Local User Management

Local User Management & File Security

DE HOGESCHOOL
MET HET NETWERK

Hogeschool PXL – Dep. PXL-IT – Elfde-Liniestraat 26 – B-3500 Hasselt
www.pxl.be - www.pxl.be/facebook

identify yourself

- `whoami`
  toont je je username
- `who`
  toont je informatie over wie ingelogd is
- `who am i`
  toont je informatie over wie ingelogd is in je huidige sessie
- `w`
  toont wie ingelogd is en wat ze aan het doen zijn
- `id`
  toont je je user id, primary group id en een lijst van groepen waar je lid van bent

users

- user management
  - 3 mogelijkheden
    - graphical tools *(→ Desktop OS, doen we dit jaar niet)*
    - commandline tools *(herhalen we dit jaar)*
    - edit the local configuration files *(moet je dit jaar ook kunnen)*

users

- `/etc/passwd`
  - local user database
  - 7 velden
    username:x:user id:primary group id:description:home directory:login shell

    x als password → geëncrypteerd password in /etc/shadow
- root
  - superuser
  - user id 0

- `useradd`
  - commando om een user toe te voegen
  - zie man useradd

users

- `/etc/default/useradd`
  - default user options
  - `useradd -D`
- `userdel`
  - commando om een user te deleten
  - zie `man userdel`
- `usermod`
  - commando om properties van een user te wijzigen
  - zie `man usermod`

passwords

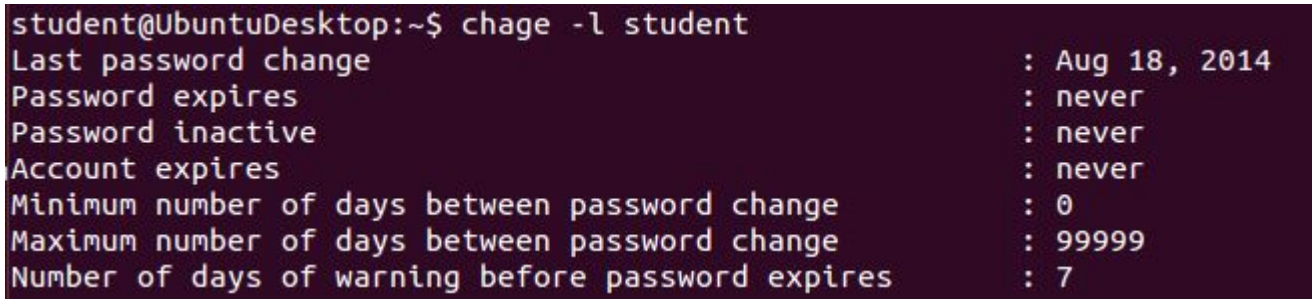
- `passwd`
  - commando om een user een password toe te kennen

- `/etc/shadow`
  - user passwords worden geëncrypteerd en bijgehouden in deze file
  - read-only, en enkel leesbaar voor root
  - 9 velden:
    user name:encrypted password:day the password was last changed:
    number of days the password must be left unchanged:password expiry day:
    warning number of days before password expiry:number of days after expiry
    before disabling the account:day the account was disabled:field without any
    meaning

passwords

- password encryption
  - met `passwd`
    - geëncrypteerd formaat
    - via `crypt` functie
  - met chpasswd
    - sudo adduser -m gert # user gert wordt aangemaakt
    - echo gert:pxl | sudo chpasswd # user gert krijgt paswoord pxl
  - met openssl
    - via commando `openssl passwd` een geëncrypteerd wachtwoord aanmaken om als argument te gebruiken bij de optie `-p` van het commando `useradd`

passwords

- password defaults
  - `/etc/login.defs`
  - `chage`
    - zie `man chage`
    - 

passwords

- disabling a password
  - als het password start met ! in `/etc/shadow`, kan het password niet gebruikt worden
  - = locking, disabling, suspending a user account
  - kan via het commando `usermod -L <username>` of via `vi` of `vipw`
  - root of sudoers kunnen nog via `su` inloggen met een gelocked account, aangezien ze het password van dat account niet moeten ingeven

- editing local files
  - edit `/etc/passwd` en `/etc/shadow` via `vi(m)`
  - of via `vipw`

home directories

- creating home directories
  - `useradd -m`
  - manueel:
    - `mkdir`
    - `chown`
    - `chmod`

- `/etc/skel/`
  - inhoud van `/etc/skel/` wordt gekopieerd naar elke nieuwe home directory
  - meestal hidden files
  - uiteraard niet als je de home directory manueel aanmaakt !!

home directories

- deleting home directories
  - `userdel -r`

    `userdel:` je delete de user
    `-r:` én zijn home directory

user shell

- login shell
  - gespecifieerd in `/etc/passwd`
  - kan gewijzigd worden via `usermod -s` of via `chsh`

```
student@UbuntuDesktop:~$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/bin/dash
/bin/bash
/bin/rbash
```

dash: Debian Almquist shell
(veel kleiner dan bash)
bash: GNU Bourne-Again Shell

in ubuntu:

```
student@UbuntuDesktop:~$ ls -l /bin | grep sh
-rwxr-xr-x 1 root root 1017016 Apr 24  2014 bash
-rwxr-xr-x 1 root root  121272 Feb 19  2014 dash
lrwxrwxrwx 1 root root       4 Aug 18 21:47 rbash -> bash
lrwxrwxrwx 1 root root       4 Aug 18 21:47 sh -> dash
lrwxrwxrwx 1 root root       4 Aug 18 21:47 sh.distrib -> dash
lrwxrwxrwx 1 root root       7 Aug 18 21:47 static-sh -> busybox
```

switch users with su

- su to another user
- su to root
- su as root
  - geen password nodig
- su - $username
  - wordt deze user en krijg ook de omgeving van deze user
- su -
  - geen username → root

run a program as another user

- about `sudo`
  - laat toe dat een user een programma start met de credentials van een andere user
  - `/etc/sudoers`
- setuid on sudo
  - `setuid` → zie file security
- visudo
  - edit the sudoers file

run a program as another user

- `sudo su`
  - in Ubuntu heeft de user root geen password,
    hierdoor kan je niet inloggen met root (security)
  - met “sudo su” kan je dan toch nog root worden
  - `sudo su -`
    je wordt root zonder het root password te kennen
    (password prompt is voor het sudo password)

shell environment

Overzicht van bash startup scripts in Debian/Ubuntu

script	su	su -	ssh	gdm
`~/.bashrc`	no	yes	yes	yes
`~/.profile`	no	yes	yes	yes
`/etc/profile`	no	yes	yes	yes
`/etc/bash.bashrc`	yes	no	no	yes

GNOME Display Manager

The Ubuntu desktop session is no longer affected by .profile (PTS)
In a TTY, bash doesn't parse .profile if either .bash_profile or .bash_login exists
(Zie comments in .profile)

groups

- about groups
  - users kunnen toegevoegd worden aan een group
  - permissions op group level

- `groupadd`
  - nieuwe group aanmaken

- `/etc/group`
  - 4 velden
    group name:(encrypted) password:group id:list of members

groups

- `usermod`
  - `usermod -a -G <groupname> <username>`
  - append supplementary group
- `groupmod`
  - wijzig een group (bvb. de group name)
  - zie `man groupmod`
- `groupdel`
  - verwijder een group

groups

- `groups`
  - toon een lijst van groepen waartoe een user behoort
- `gpasswd`
  - geef de controle van group membership aan een andere user
  - zie `man gpasswd`
  - `/etc/gshadow`
- `vigr`
  - edit `/etc/group`

maak user en group
a.d.h.v. local configuration files

1. sudo su -

2. vim /etc/passwd
   voeg 1 user toe (eventueel copy-paste een van de vorige lijen)

```
root@UbuntuDesktop:~# tail -1 /etc/passwd
veerle:x:1004:1004:veerle,,,:/home/veerle:/bin/bash
```

   Let op uid en gid !! → moeten uniek zijn

3. vim /etc/group
   voeg een group toe met het zonet gebruikte gid

```
root@UbuntuDesktop:~# tail -1 /etc/group
groupforveerle:x:1004:veerle
```

Voorbeeld:
user: veerle
group: groupforveerle

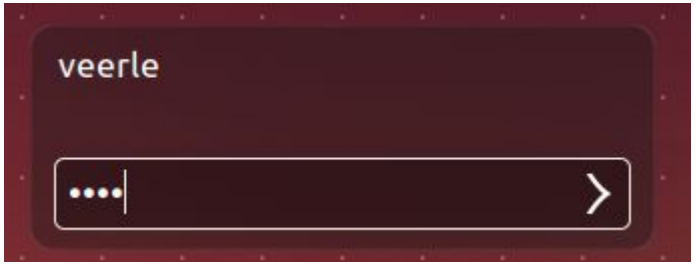
maak user en group
a.d.h.v. local configuration files

7. test (als gewone user, zodat je je password ook kan testen)

```
student@UbuntuDesktop:~$ su - veerle
Password:
veerle@UbuntuDesktop:~$ pwd
/home/veerle
```

of log in (op een andere tty)

```
Ubuntu 14.04.1 LTS UbuntuDesktop tty1

UbuntuDesktop login: veerle
Password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

veerle@UbuntuDesktop:~$ pwd
/home/veerle
veerle@UbuntuDesktop:~$
```



alternatieve commando’s

- `adduser`: alternatief voor `useradd`, maar:
  - paswoord kan onmiddelijk opgegeven worden
  - homedir wordt ook aangemaakt

- `addgroup`: alternatief voor `groupadd`, maar:
  - groupid wordt getoond na uitvoeren van het commando

File Security

file permissions - acl

DE HOGESCHOOL
MET HET NETWERK

Hogeschool PXL – Dep. PXL-IT – Elfde-Liniestraat 26 – B-3500 Hasselt
www.pxl.be - www.pxl.be/facebook

file ownership

- user owner and group owner
  - elke file heeft een user owner en een group owner
  - `ls -l`
- listing user accounts
  - `cut -d: -f1 /etc/passwd | column`
- `chgrp`
  - wijzig de group owner
- `chown`
  - wijzig de user owner

file ownership

- list of special files

eerste character (`ls -l`)	file type
-	regular file
d	directory
l	symbolic link
p	named pipe
b	block device
c	character device
s	socket

permissions

- rwx
  - r read
  - w write
  - x execute

permission	on a file	on a directory
r	read file contents (`cat`)	read directory contents (`ls`)
w	change file contents (`vi`)	create files in (`touch`)
x	execute the file	enter the directory (`cd`)

permissions

- three sets of rwx
  - `ls -l`

position	characters	function
1	-	this is a regular file
2-4	rwx	permissions for the **user owner**
5-7	r-x	permissions for the **group owner**
8-10	r--	permissions for **others**

permissions

- setting permissions
  - `chmod`
  - voorbeelden
    - `chmod u+x`
    - `chmod g-r`
    - `chmod o-r`
    - `chmod a+w`
    - `chmod +x`
    - `chmod u=rw`
    - `chmod u=rw,g=rw,o=r`
    - `chmod u=rwx,ug+rw,o=r`

permissies toevoegen

permissies verwijderen

a is niet nodig

expliciet permissies toekennen, i.p.v. toevoegen of verwijderen

combinatie

permissions

- setting octal permissions

binary	octal	permissions
000	0	---
001	1	--x
010	2	-w-
011	3	-wx
100	4	r--
101	5	r-x
110	6	rw-
111	7	rwx

permissions

- umask
  - bepaald de default permissies voor een file of directory

```
student@UbuntuDesktop:~$ umask
0002
```

  - een file is default nooit executable !!
  - 1e digit → speciale permissies (zie verder in de slides)
    0: geen speciale modus
  - voorbeeld berekening:

	777	
umask	002	(aftrekken)
permissions	775	file: rw-rw-r--
		dir: rwxrwxr-x

	777	
umask	033	(aftrekken)
permissions	744	file: rw-r--r--
		dir: rwxr--r--

  - `mkdir -m`
    - permissies meegeven tijdens creatie van een directory
    - `mkdir -m 700 mydir`

permissions

- sticky bit on directory
  - om te voorkomen dat users files wissen waarvan ze geen user owner zijn
  - op de locatie van de x permission voor others
  - t ⟶ sticky bit + x, T ⟶ sticky bit, geen x voor others
  - 4 digits: 1e digit ⟶ 1

```
student@UbuntuDesktop:~/oefperm$ mkdir mydir
student@UbuntuDesktop:~/oefperm$ ls -ld mydir/
drwxrwxr-x 2 student student 4096 Nov 15 14:39 mydir/
student@UbuntuDesktop:~/oefperm$ chmod +t mydir/
student@UbuntuDesktop:~/oefperm$ ls -ld mydir/
drwxrwxr-t 2 student student 4096 Nov 15 14:39 mydir/
```

```
student@UbuntuDesktop:~/oefperm$ chmod 1700 mydir/
student@UbuntuDesktop:~/oefperm$ ls -ld mydir/
drwx------T 2 student student 4096 Nov 15 14:39 mydir/
```

- typisch voor /tmp

```
student@UbuntuDesktop:~$ ls -ld /tmp
drwxrwxrwt 9 root root 4096 Nov 15 14:37 /tmp
```

permissions

- setgid bit on directory
  - om te verzekeren dat alle files in deze directory dezelfde group owner hebben
  - op de locatie van de x permission van group owner
  - s → setgid + x, S → setgid, geen x voor group owner
  - 4 digits: 1e digit → 2

```
student@UbuntuDesktop:~/oefperm$ ls -ld mydir2
drwxrwxr-x 2 student student 4096 Nov 15 14:51 mydir2
student@UbuntuDesktop:~/oefperm$ chmod 2775 mydir2
student@UbuntuDesktop:~/oefperm$ ls -ld mydir2
drwxrwsr-x 2 student student 4096 Nov 15 14:51 mydir2
student@UbuntuDesktop:~/oefperm$ chmod a-x mydir2
student@UbuntuDesktop:~/oefperm$ ls -ld mydir2
drw-rwSr-- 2 student student 4096 Nov 15 14:51 mydir2
```

```
student@UbuntuDesktop:~/oefperm$ find / -type d -perm -2000 2> /dev/null
/home/student/oefperm/mydir2
/var/local
/var/cache/man
/var/cache/man/cat1
```

permissions

- setgid and setuid on regular files
  - een executable file wordt uitgevoerd met de permissies van de file owner i.p.v. de executing owner
    → eender welke user kan een programma waarvan root owner is uitvoeren als root (indien de setuid bit is toegepast op dat programma)
  - setuid:
    - op de locatie van de x permission van user owner een s
    - 4 digits: 1e digit → 4
  - Voorbeeld:
    commando `passwd` maakt gebruik van `/etc/shadow`
    een gewone user kan zijn password zelf aanpassen

```
student@UbuntuDesktop:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1425 Okt 18 20:48 /etc/shadow
student@UbuntuDesktop:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 47032 Feb 17  2014 /usr/bin/passwd
```

access control lists

Standard unix permissions kunnen soms niet voldoen.

Access Control Lists (ACL's) kunnen files en directories verder beschermen.

https://help.ubuntu.com/community/FilePermissionsACLs

- `/etc/fstab`
  - file systems die acl's ondersteunen, moeten gemount worden met de acl optie in /etc/fstab
  - 4e veld → acl

```
student@server2:/home/testacl$ sudo tail -1 /etc/fstab
/dev/vg/lvol1   /home/testacl   ext4    acl,defaults    0       0
```

op server:

```
student@server2:/home/testacl$ sudo apt-get install acl
```

access control lists

- `getfacl`

```
student@UbuntuDesktop:~$ getfacl testfile
# file: testfile
# owner: student
# group: student
user::rw-
group::rw-
other::r--
```

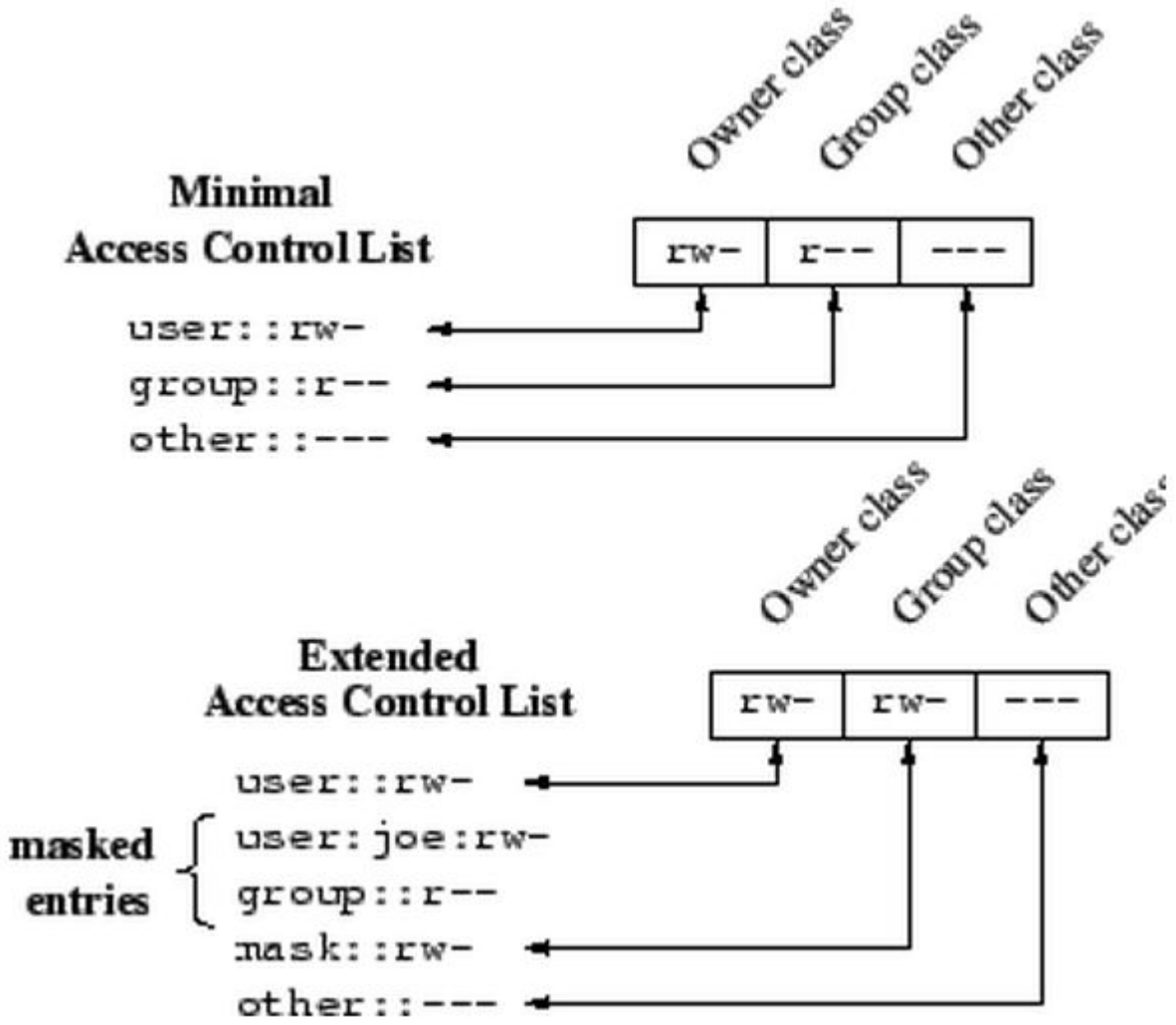
access control lists

- `setfacl`

```
student@UbuntuDesktop:~$ setfacl -m u:testuser:7 testfile
student@UbuntuDesktop:~$ setfacl -m g:testgroup:6 testfile
student@UbuntuDesktop:~$ getfacl testfile
# file: testfile
# owner: student
# group: student
user::rw-
user:testuser:rwx
group::rw-
group:testgroup:rw-
mask::rwx
other::r--

student@UbuntuDesktop:~$ ls -l | grep testfile
-rw-rwxr-+  1 student student     0 Okt 18 23:05 testfile
```

-m modify

\+ duidt aan dat ACL wordt gebruikt op deze file
dit is een extensie op het gewone POSIX permissions system


Owner class
Group class
Other class
Minimal
Access Control List
rw-
r--
---
user::rw-
group::r--
other::---
Owner class
Group class
Other clas
Extended
Access Control List
rw-
rw-
---
user::rw-
masked
entries
user:joe:rw-
group::r--
mask::rw-
other::---

access control lists

- remove an acl entry
  - -x

```
student@UbuntuDesktop:~$ setfacl -x testuser testfile
student@UbuntuDesktop:~$ getfacl testfile
# file: testfile
# owner: student
# group: student
user::rw-
group::rw-
group:testgroup:rw-
mask::rw-
other::r--
```

access control lists

```
student@UbuntuDesktop:~$ setfacl -b testfile
student@UbuntuDesktop:~$ getfacl testfile
# file: testfile
# owner: student
# group: student
user::rw-
group::rw-
other::r--
```

ete acl

access control lists

- the acl mask
  - definieert het maximum effective permissions voor een acl entry
  - wordt berekend telkens als `setfacl` of `chmod` wordt uitgevoerd
  - deze berekening kan je voorkomen door de optie `--no-mask` te gebruiken

```
student@UbuntuDesktop:~$ setfacl --no-mask -m u:testuser:7 testfile
student@UbuntuDesktop:~$ getfacl testfile
# file: testfile
# owner: student
# group: student
user::rw-
user:testuser:rwx                #effective:rw-
group::rw-
mask::rw-
other::r--
```

Entry type	Text form	Permissions
Named user	user:joe:r-x	r-x
Mask	mask::rw-	rw-
Effective permissions		r-

- http://www.vanemery.com/Linux/ACL/POSIX_ACL_on_Linux.html

access control lists

- eiciel
  - graphical tool

```
student@UbuntuDesktop:~$ sudo apt-get install eiciel nautilus-actions
```