

목차

00. 개요

01. 파일의 속성

02. 파일의 접근 권한

03. 기호를 이용한 파일 접근 권한 변경

01 파일의 속성

■ 파일 접근 권한 보호

- 리눅스는 파일에 무단으로 접근하는 것을 방지하고 보호하는 기능을 제공
- 사용자는 자신의 파일과 디렉터리 중에서 다른 사용자가 접근해도 되는 것과 그렇지 않은 것을 구분하여 접근 권한을 제한

■ 파일의 속성

```
user1@myubuntu:~$ ls -l /etc/hosts
-rw-r--r-- 1 root root 223  2월 20 21:17 /etc/hosts
user1@myubuntu:~$
```

파일의 속성

번호	속성 값	의미
1	-	파일의 종류(-: 일반 파일, d: 디렉터리)
2	rw-r--r--	파일을 읽고 쓰고 실행할 수 있는 접근 권한 표시
3	1	하드 링크의 개수
4	root	파일 소유자의 로그인 ID
5	root	파일 소유자의 그룹 이름
6	223	파일의 크기(바이트 단위)
7	2월 20 21:17	파일이 마지막으로 수정된 날짜
8	/etc/hosts	파일명

01 파일의 속성

■ 파일의 종류

- 파일 속성의 첫 번째 항목은 파일의 종류를 표시
- -는 일반 파일을, d는 디렉토리를 의미
- 파일의 종류를 알려주는 명령

file

기능 지정한 파일의 종류를 알려준다.

형식 file 파일명

사용 예 file /etc/services

```
user1@myubuntu:~$ file /etc/hosts temp
/etc/hosts: ASCII text
temp:      directory
user1@myubuntu:~$
```

■ 파일의 접근 권한 표시

- 파일의 소유자와 그룹이나 기타 사용자들이 파일에 대해 가지고 있는 접근 권한을 표시

■ 하드 링크의 개수

- 하드 링크는 한 파일에 대해 여러 개의 파일명을 가질 수 있도록 하는 기능

01 파일의 속성

■ 파일 소유자의 로그인 ID

- 리눅스에서 모든 파일은 소유자가 있음

■ 파일 소유자의 그룹 이름

- `ls -l` 명령에서 출력되는 그룹명은 파일이 속한 그룹
- 사용자가 속한 기본 그룹은 시스템 관리자가 사용자를 등록할 때 결정
- 사용자가 속한 그룹을 알려주는 명령은 `groups`

groups

기능 사용자가 속한 그룹을 알려준다.

형식 `groups [사용자명]`

```
user1@myubuntu:~$ groups
user1 adm cdrom sudo dip plugdev lpadmin sambashare
user1@myubuntu:~$ groups root
root : root
user1@myubuntu:~$
```

■ 파일의 크기: 바이트 단위

■ 파일이 마지막으로 수정된 날짜

02 파일의 접근 권한

■ 접근 권한의 종류

- 읽기 권한, 쓰기 권한, 실행 권한 등 세 가지로 구성

파일과 디렉터리의 접근 권한

권한	파일	디렉터리
읽기	파일을 읽거나 복사할 수 있다.	ls 명령으로 디렉터리 목록을 볼 수 있다(ls 명령의 옵션은 실행 권한이 있어야 사용할 수 있다).
쓰기	파일을 수정, 이동, 삭제할 수 있다(디렉터리에 쓰기 권한이 있어야 한다).	파일을 생성하거나 삭제할 수 있다.
실행	파일을 실행할 수 있다(셸 스크립트나 실행 파일의 경우).	cd 명령을 사용할 수 있다. 파일을 디렉터리로 이동하거나 복사할 수 있다.

■ 접근 권한의 표기 방법

- 사용자 카테고리별로 누가 파일을 읽고 쓰고 실행할 수 있는지를 문자로 표현한 것
- 읽기 권한은 r, 쓰기 권한은 w, 실행 권한은 x로 나타내며, 해당 권한이 없는 경우에는 -로 표기
- 사용자 카테고리별로 세 가지 권한의 부여 여부를 rwx 세 문자를 묶어서 표기

```
user1@myubuntu:~$ ls -l /etc/hosts
-rw-r--r-- 1 root root 223  2월 20 21:17 /etc/hosts
user1@myubuntu:~$
```

02 파일의 접근 권한

■ 접근 권한의 표기 방법



파일의 접근 권한 표기

다양한 접근 권한 조합의 예

접근 권한	의미
<code>rwxr-xr-x</code>	소유자는 읽기, 쓰기, 실행 권한을 모두 가지고 있고 그룹과 기타 사용자는 읽기와 실행 권한만 가지고 있다.
<code>r-xr-xr-x</code>	소유자, 그룹, 기타 사용자 모두 읽기와 실행 권한만 가지고 있다.
<code>rw-----</code>	소유자만 읽기, 쓰기 권한을 가지고 있고 그룹과 기타 사용자는 아무 권한이 없다.
<code>rw-rw-rw-</code>	소유자, 그룹, 기타 사용자 모두 읽기와 쓰기 권한을 가지고 있다.
<code>rwxrwxrwx</code>	소유자, 그룹, 기타 사용자 모두 읽기, 쓰기, 실행 권한을 가지고 있다.
<code>rwx-----</code>	소유자만 읽기, 쓰기, 실행 권한을 가지고 있고 그룹과 기타 사용자는 아무 권한이 없다.
<code>r-----</code>	소유자만 읽기 권한을 가지고 있다.

02 파일의 접근 권한

■ 접근 권한의 변경 명령

chmod

기능	파일이나 디렉터리의 접근 권한을 변경한다.
형식	chmod [옵션] 권한 모드 파일 또는 디렉터리명
옵션	-R : 하위 디렉터리까지 모두 변경할 수 있다.

- 기호 모드 : 접근 권한을 변경하기 위해 문자와 기호를 사용하여 권한을 표시
- 숫자 모드 : 접근 권한을 변경하기 위해 숫자를 사용

03 기호를 이용한 파일 접근 권한 변경

■ 기호 모드



기호 모드의 구성 요소

기호 모드에서 사용하는 문자와 기호

구분	문자/기호	의미
사용자 카테고리 문자	u	파일 소유자
	g	소유자가 속한 그룹
	o	소유자와 그룹 이외의 기타 사용자
	a	전체 사용자
연산자 기호	+	권한 부여
	-	권한 제거
	=	접근 권한 설정
접근 권한 문자	r	읽기 권한
	w	쓰기 권한
	x	실행 권한

03 기호를 이용한 파일 접근 권한 변경

■ 기호 모드를 사용한 접근 권한 설정의 예

기호 모드를 사용한 접근 권한 설정의 예

권한 표기	의미
u+w	소유자(u)에게 쓰기(w) 권한 부여(+)
u-x	소유자(u)의 실행(x) 권한 제거(-)
g+w	그룹(g)에 쓰기(w) 권한 부여(+)
o-r	기타 사용자(o)의 읽기(r) 권한 제거(-)
g+wx	그룹(g)에 쓰기(w)와 실행(x) 권한 부여(+)
+wx	모든 사용자에게 쓰기(w)와 실행(x) 권한 부여(+)
a+rw	모든 사용자에게 읽기(r), 쓰기(w), 실행(x) 권한 부여(+)
u=rwx	소유자(u)에게 읽기(r), 쓰기(w), 실행(x) 권한 부여(=)
go+w	그룹(g)과 기타 사용자(o)에게 쓰기(w) 권한 부여(+)
u+x,go+w	소유자(u)에게 실행(x) 권한을 부여하고(+) 그룹(g)과 기타 사용자(o)에게 쓰기(w) 권한 부여(+)

03 기호를 이용한 파일 접근 권한 변경

■ 기호를 이용한 접근 권한 변경 예

§현재 접근 권한 확인: `rw-r--r--`

```
user1@myubuntu:~/linux_ex/ch5$ ls -l
합계 4
-rw-r--r-- 1 user1 user1 223  2월 24 01:24 test.txt
user1@myubuntu:~/linux_ex/ch5$
```

§소유자의 쓰기 권한을 제거: `u-w`

```
user1@myubuntu:~/linux_ex/ch5$ chmod u-w test.txt
user1@myubuntu:~/linux_ex/ch5$ ls -l
합계 4
-r--r--r-- 1 user1 user1 223  2월 24 01:24 test.txt
user1@myubuntu:~/linux_ex/ch5$
```

03 기호를 이용한 파일 접근 권한 변경

■ 실습

- 그룹에 쓰기와 실행 권한을 부여한다
- 기타 사용자에게 실행 권한을 부여한다
- 그룹과 기타 사용자의 실행 권한을 제거한다
- 모두에게 실행 권한을 부여한다
- 소유자에게 쓰기 권한을 부여하고 그룹의 쓰기 권한은 제거한다