4.3.3 File Permission Facts

This lesson covers managing file system permissions.

Managing File System Permissions

On a Windows system, access to files is controlled through two sets of permissions, share and New Technology File System (NTFS). The following table describes permissions specific to each type.

Permission Type	Description
Share	Share permissions control access through a network connection with the file server. - If files are accessed locally, share permissions do not control access. - Share permissions have three levels of permissions: - Reader (read only) - Contributor (read and write) - Owner or Co-owner (full control, or all permissions) - Share permissions can be set only on a folder.
NTFS	NTFS permissions: - Can be set on drives, folders, and files. - Control both local and network access. - Have dozens of permissions that offer granular control over what actions are allowed. - Can be set only on volumes formatted with NTFS.

Be aware that:

- Both share and NTFS permissions use a discretionary access control list (DACL) for controlling access. The access list identifies the users or groups and their associated permissions to files or folders.
- Both share and NTFS permissions include Allow or Deny permissions. Deny permissions override Allow permissions.
- Both share and NTFS permissions must be configured to allow access through the share. If a user is allowed share access but no NTFS permissions are set for the user or a group to which the user belongs, no access will be allowed.
- Effective permissions to shared folders are the more restrictive of either share or NTFS permissions.
- A user's effective permissions cannot be greater than the share permissions assigned to the user or a group to which the user belongs. For this reason, a common strategy for combining share and NTFS permissions is to:
  - Assign Co-owner share permissions to Everyone.
  - Use NTFS permissions to control access. Use the principle of least privilege by assigning NTFS permissions only to necessary groups and by assigning only the necessary permissions to those groups. Even though Everyone has share permissions, only the users or groups with NTFS permissions will have access.

- Permissions for folders and files can be inherited. On Windows systems, the Advanced Security settings identify when permission inheritance is in effect.

- Whenever possible, assign permissions to groups, rather than users. Users receive the permissions assigned to their groups.