5. 권한관리

홍필두 교수
(리눅스프로그래밍)

한국폴리텍대학
분당융합기술교육원

1. 사용자 그룹관리
1)사용자,그룹, 권한관리
2)그룹관리 명령어
3)패스워드, 그룹관련 설정 파일

2. 권한의 이해 및 표시
1)파일,디렉토리의 소유자
2)권한의 이해
3)권한의 숫자 표기법
4)권한설정

3.링크파일
1)하드링크
2)심볼릭링크

1. 강의 들어가기

✓ 학습내용 소개

- 리눅스 서버 운영체계는 다양한 사용자가 접속하여 시스템을 이용하게 된다. 각각의 사용자는 서버 시스템을 사용할 수 있는 범위를 제한을 가지고 파일과 디렉토리등에 접근할 수 있도록 되어 있다. 시스템 관리자는 모든 권한을 가지고 시스템을 운영할 수 있으며, 일반 사용자는 자기의 영역을 사용하고 이 영역을 다른 사용자들이 사용하거나, 사용하지 못하게 조정할 수 도 있다. 이번 강의에서는 리눅스 권한관리 부분을 이해 후 실습하도록 한다.
- 앞에서 서버에 접속하기 위하여 간단하게 사용자 및 그룹의 개념에 대하여 학습하였다. 이러한 사용자와 그룹을 관리하는 방법과 설정파일에 대하여 하나 하나 배워보도록 한다.

✓ 학습목표 제시

- 사용자,그룹, 권한관리에 대하여 이해할 수 있다.
- 그룹을 관리 할 수 있다.
- 파일이나 디렉토리의 소유자의 개념을 이해할 수 있다.
- 권한의 개념을 이해하고 변경 할 수 있다.
- 링크파일의 개념을 이해할 수 있다.

2. 생각해볼 문제 및 용어

✓ 학습전 생각해볼 문제

- 윈도우에서 일반 사용자를 만들어 관리자(Administrator)와 다른 권한을 주는 방법을 알아봅니다.
- 윈도우의 탐색기를 통하여 파일 속성([읽기전용] [숨김] 등)을 바꿔봅니다.
- 바탕화면의 아이콘과 실행파일(*.exe)의 차이를 알아봅니다.

✓ 용어 (강의 정리 시 필기 할 것)

- Link
- 권한, 관리자

3. 이해하기

(1) 사용자 그룹관리

앞에서 서버에 접속하기 위하여 간단하게 사용자 및 그룹의 개념에 대하여 학습하였다. 이러한 사용자와 그룹을 관리하는 방법과 설정파일에 대하여 하나 하나 배워보도록 한다.

1) 사용자, 그룹, 권한관리

유닉스,리눅스는 여러 사람이 사용하는 다중사용자 운영체계로 사용자 묶음의 그룹 개념이 존재한다

①사용자는 여러 개의 그룹에 포함될 수 있음

②사용자 및 그룹관리 명령어

·id : 현재의 사용자를 알아보는 명령 uid(user) gid(group) 시작 id 1000번

·groups : 현재의 그룹을 알아보는명령

·adduser : 사용자를 등록하는 명령어

·addgroup: 그룹을 등록하는 명령어

·deluser: 그룹을 등록하는 명령어

·delgroup: 그룹을 등록하는 명령어

③사용자와 그룹은 시스템 내부에서 숫자로 표시됨

·uid: 사용자를 표시하는 숫자

·gid: 그룹을 표시하는 숫자

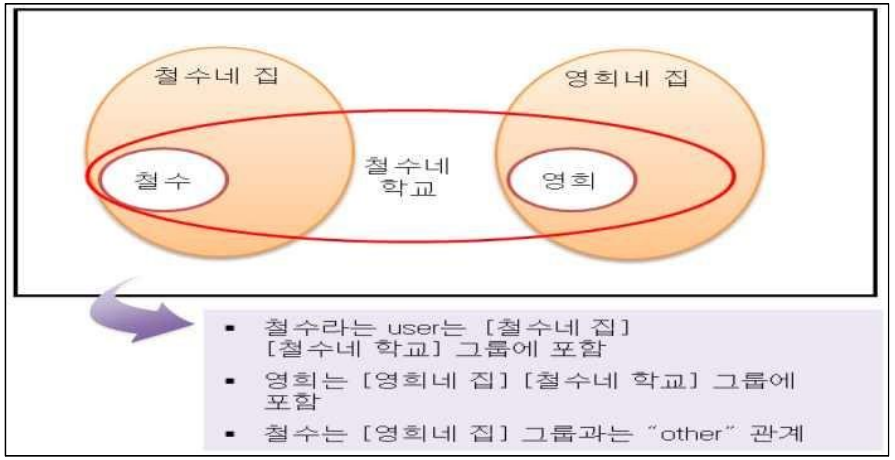
·<그림 II-xx>에서 보면 kopoctc이라는사용자는 uid(사용자id)가 1000이고 gid(그룹id)는 1000이며, 해당되는 그룹은 kopoctc이라는 그룹 한 개에만 속함

3. 이해하기

```
kopoctc@kopoctc:~$ id
uid=1000(kopoctc)                                    gid=1000(kopoctc)
groups=1000(kopoctc),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),114(lpadmin)
,115(sambashare)
kopoctc@kopoctc:~$ groups
kopoctc adm cdrom sudo dip plugdev lpadmin sambashare
kopoctc@kopoctc:~$
```

<그림 II-1> id, groups 명령어

④ 사용자와 그룹관계를 나타내는 그림 **<II-1>** 참고



<그림 II-2> 사용자와 그룹의 관계

2) 그룹관리 명령어

파일을 탐색하기 위한 명령으로 pwd, cd, ls가 있다. <그림 Ⅰ-35>

① 그룹조회

- 자기가 속한 그룹 : groups , id
- 서버 내 전체 정의되어 있는 그룹을 보려면 /etc/group 파일을 봄 <그림 Ⅱ-3>

```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kopoctc,syslog
tty:x:5:
disk:x:6:
voice:x:22:
cdrom:x:24:kopoctc
floppy:x:25:
tape:x:26:
sudo:x:27:kopoctc
audio:x:29:  dip:
x:30:kopoctc
"/etc/group" [readonly] 57L, 774C
```

<그림 Ⅱ-3> group 정의 파일

② 그룹을 생성하기 위하여 groupadd를사용

Tip 예) groupadd -g 900 kopoctc : kopoctc라는 그룹을 gid를 900번으로 생성

3. 이해하기

③ 그룹을 변경하기 위하여 **groupmode**를사용

Tip 예) groupmod –g 700 kopogroup: koporoup라는 그룹을 gid를 700번으로 변경

Tip 예) groupmod –n newkopo kopogroup : kopogroup라는 그룹을 명칭을 newkopo로 변경

③ 그룹을 삭제하기 위하여 **delgroup**을사용

Tip 예) delgroup newkopo : newkopo라는 그룹을 삭제

3) 패스워드, 그룹관련 설정 파일

유닉스, 리눅스 시스템에는 패스워드, 사용자, 그룹에 관련되어 설정되어 있는 중요파일이 있다.

①사용자 정보 파일

·/etc/passwd파일

·사용자의 정보로 user, password, uid, pid 정보가 기록되며 해당 파일의 수정 삭제 등으로 사용자관련 설정 변경도 가능

②그룹 정보 파일

·/etc/group파일

·그룹의 정보가 기록되며 해당 파일의 수정 삭제 등으로 사용자 관련 설정 변경도 가능

·groupadd, groupmod, delgroup 의 명령어를 통하여 그룹관리를 하는 것이 일반적

③패스워드관련 파일

·/etc/shadows파일 : /etc/passwd파일과 함께 사용자 패스워드를 저장

· 단 페스워드는 암호화 되어있는 문장으로 패스워드는 함부로 바꿀 수 없으며 이 파일에서 패스워드 필드를 고치면 시스템 오류가 발생

· passwd 파일 내부 형식

```
username:password:uid:gid:gecos:homedir:shell
```

·username : 사용자 명

·password : 사용자 암호

·uid: 사용자아이디, 그룹아이디

3. 이해하기

·gid : 사용자아이디, 그룹아이디

·gecos : General Electric Comprehensive Operating System (예전 Unix서비스와 호환성을 갖추기 위하여 만든 필드, 처음 사용자 정보 넣은 값들이 저장)

·homedir : 해당 사용자의 기본 디렉토리

·shell : 해당 사용자가 사용하는 Unix shell의 종류

Tip 모든 시스템 정보파일은 root 사용자만 수정 및 쓰기 권한을 갖을 수 있도록 권한이 제한되어 있다. 그러므로 해당 파일을 조회할 때도 수정되지 않도록 주의를 기울인다.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:103:106::/var/run/dbus:/bin/false
"/etc/passwd" [readonly] 29L, 1415C
```

<그림 II-4> 사용자 정보파일

4. 실습하기(1)

1) 사용자, 그룹 관리

① /etc/passwd 조회 (cat으로 조회후 캡처)

② 각 위치의 내용을 확인하고 앞 설명과 일치하는 지 확인(생략)

③ 사용자 생성, 삭제를 통한 passwd파일 변경확인(패스워드 변경전후 캡쳐)

④ 해당 id로 로그인 한 후 해당 id가 속하는 그룹과 홈 디렉토리 등을 확인 (두개이상ID로 로그인 후 기본디렉토리 캡쳐)

⑤ 그룹조회, 그룹생성, 그룹변경, 그룹삭제 과정 실습.

⑥ 각 절차 별로 /etc/group파일을 조회하여 변경유무를 확인

⑦ 사용자(user)가 속하는 그룹을 변경, 추가함에 따라 권한이 변경되는지 확인.

⑧ /etc/shadow파일 조회 캡쳐

(2) 권한의 이해 및 표기

다중 사용자를 위한 운영체계인 유닉스, 리눅스에서는 파일이나 디렉토리에 대하여 권한을 주어서 관리한다. 이러한 권한을 표기하거나 관리하는 방법에 대하여 하나하나 배워보도록 한다.

1) 파일, 디렉토리의 소유자

파일이나 디렉토리는 소유자가 해당사용권한을 가지고 있으며, 해당 파일과 디렉토리의 사용자 및 관리자(root)는 이러한 권 한을 바꿀 수 있다.

① 파일이나 디렉토리의 소유자

· 처 음 파일이나 디렉토리를 생성한 User의 소유로 생성.

kopoctc 라는 사용자로 접속하여 파일을 하나 만들었다면, 해당 파일은 kopoctc가 소유권을 가짐

② 파일,디렉토리 소유 사용자 권한 변경

·chown :파일 또는 디렉토리의 소유사용자를 바꿈

change owner

Tip 예) chown kopoctc aa : aa파일을 kopoctc 라는 사용자의 소유로 바꿈

③ 파일,디렉토리 소유 그룹 권한 변경

·chgrp :파일 또는 디렉토리의 소유 그룹을 바꿈

change group

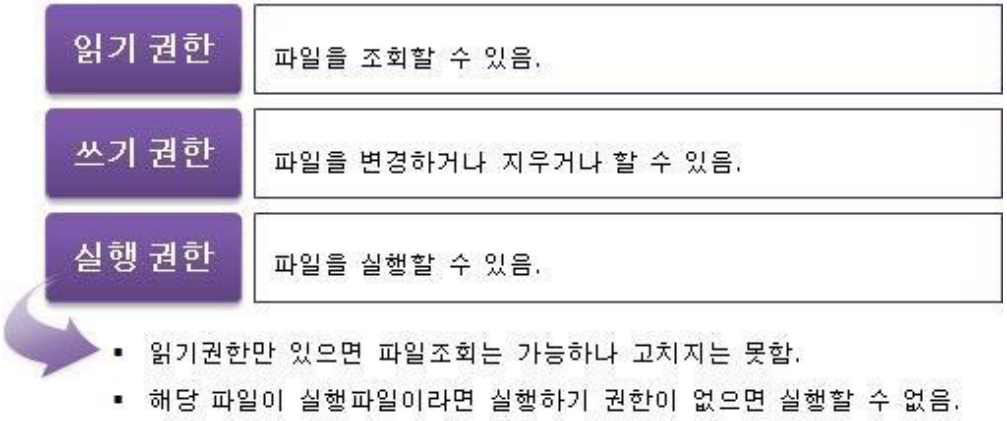
Tip chgrp kopoctc aa : aa파일을 kopoctc라는 그룹의 소유로 바꿈

2) 권한의 이해

파일이나 디렉토리에 대하여 관련 사용자와 그룹의 권한(permission)을 표기하고 관리하는 방법에 대하여 알아본다.

① 3단계권한

·파일이나 디렉토리의 권한은 <그림 Ⅱ-5> 와 같이 읽기, 쓰기, 실행 권한의 3단계로 나누어짐



<그림 Ⅱ-5> 3단계 권한

·권한 부여는 소유자(user), 그룹(group), 다른 사용자(other)에 대하여 부여함.

· 즉 하나의 파일이나 디렉토리에 대하여 소유자, 같은 그룹의 사용자, 그 외에 사용자에 대하여 파일 읽기, 쓰기, 실행하기의 권한을 지정

② ls -al 로 조회

·ls -al 명령으로 보여지는 내용으로 각각의 파일, 디렉토리의 권한을 알 수 있음

3. 이해하기

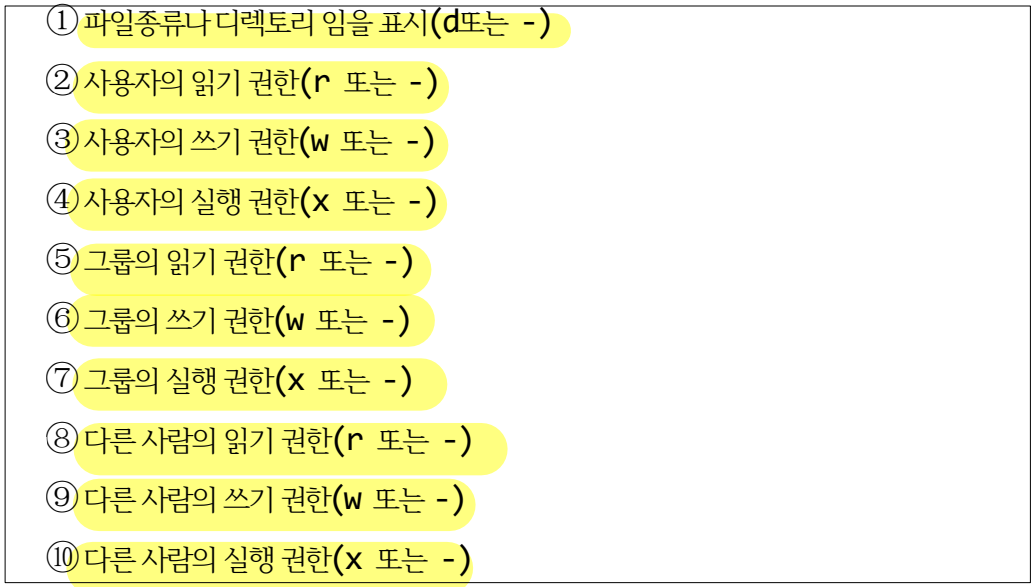
d로시작 디렉토리
-로시작 파일

```
kopoctc@kopoctc:~$ ls -al
total 44
drwxr-xr-x 4 kopoctc kopoctc 4096 Jan 18 11:16 .
drwxr-xr-x 4 root    root    4096 Jan 18 11:09 ..
-rw------- 1 kopoctc kopoctc  577 Jan 18 11:11 .bash_history
-rw-r--r-- 1 kopoctc kopoctc  220 Dec 23 11:44 .bash_logout
-rw-r--r-- 1 kopoctc kopoctc 3486 Dec 23 11:44 .bashrc
drwx------ 2 kopoctc kopoctc 4096 Dec 23 11:45 .cache
-rw-r--r-- 1 root    root       7 Jan 18 10:50 help2.txt
-rw-r--r-- 1 root    root       7 Jan 18 10:50 hepl3.txt
drwxrwxr-x 2 kopoctc kopoctc 4096 Jan 18 11:06 mydir
-rw-r--r-- 1 kopoctc kopoctc  675 Dec 23 11:44 .profile
-rw------- 1 kopoctc kopoctc 3001 Jan 18 11:16 .viminfo
kopoctc@kopoctc:~$
```

<그림 II-6> ls -al 실행

- 파 일 또는 디렉토리를 나타내는 해당 라인의 처음 필드 10자리는 다음과 같은 의미를 가짐

3. 이해하기



<그림 II-7> 10자리 권한표시

Tip

예)처음 10개의 필드가 drwxr—r— 로 표기되었다고 가정한다면

ls에서 조회되는 처음 10개의 문자는 (1, 3, 3, 3)으로 나누어 보면(d rwx r- r--)

a) 처음 비트는 파일이면 - , 디렉토리이면 d로 표시
b) 다음 3자리는 소유자 (user)의 허가권
c) 다음 3자리는 그룹의 허가권
d) 다음 3자리는 소유자도 그룹도 아닌 자(other)의 허가권

그러므로 해당내용은 먼저 해당파일은 디렉토리이며, 소유자는 읽고 쓰고 실행하는 것 이 가능하고, 같은 그룹의 사용자는 읽기는 가능하지만 쓰거나 실행할 수 없고, 관련없 는 다른 사용자는 읽기는 가능하지만, 쓰거나 실행할 수 없음을 의미함

3) 권한의 숫자 표기법

앞서서 파일이나 디렉토리에 대한 권한(permission)을 10개의 자리로 표기하는 방법을 알아보았다. 권한을 관리하는데 이러한 10개의 표기법과 함께 이를 숫자로 나타내는 방법이 있는데 이에 대하여 알아보도록 한다.

① 권한의 숫자 표기법

·권한에 대한 부분을 대상자와 3단계 권한을 결합하여 다음과 같이 3자리 숫자로 나타냄

·3자리 숫자는 순서대로 사용자, 같은그룹사용자, 다른사용자를 의미

·읽기(4), 쓰기(2), 실행하기(1)로 보고 각각의 권한 부여를 더한 값을 사용<표 II-1>

파일 속성	소유자(User)			그룹(Group)			다른 사람(Other)		
	읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행
	r(4)	w(2)	x(1)	r(4)	w(2)	x(1)	r(4)	w(2)	x(1)

<표 II-1> 10자리 권한표시

Tip

예) 사용자가 rx의 권한, 그룹이 wx의 권한, 다른 사람은 아무 권한을 가지지 않는다면, 사용자 r(4) + x(1) = 5 , 그룹 w(2) + x(1) = 3, 다른 사람 0으로 보고 그 파일은 530의 권한을 가지고 있다고 표현

4)권한설정

권한을 설정하는 방식은 상대모드와 절대모드가 있다.

chmod 775 aa (절대모드)

① 상대모드

- 현 재 권한을 기준으로 권한을 제거하거나 부여하는 방식
- 상대모드 표현시 아래와 같은 방식으로 표기

u+r -r
u+w
+x

chmod u
g
o
a

Operator	의미	Access_class	의미
+	권한부여	u	사용자
-	권한제거	g	해당 그룹의 멤버들
=	권한유지	o	다른 사람
S	사용자와 그룹만 실행	a	사용자, 그룹, 다른 사람 모두 권한부여

<그림 II-8> 상대모드 권한표시

Tip 예) chmod g-w aaa : aaa파일에서 그룹의 쓰기권한을 제거

Tip 예) chmod g+rw aaa : aaa파일에서 그룹의 읽기 쓰기권한 부여

Tip 예) chmod a+x aaa : aaa파일에서 모두 실행권한을 부여

Tip 예) chmod o-rwx aaa : aaa파일은 다른 사람은 읽거나, 쓰거나, 실행하지도 못하도록 함.

② 절대모드

- 권한의 숫자표기법을 이용하여 권한을 표기
- 기존 부여된 권한은 무시되며 새롭게 지정된 권한으로 재 설정
- 앞에서 설명된 권한 숫자표기 방식대로 사용자 r(4) w(2) x(1), 그룹r(4) w(2) x(1), 다른사람 r(4) w(2) x(1)으로 표시한값을 각 권한자 별로 더한 값으로 나타냄 <그림 II-xx>

파일 속성	소유자(User)			그룹(Group)			다른 사람(Other)		
	읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행
	r(4)	w(2)	x(1)	r(4)	w(2)	x(1)	r(4)	w(2)	x(1)

<표 II-2> 10자리 권한표시

Tip

예) 사용자가 읽고, 실행하고, 그룹 멤버는 쓰고 실행할 수 있는데, 다른 사람은 실행할 수 없게 하는 권한은?

- 사용자 r(4) + x(1) = 5 , 그룹 w(2) + x(1) = 3, 다른 사람 0 이므로 권한의 숫자 표현은 530임.
- 이런 권한을 aa파일에 부여한다면 [chmod 530 aa]로 명령

Tip

- 시스템 설정 파일 등은 관리자 이외에는 읽기, 쓰기, 실행하기 등을 제한하여야 함
- 일반 사용자가 시스템 설정을 마음대로 바꿔서는 안 되며, 사용하다 실수로 바뀌어 서도 안 됨

2) chown, chgrp실습
① kopoctc 사용자로 접속하여 파일을 생성 : kopoctc의 소유권. (각자의 id)
② chown s1111111 aa : aa파일을 s1111111 라는 사용자의 소유로 바꿈 (id하나생성)
③ chgrp s1111111 aa : aa파일을 s1111111 라는 그룹의 소유로 바꿈
④ 앞 실습을 하며 ls –al명령으로 각 파일의 권한을 조회하고 어떤 권한이 있는지 확인

3) 상대모드 실습
① chmod g-w aaa
② chmod g+rw aaa
③ chmod a+x aaa
④ chmod o-rwx aaa
⑤ 실행 후 ls –al로 권한설정 변경 확인

4)절대모드 실습
① chmod 744 aaa (어떤 명령일까요?)
② chmod 553 aaa
③ chmod a-x aaa를 절대모드로 변경하면?
④ chmod o-rwx aaa : 절대모드로 어떻게 변경해야 하나?
(권한 조회를 하고 사용자와 그룹의 권한은 그대로 주어야 함)
⑤ chmod –R 555 디렉토리명 : 하위 디렉토리에 모든 파일들의 권한을 바꿈

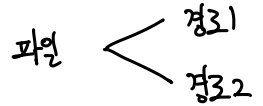
(3) 링크 파일 (윈도우 바로가기)

시스템을 운영하다 보면 하나의 파일을 여러 디렉토리에 가져다 사용하는 경우가 있다. 윈도우 운영체계에서 예를 들면 아이 콘이 이와 비슷한 개념이다. 바탕화면에 있는 윈도우 브라우저 아이콘은 바탕화면의 아이콘을 클릭하여 해당 프로그램이 실행 되지만 해당 파일은 바탕화면 디렉토리가 아닌, 윈도우의 프로그램의 익스플로러 디렉토리의 실행파일이 연결되어 있는 경우이 다. 바탕화면의 아이콘을 삭제한다고 해당 파일이 지워지는 것은 아니며, 연결만 지워지는 경우이다. 유닉스와 리눅스에도 이러 한 파일이 있는데 링크파일이 그러한 역할을 한다. 이번에는 링크파일에 대하여 하나하나 배워보도록 한다.

1) 하드링크

하드링크(hard link)의 두 파일명은 같은 디스크에 위치한 같은 데이터를 가리키며 다음과 같은 특징이 있다.

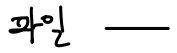
① 특징



·하드링크의 두 파일명은 같은 디스크에 위치한 같은 데이터를 가리킴

·하드링크는 원본파일과 완전히 동일하고, 부가적인 디스크 공간을 차지하지 않음

·하드링크 파일은 원본과 동일하기 때문에 하드링크 파일을 지우면 원본도 삭제됨 윈도우운영체계에는 없는 개념



② 하드링크로 연결하기

·하드링크로 연결 ln명령

·ln abc abc2: abc라는파일을 abc2라는하드링크파일로 연결, abc2 파일은 새로 생성됨

·해 당 파일상태를 보는 명령은 stat

·<그림 Ⅱ-9>에서ln abc l_abc로하드링크를 실행한 경우, abc와l_abc 는 동일한 파일이 연결되어 있음을 알 수 있다

3. 이해하기

데이터 확인

```
kopoctc@kopoctc:~$ stat abc
  File: ‘abc’
  Size: 7               Blocks: 8          IO Block: 4096   regular file
Device: fc00h/64512d    Inode: 261898      Links: 2 — Links: 1이면 하드링크X
Access: (0644/-rw-r--r--) Uid: ( 1000/ kopoctc)    Gid: ( 1000/kopoctc)
Access: 2021-01-18 11:17:24.532815359 +0900
Modify: 2021-01-18 11:17:24.532815359 +0900
Change: 2021-01-18 11:17:32.516815359 +0900
 Birth: -
kopoctc@kopoctc:~$ stat l_abc
  File: ‘l_abc’
  Size: 7               Blocks: 8          IO Block: 4096   regular file
Device: fc00h/64512d    Inode: 261898      Links: 2
Access: (0644/-rw-r--r--) Uid: ( 1000/ kopoctc)    Gid: ( 1000/kopoctc)
Access: 2021-01-18 11:17:24.532815359 +0900
Modify: 2021-01-18 11:17:24.532815359 +0900
Change: 2021-01-18 11:17:32.516815359 +0900
 Birth: -  kopoctc
@kopoctc:~$
```

<그림 II-9> 하드링크 파일 상태조회

Tip 하드링크로 생성된 파일은 단순링크가 아니라 다른 이름의 동일한 파일이므로 삭제등 작업을 주의할 것

2) 심볼릭 링크

심볼릭 링크(symbolic link)는 원 파일을 연결해 주는 파일로 단순 링크된 파일이며 다음과 같은 특징이 있다.

① 특징

·심볼릭 링크는 작은 파일로 존재하고 이 파일은 링크된 파일을 가리킴.

·윈도우에서 바탕화면의 바로가기 아이콘 개념. 아이콘을 지운다고 해당 파일이 지워지지는 않음.

② 심볼릭 링크로 연결하기

·하드링크로 연결 ln -s 명령

·ln -s abc abc2: abc라는파일을 abc2라는하드링크파일로 연결, abc2 파일은 새로 생성됨

·해당 파일상태를 보는 명령은 stat

·<그림 Ⅱ-10>에서ln -s efg l_efg로 심볼릭 링크를 실행한 경우

·efg와 l_efg 는 전혀 다른 파일임을 알 수 있다

3. 이해하기

```
kopoctc@kopoctc:~$ ln -s efg l_efg
kopoctc@kopoctc:~$ stat efg
  File: ‘efg’
  Size: 7               Blocks: 8  De      IO Block: 4096   regular file
vice: fc00h/64512d      Inode: 263076      Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/ kopoctc)   Gid: ( 1000/kopoctc)
Access: 2021-01-18 11:18:17.332815359 +0900
Modify: 2021-01-18 11:18:17.332815359 +0900
Change: 2021-01-18 11:18:17.332815359 +0900
 Birth: -
kopoctc@kopoctc:~$ stat l_efg
  File: ‘l_efg’ -> ‘efg’
  Size: 3               Blocks: 0  De      IO Block: 4096   symbolic link
vice: fc00h/64512d      Inode: 263078      Links: 1
Access: (0777/lrwxrwxrwx)  Uid: ( 1000/ kopoctc)   Gid: ( 1000/kopoctc)
Access: 2021-01-18 11:18:28.132815359 +0900
Modify: 2021-01-18 11:18:28.132815359 +0900
Change: 2021-01-18 11:18:28.132815359 +0900
 Birth: -  kopoctc
@kopoctc:~$
```

<그림 II-10> 심볼릭 링크 파일 상태조회

5) Hard Link
① abc : 파일을 생성
② ln abc l_abc : abc파일과 l_abc파일을 하드링크 함
③ ls –al *로 두 파일을 확인
④ stat abc, stat l_abc로 두 파일의 디스크 상황을 보고 하드링크를 확인

6) Symbolic Link
① efg : 파일을 생성
② ln –s efg s_efg : efg파일과 s_efg파일을 심볼릭 링크함
③ ls –al *로 두 파일을 확인
④ stat efg , stat s_efg 로 두 파일의 디스크 상황을 보고 하드링크를 확인

4. 실습하기 (4 – Jump Up)

1) 금일 배운 명령어를 man으로 찾아보고 각종 옵션에 대하여 조사 후 실습
2) 다음 장 실습 먼저 해보기

5. 퀴즈

문제	보기	정답 및 해설
1)사용자의 정보가 기록되며 해당 파일의 수정 삭제 등으로 사용자관련 설정 변경도 가능한 파일은?	가)/etc/shadow 나) /etc/xinetd 다) /etc/passwd 라) /etc/groups	다) /etc/passwd파일을 의미합니다
2) s1이라는 사용자가 만든 aa파일을 s2라는 사용자가 만든 파일처럼 사용하기 위하여 사용되는 명령어는?	가)chown s1 aa 나)chown aa s2 다)chgrp aa s2 라)chown s2 aa	라) aa파일의 소유권을 s2로 바꾸는 명령은 chown s2 aa입니다
3) aa파일의 그룹에 대하여 읽기와 쓰기 권한을 막는 명령어는?	가)chgrp –rw aa 나)chown g-rw aa 다)chown g+rw aa 라)chmod g-rw aa	라) 권한의 상대모드로 chmod g-rw aa가 맞는 명령어입니다.
4) aaa파일의 소유자는 kopo이고, kopo2사용자는 kopo와 같은 그룹이나 kopo3은 kopo와 다른 그룹이다, “chmod 754 aaa” 라는 명령어 이후 설명으로 옳지 않은 것은?	가)kopo사용자는 읽기가능 나)kopo사용자는 실행가능 다)kopo2사용자는 쓰기가능 라)kopo3사용자는 읽기 가능	다) [!c]라고 명령하면 지금까지 실행한 명령어 중 c로 시작하는 명령어를 실행합니다. 754는 소유자는 읽기, 쓰기, 실행가능, 같은 그룹은 읽기,실행가능, 다른 사람은 읽기 가능한 권한 입니다.

6. 정리하기

✓ 다음 제시된 내용을 자필로 작성하여 제출 하시오 (상단 학번, 이름 기입)

1. 사용자 그룹관리

1)사용자,그룹, 권한관리를 설명하셔요

2)그룹관리 명령어를 옵션과 함께 설명하시오

3)패스워드, 그룹과 관련된 설정 파일을 예를 들어 설명하시오

2. 권한의 이해 및 표시

1)권한의 대하여 정의하시오

2)권한의 숫자 표기법을 설명하시오

3)권한설정의 절대, 상대방법에 대하여 설명하시오

3.링크파일

1)하드링크와 심볼릭링크를 설명하고 차이점을 설명하시오

7. 차시 예고

✓ 차시 학습내용

- vi 편집기의 기본명령어를 활용할 수 있다.
- vi 편집기를 이용한 파일조회,작성,문자열 변경 등을 할 수 있다.
- vi 편집기에서 여러 개 파일을 동시에 편집하거나 쉘모드를 사용할 수 있다.
- FTP 서비스를 설정하고 FTP를 이용하여 파일을 편집할 수 있다
- notepad++을 이용하여 파일을 편집할 수 있다

✓ 차시 준비

- 개행 문자인 CR(Carriage Return)과 LF(Line Feed)에 대하여 검색 등을 통하여 알아봅니다.
- 윈도우의 TEXT파일에서의 개행 방법과 유닉스 리눅스에서 개행 방법에 대하여 알아봅니다