



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](https://www.facebook.com/pxl.be)



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
 - comando 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 ppxl
 - 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
 - ziemann chage

```
student@ubuntudesktop01:~$ chage -l student
Last password change : Sep 19, 2018
Password expires      : never
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```



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

- gespecificeerd in /etc/passwd
- kan gewijzigd worden via usermod -s of via chsh

```
student@ubuntudesktop01:~$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/bin/bash
/bin/rbash
/bin/dash
```

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

in ubuntu:

```
student@ubuntudesktop01:~$ ls -l /bin | grep sh
-rwxr-xr-x 1 root root 1113504 Apr  4 20:30 bash
-rwxr-xr-x 1 root root 121432 Jan 25 2018 dash
lrwxrwxrwx 1 root root      4 Sep 19 12:01 rbash -> bash
lrwxrwxrwx 1 root root      4 Sep 19 12:01 sh -> dash
lrwxrwxrwx 1 root root      4 Sep 19 12:01 sh.distrib -> dash
lrwxrwxrwx 1 root root      7 Sep 19 12:01 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	GNOME Display Manager
<code>~/.bashrc</code>	no	yes	yes	yes	
<code>~/.profile</code>	no	yes	yes	yes	
<code>/etc/profile</code>	no	yes	yes	yes	
<code>/etc/bash.bashrc</code>	yes	no	no	yes	

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 (vb. 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 lijnen)

```
root@ubuntudesktop01:~# tail -1 /etc/passwd
veerle:x:1001:1001: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@ubuntudesktop01:~# tail -1 /etc/group
groupforveerle:x:1001:veerle
```

Voorbeeld:
user: veerle
group: groupforveerle



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

4. encrypteer je password

```
root@ubuntudesktop01:~# openssl passwd  
Password:  
Verifying - Password:  
VrSISrw39vM4I
```

5. vim /etc/shadow

voeg een lijn toe voor je user (eventueel met copy/paste) en gebruik je

```
root@ubuntudesktop01:~# tail -1 /etc/shadow  
veerle:VrSISrw39vM4I:17793:0:99999:7:::
```



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

6. maak een homedirectory met de inhoud van /etc/skel en de juiste ownerships en permissions

```
root@ubuntudesktop01:~# cp -r /etc/skel /home/veerle
root@ubuntudesktop01:~# chown -R veerle:groupforveerle /home/veerle
root@ubuntudesktop01:~# ls -la /home/veerle/
total 32
drwxr-xr-x 2 veerle groupforveerle 4096 Sep 19 12:44 .
drwxr-xr-x 4 root    root        4096 Sep 19 12:33 ..
-rw-r--r-- 1 veerle groupforveerle  220 Sep 19 12:44 .bash_logout
-rw-r--r-- 1 veerle groupforveerle 3771 Sep 19 12:44 .bashrc
-rw-r--r-- 1 veerle groupforveerle 8980 Sep 19 12:43 examples.desktop
-rw-r--r-- 1 veerle groupforveerle  807 Sep 19 12:44 .profile
```

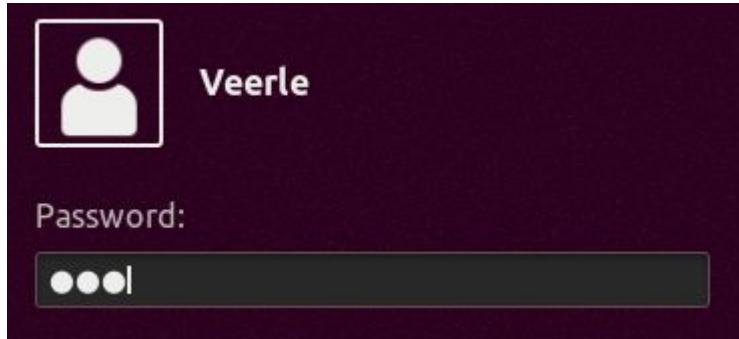


maak user en group a.d.h.v. local configuration files

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

```
student@ubuntudesktop01:~$ su - veerle
Password:
veerle@ubuntudesktop01:~$ pwd
/home/veerle
```

of log in (op een andere tty)



```
Ubuntu 18.04.1 LTS ubuntudesktop01 tty8
ubuntudesktop01 login: veerle
Password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-29-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch
```

40 packages can be updated.
17 updates are security updates.

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@ubuntudesktop01:~$ pwd
/home/veerle
```



alternatieve commando's

- adduser: alternatief voor useradd, maar:
 - paswoord kan onmiddellijk opgegeven worden
 - homedir wordt ook aangemaakt
- addgroup: alternatief voor groupadd, maar:
 - groupid wordt getoond na uitvoeren van het commando





File Security

file permissions

**DE HOGESCHOOL
MET HET NETWERK**

Hogeschool PXL – Dep. PXL-IT – Elfde-Liniestraat 26 – B-3500 Hasselt
www.pxl.be - [www.pxl.be/facebook](https://www.facebook.com/pxl.be)



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 karakter (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

permissies toevoegen

- chmod g-r

permissies verwijderen

- chmod o-r

- chmod a+w

a is niet nodig

- chmod +x

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

- chmod u=rw

- chmod u=rw, g=rw, o=r

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

- bepaalt de default permissies voor een file of directory

```
student@ubuntudesktop01:~$ umask  
0022
```

- een file is default nooit executable !!
- 1e digit → speciale permissies (advanced file permissions)
0: geen speciale modus
- voorbeeld berekening:

umask 033

directory: 777	=	111 111 111	file: 666	=	110 110 110
umask 033	=	000 011 011	umask 033	=	000 011 011
~033	=	111 100 100	~033	=	111 100 100
777 & ~033	=	111 100 100	666 & ~033	=	110 100 100
		rwX r-- r--			rW -r-- r--

- mkdir -m

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



permissions

- umask
 - Vereenvoudigde berekening van de permissies op basis van de umask

umask	<u>002</u>	777 (af trekken)
permissions	775	file: rw-rw-r-- dir: rwxrwxr-x

umask	<u>033</u>	777 (af trekken)
permissions	744	file: rw-r--r-- dir: rwxr--r--



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@ubuntudesktop01:~/oefperm$ mkdir mydir
student@ubuntudesktop01:~/oefperm$ ls -ld mydir/
drwxr-xr-x 2 student student 4096 Sep 19 13:06 mydir/
student@ubuntudesktop01:~/oefperm$ chmod +t mydir/
student@ubuntudesktop01:~/oefperm$ ls -ld mydir/
drwxr-xr-t 2 student student 4096 Sep 19 13:06 mydir/
```

```
student@ubuntudesktop01:~/oefperm$ chmod 1700 mydir/
student@ubuntudesktop01:~/oefperm$ ls -ld mydir/
drwx-----T 2 student student 4096 Sep 19 13:06 mydir/
```

- typisch voor /tmp

```
student@ubuntudesktop01:~/oefperm$ ls -ld /tmp/
drwxrwxrwt 18 root root 4096 Sep 19 13:09 /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@ubuntudesktop01:~/oefperm$ ls -ld mydir2
drwxr-xr-x 2 student student 4096 Sep 19 13:51 mydir2
student@ubuntudesktop01:~/oefperm$ chmod 2775 mydir2
student@ubuntudesktop01:~/oefperm$ ls -ld mydir2
drwxrwsr-x 2 student student 4096 Sep 19 13:51 mydir2
student@ubuntudesktop01:~/oefperm$ chmod a-x mydir2
student@ubuntudesktop01:~/oefperm$ ls -ld mydir2
drw-rwSr-- 2 student student 4096 Sep 19 13:51 mydir2
```



permissions

- setgid bit on directory

```
student@ubuntudesktop01:~/oefperm$ find / -type d -perm -2000 2> /dev/null
/usr/local/share/fonts
/usr/local/share/emacs
/usr/local/share/emacs/site-lisp
/usr/local/lib/python3.6
/usr/local/lib/python3.6/dist-packages
/usr/share/ppd/custom
/var/metrics
/var/local
/var/crash
/var/mail
/var/log/journal
/var/log/journal/1d5e74b1ff5344bc9f360288ad65ef85
/snap/core/4917/etc/chatscripts
/snap/core/4917/etc/ppp/peers
/snap/core/4917/usr/local/lib/python3.5
/snap/core/4917/usr/local/lib/python3.5/dist-packages
/snap/core/4917/var/local
/snap/core/4917/var/mail
/etc/ppp/peers
/etc/chatscripts
/home/student/oefperm/mydir2
```



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@ubuntudesktop01:~/oefperm$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1313 Sep 19 12:30 /etc/shadow
student@ubuntudesktop01:~/oefperm$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd
```

