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 information with each folder and file
  - Along with other characteristics including volume label, designation as a subfolder, date of creation, and time of creation
- The advanced attributes are archive, index, compress, and encrypt

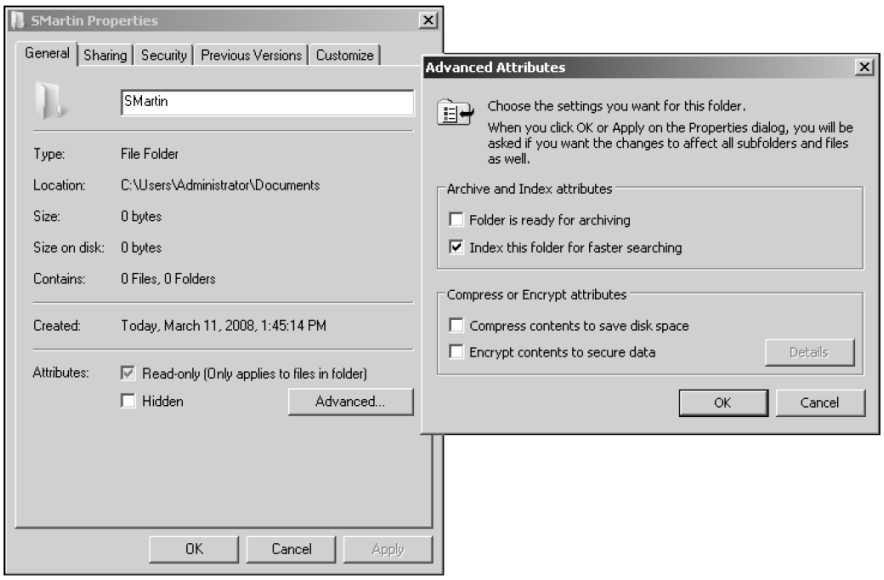

Figure 5-1 Attributes of a folder on an NTFS formatted disk

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
- Index attribute
  - The index attribute is used to index the folder and file contents so that file can be quickly searched in Windows Search Service.
  - To use the Windows Search Service, you must install the File Services role via Server Manager

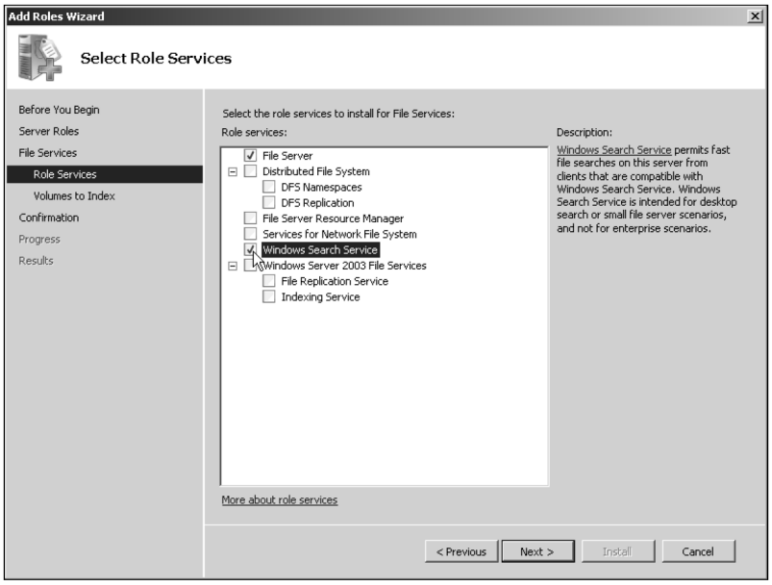

Figure 5-2 Installing the Windows Search Service with the File Services role

Configuring Folder and File Attributes (continued)

- Compress attribute
  - A folder 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.
  - 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 Permissions

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

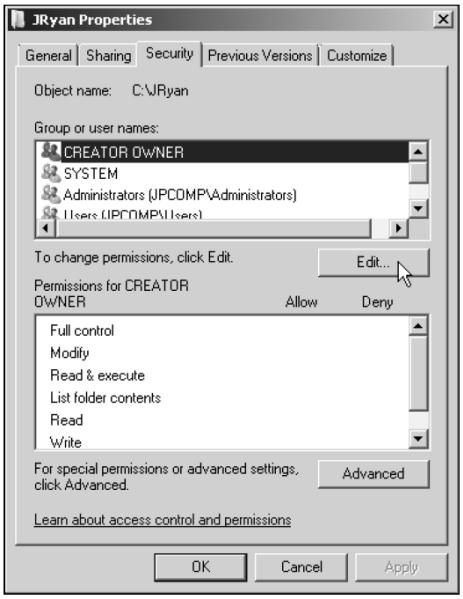

Figure 5-4 Configuring folder permissions

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 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 special permissions

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 one of the following permissions:
  - The Take ownership special permission
  - Full control permission

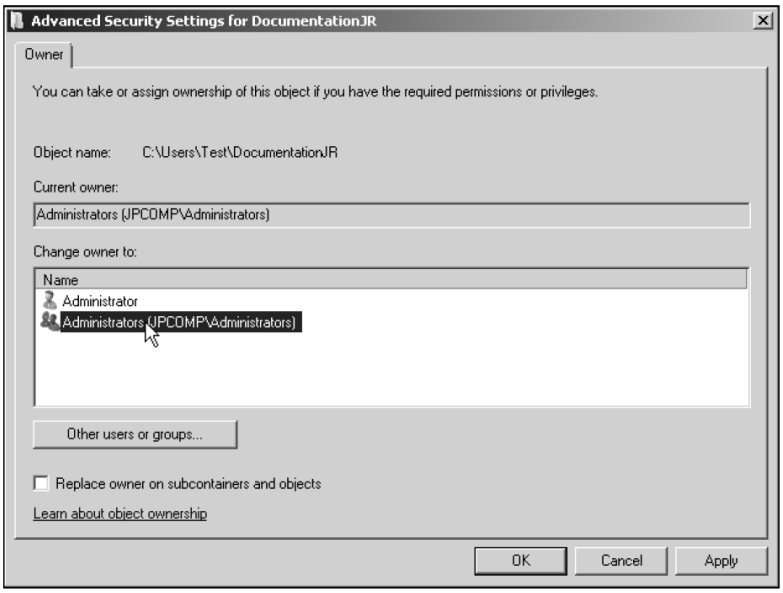

Figure 5-9 Taking ownership of a folder

Configuring Shared Folders and Shared Folder Permissions

- A folder can be set up as a shared folder for users to access over the network.
- Windows Server 2008 has improved the security when sharing folders more than older Windows Server versions.
- The first step for sharing a folder over the network is to turn on file sharing

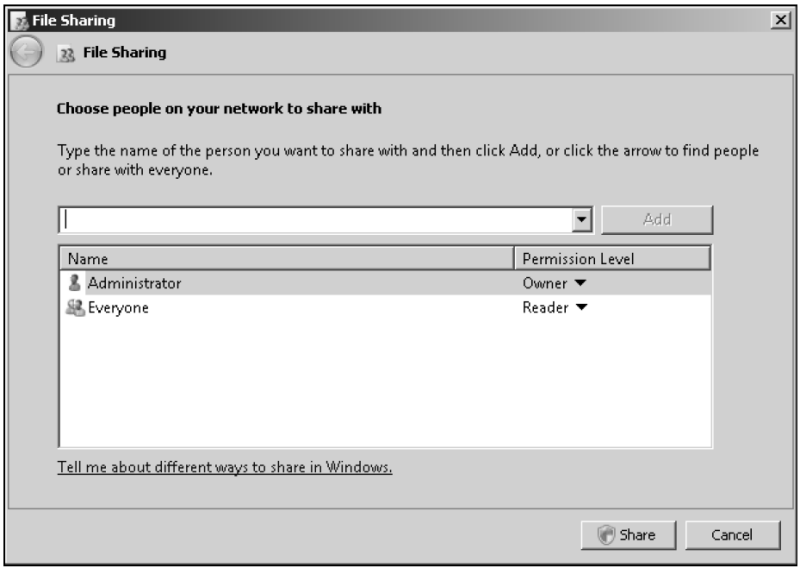

Figure 5-10 File Sharing dialog box

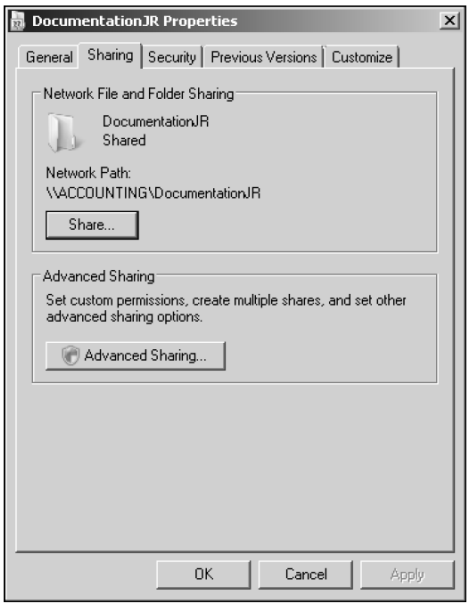

Figure 5-11 Sharing tab

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
- Share permissions:
  - Reader
  - Contributor
  - Co-owner
  - Owner

Configuring Shared Folders and Shared Folder Permissions (continued)

- You can make the contents of a shared folder available offline by caching it.
  - 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

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

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

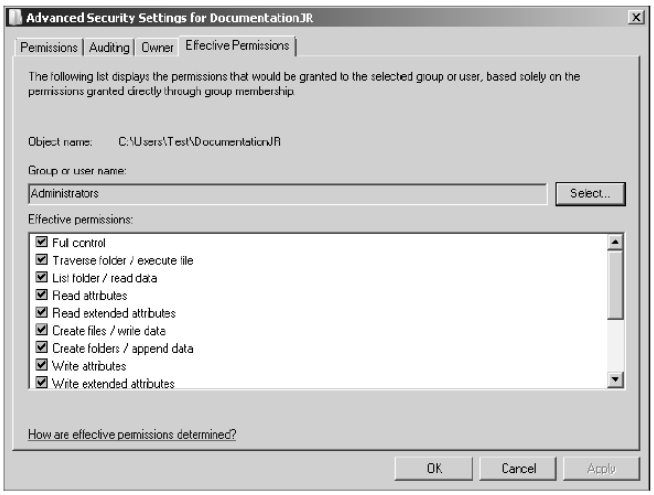

Figure 5-13 Examining effective permissions as a troubleshooting aid

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

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

Implementing a Distributed File System (continued)

- DFS advantages:
  - Shared folders can be set up so that they appear in one hierarchy of folders
  - Access to shared folders can be distributed across many servers (**load balancing**)
  - Access is improved to resources for Web-based Internet and intranet sites

Implementing a Distributed File System (continued)

- DFS advantages: (continued)
  - Critical 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
  - Folders can be replicated automatically or manually in a domain through the use of Microsoft File Replication Service

DFS Models

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

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

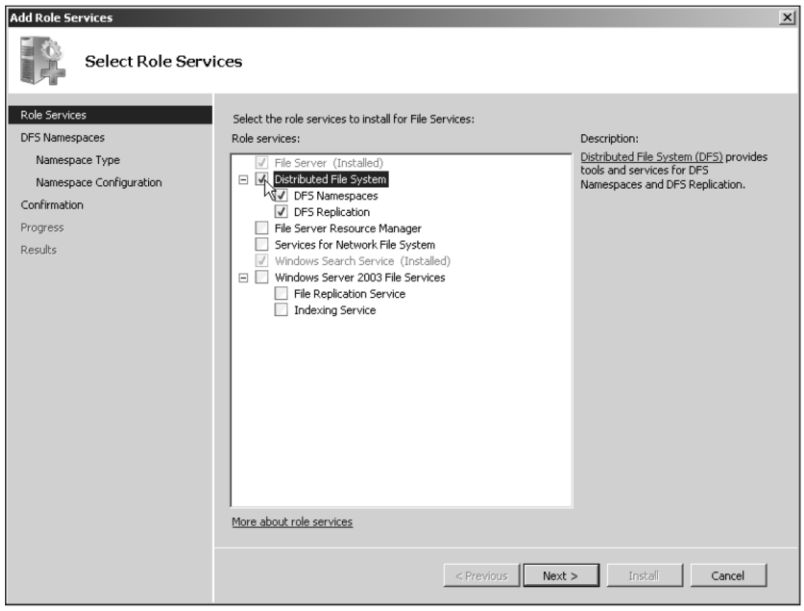

Figure 5-14 Selecting to install DFS

Configuring Disk Quotas

- Disk quotas means dividing the disk volume into partitions.
- Disk quotas advantages:
  - Preventing users from filling the disk capacity
  - Encouraging users to help manage disk space
  - Tracking disk capacity needs for each user can help for future planning of the optimal quotas size for each user.
  - Providing server administrators with information about when users have reached their quota limits

Configuring Disk Quotas (continued)

- Disk quotas can be set on any local or shared volume
- 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)

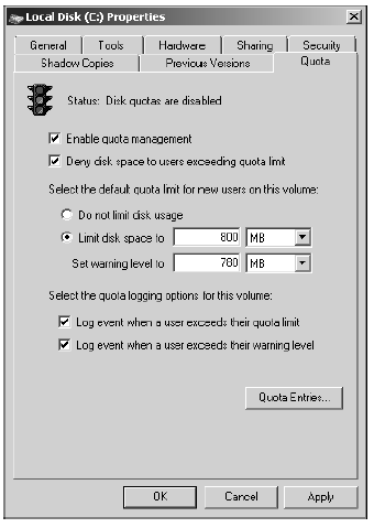

Figure 5-18 Setting default disk quotas

Using UNIX Interoperability in Windows Server 2008

- **Subsystem for UNIX-based Applications (SUA)**
  - Provides compatibility 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

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

Using UNIX Interoperability in Windows Server 2008 (continued)

- Windows Server 2008 offers several important new features for SUA:
  - Ability for UNIX/Linux applications to connect to Oracle and SQL Server databases
  - Support of 64-bit applications and utilities.
  - Ability for application developers to use Microsoft Visual Studio for designing UNIX/Linux applications

Using UNIX Interoperability in Windows Server 2008 (continued)

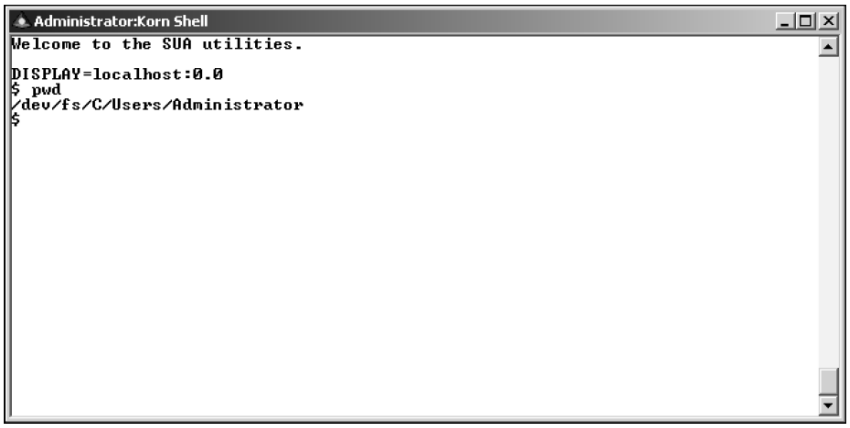

Figure 5-19 Window for using the Korn shell