DISK MANAGEMENT

There are two disk Categories :

DISK	Benefits
Basic Disks	• Use to create segregated space to organize data. • Can be divided into up to 4 primary partitions, or up to 3 primary partitions and one extended partition.
Dynamic Disks	• Use to create volumes that span multiple disks. • No limit on the number of volumes per disk. • Use to create fault-tolerant disks that ensure data integrity when hardware failures occur.

Basic Disk:

A basic disk is a type of hard drive configuration, available with the Windows operating system.

To manage all partitions and data on the hard disk, normal partition tables or logical drives are used. They are the storage types most often used with Windows.

It can contain up to four primary partitions, or three primary partitions and an extended partition with multiple logical drives.

Operations to be performed:

- Create and delete primary and extended partitions.
- Create and delete logical drives within an extended partition.
- Format a partition and mark it as active.

Dynamic Disk:

A disk that has been initialized for dynamic storage is called a dynamic disk.

It gives more flexibility than a basic disk because it does not use a partition table to keep track of all partitions.

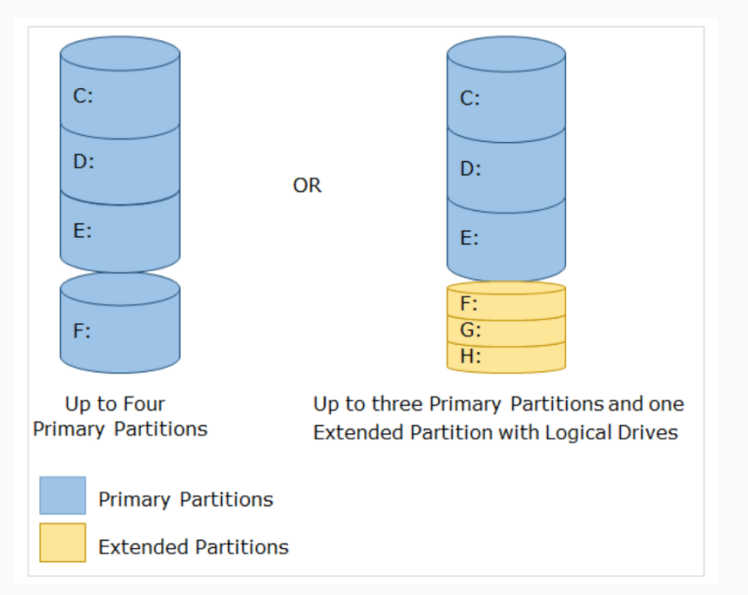
The partition can be extended with dynamic disk configuration. It uses dynamic volumes to manage data.

Operations to be performed:

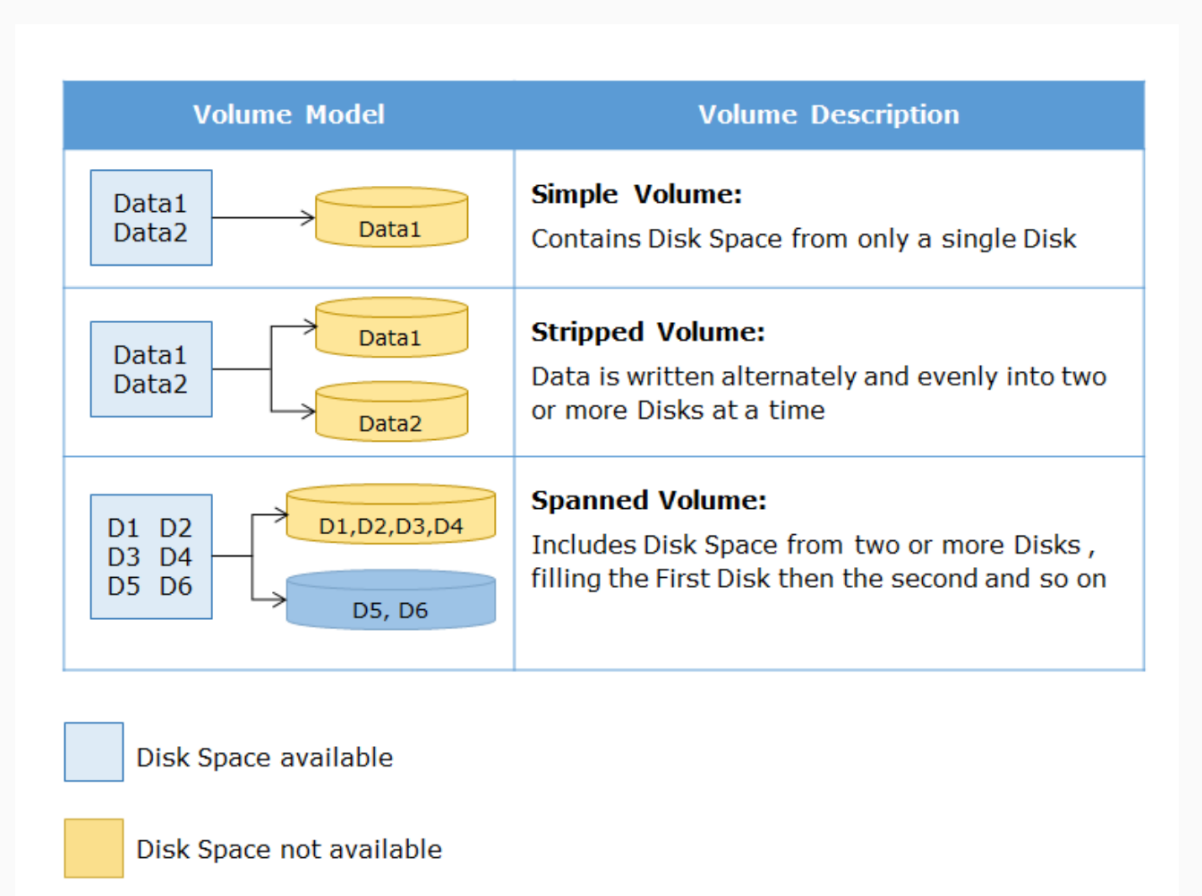
- Create and delete simple, spanned, striped, mirrored, and RAID-5 volumes.
- Extend a simple or spanned volume.
- Repair mirrored or RAID-5 volumes.
- Reactivate a missing or offline disk.

BASIC DISK PARRTITIONING:

Basic disks have four partitions. These partitions can either be four primary partitions or three primary partitions and one extended block which can have multiple logical drives.



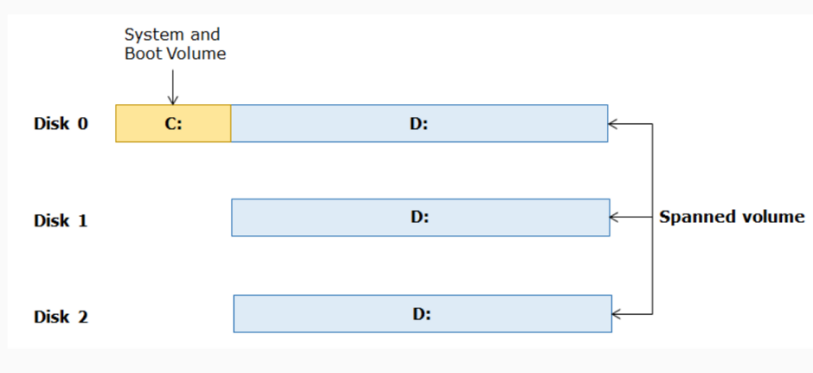
DYNAMIC DISK PARTITION:



Dynamic Disk Types:

Spanned Volume:

- Spanned volumes are preferred when we need a single partition having disk space taken from multiple hard disks.
- Involves multiple hard disks
    - Min: 2 disks
    - Max: 32 disks



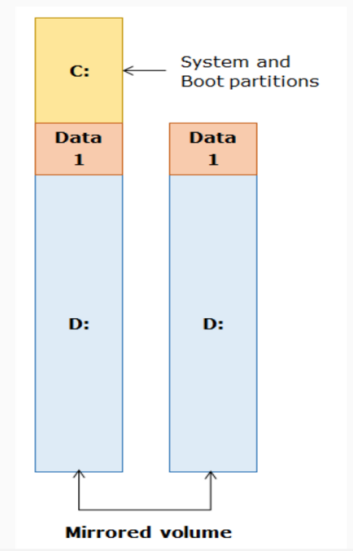
In the above image, C: drive partition is created from a single disk named Disk 0 whereas D: drive partition is created from three disks named Disk 0, Disk 1 and Disk 2.

Mirrored Volume:

- Provides 100% fault tolerance
- 50% disk utilization

Mirrored volumes are preferred for disk partitions which is very critical.

Example : The partition C: where OS is typically installed.



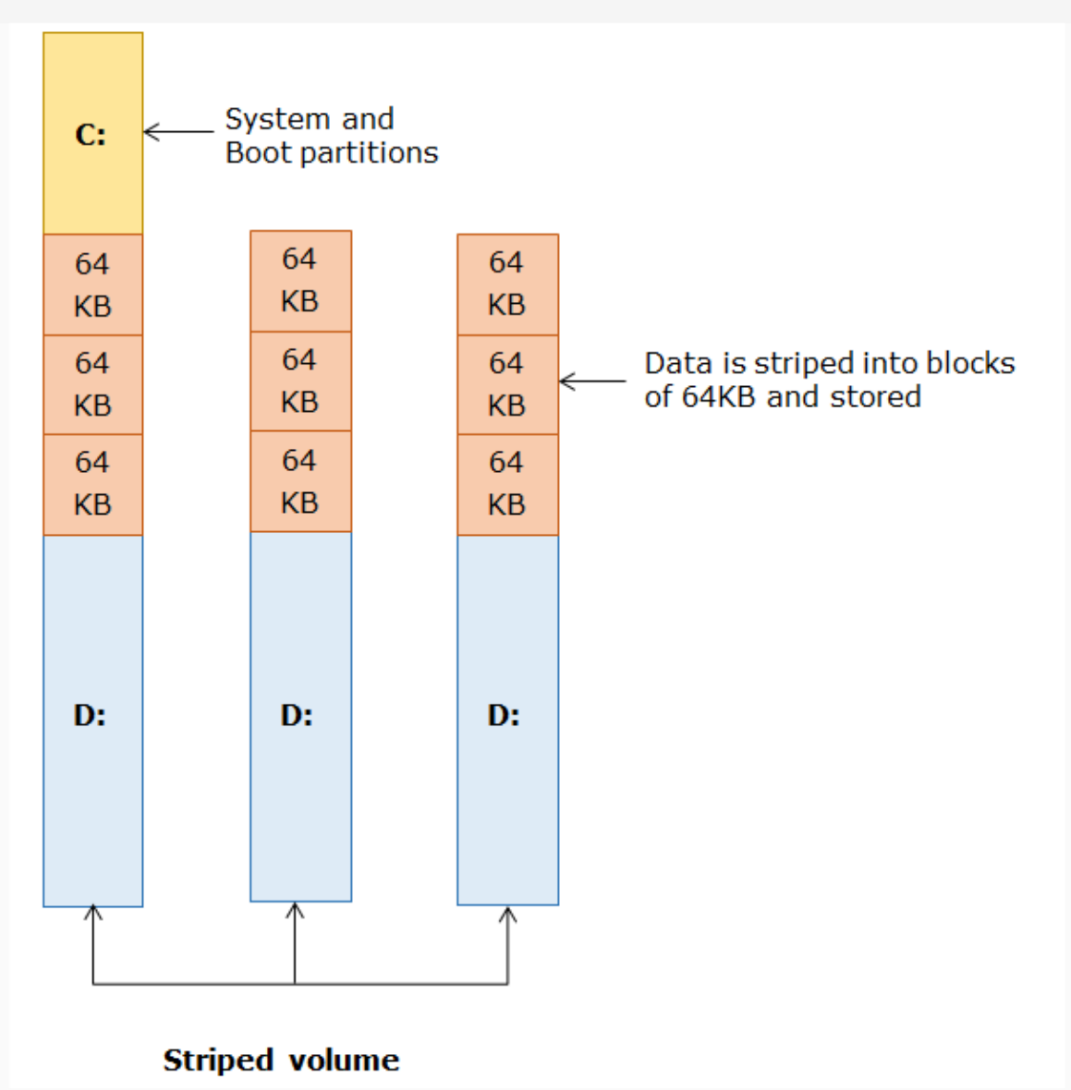
Striped Volume:

Striped volumes are preferred for partitions where high Read/Write operations are expected.

Example: The drive in which SQL log files are stored are normally created as Striped volume.

Involves multiple hard disks:

- Min: 2 disks
- Max: 32 disks

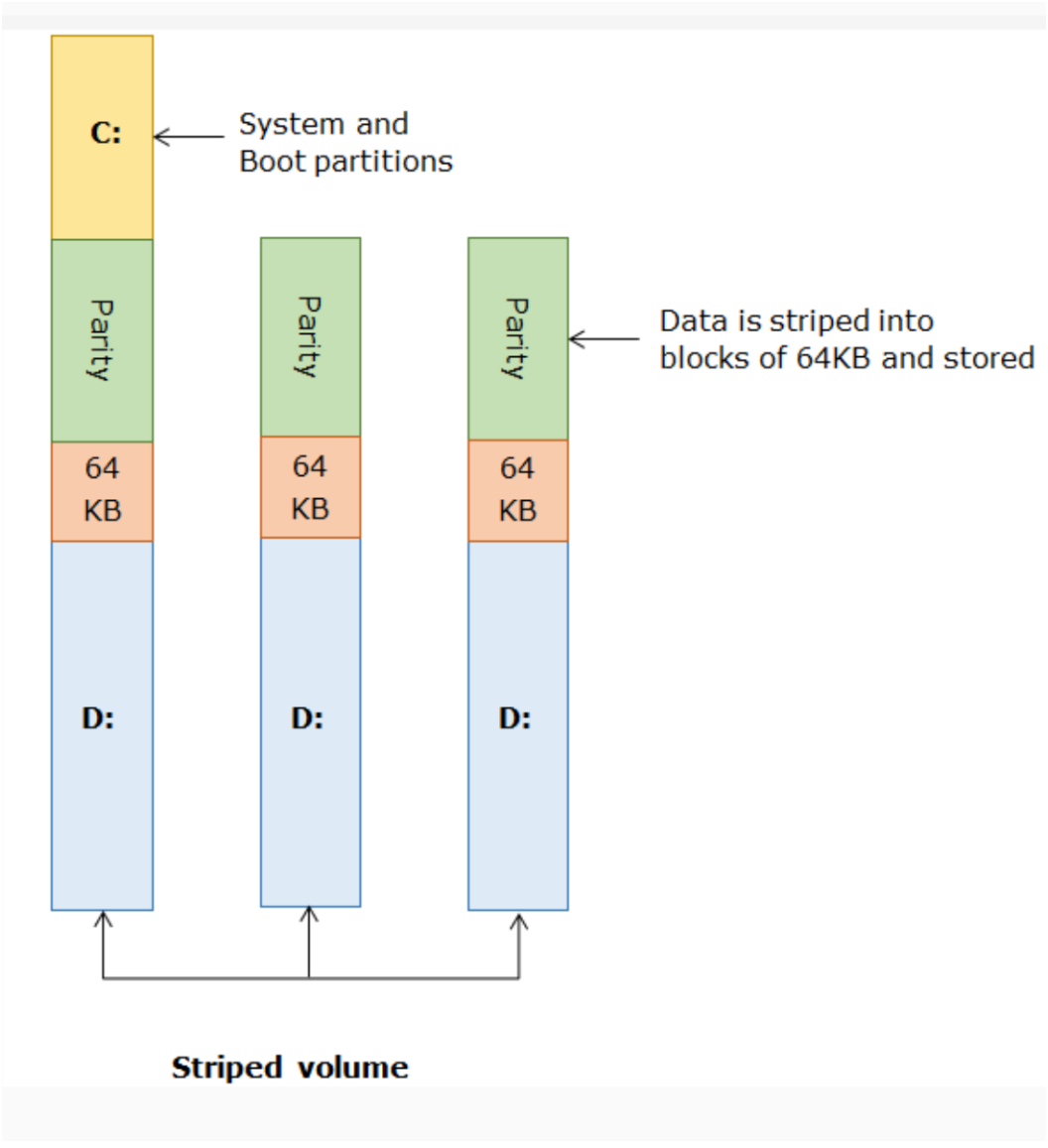


Striped with Parity:

Striped with Parity volumes are chosen where we need to strike a balance between fault tolerance and better Read/Write speed. This volume type can provide fault tolerance up to 1 disk failure and has a good Read/Write speed.

Involves multiple hard disks:

- Min: 3 disks
- Max: 32 disks



SHARING A FOLDER

1. NTFS stands for New Technology File system.

   NTFS permissions are the security controls that the administrators can enforce on files and folders on a Windows server machine.

2. NTFS permission works based on three thumb rules:

- They are cumulative in nature.
- By default, they are inherited by the child objects from the parent objects.
- "Deny permission" always takes the precedence over "Allow permission".

1. Full Control:

   Complete access on a folder and can delegate access to others.

2. Modify:

   Complete access on a folder without the access to delegate permissions to other users.

3. Read and Execute:

   View the contents of the folder and run any executable file in the folder.

4. List Folder Contents:

   View the contents on the folder.

5. Read:

   View and read the contents of the folder.

6. Write:

   View, read and write contents on the folder.

OWNERSHIP AND INHERITENCE:

Ownership:

- Owner has the right to deny or allow access to a folder.
- Administrators and Backup operators can take the ownership of a file.
- Default owner is the user who has created it.

Inheritance:

- By default, NTFS permissions are inheritable.
- Inheritance can be prevented in three ways:
    - Stop Inheritance from parent folder.
    - Configuring the parent folder.
    - Override the inherited permission with Deny permissions.

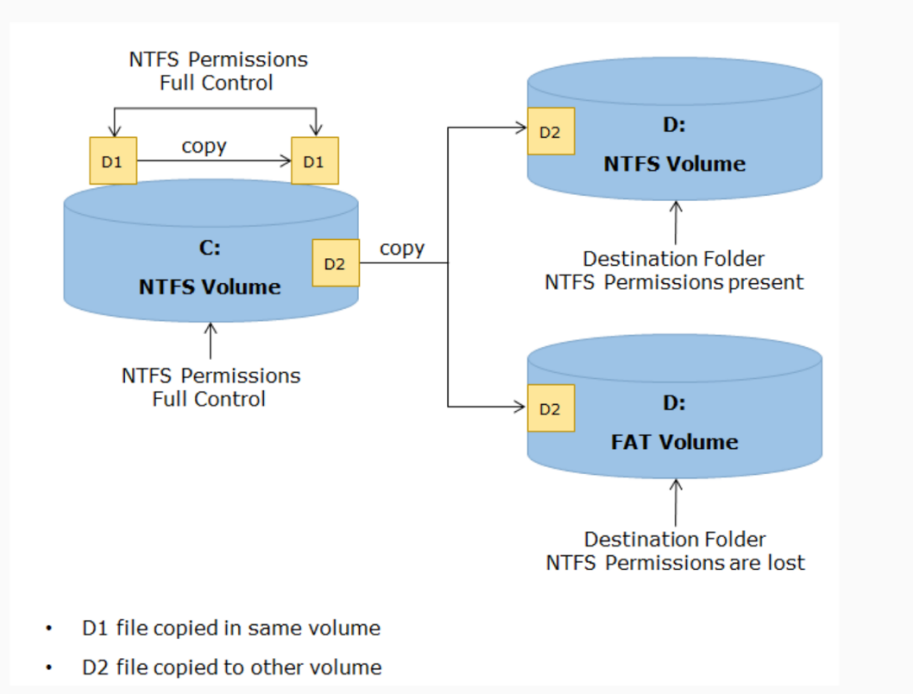
EFFECTIVE PERMISSIONS:

- A user's effective permissions for a resource are the sum of the NTFS permissions that you assign to the individual user account and to all the groups to which the user belongs.

- If a user is granted Read permission for a folder and is a member of a group with Write permission for the same folder, the user has both Read and Write permissions for that folder.

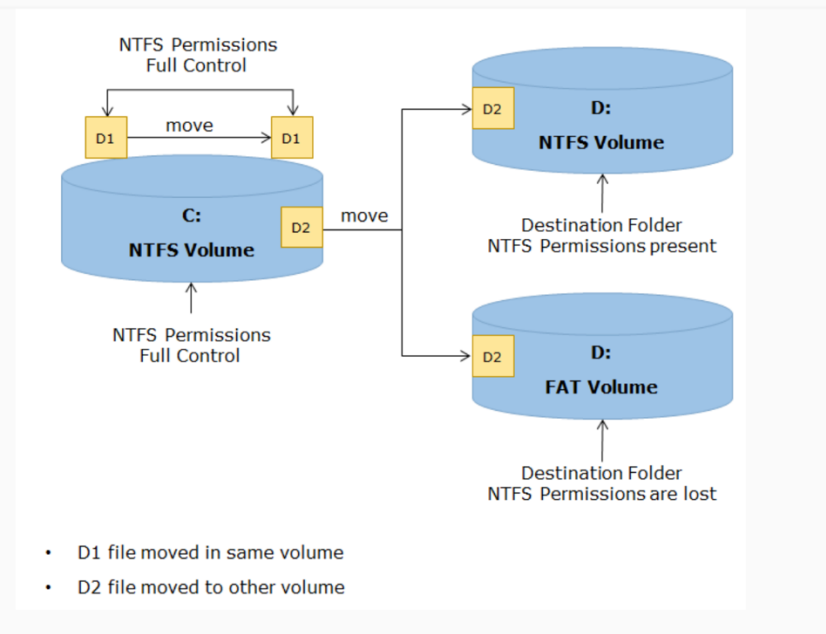
NTFS permissions while COPYING files and folders:

When you copy files or folders from one folder to another or from one volume to another, permissions change as shown in the figure:



NTFS permissions while MOVING files and folders:

- When you move a file or folder, permissions may or may not change, depending on where you move the file or folder.



Shared Folder Permissions include the following:

1. Read: Display folder names, file names, file data, and attributes; run program files; and change folders within the shared folder.

2. Change: Create folders, add files to folders, change data in files, append data to files, change file attributes, and delete folders and files; also allows the user to perform actions that are permitted by the Read permission.

3. Full Control: Change file permissions, take ownership of files and perform all tasks that are permitted by the Change permission.

- Shared folder permissions apply to folders and not to individual files.
- Shared folder permission provides less security than NTFS permissions as we can apply shared folder permission to the entire shared folder and not to subfolders or individual files in the shared folder.

- Shared folder permissions are applied to users who try to access the folder over network.

- Shared folder permissions do not provide restriction to users who access the folder locally by logging on to the computer.

The default shared folder permission is "Read". When a folder is shared, it is assigned to "Everyone".

When shared folder permissions are applied on NTFS volume, following rules apply:

- Different NTFS permissions can be applied to each subfolders and files in the shared folder.
- Apart from shared folder permissions, appropriate NTFS permissions should be provided for users to access subfolders and files in the shared folder.
- When shared folder permissions and NTFS permissions are combined, the most restrictive permission is applied.