## Lesson 4: Configuring File and Share Access

MOAC 70-410: Installing and Configuring Windows Server 2012



WILEY

## Overview

- Exam Objective 2.1: Configure File and Share Access
- Designing a File Sharing Strategy
- Creating Folder Shares
- Assigning Permissions
- Configuring Volume Shadow Copies
- Configuring NTFS Quotas

## Designing a File Sharing Strategy

Lesson 4: Configuring File and Share Access

© 2013 John Wiley & Sons, Inc.

## Designing a File-Sharing Strategy

Why store user files on shared server drives?

- To enable users to collaborate on projects by sharing files
- To back up document files more easily
- To protect company information by controlling access to documents
- To reduce the number of shares needed on the network
- To prevent the need to share access to workstations
- To monitor users' storage habits and regulate their disk space consumption
- To insulate users from the sharing and permission assignment processes

## **Arranging Shares**

- A well-designed sharing strategy provides each user with three resources:
  - A private storage space, such as a home folder, to which the user has exclusive access.
  - A public storage space, where each user can store files that he or she wants colleagues to be able to access.
  - Access to a shared work space for communal and collaborative documents.

# **Controlling Access**

- The principle of "least privileges" states that users should have only the privileges they need to perform their required tasks and no more.
- Users should have complete access and control of their own files and no privileges to others' private files.
- Users should have complete control of their own Public folder, but limited access to others'.
- In the shared work space, users should have privileges based on their individual needs.
- Administrators should have privileges to have full control over users' private and public folders.

## **Controlling Access**

- Always assign permissions to security groups, not to individuals.
- Utilize domain local groups and global or universal groups to simplify administration of permissions.
- In special cases, use the Deny Access NTFS permission to override assigned permissions.

# Mapping Drives

- Folder Redirection settings in Group Policy can be used to map each user's Documents folder to his or her home folder on the network share.
- This practice enables users to work with their files without ever knowing they are stored on a network drive.
- Login scripts can be used to map each user's directory to a drive letter on that user's computer.
- Users know they must save their files to their F: drive, for example, not knowing it is pointing to a network share.

## **Creating Folder Shares**

Lesson 4: Configuring File and Share Access

© 2013 John Wiley & Sons, Inc.

## **Creating Folder Shares**

- Shares must be created in order for network users to be able to access the disks on the servers. You must determine:
  - What folders you will share
  - What names you will assign to the shares
  - What permissions you will grant users to the shares
  - What Offline Files settings you will use for the shares

## Creator/Owner

- You can share your own folders.
- Right-click and select Share with > Specific
   People to access a simplified interface.
- Use **Sharing** tab of the folder's Properties sheet for greater control.

### **Creating Folder Shares**

		_ 0	
g File Sharing			
Choose people on your network to share v	with		
the second s			
ype a name and then click Add, or click the arrow to f	ind someone.		
	~	Add	
Name	Permission Lev	el	
🔏 Administrator	Read/Write 🔻		
Administrators	Owner		
See Everyone	Read 🔻		
m having trouble sharing			
	(in the second s	hare Can	

The File Sharing dialog box

### **Creating Folder Shares**

	Advanced Sharing
Share this f	older
Settings	
Share name	51
	×
Add	Remove
Limit the nu	mber of simultaneous users to:
Commontes	
commences	
Permissio	ons Caching
	OK Cancel Apply

The Advanced Sharing dialog box

# **Types of Folder Shares**

## Server Message Blocks (SMB)

- The standard file-sharing protocol used by all versions of Windows.
- Requires the File Server role service.

## Network File System (NFS)

- The standard file sharing protocol used by most UNIX and Linux distributions.
- Requires the Server for NFS role service.

h		Server Manager	
E	• • Shares	• © I	Manage Tools View Help
	Servers Volumes Disks Storage Pools Shares iSCSI	SHARES         All shares   0 total         There are no shares.         To create a file share, start the New Share Wizard.	VOLUME No share is selected. Select a share to display its related volume.  Go to Volumes Overview > QUOTA No data available.
			QUOTA No data available.

#### The Shares homepage

Ъ	New Share	Wizard 📃 🗖 🗙
Select the profi Select Profile Share Location Share Name Other Settings Permissions Confirmation Results	le for this share File share profile: SMB Share - Quick SMB Share - Advanced SMB Share - Applications NFS Share - Quick NFS Share - Advanced	Description: This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers. • Suitable for general file sharing • Advanced options can be configured later by using the Properties dialog
		< Previous Next > Create Cancel

The Select the profile for this share page in the New Share Wizard

<b>b</b>	Nev	v Share Wizard				-		x
Select the server a	nd path for th	is share						
Select Profile	Server:							
Share Location	Server Name	Status	Cluster l	Role	Owner Node			
Share Name	ServerA	Online	Not Clu	stered				
Other Settings								
Permissions								
Confirmation								
Contration								
Results:	Share location:							
	Select by volume:							
	Volume	Free Space	Capacity	File Syste	m			
	C:	49.1 GB	59.7 GB	NTFS				
								_
	The location of the fil volume.	e share will be a new fold	der in the \S	Shares dire	ctory on the s	elect	ed	
	O Type a custom path:							
						Br	owse,	
		Provinces	Nevts		Craata		ancol	
		< Previous	ivex( >		Create		ancei	

The Select the server and path for this share page of the New Share Wizard

<b>1</b> 2	New Share Wizard		x
Specify share na Select Profile Share Location Share Name Other Settings Permissions Confirmation Results	New Share Wizard         Sme         Share name:         Share description:         Local path to share:         E:\Shares\         If the folder does not exist, the folder is created.         Remote path to share:         \\ServerB\		×
	<pre>     Create     [ </pre>	Cancel	

The Specify share name page of the New Share Wizard

6	New Share Wizard	-		x	
Configure share s Select Profile Share Location Share Name Other Settings Permissions Confirmation Results	New Share Wizard         Settings         Enable access-based enumeration         Access-based enumeration displays only the files and folders that a user has perm access. If a user does not have Read (or equivalent) permissions for a folder, Wind folder from the user's view.         Image: Allow caching of share         Caching makes the contents of the share available to offline users. If the BranchCache on the share.         Image: Enable BranchCache on the file share         BranchCache enables computers in a branch office to cache files downloaded	nissior lows t	ns to nides or	x	
	Share, and then allows the files to be securely available to other computers in the Learn more about configuring SMB cache settings           Encrypt data access           When enabled, remote file access to this share will be encrypted. This secures the unauthorized access while the data is transferred to and from the share. If this bo and grayed out, an administrator has turned on encryption for the entire server.	data k is ch	again eckee	ist d	

The Configure share settings page of the New Share Wizard

Ta l		New Share Wiz	ard		-		x
Specify permine Select Profile Share Location Share Name	Permission Permission Share perr Folder per	ontrol access ns to access the files on a sha ns, and, optionally, a central a missions: Everyone Full Contr missions:	ire are set using a access policy. rol	combination of folder permi	ission	ıs, sha	re
Diner Settings	Tune	Principal	Access	Applies To			<u> </u>
Confirmation Results	Allow Allow Allow Allow Allow Allow Allow Allow	Everyone BUILTIN\Users BUILTIN\Users CREATOR OWNER NT AUTHORITY\SYSTEM BUILTIN\Administrators BUILTIN\Administrators	Read & execute Special Special Full Control Full Control Full Control Full Control	This folder, subfolders, and This folder, subfolders, and This folder and subfolders Subfolders and files only This folder, subfolders, and This folder, subfolders, and This folder only	d files d files d files d files		
		< [	Previous <u>N</u> ex	xt > Create	(	Cancel	I

The Specify permissions to control access page of the New Share Wizard

L.	New Share	Wizard	_ 🗆 🗙
Confirm selection Select Profile Share Location Share Name Other Settings Permissions Confirmation Results	New Share	Wizard are the correct settings, and then click ServerB Not Clustered E:\Shares\Docs Docs SMB Disabled Enabled Disabled Disabled	Create.
		< Previous Next > Create	Cancel

The Confirm selections page of the New Share Wizard

<b>a</b>	Server Manager	_ <b>_</b> X
Shares	• @	)   Manage Tools View Help
<ul> <li>Servers</li> <li>Volumes</li> <li>Disks</li> <li>Storage Pools</li> <li>Shares</li> <li>iSCSI</li> </ul>	SHARES All shares   1 total TASKS Filter Share Local Path ServerB (1) Docs E:\Shares\D	VOLUME Docs on ServerB TASKS New Volume (E:) Capacity: 20.0 GB 0.8% Used 156 f 19.9 Go to Volumes Overview > QUOTA Docs on ServerB

The new share on the Shares homepage in Server Manager

## Assigning Permissions

Lesson 4: Configuring File and Share Access

© 2013 John Wiley & Sons, Inc.

# **Assigning Permissions**

The four permissions systems:

- Share permissions: Control access to folders over a network.
- **NTFS permissions:** Control access to the files and folders stored on disk volumes formatted with the NTFS file system.
- **Registry permissions:** Control access to specific parts of the Windows registry.
- Active Directory permissions: Control access to specific parts of an Active Directory Domain Services (AD DS) hierarchy.

## Windows Permissions Architecture

- Access Control List (ACL)
- Access Control Entries (ACEs)



### Windows Permissions

	02	-	·		
ieneral	Sharing	Security	Previous Versions	Customize	
Object i	name: E	:\Shares\	Docs		
Group	or user nan	nes:			
SR Ev	reryone				^
Sec.	REATOR	WNER			
S)	STEM				×
< 4	Iminietrator	s (SERVE	R\Administratore)	)	× 1
To cha	nge permis	sions, click	c Edit.	Eda	_
				Cuit	
Permiss	ions for Ev	veryone	Allov	w Deny	1
Full o	ontrol				^
Modi	fy				
Read	& execut	е	$\checkmark$		=
List f	older conte	ents	$\checkmark$		
Read	ł		~		
Write	•				4
For spe click Ac	cial permis Ivanced.	sions or ad	vanced settings,	Advanced	đ
Leam a	bout acce	ss control a	and permissions		

The Security tab of a Properties sheet

## Basic and Advanced Permissions

- Permissions allow you to grant specific degrees of access to security principals.
- Preconfigured permission combinations are called **Basic Permissions**.
- Advanced Permissions are more granular and can be applied individually, but are rarely used.

## Allowing and Denying Permissions

### Additive

 Start with no permissions and then grant Allow permissions (preferred method).

### Subtractive

 Start by granting Allow permissions and then grant Deny permissions.

## **Inheriting Permissions**

Permissions run downward through a hierarchy



© 2013 John Wiley & Sons, Inc.

## **Effective Access**

The combination of Allow permissions and Deny permissions that a security principal receives for a system element:

- Allow permissions are cumulative.
- Deny permissions override Allow permissions.
- Explicit permissions take precedence over inherited permissions.

### **Effective Access**

Name:	E:\Shares\Docs					
Owner:	Administrators (SEF	RVERB\Admini	strators) 😗 Change			
Permissions	Share	Auditing	Effective Access			
Effective Acces domain, you ca	s allows you to view t an also evaluate the ir	the effective p	ermissions for a user, group ions to the security token f	), or device acc or the account	count. If <mark>the</mark> account is	s a member of a
User/ Group:	Select a user					
	Include group men	nbership	Click Add items	Ý	Add items	
Device:	Select a device					
	Include group men	nbership	Click Add items	Y	Add items	
View effectiv	/e access					

The Effective Access tab of the Advanced Security Settings dialog box

© 2013 John Wiley & Sons, Inc.

l.	Permissio	ns for Docs	x
Share Permissions			
Group or user name	35:		
Se Everyone			
-			
		A <u>d</u> d	<u>R</u> emove
Permissions for Eve	eryone	Allow	Deny
Full Control		~	
Change		~	
Read		~	
Leam about acces	s control and	permissions	

The Share Permissions tab for a shared folder

## **Share Permissions**

Share permission	Allows or denies security principals the ability to:
Full Control	Change file permissions. Take ownership of files. Perform all tasks allowed by the Change permission.
Change	Create folders. Add files to folders. Change data in files. Append data to files. Change file attributes. Delete folders and files. Perform all actions permitted by the Read permission.
Read	Display folder names, filenames, file data, and attributes. Execute program files. Access other folders within the shared folder.

ia		C	ocs Properties		-		x
Docs							
General Permissions	Show All +	Permiss	sions				
Settings	+	Permission folder perr policy. Share pern	is to access the files on a sha missions, share permissions, nissions: Everyone Full Cont	are are set using a and, optionally, a o rol	combinatior central acces	n of ss	
		<u>F</u> older per	missions:				
		Туре	Principal	Access	Applies To		
		Allow	Everyone	Read & execute	This folder	r, subfo	olc
		Allow	BUILTIN\Users	Special	This folder	r, <mark>sub</mark> fo	olc
		Allow	BUILTIN\Users	Special	This folder	and s	ub
		Allow	CREATOR OWNER	Full Control	Subfolder	s and fi	ile
		Allow	NT AUTHORITY\SYSTEM	Full Control	This folder	, <mark>sub</mark> fo	olc
		Allow	BUILTIN\Administrators	Full Control	This folder	r, <mark>sub</mark> fo	olc
		Allow	BUILTIN\Administrators	Full Control	This folder	only	
		<	111				>
		<u>C</u> ustom	ize permissions				
5				OK Canc	el <u>/</u>	Apply	

The Permissions page of a share's Properties sheet in Server Manager

			Ad	vanced Security Setting	gs for Docs	_ <b>D</b> X
Name Owne	2: 217	E:\Shares\Docs Administrators (Sl	ERVERB\Admin	istrators) <u>C</u> hange		
Perm	nissions	Share	Auditing	Effective Access		
To m Netwo Permi	odify shar ork locatio ission ent	re permissions, select on for this share: \\ ries:	ct the entry and ServerB.adatun	click Edit. n.local\Docs		
52	Туре	Principal			Access Full Control	
<u>م</u>	\ <u>d</u> d	Remove	View			
					OK	ancel Apply

The Share tab of the Advanced Security Settings dialog box for a share in Server Manager

	Permission Entry for Docs				ĸ
Principal: Type:	Select a principal Allow				
Permission	ISE - Full Control - Change V Read - Special permissions		Clear	all	
		OK	Ca	incel	Ĭ
	A Permission Entry dialog box for a share in				

Server Manager

User, Group, or Built-in security principal	Object Types
From this location:	
adatum.local	Locations
Enter the object name to select (examples):	
	Check Name:

## The Select User, Computer, Service Account, or Group dialog box

			Adv	vanced Security Settir	igs for Docs	-	
Name	e:	E:\Shares\Docs					
Owne	er:	Administrators (S	SERVERB\Admini	strators) <u>C</u> hange			
Pern	nissions	Share	Auditing	Effective Access			
To m Netw Perm	odify shar ork locatio ission ent	e permissions, sele on for this share: \ ries:	ect the entry and	click Edit. n.local\Docs			
	Туре	Principal			Access		_
82	Allow	Everyone			Full Control		
82	Allow	Domain Use	rs (ADATUM\Do	main Users)	Change		
	ada tatatan						

A new share permission entry in a share's access control list

## **NTFS** Authorization

- NTFS and ReFS support permissions.
- Every file and folder on an NTFS or ReFS drive has an ACL with ACEs, each of which contains a security principal and their permissions.
- Security Principals are users and groups identified by Windows using security identifiers (SIDs).
- During authorization, when a user accesses a file/folder, the system compares the user's SIDs to those stored in the element's ACEs to determine that user's access.

## NTFS Basic Permissions – Full Control

### Folder

- Modify the folder permissions.
- Take ownership of the folder.
- Delete subfolders and files contained in the folder.
- Perform all actions associated with all other NTFS folder permissions.

- Modify the file permissions.
- Take ownership of the file.
- Perform all actions associated with all other NTFS file permissions.

## NTFS Basic Permissions – Modify

### Folder

- Delete the folder.
- Perform all actions associated with the Write and the Read & Execute permissions.

- Modify the file.
- Delete the file.
- Perform all actions associated with the Write and the Read & Execute permissions.

## NTFS Basic Permissions – Read & Execute

### Folder

- Navigate through restricted folders to reach other files and folders.
- Perform all actions associated with the Read and List Folder Contents permissions.

- Perform all actions associated with the Read permission.
- Run applications.

## NTFS Basic Permissions – List Folder Contents

### Folder

- View the names of the files and subfolders contained in the folder.
- Not applicable

## NTFS Basic Permissions – Read

## Folder

- See the files and subfolders contained in the folder.
- View the ownership, permissions, and attributes of the folder.

- Read the contents of the file.
- View the ownership, permissions, and attributes of the file.

## NTFS Basic Permissions – Write

## Folder

- Create new files and subfolders inside the folder.
- Modify the folder attributes.
- View the ownership and permissions of the folder.

- Overwrite the file.
- Modify the file attributes.
- View the ownership and permissions of the file.

### **Assign Basic NTFS Permissions**

ame:	E:\Shares\Docs			
wner:	Administrators (SERVERB\Adn	ninistrators) <u>C</u> hange		
ermissions	Share Auditing	g Effective Access		
or additiona ermission er	l information, double-click a pern ntries:	nission entry. To modify a p	permission entry, select	the entry and click Edit (if available).
Туре	Principal	Access	Inherited from	Applies to
& Allow	Administrators (SERVERB\Ad	Full control	None	This folder only
省 Allow	Administrators (SERVERB\Ad	Full control	E:\	This folder, subfolders and files
& Allow	SYSTEM	Full control	E:\	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	E:\	Subfolders and files only
& Allow	Users (SERVERB\Users)	Special	E:\	This folder, subfolders and files
& Allow	Everyone	Read & execute	E:\	This folder, subfolders and files
& Allow	Users (SERVERB\Users)	Create folders / appen	E:\	This folder and subfolders
A <u>d</u> d Disable <u>i</u> nh Replace all	<u>R</u> emove <u>V</u> iew neritance child object permission entries w	ith inheritable permission e	ntries from this object	

#### The Advanced Security Settings dialog box for a share in Server Manager

### Assigning Advanced NTFS Permissions

	Permission	Entry for Docs	_ <b>D</b> X
Principal: Type:	Domain Users (ADATUM\Domain Users) Select a principal		
Applies to:	This folder, subfolders and files 🗸 🗸		
Advanced	permissions:	☐ Write attributes	Show basic permissions
	Traverse folder / execute file  List folder / read data  Read attributes	Write extended attributes Delete subfolders and files Delete	
	<ul> <li>✓ Read attributes</li> <li>✓ Read extended attributes</li> <li>□ Create files / write data</li> </ul>	Delete     Read permissions     Change permissions	
	Create folders / append data	Take ownership	
Only ap	ply <u>t</u> hese permissions to objects and/or containers within this containe		Clear all
Add a con A <u>d</u> d a con	dition to limit access. The principal will be granted the specified permis dition	sions only if conditions are met.	
			OK Cancel

The Permission Entry dialog box displaying Advanced Permissions

© 2013 John Wiley & Sons, Inc.

## **Resource** Ownership

- Every file and folder on an NTFS drive has an owner.
- The owner always has the ability to modify the permissions, even if current permissions settings deny them access.
- The owner is the person who created the file or folder.
- Others with the Take Ownership permission can become the owner.

## Combining Share and NTFS Permissions



## Configuring Volume Shadow Copies

Lesson 4: Configuring File and Share Access

© 2013 John Wiley & Sons, Inc.

## **Volume Shadow Copies**

- Allow you to maintain previous versions of files on a server.
- A copy of a file can be accessed even if a file has been accidentally deleted or overwritten.
- Can be implemented for entire volumes only.

## **Configure Shadow Copies**

elect a volume	e: Next Pup Time	Charme	Llaad
	Disabled	O	Used
	Disabled	0	
E:	Disabled	1	
■F:\	Disabled	0	
			Create Now
			Create Now Delete Now

The Shadow Copies dialog box

## **Configure Shadow Copies**

N	
Storage area	
Located on this volume:	
F:\	✓ Details
	2024 6
<ul> <li>Use limit:</li> </ul>	ZU34 MP
Note: You need at least 300MB free	e space to create a shadow copy.
Note: You need at least 300MB free	e space to create a shadow copy.
Note: You need at least 300MB free	e space to create a shadow copy.
Note: You need at least 300MB free Schedule	e space to create a shadow copy.
Note: You need at least 300MB free	e space to create a shadow copy.
Note: You need at least 300MB free Schedule	space to create a shadow copy.  Schedule two shadow copies per day. Avoid
Note: You need at least 300MB free Schedule Note: The default schedule creates creating shadow copies more freque	space to create a shadow copy. Schedule two shadow copies per day. Avoid ently than once per hour.

The Settings dialog box

## **Configuring NTFS Quotas**

Lesson 4: Configuring File and Share Access

© 2013 John Wiley & Sons, Inc.

## NTFS Quotas

- Enable administrators to set a storage limit for users of a particular volume.
- Users exceeding the limit can be denied access or just receive a warning.
- Space consumed by users is measured by the size of the files they own or create.

## **Configure NTFS Quotas**

Previous Versions       Quota       Customize       NFS Sharing         Status:       Disk quotas are disabled	Gonordi	Tools Ha	rdware Sh	naring Sec	urity	Shadow Copie
Status: Disk quotas are disabled	Previou	is Versions	Quota	Customia	ze	NFS Sharing
Enable quota management  Deny disk space to users exceeding quota limit  Select the default quota limit for new users on this volume:  Do not limit disk usage	\$	Status: Disk	quotas are o	lisabled		
Deny disk space to users exceeding quota limit Select the default quota limit for new users on this volume: <ul> <li>Do not limit disk usage</li> <li>Limit disk space to</li> <li>KB</li> <li>Set warning level to</li> <li>KB</li> <li>KB</li> <li>Select the quota logging options for this volume:</li> <li>Log event when a user exceeds their quota limit.</li> </ul>		Enable quota	managemen	t		
Select the default quota limit for new users on this volume: <ul> <li>Do not limit disk usage</li> <li>Limit disk space to</li> <li>KB </li> <li>Set warning level to</li> <li>KB </li> </ul> Select the quota logging options for this volume: <ul> <li>Log event when a user exceeds their quota limit.</li> </ul>		<u>D</u> eny <mark>d</mark> isk spa	ice to users	exceeding q	uota lim	iit
<ul> <li>Do not limit disk usage</li> <li>Limit disk space to</li> <li>KB </li> <li>Set warning level to</li> <li>KB </li> <li>KB </li> <li>Select the quota logging options for this volume:</li> <li>Log event when a user exceeds their quota limit.</li> </ul>	Sel	ect the defaul	t quota limit I	or new user:	s on this	s volume:
Egret with disk space to     I KB     KB     Set warning level to     Select the quota logging options for this volume:     Log event when a user exceeds their quota limit.	6	) Do not limit	disk usage			
Set warning level to KB v Select the quota logging options for this volume:	6	) Limit diek er	ace to	1	KB	
Set warning level to KB Select the quota logging options for this volume: Log event when a user exceeds their quota limit .					14D	
Select the quota logging options for this volume:		Set warning	level to	<u>, 1</u>	KB	~
Log event when a user exceeds their quota limit	Sel	ect the quota	logging optic	ons for this v	olume;	
		Log event v	when a user	exceeds the	ir quota	limit
Log event when a user exceeds their warning level					le ture les la	na level
	E	_ Log e <u>v</u> ent v	vhen a user	exceeds the	ii wamii	ng lovor
	E	Log e <u>v</u> ent v	vhen a user	exceeds the	ii wanii	ig lover
<u>Q</u> uota Entries	[ [	Log e <u>v</u> ent v	vhen a user	exceeds the		ta Entries
Quota Entries	[ [	_ Log e <u>v</u> ent v	vhen a user	exceeds the		ta Entries
<u>Q</u> uota Entries	E E	_ Log e <u>v</u> ent v	vhen a user	exceeds the		ita Entries
<u>Q</u> uota Entries	E	_ Log e <u>v</u> ent v	vhen a user	exceeds the		ita Entries
Quota Entries	[	Log e <u>v</u> ent v	vhen a user	exceeds the		ita Entries

The Quota tab of a volume's Properties sheet

## Lesson Summary

- Creating folder shares makes the data stored on a file server's disks accessible to network users.
- Windows Server 2012 has several sets of permissions that operate independently of each other, including NTFS permissions, share permissions, registry permissions, and Active Directory permissions.
- NTFS permissions enable you to control access to files and folders by specifying the tasks individual users can perform on them. Share permissions provide rudimentary access control for all of the files on a network share. Network users must have the proper share and NTFS permissions to access file server shares.
- Access-based enumeration (ABE) applies filters to shared folders based on individual user's permissions to the files and subfolders in the share. Users who cannot access a particular shared resource are unable to see that resource on the network.

## Lesson Summary

- Offline Files is a Windows feature that enables client systems to maintain local copies of files they access from server shares.
- Volume Shadow Copies is a Windows Server 2012 feature that enables you to maintain previous versions of files on a server, so that if users accidentally delete or overwrite a file, they can access a copy. You can only implement Shadow Copies for an entire volume; you cannot select specific shares, folders, or files.
- NTFS quotas enable administrators to set a storage limit for users of a particular volume. Depending on how you configure the quota, users exceeding the limit can be denied disk space, or just receive a warning.

### Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



