The wizard closes and the HomeGroup control panel changes to reflect its current status.

When a Windows 10 computer using the Private network location does detect a HomeGroup on the network, the Network and Sharing Center control panel appears with an Available to Join link.

Figure 2-16

Opening the HomeGroup control panel



JOIN A HOMEGROUP

GET READY. Log in to Windows 10 using an account with Administrator privileges. Make sure that the system is configured to use the Private network location. To join a HomeGroup, perform the following steps.

- Open Control Panel and click Network and Internet > Network and Sharing Center. The Network and Sharing Center Control Panel appears.
- 2. Click the HomeGroup link. The HomeGroup control panel appears.
- 3. Click Join Now. The Join a HomeGroup Wizard appears.
- 4. Click Next. The Share with other homegroup members page appears.
- Select the libraries that you want to share and then click Next. The Type the homegroup password page appears.
- 6. In the Type the password text box, type the password supplied by the Create a HomeGroup Wizard and then click **Next**.
- 7. The You have joined the homegroup page appears.
- 8. Click **Finish**. The wizard closes and the HomeGroup control panel changes to reflect its current status.

To modify the default HomeGroup sharing configuration, you can select one of your shared libraries in File Explorer and then, on the Toolbar, click Share. Using the controls that appear in the ribbon, you can change other HomeGroup users' access to the library from Read to Read/Write. You can also limit access to specific HomeGroup users or prevent anyone on the network from accessing that library.

Mapping Drives

Drive mapping allows you to create a shortcut to a shared folder across a network. Instead of finding and connecting to the shared drive each time you log on, you can create a mapped drive that is available at all times. Just double-click the mapped drive to access the shared folder.

When you share a folder in Windows, you are usually using SMB, also known as Common Internet File System (CIFS). SMB has been around for years to provide shared access to files and printers. While SMB is usually associated with computers running Windows, it has become the de facto standard, which is access by most other operating systems including Linux, UNIX and Macintosh systems. To access a shared folder, you use the *universal naming convention (UNC)* based on the \\servername\sharename format. The UNC identifies the name of the server and the shared folder on the server.

Once you share a folder or drive on your computer with other users, an easy way for them to get to the shared item is by mapping a drive. A *mapped drive* is a shortcut to a shared folder or drive on another computer across a network. Windows Explorer makes this process easy and straightforward.

By default in Windows 10, network drive letters start from the back of the alphabet (Z: is the first default drive letter that displays) and work down, so as not to interfere with local drives (which start with A: and work up). When mapping a drive, you can select any drive letter that's not already in use.

A mapped network drive is displayed in Windows Explorer under Computer in the navigation pane.

The mapped drive displays in the Windows Explorer navigation pane. Click it to access the shared folder.



GET READY. To assign a drive letter to a shared folder on the network in Windows 10, perform the following steps.

- 1. Open File Explorer.
- Click the Home menu, click Easy access (as shown in Figure 2-17), and then click Map as drive.



3. The Map Network Drive Wizard starts. In the drop-down menu, select a drive letter of your choice (see Figure 2-18).

What n	etwork folder would you like to map?
Specify th	e drive letter for the connection and the folder that you want to connect to:
Drive:	Z: ~
Folder:	Browse
	Example: \\server\share
	Reconnect at sign-in
	Connect using different credentials
	Connect to a Web site that you can use to store your documents and pictures.

- **4.** Click **Browse** and then navigate to the shared folder you want to map to. Alternately, type the UNC path of the folder.
- 5. Select the shared folder and then click OK.
- **6.** By default, the **Reconnect at sign-in** check box is selected. This means the drive mapping will persist until you manually disconnect it (using the Disconnect network drive entry in the Tools menu in Windows Explorer). When you're done, click **Finish**.

Figure 2-18

Selecting a drive letter

Sharing Printers

One basic network services is network printing, in which multiple users can share the same printer. This is a cost-effective solution when you have multiple employees in different locations.

As an administrator, you can install two types of printers: local and network. Today, most local printers are connected using USB ports, although some legacy printers may use parallel or serial ports. Network printers can be shared local printers or printers that connect directly to a network with built-in network cards or expandable jet-direct cards.

When you install a physical printer, which Microsoft refers to as a *print device*, you must first connect the printer and turn it on. Next, you need to create a logical printer (Microsoft refers to this as the *printer*), which will provide a software interface between the print device and the applications. When you create the printer, you also load a print driver that acts as a translator for Windows and the programs running on Windows so that they do not have to worry about the specifics of the printer's hardware and printer language.

When you print a document in Windows, the printer uses the logical printer and printer driver to format the document into a form that is understood by the printer, including rendering it into a printer language such as HP's Printer Control Language or Adobe's Postscript to create an enhanced metafile (EMF). The *print job* is then sent to the local spooler, which provides background printing, allowing you to print and queue additional documents while your first document is being printed.

If a print job is being sent to the local print device, it will temporarily save it to the local hard drive's spool file. When the printer is available, it will then send the print job to the local print device. If Windows determines that the job is for a network print device, Windows sends the job to the print server's spooler. The print server's spooler will save it to the print server's hard drive spool file. Then, when the network print device becomes available, the job will print on the network print device.

INSTALLING PRINTERS

If you have the correct permissions to add a local printer or a remote shared printer, you can use the Add Printer Wizard to install the printer. After the printer is installed, it will appear in the Devices and Printers folder as well as in the Device Manager.



ADD A LOCAL PRINTER

GET READY. To add a local printer in Windows 10, perform the following steps.

- 1. Right-click the Start button and click Control Panel.
- 2. Under Hardware and Sound, click View Devices and Printers.
- 3. To start the Add Printer Wizard, click Add a printer.
- 4. If it does not find a printer, click The printer that I want isn't listed.
- **5.** On the Find a printer by other options page, click the **Add a local printer or network printer with manual settings**, as shown in Figure 2-19. Click **Next**.
- 6. On the Choose a printer port page, specify the port to which the printer is connected. See Figure 2-20. If the port already exists, such as an LPT1 or a network port specified by an IP address, select the port from the Use an existing port drop-down list. If the port does not exist, click **Create a new port**, select **Standard TCP/IP Port**, and then click **Next**. For the device type, you can select either Auto detect, TCP/IP device, or Web services device. Then specify the IP address or DNS name of the printer and the Port Name. If you type the address in hostname or IP address box, it will populate the IP address in the port name. It will then try to communicate with the printer using the address you specified.

76 | Lesson 2

Figure 2-19	X
Selecting the type of printer	- 🔶 📾 Add Printer
	Find a printer by other options
	 My printer is a little older. Help me find it. Select a shared printer by name Example: \\computername\printername or http://computername/printername/.printer Add a printer using a TCP/IP address or hostname Add a Bluetooth, wireless or network discoverable printer Add a local printer or network printer with manual settings
Figure 2-20	Next Cancel
Adding a local printer	- ← → Add Printer
	Choose a printer port
	A printer port is a type of connection that allows your computer to exchange information with a printer.
	Use an existing port: LPT1: (Printer Port) Create a new port:
	Type of port: Local Port ~

- **7.** If Plug and Play does not detect and install the correct printer automatically, you will be asked to specify the printer driver (printer manufacturer and printer model). If the printer is not listed, you will have to use the **Have Disk** option.
- 8. In the Type a Printer Name dialog box, type the name of the printer. If you want this to be the default printer for the system, select the Set as the default printer option. Click the Next button.
- 9. In the Printer Sharing dialog box, type the share name. You can also type the Location or Comments. Although Windows 10 supports long printer names and share names (including spaces and special characters), it is best to keep names short, simple, and descriptive. The entire qualified name, including the server name (for example, \\Server1\HP4100N-1), should be 32 characters or fewer.
- **10.** When the printer is successfully added, you can print the standard Windows test page by clicking the **Print a test page** button. Click **Finish**.

TAKE NOTE*

The TCP/IP printer port uses host port 9100 to communicate. Windows Servers can provide a driver to the clients if the driver is loaded on the server. For example, because Windows Server 2008 R2 is only available in 64-bit versions, it will have a 64-bit print driver so that the server can print to the printer. However, most computers used within organizations today will most likely be 32-bit clients that need to use 32-bit print drivers. Therefore, you would load both 64-bit and 32-bit print drivers on the server so that it can hand out either driver as needed.

ADD ADDITIONAL PRINT DRIVERS

GET READY. To add additional print drivers in Windows 10, perform the following steps.

- 1. Right-click the **Start** button and choose **Control Panel**.
- 2. Under Hardware and Sound, click View Devices and Printers.
- 3. Click a printer and then click the Print server properties button.
- **4.** Select the **Drivers** tab.
- 5. Click the Change Driver Settings.
- 6. Click Add.
- 7. In the Welcome to the Add Printer Driver Wizard, click Next.
- 8. Select the appropriate processor and operating system drivers and click Next.
- 9. On the Printer Driver Selection page (as shown in Figure 2-21), select the manufacturer or printer. If the printer that you want to add is not included, click **Have Disk** and provide a path for the printer driver. When the printer is selected, click Next.

Figure 2-21	Add Printer Driver Wizard	x
Selecting a print driver	Printer Driver Selection The manufacturer and model determine which printer driver to use.	
	Select the manufacturer and model of the printer driver to install. If the driver you want is not listed, click Have Disk to select the driver you want. If Windows Update is available, click it for more drivers for this processor.	
	Manufacturer Printers Brother Brother Color Leg Type1 Class Driver Canon Brother Color Type3 Class Driver Dell Brother Color Type4 Class Driver Eastman Kodak Company Brother Color Type4 Class Driver This driver is digitally signed. Have Disk Tell me why driver signing is important	
	< Back Next > Canoel	

10. When the wizard is complete, click Finish.

UNDERSTANDING PRINTER PROPERTIES

With most printers, you have a wide range of options. Although these options vary from printer to printer, they are easily accessible by right-clicking the printer in the Devices and Printers folder and choosing Printer Properties.

When you open Printer Properties, you will find the following options:

- General tab: Allows you to configure the printer name, location, and comments and to print a test page (see Figure 2-22). In addition, when you click the Preferences button, the default paper size, paper tray, print quality/resolution, pages per sheet, print order (such as front to back or back to front), and number of copies will display. The actual options that are available will vary depending on your printer.
- Sharing tab: Allows you to share a printer. You can also publish the printer in Active Directory if you chose the List in the directory option. Because a printer on a server can be used by other clients connected to the network, you can add additional drivers by clicking the Additional Drivers button.

TAKE NOTE*

You can also use group policies to install and configure printers.

78 | Lesson 2

Figure 2-22

The General tab

General Sharing Ports Advanced Color Managemer Image: Color Mathematical State Image: Color Mathematical State Image: Color Mathematical State Image: Color Mathematical State Location: Image: Color Mathematical State Image: Color Mathematical State Image: Color Mathematical State Location: Image: Color Mathematical State Image: Color Mathematical State Image: Color Mathematical State Model: HP LJ300-400 color M351-M451 PCL 6 Features Image: Color Nes Paper available: Double-sided: Yes Image: Color State Image: Color State Image: Color State State: No Speed: 18 ppm Image: Color State Image: Color State Maximum resolution: 600 dpi Image: Color State Image: Color State	Securi	ty	Device	Settings	About
	General	Sharing	Ports	Advanced	Color Manageme
Location: Comment: Model: HP LJ300-400 color M351-M451 PCL 6 Features Color: Yes Paper available: Double-sided: Yes Staple: No Speed: 18 ppm Maximum resolution: 600 dpi		Hewlett-Pa	ackard HP La	serJet 400 color N	1451dn
Comment: Model: HP LJ300-400 color M351-M451 PCL 6 Features Color: Yes Paper available: Double-sided: Yes Staple: No Speed: 18 ppm Maximum resolution: 600 dpi	Location:				
Model: HP LJ300-400 color M351-M451 PCL 6 Features Color: Yes Paper available: Double-sided: Yes Staple: No Speed: 18 ppm Maximum resolution: 600 dpi	Comment:				
Color: Yes Paper available: Double-sided: Yes Staple: No Speed: 18 ppm Maximum resolution: 600 dpi					
Double-sided: Yes Letter A Staple: No Speed: 18 ppm Maximum resolution: 600 dpi	Model:	HP LJ300-4	00 color M35	1-M451 PCL 6	
Staple: No Speed: 18 ppm Maximum resolution: 600 dpi	Model: Features Color: Yes	HP LJ300-4	00 color M35	1-M451 PCL 6 Paper available:	
Speed: 18 ppm Maximum resolution: 600 dpi 🛛 🗸 🗸 🗸	Model: - Features Color: Yes Double-sid	HP LJ300-4 ded: Yes	00 color M35	1-M451 PCL 6 Paper available:	~
Maximum resolution: 600 dpi	Model: Features Color: Yes Double-sio Staple: No	HP LJ300-4	00 color M35	1-M451 PCL 6 Paper available: Letter	^
	Model: Features Color: Yes Double-sid Staple: No Speed: 18	HP LJ300-4 ded: Yes	00 color M35	1-M451 PCL 6 Paper available: Letter	^
	Model: Features Color: Yes Double-sic Staple: No Speed: 18 Maximum	HP LJ300-4 ded: Yes ppm resolution: 60	00 color M35 00 dpi	1-M451 PCL 6 Paper available: Letter	~

- **Ports tab:** Allows you to specify which port (physical or TCP/IP) the printer will use, as well as to create new TCP/IP ports.
- Advanced tab: Allows you to configure the driver to use with the printer, the priority of the printer, when the printer is available, and how print jobs are spooled.
- Security tab: Allows you to specify the permissions for the printer.
- **Device Settings tab:** Allows you to configure the trays, font substitution, and other hardware settings.

SETTING PRINTER PERMISSIONS

Printers are considered objects. Therefore, as with NTFS files and folders, you can assign permissions to a printer so that you can specify who can use the printer, who can manage the printer, and who can manage the print jobs.

Printer permissions define what can access a user or group has to printers. On the Security tab, Windows 10 provides the following printer permissions (see Figure 2-23):

- Print: Allows users to send documents to the printer.
- Manage this printer: Allows users to modify printer settings and configurations, including the ACL itself.

Security aircup or user names: Leveyone LALL APPLICATION CREATOR OWNER Pat (PAT8\Pat) Administrators (PAT8	PACKAGES	ce Settings		About
Aroup or user names:	PACKAGES t 3\Administrators)			
Everyone ALL APPLICATION CREATOR OWNER Pat (PAT8\Pat) Administrators (PAT8	PACKAGES t 3\Administrators)			
Image: ALL APPLICATION CREATOR OWNER Pat (PAT8\Pat) Administrators (PAT8)	PACKAGES t 3\Administrators)			
CREATOR OWNER Pat (PAT8\Pat)	t 3\Administrators)			
Administrators (PAT8)	3\Administrators)			
Administrators (PA16	s (Administrators)			
			Add	Remove
				-
emissions for Everyone			Allow	Deny
Print				Ц
Manage this printer				
Manage documents				
Special permissions				

Figure 2-23

Managing printer permissions

- Manage documents: Provides the ability to cancel, pause, resume, or restart a print job.
- **Special permissions:** Permissions typically used only by system administrators, such as a permission to change the printer owner.

By default, the Print permission is assigned to the Everyone group. If you need to restrict who can print to the printer, you will need to remove the Everyone group and add another group or user and assign the Allow print permission to the user or group. Of course, it is still recommended that you use groups instead of users. As with file permissions, you can also deny print permissions.

MANAGING PRINT JOBS

The print spooler is an executable file that manages the printing process, which includes retrieving the location of the correct print driver, loading the driver, creating the individual print jobs, and scheduling the print jobs for printing.

On occasion, a print job may have been sent that was not intended, or you may decide it is not necessary to print a job. Therefore, you need to delete the print job from the print queue.



Figure 2-24

Viewing the print queue

VIEW THE PRINT QUEUE

GET READY. To view the print queue in Windows 10, perform the following steps.

- 1. Right-click the Start button and click Control Panel.
- 2. Under Hardware and Sound, click View Devices and Printers.
- 3. Double-click the printers for which you want to view the print jobs waiting to print.
- **4.** To view the print queue, click **See what's printing**. A dialog box opens, as shown in Figure 2-24.

/	10.1.1.0.0.1.1.1					
← → • ↑ 🔮 « Devic	es and Printers > Hewlett-Packard H	P LaserJet 400 color M45	Idn on pat8	~	C Searc	ch Hewlett-Packard H
	\\pat8\Hewlett-Packard	HP LaserJet 400 c	olor M451d	n		
	HP L J300-400 color M351-M45	1				
	HD Lacorlet: Logondan; roli	ability and superior prin	t quality			
	Original HP print cartridge	s: Save time and money	t quanty			
	HP Eco Solutions for printi	na: Reduce. Recycle. Rei	nvent.			
-	- The cooperations for print	ngi neadeei neeyelei nei				
		L	1 10			
Drinter Antinue	Mewlett-Packard HP	LaserJet 400 color M451	dn on pat8			- 0
Print photos, docum	ents and adj	ew				
See what's printing	Customize y Document Name	Status	Owner	Pages	Size	Submitted
More Software						
Explore new HP Apps	; for your we					
·						
	<					

The print queue shows information about a document, such as print status, owner, and number of pages to be printed. To pause a document, open the print queue, right-click on the document you want to pause and choose Pause. If you want to stop printing the document, right-click on the document that you want to stop printing and choose Cancel. You can cancel the printing of more than one document by holding down the Ctrl key and clicking on each document that you want to cancel. By default, all users can pause, resume, restart, and cancel their own documents. To manage documents that are printed by other users, however, you must have the Allow manage documents permissions.

When the print device is available, the spooler retrieves the next print job and sends it to the print device. By default, the spool folder is located at C:\Windows\\System32\Spool\ PRINTERS. If you have a server that handles a large number of print jobs or several large print jobs, make sure the drive where the spool folder is has sufficient disk space.

CHANGE THE LOCATION OF THE SPOOL FOLDER

GET READY. To change the location of the spool folder in Windows 10, perform the following steps.

- 1. Open the Devices and Printers folder.
- 2. Click a printer and select the Print server properties.
- 3. Click the Advanced tab.
- 4. Click the Change Advanced Settings button.
- **5.** Specify the new location and click **OK**.

On occasion, the print spooler may freeze or become unresponsive. You can restart the print spooler by following these steps:

- 1. Open the Services console located in Administrative Tools.
- 2. Right-click Print Spooler and choose Restart.

You can also stop and start the service.

Understanding Data Encryption

THE BOTTOM LINE

In Lesson 1, you learned about encryption as well as Encrypting File System and BitLocker. Encryption was defined as the process of converting data into a format that connect be read by another user while decryption is the process of converting data from encrypted format back to its original format.

CERTIFICATION READY Describe data encryption 2.5 Encryption algorithms can be classified according to three types:

- Symmetric
- Asymmetric
- Hash function

Symmetric encryption uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption. To use symmetric key algorithms, you need to initially send or provide the secret key to both the sender and the receiver.

Asymmetric key, also known as *public-key cryptography*, uses two mathematically related keys. One key is used to encrypt the data and the second key is used to decrypt the data. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. Instead, you can make the *public key* known to anyone and the *private key* is used only by the person or organization that wants to secure data.

Use the other key to encrypt or decrypt the data. The public key can be sent to someone or it can be published within a digital certificate via a CA. Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Pretty Good Privacy (PGP) use asymmetric keys. Those topics are covered later in this lesson.

For example, say you want a partner to send you data. Therefore, you send the partner the public key. The partner then encrypts the data with the key and sends you the encrypted message. You then use the private key to decrypt the message. If the public key falls into someone else's hands, that person still cannot decrypt the message.

The last type of encryption is the *hash function*. Different from the symmetric and asymmetric algorithms, a hash function is meant as one-way encryption. That means that after the data has been encrypted, it cannot be decrypted. One example of its use is to use the hash function to encrypt a password that is stored on disk. Anytime a password is entered and it needs to be verified that it is the correct password, the same hash calculation is performed on the entered password and compared to the hash value of the password stored on disk. If the two match, the user must have typed in the password. This avoids storing the passwords in a readable format that a hacker might try to access.

No matter what encryption algorithm you choose, they all use keys to encrypt data. The key must be long enough so that an attacker cannot try all possible combinations to figure out what the key is. Therefore, a key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms. 128-bit keys are commonly used and considered strong.

Understanding Certificates and Their Use

Digital certificates are very common in today's computer world. They are used in encryption as the component that stores the public key, they are used to identify a person (authentication) or organization, and they are used to ensure that something has not been modified.

A digital certificate is similar to an electronic identification card used to certify the online identify of individuals, organizations, and computers. It contains a person's or an organization's name, a serial number, an expiration date, a copy of the certificate holder's public key (used for encrypting messages and creating digital signatures), and the digital signature of the Certificate Authority (CA)—described later in this lesson—that assigned the certificate so that recipients can verify that the certificate is real.

UNDERSTANDING SECURE SOCKETS LAYER (SSL)

When you surf the Internet, there are times when you need to transmit private data over the Internet such as credit card numbers, social security numbers and so on. During these times, you should be using SSL over http (https) to encrypt the data sent over the Internet. By convention, URLs that require an SSL connection start with https: instead of http:.

Secure Socket Layer (SSL) uses a cryptographic system that uses two keys to encrypt data, a public key known to everyone and a private or secret key known only to the recipient of the message. The public key is published in a digital certificate, which also confirms the identity of the web server.

When you connect to a site that is secured using SSL using Internet Explorer 11. Clicking the lock icon displays more information about the site, including the identity of the CA that issued the certificate, as shown in Figure 2-25. For even more information, you can click the View Certificate link to open the Certificate dialog box.

When visiting certain websites, Internet Explorer may find problems with the digital certificate, such as the certificate has expired, it is corrupted, it has been revoked, or it does not match the name of the website. When this happens, IE will block access to the site and display a warning stating that there is a problem with the certificate. You then have a chance to close the browser window or ignore the warning and continue on to the site. Of course, if you chose to ignore the warning, make sure you trust the website and you believe that you are communicating with the correct server.

Figure 2-25

Viewing the SSL website identification in Internet Explorer 11



Transport Layer Security (TLS) is an extension of SSL, which is supported by Internet Engineering Task Force (IETF) so that it could be an open, community-supported standard, which could then be expanded with other Internet standards. While TLS is often referred to as SSL 3.0, it does not interoperate with SSL. While TLS is usually default for most browsers, it has a downgrade feature that allows SSL 3.0 to run as needed.

USING DIGITAL CERTIFICATES TO ENCRYPT DATA

Since email is sent over the Internet, one may be concerned with the data packets being captured and read. Therefore, there is a need to encrypt emails that contain confidential information. There are multiple protocols that can be used to encrypt emails. They include:

- Secure multipurpose Internet Mail Extension (S/MIME)
- Pretty Good Privacy (PGP)

Secure multipurpose Internet Mail Extension (S/MIME) is the secure version of MIME, used to embed objects within email messages. It is the most widely supported standard used to secure email communications, which uses the PKCS #7 standard. S/MIME is included popular web browsers and has also been endorsed by other vendors that make messaging products.

Pretty Good Privacy (PGP) is a freeware email encryption system that uses symmetrical and asymmetrical encryption. When email is sent, the document is encrypted with the public key and also a session key. The session key is a one-use random number used to create the ciphertext. The session key is encrypted with the public key and sent with the ciphertext. When the message is received, the private key is used to extract the session key. The session key and the private key are used to decrypt the ciphertext.

If someone steals a hard drive that is protected by NTFS permissions, they could take the hard drive, put it in a system in which they are an administrator of and access all files and folders on the hard drive. Therefore, to truly protect a drive that could be stolen or accessed illegally, you can encrypt the files and folders on the drive.

Windows 10 offers two file-encrypting technologies: Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders while BitLocker protects entire drives.

Virtual Private Networks (VPNs)—covered later in this lesson—allow remote users to connect to a private network by using tunneling protocol, such as Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP). Digital certificates are also used with IP Security (IPsec), which are often to connect two computers together or to have a remote computer connect to a corporate office over the Internet. The IP Security extensions enable you to encrypt and digitally sign communications, to prevent intruders from compromising them as they are transmitted over a network.

DIGITAL CERTIFICATES USED IN WIRELESS COMMUNICATIONS

Within a few months after the security weaknesses were identified with Wired Equivalent Privacy (WEP), IEEE created Wi-Fi Protected Access (WPA) as an interim standard prior to the ratification of 802.11i followed by WPA2. WPA provides strong data encryption via Temporal Key Integrity Protocol (TKIP), while Wi-Fi Protected Access 2 (WPA2) provides enhanced data encryption via Advanced Encryption Standard (AES), which meets the Federal Information Standard (FIPS) 140-2 requirement of some government agencies. To help prevent someone from hacking the key, WPA and WPA2 rotate the keys and change the way keys are derived.

Both WPA and WPA2 can run in both personal and enterprise mode. Personal mode, designed for home and small office networks, provides authentication via a pre-shared key or password.

Enterprise mode provides authentication using IEEE 802.1X and Extensible Authentication Protocol (EAP). 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority such as a RADIUS server (RADIUS is described in more depth later in this lesson). Since it uses EAP, the actual algorithm that is used to determine whether a user is authentic is left open so that multiple algorithms can be used and even added as new ones are developed. Enterprise mode uses two sets of keys: the session keys and group keys. The session keys are unique to each client associated between an access point and a wireless client. Group keys are shared among all clients connected to the same access point. Both sets of keys are generated dynamically and are rotated to help safeguard the integrity of keys over time. The encryption keys could be supplied through a certificate or smart card.

DIGITAL SIGNATURE

A *digital signature* is a mathematical scheme that is used to demonstrate the authenticity of a digital message or document. It is also used to ensure that the message or document has not been modified. The sender uses the receiver's public key to create a hash of the message, which stored in the message digest. The message is then sent to the receiver. The receiver will then use his or her private key to decrypt the hash value, perform the same hash function on the message and compare the two hash values. If the message has not been changed, the hash values will match.

To prove that a message comes from a particular person, you can perform the hashing function with your private key and attach the hash value to the document to be sent. When the document is sent and received by the receiving party, the same hash function is completed. You then use the sender's public key to decrypt the hash value included in the document. If the two hash values match, the user who sent the document must have known the sender's private key, proving who sent the document. It will also prove that the document has not been changed.

USING A SMART CARD

A *smart card* is a pocket-sized card with embedded integrated circuits consisting of non-volatile memory storage components, and perhaps dedicated security logic. Non-volatile memory is memory that does not forget its content when power is discontinued. They can contain digital certificates to prove the identity of someone carrying the card and may contain permissions and access information. Since a smart card can be stolen, some smart cards will not have any markings on it so that it cannot be easily identified on what it can open. In addition, many organizations will usually use a password or PIN in combination of the smart card.

The restricted enrollment agent allows limiting the permissions that users designated as enrollment agents have for enrolling smart card certificates on behalf of other users.

USING SOFTWARE CODE SIGNING

Today, executable file, scripts and drivers can be signed to prove where it came from and if the software, script or driver has been modified. Microsoft's Authenticode is one technology that uses certificates to confirm that the software a user downloads and installs actually come from the publisher and has not been modified. In today's 64-bit versions of Windows, you cannot install a driver that has not been signed.

Managing Certificates

The most common digital certificate is the X.509 version 3. The X.509 version 3 standard specifies the format for the public key certificate, certificate revocation lists, attribute certificates, and a certificate path validation algorithm.

Some of the X.509 digital certificate (see Figure 2-26) includes the following fields:

- Version: The version of the certificate format, such as version 3.
- Serial number: The unique serial number that is assigned by the issuing CA. Based on the serial number, the CA maintains an audit history for each certificate so that certificates can be traced, including when the certificate has been revoked.
- **Signature algorithm and Signature hash algorithm:** The public key cryptography and message digest algorithms that are used by the issuing CA to digitally sign the certificate.
- **Issuer:** The name of the issuing CA.
- Validity from and Valid to: The certificate's start and expiration dates.
- Subject: The person, entity, or owner identified in the certificate.
- Public key: The public key and a list of the public key cryptography algorithms.
- **Key usage:** The purpose of the public key, such as encipherment, signature, certificate signing, and so on).
- **Thumbprint:** The digest or mathematical calculation of the certificate information that can be used to determine if the digital certificate was altered.

There are only so many root CA certificates that are assigned to commercial third-party organizations. Therefore, when you acquire a digital certificate from a third-party organization, you might need to use a certificate chain to obtain the root CA certificate so that it can be



trusted. In addition, you might need to install an intermediate digital certificate that links the assigned digital certificate to a trusted root CA certificate. The *certificate chain*, also known as the *certification path*, is a list of certificates used to authenticate an entity. It begins with the certificate of the entity and ends with the root CA certificate.

The third tab of a certificate is the certification path, as shown in Figure 2-27. The path starts with the Subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

Figure 2-27	Certificate	×
Viewing a certification path	General Details Certification Path Certification path VerSign Symantec Class 3 EV SSL CA - G3	ate
	Certificate status:	ОК

On a local computer running Windows, the certificates are stored in a certificate store. Using the Certificates MMC snap-in, you can display the certificate store for a user, a computer, or a service according to the purpose for which the certificates were issued or by using their logical storage categories. Certificates are then organized into the following folders:

- **Personal:** These are certificates associated with public keys to which you have access. These are the certificates that have been issued to the user, the computer, or service that you are viewing.
- **Trusted Root Certificate Authorities:** Implicitly trusted CAs, including all of the certificates in the third-party root CAs, store plus root certificates from your organization and Microsoft.
- Enterprise Trust: This is a container for certificate trust lists, including self-signed root certificates from other organizations.
- Intermediate Certificate Authorities: These are certificates issued to subordinate CAs.
- **Trusted People:** These are certificates issued to users or end entities that are explicitly trusted. Most often these are self-signed certificates or certificates explicitly trusted in an application such as Microsoft Outlook.
- **Other People:** These are certificates issued to users or end entities that are implicitly trusted. These certificates must be part of a trusted certification hierarchy. Most often these are cached certificates for services such as Encrypting File System, where certificates are used for creating authorization for decrypting an encrypted file.
- **Trusted Publishers:** These are certificates from CAs that are trusted by Software Restriction policies.
- Third-Party Root Certificate Authorities: Trusted root certificates from CAs other than Microsoft and your organization.
- Certificate Enrollment Requests: These are pending or rejected certificate requests.
- Active Directory User Object: These are certificates associated with your user object and published in Active Directory.

ACCESS A CERTIFICATE STORE

GET READY. To access a certificate store in Windows 10, perform the following steps.

- 1. Click the Start button, type mmc.exe, and then press Enter.
- 2. When the console opens, click File > Add/Remove snap-in.
- 3. In the Add or Remove Snap-ins dialog box, double-click Certificates.
- 4. On the Certificates snap-in dialog box, click one of the following:

My user account

Service account

Computer account

- If you click My user account, click Finish. If you click Computer account, click Next, choose Local computer, and then click Finish. If you click Service Account, click Local computer, click Next, click a service account to manage, and then click Finish.
- **6.** In the Add or Remove Snap-ins dialog box, click **OK**. The Certificates store opens (see Figure 2-28).

Windows can also publish certificates to Active Directory. Publishing a certificate in Active Directory enables all users or computers with adequate permissions to retrieve the certificate as needed.

Digital certificates can be imported and exported via electronic files. Four common formats are as follows:

- **Personal Information Exchange (PKCS #12):** The Personal Information Exchange format (PFX, also called PKCS #12) supports secure storage of certificates, private keys, and all certificates in a certification path. The PKCS #12 format is the only file format that can be used to export a certificate and its private key. It usually has a .pfx or .p12 filename extension.
- **Cryptographic Message Syntax Standard (PKCS #7):** The PKCS #7 format supports storage of certificates and all certificates in a certification path. It usually has a .p7b or .p7c filename extension.
- **DER-encoded binary X.509:** The Distinguished Encoding Rules (DER) format supports storage of a single certificate. This format does not support storage of the private key or certification path. It usually has a .cer, .crt, or .der filename extension.
- **Base64-encoded X.509:** The Base64 format supports storage of a single certificate. This format does not support storage of the private key or certification path.

a Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]						
File Action View Favorites Window	Help					_ 8 ×
						,
Console Root	Issued To	Issued By	Expiration Da	Intended Purposes	۴^	Actions
 Console Additional Console Additin Console Additional Console Additional Console Additional Con	Issued Io AddTrust External CA Root AddTrust External CA Root Case Baltimore CyberTrust Root Class 3 Public Primary Certificat Digitation Case Case Case Case Case Case Case Case	Issued By AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Global Root CA DigiCert Global Root CA GlobalSign Root CA Microsoft Root Certificate Authori Microsoft Root Certificate Authori NO LIABLILTY ACCEPTED, (c)97 Ve SecureTrust CA Starfield Root Certificate Authorit Symantec Enterprise Mobile Root Thawte Premium Server CA	Expiration Da 5/30/2020 5/12/2025 8/1/2028 12/30/1999 11/9/2031 11/9/2031 11/9/2031 11/9/2031 8/22/2018 8/22/2018 8/22/2018 8/13/2018 12/31/1999 12/31/2020 5/9/2021 6/23/2035 3/22/2036 1/7/2004 12/31/2029 12/31/2029 12/31/2029 12/31/2020	Intended Purposes Server Authenticati Secure Email, Client Time Stamping Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Secure Email, Client Secure Famil, Code <all> <all> <all> Time Stamping Server Authenticati Code Signing Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati</all></all></all>	 	Certificates A More >
< >	<				>	
Trusted Root Certification Authorities store contai	ns 26 certificates.					

Figure 2-28

Viewing a certificate store

Understanding Certificate Services

Active Directory Certificate Services (AD CS) is a server role that allows you to issue and manage digital certificates as part of a public key infrastructure. Public key infrastructure (PKI) is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates. PKI consists of certificate authorities and registration authorities that verify and authenticate the validity of each entity that is involved in an electronic transaction through the use of public key cryptography. Within the PKI, the certificate authority (CA), also known as certificates authority, binds a public key with respective user identities and issues digital certificates containing the public key.

When you install a CA, you have the following choices:

- Standalone CA or Enterprise CA
- Root CA or Subordinate CA

The *standalone CA* works without Active Directory and does not need Active Directory, however, the server can be a member of a domain. Users can request certificates using a manual procedure or web enrollment, where they have to identify information and specify the certificate they need. By default, all certificate requests submitted to standalone CAs are held in a pending queue until a CA administrator approves them. However, you can configure standalone CAs to issue certificates automatically upon request, but this is less secure and is usually not recommended.

An *enterprise CA* requires Active Directory and is typically used to issue certificates to users, computers, devices, and servers for an organization. Users can request certificates using manual enrollment, web enrollment, auto-enrollment, or an enrollment agent. Because information for a user or computer can be retrieved from Active Directory, templates can be used to generate certificates with the appropriate attributes for the specified certificate type.

The top of the certificate hierarchy is the *root CA*. Because everything branches from the root, it is trusted by all clients within an organization. Although smaller organizations have only one CA, larger organizations have a root CA with multiple subordinate CAs. Although the enterprise CA can issue certificates to end users, it is usually used to issue certificates to subordinate CAs.

Although there is only one root CA, there can be one or more *subordinate CA*. The number of subordinate CAs needed is determined by geographical location and number of clients.

If a CA is compromised, all certificates issued by the CA and any subordinate CAs that are under the compromised CA (and corresponding issued certificates) are also considered compromised.

If you have an enterprise CA, the domain computers will automatically receive a copy of the enterprise CA certificate in the Certificates (Computer)\Trusted Root Certification Authorities\Certificates folder so that the client computer automatically trusts the enterprise CA and the certificates that come from the CA.

To trust a CA including local standalone CAs, you need to manually add the CA certificate to the Trusted Root Certification Authorities\Certificates folder or you can use Group Policies to add the certificates. To use group policies, you need to export the CA certificate to a file and then use Group Policy Management console to create or modify a Group Policy Object (GPO).

Moving and Copying EFS-Encrypted Folders

When you move or copy files from one location to another, you need to understand what happens to the files' NTFS permissions.

When working with EFS, keep the following in mind:

- You can encrypt or compress NTFS files only when using EFS; you can't do both. If the user marks a file or folder for encryption, that file or folder is uncompressed.
- If you encrypt a file, it is automatically decrypted if you copy or move the file to a volume that is not an NTFS volume.
- Moving unencrypted files into an encrypted folder automatically causes those files to be encrypted in the new folder.
- Moving an encrypted file from an EFS-encrypted folder does not automatically decrypt files. Instead, you must explicitly decrypt the file.
- Files marked with the System attribute or that are in the root directory cannot be encrypted.
- Remember that an encrypted folder or file does not protect against the deletion of the file, listing the files or directories. To prevent deletion or listing of files, use NTFS permissions.
- Although you can use EFS on remote systems, data that is transmitted over the network is not encrypted. If encryption is needed over the network, use SSL/TLS (Secure Sockets Layer/Transport Layer Security) or IPsec.

When copying and moving files, the following three scenarios can result:

- If a folder or file is copied, the new folder or file will automatically acquire the permissions of the drive or folder to which it is being copied.
- If a folder or file is moved within the same volume, the folder or file will retain the same permissions that were already assigned.
- If a folder or file is moved from one volume to another volume, the folder or file will automatically acquire the permissions of the drive to which it is being moved.

Using BitLocker To Go

BitLocker To Go enables users to encrypt removable USB devices, such as flash drives and external hard disks. While BitLocker has always supported the encryption of removable drives, BitLocker To Go enables you to use the encrypted device on other computers without having to perform an involved recovery process. Because the system is not using the removable drive as a boot device, a TPM chip is not required.

As mentioned earlier in the lesson, BitLocker is used to encrypt an entire disk or volume. It is used to protect sensitive data stored on fixed disks in situations that they are lost, stolen, or moved to another computer. BitLocker was described in Lesson 2; BitLocker To Go is an extension of BitLocker that is used to encrypt removal USB devices.

To use BitLocker To Go, insert the removable drive and open the BitLocker Drive Encryption Control Panel. The device appears in the interface with a Turn on BitLocker link just like that of the computer's hard disk drive.

Using a Virtual Private Network (VPN)

Today, it is very common for an organization to use a *remote access server (RAS)*, which enables users to connect remotely to a network using various protocols and connection types. By connecting to the RAS over the Internet, users can remotely connect to their organization's network and access data files, applications, and email just as if they were sitting in their offices.

A *Virtual Private Network (VPN)* is a private network that uses a public network (for example, the Internet) to connect remote sites and users. The VPN makes it appear to computers, on each end of the connection, as if they are actually connected to the same network. This point-to-point connection is emulated by encapsulating the packet in an IP Header. The information in the header is used to route the information between the two VPN endpoints.

Tunneling protocols, authentication protocols and encryption levels applied to the VPN connections determine the level of VPN security you have available. In order for a VPN to work both the client and server will need to utilize the same protocols. Overall, VPNs can provide the following capabilities:

- Data encryption (confidentiality)
- Authentication
- Data Integrity (ensure the packets are not modified while in transit)
- Non-Repudiation (guarantee the packets came from the source at a specific time)

The VPN uses the concept of tunneling (see Figure 2-29) to establish and maintain a logical network connection.

There are four types of VPN Tunneling protocols you will encounter:

- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec)
- Secure Socket Tunneling Protocol (SSTP)
- VPN Reconnect (or IKEv2)

The four types of tunneling protocols used with a VPN/RAS server running on Windows 10:

- *Point-to-Point Tunneling Protocol (PPTP)*: A VPN protocol based on the legacy Point-to-Point protocol used with modems. Unfortunately, PPTP is easy to set up but is considered to use weak encryption technology.
- *Layer 2 Tunneling Protocol (L2TP)*: Used with IPSec to provide security. L2TP is the industry standard when setting up secure tunnels.
- *Secure Socket Tunneling Protocol (SSTP)*: Introduced with Windows Server 2008 and Windows Vista allows users to use HTTPS protocol over TCP port 443 to pass traffic through firewalls and web proxies that might block PPTP and L2TP/IPSec.
- *Internet Key Exchange Version 2 (IKEv2)*: Also known as *VPN Reconnect*, this is a feature introduced with Routing and Remote Access Services (RRAS) in Windows Servers. It is designed to provide users with consistent VPN connectivity and automatically reestablish a VPN when users temporarily lose their Internet connection.



When using VPNs, Windows 10 support the following forms of authentication:

- *Password Authentication Protocol (PAP)*: Uses plain text (unencrypted passwords). PAP is the least secure authentication and is not recommended.
- *Challenge Handshake Authentication Protocol (CHAP)*: A challenge-response authentication that uses the industry standard md5 hashing scheme to encrypt the response. CHAP was an industry standard for years and is still quite popular.
- *Microsoft CHAP version 2 (MS-CHAP v2):* Provides two-way authentication (mutual authentication). MS-CHAP v2 provides stronger security than CHAP.
- *Extensible Authentication Protocol (EAP-MS-CHAPv2)*: A universal authentication framework that allows third-party vendors to develop custom authentication schemes including retinal scans, voice recognition, fingerprint identifications, smart cards, Kerberos, and digital certificates. It also provides a mutual authentication method that supports password-based user or computer authentication.

Windows 10 provides a simple Getting Started Wizard—also known as the Get Connected Wizard (GCW)—that helps make the setup and configuration of a VPN connection quick and simple for end users.

To make the process of setting up a VPN profile and connecting to a VPN much simpler in Windows 10, you can use the Create a VPN Connection Wizard.

The Getting Started Wizard requires that you enter the server information and then it autodiscovers the authentication methods and tunneling protocols during the initial connection process.

 Θ

CREATE A VPN CONNECTION USING THE GETTING STARTED WIZARD

GET READY. To create a VPN using the Getting Started Wizard in Windows 10, perform the following steps.

- 1. On the Taskbar, right-click the Network Status icon and choose Open Network and Sharing Center.
- 2. In the Network and Sharing Center window, click setup a new connection or network.
- In the Set Up a Connection or Network Wizard, click Connect to a workplace and then click Next.
- 4. On the How do you want to connect page, click Use my Internet connection (VPN).
- **5.** On the Type the Internet address to connect to page (as shown in Figure 2-30), in the Internet address text box, type the host name or IP address of the Remote Access server. In the Destination name text box, type a label that will identify the VPN connection. Click **Create**.

Figure 2-30			×
Creating a VPN connection	← La Connect to a Workplace		
	Type the Internet address to connect to		
	Your network administrator can give you this address.		
	Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]		
	Destination name: VPN Connection		
	 ☐ Use a smart card ☑ Remember my credentials ☑ Allow other people to use this connection This option allows anyone with access to this computer to use this connection. 		
	Create	Ca	incel

Authentication and Tunneling protocols will be negotiated and configured during the first successful connection attempt using the user name and password.

- 6. To see the VPN connections, you can click the Network Status icon on the Taskbar.
- 7. Click the VPN connection you created and then click Connect.
- 8. Type your credentials and then click OK.

You can also view and edit your connection by opening the Network and Sharing Center, and clicking Change adapter settings. Then right-click VPN connection and choose Properties.

The following provides a brief explanation for each tab:

- General: Provides host name and IP address of VPN server.
- Options: Enables and disables your credentials, sets idle time before hanging up, and configures PPP settings.
- Security: Configures Data encryption settings, authentication, and tunneling protocols, as shown in Figure 2-31.
- Networking: Configures transports (IPv6, IPv4, File and Printer Sharing, and Client for Microsoft Networks).
- Sharing: Enables settings that allow others to connect through this computer's network connection.

igure 2-31	VPN Connection Properties
onfiguring the type of VPN onnection and data encryption sed	General Options Security Networking Sharing
	Automatic
	Advanced settings
	Optional encryption (connect even if no encryption) $$
	Authentication
	O Use Extensible Authentication Protocol (EAP) Properties
	Allow these protocols
	EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.
	Unencrypted password (PAP)
	Challenge Handshake Authentication Protocol (CHAP)
	Microsoft CHAP Version 2 (MS-CHAP v2)
	 Automatically use my Windows logon name and password (and domain, if any)

SUMMARY SKILL MATRIX

OK Cancel

IN THIS LESSON YOU LEARNED:

- Using public cloud services such as OneDrive and Office 365 enables you to take advantage of hosted solutions. This means users have the ability to access their information from anywhere at any time across multiple devices.
- Public cloud services provide a way to access information from anywhere at any time. There are many definitions for the cloud. Microsoft defines a public cloud as a web-based service that is hosted outside of your organization.
- OneDrive is a free, secure file-hosting service that enables users to store, sync, and share • files across devices using the cloud. OneDrive is free online personal storage that is included with a Microsoft account or Outlook.com account and includes a light version of Office apps. OneDrive for Business is online storage intended for business purposes and it's built on online SharePoint.

F

C C u

- Taking advantage of cloud computing services such as Microsoft Office 365 can reduce the workload on your IT staff. It can also improve the collaboration between your team members.
- Azure Storage is cloud storage designed for large-scale applications including providing a storage foundation for Azure virtual machines. The cost for Azure Storage is based on the amount of data stored and the number of requests made.
- Storage Spaces is a feature in Windows 10/Windows Server 2016 that allows you to combine
 multiple disks into a single logical volume that can be mirrored to protect against one or
 more drive failures. When the drives are combined, Windows places them into a storage pool.
- A file system is a method of storing and organizing computer files and the data they contain to make it easy to find and access this information. A file system also maintains the physical location of the files so that you can find and access the files in the future. Windows 10 supports FAT16, FAT32, NTFS and Resilient File System (ReFS) file systems on hard drives.
- A permission is defined as the type of access that is granted to an object, such as NTFS files and folders. When files and folders are created on an NTFS volume, a security descriptor known as an Access Control List (ACL) is created.
- The folder/file structure on an NTFS drive can be complicated, with many folders and nested folders. In addition, because you can assign permissions to groups and at different levels on an NTFS volume, figuring out the effective permissions of a particular folder or file for a particular user can be tricky.
- Most users are not going to log onto a server directly to access their data files. Instead, a drive
 or folder will be shared (known as a shared folder), and they will access the data files over a
 network. To help protect against unauthorized drive or folder access, you should use share
 permissions along with NTFS permissions (assuming the shared folder is on an NTFS volume).
- One basic network services is network printing, in which multiple users can share the same printer. This is a cost-effective solution when you have multiple employees in different locations.
- Encryption was defined as the process of converting data into a format that connect be read by another user while decryption is the process of converting data from encrypted format back to its original format.

Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

- A pocket-sized card with embedded integrated circuits that is used for authentication is known as a(n) _____.
- 2. A(n) ______ defines the type of access over an object or the properties of an object such as an NTFS file or printer.
- 3. _____ permissions flow from a parent object to a child object.
- **4.** ______ is a Microsoft file-hosting service that allows you to store and create files and folders and share them with other users and groups.
- 5. ______ is a Microsoft cloud storage designed for large-scale applications including providing a storage foundation for Azure virtual machines.
- 6. ______ allow you to combine multiple smaller drives into a single larger logical volume
- 7. When using storage spaces, you will need a minimum of ______ drives to create a three-way mirror.
- 8. Most Windows 10 users use the ______ file system because it supports larger disks than FAT32 or FAT.
- 9. The newest file system used in Windows that is designed to increase data availability, even when there are errors, is _____.
- **10.** The ______ permission needed for a user to manage his print jobs.

Multiple Choice

Circle the letter that corresponds to the best answer.

- 1. Which NTFS permission is needed to change attributes and permissions?
 - **a.** Full Control
 - **b.** Modify
 - **c.** Read and Execute
 - **d.** Write
- 2. Which type of permission is granted directly to a file or folder?
 - **a.** Explicit
 - **b.** Inherited
 - **c.** Effective
 - **d.** Share
- **3.** If you copy a file or folder to a new volume, which permissions will that file or folder have?
 - **a.** The same permissions that it had before.
 - **b.** The same permissions as the target folder.
 - c. The same permissions as the source folder.
 - **d.** No permissions at all.
- **4.** Which of the following uses an ACL?
 - **a.** NTFS folder
 - **b.** Active Directory user
 - **c.** Registry key
 - d. Login rights
- 5. Which type of key has one key for encryption and a different key for decryption?
 - **a.** Symmetric
 - **b.** Asymmetric
 - c. Hash function
 - d. PKI
- 6. Which infrastructure is used to assign and validate digital certificates?
 - a. Asymmetric algorithm
 - **b.** Active Directory
 - c. PKI
 - d. VPN
- 7. Which of the following is *not* a share permission?
 - a. Full Control
 - **b.** Write
 - **c.** Change
 - **d.** Read
- **8.** Which of the following is a subscription-based software service that enables users to use Office Apps via the Web?
 - a. Microsoft Office 365
 - **b.** Skynet
 - **c.** AppLocker
 - d. GPOs

- **9.** The person who signs up for the business and enterprise Office 365 subscription is assigned which of the following roles by default?
 - a. Global Administrator
 - b. User Management Administrator
 - c. Billing Administrator
 - d. Service Administrator
- **10.** Which method provides the easiest way to quickly share files and folders with other users on the network just by copy the files and folders?
 - a. Advanced Sharing
 - **b.** Quick share
 - **c.** Public folders
 - **d.** HomeGroup

True / False

Circle T if the statement is true or F if the statement is false.

- **T** | **F** 1. If full control is assigned to a parent object for a user, the full control permission will overwrite explicit permissions at a child object.
- **T F 2.** When calculating the NTFS and share permissions, you would apply the more restrictive permissions between the NTFS and shared permission.
- $\mathbf{T} \mid \mathbf{F} \mid \mathbf{3}$. When mapping a drive, you specify the UNC.
- T F 4. Full Control NTFS permissions override the Deny permission.
- **T F 5.** When using thin provisioning, you install some of the disks when you begin and then install additional drives when you start running out of disks.

Case Projects

Scenario 2-1: Configuring Collaboration

You are an administrator for the Contoso Corporation, which has approximately 300 users and consists of a corporate office with several sites. In addition, several mobile users who work from home and those need to easily collaborate on projects no matter where they are working. The primary documents are Microsoft Office documents. Describe how you can accommodate this situation for the Contoso Corporation.

Scenario 2-2: Creating a Large Volume

You have a new desktop running Windows 10. However, you try to copy your file repository and find out that you do not have enough disk space. You have 400 GB of free disk space on your C drive and you have 3 smaller 500 GB drives. Describe how to use these disks to create a larger disk.

Scenario 2-3: Sharing a Folder

You are working on a company-wide project. To collaborate, you will create a folder for users to access the project files. The team will consist of several users from each department. Some users will have Read access while other users need to create and modify documents. Describe how to manage this folder.

Scenario 2-4: Managing Printers

You are an administrator for the Contoso Corporation and you administer several sites. These sites have a file server and several shared printers. You need to make sure that the manager at each site can delete print jobs that get stuck or are having problems while allow users to manage their own print jobs. Describe how to configure the printers for this scenario.

Understanding Device Security

LESSON

3

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Understanding the Differences Between the Internet, an Intranet, and an Extranet • Defining LANs, MANs, and WANs • Defining Private and Public Networks • Defining Different Types of Networks • Understanding Firewalls • Understanding the Cloud	Describe the differences between the Internet, an intranet, and an extranet	3.1
 Understanding User Authentication Authenticating with What You Know Authenticating with What You Own or Possess Authenticating with What You Are Using Windows Rights Management Services (Windows RMS) 	Describe user authentication	3.2
Understanding PermissionsConfiguring NTFS PermissionsSetting Share Permissions	Describe permissions	3.3
 Understanding Malware Understanding Malware Identifying Malware Developing Antivirus and Antimalware Strategies 	Describe malware	3.4

KEY TERMS		
accounting	Azure Rights Management	authorization
Active Directory Domain	(Azure RMS)	backdoor
Services (AD DS)	advanced permissions	basic permissions
Active Directory permissions	adware	biometrics
Active Directory Rights	auditing	brute force attacks
Management Services (AD RMS)	authentication	buffer overflow

demilitarized zone (DMZ) denial of service (DoS) dictionary attack digital certificate End User License extranet File Classification Infrastructure firewalls Internet internet Internet Engineering Task Force (IETF) internetwork intranet Local Area Networks (LANs)	malicious software (malware) Metropolitan Area Networks (MANs) Multi-Factor Authentication (MFA) network Network Address Translation (NAT) Nonrepudiation NTFS permissions password perimeter network permissions personal identification number (PIN) private network public network	registry permissions rights rootkit security token share permissions smart card spyware Trojan horse virus Web 2.0 Wide Area Networks (WANs) Windows Defender Windows Rights Management Services (Windows RMS) World Wide Web (WWW) worm
--	---	---

You work as an administrator for the Contoso Corporation and you need to control who can access what on your network. In addition, you need to protect the confidential information of the company. Therefore, you decide to use a multi-layered approach when planning out the corporate security, including establishing firewalls to defining rights and permissions to installing antivirus software packages.

Understanding the Differences Between the Internet, an Intranet, and an Extranet

THE BOTTOM LINE

A *network* is comprised of two or more computers connected together to share resources such as files or a printer. For a network to function, it requires a network service to share and access a common media or pathway to connect the computers. To bring it all together, protocols give the entire system common communication rules.

CERTIFICATION READY

Describe the differences between the Internet, an intranet, and an extranet 3.1 Networks can be categorized as follows:

- LANs, MANs, or WANs
- Public networks or private networks
- Internet, intranets, or extranets

Defining LANs, MANs, and WANs

Data networks come in two major categories, with a third category sometimes being used to describe a network ranging in size between the first category and the second category. The two main categories are called Wide Area Networks and Local Area Networks. These networks are generally referred to as WANs and LANs respectively. A *Wide Area Network (WAN)* is a very large network that can stretch across large geographical areas. The biggest WAN in existence is the Internet, but networks that connect several cities, states, nations, counties, and so on also qualify as WANs. Many companies use WANs in offices or buildings in widely dispersed areas to keep all the facilities and employees connected to each other. A WAN of this nature is sometimes called an enterprise network.

Whereas a WAN can spread across very large geographic areas, *Local Area Networks (LANs)*, as their name implies, are limited to a local area. LANs are usually limited to just one building, or at most, several buildings that are near one another. Sometimes LANs are limited to only certain rooms in a given building. The technologies used by LANs and WANs, while similar, are slightly different from each other.

Networks that are larger than LANs, but are slightly too small to be considered WANs, are sometimes called *Metropolitan Area Networks (MANs)*. MANs are networks that are generally no more than about 50 kilometers across. MANs are used to link together areas—from the size of a college campus to the size of cities—into a single data network that can be either privately owned by a company or publicly owned by a municipality. Some cities have set up MANs as public utilities so that local businesses and individuals can link computers and LANs together to share various network services provided by the city to individuals and companies that are linked to the MAN. MANs and WANs generally use the same technologies, although newer WAN technologies generally find their way into MANs before they spread out to the larger WANs. It is cheaper and easier to upgrade MANs than it is WANs, so MANs are upgraded more often.

Defining Private and Public Networks

A *public network* is a network that is not owned by any one person, company, or organization and anyone can connect to it. The best-known example of a public network is the Internet. A private network is owned by a person, company, or organization and access is restricted. Examples of a private network include a corporate network or a school network.

A private network consists of network links to which the person, company, or organization has exclusive access. In other words, the person, company, or organization has dedicated links. Of course, since the links are dedicated, they are much more expensive than public networks. Since public networks are shared by multiple users, companies, and organizations, public networks are less expensive than private networks.

Defining the Different Types of Networks

Networks can also be organized according to Internet, intranet, or extranet. You can think of the Internet as the external network and the intranet as the internal network. The extranet is a computer network that allows controlled access from outside of an organization's intranet.

An *intranet* is a private computer network or single website that an organization implements in order to share data with employees around the world. User authentication is necessary before a person can access the information in an intranet; ideally, this keeps the general public out, as long as the intranet is properly secured.

Generally, a company refers to its intranet as its private website, or perhaps the portion of the company website that is private. However, intranets use all of the inherent technologies characteristic of the Internet. For instance, within an intranet, TCP/IP protocols such as HTTP and FTP and email protocols like POP3 and SMTP are all employed just the same way

as they are on the Internet. Again, the only difference is an intranet is a privatized version of the Internet, and any company can have one.

An *internet* (also known as an *internetwork*) is connecting a computer network with other networks to form a larger network by using gateways to provide a common method of routing information packets between the networks. The best-known example of an internet is the Internet, which is associated with the World Wide Web.

The *Internet* is the largest public WAN in the world. It is a public domain available to everyone in the United States, and it is available to most other countries as well. The Internet is a worldwide system of connected computer networks. Computers that connect to the Internet use the TCP/IP protocol suite. It is estimated that there currently are over 3 billion Internet users, although it is difficult to estimate this due to Network Address Translation (NAT)—discussed later in this section—and other similar services. The origins of the Internet can be traced back to ARPANET, which was developed by the United States government for security purposes; however, ARPANET was a disjointed group of networks using outmoded or non-uniform protocols. By using TCP/IP to join different types of networks together, the true Internet was created.

The Internet is not controlled by any one governing body—except for two technical aspects. First, the IP classification system is defined by the IANA (Internet Assigned Numbers Authority). Second, DNS is defined by the *Internet Engineering Task Force (IETF)*. Otherwise, the Internet is "controlled" by various ISPs and network providers depending on the location. These companies define how the Internet is accessed.

Companies use the Internet for many reasons, including:

- To transmit messages, such as email
- To gather information, often through the use of web pages
- To share information, often through the use of a web server
- For e-commerce
- To collaborate with other companies, organizations, and users

Individuals use the Internet for these reasons as well as for social networking, shopping, file sharing, gaming, and other multimedia use.

Though the World Wide Web is a big part of the Internet, it is not the entire Internet. However, users quite often use the terms interchangeably. Technically, the Internet is the entire data communications system that connects the world, including hardware and software. Meanwhile, the *World Wide Web (WWW)* is an enormous system of interlinked hypertext documents that can be accessed with a web browser. The World Wide Web Consortium defines standards for how these documents are created and interlinked. Currently, the World Wide Web is in a stage known as *Web 2.0* (with Web 3.0 just now getting underway). Web 2.0 is an interactive type of web experience compared to the previous version 1.0. Web 2.0 allows users to interact with each other and act as contributors to Web sites as well. Currently, when most people access the Internet, they do so through a web browser, but there are many other tools that can also be used to access the Internet, including instant messaging programs, FTP clients, third-party media programs, and more.

Intranets and extranets are used by organizations to share data with select individuals. Whereas an intranet is used by an organization to share data with its employees, an extranet is used to share data with sister companies or other partnered organizations.

An *extranet* is similar to an intranet except that it is extended to users outside a company and possibly to entire organizations that are separate from or lateral to the company. For instance, if a company often needs to do business with a specific organization, it might choose to set up an extranet in order to facilitate information sharing. User authentication is still necessary, and an extranet is not open to the general public.

Figure 3-1 illustrates both an intranet and extranet. Users can connect to intranets and extranets by simply logging in to a website or by using a virtual private network (VPN).

X REF

Figure 3-1

Intranet and extranet

VPNs are discussed in Lesson 2 and later in this section.

Network Address Translation (NAT) is a technique used to modify the network address information of a host while traffic is traversing a router or firewall. This technique hides the network information of a private network while still permitting traffic to be transferred across a public network like the Internet.



NAT was originally created as a workaround for IP addressing issues. In the early days of the Internet, when the TCP/IP protocol and related addressing was being developed, the 32-bit addressing scheme (known as IPv4) was considered more than adequate for any potential network growth. Technically, there were 4,294,967,296 unique addresses available using a 32-bit address, and even discounting the reserved ranges, there were still more than 3 billion possible addresses. At the time, that was enough to provide an address for every person on the planet, including children. Unfortunately, the designers of this addressing scheme dramatically underestimated the explosive growth of the Internet, as well as the widespread adoption of TCP/IP in business and home networks—both of which threatened to exhaust the pool of IPv4 IP addresses. Without unique addresses, the Internet would be unable to successfully route TCP/IP traffic. NAT was the resulting solution for maintaining Internet functionality given the limited number of IP addresses available.

Today, one practical use for NAT is that it allows you to use one set of IP addresses on an internal LAN and a second set of IP addresses for an Internet connection. There is a device (usually a router or firewall) located between the two networks that provides NAT services, managing the translation of internal addresses to external addresses. This allows companies to use large numbers of unregistered internal addresses while only needing a fraction of that number of addresses on the Internet, thus conserving the addresses. This permits the reuse of addresses within private networks while ensuring that the addresses used on the Internet remain unique.

VPN (Virtual Private Network) is a technology that uses encrypted tunnels to create secure connections across public networks like the Internet. There are a variety of uses for this technology, but three of the most common are shown in Figure 3-2. VPNs are commonly used by remote users for secure access to the internal network; VPNs create secure network-to-network connections for branch offices or business partner connections. A fourth use of VPNs is to create secure host-to-host connections for additional security and isolation in an internal network. VPNs utilize encryption and authentication to provide confidentiality, integrity, and privacy protection for data.



Understanding Firewalls

Firewalls are used to protect a network from malicious attack and unwanted intrusion. It is the most commonly used security device in an organization's perimeter.

Firewalls are primarily used to protect one network from another. They are often the first line of defense in network security. There are several types of firewalls; some run as software on server computers, some run as a standalone dedicated appliances, and some work as just one function of many on a single device. They are commonly implemented between the LAN and the Internet, as shown in Figure 3-3.



Generally, there will be one firewall, with the network and all devices and computers residing "behind" it. When a device is "behind" the firewall, it is also considered to be "after" the firewall, and if the device is "in front of" the firewall, it is also known as being "before" the firewall. In Figure 3-3, the devices on the LAN, the switch, and the router are behind the firewall. The devices that are on the cloud or Internet are in front of the firewall.

In Figure 3-3, the firewall has a local address of 10.254.254.249, which connects it to the LAN. It also has an Internet address of 87.69.11.124, which allows connectivity for the entire



LAN to the Internet. It also hides the LAN IP addresses. By default, the IP address 87.69.11.124 should be completely shielded. This means that all inbound ports are effectively closed and will not allow incoming traffic, unless a LAN computer initiates a session with another system on the Internet.

Perimeter networks are small networks that usually consist of only a few servers that are accessible from the Internet in some way. Generally, the term perimeter network is synonymous with *demilitarized zone* (or *DMZ*). You should be able to identify a DMZ and its purpose in an organization, as well as know how to implement a basic DMZ.

A *perimeter network* is a small network that is set up separately from a company's private local area network and the Internet. It is called a perimeter network because it is usually on the edge of the LAN, but DMZ has become a much more popular term. The DMZ allows users outside of the company LAN to access specific services located on the DMZ. However, when set up properly, those users are blocked from gaining access to the company LAN. Users on the LAN will quite often connect to the DMZ as well, but without having to worry about outside attackers gaining access to their private LAN. The DMZ might house a switch with servers connected to it that offer web, email, and other services. Two common configurations of a DMZ include:

- **Back-to-back configuration.** This configuration has a DMZ situated in between two firewall devices (see Figure 3-4). An attacker would have to get through two firewalls in order to gain access to the LAN.
- **3-Leg perimeter configuration.** In this configuration, the DMZ is usually attached to a separate connection of the company firewall. So the firewall would have three connections: one to the company LAN, one to the DMZ, and one to the Internet (as shown in Figure 3-5). Once again, this could be done with a firewall appliance. In this configuration, an attacker needs only to break through one firewall to gain access to the LAN. While this is a disadvantage, technologies such as network intrusion detection/ prevention systems can help alleviate most security issues. Also, by having only one firewall, there is less to manage as an administrator.



Understanding the Cloud

In Lesson 1, the cloud was described a way to access information from anywhere at any time. Cloud computing is usually associated with the Internet since most of these services are accessed over the Internet. The cloud allows you to access existing technologies without having a deep knowledge about or expertise of the technologies. Since the cloud often consists of shared resources or technology, the cloud can cut costs and allow users to focus on their core business instead of being impeded by IT obstacles.

The main technology that makes cloud computing possible is virtualization. Virtualization allows a physical computer to run one or multiple virtual devices. Each virtual device can be used to perform specific computing tasks. Each virtual device can be configured to operate as an isolated device or a device that interacts with other virtual devices.

The virtual devices can be quickly created and its resources provisioned, providing a scalable infrastructure. While physical devices often have memory and processing that is not used, virtual devices can be grouped or pooled together to utilize resources (such as processor and memory) more efficiently. As a result, you don't have as many wasted resources, which means you are running fewer physical servers. Since you are using resources more efficiently, and you can install virtual devices quickly results in reduced cost.

Understanding User Authentication



In the world of information security, AAA (authentication, authorization, and accounting) is a leading model for access control. Here, *authentication* is the process of identifying an individual, usually based on a username and password. After a user is authenticated, she can access network resources based on her authorization. *Authorization* is the process of giving individuals access to system objects based on their identities. Finally, *accounting* (also known as *auditing* is the process of keeping track of a user's activity while accessing network resources, including the amount of time spent in the network, the services accessed while there, and the amount of data transferred during each session.

CERTIFICATION READY Describe user authentication 3.2

Nonrepudiation prevents one party from denying the actions it has carried out. If you have established proper authentication, authorization, and accounting, appropriate mechanisms of nonrepudiation should be in place and no user should be able to deny the actions he has carried out while in your organization's system.

Before users can access a computer or a network resource, they will most likely log in to prove they are who they say they are and to see whether they have the required rights and permissions to access the network resources.

Logging in is the process through which you are recognized by a computer system or network so that you can begin a session. A user can authenticate via one or more of the following methods:

- **By using what he or she knows:** For example, by supplying a password or a personal identification number (PIN)
- By using what he or she owns or possesses: For example, by providing a passport, smart card, or an ID card.
- By proving what he or she is: For instance, by supplying biometric factors based on fingerprints, retinal scans, voice input, etc.

When two or more authentication methods are used to authenticate someone, a *Multi-Factor Authentication (MFA)* system is said to be in place. Of course, a system that uses two authentication methods (such as smart cards and passwords) can be referred to as a two-factor authentication system.

Authenticating with What You Know

For both individual computers and entire networks, the most common method of authentication is the password. A *password* is a secret series of characters that enables a user to access a particular file, computer, or program.

USING PASSWORDS

When seeking access to a file, computer, or network, hackers will first attempt to crack passwords by trying obvious possibilities, including the names and birthdays of a user's spouse or children, key words used by the user, or the user's hobbies. If these efforts don't work, most hackers will next attempt *brute force attacks*, which consist of trying as many possible combinations of characters as time and money permit. A subset of the brute force attack is the *dictionary attack*, which attempts all words in one or more dictionaries. Lists of common passwords are also typically tested.

To make a password more secure, you need to choose a word that nobody can guess. Therefore, whatever you choose should be long enough and should be considered a strong or complex password.

Because today's computers are much more powerful than the computers of years past (which are often used to crack passwords), some experts recommend passwords that are at least 14 characters long. However, remembering long passwords can be cumbersome for some people, and these individuals might write their passwords on a piece of paper near their desks. In these situations, you should start looking for other forms of authentication, such as a smart cards or biometrics.

Users should also change their passwords regularly; that way, if a user's password is revealed to someone else, it won't be long until that password is no longer valid. In addition, changing passwords routinely also shortens the amount of time that an individual has to guess your password, because he or she will have to start the entire cracking process all over again once your password is changed.

Microsoft includes password policy settings within group policies so that you can easily enforce standards such as minimum number of characters, minimum level of password complexity, how often users must change their passwords, how often users can reuse passwords, and so on.

Although passwords are the easiest security method to implement and the most popular authentication method, use of passwords also has significant disadvantages, including the likelihood of passwords being stolen, spoofed, and/or forgotten. For example, a hacker might call a company's IT department for support and pretend to be a legitimate user, eventually convincing the department to reset that user's password to whatever he or she requests.

Given such scenarios, it's essential that you establish a secure process to reset all user passwords. For example, you could establish a self-service process in which a user's identity is verified by asking questions and comparing the answers to responses that have been stored previously, such as the person's birthday, the name of her favorite movie, the name of her pet, and so on. However, these can be relatively easily guessed by an attacker, determined though low-effort research, or discovered through social engineering.

Accordingly, when resetting passwords, you must have a method to positively identify the user who is asking for the password change. Also, you should not send new passwords via email because if a user's existing password is compromised, the hacker will likely be able to access the user's email account and obtain the new password as well. To avoid these problems, you could meet face-to-face with the person who is requesting a password change and ask for identification. Unfortunately, with large networks and networks that include multiple sites, this might not be plausible. You could also call back and leave the password on the person's voicemail, indicating he needs to provide a PIN to access it, or you could send the password to the user's manager or administrative assistant. In either case, you should have the user reset the password immediately after he or she logs on.

USING A PERSONAL IDENTIFICATION NUMBER (PIN)

A *personal identification number (PIN)* is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Because they only consist of digits and are relatively short (usually four digits), PINs are used for relatively low-security scenarios, such as gaining access to a system, or in combination with another method of authentication.

Authenticating with What You Own or Possess

A second category of authentication is based on what you own or possess. The most common examples of this type of authentication involve use of digital certificates, smart cards, and security tokens.

A *digital certificate* is an electronic document that contains an identity, such as a user or organization name, along with a corresponding public key. Because a digital certificate is used to prove a person's identity, it can also be used for authentication. You can think of a digital certificate as similar to a driver's license or passport that contains a user's photograph and fingerprint so that there is no doubt who that user is.

A *smart card* is a pocket-sized card with embedded integrated circuits consisting of nonvolatile memory storage components and perhaps dedicated security logic. Nonvolatile memory is memory that does not forget its content when power is discontinued. This kind of memory might contain digital certificates to prove the identity of the person who is carrying the card, and it might also contain permissions and access information. Because smart cards can be stolen, some do not have any markings on them; this makes it difficult for a thief to identify what the card can be used to access. In addition, many organizations require users to supply passwords or PINs in combination with their smart cards.

A *security token* (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token, or key fob) is a physical device that an authorized computer services user is given to ease authentication. Hardware tokens are typically small enough to be carried in a pocket and are often designed to attach to a user's keychain. Some of these security tokens include a USB connector, RFID functions, or Bluetooth wireless interface to enable transfer of a generated key number sequence to a client system. Some security tokens might also include additional technology, such as a static password or digital certificate built into the security token, much like a smart card. Other security tokens might automatically generate a second code that users must input in order to be authenticated.

Authenticating with What You Are

Biometrics is an authentication method that identifies and recognizes users based on physical traits, such as fingerprints, face recognition, iris recognition, retinal scans, and voice recognition. Many mobile computers include a finger scanner, and it is relatively easy to install biometric devices on doors and cabinets to ensure that only authorized users enter secure areas.

To use biometric devices (see Figure 3-6), you must have a biometric reader or scanning device, software that converts the scanned information into digital form and compares match points, and a database that stores the biometric data for comparison.



To launch the biometric system, you will need to set up a station where an administrator enrolls each user; this includes scanning the biometric feature you want to use for authentication. When selecting a biometric method, you should consider its performance, difficulty, reliability, acceptance, and cost. You also need to look at the following characteristics:

- False reject rate (false negative): This is the percentage of authorized users who are incorrectly denied access.
- False accept rate (false positive): This is the percentage of unauthorized users who are incorrectly granted access.

Using Windows Rights Management Services (Windows RMS)

Rights Management Services, also known as *Windows Rights Management Services (Windows RMS)*, provides an extra level of security to documents such as email and Microsoft Office documents by using encryption to limit who can access a document or web page and what can be done with that document or web page. For example, you can determine whether a document or web page can be printed, copied, edited, forwarded, or deleted. RMS helps contain confidential information so that it stays within the organization and helps limit who can access the data.

Enterprise organizations might install an on-premise rights management system known as *Active Directory Rights Management Services (AD RMS)*. For the cloud, Microsoft offers *Azure Rights Management (Azure RMS)*. Azure RMS uses encryption, identity, and authorization policies to help secure your files and email across multiple devices—phones, tablets, and PCs—and can protect inside and outside your organization.

Basic security mechanisms included with Windows are rights and permissions. *Rights* specify what a user or group can do on a system. For example, backup operators can back up files even if the user or group does not have permissions to the file or folder. Rights also define who can shut down or reboot a computer, who can logon to a computer, and so on. Rights are defined using Group Policy Objects (GPOs).

Permissions specify what a user or group can do with an object. For example, NTFS permissions are used to specify who can access and read a file, who can modify a file, who can delete a file, and who can manage the file.

Figure 3-6 Finger scanner Although rights and permissions are powerful tools, they do have their limitations. For example, anyone who can access and read a file protected with NTFS can copy the file to a USB drive or other storage device, email the file, or print the file, allowing a user to easily steal or copy confidential information.

Windows RMS is an information protection technology is used to minimize unauthorized transmission of data or data leakage, specifically with Microsoft products and operating systems, including Exchange, SharePoint, and the Office suite.

To control who can access a file or email, Windows RMS encrypts the file or email. To read the file, the user will need the encryption key to decrypt the file, which is stored in the Windows RMS server. As a user opens or accesses the file, he or she will automatically retrieve the key from the Windows RMS server and open the file. Since Microsoft products are Windows RMS aware, they also help limit what you can do with a document as specified with the rights assigned using rights management.

If someone copies the file to a USB storage device and takes it offsite or emails it to someone else, whoever opens the file needs to access the Windows RMS to retrieve the keys. If the person cannot access the rights management server (for whatever reason) or is not authorized to access the file, he will not get the key and will not be able to open and read its content.

Azure RMS provides the Rights Management capabilities for Office 365 and it can be used with generic protection (*.pfile) files and Protected PDF (.ppdf) files. As a result, it can protect all Office documents and it can protect other documents, such as PDF, TXT, XML, JPG, JPEG, TIFF, GIF, BMP, and more.

It supports Windows, Mac OS, iOS, Android, and Windows Phone. In addition, it supports on-premises services when you deploy the RMS connector on Microsoft Exchange Server, Microsoft SharePoint Server, and Windows Server running *File Classification Infrastructure*. File Classification Infrastructure is used to classify and apply policies to Office documents in a folder.

One advantage that Azure RMS has over Active Directory RMS is that since it is a cloud service, you do not need to configure trusts with other organizations before you can share protected content with those organizations. Windows Management can be activated from the Office 365 admin center or from the Azure Management Portal. Organizations using Office 365 or an Azure AD (AAD) directory can collaborate with each other. Users who do not have Office 365 or are using Azure AD directory can sign up for the free RMS for individual subscription.

When accessing secure documents, the decryption of a document occurs transparently. In addition, when using applications that are aware of Windows RMS, it is quite easy to secure a document (see Figure 3-7) or email. For example, when cloud storage is configured to use Window RMS, any document that gets dropped in the cloud storage is automatically protected. If an application or browser does not support Windows RMS, the user will not be able to open RMS-protected content.

Understanding Permissions



Permissions specify what a user or group can do with an object, such as NTFS files and folders or an Active Directory object. As a user accesses an object, she must be authenticated in order to prove her identity. Then permissions are used to control authorization to the objects.

Figure 3-7

Using Microsoft Word with Windows RMS to restrict access to a document

			test docs - Word		2
(c)			CESCUDEX * WORD		Patrick Regan -
\smile					(5) I
	Info				
	test				
Open	Desktop				
	Protect I	Document		Properties *	
	Control what	t types of changes	people can make to this	Size	0 bytes
Save As	Document -			Pages	1
Drint				Words	0
	Mark as Final			Total Editing Time	0 Minutes
Share	final and make it read-o	cument is		Title	Add a title
	C Franktick Brand		rare that it contains:	Tags	Add a tag
	Password-protect this d	ocument	uthor's name	Comments	Add comments
Close				Related Dates	
	Restrict Editing			Lart Modified	
	can make	inges others		Casted	T-1- 10 10 414
	Restrict Access		Connect to Digital Rights	s Management Servers and get 1	roday, 10:46 Alvi templates
	Grant people access wh	ile removing	2		
Options	their ability to edit, copy	/, or print.		Related People	
	Add a Digital Signature			Author	
	Ensure the integrity of the hy adding an invisible d	he document igital signature		Addior	Patrick Regan
		a			Add an author
				Last Modified By	Not saved yet
					Hot survey yet

CERTIFICATION READY Describe permissions 3.3

Permissions are privileges granted to specific system entities—such as users, groups, or computers—enabling them to perform a task or access a resource. For example, you can grant a specific user permission to read a file while also denying that same user the permissions needed to modify or delete the file.

Windows 10 has several sets of permissions and those permissions operate independently of each other. As an administrator, you should be familiar with the operation of the following four permission systems:

- **Share permissions:** Control access to folders over a network. To access a file over a network, a user must have appropriate share permissions (and appropriate NTFS permissions, if the shared folder is on an NTFS volume).
- **NTFS permissions:** Control access to the files and folders stored on disk volumes formatted with the NTFS file system. To access a file, whether on the local system or over a network, a user must have the appropriate NTFS permissions.
- **Registry permissions:** Control access to specific parts of the Windows registry. An application that modifies registry settings or a user attempting to manually modify the registry must have the appropriate registry permissions.
- Active Directory permissions: Control access to specific parts of an Active Directory Domain Services hierarchy. Although file servers typically do not function as AD DS domain controllers, server administrators might utilize these permissions when servicing computers that are members of a domain.

MORE INFORMATION

Active Directory Domain Services (AD DS) is the Microsoft directory services that is used to locate and manage resources such as computers, users, and printers. AD DS is usually associated with Windows computers. AD DS is also responsible for the user logon process, authentication, authorization, and directory searches.

All of these permission systems operate independently of each other and sometimes combine to provide increased protection to a specific resource. For example, an administrator might grant Ralph the NTFS permissions needed to access a spreadsheet stored on a file server

volume. When Ralph sits down at the file server console and logs on as himself, he will be able to access that spreadsheet. However, when Ralph is working at his own computer, he will not be able to access the spreadsheet until the administrator creates a share containing the file and also grants Ralph the proper share permissions.

таке поте *

While all of these permissions systems are operating all the time, server administrators do not necessarily have to work with them all on a regular basis. In fact, many administrators never have to manually alter a Registry or Active Directory permission. However, many server administrators do work with NTFS and share permissions on a daily basis.

For network users to be able to access a shared folder on an NTFS drive, you must grant them both share permissions and NTFS permissions. As you learned earlier in this lesson, you can grant these permissions as part of the share creation process, but you can also modify the permissions at any time afterwards.

Configuring NTFS Permissions

As discussed in Lesson 2, NTFS permissions allow you to restrict the actions other users can take on files that are stored on an NTFS volume. Permissions can be granted or revoked by the owner of a resource, system administrators, and users with administrative accounts.

Typically when you assign permissions, you will assign them based on basic NTFS permissions. However, when you need more granular control, you can assign permissions based on advanced permissions.

CONFIGURING BASIC NTFS PERMISSIONS

The basic permissions provide preconfigured permission combinations suitable for most common access control chores. When you open the Properties sheet for a system element and look at its Security tab, the NTFS permissions you see are called *basic permissions*. The basic permissions included Full Control, Modify, Read & Execute, Read, and Write. When assigning permissions, you should use the principle of "least privileges" that states that users should have only the privileges they need to perform their required tasks.

\ominus

CHECK AND MANAGE PERMISSIONS FOR A FILE OR FOLDER

GET READY. To check the permissions of a file or folder in Windows 10 perform the following steps.

- 1. In Windows Explorer, right-click a file or folder and choose Properties.
- 2. Click the Security tab.
- 3. In the Group or user names section, click a user name or group.

The permissions for the selected user or group display in the Permissions section (lower portion) of the Properties dialog box. See Figure 3-8.

To change a permission for a user, perform the following steps.

- **4.** With the user selected in the Properties dialog box, click **Edit**. The Permissions dialog box displays.
- **5.** In the Group or user names section, click a user name.

Figure 3-8

Figure 3-9

Changing permissions

Viewing permissions for a file or folder

eneral Security Details Previou	s Versions	
Diject name: C:\Users\patri\Des	dop/TestFolder/	Test.bt.bt
mup or user names.		
SYSTEM		
2 Patrick Regan (patrick_regan 12	23456@hotmail.c	om)
Administrators (WIN10A\Admini	strators)	
o change permissions, click Edit		
e enange permeente, enen zam		Edit
remissions for STSTEM	Allow	Deny
Full control	\checkmark	
Modify	~	
Read & execute	1	
Read	~	
Write	~	
TVILC		
Special permissions		

6. Select and deselect the boxes in the Permissions section to Allow or Deny access (see Figure 3-9).

	auri (Desklob	\lestrolder	\Test.bd.b
C			
Cluest (WIN10A)Gues	H)		
SYSTEM	-y		
2 Patrick Regan (patrick	_regan 12345	6@hotmail	com)
Administrators (WIN10	A\Administrat	ors)	
		da l	Pomou
	F	dd	Remov
Permissions for Guest	F	Allow	Remov
Permissions for Guest	ļ	Allow	Remov Deny
Permissions for Guest Full control Modify	F	Allow	Remov Deny
Permissions for Guest Full control Modify Read & execute	F	Allow	Remov Deny
Permissions for Guest Full control Modify Read & execute Read	-	Allow	Remov Deny
Permissions for Guest Full control Modify Read & execute Read Write	<i>.</i>	Allow	Remov Deny

7. Click **OK** to apply the permissions and close the dialog box.

CONFIGURING ADVANCED NTFS PERMISSIONS

NTFS permissions are designed to be granular, enabling you to grant specific degrees of access to security principals. Basic permissions are actually combinations of *advanced permissions*, which provide the most granular control over the element.

For example, the NTFS permission system has 14 advanced permissions that you can assign to a folder or file. However, there are also six basic permissions, which are various combinations of the 14 advanced permissions. In most cases, administrators work only with basic permissions. Many administrators rarely, if ever, work directly with advanced permissions.

If you do find it necessary to work with advanced permissions directly, Windows makes it possible. When you click the Advanced button on the Security tab of any Properties sheet, an Advanced Security Settings dialog box appears (see Figure 3-10), enabling you to access the ACEs for the selected system element directly. System Manager provides access to the same dialog box through a share's Properties sheet.

110 | Lesson 3

Figure 3-10

The Advanced Security Settings dialog box

Ad	vanced S	Security Settings for Test.txt		- 0	×
Nam	ne:	C:\Users\patri\Desktop\TestFolder\Test.bt.t	xt		
Owr	ner:	Patrick Regan (patrick_regan123456@hotma	ail.com) 🌘 Change		
Per	missions	Auditing Effective Access			
For a Pern	additiona nission e	al information, double-click a permission entry. Intries:	To modify a permissi	on entry, select the entry and click Edit (if available).	
	Туре	Principal	Access	Inherited from	
58	Allow	SYSTEM	Full control	Parent Object	-
2	Allow	Patrick Regan (patrick_regan123456@hotm	Full control	Parent Object	
92	Allow	Administrators (WIN10A\Administrators)	Full control	Parent Object	
	Add	Remove View			
D	isable inl	heritance			
				OK Cancel App	oly

COPYING AND MOVING FILES AND FOLDERS ON AN NTFS VOLUME

In Lesson 2, you learned that NTFS permissions inherit from the parent folder. In other words, permissions typically flow from the parent folder to the child objects. Of course, this can be modified by overwriting permissions at a lower level or by removing the inherited permissions.

However, you need to be aware of what happens when you copy or move files from one place to another place:

- When users copy files and folders, the files and folders inherit permissions of the destination folder.
- When users move files and folders within the same volume, they retain their permissions.
- When users move files and folders to a different volume, they inherit the permissions of the destination folder.

TAKING OWNERSHIP, DELEGATING, AND VIEWING RESULTANT PERMISSIONS

As you study the NTFS permission system, it might occur to you that it seems possible to lock out a file or folder—that is, to assign a combination of permissions that permits access to no one at all, leaving the file or folder inaccessible. In fact, this is true.

When assigning permissions to a folder, by default, the permissions apply to both the folder and the subfolders and files within it. To stop permissions from being inherited, click the Disable inheritance button. When you disable inheritance, you can convert the inherited permissions into explicit permissions, or remove all inherited permissions.

A user with administrative privileges can revoke his own permissions, as well as everyone else's, preventing him from accessing a resource. However, the NTFS permissions system includes a "back door" that prevents these orphaned files and folders from remaining permanently inaccessible.

Every file and folder on an NTFS drive has an owner and the owner always has the ability to modify the permissions for the file or folder, even if the owner has no permissions herself. By default, the owner of a file or folder is the user account that created it. However, any account possessing the Take Ownership special permission (or the Full Control standard permission) can take ownership of the file or folder.

The Administrator user can take ownership of any file or folder, even those from which the previous owner has revoked all of Administrator's permissions, by clicking the Change option for Owner on the Advanced Security Settings dialog box. After the Administrator user has taken ownership of a file or folder, the Administrator user cannot assign ownership

back to the previous owner. This prevents the Administrator account from accessing other users' files undetected.

The other purpose for file and folder ownership is to calculate disk quotas. When you set quotas specifying the maximum amount of disk space particular users can consume, Windows calculates a user's current disk consumption by adding the sizes of all the files and folders that the user owns.

To change the ownership of a file or folder, you must open the Effective Access tab of the Advanced Security Settings dialog box and click the Change link by the Owner setting.

As you learned in Lesson 2, when you calculate effective permissions, you must first calculate the explicit and inherited permissions for an individual or group and then combine them. When combining user and group permissions for NTFS security, the effective permission is the cumulative permission. The only exception is that Deny permissions always apply. To view the effective rights for a user or group, you can open the Advanced Security Settings dialog box by using the Effective permissions tab.

VIEW NTFS EFFECTIVE PERMISSIONS

GET READY. To view the NTFS effective permissions for a file or folder in Windows 10, perform the following steps.

- 1. Right-click the file or folder and choose Properties.
- 2. Click the Security tab.
- 3. Click the Advanced button.
- 4. Click the Effective Access tab.
- 5. Click the Select a user option
- 6. In the Select User, Computer, Service Account, or Group dialog box, type the name of the user or group you want to view. Click **OK**.
- 7. Click the Effective Access tab. See Figure 3-11.
- 8. Click **OK** to close the Advanced Security Settings dialog box and then click **OK** to close the Properties dialog box.

	C:\Users\patri\Des	ktop\TestFolder\Test.txt.txt	
Owner:	Patrick Regan (pati	rick_regan123456@hotmail.com)	Change
Permissions	Auditing	Effective Access	
Effective Acces you can also e group, any gro User/ Group:	ss allows you to view valuate the impact of oup that the intended Administrator (WII	the effective permissions for a us potential additions to the securit group is a member of must be a V10A\Administrator) Select a u	ser, group, or device account. If the account is a member of a dor by token for the account. When you evaluate the impact of addin dded separately. ser
View effecti	ve access		
Effective acce	55	Permission	Access limited by
2		Full control	
*		Traverse folder / execute file	
*		List folder / read data	
		Read attributes	
*			
***		Read extended attributes	
张 张		Read extended attributes Create files / write data	
联 联 威 威		Read extended attributes Create files / write data Create folders / append data	
或或或或或		Read extended attributes Create files / write data Create folders / append data Write attributes	
或或或或或		Read extended attributes Create files / write data Create folders / append data Write attributes Write extended attributes	
纸 纸 纸 纸 纸 纸		Read extended attributes Create files / write data Create folders / append data Write attributes Write extended attributes Delete	
战 威 威 威 威 威 威		Read extended attributes Create files / write data Create folders / append data Write attributes Write extended attributes Delete Read permissions	
成成成成成成成		Read extended attributes Create files / write data Create folders / append data Write attributes Write extended attributes Delete Read permissions Change permissions	

Figure 3-11

Viewing NTFS effective permissions

Setting Share Permissions

In Windows 10 shared folders have their own permission system that is completely independent from the other Windows permission systems.

For network users to access shares on a file server, you must grant them the appropriate share permissions. By default, the Everyone special identity receives the Allow Full Control share permission to any new shares you create.

To modify the share permissions for an existing share using Windows Explorer, open the Properties sheet for the shared folder, click the Sharing tab, and then click Advanced Sharing and Permissions to open the Share Permissions tab. To specify the share permissions, click the Permissions button to open the Permissions dialog box, as shown in Figure 3-12.



nare Permissions		
Group or user names:		
Everyone		
	Add	Pamaua
	Aug	nemove
Permissions for Everyone	Allow	Deny
Full Control		
Change		
Read	\checkmark	

Understanding Malware

THE BOTTOM LINE

Users utilize client computers to connect to servers and network applications. Because these client computers are connected to an organization's network, they must be protected from malware.

CERTIFICATION READY Describe malware 3.4 *Malicious software*, sometimes called *malware*, is software that is designed to infiltrate or affect a computer system without the owner's informed consent. The term "malware" is usually associated with viruses, worms, Trojan horses, spyware, rootkits, and dishonest adware. As a network administrator or computer technician, you need to know how to identify malware, how to remove it, and how to protect a computer from it.

Understanding Malware

By understanding the types of malware, you will gain a better understanding of how malware might cause problems with your computer and how a computer might receive malware.

Because it is now quite common for computers to be connected to the Internet, there are more opportunities than ever before for your organization's computers to be infected by malware. Indeed, over the past few years, a staggering amount of malware has been produced. As a security professional, you are responsible for protecting your organization's computers against

infection. Furthermore, when a computer on your network does get infected by malware, you must make sure this infection does not spread to other computers.

Many early forms of malware were written as experiments or pranks. In most instances, they were intended to be harmless or merely annoying. However, as time passed, malware increasingly became a tool for vandalism or for compromising private information. Today, malware can even be used to launch *denial of service (DoS)* attacks against other systems, networks, or websites, causing those systems to have performance problems or become inaccessible. For example, a DoS attack might send thousands of packets in a short period of time that overwhelm the network equipment or server.

As previously mentioned, malware can be organized into several categories:

- Viruses
- Worms
- Trojan horses
- Spyware and dishonest adware
- Rootkits
- Backdoors

A computer *virus* is a program that can copy itself and infect a computer without the user's consent or knowledge. Early viruses were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file (for example, a filename with an .exe or .com extension). Later, as macro languages began to be used in software applications (such as word processors and spreadsheet programs), virus creators seized upon this technology, embedding malicious macros in documents of various types. Unfortunately, because macro code is automatically executed when a document is opened, these documents can infect other files and cause a wide range of problems on affected computer systems. Today, websites also pose a virus threat because they can be written in various programming and scripting languages and might include executable programs. Therefore, whenever you access the Internet, your system is under constant threat of infection.

A *worm* is a self-replicating program that copies itself to other computers on a network without any user intervention. Unlike a virus, a worm does not corrupt or modify files on the target computer. Instead, it consumes bandwidth and processor and memory resources, slowing the system down or causing it to be unusable. Worms usually spread via security holes in operating systems or TCP/IP software implementations.

Trojan horses derive their name from the Trojan horse story in Greek mythology. In short, a *Trojan horse* is an executable program that appears as a desirable or useful program. Because it appears to be desirable or useful, users are tricked into loading and executing the program on their systems. After the program is loaded, it might cause a user's computer to become unusable or it might bypass the user's system security, allowing his private information (including passwords, credit card numbers, or his Social Security number) to be accessible by an outside party. In some cases, a Trojan horse might even execute adware.

Spyware is a type of malware that is installed on a computer to collect a user's personal information or details about her browsing habits, often without the user's knowledge. Spyware can also install additional software, redirect your web browser to other sites, or change your home page. One example of spyware is the keylogger, which records every key a user presses. When a keylogger is installed on your system, whenever you type credit card numbers, Social Security numbers, or passwords, that information is recorded and eventually sent to or read by someone without your knowledge. (It should be noted that not all keyloggers are bad, however, as some corporations use them to monitor their corporate users.)

Adware is any software package that automatically plays, displays, or downloads advertisements to a computer after the software is installed or while the application is being used. Although adware might not necessarily be bad, it is often used with ill intent.

A *rootkit* is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel, or less commonly, libraries or applications.

A *backdoor* is a program that gives someone remote, unauthorized control of a system or initiates an unauthorized task. Some backdoors are installed by viruses or other forms of malware. Other backdoors might be created by programs on commercial applications or with a customized application made for an organization.

Viruses and worms often exploit what is known as a *buffer overflow*. In all application programs, including Windows itself, there are buffers that hold data. These buffers have a fixed size. If too much data is sent to these buffers, a buffer overflow occurs. Depending on the data sent to the overflow, a hacker might be able to use the overflow to send passwords to himself, alter system files, install backdoors, or cause errors on a computer. When patches are released to fix a potential buffer overflow, the patch adds code to check the length of data sent to the buffer to make sure that it does not overflow.

Identifying Malware

The first step in removing malware is detecting that you have it. Sometimes it is easy to see that you are infected with malware. Other times, you might never know that you have it.

Some common symptoms of malware include the following:

- Poor system performance
- Unusually low levels of available memory
- · Poor performance while connected to the Internet
- Decreased response rates
- Longer start-up times
- Instances in which your browser closes unexpectedly or stops responding
- · Changes in your browser's default home or default search pages
- Unexpected pop-up advertising windows
- · Addition of unexpected toolbars to your browser
- · Instances in which unexpected programs automatically start
- Inability to start a program
- Malfunctions in Windows components or other programs
- Missing programs or files
- Unusual messages or displays on your monitor
- Unusual sounds or music played at random times
- · Creation and/or installation of unknown programs or files
- Appearance of unknown browser add-ins
- Corrupted files
- Unexpected changes in file sizes

Of course, to see these symptoms, you might need to actively look for them. For example, when your Windows machine becomes slow, you might start Task Manager to view processor and memory utilization. You could then look at the ongoing processes to see which process is using the greatest amount of processor and memory resources. You might also review the processes and services in memory (again, you can use Task Manager). In addition, you could use the System Configuration. Of course, to be able to determine which processes and services are rogue, you need to have a baseline of what processes and services are currently

running on your healthy system for comparison purposes. Finally, to detect malware, you should use an up-to-date antivirus program and an up-to-date antispyware package, which together can scan your entire system and look for malware in real time as you open files and access websites.

With the many tools attackers can now use to deliver malware, it is easy to see the importance of protecting your computer from all types of malware threats. Of course, when protecting yourself, a little common sense can go a long way. For example, you should not open documents or executable files from unknown or untrusted sources and you should be cautious before providing any personal information, including username and passwords.

Developing Antivirus and Antimalware Strategies

Protecting your system from viruses and other malware is not a simple solution. To prevent the exploitations of security holes, you need to keep your system up to-date with Windows updates and other application software updates. In addition, you should use a reputable antivirus software.

Some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or some other software package. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes.

The second step in protecting your computer from malware is to use an up-to-date antivirus software package. In addition, if your antivirus software does not include an antispyware component, you should install an antispyware software package. Then, you should be sure to perform a full system scan with your antivirus software at least once a week.

Windows Defender (as shown in Figure 3-13) is included with Windows 10 and is intended to prevent, remove, and quarantine viruses, spyware, and other malicious software. This program helps protect your computer against pop-ups, slow performance, and security threats caused by malware. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it to scan for malware when your computer isn't working properly, when you've clicked a suspicious link online, or in an email message. Of course, as with any antivirus package, you must keep Windows Defender up to date.



To avoid malware, it's also important to use common sense. Therefore, you should always follow these steps:

- 1. Don't install unknown software or software from an nonreputable source.
- 2. Don't open strange email attachments.
- 3. Don't click on hyperlinks from unknown people when you don't know what the links are supposed to do. This applies not just to hyperlinks sent via email but to hyperlinks sent using instant messaging services.
- 4. If your email client supports auto launch, turn it off. Otherwise, you might automatically activate a computer virus just by opening an email.
- 5. Don't visit questionable websites, especially porn sites or sites that allow you to download pirated software, music, or video.
- 6. If your web browser alerts you that a particular site is known for hosting malware, heed this warning.
- 7. When surfing the Internet, if you encounter browser pop-ups that tell you that you need to download the newest driver or check your system for viruses, proceed with caution.
- 8. Don't forget to perform regular backups. That way, if you get a virus and lose any data, you can restore your system from your backup.

SUMMARY SKILL MATRIX

IN THIS LESSON YOU LEARNED:

- Networks can also be broken into an Internet, intranet, or extranet. You can think of the Internet as the external network and the intranet as the internal network. The extranet is a computer network that allows controlled access from outside of an organization's intranet.
- The Internet is the largest public WAN in the world. It is a public domain available to everyone in the United States and it is available to most other countries as well. The Internet is a worldwide system of connected computer networks. Computers that connect to the Internet use the TCP/IP protocol suite.
- Firewalls are primarily used to protect one network from another. They are often the first line of defense in network security.
- Authentication is the process of identifying an individual, usually based on a username and password. After a user is authenticated, she can access network resources based on her authorization. It includes what you know, what you own or possess, and what you are.
- Permissions specify what a user or group can do with an object, such as NTFS files and folders or an Active Directory object. As a user accesses an object, she will have to be authenticated to prove who she is. Then permissions are used to control authorization to the objects.
- Malicious software, sometimes called malware, is software that is designed to infiltrate or affect a computer system without the owner's informed consent. The term "malware" is usually associated with viruses, worms, Trojan horses, spyware, rootkits, and dishonest adware.
- To prevent the exploitations of security holes, you need to keep your system up to-date with the Windows and other application software updates. In addition, you should use a reputable antivirus software.

Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

- 1. A network zone that allows remote access for employees of your company is known as a(n) ______.
- 2. The ______ is an enormous system of interlinked hypertext documents.
- 3. The type of attack that uses an extensive list of potential passwords is known as a(n)
- **4.** A(n) ______ is a numeric password shared between a user and a system that can be used to authenticate the user to the system.
- 5. A device that can provide you with a second password to log in to a system is a(n)
- 6. _____ permissions flow from a parent object to a child object.
- 7. A(n) ______ defines the type of access over an object or the properties of an object, such as an NTFS file or printer.
- 8. _____ is software that is designed to infiltrate or infect a computer, usually with ill intent.
- **9.** A(n) ______ is a self-replicating program that copies itself to other computers while consuming network resources.
- **10.** Microsoft's antispyware program is called ______.

Multiple Choice

Circle the letter that corresponds to the best answer.

- 1. Your manager asks you to set up an area that is not on the LAN but not quite on the Internet. This area will house servers that will serve requests to users connecting to your intranet. Which type of zone does your manager want you to set up?
 - a. DMZ
 - **b.** extranet
 - c. FTP
 - d. VPN
- 2. You have been tasked with setting up an authentication server on a DMZ that will allow only users from a partner company. Which kind of network are you configuring?
 - a. Internet
 - **b.** Intranet
 - **c.** Extranet
 - d. World Wide Web
- Which of the following are common types of password attacks? (Choose all that apply)
 a. Dictionary
 - **b.** Worm
 - **c.** Rootkit
 - **d.** Spyware
 - **e.** Brute force

- 4. Which of the following is *not* a method for authentication?
 - **a.** Something the user knows
 - **b.** Something the user owns or possesses
 - c. Encryption
 - **d.** Something the user is
- 5. Which of the following is *not* a biometric device?
 - a. Password readers
 - **b.** Retinal scanners
 - c. Fingerprint scanners
 - **d.** Face scanners
- 6. Which of the following file systems offers the best security?
 - a. FAT
 - **b.** FAT32
 - c. NTFS
 - **d.** EFS
- 7. Which NTFS permission is needed to change attributes and permissions?
 - a. Full Control
 - **b.** Modify
 - **c.** Read and Execute
 - **d.** Write
- 8. Which type of permission is granted directly to a file or folder?
 - a. Explicit
 - **b.** Inherited
 - **c.** Effective
 - **d.** Share
- 9. Which of the following uses an ACL? (Choose all that apply)
 - a. NTFS folder
 - **b.** Active Directory user
 - c. Registry key
 - d. Login rights
- **10.** Which type of malware copies itself onto other computers without the owner's consent and will often delete or corrupt files?
 - a. Virus
 - **b.** Worm
 - **c.** Trojan horse
 - **d.** Spyware
- **11.** Which type of malware collects personal information or browsing history, often without the user's knowledge?
 - a. Virus
 - **b.** Worm
 - c. Trojan horse
 - **d.** Spyware
- **12.** Your computer seems to be slow and you notice that you have a different default web page than usual. Which of the following is the most likely the cause of problems?
 - a. Your ISP has slowed your network connection.
 - **b.** Your computer has been infected with malware.
 - c. You did not update your computer.
 - d. You did not lock your default home page.

- 13. Besides installing an antivirus software package, you should always ______ to protect your computer against malware.
 - **a.** keep your machine up to date with the latest security patches
 - **b.** reboot your computer on a regular basis
 - c. allow only one user to use your computer
 - d. spoof your IP address
- **14.** Which technique is used to modify the network address information of a host while traffic is traversing a router or firewall?
 - **a.** brute force
 - **b.** multifactor authentication
 - c. Network Address Translation
 - d. Nonrepudiation
- 15. Which of the following is the largest public WAN in the world?
 - a. DMZ
 - **b.** intranet
 - **c.** extranet
 - **d.** Internet

Case Projects

Scenario 3-1: Dealing with Viruses

You are an administrator with the Contoso Corporation and you have recently received reports that user computers are infected with viruses and other forms of malware. You are concerned that personal or confidential information could have been compromised. Describe how to protect computers from malware in the future.

Scenario 3-2: Understanding the Disadvantages of Biometrics

You are an administrator with the Contoso Corporation and your CIO wants you to investigate the possible use of biometrics for security purposes. The CIO understands what biometrics are and how this technology can be used, but he does not understand the potential disadvantages of using biometrics. Describe your response.

Scenario 3-3: Changing Passwords

You are an administrator with the Contoso Corporation and a user tells you that he just received a message on his computer indicating that he must change his password. He wants to know why he must use such a relatively long password and why he must change that password on a regular basis. Describe your response.

Scenario 3-4: Setting Up a DMZ

A client wants you to set up a DMZ with two servers. Each server will service a different set of users:

- 1. Server 1 services employees who work from home.
- 2. Server 2 services two partner companies.

Which types of network zones will enable this functionality?



LESSON

Understanding Cloud Services

OBJECTIVE DOMAIN MATRIX

Technology Skill	OBJECTIVE DOMAIN DESCRIPTION	Objective Domain Number
Understanding the Types of Cloud Services	Describe the types of cloud services	4.1
 Understanding Microsoft Intune Understanding Microsoft Intune Capabilities Deploying the Microsoft Intune Client Reviewing Microsoft Intune Administrator Roles Managing User and Computer Groups Managing Microsoft Intune Policies Supporting Mobile Device Management Using Microsoft Intune 	Describe Microsoft Intune	4.2
 Understanding Microsoft Azure Understanding Virtual Machines Understanding Azure Services Understanding Disaster Recovery, High Availability, Redundancy, and Fault Tolerance 	Describe Microsoft Azure	4.3

KEY TERMS		
Azure Active Directory (Azure AD/AAD) cloud services Communication as a Service (CaaS) communications services criteria membership	Desktop as a Service (DaaS) direct membership disaster recovery (DR) hosted private cloud hybrid cloud hypervisor	Infrastructure as a Service (IaaS) Microsoft Azure Microsoft Azure Fabric Controller (FC) Microsoft Azure Site Recovery Microsoft Intune

Mobile Device Management	Software as a Service (SaaS)	Microsoft Intune Cloud +
(MDM)	storage services	On-Premise Configuration
Monitoring as a Service (MaaS)	System Center 2012 R2/2016	Microsoft Intune Groups
Network as a Service (NaaS)	Virtual Machine Manager	Microsoft Intune Service
Platform as a Service (PaaS)	(VMM)	Administrator
private cloud	virtual machines (VMs)	Microsoft Intune Stand-Alone
productivity services	Microsoft Intune + System	Cloud Configuration
public cloud	Center Configuration	Microsoft Intune Tenant
search services	Manager	Administrator

You are an administrator for the Contoso Corporation. Your network infrastructure has grown steadily over the last few years and is close to reaching certain limits, so you are considering the cloud as a solution to expanding the corporation's network infrastructure.

Understanding the Types of Cloud Services



The cloud is a network of servers and each server performs a different function (such as web services, databases, or authentication). Some servers run applications and others deliver services. By using the cloud, you don't have to have the individual application or services running on the user's computers. In addition, the cloud allows you to share resources and technology so that they can be accessed by multiple users. From the standpoint of users, the cloud is simply a black box that the user accesses. However, users are not concerned with what happens inside the black box. With regard to cloud services, an organization signs up for cloud services and the cloud service is provided without concerns about how those services are provided.

CERTIFICATION READY Describe the types of cloud services 4.1 Public cloud services provide a way to access information from anywhere at any time. Microsoft defines a *public cloud* as a web-based service that is hosted outside of your organization. This means the information technology infrastructure (hardware, servers, software, and so on) is located somewhere other than your office and is managed by a third party (such as hosted). If you use mobile banking—accessing web-based email or storing your photos online in one of the many services provided—you are interacting with "the cloud."

Using public cloud services such as OneDrive and Office 365 enable you to take advantage of hosted solutions. This means users have the ability to access their information from anywhere at any time across multiple devices. By using cloud-based services, your users can collaborate via calendars, email, and through document sharing. From an administrative perspective, it means you gain access to services and programs without the additional overhead of maintenance and software upgrades.

A *private cloud* offers the same features and benefits of the public cloud, but is contained within the corporate network and is controlled by the corporate IT department. The private cloud offers higher security and privacy and allows for more control of its resources and data.

A *hosted private cloud* is provided by a third-party company but is accessible only by users within a specific organization. In other words, the resources are leased or owned by the organization but are managed and located away from the organization. However, the hosted

private cloud tends to be cheaper than the private cloud because some of the cost for the building, power, and personnel is consolidated amount several companies.

A *hybrid cloud* is a cloud-computing environment in which the organization will manage some of the resources in-house and a third-party organization will provide the cloud resources externally. In other words, a hybrid cloud utilizes both a public cloud and a private cloud.

When looking at the cloud, you should know the following terms:

- *Communication as a Service (CaaS)*: Allows the deployment of communications services through cloud computing without the need to purchase their own equipment. It can include Voice over IP (VoIP), VPN services, and business telephone service that you would find on a private branch exchange (PBX) such as phone menus and voice mails.
- *Desktop as a Service (DaaS)*: Provides a desktop or work environment to run applications, access emails, or back up data.
- *Infrastructure as a Service (IaaS)*: Provides the infrastructure that the cloud runs on, such as servers, switches, routers, storage area networks, firewalls, and other equipment.
- *Monitoring as a Service (MaaS)*: Allows you to monitor software applications so that the correct personnel are notified when it is down or not fully performing as needed.
- *Network as a Service (NaaS)*: Offers network services such as network infrastructure/IaaS and communication services/CaaS.
- *Platform as a Service (PaaS)*: Allows you to buy, develop, test, deploy, and manage software applications so that the applications can be accessed by users.
- **Software as a Service (SaaS):** Allows the development and provisioning of software for users, including providing servers on which the software runs on. Typically, the SaaS runs on demand through the remote desktop services or through a web browser. Often, the cloud provider owns the software licenses and charges a fee to the subscribers.

The cloud can provide the following services:

- *Productivity services:* Allow users to work and collaborate. An example of productivity services is Office 365, which allows users to create and share documents.
- *Storage services*: Provides a storage platform for data. By storing data on the cloud, the data can be accessed by any user or device. An example of storage services is Azure Storage.
- **Communications services:** Provides communication between users. Examples of communications services include Exchange Online and Skype for Business Online. Exchange Online provides email, calendar, and contact sharing; Skype for Business Online provides instance messaging, PC-to-PC audio and video calls, and screen sharing.
- *Search services*: Provides search functionality into custom applications. In addition, it can provide a search engine and storage of data that can be accessed on an Application Programming Interface (API). An example of search services is Azure Search.

Understanding Microsoft Intune



Microsoft Intune, formerly called Windows Intune, is a cloud-based management solution that allows you to manage your computers when they are not inside your corporate network. Microsoft Intune helps you manage your computers and mobile devices through a web console. It provides the tools, reports, and licenses to ensure your computers are always current and protected. For mobile devices, it also allows you to manage your remote workforce by working through Exchange ActiveSync or directly through Microsoft Intune.

CERTIFICATION READY Describe Microsoft Intune 4.2

Microsoft Intune can be operated in cloud-only mode or in a new unified configuration option that integrates the cloud-based environment with System Center 2012 Configuration Manager Service Pack 1 or higher or System Center 2012 R2/2016 Configuration Manager. Microsoft Intune utilizes a subscription model in which you are charged on a per-user basis.

Understanding Microsoft Intune Capabilities

When you use Microsoft Azure, you are leasing cloud resources provided by Microsoft. The Microsoft Azure resources can be self-contained in the cloud (such as when you want to have websites with databases) or you can extend your organization's data center to the cloud by using IaaS. By using IaaS, you can run applications in the cloud while maintaining full control over the virtual machines themselves.

Microsoft Azure includes the following features:

- Websites with support for ASP.NET, PHP, Node.js, or Python that can be deployed using FTP, Git, Mercurial, or Team Foundation Server
- Virtual machines that run both Windows Server and Linux virtual machines
- Cloud services including Microsoft's platform as a service (PaaS) environment that are used to create scalable applications and services
- Data management using SQL Database (formerly known as SQL Azure Database) that can integrate with Active Directory, Microsoft System Center, and Hadoop
- Media services that use PaaS to provide encoding, content protection, streaming, and/or analytics

Here are some of the things you can do with this cloud-based management solution:

- Manage your mobile devices and computers through a web-based console anywhere at any time through Exchange ActiveSync and System Center 2012 R2/2016 Configuration Manager.
- Manage your Microsoft Intune subscription, add new users and security groups, set up and manage service settings, and access service status via a Microsoft Intune Account portal.
- Assess the overall health of devices across your organization using the Microsoft Intune Administration console.
- Organize users and devices into groups (geographically, by department, and by hardware characteristics).
- Manage updates for computers in your organization.
- Enhance security of your managed devices by providing real-time protection, by keeping virus definitions current, and by automatically running scheduled scans.
- Access the overall health of your managed devices through the use of alerts.
- Deploy policies to secure data on mobile devices to determine which mobile devices can connect, enroll, rename, and un-enroll devices.
- Wipe mobile devices in case they are stolen.
- Deploy software and detect and manage software installed on computers.
- Manage licenses purchased through Microsoft volume Licensing agreements.
- Run reports on software, hardware, and software licenses to help confirm current needs and to plan for the future.
- Provide a cloud-based, self-service portal where users can enroll and manage their devices, search for and install software applications, and request help.

Microsoft Intune deploys a client agent on each device that you want to manage. The Microsoft Intune agent communicates back to the Microsoft Intune administration console, allowing you to inventory software and hardware assets in your organization.

Microsoft Intune can be deployed with the following configurations:

- *Microsoft Intune Stand-Alone Cloud Configuration:* With this configuration, you have to administer your computers and devices (Windows 10, Windows 8/8.1, Windows RT, Windows Phone 8, and Apple iOS) through the Administrator console. Although this configuration allows you to create and manage policies, inventory your devices, and upload and publish software, it does not support the discovery of mobile devices.
- *Microsoft Intune Cloud* + *On-Premise Configuration*: This configuration integrates Microsoft Intune with your existing Active Directory and Exchange environment. With this configuration, you can discover mobile devices using Exchange ActiveSync, synchronize your user accounts with your Active Directory, and manage your mobile devices through Microsoft Intune.
- *Microsoft Intune* + *Configuration Manager*: This configuration allows you to manage your computers and mobile devices from the Configuration Manager console.

SIGN UP FOR MICROSOFT INTUNE

GET READY. To sign up for Microsoft Intune, perform the following steps.

- 1. On the Start screen, click Internet Explorer.
- 2. Go to http://www.microsoft.com/en-us/windows/windowsintune/try.aspx.
- 3. Click the Try tab and then click Sign up for a free Microsoft Intune.
- **4.** On the signup page, type the following information:

Country or Region: <Your country or region>

Organization language: <Your language>

First Name: <Your first name>

Last Name: <Your last name>

Organization: <Your last name> Corporation

Address: <Your street address>

City: <Your city>

State: <Your state>

Zip code: <Your zip code>

Phone number: <Your phone number>

Email address: <Your email address>

5. In the New domain name text box, type the following:

<FirstName><LastName>Training<Month><Year>

Therefore, if your name is John Smith and you are performing this lab in June 2016, you would type the following:

JohnSmithTraining062016 in front of .onmicrosoft.com

- 6. Click Check availability.
- **7.** In the New user ID text box, type your first initial and last name. Therefore, if your name is John Smith, type JSmith.
- 8. For the Create new password text box and the Confirm new password text box, type Pa\$\$wOrd.
- **9.** In the Verification text box, type the code displayed.

- 10. Click I accept and continue.
- 11. Click Continue.
- **12.** If a Microsoft Intune login screen appears, in the Password text box, type **Pa\$\$wOrd** and then click **Sign in**.
- 13. If a Don't lose access to your account displays, click Remind me later.
- **14.** On the Microsoft Intune Admin Overview screen, in the menu bar just below the webpage address, click **Admin Console**.
- 15. If a message appears, indicating the application requires Microsoft Silverlight, click Get Microsoft Silverlight. When you are prompted to run or save Silverlight_x64.exe, click Run. If the User Account Control dialog box displays, click Yes.
- **16.** In the Install Silverlight dialog box, click **Install now**. When you are prompted to enable Microsoft Update, click **Next**. Click **Close**.
- 17. If you are prompted to log in, type **Pa\$\$wOrd** in the Password text box.

When done, the Admin Console should open as shown in Figure 4-1. The left side of the screen includes vertical tabs including the dashboard, groups, alerts, software, policy, reports and Admin.



Deploying the Microsoft Intune Client

You can install the Microsoft Intune client on computers running Windows XP Professional (SP3), Windows Vista (Enterprise, Ultimate, or Business Edition), Windows 7 (Enterprise, Ultimate, or Professional), Windows 8/8.1 (Professional and Enterprise), and Windows 10. You can deploy the Microsoft Intune client on both physical computers and virtual machines. Before installing the Microsoft Intune client, you need to consider how you want to handle malware. If you have existing software that protects against these types of threats, Microsoft Intune Endpoint Protection detects the software and does not install the Endpoint component.

The following options are available for deploying the client:

- Administrator Deployment: Using this option, you basically download the client software and manually install it on the target computers. You can automate the process by using Group Policy if you need to install it on a large number of computers.
- User-Initiated Enrollment for Computers: Using this option, users can self-enroll their computers through the Microsoft Intune company portal.
- Install the client software as part of an image: Using this option, you can deploy the Microsoft Intune client as part of a system image deployment. The computer is automatically enrolled when the image is installed.

PERFORM AN ADMINISTRATOR DEPLOYMENT OF THE MICROSOFT INTUNE CLIENT

GET READY. You need to agree to and set up a Microsoft Intune account to complete this exercise. To complete an administrative deployment of the Microsoft Intune client on a Windows 10 computer, perform the following steps.

- 1. Log in to the Windows 10 computer on which you want to install the Microsoft Intune Client software.
- 2. Open Internet Explorer, type https://admin.manage.microsoft.com into the address field and then press Enter.
- 3. If the message This application requires Microsoft Silverlight appears, click Get Microsoft Silverlight and then select Run.
- 4. To accept the licensing agreement, click Install now.
- On the Enable Microsoft Update page, click Next.
- 6. In the Microsoft Intune console's left pane, click Admin.



Figure 4-2

Viewing the Admin console

- 7. Click Client Software Download.
- 8. On the Client Software Download page, click **Download Client Software** (see Figure 4-3).



- 9. From the Windows Internet Explorer box, click Save as.
- In the Save As box, click **Desktop** and then click **Save**. This places a file named Windows_Intune_Setup.zip on your desktop.
- 11. Minimize the Microsoft Intune console, right-click the Windows_Intune_Setup.zip file and choose Extract All.
- 12. In the Select a Destination and Extract Files box, click Extract. After the extraction has completed, you should see two files: Windows_Intune_Setup.exe and WindowsIntune.accountcert. These files must be kept together at all times. The WindowsIntune.accountcert is used by the setup program.
- 13. Double-click Windows_Intune_Setup.exe. If you are prompted to open the Microsoft _Intune_Setup.zip, click Open. When the zip files open, double-click the Microsoft_ Intune_Setup application.
- 14. When the Microsoft Intune Setup Wizard opens, click Next.
- **15.** Click **Finish**. Microsoft Intune continues to update and install software on the computer. You can use the computer while the process continues in the background.
- Maximize the Microsoft Intune console and then click in the left pane. When the pane slides out, click Groups > All Devices. When the installation is done, you should see the computer name listed (see Figure 4-4).

Figure 4-3

Downloading Microsoft Intune client software

Figure 4-4

Viewing the computer as it appears in the Microsoft Intune Administration console



MORE INFORMATION

After the installation has completed, the protection and update agents continue to perform additional setup and configuration steps. This includes downloading the required malware definitions and any other agent updates. The computer should appear in the Microsoft Intune Administration console in a few minutes, but it can take up to 30 minutes to complete the inventory and status updates process.

In the previous exercise, you performed an Administrative deployment, and the Windows 10 computer was enrolled as part of the installation. If you wanted to allow your users to selfenroll their computers, they would need to be an administrator on the local computer, connect to the Microsoft Intune portal using an Internet Explorer browser, and use a Microsoft Online ID. To learn more about how self-enroll works, visit Microsoft.com and search for Microsoft Intune User-Initiated Enrollment for Computers. When performing this process, perform the following general steps:

- 1. Click All My Devices.
- 2. Click Enroll your computer.
- 3. Click Download Software.
- 4. Click Run.
- 5. Click Next to. To start the Microsoft Intune Setup Wizard, click Next.
- 6. When the installation is completed, click Finish.

Reviewing Microsoft Intune Administrator Roles

Microsoft Intune supports two types of administrator roles: Microsoft Intune Tenant Administrator and Microsoft Intune Service Administrator. Although both can gain access to the Microsoft Intune Administration console, they do differ in the tasks they can execute.
Descriptions of the two administrator roles are as follows:

- *Microsoft Intune Tenant Administrator* role: Has full control and rights regarding the Administrator console. They can add or delete service administrator accounts and assign other tenant administrators. The person who sets up Microsoft Intune and accepts the Microsoft Online Subscription Agreement when it is purchased is assigned this role. You should create at least one more person with this role as a backup. You assign Window Tenant Administrators via the Microsoft Intune account portal at https://admin.manage.microsoft.com.
- *Microsoft Intune Service Administrator* role: Has full access to the Microsoft Intune Administration console and can perform all operations including adding or deleting another Services Administrator account. They cannot modify data in the console but instead can only view the data it contains and run reports. Microsoft Intune Service Administrators are assigned via the Microsoft Intune Administrator console at https://admin.manage.microsoft.com.

Managing User and Computer Groups

To make the process of deploying Microsoft Intune policies, software packages, and software updates more efficient, consider using Microsoft Intune Groups. *Microsoft Intune Groups*, which are used to quickly organize and manage your computers and users, are created and managed in the Groups workspace. These groups apply only to Microsoft Intune and are completely separate from Active Directory groups, although you can use AD security groups as part of a query to select members when creating a group. After your groups are set up, you can deploy Microsoft Intune policies, software packages, and software updates to them.

You can create groups that include users and you can create groups that include devices. What you cannot do is include users and devices in the same group. Most administrators create groups that are organized in one or more of the following ways:

 Geographical organization: 	Portland, Seattle, Los Angeles
• Departmental organization:	Executives, Human Resources, Marketing
Physical organization:	Desktops, Laptops

In the Groups workspace, you see the default groups created for devices and for users when Microsoft Intune is initially setup. For example, you will find the Windows 10 computer you installed the Microsoft Intune Client software on earlier, under the All Computers group.

After a closer look, you should see there is a hierarchy for the groups. For example, the All Direct Managed Devices and the All Exchange ActiveSync Managed Devices are child groups under the parent All Mobile Devices. You can deploy software updates, policies, and software applications to multiple groups or to a parent group while excluding one or more child groups. You can also add and exclude specific group members.

MORE INFORMATION

To protect your production environment, consider creating a test computer group that can be used to roll out and trial new updates. Once in place, you can select the members from within the Microsoft Intune console. This should be reflective of the different operating systems you want to test on. Even though computers are added to the new group, they still retain their membership in any other groups. This allows you to still assign updates to them without impacting other computers in those groups. When setting up a group in Microsoft Intune, you have the option to manually or dynamically add users or devices to a group. You can also take a mixed approach and use both methods when creating a group.

- *Direct membership*: The process of manually adding users or devices from within the Microsoft Intune console. You manually include and exclude specific members from the group.
- *Criteria membership:* This involves defining certain types of criteria that Microsoft Intune runs a query against to find users or devices. When it finds users or computers that match the criteria, it dynamically adds them as members to the group. The group automatically updates with members as changes occur.
- Mixed: A group that consists of members added manually and dynamically.

When adding devices to a group using membership criteria, you have the following options to include or exclude members from the parent group (see Figure 4-5):

- Computers from organizational units you specify
- Computers from domains you specify

d: try			Previous Next 🛛 🍠 Options 🕶	
	Grou	ıps	Groups Oversion	Search devices
SHBOARD	Overv	🖬 Create Group		×
	🔺 All Us	Specify the criteria that deter	nine which members of the parent group will be included in this gro	oup.
GROUPS	U	General	Define Membership Criteria	
	All De	General	Parent Group:	
2	D AL	Criteria Membership	All Devices	
	Δι	Direct Membership	Device type:	
*		Direct Hembership	computer	
OTECTION		Summary	Start group membership with:	
			Empty group 🔻	
0			Include or evolute members from the parent group using	the following criteria:
ALERTS			Include of exclude members from the parent group using	and following encenter
0			Include all computers from these organizational units:	Exclude all computers from these organizational units:
OFTWARE			Browse	Browse
			Numerous Cod	
			None specified	None specified
ICENSES				
E.			Include all computers from these domains:	Exclude all computers from these domains:
E POLICY			Browse	Browse
POLICY				
			None specified	None specified
REPORTS				
0.1				
10				< Previous Next > Einish Cancel
ADMIN				< Previous Next > Tillisit Calleet

When defining direct membership, you have the option to include or exclude specific members form groups you specify.

Group membership is recursive. This means that if you use a dynamic membership query and set the criteria that a user is a member of an AD DS security group named marketing to be included in the group, you can pick up additional indirect users in the query. For example, if Mary is a member of the Marketing Interns security group and the Marketing Interns security group is a member of the Marketing security group, then she is included in your query and added to the Marketing group.

Figure 4-5

Defining membership criteria

CREATE A DEVICE GROUP USING DIRECT MEMBERSHIP

GET READY. To create a device group using Direct-based membership, from the Microsoft Intune Administrator console, perform the following steps.

- Log in to the Microsoft Intune Administrator console at https://admin.manage. microsoft.com.
- 2. In the left pane, select the Groups.
- **3.** Click **Tasks > Create Group**.
- **4.** In the Group name field, type **My Test Group**.
- 5. In the Description field, type Computers used to test deployments of new updates.
- 6. Under the Select a parent group, click All Devices.
- 7. Click Next.
- 8. On the Define Membership Criteria page, click Next.
- **9.** On the Define Direct Membership screen, click **Browse**. Be careful to select the Browse button that is just to the right of the Include specific members field. If you select the one on the far right, you will exclude specific members.
- 10. Choose the Windows 10 computer you installed the Microsoft Intune client software on in the earlier exercise and then click Add. Your Windows 10 computer should appear in the Include specific members column. Click OK to continue.
- 11. On the Define Direct Membership page, click Next.
- **12.** Review the General Criteria Membership and Direct Membership summary page and then click **Finish**.
- **13.** Under Groups, click **My Test Group** and then click **Devices**. The computer should appear as a member of the group.

Managing Microsoft Intune Policies

To help control the security settings on mobile devices, computer updates, Endpoint Protection, firewall settings, and the end-user experience, Microsoft Intune has policies. These policies apply to domain-joined computers in any domain and to non-domain joined computers.

Since Group Policy can be used to set many of the same settings, when you deploy Microsoft Intune client software and establish Microsoft Intune policies, you need to ensure that the clients do not receive GPOs with similar and/or conflicting settings.

SET UP THE DEFAULT MICROSOFT INTUNE POLICIES

GET READY. To set up the default Microsoft Intune Policies, perform the following steps.

- 1. Open the Microsoft Intune Administration console.
- 2. In the workspace shortcuts pane, click the Policy icon.
- 3. Under Tasks, click Add Policy.
- **4.** In the Create a New Policy dialog box (as shown in Figure), the following policy templates are displayed in the list of templates in the left pane:
 - Mobile Device Security Policy
 - Windows Firewall Settings
 - Microsoft Intune Agent Settings
 - Microsoft Intune Center Settings

132 | Lesson 4

Figure 4-6

policy

Create a New Policy Adding a Microsoft Intune Select a template for the new policy Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy and then you can configure the settings in that policy. You cannot change a template. ▷ Android ⊳ iOS Select a policy template from these ▲ Windows categories to manage settings on your managed computers, mobile devices, and for Custom Configuration (Windows 10 Desktop and Mobile and later) software that you deploy using Microsoft Custom Configuration (Windows Phone 8.1 and later) Intune Email Profile (Windows Phone 8 and later) General Configuration (Windows 8.1 and later) General Configuration (Windows Phone 8.1 and later) PKCS #12 (.PFX) Certificate Profile (Windows 10 Desktop and Mobile SCEP Certificate Profile (Windows 8.1 and later) SCEP Certificate Profile (Windows Phone 8.1 and later) Trusted Certificate Profile (Windows 8.1 and later) Tructed Certificate Drofile (Mindows Dhone & 1 and later

5. Select the policy template you wish to set up and click **Create and Deploy a Policy** with the Recommended Settings. To view the settings before you create the policy, click View the recommended settings for this policy template that will be used as the default for this policy.

Create Policy Cancel

- **6.** After you configure the settings that you want to apply in your default policy, type a name and an optional description for the policy and then click Save Policy.
- 7. When prompted to specify whether you want to deploy the policy now, click Yes.
- 8. In the Select the groups to which you want to deploy this policy dialog box, select the All Devices group or All Users group (depending on the policy you have selected) and click **OK**.
- **9.** Repeat these steps as needed for your other default policy settings.

Supporting Mobile Device Management Using Microsoft Intune

Microsoft Intune provides comprehensive Mobile Device Management (MDM) for mobile devices. With Microsoft Intune, you can deploy polices to secure mobile devices, perform a hardware inventory on devices, distribute applications to devices, or wipe mobile devices. In addition, MDM can report a device's compliance to Azure Active Directory (Azure AD or AAD), so that Azure AD can provide the device with access to corporate resources or applications that are secured by Azure AD.

With Microsoft Intune, you can manage mobile devices directly or through Exchange ActiveSync. Exchange devices can be managed using on-premises servers and hosted Microsoft Office 365 Exchange services in the cloud. If Configuration Manager is deployed in your environment, you can use the Microsoft Intune service to manage mobile devices while performing all management tasks in the System Center Configuration Manager console.

Microsoft Intune can manage Windows Phone 10 devices, Windows Phone 8/8.1 devices, iOS devices, and Android devices. To enroll Windows devices, you must deploy the Windows Phone 10/8.1/8 company portal app to the devices. The company portal app, which can be downloaded from Microsoft's Download Center, must be code-signed with a certificate that is trusted by Windows Phone 10/8.1/8 devices.

To enroll iOS devices, you need to obtain an Apple Push notification service certificate that enables Microsoft Intune to securely communicate with the Apple Push Notification service. To obtain an Apple Push Notification, you must download the Certificate Signing Request from Microsoft Intune and then request an Apple Push Notification service certificate from the Apple website.

To enroll Android devices, you must download the Android company portal app from Google Play. This application will let you enroll Android devices for direct management.

To enroll devices, you will need to perform the following steps:

- 1. Set the Mobile Device Management Authority for Microsoft Intune.
- 2. Set up direct management for mobile devices.
- 3. Provision users for device enrollment.
- 4. Enroll devices.

SET THE MOBILE DEVICE MANAGEMENT AUTHORITY

GET READY. To set the Mobile Device Management Authority, perform the following steps.

- 1. Open the Microsoft Intune administrator console.
- 2. In the workspace shortcuts pane, click the Admin icon.
- **3.** In the navigation pane, click **Mobile Device Management**. The Mobile Device Management page appears (see Figure 4-7).



- **4.** In the main pane on the right of the page, click **Set Mobile Device Management Authority**.
- 5. The Set MDM Authority dialog box appears. You cannot change this selection at a later time. Therefore, if you will use the Microsoft Intune console to manage mobile devices in the future, check the box and click Yes if you want to use Microsoft Intune to manage mobile devices.

Figure 4-7

Opening the Mobile Device Management page

SET UP DIRECT MANAGEMENT FOR MOBILE DEVICES

GET READY. To set up direct management of Windows Phone 8/8.1 devices, perform the following steps.

- 1. Open the Microsoft Intune administrator console.
- 2. In the workspace shortcuts pane, click the Admin icon.
- **3.** In the navigation pane, under Mobile Device Management, click **Windows Phone**. Figure 4-8 shows the Windows Phone Mobile Device Management Setup page.

- 0 ×

Figure 4-8

Setting up Windows Phone Mobile Device Management

ind: try	Pres	rious Next 🖉 Options 🔻	
crosoft Intur	he	Help Sign Ou	it Welcome Regan Corporatio
GROUPS	Administration Overview Updates Alerts and Notifications > Alert Types Recipients Notification Rules 4 Administrator Management	Windows Phone Mobile Device Management Setup Step 1: Enrollment Server Address Either specify a verified domain name (such as contors.com), or tell your users to manually enter manage.microsoft.com as the server name during enrollment. Learn more about setting your DNS server for enrollment Test Auto-Detection	Learn About Windows Phone Mobile Devi Setup Getting a Symantec code-sig Device Enrollment Evaluating Company Portal
ALERTS	Administrators Service Administrators Tenant Administrators Device Enrollment Managers Client Software Download Storage Use Mobile Device Management Windows	Step 2: Obtain an Enterprise ID and Code Signing certificate (Optional) Windows Phone 8: To be able to manage Windows Phone 8 devices you must get a code signing certificate from Symantec. Windows Phone 8.1: You can enroll and manage Windows Phone 8.1 devices without a code signing certificate. However without a code signing certificate you will not be able to sideload apps.	
	Hildone inclue Hildone inclue Microsoft Exchange Multi-factor Authentication NDES Connector Company Portal	Step 3: Download and sign the Company Portal app Windows Phone 8: Download the Company Portal app installation file and sign it with your Symantec code-signing certificate. Download the Company Portal app installation file Windows Phone 8.1:	
ADMIN	ĺ	Install the Company Portal app from the Windows Phone Store. Step 4: Upload and deploy the signed Company Portal app Windows Phone 8:	

- **4.** Under Step 1: Enrollment Server Address, type the name of the verified domain and then click **Test Auto-Detection**.
- Scroll down to Step 5: Upload and Deploy the Company Portal and click Upload Signed App File. To open the Microsoft Intune Software Publisher Wizard. Click Next.
- **6.** On the Software setup page for the Specify the location of the software setup files option, click the **Browse** button to browse to the signed Windows Phone 8 company portal app that you generated when you completed the prerequisites.
- **7.** Under the Code-signing certification option, click the **Browse** button to browse to the code-signing certificate (.pfx) file. In the Certificate password text box, type a password for the certificate. Click **Next**.
- 8. On the Software description page, complete the fields (Publisher, Name, and Description). These fields will be seen by the users on their devices. You will also specify an URL for software information and specify a category. Click **Next**.
- 9. On the Summary page, click Upload.
- **10.** When the software is uploaded, click **Close**. The company portal can now be automatically deployed to all users who enroll.

Before users are able to enroll their devices, users must be members of a Microsoft Intune user group. When you provision users, you define device owners as managed users in Microsoft Intune.

PROVISION USERS FOR DEVICE ENROLLMENT

GET READY. To add users manually to the Microsoft Intune account portal, perform the following steps.

- 1. Open the Microsoft Intune account portal.
- 2. In the header, click Admin.
- 3. In the left pane, under Management, click Users.
- 4. On the Users page, click New > User.
- On the Details page, complete the user information. Click the arrow next to Additional details to add optional user information (such as job title or department) and then click Next.
- 6. On the Settings page, if you want the user to have an administrator role, select **Yes** and then select an administrator role from the list.
- 7. Under Set user location, select the user's work location and then click Next.
- **8.** On the Group page, under Microsoft Intune user group, ensure that the name of the user is selected.
- **9.** On the Send results in email page, select **Send email.** In the Send email text box, you can add as many as 5 email addresses, separated by semicolons; the user name and temporary password would be sent to these email addresses. Click **Create**.
- On the Results page, the new user name and a temporary password is displayed. After you review the results, click Finish.

To enroll Windows 10/8.1/8 devices, log in to the Intune portal and click Add Device. During this process, users will provide their credentials. After a certificate is installed on the device, the user must select Install company app or Hub, so that the device can be managed by Intune.

UNDERSTANDING SELECTIVE WIPE

Since mobile devices can carry sensitive information, and have a chance of being lost or stolen as compared to desktop computers, Microsoft Intune allows you to selective wipe, full wipe, remote lock, and passcode reset mobile devices. If the mobile device is lost or stolen, an administrator can issue a remote device wipe command from the Microsoft Intune administrator console or the user can issue a remote device wipe commands from the Microsoft Intune company portal.

A full wipe will restore the device to its factory defaults for Windows Phone, iOS, and Android devices. A select wipe removes only company data.



PERFORM A SELECTIVE WIPE

GET READY. To add users manually to the Microsoft Intune account portal, perform the following steps.

- 1. Open the Microsoft Intune account portal.
- 2. In the Microsoft Intune administration console, click Groups > All Users.
- Click the name of the user whose mobile device you want to wipe, and then click View Properties.
- On the properties page for the user, click the Devices tab, and then click the name of the mobile device that you want to wipe.
- 5. Click Retire/Wipe.
- 6. A message appears (as shown in Figure 4-9), prompting you to confirm if you want to retire the device.
 - a. To perform a selective wipe, which only removes company content, click Yes.
 - **b.** To perform a factory reset on a device, select **Wipe the device before retiring**. This action applies to all platforms except Windows 10/8.1.

Figure 4-9

Wiping a device



UNDERSTANDING LOCATION SETTINGS

To manage user in you will open the Admin Console, and under Management, click Users. The Details tab allows you to change names, titles, department, phone number, addresses, and country or region. When you click the Settings tab, you can assign role, set the sign-in status, or configure the user location, as shown in Figure 4-10.

- 8 ×

Figure 4-10

Configuring the user location

X Find: try	Previous Next 🖉 Options 🔻	
Regan Corporation Dashboard Setup	Patrick Regan Details Settings Group Some settings are unavailable. You cannot edit your own security settings.	
Overview Management	Assign role Do you want this user to have administrator permissions? Learn more about administrator roles	
Security Groups Domains	No Ves	
Subscriptions Manage Licenses Purchase Software	Global administrator Alternate email address This email address is used for important notifications and self service password reset. Learn more about lost password recovery patrick_regan@hotmail.com	
Support Overview Service Requests Service Health	Set sign-in status Allowed User can sign in and access services. Blocked User cannot sign in or access services. 	
	Set user location	
	The services available vary by location. Learn more about licensing restrictions * Required	
	United States	
	Save Cancel	
Microsoft ©2015 Microsoft Leg	al Privacy Community	Feedback

Understanding Microsoft Azure



Microsoft Azure (formerly known as Microsoft Azure) is a cloud-computing platform used for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters. Although Microsoft Azure has its own web-based tools, you can also use System Center 2012 R2/2016 Virtual Machine Manager (VMM) and App Controller.

CERTIFICATION READY Describe Microsoft Azure 4.3 Microsoft Azure includes the following features:

- Websites with support for ASP.NET, PHP, Node.js, or Python that can be deployed using FTP, Git, Mercurial, or Team Foundation Server
- Virtual machines that run both Windows Server and Linux virtual machines
- Cloud services including Microsoft's platform as a service (PaaS) environment that are used to create scalable applications and services
- Data management using SQL Database (formerly known as SQL Azure Database) that can integrate with Active Directory, Microsoft System Center, and Hadoop
- Media services that use PaaS to provide encoding, content protection, streaming, and/or analytics

When you use Microsoft Azure, you lease cloud resources provided by Microsoft. The Microsoft Azure resources can be self-contained in the cloud (such as when you want to have websites with databases), or you can extend your organization's data center to the cloud by using IaaS. By using IaaS, you can run applications in the cloud while maintaining full control over the virtual machines themselves.

As a virtual environment, you can create multiple virtual machines by deploying the Windows Server 2012 R2/2016 operating system on the Hyper-V host or cloud service that it runs under. You can also upload a Windows Server 2012 R2/2016 image template VHD file or a Windows Server 2012 R2/2016 preconfigured image VHD file. You can then use the cloud tools to manage the hosted virtual machines.

Microsoft provides several tools to deploy and manage servers running Windows Server 2012 R2/2016 on public and private clouds:

- System Center 2012 R2/2016 Virtual Machine Manager (VMM)
- Microsoft Azure virtual machine (VM) tools such as Azure Management Portal
- System Center 2012 R2/2016 App Controller
- Remote Desktop Connection

Virtual Machine Manager (VMM) provides a single administrative tool for deploying virtual servers and managing a virtualization infrastructure, including hosts, virtual machines, storage, networks, and libraries. You can also use VMM to update virtual servers.

The Microsoft Azure web portal includes multiple tools for creating and managing virtual machines that are hosted on the Microsoft Azure cloud platform. With these tools, you can create VMs, attach disks, upload a Windows Server VHD file, load balance virtual machines, and manage availability of virtual machines.

The App Controller application allows administrators to deploy and manage services across the Microsoft private cloud services and the Microsoft public cloud services, such as Microsoft Azure. App Controller has a web-based interface that enables administrators to manage services rather than servers.

Understanding Virtual Machines

Virtualization has become quite popular during the last few years. By using virtual machine technology, you can run multiple operating systems concurrently on a single machine, which allows separation of services while keeping cost to a minimum. It can also be used to create Windows test systems in a safe, self-contained environment. Microsoft Hyper-V is a hypervisor-based virtualization system for x64 computers starting with Windows Server 2008. The *hypervisor* is installed between the hardware and the operating system and is the main component that manages the virtual computers.

Server virtualization in Windows Server 2012 R2/2016 is based on a module called a hypervisor. Sometimes called a *System Center 2012 R2/2016 Virtual Machine Manager (VMM)*, the hypervisor is responsible for abstracting the computer's physical hardware and creating multiple virtualized hardware environments, called *virtual machines (VMs)*. Each VM has its own (virtual) hardware configuration and can run a separate copy of an operating system. Therefore, with sufficient physical hardware and the correct licensing, a single computer running Windows Server 2012 R2/2016 with the Hyper-V role installed can support multiple VMs, which you can manage as though they were standalone computers.

To run several virtual machines on a single computer, you need to have sufficient processing power and memory to handle the load. However, since most servers often sit idle, virtualization utilizes the server's hardware more efficiently.

To keep each virtual server secure and reliable, each server is placed in its own partition. A partition is a logical unit of storage in which operating systems execute. Each virtual machine accesses the hypervisor, which handles interrupts to the processor and redirects them to the respective partition.

By using Hyper-V Manager, you can create new virtual machines and define the hardware resources that the system should allocate to them. In the settings for a particular virtual machine, depending on the physical hardware available in the computer and the limitations of the guest operating system, you can specify the number of processors and the amount of memory a virtual machine should use, install virtual network adapters, and create virtual disks using various technologies, including storage area networks (SANs).

By default, Hyper-V stores the files that make up virtual machines in the folders you specified on the Default Stores page during installation. Each virtual machine uses the following files:

- A virtual machine configuration (.vmc) file in XML format that contains the virtual machine configuration information, including all settings for the virtual machine
- One or more virtual hard disk (.vhd or .vhdx) files to store the guest operating system, applications, and data for the virtual machine

A virtual machine may also use a saved-state (.vsv) file, if the machine has been placed into a saved state.

Understanding Azure Services

Microsoft Azure has a wide range of services that you can tap into. The popular services include Cloud Services, SQL database, Storage, Virtual Machines, and Websites.

By providing the following services, Azure be customized to fulfill the needs of virtually any organization:

- *Azure Active Directory (Azure AD)*: Provides identity management and access control capabilities for your cloud applications. It can be synchronized with the on-premises domain controllers. You can also enable single sign-on to simplify user access to cloud applications.
- API Management: Allows you to publish APIs to developers, partners and employees securely.
- **Application Insights:** Can be used to detect issues, solve problems, and continuously improve your web applications by providing real time, information including availability, performance and usage.
- Automation: Allows you to automate the creation, deployment, monitoring, and maintenance of resources in your Azure environment using a highly scalable and reliable workflow execution engine.
- Azure Active Directory (Azure AD or AAD): Provides identity management and access control capabilities for your cloud applications. It can be synchronized with the onpremises domain controllers. You can also enable Single Sign-On (SSO) to simplify user access to cloud applications and support conditional access.
- Azure Rights Management: Used to protect confidential or sensitive information by using encryption, identity, and authorization policies.
- **Backup:** Allows you to back up to and restore from the cloud using familiar tools in Windows Server 2012/Windows Server 2012 R2 or System Center 2012 R2 Data Protection Manager.
- **Batch:** Allows you to run large-scale parallel and High Performance Computing (HPC) workloads in Azure.
- **BizTalk Services:** Provides Business-to-Business (B2B) and Enterprise Application Integration (EAI) capabilities for delivering cloud and hybrid integration solutions.
- **CDN:** Short for Content Delivery Network, allows you to deliver high-bandwidth content to end-users around the world with low latency and high availability via a robust network of global data centers.
- Cloud Services: Allows you to move or extend your corporate infrastructure to the cloud.
- **Data Factory:** Produces trusted information from raw data in cloud or on-premises sources. It can create, orchestrate and schedule high-available, fault tolerant work flows of data movement and transformation activities. It can also monitor all your data pipelines and service health.
- **DocumentDB:** A fully-managed NoSQL document database service that offers query and transactions over schema-free data, predictable and reliable performance, and rapid development.
- **Event Hubs:** Enables elastic scale telemetry and event ingestion with durable buffering and sub-second end to end latency for millions of devices and events.
- **ExpressRoute:** Enables you to create private connections between Azure datacenters and infrastructure at your premises or in a colocation environment.
- **HDInsight:** A Hadoop-based service that brings an Apache Hadoop solution to the cloud. It is typically used to manage Big Data on a cloud-based data platform that manages data of any type and any size.
- Key Vault: Offers an easy, cost-effective way to safeguard keys and other secrets in the cloud using Hardware Security Modules (HSMs).
- **Machine Learning:** Allows you to easily design, test, operationalize and manage predictive analytics solutions in the cloud.
- Managed Cache: Used to create a cache that will increase access to applications and data.
- **Media Services:** Offer cloud-based media solutions from many existing technologies including ingest, encoding, format conversion, content protection and both on-demand and live streaming capabilities.

- **Mobile Services:** Provides a scalable cloud backend for building Windows Store, Windows Phone, Apple iOS, Android, and HTML/JavaScript applications. It can be used to store data in the cloud, authenticate users, and send push notifications to your application within minutes.
- **Multi-Factor Authentication:** By having more than one method of authentication, you can helps prevent unauthorized access to on-premises and cloud applications.
- Notification Hubs: Allows a scalable, cross-platform push notification infrastructure that can be used for broadcast push notifications to millions of users at once or tailor notifications to individual users.
- **Operational Insights:** Enables you to collect, correlate and visualize all your machine data such as event logs, network logs, performance data from on premise and cloud assets.
- Redis Cache: A popular open source cache for your Azure applications.
- **RemoteApp:** RemoteApp helps employees stay productive anywhere, on a variety of devices Windows, Mac OS X, iOS, or Android.
- Scheduler: Allows you to invoke actions that call HTTP/S endpoints or post messages to a storage queue on any schedule.
- Azure Search: A fully-managed service for adding sophisticated search capabilities to web and mobile applications.
- Service Bus: A messaging infrastructure that sits between applications.
- **Site Recovery:** Provides a simple, cost effective disaster recover that can replicate and if needed recover resources in the private cloud.
- **SQL Database:** A relational database service that enables you to rapidly create, extend, and scale relational applications into the cloud.
- Storage: Offers non-relational data storage including Blob, Table, Queue and Drive storage.
- **StorSimple:** Offers a unique hybrid cloud storage solution which provides primary storage, archive and disaster recovery.
- **Stream Analytics:** An event processing engine that helps uncover insights from devices, sensors, cloud infrastructure, and existing data properties in real-time.
- **Traffic Manager:** Allows you to load balance incoming traffic across multiple hosted Azure services whether they're running in the same datacenter or across different datacenters around the world.
- Virtual Machines: Enable you to deploy a Windows Server or Linux image in the cloud.
- **Virtual Network:** Enables you to create Virtual Private Networks (VPNs) within Azure and securely link these with on-premises network.
- **Visual Studio Online:** A cloud-based Application Lifecycle Management (ALM) solution that provides a hosted code repos and issue tracking to load testing and automated builds. Visual Studio Online is licensed separately from Azure Services.
- **Websites:** Enables you to deploy web applications on a scalable and reliable cloud infrastructure.

Understanding Disaster Recovery, High Availability, Redundancy, and Fault Tolerance

Microsoft Azure has a wide range of tools that provide high availability, redundancy and fault tolerance, to keep your cloud components running 24/7 and provide wide range of tools to recover from a disaster.

When deploying any application or service, you need to look at availability, the amount of time the applications and service can be accessed and that are working properly. The effective availability of your cloud service is also affected by the various SLA of the other dependent services.

For example, Azure provides the following Service Level Agreements (SLAs):

- Compute: 99.95 percent, which allows 21.6 minutes of downtime per month.
- **SQL Database:** 99.90 percent, which allows for 43.2 minutes of downtime per month.
- Storage: 99.90 percent, which allows for 43.2 minutes of downtime per month

If any of these go down, an application will go down. When you combine all of the SLAs (99.95%×99.90%×99.90%), you are left with 99.65%, which gives you 108 minutes down-time per month. To provide high availability, Microsoft Azure provides the Azure Business Continuity Technical Guidance, which can be found by searching the Microsoft website.

The *Microsoft Azure Fabric Controller (FC)* is responsible for provisioning and monitoring the condition of the Azure compute instances. When it checks the status of the hardware and software of the host and guest machine instances, and it detects a failure, it will automatically relocate the VM instances.

To provide redundancy to your application, it is recommended that you group two or more virtual machines in an Availability Set. By using an availability set, two VMs that provide the same service will be hosted on two different physical host so that if one physical host goes down, the other VM is not affected. As a result, Availability Sets provide redundancy including when you are performing maintenance, or when one of the hosts go down.

A *disaster recovery (DR)* site is a backup site that is used to relocate services when the primary data center faces a disaster (such as a fire, a flood, an earthquake, or a terrorist attack). The DR site is usually located away from the primary data center to ensure that the same disaster does not take both data centers down. The data center can by hosted by the organization, or contacted via a third-party company that specializes in disaster recovery services.

Microsoft Azure Site Recovery is a software component used to orchestrate protection for virtual machines that are located on on-premises Hyper-V host servers located in the VMM cloud. With Microsoft Azure Site Recovery, you can configure:

- **On-premises to on-premises protection:** Replicates on-premise virtual machines to another on-premise site.
- **On-premises to Azure protection:** Replicates on-premise virtual machines to Azure by configuring and enabling protection settings in Azure Site Recovery vaults. Virtual machine data replicates from an on-premises Hyper-V server to Azure storage.

Microsoft Azure Site Recovery can be used to replicate a large number of virtual machines between the primary site and a disaster recovery site. By using the Microsoft Azure cloud and the Recovery Manager service, you can access all of the components necessary to orchestrate the failover of virtual machines in one data center to another, even when one of the data center sites is unresponsive.

Recovery Manager has the following requirements:

- System Center 2012 R2/2016 VMM or VMM 2012 SP1 with cumulative update 3
- Windows Server 2012 with latest updates or Windows Server 2012 R2/2016

To configure Azure Site Recovery, perform the following steps:

- 1. Create an Azure Site Recovery vault, including specifying a vault key.
- 2. Install the Site Recovery agent on the VMM servers that you want to register in the vault.
- 3. Specify protection settings for the cloud, including source and target settings, recovery points and snapshots, and initial replication settings.
- 4. Create mappings between VM networks on source and destination VMM servers.
- 5. Create mappings between storage classifications on source and target VMM servers.
- 6. Enable protection for virtual machines.
- 7. Create and customize recovery plans that specify how virtual machines should be grouped and failed over.

SUMMARY SKILL MATRIX

IN THIS LESSON YOU LEARNED:

- The cloud is a network of services, and each server has different function. Some servers run applications or deliver a service. By using the cloud, you don't have to have the individual application or services running on the user's computers. In addition, the cloud allows you to share resources and technology, so that they can be accessed by multiple users.
- Microsoft Intune is a cloud-based management solution that allows you to manage your computers when they are not inside your corporate network. Microsoft Intune helps you manage your computers and mobile devices through a web console. It provides the tools, reports, and licenses to ensure your computers are always current and protected. For mobile devices, it also allows you to manage your remote workforce by working through Exchange ActiveSync or directly through Microsoft Intune.
- Microsoft Azure (formerly known as Microsoft Azure) is a cloud-computing platform used for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters. Although Microsoft Azure has its own web-based tools, you can also use Virtual Machine Manager (VMM) and App Controller.
- By using virtual machine technology, you can run multiple operating systems concurrently on a single machine, which allows separation of services while keeping cost to a minimum. It can also be used to create Windows test systems in a safe, self-contained environment. Microsoft Hyper-V is a hypervisor-based virtualization system for x64 computers starting with Windows Server 2008.
- Microsoft Azure has a wide range of tools that provide high availability, redundancy and fault tolerance, to keep your cloud components running 24/7 and provide wide range of tools to recovery from a disaster.

Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

- 1. The ______ is a web-based service that is hosted outside of your organization and allows users to access services and documents over the Internet.
- 2. ______ allows you to buy, develop, test, deploy, and manage software applications so that the application can be accessed by the user.
- **3.** _____ provides the infrastructure that the cloud runs on such as servers, switches, routers, and other equipment.
- 4. _____ provide communications between users over the cloud.
- 5. _____ is a cloud-based management solution that allows you to manage your computers when the users are not inside your corporate network.
- 6. ______ are used to quickly organize and manage your computers and users for Microsoft Intune.
- 7. ______ is a cloud-computing platform used for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters.
- **8.** ______ is a software component that is used to orchestrate protection for virtual machines that are located on on-premises Hyper-V host servers located in the VMM cloud.

- 9. The _____ provides a blackbox approach when users access services on the Internet.
- **10.** Microsoft Intune ______ are used to apply settings that apply to domain-joined computers in any domain.

Multiple Choice

Circle the letter that corresponds to the best answer.

- 1. Which of the following represent security and management tasks that can be handled with Microsoft Intune? (Choose all that apply)
 - a. Track hardware and software inventory
 - **b.** Provide remote assistance
 - c. Protect computers from malware.
 - **d.** Manage the deployment of software updates.
- 2. On which operating system can you install the Microsoft Intune? (Choose all that apply)
 - a. Windows XP Professional (SP3)b. Windows Vista Business Edition
 - **c.** Windows 10 Professional (physical computer)
 - **d.** Windows 8/8.1 Consumer (virtual client)
 - **u.** Windows 0/0.1 Consumer (virtual circuit)
- **3.** Which administrator role in Microsoft Intune can create and delete *all* other types of accounts?
 - a. Microsoft Intune Service administrator role
 - b. Microsoft Intune User Management Administrator role
 - c. Microsoft Intune Tenant Administrator
 - d. Microsoft Intune SuperAdmin Role
- 4. Which type of group is created manually in the Microsoft Intune Administration console?
 - a. dynamic query-based group
 - b. direct-based group
 - **c.** security group
 - **d.** dynamic group
- **5.** You have a phone that is being managed by Microsoft Intune and the phone is stolen. What should you do?
 - a. Change the password
 - **b.** Wipe the phone
 - **c.** Ping the phone
 - d. Run an inventory report for the phone
- **6.** Which configuration allows you to see devices that are managed by Microsoft Intune to appear in Configuration Manager?
 - a. Microsoft Intune Stand-Alone Cloud Configuration
 - b. Microsoft Intune Cloud + On-Premise Configuration
 - c. Microsoft Intune + Configuration Manager
 - d. Microsoft Intune with System Center Plug-in
- 7. Which type of membership should you be used to add devices automatically to groups in Microsoft Intune?
 - a. Direct
 - **b.** Criteria
 - **c.** Dynamic
 - **d.** Auto

- **8.** Which of the following can be used to deploy and manage servers running Windows Server 2012 R2 on the Microsoft Azure? (Choose all that apply)
 - a. Microsoft Azure virtual machine (VM) tools
 - b. Virtual Machine Monitor (VMM)
 - c. Virtual Machine Manager (VMM)
 - d. App Controller
- **9.** When using Microsoft Azure, which of the following is a popular open source cache for your Azure applications?
 - a. Service Bus
 - **b.** Managed Cache
 - **c.** Redis Cache
 - d. Stream Analytics
- **10.** Which cloud service is provided by Microsoft Office 365?
 - **a.** Productivity services
 - **b.** Storage services
 - c. Communication services
 - **d.** Search services

True / False

Circle T if the statement is true or F if the statement is false.

- $\mathbf{T} \mid \mathbf{F} = \mathbf{1}$. The public cloud offers a more secure environment than the corporate network.
- T F 2. Active Directory Group Policy allows more granular control than Microsoft Intune policies.
- T | F 3. When deploying software using Microsoft Intune, it is best to deploy to groups.
- T F 4. When a phone is stolen, it is best to wipe the phone.
- $\mathbf{T} \mid \mathbf{F} = \mathbf{5}$. OneDrive is considered a productivity service.

Case Projects

Scenario 4-1: Creating a Disaster Recovery Site

You are administrator for the Contoso Corporation and you manage a network that has around 30 servers. You need to create a disaster recovery (DR) site that can provide the same services while keeping cost to a minimum. Describe your proposed solution.

Scenario 4-2: Collaborating with a Partner Company

You are administrator for the Contoso Corporation, which has formed a partnership with Litware. com. You need to determine a secure method that will allow Litware users to access project files. For security reasons, you don't want to create a VPN tunnel for Litware users to access your network. To minimize costs, you are considering the cloud. Describe your proposed solution.

Scenario 4-3: Managing Stolen Phones

You are administrator for the Contoso Corporation and you manage several mobile devices by using Microsoft Intune. You want to develop a plan to help protect the smart phones that may have confidential information and develop a plan when a phone is stolen or lost. Describe your proposed solution.

Understanding Enterprise Mobility



5

OBJECTIVE DOMAIN MATRIX

		OBJECTIVE DOMAIN NUMPER
 Understanding Identity Services Understanding Windows Server Active Directory Understanding Azure Active Directory Understanding Microsoft Accounts Understanding Federation Services 	Describe identity services	5.1
 Understanding Business Data Access Configuring the Company Portal Customizing the Company Portal Using Work Folders Understanding Azure RemoteApp 	Describe business data access	5.2
 Understanding Bring Your Own Device (BYOD) Deploying and Managing Applications by Using Microsoft Intune Understanding Device-Centric to People-Centric IT Understanding Desktop Virtualization Understanding Dynamic Access Control (DAC) Policies Understanding Windows Rights Management 	Describe Bring Your Own Device (BYOD)	5.3

KEY TERMS		
account organizations	attribute store	Azure RemoteApp
Active Directory Domain Services	Azure Active Directory (AD) Azure AD Join	Bring Your Own Device (BYOD) policies
Active Directory Federation Services (AD FS)	Azure Active Directory Sync (DirSync) tool	built-in groups Central Access Policy

Central Access Rules	(GUID)	Remote Desktop Protocol
claim	group	(RDP)
claim rules	identity services	resource organizations
claims	Kerberos	security group
claims provider	Lightweight Directory Access	security identifier (SID)
claims provider trust	Protocol (LDAP)	Security Token Service (STS)
claims-based access control	Line of Business (LOB) apps	sideloading
computer accounts	local user account	Single Sign-On (SSO)
deeplinking	member server	site
Device Registration Service	Microsoft Intune Mobile	token
(DRS)	Application Management	trust relationships
directory service		trusted identity provider
distribution group	Microsoft Intune Company Portal	trusted publishing domain
domain	object	
domain controller	organizational units (OUs)	trusted user domains (TODS)
domain local group	RD Connection Broker	universal group
domain tree	RD Gateway	user account
domain user account	RD Licensing	Virtual Desktop Infrastructure
Dynamic Access Control (DAC)	RD Session Host	
federated trust relationship	RD Virtualization Host	Infrastructure
federation server	RD Web Access	Web Application Proxy
forest	relying parties	Work Folders
global group	relying parties	Worknlace Join
globally unique identifier	RemoteApp	Horapiace Join

You are an administrator of the Contoso Corporation. With the popularity of mobile devices used within the corporate environment, you need to determine how mobile devices can access corporate resources while maintaining security. For example, sales employees need to access price lists and presentations that will be used on sales visits. Project team members will have to access shared documents so that they can collaborate.

Understanding Identity Services

THE BOTTOM LINE

Identity services provides credentials that can be registered with an Access Control Service (ACS), such as Microsoft Azure, that allow users to authenticate directly with an ACS and receive a token for accessing the ACS. The ACS may contain many service identities.



In Lesson 4, you learned that Microsoft Azure is an ACS. Some of the identity services discussed in this section include Windows Server Active Directory, Azure Active Directory, Microsoft Account, and federation services.

CERTIFICATION READY Describe identity services 5.1

Understanding Windows Server Active Directory

A *directory service* stores, organizes, and provides access to information in a directory. Directory services are used for locating, managing, administering, and organizing common items and network resources, such as volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. One popular directory service used by many organizations is Microsoft's Active Directory.

Active Directory Domain Services is a technology created by Microsoft that provides a variety of network services, including the following:

- LDAP
- Kerberos-based and Single Sign-On (SSO) authentication
- DNS-based naming and other network information
- A central location for network administration and delegation of authority

The *Lightweight Directory Access Protocol (LDAP)* is an application protocol for querying and modifying data using directory services running over TCP/IP. Within the directory, the sets of objects are organized in a logical hierarchical manner so that you can easily find and manage them. The structure can reflect geographical or organizational boundaries, although it tends to use DNS names for structuring the topmost levels of the hierarchy. Deeper inside the directory, there might be entries representing users, organizational units, printers, documents, groups of users, or anything else that represents a given tree entry (or multiple entries). LDAP uses TCP port 389.

Kerberos is a computer network authentication protocol that allows hosts to prove their identity over a nonsecure network in a secure manner. It can also provide mutual authentication so that both the user and server verify each other's identity. For security reasons, Kerberos protocol messages are protected against eavesdropping and replay attacks.

Single Sign-On (SSO) allows you to log on once and access multiple related but independent software systems without having to log in again. As you log on with Windows using Active Directory, you are assigned a token that can then be used to sign on to other systems automatically.

Finally, Active Directory allows you to organize all of your network resources, including users, groups, printers, computers, and other objects, so that you can assign passwords, permissions, and rights to the users on your network. You can also assign who can manage a group of objects.

INTRODUCING DOMAINS, TREES, AND FORESTS

Active Directory domains, trees, and forests are logical representations of your network organization. Because they are logical components, you can organize them in the best way to manage your resources. To identify domains, trees, and forests, Active Directory is closely tied to DNS.

A *domain* defines an administrative boundary for users and computers that are stored in a common directory database. A single domain can span multiple physical locations or sites and can contain millions of objects. A domain uses a single Active Directory database to share its common security and user account information for all computers within the domain, allowing centralized administration of all users, groups, and resources on the network.

Because some organizations contain thousands of users and thousands of computers, it might make sense to categorize an organization into more than one domain. An Active Directory forest contains one or more transitive, trust-linked trees, with each tree linked in a transitive trust hierarchy, so that users and computers from one domain can access resources in another domain.

A *domain tree* is a collection of domains grouped into hierarchical structures and share a common root domain. A domain tree could have a single domain or many domains. A domain

(known as the parent domain) can have a child domain. Likewise, a child domain can have its own child domain. Because the child domain is combined with the parent domain name to form its own unique DNS name, the domains with a tree have a contiguous namespace.

The domains within a tree have the same contiguous name space. For example, you could have one domain assigned to an organization's developers and another domain assigned to its salespeople:

Developers.microsoft.com

Sales.microsoft.com

The Developers and Sales domains would both be child domains of the microsoft.com domain.

A *forest* is a collections of domains trees that share a common schema. A forest can contain one or more domain trees or domains, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. A forest can consist of a single domain tree or even a single domain. The first domain in the forest is called the forest root domain. If you have multiple domain trees, each domain tree would consist of a unique namespace.

A forest differs from a tree because it uses disjointed namespaces between the trees. For example, in a forest, microsoft.com might be the root for one tree. Should Microsoft purchase a company called Contoso (contoso.com), contoso.com then becomes the root of another tree. Each tree could be combined into a forest, yet each tree's identity could be kept separate.

To allow users in one domain to access resources in another domain, Active Directory uses *trust relationships*, whereby one domain trusts another domain so that users from one domain can access resources from another domain. As previously discussed, domains with a tree and forest are automatically created as two-way transitive trusts. A transitive trust is based on the following concept:

If domain A trusts domain B, and domain B trusts domain C, then domain A trusts domain C.

However, if you have a partnership with another company and you need users from one domain within one organization to access resources in another domain, you can configure an explicit nontransitive trust to be either one way or two way.

INTRODUCING SITES AND DOMAIN CONTROLLERS

Although domains, trees, and forests are logical representations of your organization, sites and domain controllers represent the physical structure of your network.

A *site* is one or more IP subnets that are connected by a high-speed link, typically defined by a geographical location. As an example, let's say Contoso is four-story office building. Although the building includes several subnets, all of the computers within the building use layer-2 and layer-3 switches to communicate with each other. If you have multiple sites, each site is connected to other sites over a much slower WAN link (at least slower than the LAN speeds you would find within an individual site). You can then define various network traffic patterns based on how the sites are defined.

When a user logs on, Active Directory clients locate an Active Directory server (using the DNS SRV resource records) known as a domain controller in the same site as the computer. Each domain has its own set of domain controllers to provide access to the domain resources, such as users and computers.

For fault tolerance, a site should have two or more domain controllers. That way, when one domain controller fails, the other domain controller can still service the clients. Note that whenever an object (such as a username or password) is modified, it is automatically replicated to the other domain controllers within a domain.

TAKE NOTE*

Without DNS and SRV records, Active Directory will not be able to function properly. A *domain controller* is a Windows server that stores a replica of the account and security information for the domain and defines the domain boundaries. To make a computer running Windows Server 2008 a domain controller, you must install the Active Directory Domain Services and execute the dcpromo (short for dc promotion) command.

After you have promoted a computer to a domain controller, you can use several MMC snap-in consoles to manage Active Directory:

- Active Directory Users and Computers: Used to manage users, groups, computers, and organizational units. Figure 5-1 shows the Active Directory Users and Computers console.
- Active Directory Domains and Trusts: Used to administer domain trusts, domain and forest functional levels, and user principal name (UPN) suffixes.
- Active Directory Sites and Services: Used to administer replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest.
- Active Directory Administrative Center: Used to administer and publish information in the directory, including managing users, groups, computers, domains, domain controllers, and organizational units.
- Group Policy Management Console (GPMC): Provides a single administrative tool for managing Group Policy across the enterprise.

 Action View Help Action View Help Active Directory Users and Com Saved Queres Contoso.com Builtin Computers Domain Controllers Conceptor Provide RODC Password Replication. Security Group - Domain Local Members in this group can have th Computers Domain Controllers Energins Computers Consult of administrators of the daministrators of this group are Read-Oan Domain Controllers Cuest Domain Controllers Security Group - Global All domain users Security Group - Global All domain users	3	Active	e Directory Users and Comp	outers
Active Directory Users and Com Several Queries Contoso.com Builtin account for administrators Computers Computers Computers Computers Domain Controllers Control Computers Security Group - Clobal Domain Controllers Security Group - Global Domain Controllers Sourity Group - Global All domain guests Sourity Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Security Group - Global Members	ile Action View Help			
Active Directory Users and Com Name Type Description Seved Queries Builti-m account for administering Builti-m account for administering Builti-m account for administering Administrator User Builti-m account for administering Builti-m account for administering Security Group - Domain Local Members in this group are permitt Builti-m account for administering Security Group - Domain Local Members of this group are permitt Builti-m account for administering Security Group - Domain Local Members of this group are permitt Builti-m account for administering Security Group - Domain Local Members of this group chance that are do Builti-m account for administering Security Group - Global DNS clients who are permitted to p Bonsind Admins Security Group - Global DNS clients who are permitted to p Bornain Controllers Security Group - Global All domain controllers in the domain Bornain Controllers Security Group - Global All domain guests Bornain Users Security Group - Global All domain guests Bornain Users Security Group - Global All domain guests Bornain Users Security Group - Global All domain guests Bornain Users Security Group - Global All domain guests<	• • 🖉 🖬 🔏 🖬 🗙 🕻		1 %	
Saved Queries Administrator User Built-in account for administrations. Contoso.com Image: Adlowed RODC Password Replication Security Group - Domain Local Members in this group can have thm. Domain Controllers Computers Security Group - Global Members of this group are permitt Domain Controllers Security Group - Domain Local Members of this group are permitt Managed Service Account Denied RODC Password Replication Security Group - Domain Local Members of this group are permitted to p Managed Service Account Denied RODC Password Replication Security Group - Global DNS deministrators Group Managed Service Account Domain Computers Security Group - Global DNS deministrators of the d Domain Computers Domain Controllers Security Group - Global All workstations and servers joined Disers Domain Controllers Security Group - Global All domain quests Domain Guests Security Group - Global All domain quests Domain Guests Security Group - Global All domain users Deniar Group Policy Creator Owners Security Group - Global All domain sucers Security Group - Universal Members of this group are Read-O Members of this group are Read-O Security Group - Clobal All domain controllers </td <td>Active Directory Users and Com</td> <td>Name</td> <td>Туре</td> <td>Description</td>	Active Directory Users and Com	Name	Туре	Description
Image: Construction Image: Construction Security Group - Domain Local Members in this group can have th Image: Construction Security Group - Domain Local Members of this group can have th Image: Construction Security Group - Domain Local Members of this group can have th Image: Construction Security Group - Domain Local Members of this group can have th Image: Construction Security Group - Domain Local Members of this group cannot hav Image: Construction Security Group - Domain Local Members of this group cannot hav Image: Construction Security Group - Domain Local Members of this group cannot hav Image: Construction Security Group - Clobal Members of this group cannot hav Image: Construction Security Group - Global Designated administrators of the d Image: Construction Security Group - Global All workstations and servers joined Image: Construction Security Group - Global All workstations and servers joined Image: Construction Security Group - Global All domain controllers in the domain sers Image: Construction Security Group - Global All domain sers Image: Conseable wind wind with seread-only Domain Controllers <td>Saved Queries</td> <td>& Administrator</td> <td></td> <td></td>	Saved Queries	& Administrator		
 Bultin Computers Compation Controllers Conceable Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Controllers Security Group - Domain Local Members in this group cannot haw. Donsdhröund Donsdhröund Donsin Controllers Security Group - Global Dons Adminis Domain Controllers Domain Controllers Domain Controllers Security Group - Global All domain guests Domain Controllers Security Group - Global All domain guests Domain Controllers Security Group - Global All domain guests Domain Controllers Security Group - Global All domain guests Domain Locat Designated administrators of the d Enterprise Adminis Guest Jons Security Group - Global Members of this group can modify Guest Jons Security Group - Global Members of this group can configure and figure and f	🚔 contoso.com	& Allowed RODC Password Replicatio	Security Group - Domain Local	Members in this group can have th
 Computers Computers Compain Controllers Compain Controllers Compain Controllers Controllers Controllers<!--</td--><td>Builtin</td><td>🍇 Cert Publishers</td><td>Security Group - Domain Local</td><td>Members of this group are permitt</td>	Builtin	🍇 Cert Publishers	Security Group - Domain Local	Members of this group are permitt
 Domain Controllers Densid RODC Password Replication Security Group - Domain Local Members in this group cannot hav Designated administrators Group Dus Adminis Security Group - Global Managed Service Accoup Domain Computers System System Domain Controllers Domain Controllers Domain Computers Domain Controllers Domain Computers Security Group - Global All vorkstations and servers joined Domain Controllers Domain Controllers Domain Controllers Security Group - Global All domain controllers in the domain Domain Guests Security Group - Global All domain users Domain Users Security Group - Global All domain sucers Domain Users Security Group - Global All domain sucers Benterprise Admins Security Group - Universal Members of this group can modify Guest John Smith Guest John Smith User Key Distribution Center Service Accc Read-only Domain Controllers Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Cont	Computers	🍇 Cloneable Domain Controllers	Security Group - Global	Members of this group that are do
 PoreignSecurity FinctPart Dorsdmins DorsdminSecurity FinctPart DostAdmins DostAdmins Security Group - Global DNS deinsitators Group DNS deinsitators of the d Domain Controllers System Domain Controllers Domain Controllers Security Group - Global All domain users Domain Controllers Security Group - Global All domain controllers in the domain Domain Controllers Security Group - Global All domain controllers Domain Controllers Security Group - Global All domain users Domain Users Security Group - Global All domain users Domain Controllers Security Group - Global All domain users Domain Controllers Security Group - Global All domain users Security Group - Global All domain users Security Group - Universal Designated administrators of the e Group Policy Creator Owners Security Group - Global Members of this group are afforde Sourity Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Memb	Domain Controllers	& Denied RODC Password Replication	Security Group - Domain Local	Members in this group cannot hav
 LostAndround DostAndround Domain Computers Security Group - Global All domain controllers Security Group - Global All domain users GostAndround Security Group - Universal Members of this group are Read-O GostAndround GostAndround GostAndround GostAndround GostAndround Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controll	ForeignSecurityPrincipal:	A DnsAdmins	Security Group - Domain Local	DNS Administrators Group
 Managed Service Account Managed Service Account Derogram Data System System Domain Computers Security Group - Global All workstations and servers joined Domain Controllers Security Group - Global All domain controllers in the domain Domain Controllers Security Group - Global All domain controllers in the domain Domain Guests Security Group - Global All domain users Enterprise Admins Security Group - Global All domain users Enterprise Read-only Domain Control. Security Group - Global Members of this group are Read-On Goup Policy Creator Owners Security Group - Global Members of this group are afforde Goust User Key Distribution Center Service Acc Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members	▶ LostAndFound	😹 DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to p
▶ Program Data ▶ Domain Computers Security Group - Global All workstations and servers joined > System > Domain Controllers Security Group - Global All domain controllers in the domain > NTDS Quotas > Domain Controllers Security Group - Global All domain users > TPM Devices > Domain Controllers Security Group - Global All domain users > TPM Devices > Domain Controllers Security Group - Global All domain users > TPM Devices > Domain Controllers Security Group - Global All domain users > Group Policy Creator Owners Security Group - Global Members of this group are Read-O > Group Policy Creator Owners Security Group - Global Members of this group are afforde > John Smith User Key Distribution Center Service Acc > Nortexted Users Security Group - Global Members of this group are afforde > Read-Only Domain Controllers Security Group - Global Members of this group are afforde > Read-Only Domain Controllers Security Group - Global Members of this group are afforde > Read-Only Domain Controllers Security Group - Global Members of this group are afforde > Rea	Managed Service Accour	👫 Domain Admins	Security Group - Global	Designated administrators of the d
 System Domain Controllers Security Group - Global All domain controllers in the domain Domain Guests Domain Guests Domain Users Domain Users Security Group - Global All domain guests All domain guests Domain Users Security Group - Global All domain users Corrup Policy Creator Owners Group Policy Creator Owners Group Policy Creator Owners Group Policy Creator Owners Group Policy Creator Owners Security Group - Global Members of this group are Read-O Group Policy Creator Owners Security Group - Global Members of this group are Read-O Group Policy Creator Owners Security Group - Global Members of this group are Read-O Group Policy Creator Owners Security Group - Global Members of this group are Read-Co Frotected Users Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Security Group - Global Members of this group are afforde Security Group - Global Members of this group are Read-O Security Group - Global Members of this group are Read-O Security Group - Global<!--</td--><td>Program Data</td><td>& Domain Computers</td><td>Security Group - Global</td><td>All workstations and servers joined</td>	Program Data	& Domain Computers	Security Group - Global	All workstations and servers joined
Image: Solution of the second of the seco	System	& Domain Controllers	Security Group - Global	All domain controllers in the domain
p INICS Gubuss Security Group - Global All domain users p TPM Devices Enterprise Admins Security Group - Universal Designated administrators of the e Q Enterprise Read-only Domain Control. Security Group - Universal Members of this group are Read-O Q Group Policy Creator Owners Security Group - Global Members of this group are Read-O Q Goust User Built-in account for guest access t Q John Smith User Key Distribution Center Service Acc Q Protected Users Security Group - Global Members of this group are afforde Q Read-only Domain Controllers Security Group - Global Members of this group are afforde Q Read-only Domain Controllers Security Group - Global Members of this group are afforde Q Read-only Domain Controllers Security Group - Global Members of this group are afforde Q Read-only Domain Controllers Security Group - Global Members of this group are afforde Q Read-only Domain Controllers Security Group - Universal Designated administrators of the s Q Store adminis Security	NTDS Quetas	& Domain Guests	Security Group - Global	All domain guests
Image: Enterprise Admins Security Group - Universal Designated administrators of the e Enterprise Read-only Domain Contr Security Group - Universal Members of this group are Read-O Group Policy Creator Owners Security Group - Global Members of this group can modify Group Policy Creator Owners Security Group - Global Members of this group are Read-O Group Policy Creator Owners Security Group - Global Members of this group are afforde In John Smith User Built-in account for guest access t In Kright User Key Distribution Center Service Acc RAS and IAS Servers Security Group - Global Members of this group can access re Read-only Domain Controllers Security Group - Domain Local Servers in this group can access re Read-only Domain Controllers Security Group - Global Members of this group are Read-O Schema Admins Security Group - Domain Local Servers in this group can access re Read-only Domain Controllers Security Group - Universal Designated administrators of the s	TPM Devices	& Domain Users	Security Group - Global	All domain users
Image: Enterprise Read-only Domain Contru. Security Group - Universal Members of this group are Read-O Image: Group Policy Creator Owners Security Group - Global Members in this group can modify Image: Group Policy Creator Owners Security Group - Global Members in this group can modify Image: Group Policy Creator Owners User Built-in account for guest access t Image: Group Policy Creator Owners Security Group - Global Members of this group are afforde Image: Group Policy Creator Owners Security Group - Global Members of this group are afforde Image: Group Policy Creator Owners Security Group - Global Members of this group are afforde Image: Group Policy Creator Owners Security Group - Domain Local Servers in this group are Read-O Image: Group Policy Creator Owners Security Group - Global Members of this group are Read-O Image: Group Policy Creator Owners Security Group - Domain Local Severs in this group are Read-O Image: Group Policy Creator Owners Security Group - Global Members of this group are Read-O Image: Group Policy Creator Owners Security Group - Global Members of this group are Read-O Image: Group Policy Creator Owners Security Group - Universal Design		& Enterprise Admins	Security Group - Universal	Designated administrators of the e
Image: Source of Controllers Security Group - Global Members in this group can modify Image: Source of Controllers User Built-in account for guest access t Image: Source of Controllers User Key Distribution Center Service Acc Image: Source of Controllers Security Group - Global Members of this group are afforde Image: Read-only Domain Controllers Security Group - Global Members of this group are afforde Image: Read-only Domain Controllers Security Group - Global Members of this group are afforde Image: Read-only Domain Controllers Security Group - Global Members of this group are afforde Image: Read-only Domain Controllers Security Group - Global Members of this group are Read-O Image: Schema Admins Security Group - Universal Designated administrators of the s		👫 Enterprise Read-only Domain Contr	Security Group - Universal	Members of this group are Read-O
Loser Built-in account for guest access t John Smith User In Smith Security Group - Global In Smith Security Group - Domain Local In Schema Admins Security Group - Global In Schema Admins Security Group - Universal In Schema Administrators of the s Designated administrators of the s		& Group Policy Creator Owners	Security Group - Global	Members in this group can modify
John Smith User Krbtgt User Krbtgt User Res Distribution Center Service Acc Members of this group are afforde RAS and IAS Servers Security Group - Domain Local Read-only Domain Controllers Security Group - Global Reschema Admins Security Group - Global Members of this group are Read-O Security Group - Global		S. Guest	User	Built-in account for guest access t
List User Key Distribution Center Service Acc Reg Protected Users Security Group - Global Members of this group are afforde RAS and IAS Servers Security Group - Domain Local Servers in this group are afforde Read-only Domain Controllers Security Group - Global Members of this group are Read-O Schema Admins Security Group - Universal Designated administrators of the s		🤱 John Smith	User	
Protected Users Security Group - Global Members of this group are afforde RAS and IAS Servers Security Group - Domain Local Servers in this group can access re Read-only Domain Controllers Security Group - Global Members of this group are Read-O Schema Admins Security Group - Universal Designated administrators of the s		👫 krbtgt	User	Key Distribution Center Service Acc
RAS and IAS Servers Security Group - Domain Local Servers in this group can access re Read-only Domain Controllers Security Group - Global Members of this group are Read-O Schema Admins Security Group - Universal Designated administrators of the s		Reprotected Users	Security Group - Global	Members of this group are afforde
Read-only Domain Controllers Security Group - Global Members of this group are Read-O Schema Admins Security Group - Universal Designated administrators of the s		RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access re
Schema Admins Security Group - Universal Designated administrators of the s		Read-only Domain Controllers	Security Group - Global	Members of this group are Read-O
		& Schema Admins	Security Group - Universal	Designated administrators of the s
WinKMRemoteWMIUsers Security Group - Domain Local Members of this group can access		& WinRMRemoteWMIUsers	Security Group - Domain Local	Members of this group can access

Although these tools are installed on domain controllers, they can also be installed on client PCs so that you can manage Active Directory without logging on to a domain controller.

A server that is not running as a domain controller is known as a *member server*. To create a domain controller, you install the Active Directory Domain Services on a Windows server and then promote the server to a domain controller.

The replication path, or site topology, within a site is automatically managed by a service called the Knowledge Consistency Checker (KCC). Typically, replication within sites happens more quickly than replication between sites. The Active Directory Sites and Services MMC

Figure 5-1

Active Directory Users and Computers console

snap-in allows you to control intersite replication. You can use it to create site-link bridge objects and to configure replication patterns.

Within Active Directory, you need to define each subnet. Once you have done this, Active Directory can figure out the best way to replicate information locally and between sites.

To minimize traffic across a WAN link, bridgehead servers perform directory replication between two sites, whereas only two designated domain controllers talk to each other. If you have domain controllers from multiple domains, you will have a bridgehead server for each domain.

INTRODUCING ORGANIZATIONAL UNITS

As previously discussed, a single organization might have thousands of users and thousands of computers. With Windows NT, a domain could handle only a limited number of objects before you would encounter performance issues. With later versions of Windows, the size of the domain was dramatically increased. Although you might have previously required several domains with Windows NT to define your organization, you could now have just one domain to represent a large organization. However, you still need a way to organize and manage the objects within that domain.

To help organize objects within a domain and minimize the number of domains you require, you can use *organizational units (OUs)*. OUs can be used to hold users, groups, computers, and other organizational units. An organizational unit can only contain objects that are located in a domain. Although there are no restrictions on how many nested OUs (an OU inside of another OU) you can have, you should strive to design a shallow hierarchy for better performance.

When you first install Active Directory, there are several OUs already created. They include computers, users, domain controllers, and built-in OUs. Unlike the OUs that you create, these OUs do not allow you to delegate permissions or assign group policies to them. (Group policies will be explained later in this lesson.) Another OU worth mentioning is the domain controller, which holds the default domain controllers policy.

Containers are objects that can store or hold other objects. They include the forest, tree, domain, and organizational unit. To help manage your objects, you can delegate authority to a container, particularly the domain or organizational unit.

For example, if you have your domain organized according to physical location, you can assign a site administrator authoritative control to the OU that represents a physical location so that the user will have administrative control only to the objects within that OU. You can also structure your OUs by function or areas of management. For example, you might create a Sales OU to hold all of your sales users. You might also create a Printers OU to hold all of the printer objects and assign a printer administrator.

By delegating administration, you can assign a range of administrative tasks to the appropriate users and groups. For example, you can assign basic administrative tasks to regular users or groups and leave domain-wide and forest-wide administration to members of the Domain Admins and Enterprise Admins groups. By delegating administration, you allow groups within your organization to take more control of their local network resources. You also help secure your network from accidental or malicious damage by limiting the membership of administrator groups.

You can delegate administrative control to any level of a domain tree by creating organizational units within a domain and delegating administrative control for specific organizational units to particular users or groups.

DELEGATE ADMINISTRATIVE CONTROL OF AN OU

GET READY. To delegate administrative control of an OU, log on to the server running Windows Server 2012 R2/2016 using an account with administrative privileges and then perform the following steps.

- 1. In the Server Manager window, click **Tools > Active Directory Users and Computers**. The Active Directory Users and Computers console appears.
- Right-click the object over which you want to delegate control and choose Delegate Control. The Delegation of Control Wizard appears, displaying the Welcome page.
- 3. Click Next. The Users or Groups page appears.
- 4. Click Add. The Select Users, Computers, or Groups dialog box appears.
- **5.** Type the name of the user or group to which you want to delegate control of the object and click **OK**. The user or group appears in the Selected users and groups list.
- 6. Click Next. The Tasks to Delegate page appears, with the following options:
 - Delegate the following common tasks: This option enables you to choose from a list of predefined tasks.
 - Create a custom task to delegate: This option enables you to be more specific about the task delegation.
- Select Create a custom task to delegate and click Next. The Active Directory Object Type page appears, displaying the following options.
 - This folder, existing objects in this folder, and creation of new objects in this folder: This option delegates control of the container, including all its current and future objects.
 - Only the following objects in the folder: This option enables you to select specific objects to be controlled. You can select Create selected objects in this folder to allow selected object types to be created or you can select Delete selected objects in this folder to allow selected object types to be deleted.
- 8. Select This folder, existing objects in this folder, and creation of new objects in this folder and click Next. The Permissions page appears.
- **9.** Set the delegated permissions according to your needs for the user or group to which you delegate control. You can combine permissions from all three of the following options:
 - General displays general permissions, which are equal to those displayed on the Security tab in an object's properties. For example, selecting Full Control for general permissions is inclusive of all property rights as well.
 - Property-specific displays permissions that apply to specific attributes or properties of an object. If you select the Read permission using the General option, all read-specific properties are selected.
 - Creation/deletion of specific child objects displays permissions that apply to creation and deletion permissions for specified object types.
- 10. Click Next. The Completing the Delegation of Control Wizard page appears.
- 11. Click Finish.
- 12. CLOSE the Active Directory Users and Computers console.

LOOKING AT OBJECTS

An *object* is a distinct, named set of attributes or characteristics that represent a network resource. Common objects used within Active Directory are computers, users, groups, and printers. Attributes have values that define the specific object. For example, a user could have the first name John, the last name Smith, and the login name as jsmith, all of which identify the user.

When working with objects, administrators use the names of the objects, such as usernames. However, Active Directory objects are assigned a 128-bit unique number called a *globally unique identifier (GUID)*, sometimes referred to as a *security identifier (SID)*, to uniquely identify an object. Therefore, if a user changes her name, you can change her username yet she will still be able to access all objects and have all of the rights she had previously, because these are assigned to the GUID.

GUIDs also provide some security. In particular, if a user is deleted, you cannot create a new user account with the same username and expect to have access to all of the objects and rights the previous user had access to. Thus, if a user leaves your organization but you plan to replace that user, you can disable the account, hire the new person, rename the user account, change the password, and re-enable the account so that the new user can access all resources and have all of the rights that the previous user had.

The schema of Active Directory defines the format of each object and the attributes or fields within each object. The default schema contains definitions of commonly used objects, such as user accounts, computers, printers, and groups. For example, the schema defines that a user account has the user's first name, last name, and telephone number.

To allow Active Directory to be flexible so that it can support other applications, you can extend the schema to include additional attributes. For example, you could add badge number or employee identification number to the user object. Indeed, when you install some applications, such as Microsoft Exchange, they will extend the schema, usually by adding additional attributes or fields so that the schema can support the application.

UNDERSTANDING USER ACCOUNTS

A *user account* enables a user to log on to a computer and domain. As a result, it can be used to prove the identity of a user, and this identity information can then be used to determine what the user can access and what kind of authorization he or she has. It can also be used for auditing so that if there is a security problem in which something was accessed or deleted, the person who accessed or deleted the object can be determined.

On today's Windows networks, there are two types of user accounts:

- Local user accounts
- Domain user accounts

A user account allows users to log on and access resources on the computer in which the account was created. A *local user account* is stored in the Security Account Manager (SAM) database on the local computer. The only Windows computer that does not have a SAM database is the domain controller. The administrator local user account is the only account that is both created and enabled by default in Windows. Although this account cannot be deleted, it can be renamed.

The only other account created (but not enabled) by default is the guest account. This account was created for the occasional user who needs access to network resources on a low-security network. Use of the guest account is not recommended, and this account is disabled by default.

A *domain user account* is stored on the domain controller and allows you to gain access to resources within the domain, assuming you have been granted permissions to access those objects. The administrator domain user account is the only account that is created and enabled by default in Windows when you first create a domain. Although the administrator domain user account cannot be deleted, it can be renamed.

When you create a domain user account, you must supply a first name, last name, and user logon name. The user logon name must be unique within the domain. See Figure 5-2. After the user account is created, you can open the user account properties and configure a person's username, logon hours, telephone numbers, and addresses; which computers the user can log on to; what

groups the person is a member of, and so on. You can also specify whether a password expires, whether the password can be changed, and whether the account is disabled. Lastly, on the Profile tab, you can define the user's home directory, logon script, and profile path.

Figure 5-2	John Smith Properties 2	John Smith Properties 2
User Account in Active Directory	Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control Remote Deaktop Services Profile COM+ Attribute Edtor General Address Account Profile Telephones Organization Image: Source Service Service John Smith Image: Smith Image: Smith Image: Smith Image: Source Service Smith Image: Smith Image: Smith Image: Smith Display name: John Smith Image: Smith Image: Smith Image: Smith Office: Image: Smith Image: Smith Image: Smith Userption: Image: Smith Image: Smith Image: Smith Userption:<	Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control Remote Dektop Services Profile COM+ Attribute Editor General Address Account Profile Profile Telephones Organization User profile Profile Telephones Organization User profile Image: Comparison of the

Associated with a user account is the user profile, which is a collection of folders and data that store the user's current desktop environment and application settings. A user profile also records all network connections that are established so that when a user logs on to a computer, the computer remembers the mapped drives to shared folders. Thus, when a user logs on to a particular computer, she will see the same desktop environment she previously had on the computer.

For Windows Vista, Windows Server 2008 and higher, user profiles are stored in the C:\Users folder. In each user's folder, some of the available folders include Desktop, Documents, Start Menu, and Favorites. See Figure 5-3. When jsmith directly accesses his or her Desktop or Documents, jsmith is really accessing C:\Users\jsmith\desktop or C:\Users\jsmith\my documents.

800

Figure 5-3	File Home Share V	/iew				~ 0
A usar's profile folder	(→ ↑) → This PC	▹ Local Disk (C:)	~	🖒 Search jsmith		P
A user's prome tolder	4 📥 Local Disk (C:) 🔨	Name	Date modified	Туре	Size	^
	SRecycle.Bin	📗 AppData	12/26/2014 8:47 PM	File folder		- 10
	Documents and Setti	 Application Data 	12/26/2014 8:47 PM	File folder		
	> inetpub	Contacts	3/16/2015 5:50 PM	File folder		- 10
	PertLogs	Cookies	12/26/2014 8:47 PM	File folder		
	P in Program Files	Desktop	3/16/2015 5:50 PM	File folder		
	Program Files (x8b)	Documents	3/16/2015 5:50 PM	File folder		- 11
	ProgramData	Downloads	3/16/2015 5:50 PM	File folder		- 11
	SCCMContentLib	Pavorites	3/16/2015 5:50 PM	File folder		- 11
	> JII SMS_DPS	🔐 Links	3/16/2015 5:50 PM	File folder		
	SMSPKGCS	 Local Settings 	12/26/2014 8:47 PM	File folder		
	JIII SMSSIGS	Music	3/16/2015 5:50 PM	File folder		- 11
	System Volume Infor	My Documents	12/26/2014 8:47 PM	File folder		
	a 🔐 Users	NetHood	12/26/2014 8:47 PM	File folder		
	Þ 🏢 admin	Pictures	3/16/2015 5:50 PM	File folder		
	administrator	PrintHood	12/26/2014 8:47 PM	File folder		
	▷ 🗃 All Users	Recent	12/26/2014 8:47 PM	File folder		
	Default	Saved Games	3/16/2015 5:50 PM	File folder		
	▷ 🔊 Default User	P Searches	3/16/2015 5:50 PM	File folder		
	DefaultAppPool	SendTo	12/26/2014 8:47 PM	File folder		
	4 🚛 jsmith	Start Menu	12/26/2014 8:47 PM	File folder		
	AppData	Templates	12/26/2014 8:47 PM	File folder		- 8
	Application Data	Videos	3/16/2015 5:50 PM	File folder		
	Contacts	NTUSER.DAT	3/16/2015 5:50 PM	DAT File	512 KB	
	▷ a) Cookies	ntuser.dat.LOG1	12/26/2014 8:47 PM	LOG1 File	976 KB	- 10
	Desktop	ntuser.dat.LOG2	12/26/2014 8:47 PM	LOG2 File	56 KB	- 11
	▷ III Documents	NTUSER.DAT{bbed3e3b-0b41-11e3-8249	12/28/2014 10:35	BLF File	64 KB	
	J. Downloads	NTUSER.DAT{bbed3e3b-0b41-11e3-8249	. 12/28/2014 10:35	REGTRANS-MS File	512 KB	
	Favorites	NTUSER.DAT{bbed3e3b-0b41-11e3-8249	12/27/2014 7:07 AM	REGTRANS-MS File	512 KB	
	Links 🗸	S) nturer ini	12/26/2014 9-47 DM	Configuration sett	1 KR	~

29 items

UNDERSTANDING COMPUTER ACCOUNTS

Like user accounts, Windows *computer accounts* provide a means for authenticating and auditing a computer's access to a Windows network and access to domain resources. Each Windows computer to which you want to grant access must have a unique computer account. A computer account can also be used for auditing purposes, specifying what system was used when something was accessed.

UNDERSTANDING GROUPS

A *group* is a collection or list of user accounts or computer accounts. Different from a container, a group does not store user or computer information; rather, it just lists it. The advantage of using groups is that they simplify administration, especially when assigning rights and permissions.

A group is used to group users and computers together so that when you assign rights and permissions, you assign them to the entire group rather than to each user individually. Users and computers can be members of multiple groups, and in some instances, a group can be assigned to another group.

In Windows Active Directory, there are there are two types of groups:

- A *security group* is used to assign rights and permissions and gain access to network resources. It can also be used as a distribution group.
- A *distribution group* is used only for nonsecurity functions, such as distributing email, and it cannot be used to assign rights and permissions. See Figure 5-4.

Object	Seci	urity	Attribute	Editor
General	Members	Member	Of Mar	naged E
E Tes	tGroup			
Group name (pr	e-Windows 2000):	TestGrou	р	
Description:				
E-mail:				
Group scope		Group t	ype	
🔿 Domain lo	cal	Sec	curity	
 Global 		🔿 Dis	tribution	
O Universal				
Notes:				

Any group, whether a security group or a distribution group, is characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. The three group scopes are as follows:

- *Domain local group*: A domain local group contains global groups and universal groups, even though it can also contain user accounts and other domain local groups. It is usually in the domain with the resource to which you want to assign permissions or rights.
- *Global group*: A global group can contain user accounts and other global groups. Global groups are designed to be "global" for the domain. After you place user accounts into global groups, the global groups are typically placed into domain local groups or local groups.
- *Universal group*: A universal group scope is designed to contain global groups from multiple domains. Universal groups can contain global groups, other universal groups,

Figure 5-4

A distribution group

and user accounts. Because global catalogs replicate universal group membership, you should limit the membership to global groups. This way, if you change a member within a global group, the global catalog will not have to replicate the change.

Understanding Built-in Groups

Similar to the administrator and guest accounts, Windows has default groups called *built-in groups*. These default groups are granted specific rights and permissions to get you started. Various built-in groups are as follows:

- **Domain Admins:** Members of this group can perform administrative tasks on any computer within the domain. The default, the Administrator account, is a member.
- **Domain Users:** Windows automatically adds each new domain user account to the Domain Users group.
- Account Operators: Members of this group can create, delete, and modify user accounts and groups.
- **Backup Operators:** Members of this group can backup and restore all domain controllers by using Windows Backup.
- Authenticated Users: This group includes all users with a valid user account on the computer or in Active Directory. Use the Authenticated Users group instead of the Everyone group to prevent anonymous access to a resource.
- **Everyone:** This group includes all users who access a computer, even if a particular user does not have a valid account.

Understanding Azure Active Directory

Azure Active Directory (AAD) is a cloud-based IaaS that you can use for identity management and access control. Azure AD has been the identity provider for Office 365 since before Azure AD was made available to the public.

Azure AD provides the following features:

- Active Directory authentication services in public or private clouds
- Cloud-based storage for directory service data
- Federation services
- A service for extending an on-premises Active Directory environment to cloud services

Azure AD provides high availability and scalability. It can integrate with on-premises AD DS, including directory synchronization and Single Sign-On (SSO). You also can limit the data that synchronizes to Azure AD. Lastly, Azure AD provides an application-programming interface to perform management tasks and to query the directory data.

To authenticate through Azure AD, you can use one of the following web-based authentication protocols:

- OAuth 2.0 is an open standard for authorization that provides granular access control to destination services as specified in RFC 6749. Access can be provided temporarily.
- Security Assertion Markup Language 2.0 (SAML 2.0) is an open standard XML protocol made up of security tokens and claims. The security token used with SAML contains claims, which are typically Active Directory attributes that the workflow application uses to make decisions for authorization and access.
- Web Services Federation (WS-Federation) is a security mechanism that allows identity federation so that users in one realm (or directory) can access resources in another realm.

To integrate with an on-premises Active Directory environment, you can use one of the following:

- *Azure Active Directory Sync (DirSync) tool* runs on an on-premises domain-joined computer to provide directory synchronization to Microsoft Azure AD. Used primarily to synchronize user objects and user attributes, DirSync is a requirement for SSO.
- Active Directory Federation Services (AD FS) is deployed onsite and provides SSO for applications and services that reside onsite or in Microsoft Azure. AD FS enables all authentications to take place in the on-premises Active Directory and offers Multi-Factor Authentication (MFA).
- On-premises AD DS is the authentication provider and the source of directory data. AD DS is a requirement for DirSync, AD FS, and SSO.

If you have configured synchronization between Active Directory and Azure, you can manage your user accounts with the standard Active Directory tools such as Active Directory Users and Computers. If you are not using directory synchronization, you can manage your accounts in Azure using the Microsoft Azure AD management portal or the Azure Directory Module for Windows PowerShell.

Understanding Microsoft Accounts

As already described in Lesson 1. Microsoft accounts can be used to provide a consistent experience when working with the Windows Store apps.

Microsoft accounts can be synched with a domain account, but the capability to do so depends upon Group Policy settings. Using Group Policy, you can determine whether you want to allow the synching of the two accounts and what information can be synched.

You create a Microsoft account during the initial installation of the operating system or after the system is running.

Understanding Federation Services

The *Active Directory Federation Services (AD FS)* role allows administrators to configure SSO for web-based applications across a single organization or multiple organizations without requiring users to remember multiple usernames and passwords, although it is not required. This enables you to configure Internet-facing business-to-business (B2B) applications between organizations. For example, a user from contoso.com can use contoso.com credentials to access a web-based application hosted by adatum.com.

Traditionally, if users from one organization or domain need to access a website provided by another organization or domain, you can do it one of two ways:

- Depending on the web application, you can create web or domain accounts for users and have them log on with a second account. Unfortunately, this does not provide an SSO solution.
- You can create a virtual private network (VPN) between the two organizations and establish a trust relationship between the two Active Directory domains. Although this provides an SSO solution, it is difficult to set up and maintain.

X REF

For more information about authentication, including MFA, see Lesson 3. AD FS–enabled applications are claims-based, which allows a much more scalable authentication model for Internet-facing applications. Therefore, AD FS is an identity access solution that allows any browser-based clients to access a website with a single logon to one or more protected Internet-facing applications, even when the user accounts and applications are on different networks and exists within different organizations via a federated trust relationship.

An AD FS configuration consists of two types of organizations:

- *Resource organizations* own the resources or data that are accessible from the AD FS– enabled application, similar to a trusting domain in a traditional Windows trust relationship.
- *Account organizations* contain the user accounts that access the resources controlled by resource organizations.

Because federation can be used within a single organization, the single organization serves as the resource organization and the account organization.

Of course, to establish an identity federation partnership, both partners agree to create a *federated trust relationship*. A federated trust relationship defines how each partner defines what resources are accessible to the other organization and how access to the resources is enabled. User identities and their associated credentials are stored, owned, and managed by the organization where the user is located.

Claims-based access control uses a trusted identity provider to provide authentication. The trusted identity provider issues a token to each user, which is then presented to the application or service as proof of identity. In other words, with claims-based authentication, users can authenticate to the Active Directory located within their organization and be granted a claim based on that authentication. The claim is then presented to an application that is running in a different organization.

The organization that accepts the claim and has the application the user is trying to access will require key information in the claim—for example, an email address or User Principal Name (UPN) to identify the user, and group membership to specify the access allowed within the application by the user.

To keep the claims secure, all communications occur over HTTPS. Of course, both organizations need to agree on the format for exchanging claims. To simplify this process, a set of specifications identified as web services have been identified, which can be used when implementing AD FS.

Web services are based on Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), and Universal Discovery Description and Integration (UDDI). It also uses Security Assertion Markup Language (SAML), which is an XML-based standard for exchanging claims between an identity provider and a service or application provider. The communication between federation servers is based around an XML document that stores the X.509 certificate for token signing and stores the SAML 1.1 or 2.0 token.

AD FS uses the following components:

- *Federation server*: The server that issues, manages, and validates requests involving identity claims. A federation server is needed in each participating forest.
- *Web Application Proxy:* An optional component that is usually deployed on a perimeter network that can receive externally and forward the packets to the internal federation server.
- *Claims*: A statement made by a trusted entity about an object, such as a user, that includes key information identifying the object.
- *Claim rules*: Rules that determine what makes up a valid claim and how claims are processed by the federation servers.

- *Attribute store*: A database, such as Active Directory Domain Services (AD DS), that is used to look up claim values.
- Claims provider: The server that issues claims and authenticates users.
- *Relying parties*: The application or web service that accepts claims from the claims provider. The relying party server must have the Microsoft Windows Identity Foundation installed or use the AD FS 1.0 claims-aware agent.
- *Claims provider trust*: Configuration data that specifies which client can request claims from a claims provider and subsequently submits them to a relying party.
- *Relying party trust*: Configuration data used to provide claims about a user or client to a relying party.

In the simplest scenario, an organization can deploy a federation server to be used with its own web applications. If the web application is running on Windows and is part of the same domain as the users who are accessing the web application, you can bypass the federation server and grant access directly to the Active Directory users. However, in more complicated scenarios, an organization might require AD FS:

- The application is not running on Windows or does not support AD DS authentication.
- The Windows server is not part of the domain and requires SAML or web services for authentication or authorization.
- A larger organization consists of multiple domains or multiple forests and has multiple identities.
- Users from outside the organization need access to internal servers and are not part of the domain.

When a single organization uses AD FS, you need only one federation server (not including what might be needed for high availability). If the network with the federation server is completely isolated, you need a second server to act as a federation proxy server. For AD FS to provide SSO for a single organization, the following would happen:

- 1. The client computer accesses a web-based application on a web server by sending an HTTPS request.
- 2. When the web server receives the request and identifies that the client computer does not have a claim, the web server redirects the client computer to the federation server proxy, if a proxy is being used. If not, it will forward the request to the federation server.
- 3. If the AD FS is using a proxy, the client computer sends an HTTPS request to the federation server proxy. Depending on the configuration and setup, the federation server proxy might use the current Windows logon (Integrated Windows authentication) or prompt for a logon.
- 4. If the AD FS is using the proxy, the federation server proxy passes the request and the credentials to the federation server.
- 5. The federation server uses AD DS to authenticate the user.
- 6. If authentication is successful, the federation server collects AD DS information about the user and generates the user's claims.
- 7. The claim is put into a security token, which is passed back to the client computer.
- 8. The client presents the token to the web server and uses the claims to access to the application.

Understanding Business Data Access



When you have a large number of users using mobile devices as their primary computing device, you have to determine the best way for those users to access data they need to perform their jobs. CERTIFICATION READY Describe business data access 5.2 Many companies must set up a VPN client that will allow users to connect to the corporate network as long as they have a connection to the Internet. They can then access internal resources just as if they are working at their desks. However, other solutions can be provided, including using the Company Portal, Work Folders, or Azure RemoteApp.

Configuring the Company Portal

The *Microsoft Intune Company Portal* provides self-service connection point for users to request help and select apps to install. It gives users the access they need to perform self-service tasks, such as adding or removing their computers from Microsoft Intune, selecting applications to install (made available to them by the Administrator), and contacting the technical support administrator.

When a user connects to the Company Portal, he has the option to install a Company Portal app on his computer from the Windows Store. This will create a tile on the user's Start screen.

When the user clicks on the tile, he needs to log in using his assigned Microsoft Intune user name and password. After he is authenticated, the Company Portal page appears (see Figure 5-5).



When the user clicks the Apps tile, he is prompted to visit the Windows Store to install the Company Portal app. After completing the installation, a new Company Portal tile is placed on the Windows 10 Start menu. The user can then access the portal through this app.

Clicking on the New Apps icon enables users to view the most recently published apps made available to them via Microsoft Intune. Selecting an app presents the user with a prompt to confirm the computer and he wants to install the app on and then perform

X REF

For more information about Microsoft Intune, refer to Lesson 4.

Figure 5-5

Viewing a sample Company Portal from the user's perspective the installation process. After it is installed, the app appears as a tile on the Company Portal page.

MORE INFORMATION

Applications can be installed on a remote computer as well as a local computer. To monitor progress, you can see the application install status on the Apps page of your Company Portal.

Customizing the Company Portal

You can modify the look and feel of the Company Portal through the Microsoft Intune Administrator console.

When customizing the portal (see Figure 5-6), information that can be customized includes:

- **Company name:** Appears as the title of your company portal.
- IT department contact name: Appears on the Contact IT tile.
- IT department phone number: Appears on the Contact IT tile.
- IT department email address: Appears on the Contact IT tile.
- Additional Information (such as hours of operation): Appears on the Contact IT tile.
- **Support website URL:** Specifies the website and website name that users can contact for support (name and URL). This can include your IT department phone number, email address, and any additional information you want to provide. Only the name, not the URL, is displayed on the Contact ID page
- **Theme color:** Customize the theme color and choose a background for the Company Portal app.

MICTOSOTU DASHBOAR GROUPS CROUPS UPDATES PROTECTIO ALERTS SOFTWARE LICENSES POLICY WITCOSOTU	Administration	Help Sign Out Welcome Regan Corpo
DASHBOAR GROUPS GROUPS UPDATES PROTECTION ALERTS SOFTWARE LICENSES POLICY	Administration	Company Portal
GROUPS GROUPS UPDATES PROTECTION ALERTS SOFTWARE LICENSES POLICY	Duopiinu	company rortal
	D Overview Updates Updates Alerts and Notifications Alert Types Recipients Notification Rules Administrator Management Service Administrators Device Administrators Device Enrollment Managers Client Software Download Storage Use Mobile Device Management P Windows Phone PiOS	Specify company name, company contact information and privacy statement The company name is displayed as the title of the Microsoft Intune company portal. The contact information and details are displayed to users in the Contact IT screen of the Microsoft Intune company portal. The privacy statement is displayed when user clicks on the privacy link. Company name: Regan Corporation IT department contact name: 916-123-4567 IT department email address: IT@ergencorp.com
E 1	 ↓ Microsoft Exchange Multi-factor Authentication NDES Connector ◆ Company Portal 	Additional information:
		Company privacy statement URL:

Figure 5-6

Customizing the Company Portal

Using Work Folders

Work Folders allow users to store and access work files on a sync share from multiple devices, including personal computers and devices (including bring-your-own devices). Work Folders are for only individual data and do not support sharing files between users. However, while these files can be accessed from anywhere, the organization maintains control over corporate files by storing the files on centrally managed file servers. To maximize accessibility, you can provide file share-based access to the files stored in a Work Folder, use Work Folders with Folder Redirection and Offline Files. In addition, since the files are stored centrally, you can back up the data on a regular basis.

Work Folders use the https protocol to transport data between devices and the Work Folders server. When you configure Work Folders for a user, you configure sync access to a specific sync share. The folder for the user is created in this sync share. When you assign a group with sync access, each user in the group is given a folder on that server. Since Work Folders client synchronizes only with a single server, you should not assign a user sync access on multiple servers.

When Work Folders is configured on a device, you have the option to wipe the Work Folders data from the device, which will remove the Work Folders data only. When the user leaves your organization, it is simple to remove the Work Folders data from all of their devices.

CREATING A WORK FOLDER

To use Work Folders, Windows Server 2012 R2/2016 uses the HTTPS protocol for performing Work Folders communication. Therefore, the Work Folder server will need to have a certificate that must be must be trusted by the Work Folders devices. In most cases, you should obtain a certificate from an external third-party CA so that it will be automatically trusted.

To create a Work Folder, you will need to install the Work Folders role and then create a Sync Share.

INSTALL THE WORK FOLDERS ROLE

GET READY. To install the Work Folders role, perform the following steps.

- 1. Using Server Manager, click Manage > Add Roles and Features.
- 2. When the Add Role and Features Wizard starts, on the Before you begin page, click Next.
- 3. On the Select installation type page, click Next.
- 4. On the Select destination server page, click Next.
- On the Select server roles page, select File and Storage Services\File and iSCSI Services\Work Folders.
- 6. When you are prompted to install additional features, click Add Features.
- 7. Back on the Select server roles page, click Next.
- 8. On the Select features page, click Next.
- 9. On the Confirm installation selections page, click Install.
- **10.** When the installation completes, click **Close**.

When you create the Sync Share, you have the following available policies:

- Encrypt Work Folders: The data on the devices is encrypted, but the data on the file server is not encrypted, which will mitigates the risk of data being accessed if a device is lost or stolen.
- Automatically lock screen, and require a password: When selected, devices using Work Folders lock the screen after 15 minutes and require a password of at least six characters to unlock. Additionally, if there are 10 unsuccessful sign in attempts, the device is locked out.

CREATE A SYNC SHARE

GET READY. To create a Sync Share, perform the following steps.

1. Using Server Manager, click **File and Storage Services > Work Folders**. Figure 5-7 shows the Work Folders page.

	Managar > File and Starage Carviges > Werk Felders
Server N	
	WORK FOLDERS
Servers	All sync shares 0 total
Volumes	There are no svnc shares.
Disks	
Storage Pools	To create a sync share for Work Folders, start the New Sync Share Wizard.
Io Shares	
iSCSI	
Work Folders	
	Last refreshed on 1/25/2015 3:32:01 PM
	USERS
	No sync share is selected.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.
	Select a sync share to display the related users.

- 2. Click the To create a sync share for Work Folders, start the New Sync Share Wizard link. Alternatively, you can click Tasks > New Sync Share.
- 3. On the Before you begin page, click Next.
- **4.** On the Select the server and path page, you can select a folder that is already shared or you can specify a local path (such as **C:\Folder1**). Click **Next**.
- 5. On the Specify the structure for user folders page, select either User alias (default) or User alias@domain. The user alias is compatible with other technologies, such as folder redirection or home folders. The alias@domain option allows you to use folder names for users across domains. Click Next.
- **6.** On the Enter the sync share name page, in the Name and Description text boxes, type a sync share name and description. Click **Next**.
- **7.** On the Grant sync access to groups page, click **Add**. In the Select User or Group dialog box, in the Enter the object name to select text box, type a username or group name and then click **OK**. Back on the Grant sync access to groups page, click **Next**.
- 8. On the Specify device policies page, you can select the following options:
 - Encrypt Work Folders
 - Automatically lock screen, and require a password
- 9. On the Confirm selections page, click Create.
- **10.** When the sync share is created, click **Close**.

Figure 5-7

Opening the Work Folders page

CONNECTING TO A WORK FOLDER

To connect to a Work Folder, the computer or device would use one of the following methods:

- Auto Discovery
- URL Entry
- Group Policy

When you use Auto Discovery, you are prompted for an email address. The domain name that is derived from the email address is prepended with Work Folders to create an URL. Therefore, if the email address is JJackson@contoso.com, the resulting URL would be https://workfolders.contoso.com. If the URL does not resolve to the server with Work Folders installed, then the Auto Discovery fails.

If you have multiple Work Folders servers, you can still use Auto Discovery by modifying the msDS-SyncServerUrl attribute on the user object using ADSIEdit. You can also modify this attribute to direct users to a new Work Folders server if you move Work Folders for a specific set of users.

If Auto Discovery fails during device configuration, you can use URL Entry, which will prompt for a URL where Work Folders are installed. This can be useful if you have multiple Work Folders servers and do not have the msDS-SyncServerUrl attribute configured on the user object. This can also be useful if you have not configured a DNS host record for Work Folders in your domain.

Another way to configure devices with the URL of a Work Folders server is to use Group Policy. You can force automatic setup for Work Folders by using a computer policy or a user policy. A user policy takes effect for specified users on all devices that they access. A computer policy takes effect for all users on that device.

The user setting is stored in Users\Policies\Administrative Templates\Windows Components\ Work Folders\Specify Work Folders. After you enable the GPO setting, you will type in the Work Folder URL (such as https://workfolders.contoso.com/sync/1.0). If you then want the policy to automatically configure with the Work Folders client, check the Force automatic setup option. You can use Microsoft Intune to deliver Group Policy Objects (GPOs) for Work Folders to devices that are not domain members.

When you use Group Policy to configure Work Folders, you have the option to force automatic setup. If you force automatic setup, users are not given the option to select where Work Folders data will be stored on the local device. Work Folders data will be stored in the default location of %USERPROFILE%\WorkFolders.

CONNECT TO A WORK FOLDER

GET READY. To connect to a Work Folder, perform the following steps.

- On a computer running Windows 10, open Control Panel and click System and Security > Work Folders.
- 2. On the Manage Work Folders page, click Set up Work Folders.
- 3. On the Enter your work email address page, in the Work email address text box, type the user's email address. Alternatively, you can click Enter a Work Folders URL and, in the Work Folders URL text box, type the Work Folders URL. Click Next.
- 4. On the Introducing Work Folders page, click Next.
- On the Security policies page, select I accept these policies on my PC and then click Set up Work Folders.
- 6. Click Close. Figure 5-8 shows the user's Work Folder.



Figure 5-8

Managing your Work Folder



Work Folders uses the https protocol to transport data between devices and the Work Folders server. By using a reverse proxy server, Work Folders can be securely used over the Internet. In addition, you can use Web Application Proxy to enhance the security of Web Folders by integrating Web Folders authentication with AD FS, which will allow you to implement multi-factor authentication and restrict connectivity to Work Folders to authorized devices.

If you integrate Microsoft Azure Multi-Factor Authentication with AD FS, you can implement the following methods for additional authentication:

- **Phone calls:** You receive a call on your phone to confirm your authentication and you press the # (pound) symbol to confirm after receiving the call.
- **Text messages:** You receive a text message with a passcode. You respond to the text message and include the passcode.
- **Mobile App:** An authentication prompt appears in the mobile app that you must acknowledge.

When Work Folders is configured on a device, you can wipe the Work Folders data from the device, which will remove the Work Folders data only. When the user leaves your organization, it is simple to remove the Work Folders data from all of the user's devices.

Since Work Folders data is stored on a file server, you can perform all of the typical file management functions using File Server Resource Manager and Rights Management Services, including quotas, file screening, classification, and Rights Management.

When you modify a file, the file is replicated very quickly. However, while it is unlikely that a user will change a file on two separate devices before replication occurs, it can happen if one of the devices is offline for an extended period. In addition, if synchronization does not occur, you should check the following:

- Work Folders does not synchronize individual files larger than 10 GB.
- Ensure that there is at least 5 GB of free space on the volume with the Work Folders.
- Ensure that Quotas is not restricting access to a Work Folder.
Understanding Azure RemoteApp

Azure RemoteApp allows you to connect to Azure cloud services using Remote Desktop Services (RDS) from your corporation on-premises. With Azure RemoteApp, users can securely access applications from different devices.

Remote Desktop Services (called Terminal Services in previous releases of Windows) is a term that describes several features of the Windows server role that enables users to remotely connect to virtual desktops, session-based desktops, and RemoteApp programs over the *Remote Desktop Protocol (RDP)*. RDP is a protocol used on the computer to render display output, which is then sent in the form of packets to the RDP client. On the client, RDP is used to send mouse and keyboard inputs to the server.

The Windows server running the RDS role includes the following services:

- *RD Virtualization Host*: Integrates with Hyper-V to enable users to connect to a VM on a server hosting Hyper-V.
- *RD Session Host*: Enables a server to host RemoteApp programs or session-based desktops.
- *RD Connection Broker*: Used for session load balancing; enables users to reconnect to a virtual desktop and RemoteApp programs, and provides access to virtual desktops in a virtual desktop collection.
- *RD Web Access*: Enables users to access RemoteApps and desktop connection via the *Start* menu or through a web browser.
- RD Licensing: Manages licenses needed to connect to the RD Session Host.
- *RD Gateway:* Enables users to connect to virtual desktops, RemoteApp programs, and session-based desktops from any device connected to the Internet.

RemoteApp programs stored on a RD Session Host server and virtual desktops hosted on an RD Virtualization Host can be remotely accessed from a client desktop. *RemoteApp* programs, which look and feel like local applications even though they are accessed remotely, can be accessed via a web console, or can be launched from the users' Start menu or when they open a file associated with the application.

To install any of these services, you will use Server Manager Add Roles and Features. When you get to the Select installation type page, you can choose between Role-based or feature-based installation or Remote Desktop Services (RDS) installation. The Role-based or feature-based installation installs all parts of roles or features on a single server; the RDS installation simplifies the deployment of an RDS infrastructure and allows you to distribute the RDS role across different servers.

When using Azure RemoteApp, you don't have to install the various Remote Desktop server roles or concern yourself with the maintenance or reliability. In addition, users from Windows, iOS, Mac OS X, and Android devices can use RemoteApp applications.

There are two kinds of RemoteApp collections:

Cloud collection: Hosted in and stores all data for programs in the Azure cloud. Users can access apps by using their Microsoft account or corporate credentials that are synchronized. They can also use accounts that are federated with Azure Active Directory.

Hybrid collection: Hosted in and stores data in the Azure cloud but also lets users access data and resources stored on the organization's local network. Users can access apps by using their corporate credentials synchronized or federated with Azure Active Directory.

Understanding Bring Your Own Device (BYOD)



Many organizations have policies in place that are designed to standardize the apps being used on company-supplied computers and do not want their users installing any applications they find, even if they are certified to work with Windows 10. *Bring Your Own Device (BYOD) policies* may also be in place that require you to control access to the Store. A BYOD policy defines the standards, restrictions and procedures for end users who have authorized access to company data from their personal devices (tablets, laptops, or smartphones). The policy also includes hardware and any related software that is not approved, owned, or supplied by the company. In either case, as the administrator, you will need to make sure your strategy for accessing the Windows Store aligns with your company's policies.

CERTIFICATION READY Describe Bring Your Own Device (BYOD) 5.3

In addition to determining your strategy for controlling access to Windows Apps and the Windows Store, you will also need to consider the deployment of *Line of Business (LOB) apps*. LOB apps include apps that are critical to running the business of the company as well as apps that are unique to the main business of the company. If you want to use the new Windows Apps format for your LOB apps, you can deploy them via the Windows Store or by a process called sideloading or deeplinking, which is explained later in this section.

If you choose to deploy your LOB apps via the Windows Store, they must go through a certification process with Microsoft to ensure they are compatible with Windows 10 and meet criteria for apps being deployed from the Store. The apps will also be available to the public, which may not be what you want. To bypass the Store requirements and make the apps available to your internal users only, consider sideloading or deeplinking them as part of your overall design strategy.

Deploying and Managing Applications by Using Microsoft Intune

Mobile devices such as smartphones and tablets are computers that can run a wide range of applications. Some organizations will require certain applications to be installed on these devices so that users of the devices can do their jobs.

As mentioned in Lesson 4, Microsoft Intune supports the mobile device management of Windows, IOS, and Android devices. In that lesson, you learned how to enroll Windows, iOS, and Android devices so that they can be managed by Microsoft Intune.

Using the Software Installer, you can perform the following actions:

- Upload a signed app package to Microsoft Intune cloud storage and make the app available to users through the Microsoft Intune Company Portal.
- Upload apps that will be deployed to computers that run the Microsoft Intune computer client.
- Install apps on managed mobile devices from an installation file, bypassing the app store (known as sideloading).

Microsoft Intune can install the following file types:

• Windows Installer (*.exe, *.msi): Used to install Windows applications. To install the Windows Installer files, you need to use the entire command with parameters (such as /q)

that installs the application silently (without user interaction). Any additional files and folders that are required by the setup program must be available from the location that you specify for the app setup files. If your application requires user interaction during setup, you will not be able to use Microsoft Intune to install the application.

- App Package for Android (*.apk file): Used to install applications on an Android device. The App Package for Android is not available as a software installer type until you set the Mobile Device Management Authority to Microsoft Intune.
- App Package for iOS (*.ipa file): Used to install iOS applications. The .ipa package must be signed by Apple and the expiration date indicated in the provisioning profile must be valid. Microsoft Intune can distribute enterprise certificate iOS applications if your enterprise is registered for the iOS Developer Enterprise Program.
- Windows Phone App Package (*.xap, .appx, .appxbundle): Used to distribute a Windows Phone 8 or 8.1 app package. The Windows Phone App Package is not available as a software installer type until you set the Mobile Device Management Authority to Microsoft Intune. You must also obtain an enterprise mobile code-signing certificate.
- Windows App Package (.appx, .appxbundle): Used to distribute a Windows appx package for Windows RT and enrolled Windows 8.1 or Windows 10 devices and is not available until you set the Mobile Device Management Authority to Microsoft Intune. You must obtain a code-signing certificate and sideloading product activation keys.
- Windows Installer through MDM (*.msi): Allows you to create and deploy Windows Installer-based apps to enrolled devices that run Windows 10.

INSTALLING WINDOWS INSTALLER AND EXECUTABLE PROGRAMS

Microsoft Intune can be used to deploy Windows installer (.msi) or executable (.exe) files that support silent installation. When deploying software using Microsoft Intune, you have two installation types:

- Automatic: A required install automatically installs or pushes the software to the managed computer and requires no user interaction.
- **Manual:** An available install publishes the software to the Windows company portal or on the mobile company portal so your users can choose whether they want to install the software.

The software you upload is stored in the Microsoft Intune cloud storage that your organization purchased. To deploy software, access the Software workspace (see Figure 5-9).

The following steps provide an overview of the process for publishing and updating software:

- 1. Prepare your software files. The .msi or .exe file must be placed in a single folder along with any supporting files on the administrator's computer.
- 2. Configure and upload the package. This requires you to type the path to the setup files, the name of the software publisher, the name of the software being deployed, a description, the required architecture (32- or 64-bit), and which operating systems the package will be installed on.

You also set the detection rule (for example, look for a specific file, registry entry, or MSI product code) to see if the software is already installed when deploying an updated package. After configuration is completed, the file is compressed, encrypted, and uploaded to the Microsoft Azure storage platform. After it is uploaded, you see the application in the Managed Software workspace.

Figure 5-9

Reviewing the Microsoft Intune Software workspace



- 3. Deploy the package. Within the Managed Software workspace, click the package to deploy and select the group to deploy the software package to. The package is now ready for your users.
- 4. Client download/installations. If the client meets all the configuration requirements you set in Step 2, it downloads the package to a temporary folder and begins the silent installation. (The client is configured via a policy to check for new downloads every 8 hours.)
- 5. Monitor the deployment status. To view the progress of installations across your managed computers, you can use the administrative console.

For many applications, the manufacturer includes options to automatically check for updates directly from the client computer. If you want Microsoft Intune to manage this process, you have to disable the manufacturer's feature on each of the managed computers.

SIDELOADING WINDOWS APPLICATIONS BY USING MICROSOFT INTUNE

Sideloading is a process for installing Windows Store applications without using the Windows Store. If you have access to the app installation files, you can sideload with Microsoft Intune. However, the application can only be deployed after the operating system is deployed. When you sideload an application, you can deploy an app to all Windows accounts on a device, or to a specific Windows account on a device.

You can use Microsoft Intune only or integrate Microsoft Intune with Configuration Manager. By using Configuration Manager, you have to install the Microsoft Intune connector. Before you can deploy or sideload your application to Microsoft Intune-managed devices, you need to upload the application into Microsoft Intune.

SIDELOAD WINDOWS STORE APPS TO MICROSOFT INTUNE

GET READY. To upload Windows Store Apps to Microsoft Intune for Windows 10, perform the following steps.

- 1. Log into the Intune website, click **Admin Console**, and then click the **Software** workspace.
- Under Tasks, click Step 1: Add Apps. If you are prompted to confirm that you want to run this Microsoft Intune Software Publisher, click Run. If you are prompted to sign in, log in with an administrator account for Intune.
- 3. In the Add Software Wizard, on the Before you begin page, click Next.
- **4.** On the Software setup page, for the Select the software installer file type option, select the Windows app package software installer type. Then in the Specify the location of the software setup files text box, specify the local or Universal Naming Convention (UNC) path to the application and then click **Next**.
- **5.** On the Software description page, in the Publisher, Name and Description text boxes, type the publisher, user-friendly name, and description of the application.
- 6. In the URL for software information text box, you can type an URL where more information about the application can be found. Lastly, you can select the category of the software and upload a picture of the software. Click **Next**.
- On the Requirements page, for the Architecture is option, specify the architecture (32-bit and/or 64-bit). For the Operating System option, select the appropriate operating system. (The default is Any for both options.) Click Next.
- 8. On the Detection Rules page, specify the rules to detect whether the software is already installed by selecting Detect whether the software is installed by using the following rules (recommended). Click the Add Rule option and then select one or more of the following options:

File exists

MSI product code exists

Registry key exists

- **9.** Based on the option selected, specify the file, MSI product code, or the registry key in the appropriate text boxes. Click **Next**.
- **10.** On the Command line arguments page, click **Next**.
- 11. On the Return codes page, click Next.
- **12.** On the Summary page, click **Upload**.
- 13. When the software is uploaded, click **Close**.

After the application is uploaded into Microsoft Intune, you can deploy the application to Microsoft Intune groups, which can contain users or devices that Microsoft Intune manages.



SIDELOAD WINDOWS STORE APPS IN WINDOWS 10 USING MICROSOFT INTUNE

GET READY. To sideload Windows Store Apps in Windows 10 using Microsoft Intune, perform the following steps.

- 1. Log into the Intune website, click **Admin Console**, and then click the **Apps** workspace.
- 2. Click Managed Software (see Figure 5-10).

Figure 5-10

Managing software with Microsoft Intune

	nanage.microsoft.com/Microsof	ftIntune/Home?accountid=d551d2d2-9a28-42b2-9a9f	-82a0c98d9bb9#Wc Q - 🖨 C	crosoft lotune X	- - ×
Microsoft Intune	,			Help Sign Out Welcome	Regan Corporation
DASHBOARD	Apps Overview Detected Software	Apps (1) View Properties Add Agreements 🔻	Filters: None Manage Deployment Add App	Search Edit Delete	م ا
GROUPS	Apps	Name ReportViewer.exe	Publisher Microsoft	Installer Type Size Windows installer (*.exe, * 4.52 MB	Deployed No
ALERTS					
APPS					
LICENSES					
POLICY		ReportViewer.exe	C		~
REPORTS		No issues	General Inf Description Publisher:	s ReportViewer.exe Microsoft	
ADMIN			Size: Installer Ty Last Updat Deployed:	4.52 MB be: Windows installer (*.exe, *.msi) bd: 3/16/2015 6:31:33 PM No	
Microsoft © 2015 N	Aicrosoft. All rights reserved Pr	rivacy & Cookies Feedback			Remote Tasks

3. Click Managed Deployment.

- **4.** In the Deploy Software Wizard, on the Select Groups page, click the group that you want to deploy to and then click **Add**. Click **Next**.
- **5.** On the Deployment Action page, under Approval, select **Required Install** from the pull-down menu.
- 6. Click Finish.

DEEPLINKING WINDOWS APPLICATIONS BY USING MICROSOFT INTUNE

With *deeplinking*, you can identify an application in the Windows store that you want to deploy to Window's 8.1 and a link will be provided to the user that will take him directly to the app in the Windows store. By deeplinking, the user will not have to search for the specific app and potentially load the wrong app.

To deeplink an application, you will need to know the URL of the application. You will run the Add Software Wizard to specify the URL from which users can install the application. You will then use the Manage Software task to deploy the application to the users.

Ð

DEEPLINK A WINDOWS STORE APP IN WINDOWS 10 USING MICROSOFT INTUNE

GET READY. To deeplink a Windows Store App in Windows 10 using Microsoft Intune, perform the following steps.

- 1. Log into the Intune website, click **Admin Console**, and then click the **Software** workspace.
- 2. Under Tasks, click **Step 1: Add Software**. If you are prompted to confirm that you want to run this Microsoft Intune Software Publisher, click **Run**. If you are prompted to sign in, log in with an administrator account for Intune.

- 3. In the Add Software Wizard, on the Before you begin page, click Next.
- For the Select how this software is made available to devices option, select External link. In the Specify the URL text box, type the URL of the application and then click Next.
- On the Software description page, in the Publisher, Name and Description text boxes, type the publisher, user-friendly name, and description of the application.
- 6. On the Summary page, click Upload.
- **7.** When the software is uploaded, click **Close**.

CONFIGURING APPLICATION DEPLOYMENT POLICIES

Most experienced Windows users know how to install an application. You insert a CD or DVD in a drive and the application installation automatically starts or you double-click an installation file (such as file that has an .exe or .msi filename extension). Deploying software to hundreds of computers within your organization can be a chore. However, if all of the computers are connected to a network, you can use Group Policy to install, manage, and maintain software for your organization, particularly computers or devices that are part of the Active Directory domain.

The Windows Installer is a software component used for the installation, maintenance, and removal of software on Windows. The installation information for software is stored in a Microsoft Software Installation (MSI) file in a database installation file that has an .msi filename extension. Besides performing installation, msi files can be used in self-healing for damaged applications and to remove an application cleanly.

Besides installing MSI files with group policies, you can also install MSI transform files (.mst) and MSI patch files (.msp). MSI Transform files are used to deploy customized MSI files. For example, you can install Microsoft Office, which consists of multiple applications. You can create a transform file using the Custom Installation Wizard that is included with Microsoft Office so that you can install all the applications except Microsoft Access.

MSI Patch files are used to apply service packs and hot fixes to installed software. Rather than having a complete database found with MSI files, a patch file contains a minimum of a database transform procedure that adds patching information to the target installation package database.

Windows Installer cannot install .exe files. To distribute a software package that installs with an .exe file, you must convert the .exe file to an .msi file by using a third-party utility or you will need to define a ZAP file (a file with a .ZAP filename extension). ZAP files are created with a text editor, such as Notepad, and they can only be published (not assigned).

MANAGING OUTLOOK APPS

Microsoft Intune includes the *Microsoft Intune Mobile Application Management (MAM)*, which provides manageability and data protection to the Office mobile applications. With MAM, you can restrict access (such as disabling cut, copy, paste, and Save as capabilities) when managing corporate data between Intune-managed Outlook apps and personal apps (such as personal email, Twitter, and Facebook) and you can enable the copying/pasting and Saving as of corporate data to corporate email or corporate applications. You can also prevent users from capturing screenshots and you can require a PIN or corporate credentials to be entered before users can access corporate content.

You can also restrict unmanaged and non-compliant devices from accessing Exchange Online. When users attempt to log in with their corporate accounts from unmanaged mobile devices, they will be prompted to enroll their devices in Microsoft Intune. In addition, Outlook now supports Intune MAM's selective wipe feature, whereby corporate data is deleted when the Outlook app is retired or unenrolled. To use MAM to manage Outlook Apps, perform the following steps: Step 1: Create a mobile application management policy. Step 2: Add Outlook to your Intune app catalog.

Step 3: Deploy Outlook with your MAM policy.

Understanding Device-Centric to People-Centric IT

When looking at managing the devices of an organization, you can configure policies based on devices or based on users. For example, when installing software with Group Policy, you can install software based on a computer or based on a user.

In the past, users would typically use one computer and they would be the only user using that computer. Therefore, the IT department was focused on managing users when it came to configuring the systems and installing applications.

However, with advances in technology, users can now have a desktop computer and a mobile device (such as a laptop, tablet, or smart phone), all of which will access applications, emails, and other resources. Some of these devices might be owned by the corporation and others might be owned by users. Therefore, the configuring of these device and the installing of applications focus on people-centric IT.

You can join Windows 10 devices by using one of the following methods:

- *Workplace Join* allows users to join their devices to the organization network without joining the device to the Active Directory domain. You can then manage their access based on a wide range of attributes. You can use Workplace Join to join Windows 7, Windows 8/8.1, and Windows 10 devices.
- *Azure AD (AAD) Join* allows you to join Windows 10 devices in Azure AD and users can then sign into Windows using their Azure Active Directory accounts and passwords while having Single Sign-On (SSO) access to Office 365 and to on-premises services that use Active Directory authentication. The device can be automatically enrolled into a Mobile Device Management service (such as Microsoft Intune) at the same time. When you log on to the Microsoft Azure portal, you must enable device registration for Azure AD by selecting Configure for AAD and, for the Enable workplace join option, selecting Yes.

When you join a device using Workplace Join, *Device Registration Service (DRS)* registers a non-Domain Joined device in Active Directory and installs a certificate on the device. By joining the device, Workplace Join provides a secure SSO mechanism while controlling which resources can be accessed by the device.

When the user joins the devices using Workplace Join technology, the device becomes a known device. To use Workplace Join, you must have Windows Server 2012 R2/2016 with the AD FS role service installed. In addition, the client must be using the Windows 10 or 8.1 client operating system or iOS-based devices (such as an iPad).

The certificate will be used to represent device identity when accessing organization resources. When accessing resources on the organization, the SSO allows the user to be prompted for her domain credentials only once during the lifetime of the SSO session. However, an administrator can specify resources that enforce a password prompt or reauthentication.

To support Workplace Join, you'll need to install and configure AD FS and the new Device Registration Service. To configure the Device Registration Service, execute the following Windows PowerShell commands:

Initialize-ADDeviceRegistration

Enable-AdfsDeviceRegistration

Then open the AD FS Management console, navigate to Authentication Policies, click Edit Global Primary Authentication, click to select the Enable Device Authentication, and then click OK. Lastly, the client must trust the SSL certificate that is used for the federation server and must be able to validate certificate revocation information for the certificate.

JOIN A DEVICE

GET READY. To join a device, perform the following steps.

- 1. Log in to the client device with a Microsoft account.
- 2. On the Start screen, open the Charms bar, click the **Settings** charm, and then click **Change PC Settings**.
- **3.** On the PC Settings page, click **Network > Workplace**.
- In the Enter your UserID to get workplace access or turn on device management dialog box, type the user name (such as JSmith@contoso.com) and then click Join.
- **5.** When prompted for credentials, type the username and the associated password and then click **OK**. You should now see the message This device has joined your workplace network.

Understanding Desktop Virtualization

A *Virtualization Host Infrastructure*, also referred to as *Virtual Desktop Infrastructure (VDI)*, consists of virtual desktops running on Remote Desktop Services and Hyper-V to provide users with access to virtual desktop collections made up of personal or pooled virtual desktops and RemoteApp programs. The virtual desktops are virtual machines running Windows client operating systems such as Windows 10 and are accessed using the RDP.

RD Virtualization Host is ideal in scenarios where users need the flexibility of a full desktop rather than individual applications. There are two types of virtual desktop collections available:

- **Personal:** In a personal desktop collection scenario, each user is assigned to his own virtual machine.
- **Pooled:** In a pooled desktop collection scenario, users share virtual machines that are available with a pool of VMs.

Virtual machine-based desktop deployment is comprised of RD Virtualization Host, RD Connection Broker, and RD Web Access. The RD Gateway and RD Licensing role services can be deployed after initial configuration to provide remote users access to resources within your corporate network and RDS License management for remote users and devices.

RD Virtualization Host integrates with Hyper-V to provide pooled or personal virtual desktop collections. If Hyper-V isn't already installed, it will be installed during the role services deployment. Since the RD Virtualization Host role service requires Hyper-V, it must be installed on a physical server and cannot be virtualized. You will need to ensure that hardware virtualization support is enabled in the BIOS or the deployment will fail. The Virtual Machine-based deployment allows users to connect to virtual desktop collections that include published RemoteApp programs and virtual desktops. RD Virtualization Host is ideal in scenarios where users need the flexibility of a full desktop rather than individual applications.

When you begin the virtualization host deployment, identify where each server role will be placed and based off of your requirements determine the proper deployment scenario to follow:

- **Quick Start:** If you have a small-scale or low-intensive deployment, the Quick Start deployment will set up all roles services and publish a collection to a single server.
- **Standard:** If you need to deploy roles across multiple servers or have a specialized deployment, choose the Standard deployment type.

RD Virtualization Host deployment can be started from the Add Roles And Features Wizard with Server Manager. The deployment types are the same as an RD Session Host deployment (the types are Quick Start or Standard deployments). For the deployment scenarios, you will need to choose to perform a virtual machine-based deployment. Select the servers to host each role service for your deployment: RD Connection Broker, RD Web Access, and RD Virtualization Host.

Once the RD Virtualization Host has been provisioned, you must create the virtual machine to be used as the master image before a collection has been created. This master image will be used to create all other virtual machines in the VDI deployment. The master virtual machine must run either Windows 7 Service Pack 1 or Windows 10/8.1/8 to be supported in a Hyper-V virtual environment. To begin creating the image, you can use Hyper-V manager to run the new virtual machine wizard to create the virtual machine you will use for the master image.

You can use the new virtual machine wizard to begin creating the virtual machine within Hyper-V and install the operating system. Once the operating system has been installed, customize the virtual machine based off of your organizational requirements. The customization should include installing required updates, applications, and any needed desktop configurations. If the virtual machine will be used in a pool where RemoteFX-enabled virtual desktops are needed, add the RemoteFX 3d video adapter to the VM using the Hyper-V manager. Once all configuration and customization of the virtual machine has been completed, you will run the sysprep.exe utility with the Generalize option and shut down the VM. The generalize option will remove system specific data, which includes event logs, unique SIDs, and other information unique to the system.

Before you can create a RD Virtualization Host collection you must have created and used the sysprep tool on a virtual machine that will act as the master image for all virtual machine deployments within a VDI collection. To begin creating a new collection, you will run the Create Virtual Desktop Collection Wizard, which will include:

- Specifying which template to use
- Configuring virtual desktop settings
- Configuring the unattended settings, including specifying the Active Directory organization unit that the virtual desktop will reside
- Configuring the users and groups that can access the collection
- Specifying the number of virtual machines to create in the collection
- Configuring the prefix or suffix characters that should be added to the name of each virtual desktop.
- Configuring the assigned memory, CPU and number of virtual machines to create on specific RD Virtualization Hosts.
- Configuring the location of where to store the VMs, which can be local storage, remote storage on an SMB share, or storage on a Cluster Shared Volume (CSV).
- If user profile disks are enabled, specifying storage location and maximum allowed size. The default size of user profile disks is 2GB. (User profile disks aren't available for personal VMs.)

Understanding Dynamic Access Control (DAC) Policies

Dynamic Access Control (DAC), originally called *claims-based access control*, is used for access management. It provides an automatic mechanism to secure and control access to resources.

Claims-based access control uses a trusted identity provider to provide authentication. The **trusted identity provider** issues a token to the user, which the user then presents to the application or service as proof of identity. Identity is based on a set of information. Each piece of information is referred to as a **claim** (such as who the user or computer claims to be) and is stored as a token, which is a digital key. The **token** is a form of digital identification for the user or computer that is accessing a network resource. The token has a digital signature of the identity provider to verify the authenticity of the information stored within the token. As a user or computer needs access to a resource, the user or computer presents the token to get access to the resource.

In Windows Server 2012 R2/2016, the identity provider is the *Security Token Service (STS)* and the claims are the Active Directory attributes assigned to a user or device (such as a computer). The claims, the user's SID, and group membership are stored inside the Kerberos ticket. The ticket is then used to access protected resources. Of course, claims authorization relies on the Kerberos Key Distribution Center (KDC).

In Windows Server 2012 R2/2016, DAC allows you to perform the following:

- Identify data by using automatic and manual classification or tagging files in an organization.
- Control access to files by applying automatic policies that are controlled by Central Access Policies.
- Audit access by using a Central Audit Policy to ensure compliance and to be used in forensic analysis.
- Use Windows Rights Management Service (RMS) to encrypt sensitive documents.
- Offer Access-Denied Assistance, which provides a method for users to request access from the owner of data when he or she is denied access.

To use claims-based authorization, you need the following:

- Windows Server 2012/2012 R2/2016 must be installed on the file server that hosts the resources that DAC protects.
- At least one Windows Server 2012 or higher domain controller must be accessible by the requesting client.
- If you use claims across a forest, you must have a Windows Server 2012 or higher domain controller in each domain.
- If you use device claims, clients must run Windows 10.

When you enable DAC, you have the option to support claims, compound authentication, and armor Kerberos. Compound authentication is an extension to Flexible Authentication Secure Tunneling (FAST), which allows Kerberos to create service tickets to devices. Kerberos armoring fully encrypts Kerberos messages and signs Kerberos errors. Although Kerberos armoring enhances security, it also increases processing time. **ENABLE DAC FOR ACTIVE DIRECTORY DOMAIN SERVICES**

GET READY. To enable DAC for Active Directory Domain Services (AD DS), perform the following steps.

- 1. To enable AD DS for DAC, create a new Group Policy Object (GPO) and link the GPO to the Domain Controllers organization unit (OU) or edit the Default Domain Controllers Policy GPO. Using Server Manager, click Tools > Group Policy Management.
- 2. In the Group Policy Management console, double-click the GPO assigned to the Domain Controllers OU that you want to use to enable DAC.
- 3. In the Group Policy Management Editor, navigate to **Computer Configuration** Policies\Administrative Templates\System\KDC and double-click KDC support for claims, compound authentication and Kerberos armoring.
- 4. Click Enabled.
- 5. Under Options, Supported is already selected.
- 6. Click OK to close the KDC support for claims, compound authentication and Kerberos armoring dialog box.
- 7. Close the Group Policy Management Editor.

CONFIGURING USER AND DEVICE CLAIM TYPES

After you enable support for DAC in AD DS, you must create and configure claims and resource property objects. To create and configure claims, you primarily use the Active Directory Administrative Center.

The most common types of claims are attribute-based claims, which are usually configured with Active Directory Administrative Center, specifically using the Dynamic Access Control node (see Figure 5-11). All claims are stored in the configuration partition in AD DS, which is a forest-wide partition. As a result, all domains in the forest share the claim dictionary.

Strative center	Active Directory <	Dynamic Access Control (5)			Tasks
		Filter	◄ (#) ▼ (#)	\odot	Central Access Policies
	Contoso (local)	Name Resource Property Lists Central Access Policies Central Access Rules Claim Types Resource Properties	Type Description Container msAuthz-C msDS-Clai msDS-Reso		New Search under this node Properties Dynamic Access Control New Search under this node Properties
		Central Access Policies		~	
		Object class: msAuthz-CentralA Description:	ccessPolicies Modified: 12/13/2014 5:25 PM		

Figure 5-11

Managing DA **Directory Adm** To create a claim type, you specify a specific attribute from Active Directory. Of course, for DAC to be effective, Active Directory must contain accurate information. By default, the claim name is the name of the selected attribute name. However, you can modify this to give a more meaningful name. Lastly, you have the option to provide suggested values for the claim.

CREATE A CLAIM TYPE

GET READY. To create a claim type, perform the following steps.

- 1. Open Server Manager.
- Click Tools > Active Directory Administrative Center. The Active Directory Administrative Center opens.
- 3. Navigate to the Dynamic Access Control node and click the Claim Types container.
- **4.** In the Tasks pane, under Claim Types, click **New**, and then click **Claim Type**. The Create Claim Type dialog box opens.
- With User already selected on the right side of the dialog box, under Source Attribute, scroll down and click department.
- 6. For the display name, to give a more meaningful name, type **Company Department** and click **OK**. An entry for Company Department is listed under Claim types.
- **7.** Click **OK** to close the Create Claim Type dialog box. The description claim type appears.

After you create the claim types, you must configure the resource property objects (such as a folder or a file) using the Active Directory Administrative Center. You can create your own resource property or you can use preconfigured properties, such as Project, Department, or Folder Usage. If you choose to use a preconfigured property, they are disabled by default. Therefore, you have to enable the preconfigure property.

ENABLE RESOURCE PROPERTIES

GET READY. To enable a resource property, perform the following steps.

- 1. With Active Directory Administrative Center, navigate to and click the **Dynamic Access Control** node. Next, double-click **Resource Properties**.
- 2. To enable the Department resource property, under Resource Property, right-click **Department** and choose **Enable**.
- **3.** To enable the Confidentiality resource property, under Resource Property, right-click **Confidentiality** and choose **Enable**.
- **4.** To view the Confidentiality settings, double-click **Confidentiality**. The Confidentiality dialog box opens.
- 5. Click Cancel to close the Confidentiality dialog box.
- 6. Close Active Directory Administrative Center.

CONFIGURING FILE CLASSIFICATION

When planning DAC implementation, you should include file classification. Although file classification is not mandatory for DAC, it can enhance the automation of access control because it can be used to identify documents that you need to protect and classify them appropriately.

Classification management and file management tasks enable administrators to manage groups of files based on various file and folder attributes. After folders and files are classified, you can automate file and folder maintenance tasks, such as cleaning up stale data or protecting sensitive information. Although classification management can be done manually, you can automate this process with the File Server Resource Manager console.

Classification rules can be created and then scheduled to be applied on a regular basis so that files are automatically scanned and classified based on the content of the file. When you want to perform file classification, you need to determine the following:

- The classifications that you want to apply to documents
- The method that you will use to identify documents for classification
- The schedule for automatic classifications

Of course, to determine the success of the classification, you have to establish periodic reviews.

To manually configure a folder with a classification, you can right-click the folder and choose Properties. When the Properties dialog box opens, you can then choose the name of the classification and select the appropriate value. For example, you can select Department and then click Human Resources. Then all documents within the folder will automatically be classified as the department of Human Resources.

After DAC is configured, you can use it to apply permissions based on a condition. For example, if the user's department is set to Human Resources, you can grant specific permissions based on a user's assigned department, as shown in the next exercise.

E

IMPLEMENT CONDITIONAL ACCESS ON A FOLDER'S ACL

GET READY. To implement conditional access on a folder's ACL, perform the following steps.

- 1. Using Windows Explorer, right-click a folder and choose **Properties**. The Properties dialog box opens.
- 2. Click the Security tab.
- 3. Click the Advanced button. The Advanced Security Settings dialog box opens.
- 4. Click Add. The Permission Entry for Data dialog box opens.
- **5.** Click **Select a principal**. In the Select User, Computer, Service Account, or Group dialog box, type the name of the user or group and then click **OK**.
- 6. Select the Basic permissions as necessary.
- **7.** At the bottom of the dialog box, click **Add a condition**.
- **8.** For the condition, you can then configure the following:

Resource > Department > Equals > Value > Human Resources (see Figure 5-12). Click **OK**.

- **9.** Back in the Advanced Security Settings dialog box, the condition is displayed. Click **OK** to close the Advanced Security Settings for Data dialog box.
- **10.** Click **OK** to close the Properties dialog box.

IMPLEMENTING A CENTRAL ACCESS POLICY

Similar to file classification, a Central Access Policy is not mandatory for DAC. However, it is recommended to implement at least one Central Access Policy.

Configuring a condition for an ACL

	Permission Entry for Data	- • ×
Principal:	John Smith (JSmith@contoso.com) Select a principal	
Type:	Allow	
Applies to:	This folder, subfolders and files \checkmark	
Basic permi	sions:	Show advanced permissions
	Full control	
	Modify	
	Read & execute	
	✓ List folder contents	
	✓ Read	
	Write	
	Special permissions	
Only app	v these permissions to objects and/or containers within this container	Clear all
	y these permissions to objects and, or containers within this container	
Add a cond	tion to limit access. The principal will be granted the specified permissions only if conditions are met.	0
Add a cond	tion	Remove
		OK Cancel

Files stored in shared folders are data files that need to be accessed by multiple users. However, when you apply shared and NTFS permissions, the permissions apply to all files in a specific folder. Unless you constantly monitor the folder and modify the permissions for the folder or the individual files in the folder, the shared and NTFS permissions might not always be a good fit to keep the files secure.

A *Central Access Policy* is a policy that contains *Central Access Rules* that grant permissions to objects for a defined group of resources. By default, the rules apply to all resources, but you can limit the resources to which the rule will apply. Once the rule is defined, you can choose to apply it live or you can choose to use a "staging" mode.

Before you implement a Central Access Policy, you should do the following:

- 1. Identify the resources that you want to protect.
- 2. Define the authorization policies.
- 3. Translate the authorization policies into expressions.
- 4. Determine which claim types, resource properties, and device claims must be created to deploy the policies.

If you have one file server or one folder, you don't necessarily need to implement a Central Access Policy. Instead, you can implement conditional access on the folder's Access Control List (ACL). If you have resources across multiple servers or multiple folders, you will most likely benefit from a Central Access Policy.

In the following exercise, you will create a Central Access Rule that grants permissions to files in a folder that is classified as Confidentiality – High.



CREATE A CENTRAL ACCESS POLICY

GET READY. To create and apply a Central Access Policy, perform the following steps.

- 1. In the Active Directory Administrative Center, navigate to and click the **Dynamic** Access Control node. Then double-click Central Access Policies.
- Under Tasks, click New and then click Central Access Policy. The Central Access Policy dialog box opens.
- 3. In the Name text box, type a name of the Central Access Policy.
- 4. Under the Member Central Access Rules section, click Add.

- **5.** Because you do not have a Central Access Rule defined, click **Add a new central access rule**.
- 6. In the Create Central Access Rule dialog box, in the Name text box, type a name to identify the rule.
- 7. Under Target Resources, click Edit. The Central Access Rule dialog box opens.
- 8. For the condition, specify the following:

Resource > Confidentiality > Equals > Value > High

Click **OK** to close the Central Access Rule dialog box.

- 9. Click OK to close the Create Central Access Rule dialog box.
- **10.** Back in the Central Access Rule dialog box, the rule should be shown in the right pane. Click **OK** to close the Add Central Access dialog box.
- 11. Click OK to close the Create Central Access Policy dialog box.
- 12. Click Cancel to close the Confidentiality dialog box.
- 13. Close the Active Directory Administrative Center.

You can also take this a step further and specify that access is granted only if the user is part of the Human Resources department:

Resource > Department > Equals > Value > Human Resources

Understanding Windows Rights Management (RMS)

Windows RMS and Azure Rights Management are used to provide an extra level of security to email and Microsoft Office documents by using encryption to limit who can access a document or email and what can be done with a document or email. RMS also offers plug-in capability for other file formats, but the plug-ins are not widely used. For example, you determine whether a document or web page can be printed, copied, edited, forwarded, or deleted. RMS helps protect confidential information and controls who can access the data.

As mentioned in Lesson 3, as cloud service, Office 365 or Azure Directory allows users to easily access and share documents within the organization or with users in other organizations without requiring a Virtual Private network (VPN) connection. Organizations that do not use Office 365 or Azure Directory can use the free version of RMS for individual subscriptions. Since the information that you are encrypting with RMS can be confidential, Windows RMS provides a great tool for protecting it and should be covered in your BYOD policy.

SUMMARY SKILL MATRIX

IN THIS LESSON YOU LEARNED:

- Identity services provides credentials that can be registered with an Access Control Service (ACS), such as Microsoft Azure, that allows users to authenticate directly with an ACS and receive a token for accessing the ACS. The ACS may contain many service identities.
- A directory service stores, organizes, and provides access to information in a directory. Directory services are used for locating, managing, administering, and organizing common items and network resources, such as volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. One popular directory service used by many organizations is Microsoft's Active Directory.

X REF

For more information about Windows RMS, refer to Lesson 3.

- Azure Active Directory (AD) is a cloud-based IaaS that you can use for identity management and access control. Microsoft Azure AD has been the identity provider for Office 365 since before Microsoft Azure AD was made available to the public.
- The Active Directory Federation Services (AD FS) role allows administrators to configure SSO for web-based applications across a single organization or multiple organizations without requiring users to remember multiple usernames and passwords, although it is not required. This enables you to configure Internet-facing business-to-business (B2B) applications between organizations.
- The Microsoft Intune Company Portal provides self-service connection point for users to request help and select apps to install. It gives users the access the need to perform self-service tasks, such as adding or removing their computers from Microsoft Intune, selecting applications to install (made available to them by the Administrator), and contacting the technical support administrator.
- Work Folders allow users to store and access work files on a sync share from multiple devices, including personal computers and devices (including bring-yourown devices).
- Azure RemoteApp allows you to connect to Azure cloud services using Remote Desktop Services (RDS) from your corporation on-premises. With Azure RemoteApp, users can securely access applications from different devices.
- Bring Your Own Device (BYOD) policies may also be in place that require you to control
 access to the Store. A BYOD policy defines the standards, restrictions and procedures for
 end users who have authorized access to company data from their personal devices
 (tablets, laptops, or smartphones).
- Sideloading is a process for installing Windows Store applications without using the Windows Store. If you have access to the app installation files, you can sideload with Microsoft Intune.
- With deeplinking, you can identify an application in the Windows store that you want to deploy to Windows 10 and a link will be provided to the user that will take him directly to the app in the Windows store. By deeplinking, the user will not have to search for the specific app and potentially load the wrong app.
- Workplace Join allows users to join their devices to the organization network without joining the device to the Active Directory domain. You can then manage their access based on a wide range of attributes.
- Azure AD (AAD) Join allows you to join Windows 10 devices in Azure AD and users can sign into Windows using their Azure Active Directory accounts and passwords while having Single Sign-On (SSO) access to Office 365 and to on-premises services that use Active Directory authentication.
- A Virtualization Host Infrastructure, also referred to as Virtual Desktop Infrastructure (VDI), consists of virtual desktops running on Remote Desktop Services and Hyper-V to provide users with access to virtual desktop collections made up of personal or pooled virtual desktops and RemoteApp programs.

Knowledge Assessment

Fill in the Blank

- **2.** To simplify administration when assigning rights and permissions to multiple users, you should always use _____.

- **3.** To use SSO for a web-based application that is hosted by partner company and your company Active Directory, you should use _____.
- 4. When you use Active Directory Federation Services (AD FS), the organization that contains the user accounts that access the resources is known as the ______
- The easiest way for a user with a smartphone running Windows 10 to access your Microsoft Intune Company Portal is to install the ______ from the Windows Store.
- 6. ______ allow a user to use his personal computer from home to access company documents from a sync share.
- 7. _____ is the process for installing Windows Store applications through Microsoft Intune instead of the Windows Store.
- **8.** Although sideloading can be used to install the application using Microsoft Intune, you can provide a link to install the application by using _____.
- When creating a Central Access Policy for Dynamic Access Control, you have to define ______ that grant permissions to objects for a defined group of resources.
- When using Windows RMS, a ______ includes user domains that can access Windows RMS.

Multiple Choice

Circle the letter that corresponds to the best answer.

- 1. Which of the following allows an SSO when deploying an application for another organization on your network?
 - **a.** Active Directory Domain Services (AD DS)
 - **b.** Windows Rights Management Services (RMS)
 - c. Active Directory Lightweight Directory Services (AD LDS)
 - d. Active Directory Federation Services (AD FS)
- **2.** Which of the following is a statement made by a trusted entity for a user that includes key information to identity the user?
 - a. store
 - **b.** delegated party
 - **c.** proxy
 - **d.** claims
- 3. Which of the following is the application that accepts claims from a claim provider?
 - **a.** claims provider
 - **b.** relying party
 - **c.** attribute store
 - d. federation server proxy
- 4. Which of the following is the server that issues claims and authenticates users?
 - **a.** claims provider
 - **b.** relying party
 - **c.** attribute store
 - d. federation server proxy
- 5. In AD FS, which claim provider is used by default?
 - a. Active Directory
 - **b.** AD LDS
 - **c.** SQL database
 - d. Oracle database

- 6. Which task cannot be performed when using the Microsoft Intune Company Portal?
 - **a.** Adding a computer to Microsoft Intune
 - **b.** Removing a computer from Microsoft Intune
 - c. Contacting Technical Support
 - **d.** Installing Windows applications made available to other users by the Microsoft Intune Administrator
- 7. Which of the following allows you to store and access work files from a sync share, which can then be accessed from multiple devices (including bring-your-own devices)?
 - **a.** Offline folders
 - **b.** Folder redirection
 - c. Work Folders
 - d. Central Placement
- 8. Which of the following are methods to connect to a Work Folder? (Choose three answers)a. Group Policy
 - **b.** URL entry
 - c. Auto Discovery
 - d. ActiveSync Policy
- **9.** You have several files and more will be added in the future. You want to define the NTFS permissions for files that contain the word "legal" for users who are part of the Legal department. What should you do?
 - **a.** Enable and configure EFS
 - **b.** Enable and configure DAC
 - **c.** Enable and configure BitLocker
 - **d.** Enable and configure DRA
- 10. Which of the following is the primary naming service used in Windows?
 - a. AD
 - **b.** WINS
 - c. DNS
 - d. DHCP
- 11. Which group scope is meant to be used to assign permissions to a local resource?
 - a. Distribution group
 - **b.** Domain local
 - c. global
 - d. Captured
- 12. Which of the following authorizes a user to perform certain actions on a computer?
 - a. Permission
 - **b.** UNC
 - c. Right
 - d. Task
- **13.** Which of the following can be used to assess an application that is hosted on another computer, but the application looks like it is running locally?
 - **a.** Hyper-V
 - **b.** Remote Access
 - c. Remote Desktop
 - **d.** RemoteApp
- 14. Which of the following allows you to connect to the Azure cloud using Remote Desktop Services from your corporation on-premises?
 - a. Azure RemoteApp
 - **b.** Remote Desktop Connections
 - c. RD Web Access
 - d. RD Gateway

- **15.** Which of the following should be developed before you allow users to use their own smartphones to access company email?
 - **a.** A DRS policy
 - **b.** A Share policy
 - **c.** A LOB policy
 - **d.** A BYOD policy

Case Projects

Scenario 5-1: Deploying Software to Windows Mobile Phones

You need to deploy a mobile device for a timesheet application. Describe the best way to install the software to the mobile phones.

Scenario 5-2: Creating a Federation Partnership

You are an administrator for the Contoso Corporation, which is partnering with Litware.com. Describe how to deploy an application that the users of Litware can access over the Internet to order products from Contoso.

Scenario 5-3: Securing Smartphones and Tablets

You are an administrator for the Contoso Corporation. You have about 30 users who own Windows 10 mobile devices. Your company decided to implement a BYOD policy. Describe how to control mobile device access to resources.

Scenario 5-4: Allowing Access to an Encrypted Repository

You are an administrator for the Contoso Corporation, which already has a SharePoint file repository that is protected with Windows Rights Management. You have recently developed a partnership with litware.com, which needs access to some of these documents. Describe how to provide Litware users with access to the encrypted documents.

Appendix A Mobility and Devices Fundamentals: Exam 98-368

Ехам Овјестіvе	Skill Number	Lesson Number
Understanding Device Configurations		
Configure device options	1.1	1
Configure desktop settings	1.2	1
Configure drive encryption	1.3	1
Configure updates	1.4	1
Understanding Data Access and Management		
Describe cloud storage services	2.1	2
Describe local storage	2.2	2
Describe file systems	2.3	2
Describe file and print sharing	2.4	2
Describe data encryption	2.5	2
Understanding Device Security		
Describe the differences between the Internet, an intranet, and an extranet	3.1	3
Describe user authentication	3.2	3
Describe permissions	3.3	3
Describe malware	3.4	3
Understanding Cloud Services		
Describe the types of cloud services	4.1	4
Describe Microsoft Intune	4.2	4
Describe Microsoft Azure	4.3	4
Understanding Enterprise Mobility		
Describe identity services	5.1	5
Describe business data access	5.2	5
Describe Bring Your Own Device (BYOD)	5.3	5

Index

Α

Access control entry (ACE), 62 Access Control List (ACL), 62 implementing conditional access, 178 Accounting, 102 Account organizations, 157 Action Center, 18 Active Directory accounts, 6 Active Directory Certificate Services (AD CS), 87 Active Directory Domain Services (AD DS), 107, 147, 178 Active Directory Federation Services (AD FS), 156–157 account organizations, 157 complicated scenario, 158 components, 157-158 federated trust relationship, 157 resource organizations, 157 simplest scenario, 158 for single organization, 158 Active Directory forest, 147 Active Directory permissions, 107 Active Directory Rights Management Services (AD RMS). See Windows Rights Management Services Administrative Tools, 10 Advanced Encryption Standard (AES), 83 Advanced permissions, 109 Advanced sharing, 68 Adware, 112, 113 Allow permissions, 66 Application update, 40 Asymmetric key, 80 Attribute-based claims, 176 Attribute store, 158 Auditing, 102 Authentication, 102. See also User authentication Authentication token, 104 Authorization, 102 Azure Active Directory (Azure AD), 139, 155–156 Azure Active Directory Sync (DirSync) tool, 156 Azure RemoteApp, 165 Azure Rights Management (Azure RMS), 105 Azure storage, 55–56

В

Backdoors, 114 Base64-encoded X.509, 86 Basic permissions, 108 Basic sharing, 68 Billing Administrator, 53 Biometrics, 104–105 BitLocker configuration, 33–37

BitLocker Control Panel applet, 36–37 BitLocker Drive Encryption (BDE), 33 operational modes, 34-35 system requirements, 34 TPM security, 35-36 turning ON, 36 BitLocker Drive Encryption (BDE), 33 BitLocker To Go, 88 Bring Your Own Device (BYOD), 166-180 configuring application deployment policies, 171 deploying application, Microsoft Intune, 166–172 Desktop Virtualization, 173-174 Device-Centric to People-Centric IT, 172-173 Dynamic Access Control (DAC) policies, 175-180 Microsoft Intune Mobile Application Management (MAM), 171-172 Windows Rights Management (RMS), 180 Brute force attacks, 103 Buffer overflow, 114 Built-in groups, 154 Business Data Access, 158–165 Azure RemoteApp, 165 configuring Company Portal, 158-160 customizing Company Portal, 160 Work Folders, 161–164

С

Central Access Policy, 179 Central Access Rules, 179 Certificate authority (CA), 87 Certificate chain, 85 Certification path, 85 Challenge Handshake Authentication Protocol (CHAP), 90 Child domain, 148 Claim rules, 157 Claims, 157, 175-177 Claims-based access control, 175 Claims provider, 158 Claims provider trust, 158 Classification management, 178 Classification rules, 178 Cloud-based management solution, 123 Cloud computing, 102 Cloud services, 121-141 Microsoft Azure, 137-141 availability, 141 disaster recovery (DR), 141 features, 123, 137 redundancy, 141 Service Level Agreements (SLAs), 141

Cloud services, (Continued) services, 138-140 virtual machines, 138 Microsoft Intune, 121-137 deploying Microsoft Intune client, 125–127 managing policies, 131-132 managing user and computer groups, 129-131 reviewing administrator roles, 128-129 supporting mobile device management, 132-136 storage service (See Cloud storage services) types, 121-122 Cloud storage services, 45-59 Azure storage, 55–56 Microsoft Office 365, 52-56 OneDrive, 46–50 OneNote, 51 Outlook, 51-52 Color depth, 25 Common Internet File System (CIFS), 73 Communication as a Service (CaaS), 122 Communications services, 122 Company Portal, 159–160 configuring, 159-160 customizing, 160 Component Object Model (COM), 10 Computer accounts, 154 Computer Configuration node, 30 Control panel, 9-10 Cortana, 4, 5 Criteria membership, 130 Cryptographic Message Syntax Standard, 86 Cryptographic token, 104

D

Data access and management, 45–91 cloud storage services, 45-59 Azure storage, 55–56 Microsoft Office 365, 52–56 OneDrive, 46-50 OneNote, 51 Outlook, 51-52 encryption, 80-91 using BitLocker To Go, 88 certificates and their use, 82-83 certificate services, 87 classification, 80 managing certificates, 84-86 using VPN, 88-91 file and print sharing, 62-80 using HomeGroup, 72-73 mapping drives, 73-74 NTFS permissions, 62-67 sharing drives and folders, 67-71 sharing printers, 75-80 file system, 59–62 creating/deleting partition/logical drive, 61-62 Disk Management, 60, 61 FAT32, 59, 60 initializing new disks, 61 Resilient File System (ReFS), 60

local storage, 56-59 creating storage pools, 56-57 creating storage spaces, 57-59 Manage Storage Space tool, 58-59 Storage Spaces, 56 Data encryption. See Encryption Decryption, 31 Deeplinking applications, 170–172 Demilitarized zone (DMZ), 101 Denial of service (DoS) attacks, 113 Deny permissions, 66 Deployment, 166-174 enterprise mobility, 171-174 configuring application deployment policies, 171 RD Virtualization Host, 173-174 Microsoft Intune, 166–173 deeplinking applications, 170-172 installation types, 167 publishing and updating software, 167-168 sideloading applications, 168–170 DER-encoded binary X.509, 86 Desktop as a Service (DaaS), 122 Desktop Virtualization, 173-174 Device-Centric to People-Centric IT, 172–173 Device configuration, 1-40 desktop settings, 19-23 Personalization window, 21 screen saver, 22 Sound dialog box, 22 Start menu, 22 Taskbar and Start Menu properties dialog box, 20 device options, Windows 10, 2-20 changing date and time, 12-13 control panel, 9-10 Cortana, 4–5 Desktop, 2–3 installed programs, 2, 4 managing devices, 13-20 Microsoft accounts, 6–9 Settings option, 4, 5 Start menu, 2-3 system options, 10–12 touch screen, 5-6 display settings, 25-26 drive encryption, 31-37 BitLocker, 33–37 file encryption, 31-33 Group Policy, 27-31 using Administrative Templates, 30-31 applying order, 28-29 configuring desktop background image, 31 configuring settings, 29-30 Group Policy Management Console, 29 Group Policy objects (GPOs), 27-29 Local Group Policy Editor, 29 shortcuts, 27 updates, 37-40 application update, 40 system update, 40 Windows Update, 37-40

user profiles, 22-25 folders, 23 using mandatory user profile, 24-25 migrating user profiles, 25 Profile tab, 23, 24 using roaming profiles, 23-24 types, 23 Device driver, 13–14 Device management, 13-20 using device manager, 15–18 using the devices and printers folder, 14–15 Device Settings tab, 14 disabling, 16-17 troubleshooting problem devices, 18-20 updating device driver, 17–18 Device Manager, 15–18 Device Registration Service (DRS), 172 Devices and Printers folder, 14-15 Device security, 97–116 cloud computing, 102 extranet, 98–99 firewalls, 100-101 internet, 98 intranet, 97-99 Local Area Networks (LAN), 97 malware, 112–116 antivirus and antimalware strategies, 115–116 categories, 113-114 identification, 114-115 Metropolitan Area Networks (MAN), 97 Network Address Translation (NAT), 99–100 permissions, 106-112 NTFS, 108-111 operation, 107-108 share permissions, 112 private network, 97 public network, 97 user authentication, 102–106 biometrics, 104-105 digital certificate, 104 nonrepudiation, 102 using passwords, 103–104 using a personal identification number (PIN), 104 security token, 104 smart card, 104 Windows Rights Management Services, 105–106 Wide Area Networks (WAN), 97 Dictionary attack, 103 Digital certificates, 83, 104. See also X.509 digital certificate to encrypt data, 82–83 importing/exporting formats, 86 managing, 84-86 SSL and TLS, 81-82 used in wireless communications, 83 Digital signature, 83 Direct membership, 130, 131 Directory service, 147 Disaster recovery (DR), 141 Dishonest adware, 113 Disk Management, 60, 61

Distinguished Encoding Rules (DER), 86 Distribution group, 154 Domain, 147–148 Domain-based accounts, 6 Domain controller, 148–149 Domain local group, 154 Domain tree, 147–148 Domain user accounts, 152 Drive encryption, 31–33 decrypting file/folder, 33 encrypting file/folder, 32 Encrypting File System (EFS), 31-32 Drive mapping, 73-74 Dynamic Access Control (DAC) policies, 175-180 for Active Directory Domain Services (AD DS), 176 configuring file classification, 178 configuring user and device claim types, 176-177 implementing Central Access Policy, 178–180 implementing conditional access on folder's ACL, 178 Windows Server 2012 R2, 175

E

Effective permissions, 67 EFS-encrypted folders, 87-88 Encrypting File System (EFS), 31–32 Encryption, 32, 80-91 using BitLocker To Go, 88 certificate services, 87 classification, 80 digital certificates, 83 managing certificates, 84-86 moving and copying EFS-encrypted folders, 87-88 Secure Socket Layer (SSL), 81 Transport Layer Security (TLS), 82 using VPN, 88-91 Enterprise CA, 87 Enterprise mobility, 146–180 Bring Your Own Device (BYOD), 166–180 configuring application deployment policies, 171 deploying application, Microsoft Intune, 166–172 Desktop Virtualization, 173-174 Device-Centric to People-Centric IT, 172–173 Dynamic Access Control (DAC) policies, 180 Microsoft Intune Mobile Application Management (MAM), 171–172 Windows Rights Management (RMS), 180 Business Data Access, 158–165 Azure RemoteApp, 165 configuring Company Portal, 159–160 customizing Company Portal, 160 Work Folders, 161–164 identity services, 146-158 Active Directory domains, trees, and forests, 147-148 Active Directory Federation Services (AD FS), 156–157 Azure Active Directory (AD), 155–156 computer accounts, 154 groups, 154-155 Microsoft accounts, 156 objects, 151-152 organizational units (OU), 150-151

Enterprise mobility, (*Continued*) sites and domain controllers, 148–150 user accounts, 152–153 Windows Server Active Directory, 146–147 Explicit permissions, 66 Extensible Authentication Protocol (EAP-MS-CHAPv2), 90 Extranet, 98–99

F

FAT, 59, 60 FAT32, 59, 60 Federal Information Standard (FIPS), 83 Federated trust relationship, 157 Federation server, 157 Federation Services, 156–157 Fetching, 46 File Allocation Table (FAT). See FAT File and print sharing, 62-80 using HomeGroup, 72-73 mapping drives, 73-74 NTFS permissions, 62-67 sharing drives and folders, 67-71 sharing printers, 75-80 File classification, 177–178 File Classification Infrastructure, 106 File management, 178 File system, 59-62 creating/deleting partition/logical drive, 61-62 Disk Management, 60, 61 FAT32, 59, 60 vs. FAT and NTFS, 60 limitations, 59 initializing new disks, 61 Resilient File System (ReFS), 60 Finger scanner, 105 Firewalls, 100-101 Forest, 148

G

Global Administrator, 53 Global group, 154 Globally unique identifier (GUID), 152 Group membership, 130 Group Policy, 27–31 using Administrative Templates, 30–31 configuring desktop background image, 31 configuring settings, 29–30 Group Policy Management Console, 29 Group Policy objects (GPOs), 27–29 Local Group Policy Editor, 29 order, 28–29 Group Policy objects (GPOs), 27–29, 87 Groups, 154–155 GUID Partition Table (GPT), 61

Н

Hardware token, 104 Hash function, 81 HomeGroup, 72–73 creating, 72 joining, 73 modifying, 73 Hosted private cloud, 121–122 Hybrid cloud, 122 Hyper-V, 138, 141 Hypervisor, 138

I

Identity services, 146–158 Active Directory domains, trees, and forests, 147-148 Active Directory Federation Services (AD FS), 156-158 Azure Active Directory (AD), 155–156 computer accounts, 154 groups, 154-155 Microsoft accounts, 156 objects, 151-152 organizational units (OU), 150-151 sites and domain controllers, 148-150 user accounts, 152-153 Windows Server Active Directory, 146–147 Infrastructure as a Service (IaaS), 122 Inherited permissions, 66 Internet, 98 Internet Engineering Task Force (IETF), 82, 98 Internet Key Exchange Version 2 (IKEv2), 89 Internet Protocol Security (IPsec), 33 Internetwork, 98 Intranet, 97–99 IP Security (IPsec), 83

J

Jump List, 21

Κ

Kerberos, 147 Key fob, 104 Knowledge Consistency Checker (KCC), 149

L

Layer 2 Tunneling Protocol (L2TP), 89 Lightweight Directory Access Protocol (LDAP), 147 Line of Business (LOB) apps, 166 Live previews, 21 Live tiles, 2 Local Area Networks (LAN), 97 Local-based accounts, 6 Locally redundant storage (LRS), 56 Local user accounts, 152 Local user profile, 23

Μ

Malware (Malicious software), 112–116 antivirus and antimalware strategies, 115–116 categories, 113–114 identification, 114–115 Mandatory user profile, 24–25 Mapped drive, 73 Master Boot Record (MBR), 61 Member server, 149 Metropolitan Area Networks (MAN), 97 Microsoft accounts, 6–9, 156 creating user account using Settings program, 6-8 Sync feature, 8–9 types, 6 Microsoft Azure, 137-141 availability, 141 disaster recovery (DR), 141 features, 123, 137 recovery manager, 141 redundancy, 141 Service Level Agreements (SLAs), 141 services, 138-140 tools, 137 virtual machines, 138 web portal, 137 Microsoft Azure Fabric Controller (FC), 141 Microsoft Azure Site Recovery, 141 Microsoft CHAP version 2 (MS-CHAPv2), 90 Microsoft Intune, 121–136 Admin Console, 125 cloud-based management solution, 123 deploying application, 166–172 deeplinking applications, 170-172 installation types, 167 publishing and updating software, 167-168 sideloading applications, 168-170 deployment, 124-127 configurations, 124 Microsoft Intune client, 125–127 managing policies, 131-132 managing user and computer groups, 129-131 adding users/devices, 130 creating groups, 129 criteria membership, 130 direct membership, 130, 131 group membership, 130 mixed membership, 130 reviewing administrator roles, 128-129 signing up, 124-125 supporting mobile device management, 132-136 to add users, 135 to enroll Apple devices, 133 to enroll iOS devices, 133 to enroll Windows devices, 132 full wipe, 135 location setting, 136 Mobile Device Management Authority, 133 selective wipe, 135-136 of Windows Phone 8/8.1 devices, 134 Microsoft Intune Cloud + On-Premise Configuration, 124 Microsoft Intune Company Portal, 159 Microsoft Intune Groups, 129 Microsoft Intune Mobile Application Management (MAM), 171-172 Microsoft Intune Service Administrator, 129 Microsoft Intune Stand-Alone Cloud Configuration, 124 Microsoft Intune + System Center Configuration Manager, 124 Microsoft Intune Tenant Administrator, 129

Microsoft Management Console (MMC), 9, 15, 29 Microsoft Office 365, 52-56 administrative tasks, 52 administrator roles, 53-54 benefits, 52 features, 52 installing and managing software, 54-55 managing Office 365, 53-54 Microsoft Office 2016, 54-55 Microsoft Outlook, 51-52 Microsoft's Active Directory Domain Services (AD DS), 12 Migrating user profile, 25 Mixed membership, 130 Mobile device management (MDM), 132–136 Modern UI interface, 4 Monitoring as a Service (MaaS), 122 Multi-booting, 59 Multi-factor authentication (MFA) system, 103

Ν

Network, 96 Network Address Translation (NAT), 99–100 Network as a Service (NaaS), 122 Network printing, 75 Nonrepudiation, 102 NTFS permissions, 62–67, 107–111 advantages, 62–63 Allow and Deny, 66 to edit, 62–63 explicit, 66 inherited, 66 special, 64–65 standard, 63–64

0

Objects, 147–148 OneDrive desktop app for Windows, 50 OneDrive service, 46–50 accessing from browser, 46 accessing from desktop for Windows, 50 creating word document, 48 fetching files, 50 options, 46–47 sharing document, 49–50 uploading files, 49 OneNote service, 51 Open Database Connectivity (ODBC), 10 Organizational units (OU), 150–151 Outlook service, 51–52 Outlook Web App (OWA), 51

Ρ

Parent domain, 148 Parity, 57 Password Administrator, 54 Password Authentication Protocol (PAP), 90 Passwords, 103–104 Patch Tuesday, 37 Perimeter network, 101 Permissions, 62, 105-112. See also NTFS permissions NTFS, 108-111 operation, 107-108 share permissions, 112 Personal identification number (PIN), 104 Personal Information Exchange, 86 Pin program, 21 Platform as a Service (PaaS), 122 Point-to-Point Tunneling Protocol (PPTP), 89 Pretty Good Privacy (PGP), 82-83 Printers (Print device), 75 adding additional printer drivers, 77 adding network printer, 75 installing, 75-76 options, 77 print jobs, 75 managing, 79-80 setting permissions, 78-79 Print jobs, 75, 79-80 Private cloud, 121 Private key, 80 Private network, 97 Productivity services, 122 Public cloud, 46, 121 Public cloud services, 46 Public folders, 70-71 Public key, 80 Public key cryptography, 80 Public key infrastructure (PKI), 87 Public network, 97

R

RD Connection Broker, 165 RD Gateway, 165 RD Licensing, 165 RD Session Host, 165 RD Virtualization Host, 165, 173-174 RD Web Access, 165 Recovery manager, 141 Recycle Bin, 2 Registry permissions, 107 Relying parties, 158 Relying party trust, 158 Remote access server (RAS), 88 RemoteApp collections, 165 RemoteApp programs, 165 Remote Desktop Protocol (RDP), 165 Remote Desktop Services, 165 Resilient File System (ReFS), 60 Resolution, 25 Resource organizations, 157 Roaming user profile, 23-24 Root CA, 87 Rootkit, 114

S

Search services, 122 Secure multipurpose Internet Mail Extension (S/MIME), 82 Secure Socket Layer (SSL), 33, 81 Secure Socket Tunneling Protocol (SSTP), 89 Security group, 154 Security identifier (SID), 152 Security token, 104 Security Token Service (STS), 175 Serial ATA (SATA), 56 Service Administrator, 54 Shared folder, 67 Share permissions, 107, 112 Sharing drives and folders, 67-71 advanced sharing, 68 basic sharing, 68 using Public folders, 70-71 libraries, 70-71 sharing options, 71 share permissions, 69 Shortcuts, 27 Sideloading applications, 168-170 Simple (no resiliency), 57 Single Sign-On (SSO), 147 Site, 148 Small Computer System Interface (SCSI), 56 Smart card, 83, 104 SMB, 73 Software as a Service (SaaS), 122 Software code signing, 84 Spyware, 113 Standalone CA, 87 Storage Area Networks (SANs), 34 Storage pools, 56–59 Storage services, 122 Storage Spaces, 56-59 Subordinate CA, 87 Symmetric encryption, 80 Sync feature, 8-9 System Center Configuration Manager, 38 System Center 2012 R2 App Controller, 137 System Center 2012 R2 Virtual Machine Manager (VMM), 137, 138 System update, 40

Т

Temporal Key Integrity Protocol (TKIP), 83 Thin provisioning, 57 Three-way mirror, 57 Token, 175 Touch screen, 5–6 Transport Layer Security (TLS), 33, 82 Trojan horses, 113 Trusted identity provider, 175 Trusted Platform Module (TPM), 33–36 Trust relationships, 148 Two-way mirror, 57

U

Universal group, 154–155 Universal naming convention (UNC), 73 Universal Serial Bus (USB), 56 USB token, 104 User account, 6, 152–153 User authentication, 102-106 biometrics, 104-105 digital certificate, 104 nonrepudiation, 102 using passwords, 103-104 using a personal identification number (PIN), 104 security token, 104 smart card, 104 Windows Rights Management Services, 105–106 User Configuration node, 30 User Management Administrator, 54 User profiles, 22-25 folders, 23 using mandatory user profile, 24-25 migrating user profiles, 25 Profile tab, 23, 24 using roaming profiles, 23-24 types, 23 User State Migration Tool, 25

V

Virtual Desktop Infrastructure (VDI), 173 Virtualization, 138 Virtualization Host Infrastructure, 173 Virtual machines (VM), 138–140 Virtual Private Network (VPN), 88–91, 100 authentication, 89–90 capabilities, 89 connection properties, 91 using Getting Started Wizard, 90–91 tunneling process, 89 protocols, 89 Viruses, 113 VPN Reconnect, 89

W

Web 2.0, 98 Web Application Proxy, 157 Wide Area Networks (WAN), 97 Wi-Fi Protected Access (WPA), 83 Windows Defender, 115 Windows desktop, 20 Windows Easy Transfer, 25 Windows Rights Management (RMS), 180 Windows Rights Management Services, 105–106 permissions, 105 rights, 105 Windows Server Active Directory, 146–147 Windows Server Update Service (WSUS), 38 Windows Update, 37-40 locations, 38 screen, 38 Windows Update Advanced Options page, 3, 39 Windows Update page, 38 Wired Equivalent Privacy (WEP), 83 Wireless communications, 83 Work Folders, 161–164 additional authentication, 164 connection, 163 creating Sync Share, 161–162 installation, 161 managing, 164 synchronization, 164 Workplace Join, 172 World Wide Web (WWW), 98 Worms, 113

X

X.509 digital certificate, 84–86 accessing certificate store, 86 fields, 84 folders, 85 viewing, 84–85 certificate store, 86

Z

Zone-redundant storage (ZRS), 56

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.