Chapter 02. 리눅스 쉘과 CLI 명령어

사용자, 그룹 및 권한(퍼미션)

사용자와 권한 관련 명령어

- 계정 종류 :
  - root 유저와 사용자 계정
  - 계정 살펴보기 /etc/passwd, /etc/shadow, /etc/group
  - 내 권한 (whoami, id)
  - 그룹 계정 및 권한(sudoer & sudo)

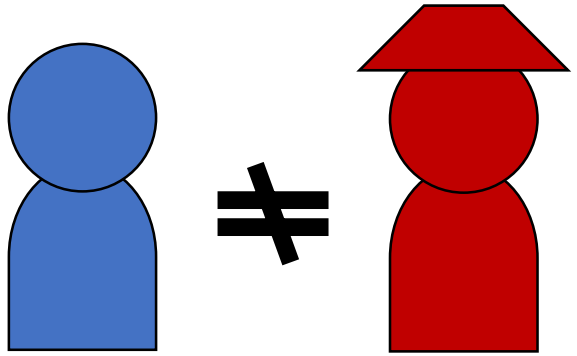
- 사용자 생성과 그룹 생성 (adduser, useradd, usermod, deluser, userdel, addgroup, delgroup)
- 파일 권한 다루기 (chmod, chown, chgrp, umask)

- 파일 다루기 상급
  - setuid, setgid

사용자 계정 - superuser 와 user

슈퍼유저란?
시스템 운영 관리자 계정으로 일반적으로 리눅스 운영체제에서는 루트(root) 유저를 말한다.
관리자 권한을 일반 사용자 권한과 구분하며 사용자의 부주의로 발생하는 시스템 손상과 바이러스, 악성코드의 침입에 의한 피해를 보호한다.

- whoami - 내가 누구인지 내 계정 확인
- id - 내가 갖고 있는 권한 (포함된 그룹) 확인



꼭 강조…
내가 관리하는 PC 라도,
나는 슈퍼유저가 아니다!!

사용자 계정 - 권한 조사

- whoami
- id

```
user1@user1-VirtualBox:~$ whoami
user1
user1@user1-VirtualBox:~$ id
uid=1000(user1) gid=1000(user1) 그룹들=1000(user1),4(adm),24(cdrom),27(sudo),30(dip),46(plug
dev),113(lpadmin),128(sambashare)
```

사용자 계정 - 권한의 대여

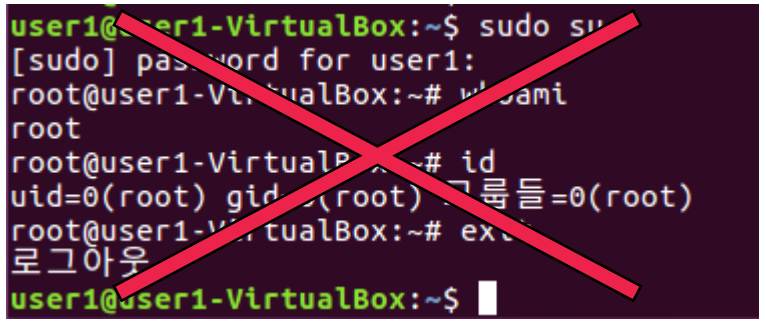
- **sudo**

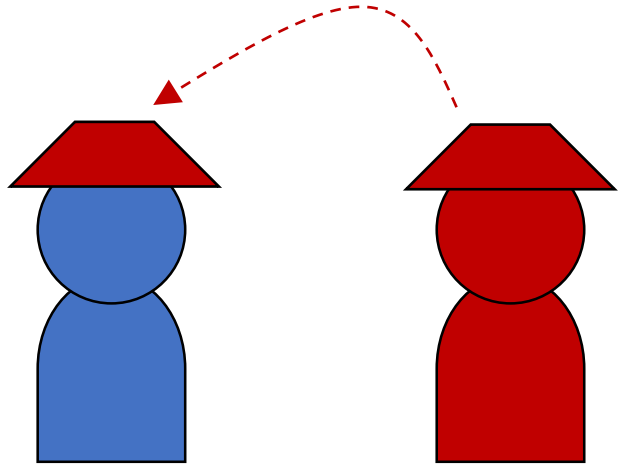
슈퍼유저(**su**peruser) 의 권한을 수행(**do**) 한다.

```
user1@user1-VirtualBox:~$ sudo whoami
root
user1@user1-VirtualBox:~$ whoami
user1
user1@user1-VirtualBox:~$ sudo id
uid=0(root) gid=0(root) 그룹들=0(root)
user1@user1-VirtualBox:~$ id
uid=1000(user1) gid=1000(user1) 그룹들=1000(user1),4(adm),
dev),113(lpadmin),128(sambashare)
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ cat /etc/shadow
cat: /etc/shadow: 허가 거부
user1@user1-VirtualBox:~$ sudo cat /etc/shadow
root:!:18357:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
```

우리는 루트 권한으로 사용하도록
하겠습니다. (제발 습관화 하지 마세요.)





사용자 계정 - 권한의 대여 - sudoer

- **sudo visudo**

슈퍼유저의 권한을 편집

```
user1@user1-VirtualBox:~$ ls -al /etc/sudoers
-r--r----- 1 root root 755  7월  4  2017 /etc/sudoers
```

설정파일을 통한 변경
- 사용자 권한
- %그룹 권한

설정파일 상세
- 계정명 호스트명=(실행계정명) 명령어
- user1 ALL=(ALL) /sbin/ifconfig

비추천

사용자를 sudo 권한에 추가
- useradd -aG user1 sudo (Ubuntu)
- useradd -aG user1 wheel (Amazon AMI)

추천

```
user1@user1-VirtualBox:~$ cat /etc/sudoers
cat: /etc/sudoers: 허가 거부
user1@user1-VirtualBox:~$ sudo cat /etc/sudoers
[sudo] password for user1:
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/u

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

사용자 계정 - 권한의 대여 - su

su [username]
사용자의 권한을 대여 (즉, 사용자로 로그인 한 것과 같은 효과)
언제 사용하느냐? 관리자가 사용자 계정을 관리하고 이슈/장애를 분석 할 때

```
user1@user1-VirtualBox:~$ su user2
암호:
user2@user1-VirtualBox:/home/user1$ exit
exit
user1@user1-VirtualBox:~$ su - user2
암호:
user2@user1-VirtualBox:~$ pwd
/home/user2
```

사용방법:

- su user2

user2의 id로 로그인 한다 (user2의 pw 필요)

- su - user2

user2 의 id로 로그인 한다 (user2의 pw 필요, user2 의 home 디렉토리 사용)

- su 혹은 su root

root 의 id 로 로그인 한다 (root의 pw 필요. 하지만 우분투는 root 암호 비활성화.)

- sudo su

내 권한을 상승하여 root 사용자의 권한으로 로그인 한다 (현재 디렉토리 사용)

- sudo su -

내 권한을 상승하여 root 사용자의 권한으로 홈 디렉토리 사용 (root의 home)

비추천 :
권한을 남용하지 마세요

- sudo su - user2

user2 사용자의 권한으로 홈 디렉토리 사용 (sudoer(user1)의 pw 필요, user2 의 home)

사용자 계정과 그룹 계정

- cat /etc/passwd : 사용자 계정 확인
- cat /etc/shadow : 사용자 암호

- cat /etc/group : 사용자 그룹 확인

```
user1@user1-VirtualBox:~$ cat /etc/passwd
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
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nolog
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nolo
backup:x:34:34:backup:/var/backups:/usr/sbin/nolo
list:x:38:38:Mailing List Manager:/var/list:/usr/
```

```
user1@user1-VirtualBox: ~
user1@user1-VirtualBox:~$ cat /etc/shadow
cat: /etc/shadow: 허가 거부
user1@user1-VirtualBox:~$ sudo cat /etc/shadow
root:!:18357:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
pulse:*:17954:0:99999:7:::
rtkit:*:17954:0:99999:7:::
saned:*:17954:0:99999:7:::
usbmux:*:17954:0:99999:7:::
user1:$6$xOde28Uj$BrMy48rH7UWG
fWxWgLRQq3oleGEriF0:18357:0:99
sshd:*:18357:0:99999:7:::
vboxadd:!:18357::::::
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,user1
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:user1
floppy:x:25:
tape:x:26:
sudo:x:27:user1
```

사용자 계정과 그룹 계정 - 사용자 계정 (/etc/passwd)

- cat /etc/passwd : 사용자 계정 확인

사용자명	패스워드	계정 UID	계정 GUI	이름	홈 디렉토리	로그인 쉘	
root	x	0	0	root	/root	/bin/bash	← 슈퍼유저
user1	x	1000	1000	user1,,,	/home/user1	/bin/bash	← 사용자
www-data	x	33	33	www-data	/var/www	/usr/sbin/nologin	← 서비스 계정

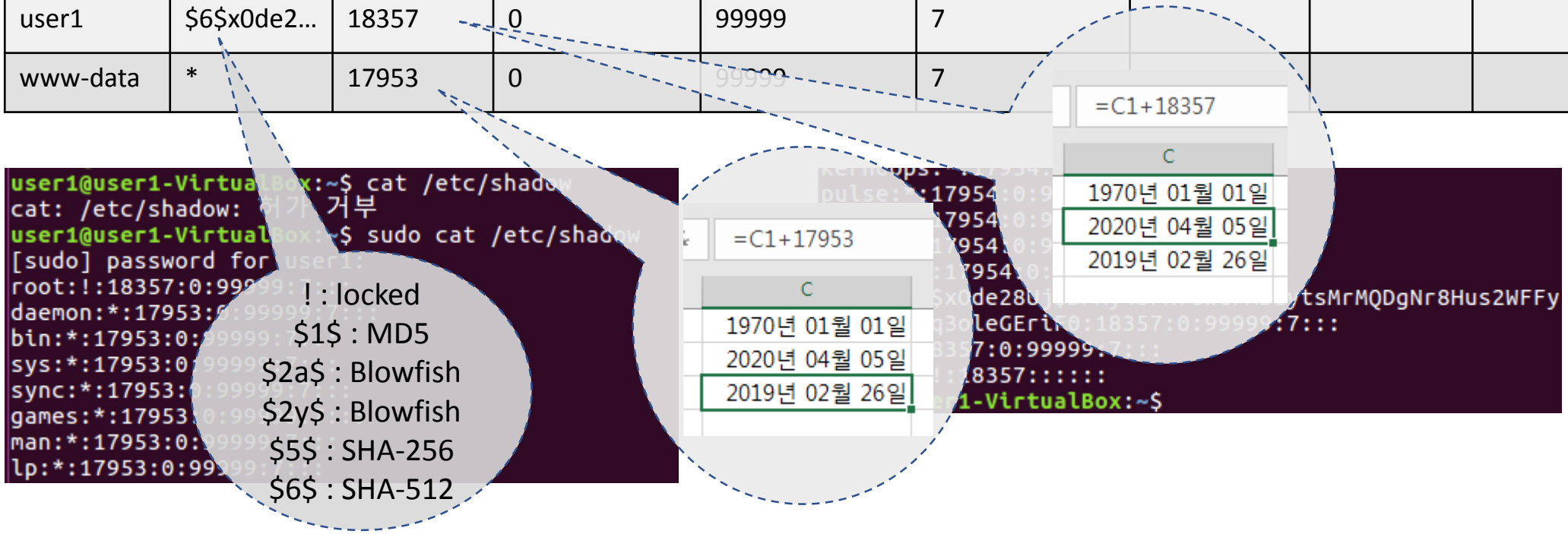
```
user1@user1-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

0 : root
1 ~ 99 : predefined
100 ~ 999 : administrative and system accounts
1000 ~ : user

사용자 계정과 그룹 계정 - 사용자 계정 (/etc/shadow)

- cat /etc/shadow : 사용자 암호
- 리눅스(유닉스)의 모든 시간 **epoch** = 1970년 1월 1일 00:00:00 UTC

사용자명	패스워드	최종 수정일	패스워드 최소 변경일	패스워드 최대 사용일	패스워드 만료 경고기간	패스워드 유예 기간	계정 만료 기간	예약필드
root	!	18357	0	99999	7			
user1	6x0de2...	18357	0	99999	7			
www-data	*	17953	0	99999	7			



사용자 추가 (adduser - add user)

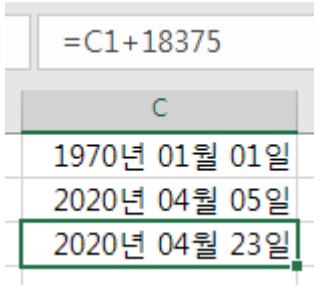
adduser [options] [--home DIR] [--shell SHELL] [--disabled-password] [--disabled-login] user
새로운 사용자 추가

```
user1@user1-VirtualBox:~$ adduser
adduser: 루트만이 사용자나 그룹을 시스템에 추가할 수 있습니다.
user1@user1-VirtualBox:~$ sudo adduser user2
'user2' 사용자를 추가 중...
새 그룹 'user2' (1001) 추가 ...
새 사용자 'user2' (1001) 을(를) 그룹 'user2' (으)로 추가 ...
'/home/user2' 홈 디렉터리를 생성하는 중...
'/etc/skel'에서 파일들을 복사하는 중...
새 UNIX 암호 입력:
새 UNIX 암호 재입력:
passwd: 암호를 성공적으로 업데이트했습니다
user2의 사용자의 정보를 바꿉니다
새로운 값을 넣거나, 기본값을 원하시면 엔터를 치세요
        이름 []: User2
        방 번호 []:
        직장 전화번호 []:
        집 전화번호 []:
        기타 []:
정보가 올바릅니까? [Y/n]
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ cat /etc/passwd

user1:x:1000:1000:user1,,,:/home/user1:/bin/bash
user2:x:1001:1001:User2,,,:/home/user2:/bin/bash
```

```
user1@user1-VirtualBox:~$ sudo cat /etc/shadow
user1:$6$xOde28Uj$BrMy48rH7UWGFMBGytsMrMQDgNr8Hus2WFFy.3U
Qq3oleGEriF0:18357:0:99999:7:::
user2:$6$mPcHqJMY$exknPE/1O23hcDWPkPZ1z/R3DxO67DURtEzZA2S
Zt1Ugh1dJkq0:18375:0:99999:7:::
user1@user1-VirtualBox:~$
```



사용자 추가 (useradd - user add with default (none-dialog 방식) / adduser 의 아래 레벨 실행파일)

useradd [options] user
사용자 (기본값으로) 추가

- useradd user3　: 사용자 user3 추가
- useradd -D　: 사용자 생성 기본값 확인
- useradd -D -b /usr　: 사용자 기본 홈 디렉토리 /usr 로 변경
- useradd -D -s /bin/bash : 사용자 기본 쉘 bash로 변경
- useradd -D -e 2020-12-31　: 사용자 계정 만료일 설정

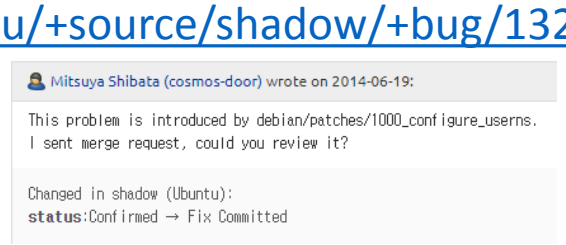
참고: 계정 생성시 참조하는 파일들
- /etc/default/useradd
- /etc/login.defs
- /etc/skel/

```
user1@user1-VirtualBox:~$ which adduser
/usr/sbin/adduser
user1@user1-VirtualBox:~$ file /usr/sbin/adduser
/usr/sbin/adduser: a /usr/bin/perl script, ASCII text executable
user1@user1-VirtualBox:~$ which useradd
/usr/sbin/useradd
user1@user1-VirtualBox:~$ file /usr/sbin/useradd
/usr/sbin/useradd: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV)
d, interpreter /lib64/l, for GNU/Linux 2.6.32, BuildID[sha1]=399e211d99c5
a9a5fcc08, stripped
```

```
user1@user1-VirtualBox:~$ sudo useradd user3
user1@user1-VirtualBox:~$
```

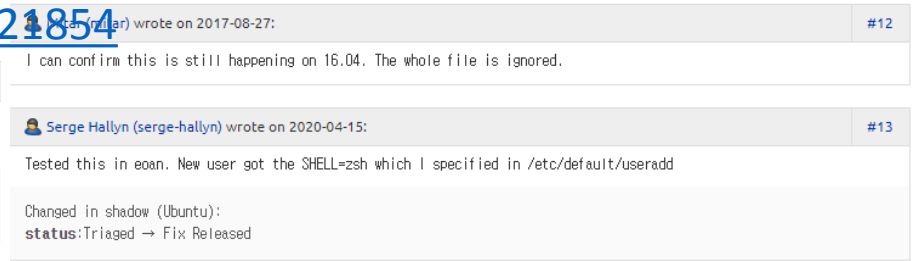
```
user1@user1-VirtualBox:~$ useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

https://bugs.launchpad.net/ubuntu/+source/shadow/+bug/1321854


Mitsuya Shibata (cosmos-door) wrote on 2014-06-19:

This problem is introduced by debian/patches/1000_configure_userns.
I sent merge request, could you review it?

Changed in shadow (Ubuntu):
status:Confirmed → Fix Committed


wrote on 2017-08-27: #12

I can confirm this is still happening on 16.04. The whole file is ignored.

Serge Hallyn (serge-hallyn) wrote on 2020-04-15: #13

Tested this in eoan. New user got the SHELL=zsh which I specified in /etc/default/useradd

Changed in shadow (Ubuntu):
status:Triaged → Fix Released

사용자 암호 정책 변경 / 암호 변경 (chage - change age / passwd)

chage [option] user
사용자 암호 정책 변경

- chage user2 : 암호 정책 변경
- chage -l user2 : 암호 정책 확인
- chage -E 2020-12-31 -m 1 -M 90 -W 7 user2

```
user1@user1-VirtualBox:~$ chage user2
chage: 권한이 거부되었습니다.
user1@user1-VirtualBox:~$ sudo chage user2
user2의 사용기한 정보를 바꿉니다
새로운 값을 넣거나, 기본값을 원하시면 엔터를 치세요

        암호의 최소 유효 기간 [0]: 1
        암호의 최대 유효 기간 [99999]: 30
        마지막으로 암호를 바꾼 날 (YYYY-MM-DD) [2020-04-23]:
        암호 사용만료 예고 [7]:
        암호를 사용할 수 없음 [-1]: 3
        계정 만료 날짜 (YYYY-MM-DD) [-1]: 2020-07-23
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ sudo cat /etc/shadow        |
user2:$6$mPcHqJMY$exknPE/1O23hcDWPkPZ1z/R3DxO67DURtEzZA
Zt1Ugh1dJkq0:18375:1:30:7:3:18466:
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ sudo chage -l user2
마지막으로 암호를 바꾼 날                                    :  4월 23,
암호 만료                                          :  5월 23, 2020
암호가 비활성화 기간                                       :  5월 26, 2020
계정 만료                                                  :  7월 23, 2020
암호를 바꿀 수 있는 최소 날 수          : 1
암호를 바꿔야 하는 최대 날 수          : 30
암호 만료 예고를 하는 날 수            : 7
user1@user1-VirtualBox:~$
```

- passwd [options] user : 암호변경
- passwd -l user : 계정 잠금
- passwd -u user : 계정 잠금 해제
- passwd -S user : 계정 상태 확인
- passwd -n <mindays> user : 암호 최소 기간
- passwd -x <maxdays> user : 암호 최대 기간
- man passwd

```
user1@user1-VirtualBox:~$ passwd user2
passwd: user2의 암호 정보를 보거나 바꿀 수 없습니다.
user1@user1-VirtualBox:~$ sudo passwd user2
새 UNIX 암호 입력:
새 UNIX 암호 재입력:
passwd: 암호를 성공적으로 업데이트했습니다
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ sudo passwd -l user2
passwd: password expiry information changed.
user1@user1-VirtualBox:~$ sudo cat /etc/shadow        |
user2:!$6$A8t2s9Zj$lMAd/lXIlfDYXEtt3dPrZFntGnlBT6ffNl/5
ekaG3rfG97u51:18375:1:30:7:3:18466:
user1@user1-VirtualBox:~$ sudo passwd -u user2
passwd: password expiry information changed.
user1@user1-VirtualBox:~$ sudo cat /etc/shadow        |
user2:$6$A8t2s9Zj$lMAd/lXIlfDYXEtt3dPrZFntGnlBT6ffNl/5l
kaG3rfG97u51:18375:1:30:7:3:18466:
user1@user1-VirtualBox:~$ sudo passwd -S user2
user2 P 04/23/2020 1 30 7 3
user1@user1-VirtualBox:~$
```

사용자 삭제 (deluser - delete user)

deluser [options] user
사용자 계정 삭제

- deluser user2
- deluser user2 --remove-home

```
user1@user1-VirtualBox:~$ sudo deluser user2
'user2' 사용자 제거 중...
경고: 'user2'그룹이 회원목록에 더이상 없음.
완료.
user1@user1-VirtualBox:~$ ls -al /home
합계 16
drwxr-xr-x  4 root  root  4096  4월 24 00:58 .
drwxr-xr-x 24 root  root  4096  4월  8 00:32 ..
drwxr-xr-x 22 user1 user1 4096  4월 23 23:30 user1
drwxr-xr-x  2  1001  1001 4096  4월 24 00:58 user2
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ sudo deluser user2 --remove-home
백업/제거할 파일들을 찾는 중...
파일 제거중 ...
'user2' 사용자 제거 중...
경고: 'user2'그룹이 회원목록에 더이상 없음.
완료.
user1@user1-VirtualBox:~$ ls -al /home
합계 12
drwxr-xr-x  3 root  root  4096  4월 24 01:36 .
drwxr-xr-x 24 root  root  4096  4월  8 00:32 ..
drwxr-xr-x 22 user1 user1 4096  4월 23 23:30 user1
user1@user1-VirtualBox:~$
```

userdel user
none-interactive 모드로 모두 삭제

- userdel user2 : 사용자 계정 삭제 (홈 삭제)
- userdel -f user2 : 로그인 중이더라도 삭제

```
user1@user1-VirtualBox:~$ sudo userdel user3
user1@user1-VirtualBox:~$
```

새로운 사용자를 동일ID 로 만들경우,
이전 디렉토리에 맵핑

그룹 생성 (addgroup - add group)

addgroup [options] group
그룹 계정 생성

groupadd [options] group
실제 addgroup 의 바이너리

```
user1@user1-VirtualBox:~$ addgroup
addgroup: 루트만이 사용자나 그룹을 시스템에 추가할 수 있습니다.
user1@user1-VirtualBox:~$ sudo addgroup developers
그룹 `developers' (GID 1002) 추가 ...
완료.
```

```
user1@user1-VirtualBox:~$ cat /etc/group
developers:x:1002:
```

```
user1@user1-VirtualBox:~$ id
uid=1000(user1) gid=1000(user1) 그룹들=1000(user1),4(adm),24(cdrom),27(sudo),30(dip),46(plug
dev),113(lpadmin),128(sambashare)
user1@user1-VirtualBox:~$
```

```
user1@user1-VirtualBox:~$ which addgroup
/usr/sbin/addgroup
user1@user1-VirtualBox:~$ ls -l /usr/sbin/addgroup
lrwxrwxrwx 1 root root 7  4월  5 18:33 /usr/sbin/addgroup -> adduser
user1@user1-VirtualBox:~$ cat /usr/sbin/adduser | grep groupadd
    my $groupadd = &which('groupadd');
        &systemcall($groupadd, '--extrausers', '-g', $new_gid, $new_name);
        &systemcall($groupadd, '-g', $new_gid, $new_name);
```

그룹 삭제 (delgroup - delete group)

delgroup [options] group
그룹 계정 삭제

```
user1@user1-VirtualBox:~$ sudo delgroup developers
'developers' 그룹 제거 중...
완료.
user1@user1-VirtualBox:~$
```

그룹 계정 / 사용자 할당 (또는 사용자 정보 수정) (usermod - user mod)

usermod [options] user
사용자 계정 정보 수정 (moduser 는 없음 (interactive 방식인…))
사용자를 그룹에 추가

- usermod -c <name change> user2 : 사용자 이름 수정
- usermod -a -G sudo user2 : user2 를 sudo 그룹에 추가
  adduser user2 sudo : user2 를 sudo 그룹에 추가
- deluser user2 sudo : user2를 sudo 그룹에서 제거
  (실행후 결과 번역 오류)

```
user1@user1-VirtualBox:~$ sudo deluser user2 sudo
'user2'그룹에서 'sudo'사용자 제거중 ...
완료.
```

Removing user ‘user2’ from group ‘sudo’ …
Done.

파일의 권한

사용자 접근 권한의 구분

소유자(User) / 그룹(Group) / 그외 (Other)

```
user1@user1-VirtualBox:~$ ls -l
합계 44
-rw-r--r-- 1 user1 user1 8980  4월  5 18:38 examples.desktop
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 공개
drwxr-xr-x 2 user1 user1 4096  4월 18 01:18 다운로드
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 문서
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 바탕화면
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 비디오
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 사진
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 음악
drwxr-xr-x 2 user1 user1 4096  4월  5 18:54 템플릿
user1@user1-VirtualBox:~$
```

유형 (d = directory, l = link)
권한
링크수
소유자
그룹
파일크기
변경일자
이름

User			**Group**			**Other**		
읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행
r	w	x	r	w	x	r	w	x
4	2	1	4	2	1	4	2	1
합산 : 7			7			7		

r : read
w : write
x : execute

0 --- : 권한무
1 --x : 실행
2 -w- : 쓰기
3 -wx : 쓰기 & 실행
4 r-- : 읽기
5 r-x : 읽기 & 실행
6 rw- : 읽기 & 쓰기
7 rwx : 읽기 & 쓰기 & 실행

파일의 생성 권한 (umask - user mask)

파일/디렉토리 생성 권한의 확인

소유자(User) / 그룹(Group) / 그외 (Other)

- 리눅스의 기본 파일 권한: 666
- 리눅스의 기본 디렉토리 권한: 777

이 말은, umask 가 0 일 경우 새로 생성되는 파일의 권한은 666 (rw-rw-rw-) 을 갖게 됨
디렉토리 권한은 777 (rwxrwxrwx) 을 갖게 됨

여기서, umask 가 2 (혹은 0002) 일 경우에는
파일 기본권한 666 에서 002를 빼면

- 110 110 110 = 666
- 000 000 010 = 002
- 110 110 100 = 664, 즉 rw-rw-r-- 로 생성 됨

디렉토리 기본권한 777 에서 002를 빼면

- 111 111 111 = 777
- 000 000 010 = 002
- 111 111 101 = 775, 즉 rwxrwxr-x 로 생성 됨

```
user1@user1-VirtualBox:~$ umask
0002
user1@user1-VirtualBox:~$ umask -S
u=rwx,g=rwx,o=rx
user1@user1-VirtualBox:~$ touch test
user1@user1-VirtualBox:~$ ls -l test
-rw-rw-r-- 1 user1 user1 0  5월  3 22:46 test
user1@user1-VirtualBox:~$ mkdir testdir
user1@user1-VirtualBox:~$ ls -dl testdir
drwxrwxr-x 2 user1 user1 4096  5월  3 22:46 testdir
user1@user1-VirtualBox:~$
```

파일의 권한 - 권한 변경 (chmod - change mode)

chmod [OPTION]… [MODE]… file…
파일/디렉토리 권한의 변경

소유자(User) / 그룹(Group) / 그외 (Other)

- chmod 777 hello.txt : 숫자값을 통한 user/group/other 에 rwx 권한 부여
- chmod 700 hello.txt : 숫자값을 통한 user 에 rwx 권한 부여 (group/other 에는 --- 권한 부여)
- chmod u+x hello.txt : user 에 x(실행) 권한 추가
- chmod u-x hello.txt : user 에 x(실행) 권한 삭제
- chmod g+rw hello.txt : group 에 rw(읽기/쓰기) 권한 추가
- chmod g-rx hello.txt : group 에 rw(읽기/쓰기) 권한 삭제
- chmod o+rwx hello.txt : other 에 rwx(읽기/쓰기/실행) 권한 추가
- chmod o-rwx hello.txt : other 에 rwx(읽기/쓰기/실행) 권한 삭제
- chmod +x hello.txt : user/group/other 에 x(실행) 권한 추가

```
user1@user1-VirtualBox:~$ chmod 777 hello.txt
user1@user1-VirtualBox:~$ ls -al hello.txt
-rwxrwxrwx 2 user1 user1 0  4월 25 01:06 hello.txt
user1@user1-VirtualBox:~$ chmod 700 hello.txt
user1@user1-VirtualBox:~$ ls -al hello.txt
-rwx------ 2 user1 user1 0  4월 25 01:06 hello.txt
user1@user1-VirtualBox:~$ chmod u+x hello.txt
user1@user1-VirtualBox:~$ ls -al hello.txt
-rwx------ 2 user1 user1 0  4월 25 01:06 hello.txt
user1@user1-VirtualBox:~$ chmod u-x hello.txt
user1@user1-VirtualBox:~$ ls -al hello.txt
-rw------- 2 user1 user1 0  4월 25 01:06 hello.txt
```

파일의 권한 - 소유권 변경 (chown - change owner, chgrp - change group)

chown [OPTION]… [USER][:GROUP] FILE…
파일/디렉토리의 소유자/그룹 변경

chgrp [OPTION]… [GROUP] FILE…
파일/디렉토리의 그룹 변경

소유자(User) / 그룹(Group) / 그외 (Other)

- chown user2 hello.txt : 해당 파일(hello.txt) 의 소유자를 user2 로 변경
- chown user2:user2 hello.txt : 해당 파일(hello.txt) 의 소유자와 그룹을 모두 user2 로 변경
- chown :user2 hello.txt : 해당 파일(hello.txt) 의 그룹을 user2 로 변경

- chgrp user2 hello.txt : 해당 파일(hello.txt) 의 그룹을 user2 로 변경

파일의 특수 실행 권한 (setuid, setgid, sticky bit)

파일의 권한을 일시적으로 소유주(setuid) 혹은 소유그룹(setgid)의 권한으로 빌려서 실행함
Sticky bit은 해당 디렉토리에 생성된 파일은 해당 사용자의 소유주로 저장됨

소유자(User) / 그룹(Group) / 그외 (Other)

- SetUID 는 4xxx, SetGID 는 2xxx 로, StickyBit 은 1xxx 로 설정한다.

각각 설정 위치는 rw**s**------, rwxrw**s**---, drwxdrxdw**t** 로 표시된다.

- 기존 권한의 위치에 덮어쓰기 때문에, 해당 기능만 존재할 경우 대문자 S/S/T 로 표기 된다.

각각 설정 위치는 rw**S**------, rwxrw**S**---, drwxdrxdw**T** 로 표시된다.
기존 권한 (실행권한) 을 포함하고 있는 경우 소문자 s/s/t로 표시된다.

- chmod u+s filename
- chmod g+s filename
- chmod +t directoryname

```
user1@user1-VirtualBox:~$ ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 136808  2월  1 03:37 /usr/bin/sudo
user1@user1-VirtualBox:~$ ls -l /usr/bin/crontab
-rwxr-sr-x 1 root crontab 36080  4월  6  2016 /usr/bin/crontab
user1@user1-VirtualBox:~$ ls -dl /tmp
drwxrwxrwt 11 root root 4096  5월  4 00:17 /tmp
user1@user1-VirtualBox:~$
```

파일의 특수 실행 권한 (setuid, setgid, sticky bit)

(다소 복잡한) 실습
시나리오 : 두명의 사용자가 있고, user1 이 만든 읽기 전용 파일에 user2 가 setuid 권한을 통해 접근

user1, user2 두명의 사용자
- user1의 readonly 파일 생성
- /bin/cat 을 복사해서 mycat 으로 생성 및 setuid 를 통해 실행 권한을 부여
  - user2 가 readonly 파일을 직접 읽을 수는 없지만,
  - setuid 가 실행된 파일로는 읽을 수 있음.