Mawlana Bhashani Science and Technology University

Lab-Report

Report No:04

Report Name:File operation and permission

Course code:ICT-3110

Course title:Operating System Lab

Date of Performance:15-09-2020

Date of Submission:19-09-2020

Submitted by

Name:Sabikun Nahar Piya

ID:IT-18020

3rd year 1stsemester

Session: 2017-2018

Dept. of ICT

MBSTU.

Submitted to

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment No:04

Experiment Name:File operation and permission

Objectives:

A file is a named collection of related information that is recorded on secondary storage such as magnetic disks, magnetic tapes and optical disks. In general, a file is a sequence of bits, bytes, lines or records whose meaning is defined by the files creator and user.

Question: What is file operation and file permission in linux operating system?

Ans:

Linux filesystems refer to how Linux-based computers organise, store and track system files. The filesystem is basically a combination of directories or folders that serve as a placeholder for addresses of other files. In other words, there is no distinction between a file and a directory in Linux filesystem, because a directory is considered to be a file containing names of other files. Hence, software programs, services, texts, images, and so forth, are all considered files. In the same way, input and output devices are considered to be files according to the filesystem. Consequently, the filesystem provides the namespace which comprises the naming convention as to how a file can be named in terms of the length and character combinations. The namespace also includes the organisational framework which is the logical structure of the files on disk, often arranged in a hierarchical form using directory.

Most file systems have methods to assign permissions or access rights to specific users and groups of users. These permissions control the ability of the users to view, change, navigate, and execute the contents of the file system. In some cases, menu options or functions may be made visible or hidden depending on a user's permission level; this kind of user interface is referred to as permission-driven.

Question: Implementation of file operation and file permission

Ans:

Numerous on-disk and in-memory configurations and structures are being used for implementing a file system. These structures differ based on the operating system and the file system but applying some general principles. Here they are portrayed below:

A boot control block usually contains the information required by the system for booting an operating system from that volume. When the disks do not contain any operating system, this block can be treated as empty. This is typically the first chunk of a volume. In UFS, this is termed as the boot block; in NTFS, it is the partition boot sector.

A volume control block holds volume or the partition details, such as the number of blocks in the partition, size of the blocks or chunks, free-block count along with free-block pointers. In UFS, it is termed as superblock; in NTFS, it is stored in the master file table.

A directory structure per file system is required for organizing the files. In UFS, it held the file names and associated 'inode' numbers. In NTFS, it gets stored in the master file table.

The FCB contains many details regarding any file which includes file permissions, ownership; the size of file and location of data blocks. In UFS, it is called the inode. In NTFS, this information gets stored within the master file table that uses a relational database (RDBM) structure, using a row per file.

Permission Groups

Each file and directory has three user based permission groups:

Owner: The Owner permissions apply only the owner of the file or directory, they will not impact the actions of other users.

Group: The Group permissions apply only to the group that has been assigned to the file or directory, they will not effect the actions of other users.

All user: The All Users permissions apply to all other users on the system, this is the permission group that you want to watch the most.

Permission Types:

Each file or directory has three basic permission types:

Read: The Read permission refers to a user’s capability to read the contents of the file.

Write: The Write permissions refer to a user’s capability to write or modify a file or directory.

Execute: The Execute permission affects a user’s capability to execute a file or view the contents of a directory.

Discussion: Most file systems have methods to assign permissions or access rights to specific users and groups of users. These permissions control the ability of the users to view, change, navigate, and execute the contents of the file system. In some cases, menu options or functions may be made visible or hidden depending on a user's permission level; this kind of user interface is referred to as permission-driven.