11.3.3 NTFS Permission Facts

With NTFS permissions, each file and folder has an access control list (ACL). The ACL identifies the users or groups and their level of access to the folder or file. The following table summarizes the NTFS permissions for folders and files:

Permission	Allowed Actions
Read	View folder details and attributes. View file attributes; open a file.
Write	Change folder or file data and attributes.
List Folder Contents	Includes all Read actions and adds the ability to view a folder's contents.
Read & Execute	Includes all Read actions and adds the ability to run programs.
Modify	Includes all Read & Execute and Write actions and adds the ability to add or delete files.
Full Control	Includes all other actions and adds the ability to take ownership of and change permissions on the folder.

Be aware of the following facts about NTFS permissions:

- When possible, assign permissions to groups rather than individual users.
- Permissions are cumulative. Users gain the sum of all permissions granted to the user account and any groups.
- Permissions can be allowed or denied. Denied permissions always override allowed permissions. For example, if a user belongs to two groups, and a specific permission is allowed for one group and denied for the other, the permission is denied.
- In addition to the standard permissions, there are special permissions that offer finer control over the actions that can be performed on the file or the folder.
- By default, users have Full Control permissions to all files in their user profile. No other users can access files in the user profile.
- NTFS permissions control access for logged on users as well as users who access files through a network connection.

You should understand how file ownership affects access and assigning permissions.

- Every object, including files and folders, has an owner.
- The owner is typically the user who created the file.
- The owner has full control over the file and can assign permissions to the file.
- Administrators have the Take Ownership right to all objects. Administrators can assign ownership of a file or folder even if they do not have permissions to access the file.
- You can reassign ownership of a file or folder to easily give a user all permissions. You might reassign ownership when someone leaves your organization.
- If you cannot access a file because of insufficient permissions, take ownership of the file and modify the permissions.

Copying or moving files with NTFS permissions can affect the permissions on the file or folder.

- You must have the proper permissions to copy or move a folder or a file:
  - To copy a file or folder, you must have the Read permission to the source file and the Write permission to the destination location.
  - To move a file or folder, you must have Read and Modify permissions to the source file, and the Write permission to the destination location.
- If you copy or move a file to a non-NTFS partition, all permissions are removed.
- In all cases, if you copy or move a file to an NTFS partition, it will inherit the permissions assigned to the parent partition and folders.
- If a file has explicit NTFS permissions assigned to that file:
  - If you copy or move the file to a different NTFS partition, the explicit permissions will be removed.
  - If you move the file to a different folder on the same NTFS partition, the explicit permissions will be kept.
  - If you copy the file to a different folder on the same NTFS partition, the explicit permissions will be removed.

  In all cases, the file will also inherit permissions from its new partition and folder.