SISTEME DE OPERARE (SO)

CURS 3

Lect. Univ. Dr. Mihai Stancu

Gestiunea utilizatorilor

Departamentul de Informatică

Suport de curs

- Suport (Introducere în sisteme de operare)
  - Secțiunea 3.1
  - Secțiunea 4.5
  - Secțiunea 10.2.3
  - Secțiunea 10.2.4
  - Secțiunea 10.3.3 (paragraful “sudo”)

Ce este un utilizator?

- perspectiva umană
  - persoană care folosește un sistem de calcul
- perspectiva sistemului de operare
  - cont pe un sistem
  - entitate de tip agent – execută acțiuni în cadrul sistemului
  - acces, drepturi (limitări, privilegii), acțiuni, proprietate (ownership)

Operatii realizate de utilizatori

- autentificare (login)
  - furnizarea unor date de autentificare (credențiale, *credentials*)
  - parolă, semnătură digitală, amprentă
- deconectare (logout)
- schimbare credențiale (parolă, detalii de acces)
- schimbarea utilizatorului (switch user)
- rulare aplicații
- creare de noi elemente (de exemplu fișiere)
- configurare permisiuni pe elemente

Login-logout

- autentficare/deconectare
- ecran/prompt de login
- presupun existența unui cont de utilizator (*user account*)
- acțiuni specifice sistemului de operare și altor aplicații
- furnizarea unor credențiale
  - nume de utilizator (*username*)
  - în general o parolă (*password*)

Parola

- forma obișnuită de obținere a accesului (login)
- șir de caractere tipăribile
- considerente de securitate
  - fără cuvinte comune (din dicționar)
  - fără date de naștere
  - dacă se notează, de avut grijă unde se notează
  - înlocuire periodică
  - caractere speciale, numere, majuscule

Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.

Clifford Stoll

Schimbarea utilizatorului

- *fast user switching* în mediul grafic
  - nu presupune logout
  - Windows + L în Windows (*Fast User Switching*)
- în linia de comandă, comanda `su` (*substitute user*)

Folosirea comenzii su

```
alin@anaconda:~$ su
Password:
root@anaconda:/home/alin# exit
alin@anaconda:~$ su -
Password:
root@anaconda:~# logout
alin@anaconda:~$ su - so
Password:
so@anaconda:~$
```

Drepturi de acces

- *access rights, permissions*
- permisiuni pe care le are un utilizator, acțiuni pe care le poate realiza
- drepturi generice: citire și scriere
  - **citire**: un fișier/o zonă de memorie poate fi vizualizat(ă)
  - **scriere**: un fișier poate fi editat, se poate scrie în memorie
- se recomandă utilizarea nivelului minim de privilegiu (*least privilege*)
- în sistemele de operare moderne, există noțiunea de proprietate pe un fișier (*ownership*)
- un utilizator poate configura drepturile pe fișiere aflate în proprietate sa (pe care le deține, pe care este *owner*)

Actiuni privilegiate

- acțiunile neprivilegiate pot fi executate de toți utilizatorii
  - parcurgerea ierarhiei de fișiere
  - rularea de programe
  - conexiuni de rețea
- acțiunile privilegiate pot fi executate doar de anumiți utilizatori
  - gestiunea utilizatorilor (adăugare, ștergere utilizatori)
  - gestiunea pachetelor
  - configurarea rețelei
  - configurarea parametrilor de boot
  - configurarea nucleului

Utilizator privilegiat

- în general, există un utilizator sau seturi de utilizatori privilegiați cu drepturi depline în sistem
  - Unix: utilizatorul `root`
  - Windows: utilizatorul `Administrator`, grupul `Administrators`
- accesul unui utilizator străin la un cont privilegiat înseamnă compromiterea sistemului
- se recomandă folosirea redusă a contului privilegiat
  - pe Unix, se poate folosi `su` sau `sudo`
  - începând cu Windows Vista, *User Account Control* (UAC)

GRUPURI

- colecție de utilizatori
- “partajarea” privilegiilor
- utile pentru acordarea unor permisiuni mai multor utilizatori de același tip
- un utilizator poate face parte din mai multe grupuri
- dacă nu ar exista grupuri, ar trebui definite permisiuni pentru fiecare utilizator în parte –> probleme de scalabilitate

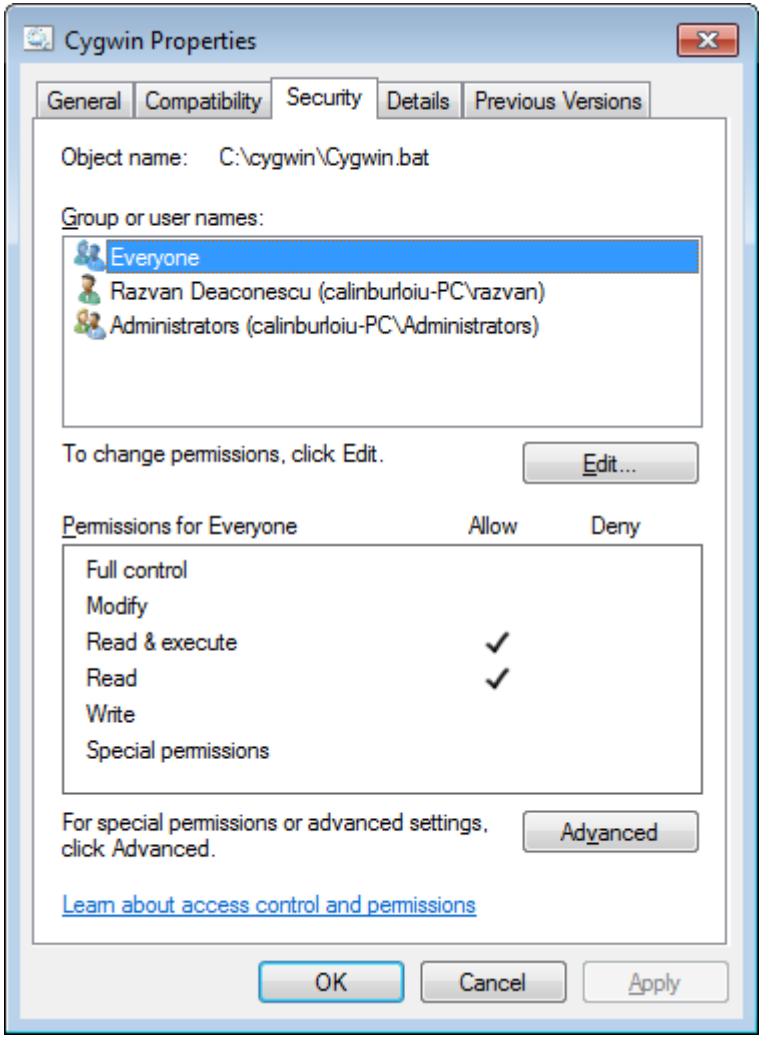
Drepturi de acces la sistemul de fisiere

- permisiuni ale utilizatorilor la intrări din SF
- drepturi/permisiuni: citire, scriere, ștergere, parcurgere
- liste de control al accesului (*Access Control Lists* – ACLs)
  - pentru fiecare fișier se creează o listă
  - o intrare a listei spune ce utilizator are ce drepturi
  - exemplu: `(Ana, citire), (Daniel, citire&scriere), (Elena, scriere)`
- în Unix, formă simplificată de ACL
  - drepturi pentru 3 entități
    - utilizator (*user*)
    - grup (*group*)
    - ceilalți (*others*)

Drepturi de acces la SF in Windows

- pe NTFS, folosind liste de control al accesului
- (WinXP) trebuie dezactivat `Use simple file sharing`
  - `Tools -> Folder Options -> View -> Advanced`

`click dreapta`
`-> Properties`
`-> tab:Security`



- Read
- Write
- Read & Execute
- List Folder Contents
- Modify
- Full Control

Drepturi de acces la SF in Unix

- 3 tipuri de entități
  - utilizator (*user*)
  - grup (*group*)
  - ceilalți (*others*)
- 3 tipuri de permisiuni
  - citire (*read*)
  - scriere (*write*)
  - execuție (*execute*)

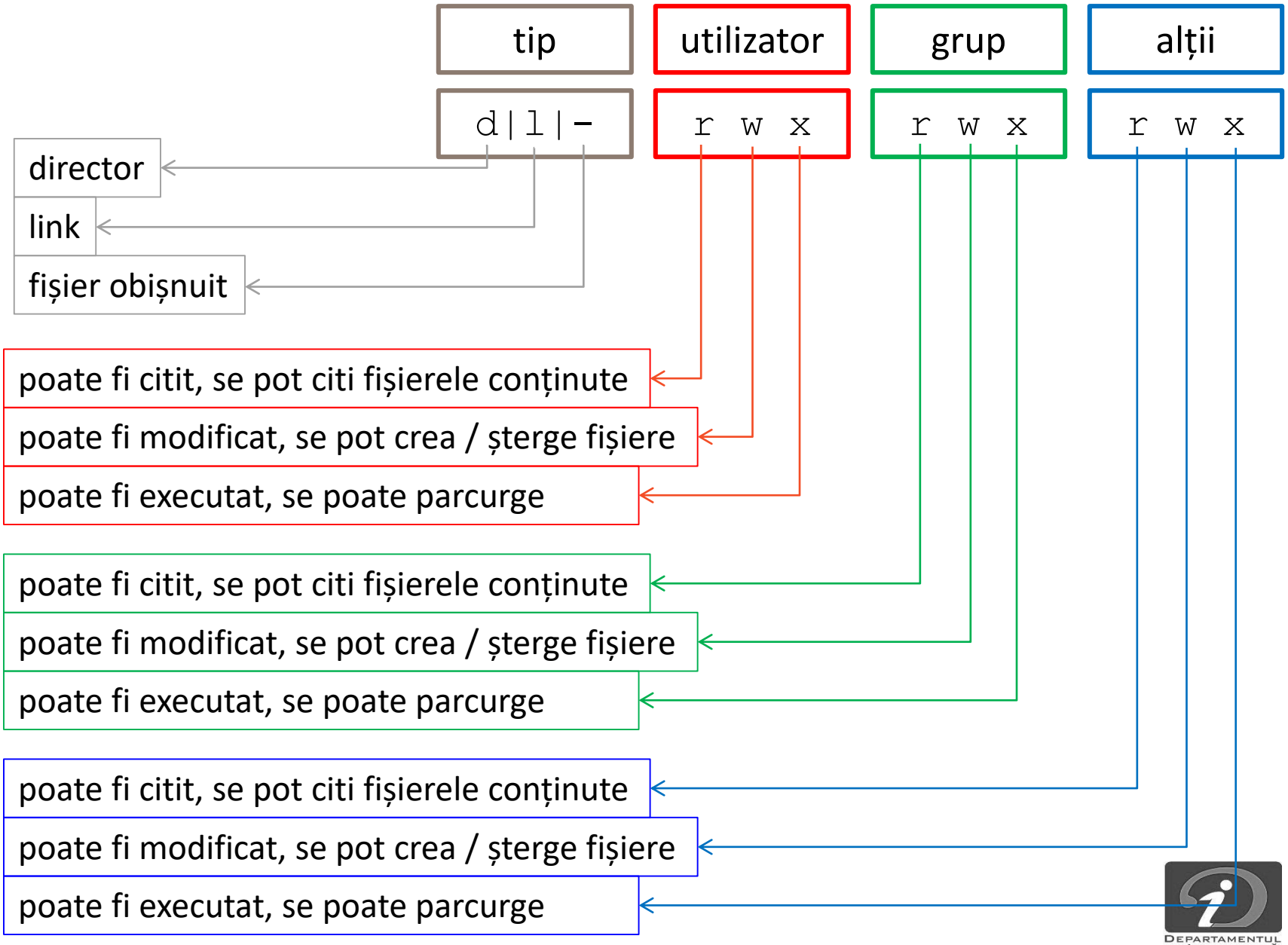
Permisiuni în Unix

```
so@anaconda:~$ ls -ld repo.git/
drwxr-xr-x 7 so so 4096 Jul 22 11:49 repo.git/
rwx - drepturi pentru utilizator (deținător)
r-x - drepturi pentru grup
r-x - drepturi pentru ceilalți
```

Drepturi de acces la SF in Unix – continuare

- drepturi pe fișiere
  - **read** – fișierul poate fi citit/vizualizat (`cat, less, view`)
  - **write** – fișierul poate fi editat (`vi, emacs, nano`) sau șters (`rm`)
  - **execute** – fișierul poate fi executat/rulat (`./file`)
- drepturi pe directoare
  - **read** – directorul poate fi listat (`ls`)
  - **write** – se pot crea noi intrări (`touch, mkdir`) sau șterge intrări (`rm, rmdir`)
  - **execute** – directorul poate fi parcurs (traversat); necesar și pentru listare

Drepturi de acces la SF in Unix – continuare



Drepturi de acces la SF in Unix – continuare

- drepturile de acces pot fi reprezentate în octal
- pentru fiecare entitate se completează 3 biți (1 sau 0) conform celor 3 drepturi
- cifre de la 0 la 7
  - `-w-` = 010 = 2
  - `-wx` = 011 = 3
  - `r-x` = 101 = 5
  - `rw-` = 110 = 6
- **`rwxr-xr-x`** = 755
- **`rw-r--r--`** = 644

CHMOD

- *change mode*
- configurarea permisiunilor pe o intrare în SF
- utilizatorul trebuie să dețină fișierul
- opțiunea `-R` pentru parcurgere recursivă a directoarelor (în adâncime)
- permite configurare de drepturi în format literal și octal
- **`u`** – *user*, **`g`** – *group*, **`o`** – *others*, **`a`** – *all*
- `r` – *read*, `w` – *write*, `x` – *execute*

CHMOD – CONTINUARE

Utilizare chmod

```
alin@anaconda:/tmp$ ls -l so-c3.test
-rw-r--r-- 1 alin alin 0 Oct 17 17:29 so-c3.test
alin@anaconda:/tmp$ chmod u+x so-c3.test
alin@anaconda:/tmp$ ls -l so-c3.test
-rwxr--r-- 1 alin alin 0 Oct 17 17:29 so-c3.test
alin@anaconda:/tmp$ chmod o-r so-c3.test
alin@anaconda:/tmp$ ls -l so-c3.test
-rwxr----- 1 alin alin 0 Oct 17 17:29 so-c3.test
alin@anaconda:/tmp$ chmod go+w so-c3.test
alin@anaconda:/tmp$ ls -l so-c3.test
-rwxrw--w- 1 alin alin 0 Oct 17 17:29 so-c3.test
alin@anaconda:/tmp$ chmod a-w so-c3.test
alin@anaconda:/tmp$ ls -l so-c3.test
-r-xr----- 1 alin alin 0 Oct 17 17:29 so-c3.test
alin@anaconda:/tmp$ chmod 644 so-c3.test
alin@anaconda:/tmp$ ls -l so-c3.test
-rw-r--r-- 1 alin alin 0 Oct 17 17:29 so-c3.test
alin@anaconda:/tmp$ chmod 513 so-c3.test
alin@anaconda:/tmp$ ls -l so-c3.test
-r-x--x-wx 1 alin alin 0 Oct 17 17:29 so-c3.test
```

CHOWN

- *change ownership*
- schimbarea utilizatorului și/sau a grupului unei intrări în SF
- poate fi realizată doar de root
- opțiunea `-R` pentru parcurgere recursivă

Utilizare chown

```
root@anaconda:/tmp# ls -l so-c3.test
-rw-r--r-- 1 alin alin 0 Oct 17 17:29 so-c3.test
root@anaconda:/tmp# chown so so-c3.test
root@anaconda:/tmp# ls -l so-c3.test
-rw-r--r-- 1 so alin 0 Oct 17 17:29 so-c3.test
root@anaconda:/tmp# chown :users so-c3.test
root@anaconda:/tmp# ls -l so-c3.test
-rw-r--r-- 1 so users 0 Oct 17 17:29 so-c3.test
root@anaconda:/tmp# chown alin:alin so-c3.test
root@anaconda:/tmp# ls -l so-c3.test
-rw-r--r-- 1 alin alin 0 Oct 17 17:29 so-c3.test
```

SUDO

- *substitute user do*
- rularea unor comenzi cu drepturile altui utilizator
- de obicei se rulează cu drepturi de root
- este solicitată parola utilizatorului care rulează comanda

Exemple de cazuri de utilizare sudo

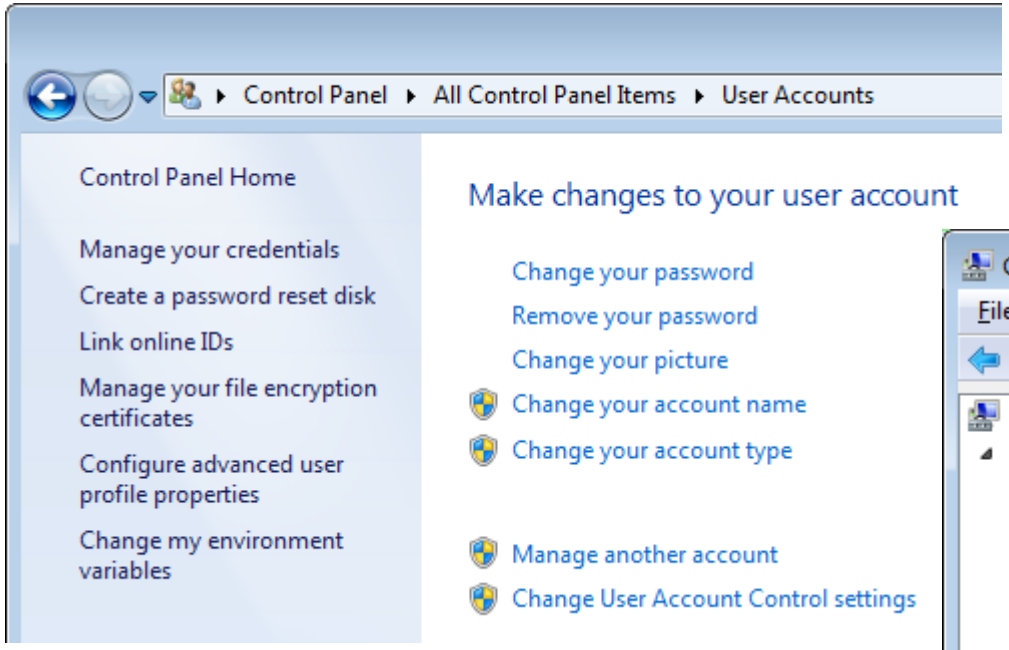
```
$ sudo apt-get install package-name    # install package-name
$ sudo su                              # open root shell
$ sudo bash                            # open root shell
```

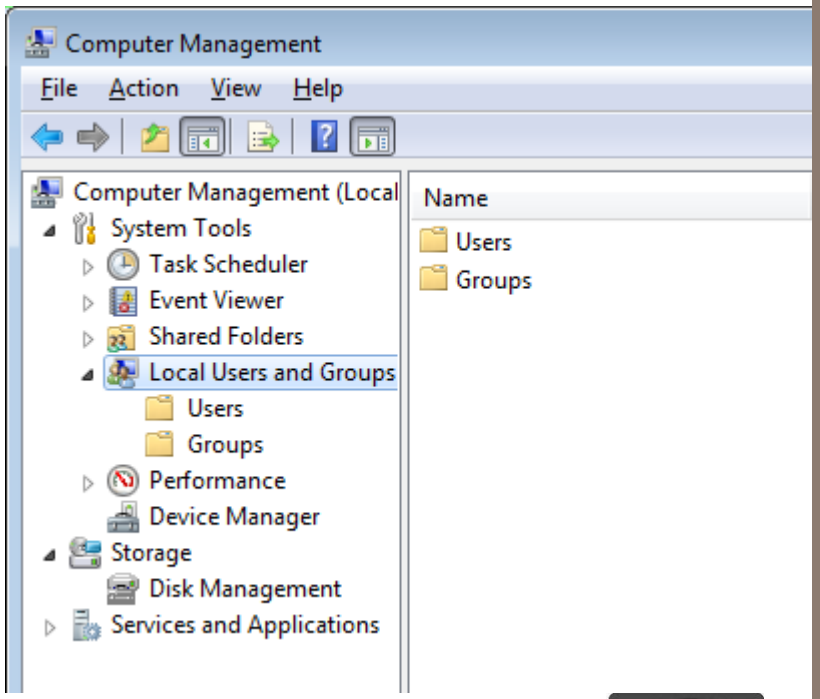
Operatii cu utilizatori si grupuri

- neprivilegiate
  - informații despre utilizatori și grupuri
- privilegiate
  - adăugare utilizator
  - ștergere utilizator
  - adăugare, ștergere grup
  - adăugare/ștergere utilizator la/din grup
  - schimbare proprietăți ale utilizatorului, grupului
  - parolă
  - nume de utilizator
  - home folder

Administrarea utilizatorilor in Windows

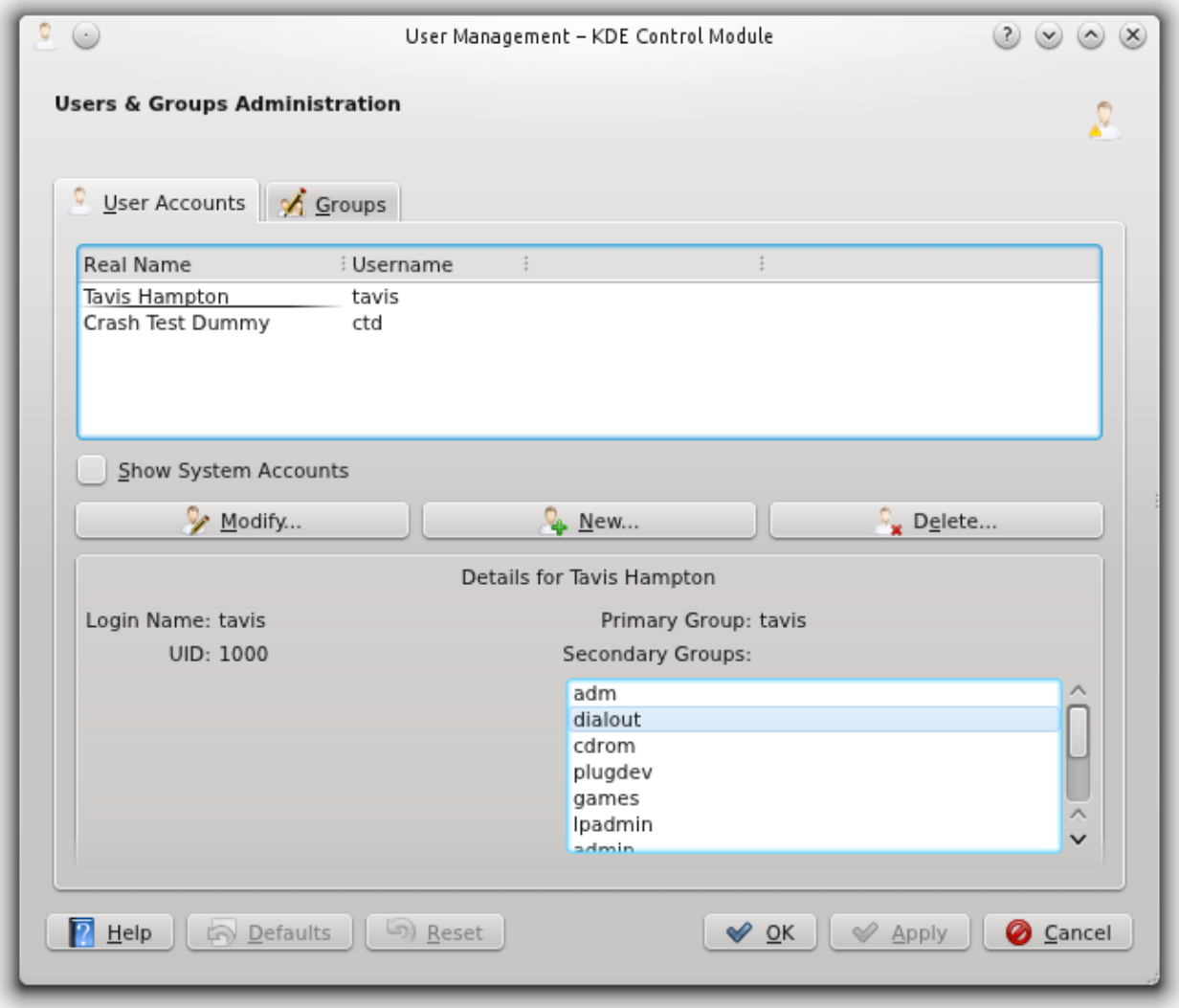
- Control Panel -> User Accounts
- click dreapta pe My Computer -> Manage -> Local Users and Groups



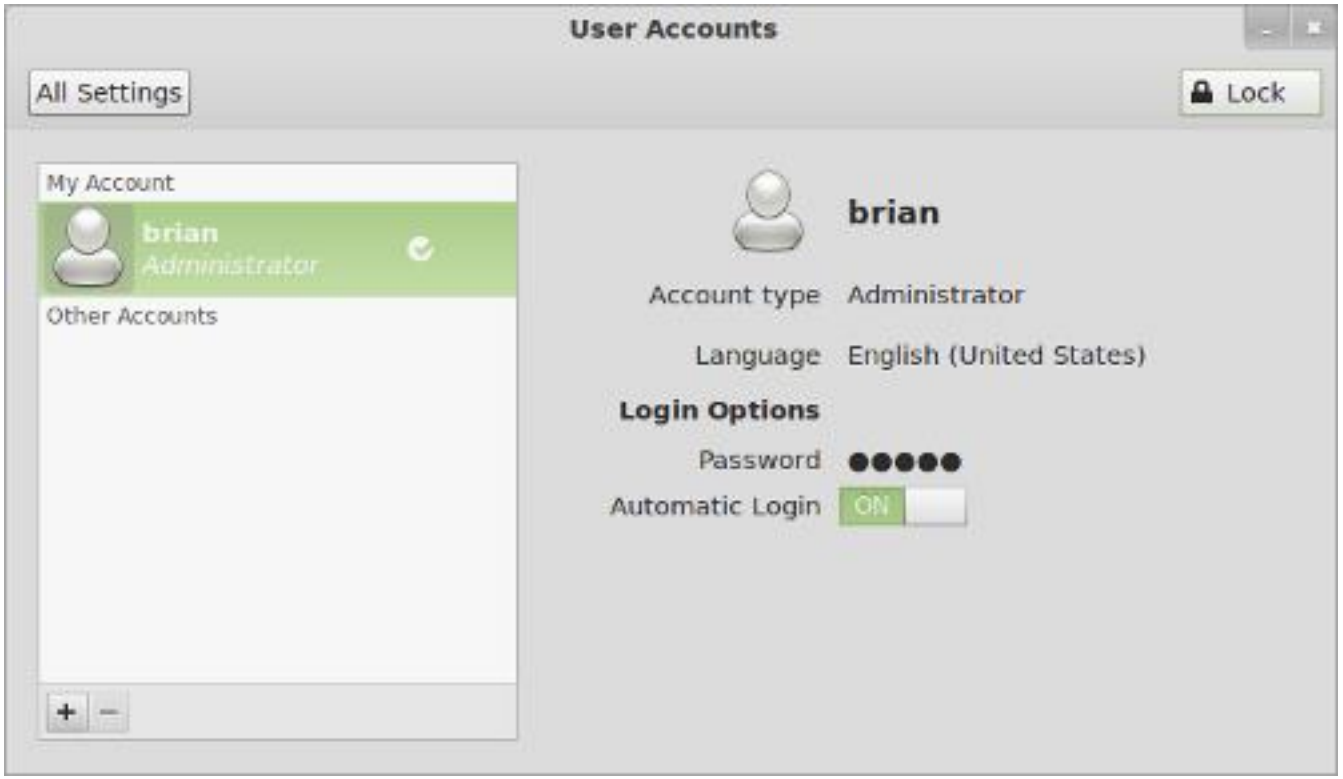


Administrarea utilizatorilor in Linux – KDE

- Start -> Applications -> Settings -> System Settings -> User Management



- `System Settings -> User Accounts`
- `gnome-control-center user-accounts` (rulat cu drepturi privilegiate)



Informatii despre utilizatori in Unix

- sistemul de operare recunoaște utilizatorii și grupurile după identificatori numerici
  - uid – user identifier
    - identificator unic al unui utilizator în sistemul de operare
  - gid – group identifier
    - identificator unic al unui grup în sistemul de operare

Informații despre utilizatori

```
so@anaconda:~$ id
uid=1001(so) gid=1009(courses) groups=1009(courses)
so@anaconda:~$ id -u
1001
so@anaconda:~$ id rl
uid=1000(rl) gid=1009(courses) groups=1009(courses)
so@anaconda:~$ finger mps
Login: mps
Name: Managementul Proiectelor Software
Directory: /home/mps
Shell: /bin/bash
so@anaconda:~$ groups pw
pw : courses
```

Adaugarea si stergerea utilizatorilor in Unix

- necesita drepturi privilegiate
- comenzile `useradd, userdel`

Lucrul cu utilizatori în Unix

```
root@anaconda:~# useradd -m -d /home/so -s /bin/bash so
root@anaconda:~# passwd so
root@anaconda:~# userdel -r so
```

- pe sistemele Debian-based există comenzi de tip *wrapper*, mai ușor de folosit: `adduser, deluser`

Lucrul cu utilizatori pe sistemele Debian-based

```
root@anaconda:~# adduser so
Adding user ‘so’ ...
Adding new group ‘so’ (1002) ...
Adding new user ‘so’ (1002) with group ‘so’ ...
Enter new UNIX password:
Retype new UNIX password:
root@anaconda:~# deluser --remove-home so
```

Adaugarea si stergerea grupurilor in Unix

- necesita drepturi privilegiate
- comenzile groupadd, groupdel
- pe sistemele Debian-based exista comenzi de tip *wrapper*: `addgroup, delgroup`

Lucrul cu grupuri în Unix

```
root@anaconda:~# addgroup test
Adding group 'test' (GID 1003) ...
Done.
root@anaconda:~# id so
uid=1002(so) gid=1002(so) groups=1002(so)
root@anaconda:~# adduser so test
Adding user 'so' to group 'test' ...
Adding user so to group test
Done.
root@anaconda:~# id so
uid=1002(so) gid=1002(so) groups=1002(so),1003(test)
root@anaconda:~# deluser so test
```

Modificarea proprietatilor utilizatorilor

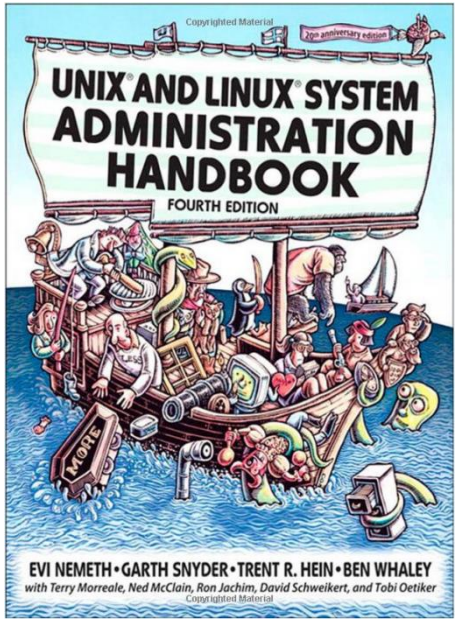
- `usermod`
  - rulat de `root`
  - modifică informații precum shell-ul de login, login name, home directory
- `passwd`
  - fără argument, schimbarea parolei utilizatorului curent (nu necesită drepturi privilegiate)
  - cu argument, schimbarea parolei utilizatorului (necesită drepturi privilegiate – `root`)

Schimbarea parolei utilizatorului `george` (rulat de `root`)

```
# passwd george
```

UNIX AND LINUX SYSTEM ADMINISTRATION HANDBOOK

- 2010, 4th Edition
- Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley
- una dintre cele mai apreciate cărți de administrare Unix/Linux
- aproape 1300 de pagini, 32 de capitole
- sistemul de fișiere, utilizatori, procese, rețelistică, servicii, securitate, virtualizare



Bram Moolenaar

- autorul Vim (Vi IMproved)
- Vim este unul dintre cele mai răspândite editoare în lumea Unix
  - programatori și administratori
- lucrează la Google

Microsoft

- http://www.microsoft.com/
- Windows, Office, Internet Explorer, Xbox, Bing
- cel mai mare producător de software
- Bill Gates, Steve Ballmer
- fondată în 1975
- DOS, Windows 3.1, Windows 95, Windows 98
- Windows NT, 2000, XP, 2003, Vista, 2008, 7, 8, 10
- a cumpărat Skype în 2011

SSO

- Single Sign-On
- un singur acces la sistemul de autentificare oferă accesul la întregul set de resurse
  - HTTP cookies
- folosirea unui sistem centralizat de servere de autentificare
  - LDAP databases

Cuvinte cheie

- utilizator
- autentificare
- parolă
- root
- su
- drepturi de access
- root
- Administrator
- grupuri
- ACL
- user, group, others
- read, write, execute
- chmod
- chown
- sudo
- id, finger, groups
- useradd, userdel, usermod
- adduser, deluser
- addgroup, delgroup
- passwd

Resurse utile

- http://en.wikipedia.org/wiki/User_%28computing%29
- http://teklimbu.wordpress.com/2008/01/20/effective-user-management-under-linuxunix/
- htttp://www.dartmouth.edu/~rc/help/faq/permissions.html
- http://en.wikipedia.org/wiki/Sudo
- http://technet.microsoft.com/en-us/library/bb727008.aspx
- http://technet.microsoft.com/en-us/library/bb726984.aspx
- http://ss64.com/bash/chmod.html
- http://pogostick.net/~pnh/ntpasswd/
- http://www.makeuseof.com/tag/how-to-reset-any-linux-password/