COURSE TECHNOLOGY
CENGAGE Learning™

Hands-On Microsoft Windows Server 2008

Chapter 5

Configuring, Managing, and Troubleshooting Resource Access

Objectives

- Set up security for folders and files
- Configure shared folders and shared folder security
- Install and set up the Distributed File System
- Configure disk quotas
- Implement UNIX compatibility

Managing Folder and File Security

- Creating accounts and groups are the initial steps for sharing resources
  - The next steps are to create access control lists (ACLs) to secure these objects and then to set them up for sharing
- **Discretionary ACL (DACL)**
  - An ACL that is configured by a server administrator or owner of an object
- **System control ACL (SACL)**
  - Contains information used to audit the access to an object

Configuring Folder and File Attributes

- Attributes are stored as header information with each folder and file
  - Along with other characteristics including volume label, designation as a subfolder, date of creation, and time of creation
- Two basic attributes remain in NTFS that are still compatible with FAT
  - Read-only and hidden
- The advanced attributes are archive, index, compress, and encrypt

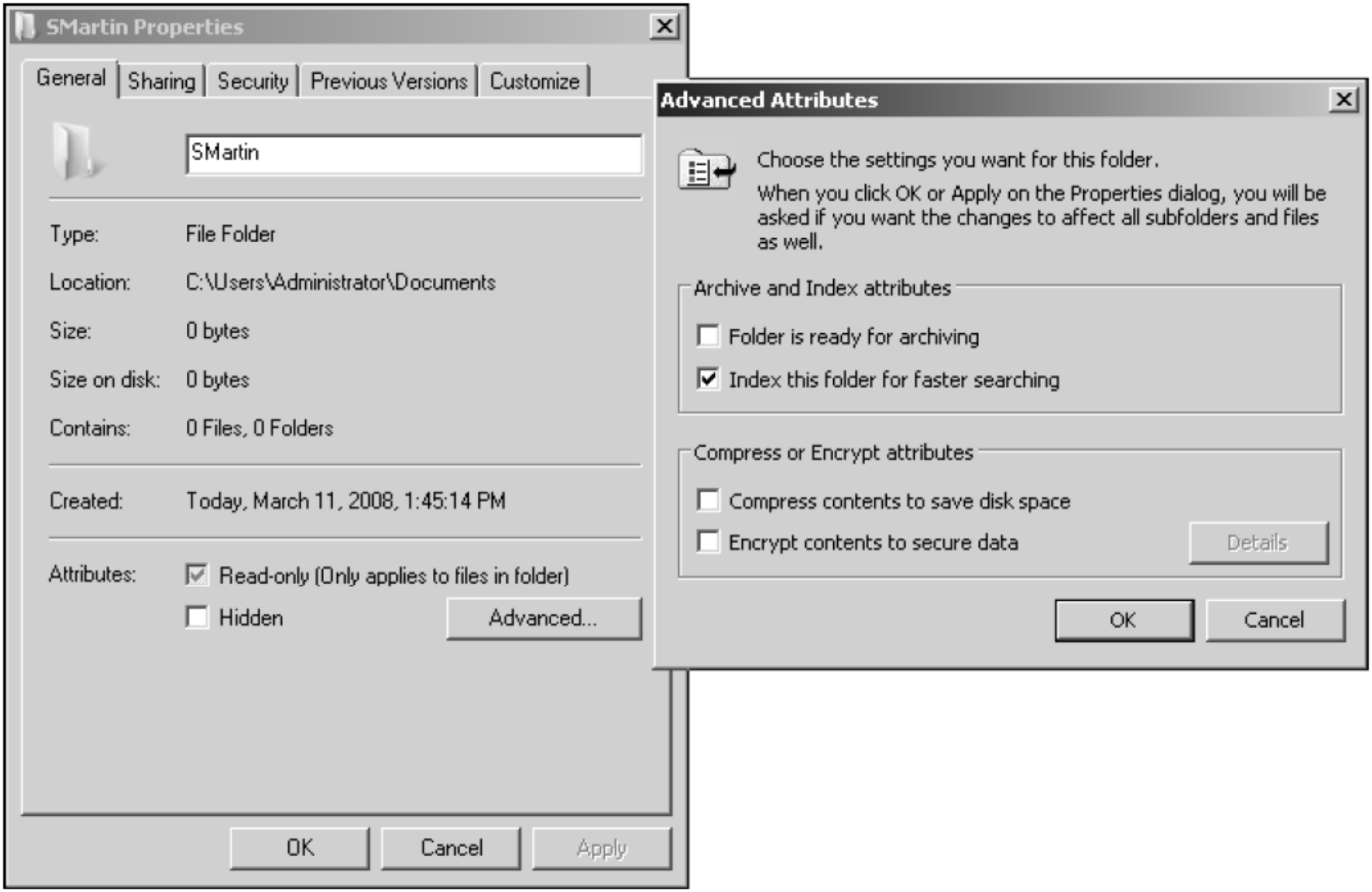

Figure 5-1 Attributes of a folder on an NTFS formatted disk

Configuring Folder and File Attributes (continued)

- Archive attribute
  - Indicates that the folder or file needs to be backed up because it is new or changed
  - File server backup systems can be set to detect files with the archive attribute to ensure those files are backed up
- Index attribute vs. Windows Search Service
  - The NTFS index attribute is used to index the folder and file contents so that file properties can be quickly searched in Windows Server 2008
    - Through the Indexing Service

Configuring Folder and File Attributes (continued)

- Index attribute vs. Windows Search Service (continued)
  - Windows Server 2008 offers a newer, faster search service called the Windows Search Service
  - To use the Windows Search Service, you must install the File Services role via Server Manager
- Multimaster replication
  - Each DC is equal to every other DC in that it contains the full range of information that composes Active Directory
- Active Directory is built to make replication efficient

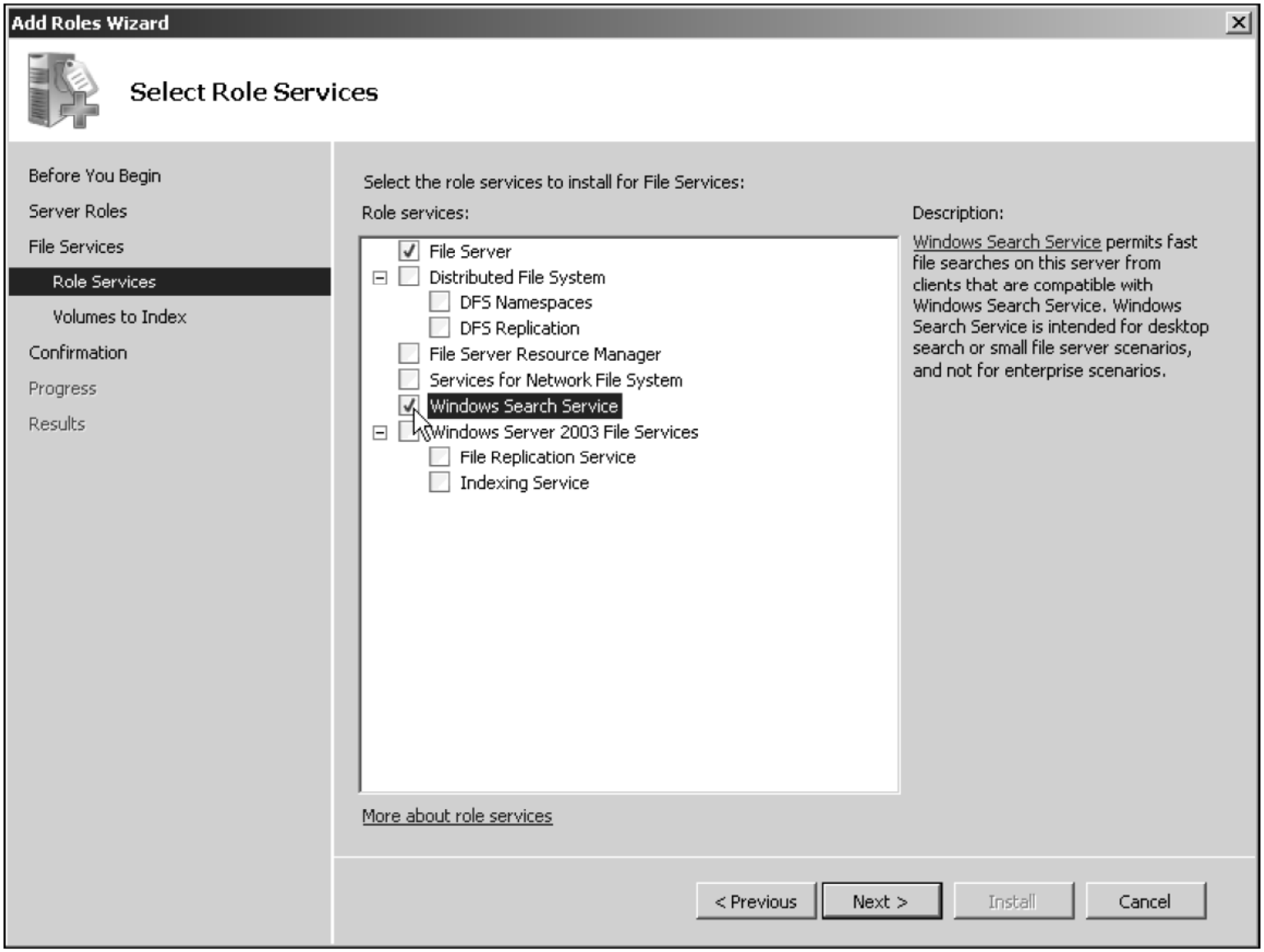

Figure 5-2 Installing the Windows Search Service with the File Services role

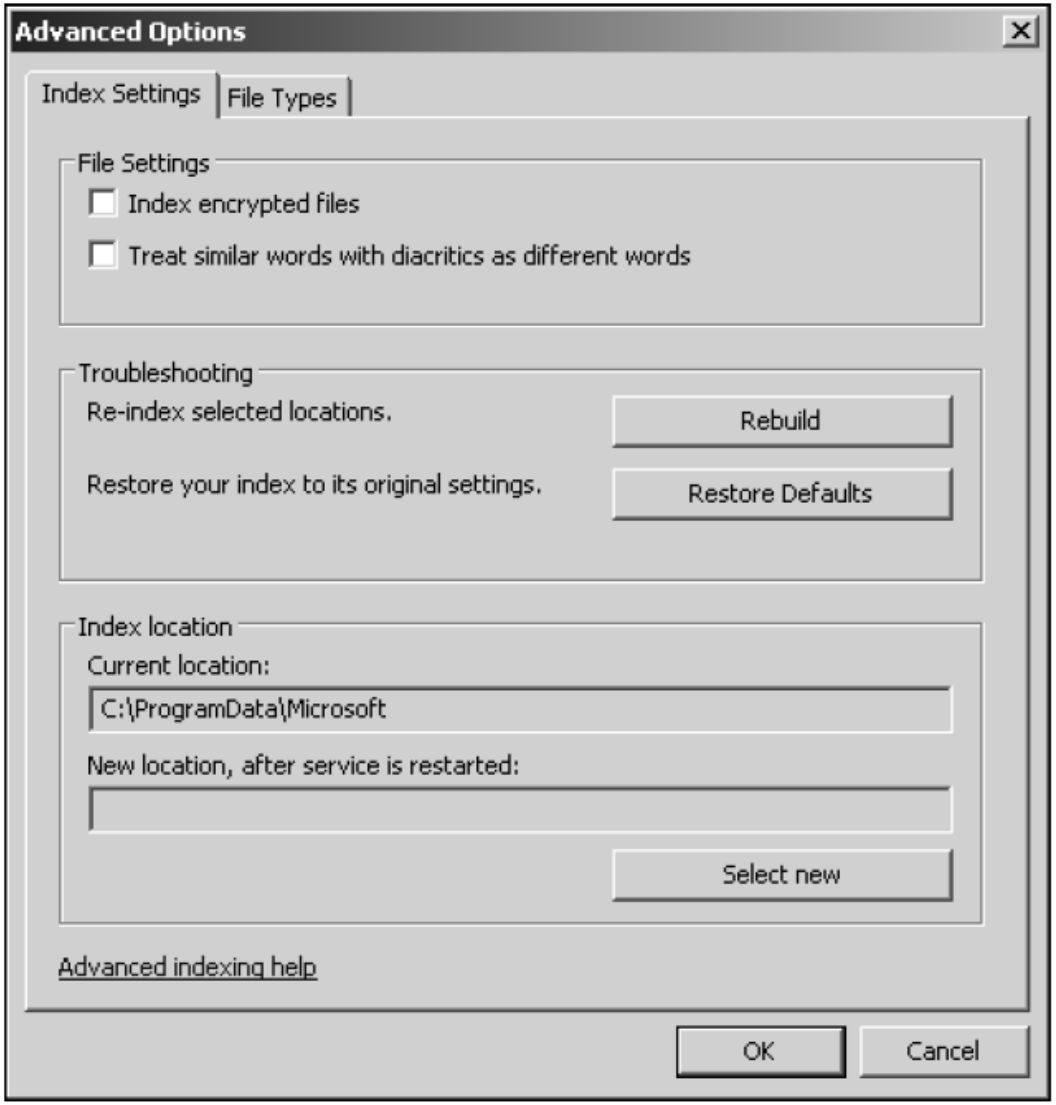

Figure 5-3 Configuring advanced indexing options

Configuring Folder and File Attributes (continued)

- Compress attribute
  - A folder and its contents can be stored on the disk in compressed format
  - Compression saves space and you can work on compressed files in the same way as on uncompressed files
  - Compressed files increase CPU overhead to open the files and to copy them

Configuring Folder and File Attributes (continued)

- Encrypt attribute
  - Protects folders and files so that only the user who encrypts the folder or file is able to read it
  - An encrypted folder or file uses the Microsoft **Encrypting File System (EFS)**
    - Which sets up a unique, private encryption key associated with the user account that encrypted the folder or file
  - EFS uses both symmetric and asymmetric encryption techniques

Configuring Folder and File Attributes (continued)

- Encrypt attribute (continued)
  - When you move an encrypted file to another folder on the same computer, that file remains encrypted, even if you rename it

Configuring Folder and File Attributes (continued)

- Activity 5-1: Encrypting Files
  - Time Required: Approximately 10 minutes
  - Objective: Encrypt files in a folder

Configuring Folder and File Permissions

- **Permissions**
  - Control access to an object, such as a folder or file
- When you configure a folder so that a domain local group has access to only read the contents of that folder
  - You are configuring permissions
- At the same time, you are configuring that folder's discretionary access control list (DACL) of security descriptors

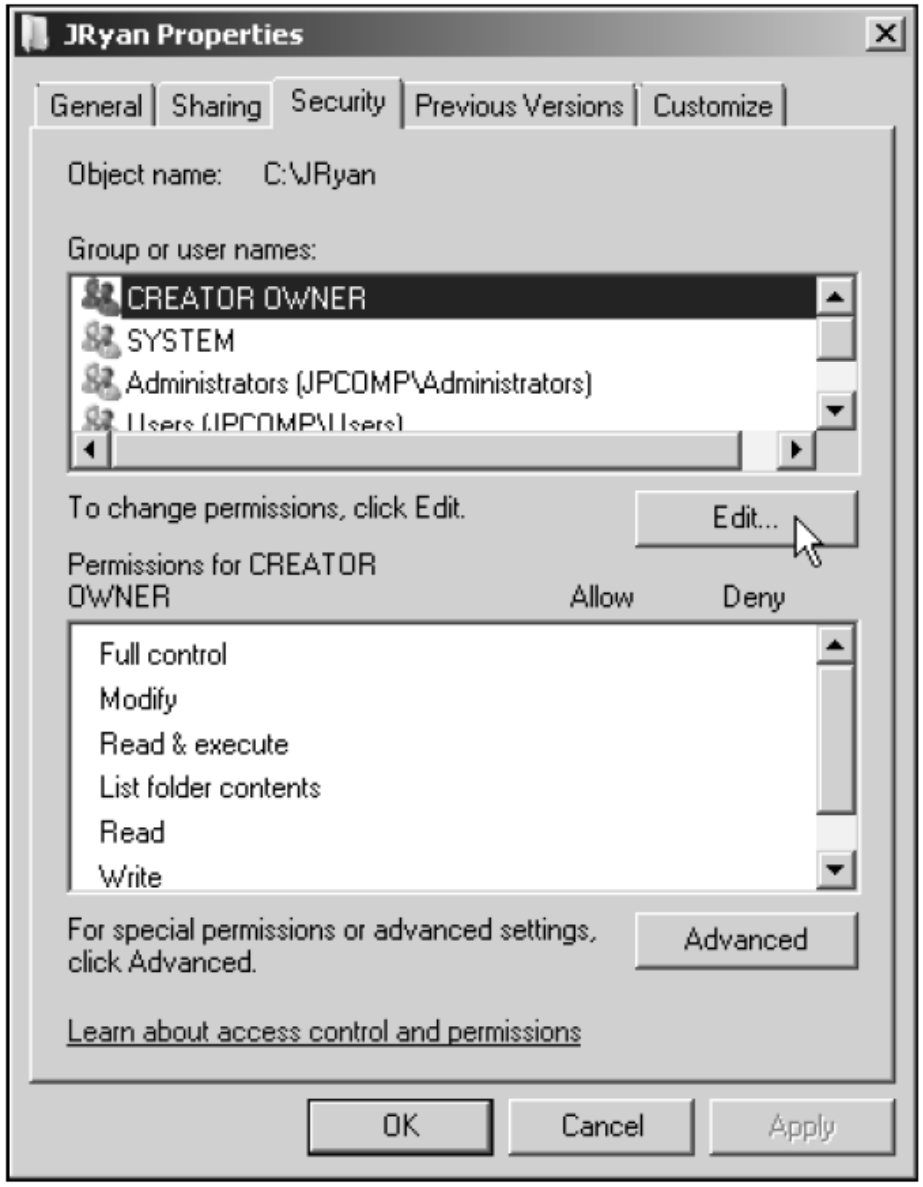

Figure 5-4 Configuring folder permissions

Configuring Folder and File Permissions (continued)

Table 5-1 NTFS folder and file permissions

Permission	Description	Applies to
Full control	Can read, add, delete, execute, and modify files plus change permissions and attributes, and take ownership	Folders and files
Modify	Can read, add, delete, execute, and modify files; cannot delete subfolders and their file contents, change permissions, or take ownership	Folders and files
Read & execute	Implies the capabilities of both List folder contents and Read (traverse folders, view file contents, view attributes and permissions, and execute files)	Folders and files
List folder contents	Can list (traverse) files in the folder or switch to a subfolder, view folder attributes and permissions, and execute files, but cannot view file contents	Folders only
Read	Can view file contents, view folder attributes and permissions, but cannot traverse folders or execute files	Folders and files
Write	Can create files, write data to files, append data to files, create folders, delete files (but not subfolders and their files), and modify folder and file attributes	Folders and files
Special permissions	Special permissions apply (see Table 5-2)	Folders and files

Configuring Folder and File Permissions (continued)

- Activity 5-2: Configuring Folder Permissions
  - Time Required: Approximately 10 minutes
  - Objective: Configure permissions on a folder so that users can modify its contents

Configuring Folder and File Permissions (continued)

- Activity 5-3: Removing Inherited Permissions
  - Time Required: Approximately 10 minutes
  - Objective: Remove inherited permissions on a folder

Configuring Folder and File Permissions (continued)

- If you need to customize permissions
  - You have the option to set up special permissions for a particular group or user

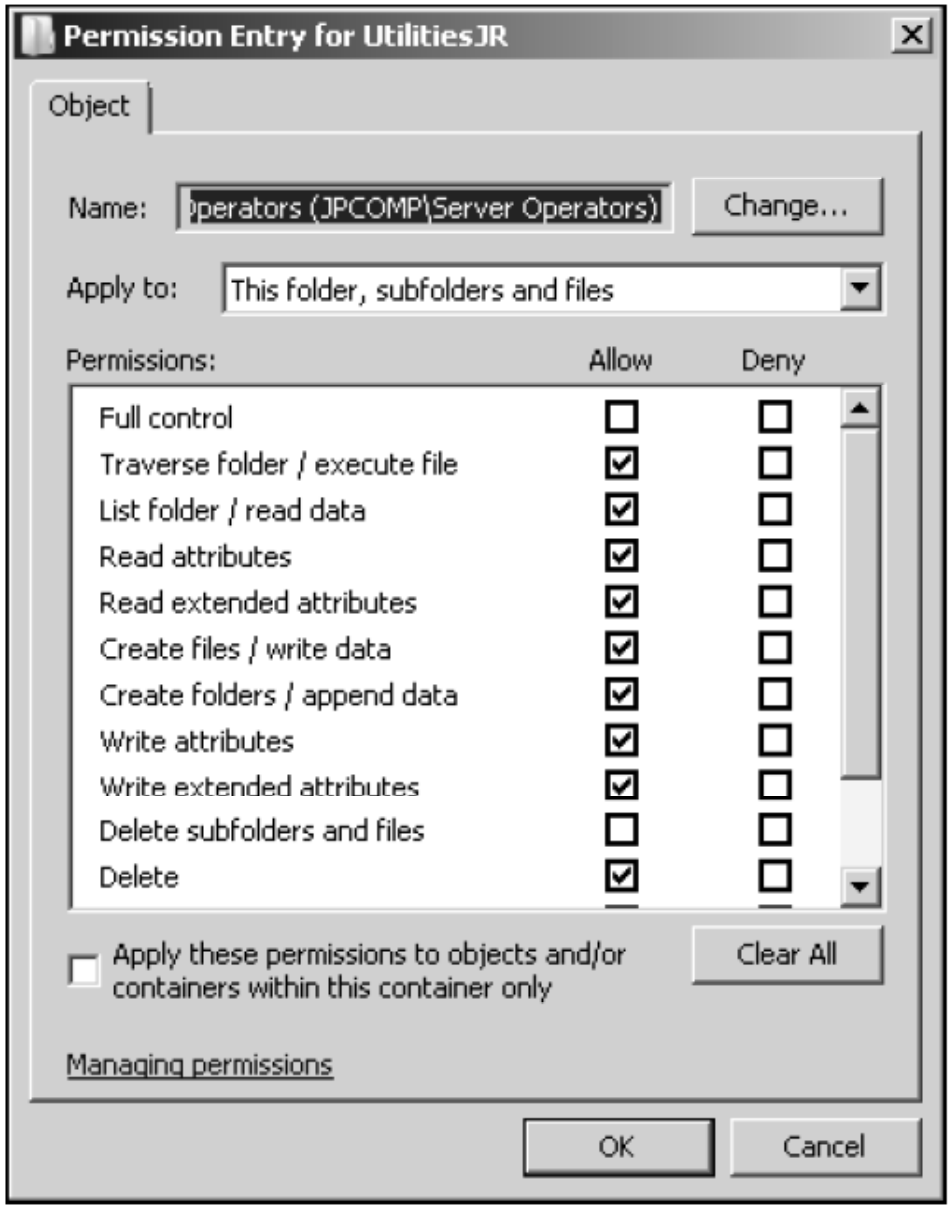

Figure 5-6 Special permissions

Table 5-2 NTFS folder and file special permissions

Permission	Description	Applies to
Full control	Can read, add, delete, execute, and modify files, plus change permissions and attributes, and take ownership	Folders and files
Traverse folder/execute file	Can list the contents of a folder and run program files in that folder; keep in mind that all users are automatically granted this permission via the Everyone and Users groups, unless it is removed or denied by you	Folders and files
List folder / read data	Can list the contents of folders and subfolders and read the contents of files	Folders and files
Read attributes	Can view folder and file attributes (read-only and hidden)	Folders and files
Read extended attributes	Enables the viewing of extended attributes (archive, index, compress, and encrypt)	Folders and files
Create files / write data	Can add new files to a folder and modify, append to, or write over file contents	Folders and files
Create folders / append data	Can add new folders and add new data at the end of files, but otherwise cannot delete, write over, or modify data	Folders and files
Write attributes	Can add or remove the read-only and hidden attributes	Folders and files
Write extended attributes	Can add or remove the archive, index, compress, and encrypt attributes	Folders and files
Delete subfolders and files	Can delete subfolders and files (the following Delete permission is not required)	Folders and files
Delete	Can delete the specific subfolder or file to which this permission is attached	Folders and files
Read permissions	Can view the permissions (ACL information) associated with a folder or file (but does not imply you can change them)	Folders and files
Change permissions	Can change the permissions associated with a folder or file	Folders and files
Take ownership	Can take ownership of the folder or file (read permissions and change permissions automatically accompany this permission)	Folders and files

Configuring Folder and File Permissions (continued)

- Activity 5-4: Configuring Special Permissions
  - Time Required: Approximately 15 minutes
  - Objective: Configure special permissions for a folder to grant a group expanded access

Configuring Folder and File Auditing

- **Auditing**
  - Enables you to track activity on a folder or file
- Windows Server 2008 NTFS folders and files
  - Enable you to audit a combination of any or all of the activities listed as special permissions in Table 5-2

Configuring Folder and File Auditing (continued)

- Activity 5-5: Auditing a Folder
  - Time Required: Approximately 10 minutes
  - Objective: Configure auditing on a folder to monitor how it is accessed and who is making changes to the folder

Configuring Folder and File Ownership

- With permissions and auditing set up, you might want to verify the ownership of a folder
- Folders are first owned by the account that creates them
- Folder owners have the ability to change permissions for the folders they create
- Ownership can be transferred only by having the Take ownership special permission
  - Or Full control permission (which includes Take ownership)

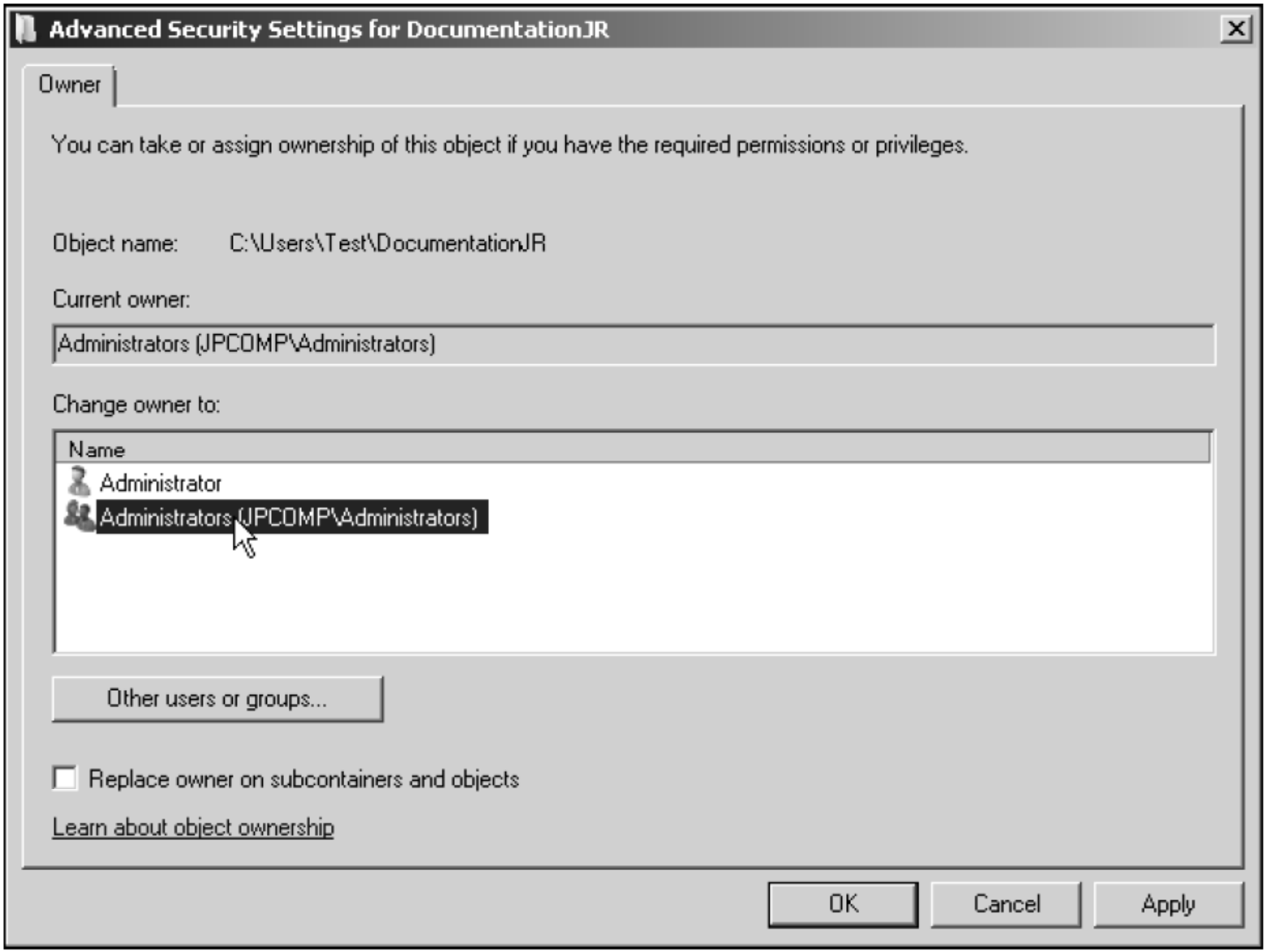

Figure 5-9 Taking ownership of a folder

Configuring Shared Folders and Shared Folder Permissions

- A folder can be set up as a shared folder for users to access over the network
- Configuring a shared folder is changed in Windows Server 2008 from previous versions
  - To help make the person offering the shared folder more aware of security options
- The first step for sharing a folder over the network is to turn on file sharing

Configuring Shared Folders and Shared Folder Permissions (continued)

- Activity 5-6: Enabling Sharing a Folder
  - Time Required: Approximately 5 minutes
  - Objective: Turn on file sharing and public folder sharing

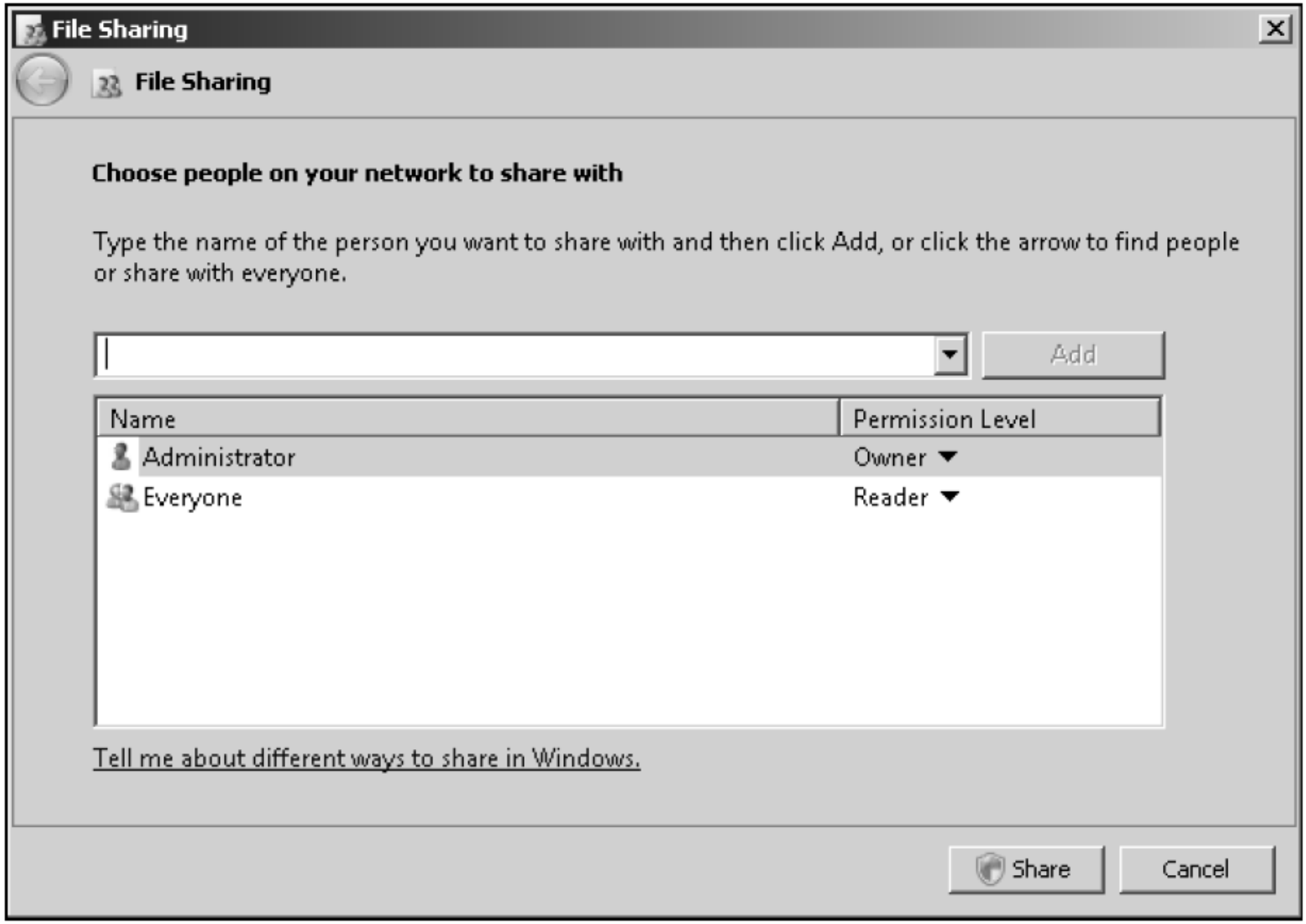

Figure 5-10 File Sharing dialog box

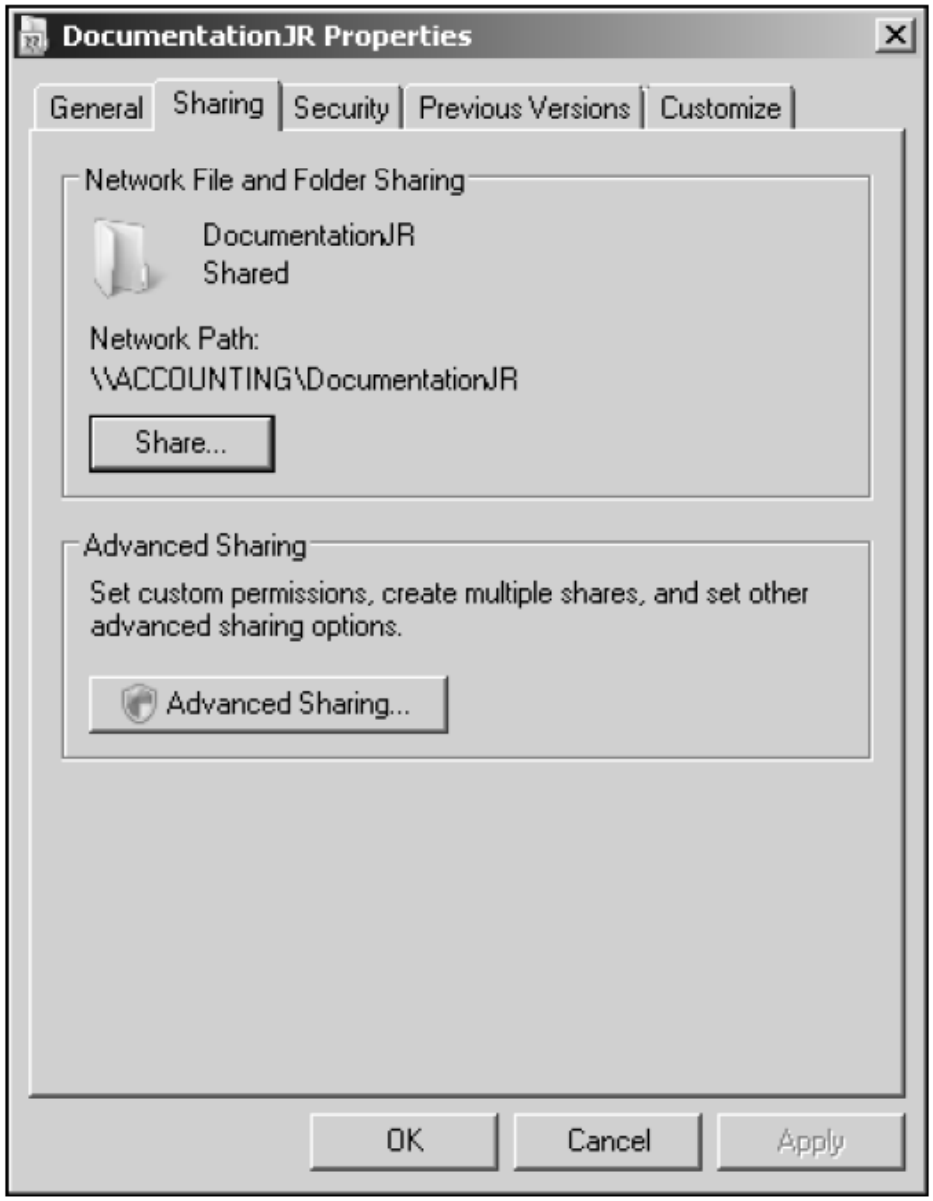

Figure 5-11 Sharing tab

Configuring Shared Folders and Shared Folder Permissions (continued)

- **Share permissions** for an object
  - Differ from the NTFS access permissions set through the Security tab
- The NTFS and share permissions are cumulative
  - With the exception of permissions that are denied
- Share permissions:
  - Reader
  - Contributor
  - Co-owner
  - Owner

Configuring Shared Folders and Shared Folder Permissions (continued)

- You can cache a folder to make the contents of a shared folder available offline
  - Any offline files that have been modified can be synchronized with the network versions of the files
- A folder can be cached in three ways:
  - Only the files and programs that users specify will be available offline
  - All files and programs that users open from the share will be automatically available offline
  - Files or programs from the share will not be available offline

Configuring Shared Folders and Shared Folder Permissions (continued)

- Activity 5-7: Configuring a Shared Folder
  - Time Required: Approximately 15 minutes
  - Objective: Configure a shared folder, share permissions, and offline access

Publishing a Shared Folder in Active Directory

- To **publish** an object
  - Means to make it available for users to access when they view Active Directory contents
    - Makes it easier to find when a user searches for that object
- **Directory Service Client (DSClient)**
  - Allows earlier Windows-based operating systems to search Active Directory
- When you publish an object, you can publish it to be shared for domain-wide access or to be shared and managed through an organizational unit (OU)

Publishing a Shared Folder in Active Directory (continued)

- Activity 5-8: Publishing a Shared Folder
  - Time Required: Approximately 5 minutes
  - Objective: Publish a shared folder in Active Directory

Troubleshooting a Security Conflict

- Windows Server 2008 offers the Effective Permissions tab in the properties of a folder or file
  - As a tool to help troubleshoot permissions conflicts
- Using the Effective Permissions tab, you can view the effective permissions assigned to a user or group
- Take into account what happens when a folder or files in a folder are copied or moved
  - A newly created file inherits the permissions already set up in a folder

Troubleshooting a Security Conflict (continued)

- Take into account what happens when a folder or files in a folder are copied or moved (continued)
  - A file that is copied from one folder to another on the same volume inherits the permissions of the folder to which it is copied
  - A file or folder that is moved from one folder to another on the same volume takes with it the permissions it had in the original folder
  - A file or folder that is moved or copied to a folder on a different volume inherits the permissions of the folder to which it is moved or copied

Troubleshooting a Security Conflict (continued)

- Take into account what happens when a folder or files in a folder are copied or moved (continued)
  - A file or folder that is moved or copied from an NTFS volume to a folder in a FAT volume is not protected by NTFS permissions
    - But it does inherit share permissions if they are assigned to the FAT folder
  - A file or folder that is moved or copied from a FAT volume to a folder in an NTFS volume inherits the permissions already assigned in the NTFS folder

Troubleshooting a Security Conflict (continued)

- Activity 5-9: Troubleshooting Permissions
  - Time Required: Approximately 10 minutes
  - Objective: View the effective permissions on a folder

Implementing a Distributed File System

- **Distributed File System (DFS)**
  - Enables you to simplify access to the shared folders on a network by setting up folders to appear as though they are accessed from only one place
  - DFS also makes managing folder access easier for server administrators
- If DFS is used in a domain, then shared folder contents can be replicated to one or more DCs or member servers

Implementing a Distributed File System (continued)

- DFS advantages:
  - Shared folders can be set up so that they appear in one hierarchy of folders
    - Enabling users to save time when searching for information
  - NTFS access permissions fully apply to DFS on NTFS-formatted volumes
  - Fault tolerance is an option by replicating shared folders on multiple servers
  - Access to shared folders can be distributed across many servers (**load balancing**)

Implementing a Distributed File System (continued)

- DFS advantages: (continued)
  - Access is improved to resources for Web-based Internet and intranet sites
  - Vital shared folders on multiple computers can be backed up from one set of master folders
- DFS reduces the number of calls to server administrators asking where to find a particular resource
- Another advantage of DFS in a domain is that folders can be replicated automatically or manually through Microsoft File Replication Service

DFS Models

- **Stand-alone DFS model**
  - No Active Directory implementation is available to help manage the shared folders
  - This model provides only a single or flat level share
- **Domain-based DFS model**
  - Takes full advantage of Active Directory and is available only to servers and workstations that are members of a domain
  - Enables a deep, root-based, hierarchical arrangement of shared folders that is published in Active Directory

DFS Topology

- **DFS topology**
  - The hierarchical structure of DFS in the domain-based model
- **Namespace root**
  - A main container (top-level folder) in Active Directory that holds links to shared folders that can be accessed from the root
- Namespace server
  - The server that maintains the namespace root
- After the namespace root is created, it is populated by shared folders for users to access

DFS Topology (continued)

- Folders are established in a level hierarchy and appear to be in one server location
  - Although they can be on many servers
- **Replication group**
  - A set of shared folders that is replicated or copied to one or more servers in a domain

Installing DFS

- DFS is installed as a service within the File Services role
- If the File Services role is already installed, but you don’t see the DFS Management tool on the Administrative Tools menu
  - This means you didn’t install Distributed File System when you installed the File Services role

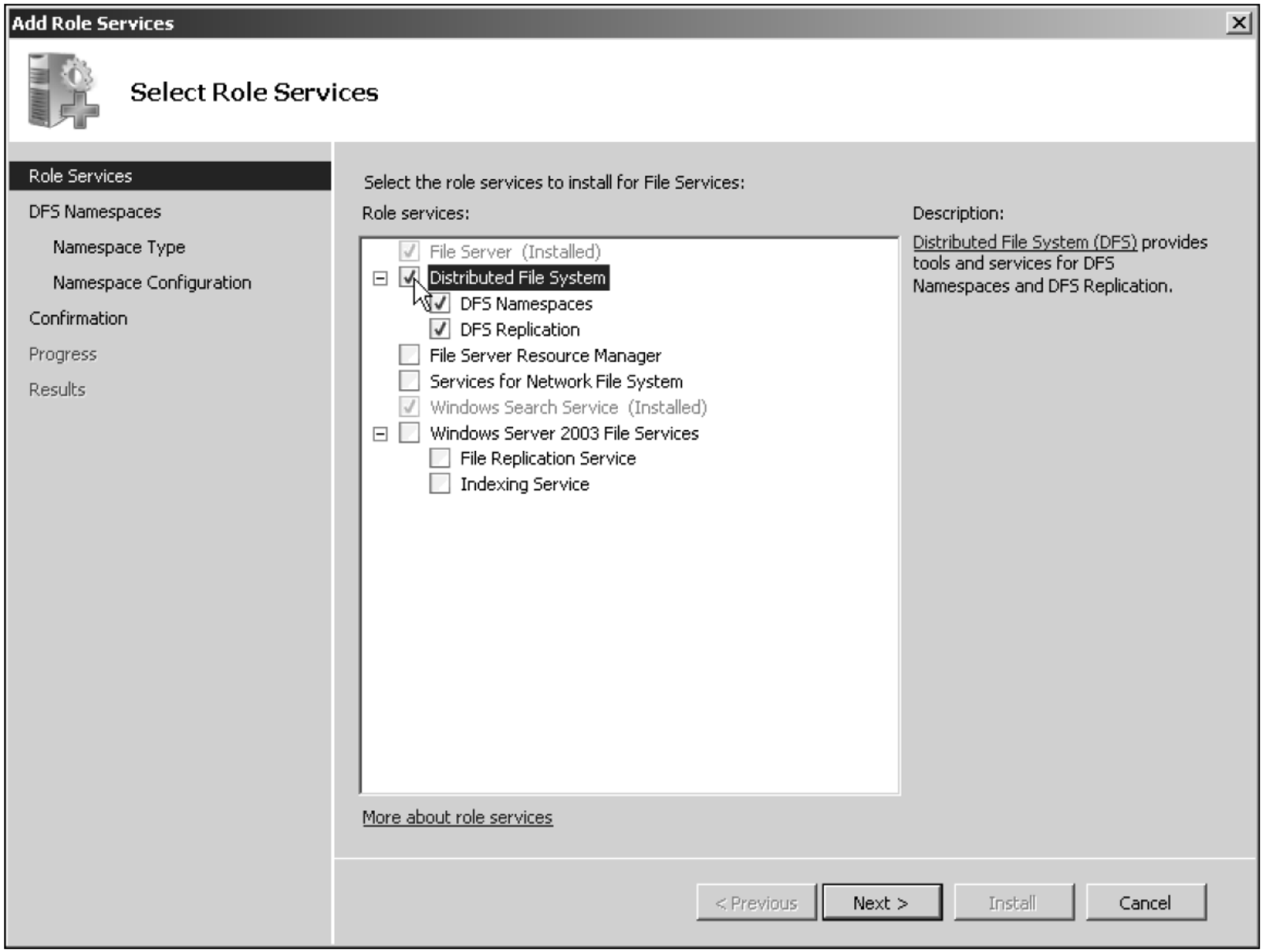

Figure 5-14 Selecting to install DFS

Installing DFS (continued)

- Activity 5-10: Creating a Namespace Root
  - Time Required: Approximately 10 minutes
  - Objective: Configure a namespace root

Managing a Domain-Based Namespace Root System

- Creating a folder in a namespace
  - A folder is simply a shared folder that you add to (or link to) the namespace root
  - **Folder target**
    - A path in the Universal Naming Convention (UNC) format, such as to a shared folder or to a different DFS path
  - **Universal Naming Convention (UNC)**
    - A naming convention that designates network servers, computers, and shared resources
  - Clients who access the namespace can see a list of folder targets ordered in a hierarchy

Managing a Domain-Based Namespace Root System (continued)

- Activity 5-11: Adding a Folder and Folder Target in DFS
  - Time Required: Approximately 5 minutes
  - Objective: Add a folder in DFS

Managing a Domain-Based Namespace Root System (continued)

- Delegating Management
  - Delegating management simply involves right-clicking the namespace and clicking Delegate Management Permissions
- Tuning a Namespace
  - Tuning options:
    - Configure the order for referrals
    - Configure cache duration for a namespace
    - Configure cache duration for a folder
    - Configure namespace polling
    - Configure folder targets as enabled or disabled

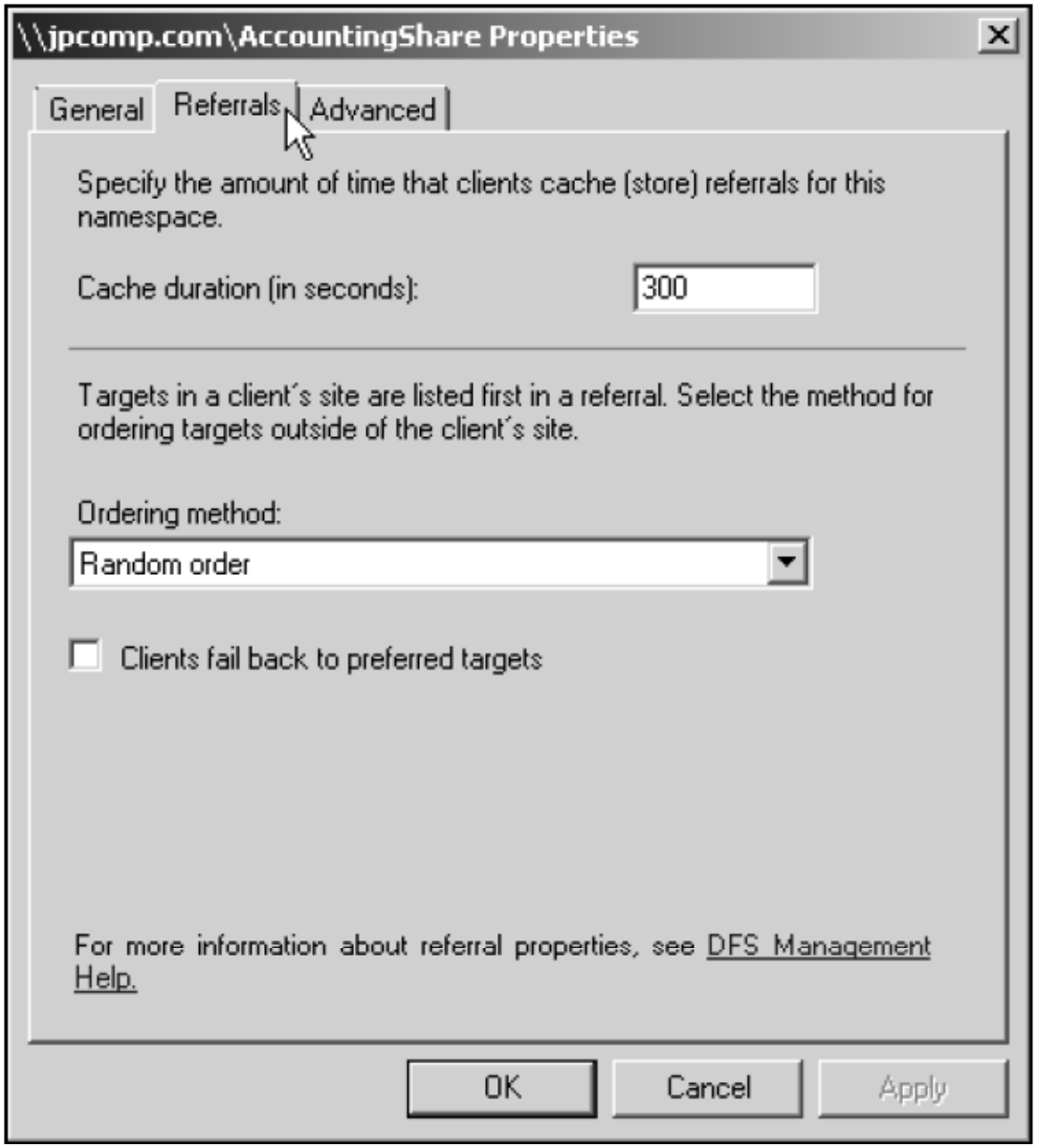

Figure 5-17 Referrals tab

Managing a Domain-Based Namespace Root System (continued)

- Deleting a namespace root
  - You can delete the namespace root via the DFS Management tool by clicking the namespace root and clicking Delete
- Using DFS Replication
  - To configure replication, you first must have defined two or more folder targets
  - You need to decide which server is to be the primary group member
    - The primary group member should be the server containing shared folders and files that are most current

Managing a Domain-Based Namespace Root System (continued)

- Windows Server 2008 includes some important improvements to DFS replication:
  - Enables faster and more reliable recovery of changes to folders in DFS when a server crashes or goes down unexpectedly, such as during a power loss
  - Replication is faster for all sizes of files
  - DFS replication is more efficient over LANs and WANs to help reduce its overhead on networks

Configuring Disk Quotas

- Disk quotas advantages:
  - Preventing users from filling the disk capacity
  - Encouraging users to help manage disk space
  - Tracking disk capacity needs on a per-user basis for future planning
  - Providing server administrators with information about when users are nearing or have reached their quota limits
- Disk quotas can be set on any local or shared volume

Configuring Disk Quotas (continued)

- You can establish disk quotas by volume or user
- Disk quota management parameters
  - Enable quota management
  - Deny disk space to users exceeding quota limit
  - Do not limit disk usage
  - Limit disk space to
  - Set warning level to
  - Log event when a user exceeds their quota limit
  - Log event when the user exceeds their warning level

Configuring Disk Quotas (continued)

- Activity 5-12: Configuring Disk Quotas
  - Time Required: Approximately 10 minutes
  - Objective: Enable disk quotas and then set a disk quota for a specific group of users

Using UNIX Interoperability in Windows Server 2008

- **Subsystem for UNIX-based Applications (SUA)**
  - Provides interoperability between Windows Server 2008 and UNIX and Linux systems
- SUA allows you to:
  - Run UNIX/Linux applications with few or no changes to the program source code
  - Run UNIX/Linux scripts
  - Use popular UNIX/Linux shells
  - Run most UNIX/Linux commands
  - Run the popular vi UNIX/Linux editor

Using UNIX Interoperability in Windows Server 2008 (continued)

- Most UNIX/Linux applications can be moved over to Windows Server 2008 SUA with only minor program code modifications
  - All applications must be recompiled in SUA
- Scripts can be moved over to Windows Server 2008 SUA and run with no or few modifications
- SUA can be set up to run in “mixed mode”
  - UNIX/Linux processes can link to Windows dynamic-link library (DLL) files

Using UNIX Interoperability in Windows Server 2008 (continued)

- **Server for Network Information Services**
  - Network Information Services (NIS) provides a naming system for shared resources on a UNIX/Linux network
  - Through the NIS server, a user can access shared resources, such as a shared partition containing shared files
  - Server for NIS also ensures the synchronization of account passwords

Using UNIX Interoperability in Windows Server 2008 (continued)

- Windows Server 2008 offers several important new features for SUA:
  - More transparent ability for UNIX/Linux applications to connect to Oracle and SQL Server databases
  - Inclusion of true 64-bit libraries for support of 64-bit applications and utilities for high-performance response
  - New utilities to support both the major UNIX versions: BSD UNIX and SVR-5 UNIX
  - Ability for application developers to use Microsoft Visual Studio for designing UNIX/Linux applications

Using UNIX Interoperability in Windows Server 2008 (continued)

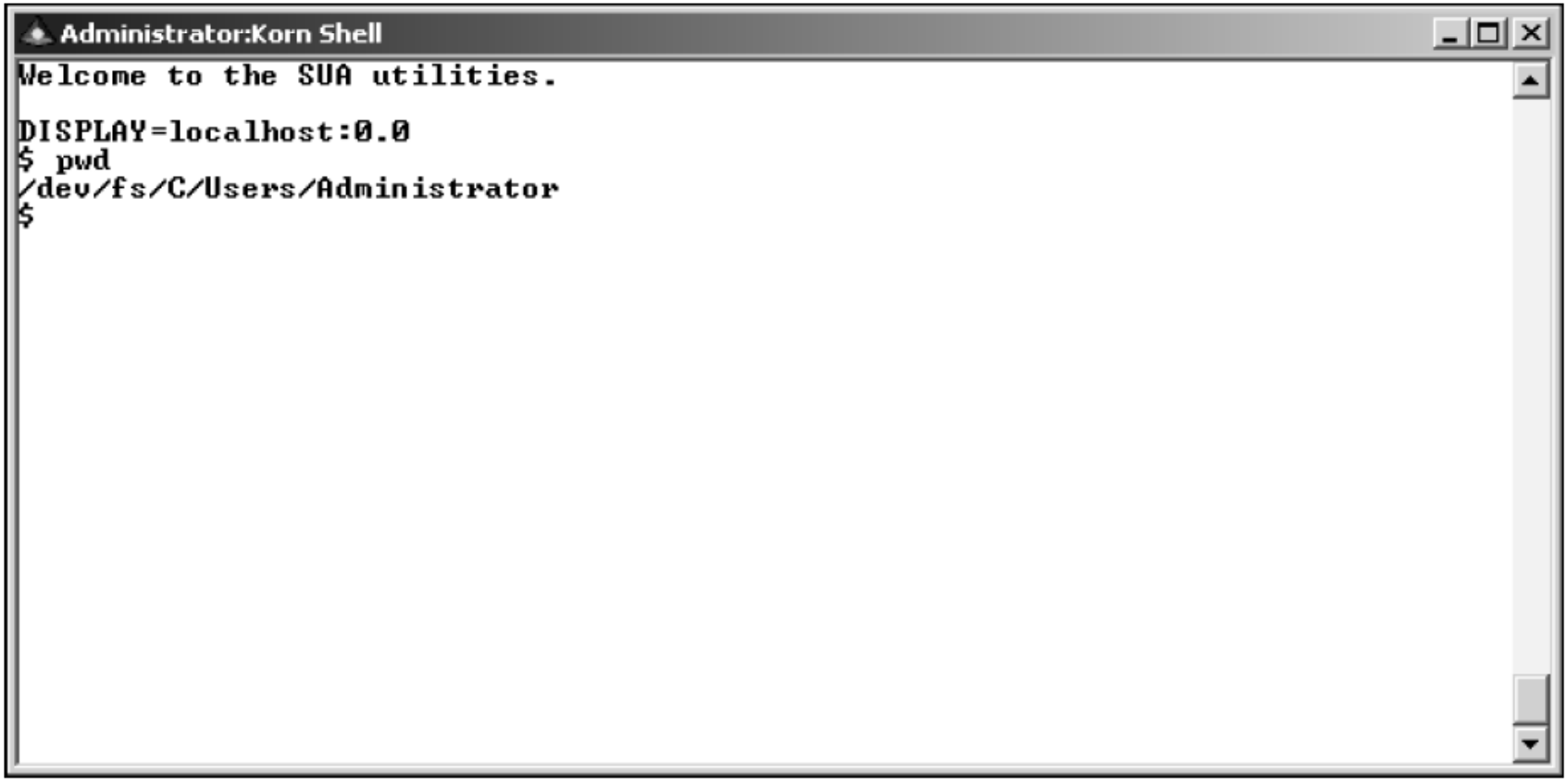

Figure 5-19 Window for using the Korn shell

Summary

- Windows Server 2008 uses discretionary access control lists for managing access to resources
- NTFS uses folder and file attributes for one level of security
- When you use the encrypt attribute, this employs the Microsoft Encrypting File System to protect files and folders
- Permissions provide another level of security for files and folders

Summary (continued)

- Special permissions provide the option to further customize security at a more granular level than basic permissions
- Folder and file auditing enable you to track who has accessed resources
- Folder and file owners have Full control permissions, including the ability to change permissions
- Folders can be shared for users to access over a network, and shared folder security is configured through share permissions

Summary (continued)

- Use the Effective Permissions capability to troubleshoot a security conflict
- The Distributed File System (DFS) enables you to set up shared folders
- Use disk quotas to manage the resources put on a server disk volume
- If you have a network that uses a combination of Windows Servers and UNIX/Linux computers, you can install the Subsystem for UNIX-based Applications