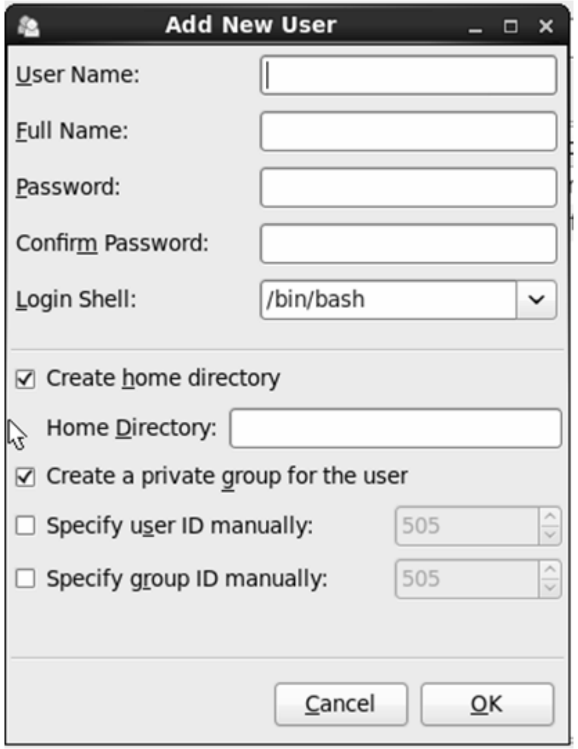
Brukerkontoer

- OS’et trenger en mekanisme for å håndtere sikkerhet
  - Vi bruker kontoer og rettigheter
- Det er to klasser med kontoer
  - root – tilgang til alt
  - Normale brukerkontoer – Har tilgang til brukerens hjemmeområdet og filer, samt “public” filer
  - Vi kan videre dele normale brukerkontoer i normale kontoer for vanlige brukere, og kontoer for programvare

Brukerkontoer: Attributter

- Brukernavn, User ID number (UID), passord
- Oppføringer i både /etc/passwd og /etc/shadow
- Privat gruppe (optional) med en Group ID number (GID), oppføring i /etc/group
- Hjemmeområde, som standard i katalogen /home, med standard filer
- Log in shell, som standard, Bash
  - Programvare kan ha en mappestruktur som ikke ligger under /home (f.eks, /usr eller /var) og kan ha login shell som /sbin/nologin for å hindre at noen logger inn som programvaren (sikkerhetsmekanisme)

Lage brukere eller gruppekontoer: GUI



User Name:	
Full Name:	
Password:	
Confirm Password:	
Login Shell:	/bin/bash

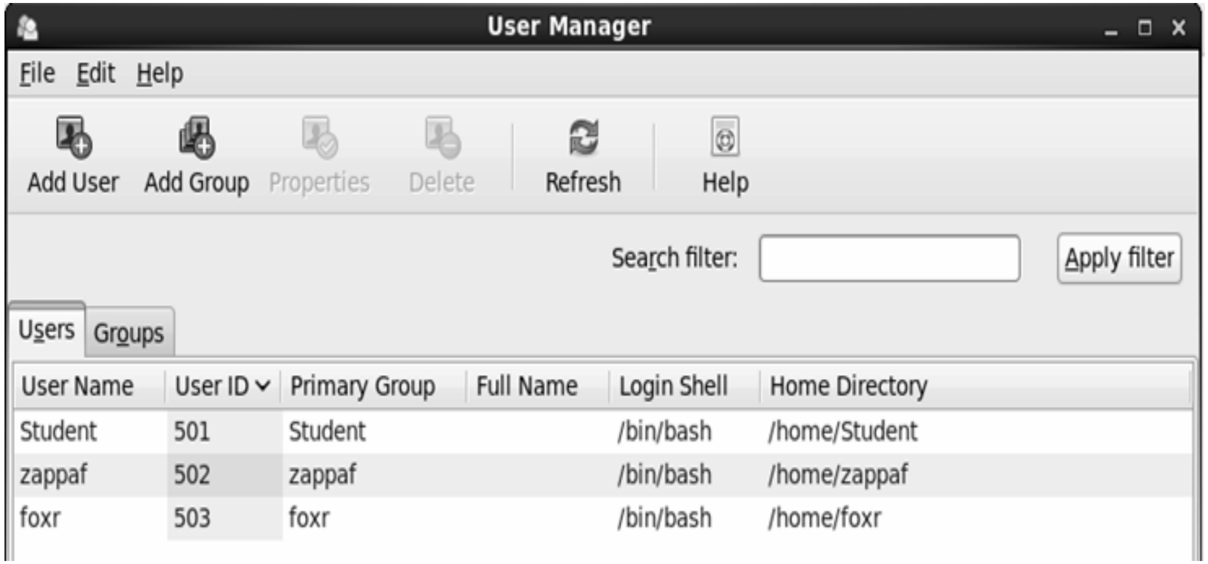
☑ Create home directory

Home Directory:

☑ Create a private group for the user

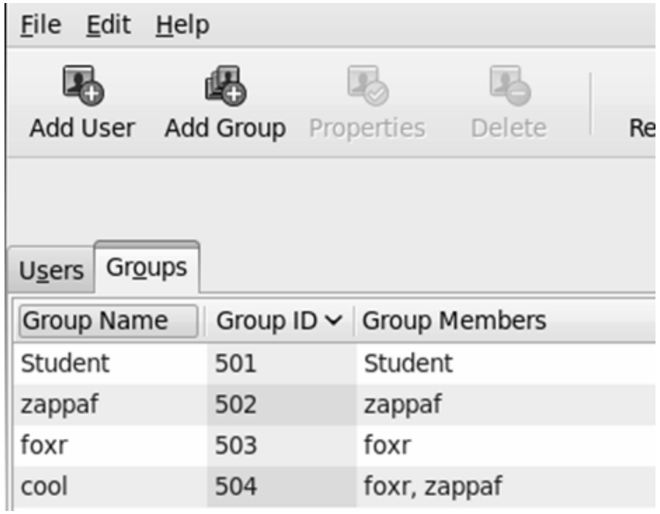
□ Specify user ID manually: 505

□ Specify group ID manually: 505



Search filter:

User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
Student	501	Student		/bin/bash	/home/Student
zappaf	502	zappaf		/bin/bash	/home/zappaf
foxr	503	foxr		/bin/bash	/home/foxr



Group Name	Group ID	Group Members
Student	501	Student
zappaf	502	zappaf
foxr	503	foxr
cool	504	foxr, zappaf

Lage brukerkontoer: Kommandolinje

- useradd kommando
  - Eneste parameter du trenger er brukernavn for å opprette kontoen
    - En hel haug med opsjoner for å unngå standard konto (som default home directory, default shell and default UID)
    - Standard UID/GID er1 større enn siste UID/GID brukt
- Kommandolinjen kan være krevende å bruke, men svært effektiv når du skal lage mange
  - Skriv kommandoen
  - Trykk control+p (eller pil opp) og modifiser forrige kommando for neste bruker
  - Rasker å skrive kommando enn å klikke og peke på kjedelig GUI ☺

Lage brukerkontoer: useradd opsjoner

Option	Meaning	Example
-c comment	Fills comment field, used to specify user's full name	"Richard Fox" – quote marks are necessary if the value has a blank space
-d directory	Used to alter the user's home directory from /home/username to directory	-d /home/faculty/foxr
-D	Print default values to see what defaults are currently set as, including directory, expiration value, default shell, default skeleton directory (see below), default shell, and whether to create an email storage location	
-e date	Set expiration date to date	-e 2014-05-31
-g GID	Alter private group ID to this value, otherwise it defaults to 1 greater than the last issued GID	-g 999
-G groups	Add user to the listed groups; groups are listed by name or GID and separated by commas with no spaces in between	-G faculty,staff,admin
-k directory	Change the default skeleton directory (this is explained in subsection G)	-k /etc/students/skel

Lage brukerkontoer: useradd opsjoner

Option	Meaning	Example
-l	Do not add this user to the lastlog or faillog log files; this permits an account to go “unnoticed” by authentication logging mechanisms, which constitutes a breach in security	
-m	Create a home directory for this user	
-M	Do not create a home directory for this user (the default case so can be omitted)	
-N	Do not create a private group for this user	
-o	Used in conjunction with –u so that the UID does not have to be unique, see –u	-u 999 –o
-p passwd	Set the user’s initial password; passwd must be encrypted for this to work	
-r	Create a system account for this user	
-s shell	Provide this user the specified shell rather than the default shell; for software, you will often use this to establish the shell as /sbin/nologin	-s /bin/csh
-u UID	Give user the UID of UID rather than the default (one greater than the last UID); can be used with –o so that two users share a UID	-u 999

Eksempler: useradd

- useradd foo1
  - create new user account foo1 with all of the default values except for a home directory (because –m was not used –Stemmer ikke I CENTOS 7)
- useradd –m foo2
  - create new user account foo2 with all of the default values including a home directory at /home/foo2
- useradd –m –d /home/students/foo3
  - create new user account foo3 with a home directory of /home/students/foo3
- useradd –m –u 1001 foo5
  - create new user account foo5 with UID of 1001
- useradd –m –o –u 1001 foo5jr
  - create new user account foo5jr who will have the same UID as foo5
- useradd –m –e 2015-12-31 –l –r backdoor
  - interested in creating a backdoor account?
- useradd –l –M –N –s /sbin/nologin softwaretitle
  - create an account for softwaretitle that has no group, no login, no home directory and is not logged in lastlog or faillog log files

Brukerkontoer: Defaults

- Standard verdi for useradd får du med følgende opsjon
  - useradd –D
- Shellet vil skrive noe slikt
  - GROUP=100 (this is the default group number to use for any user account not given a private group through –N)
  - HOME=/home
  - INACTIVE=-1
  - EXPIRE=
  - SHELL=/bin/bash
  - SKEL=/etc/skel
  - CREATE_MAIL_SPOOL=yes
- For å endre en standardverdi, bruk useradd –D optionen sin verdi som f.eks. useradd –D –s /bin/csh for å bytte standardshell fra/bin/bash til /bin/csh

Opprette grupper: CLI

- groupadd kommandoen har færre opsjoner
  - – groupadd [options] groupname

Option	Meaning
-f	Force groupadd to exit without error if the specified groupname is already in use, in which case groupadd does not create a new group
-g GID	Use the specified GID in place of the default, if used with –f and the GID already exists, it will cause groupadd to generate a unique GID in place of the specified GID
-o	Used with –g so that two groups can share a GID
-p passwd	Assign the group to have the specified passwd
-r	Create a system group

Hvordan lage mange kontoer?

- Enter initial useradd command
  - useradd –c “Mike Keneally” –m keneallym
- Use command line editing to convert the above for new user George Duke (dukeg)
  - control+p – recall the instruction
  - escape+b – move to beginning of user name
  - control+k (or escape+d) – delete username
  - dukeg – enter new user name
  - control+a, escape+f, escape+f, control+f, control+f – move to the “M” in Mike Keneally
  - escape+d, escape+d – delete Mike Keneally (if there were more than two names in quotes, do additional escape+d’s)
  - George Duke – type the new name
  - <enter>
- Repeat for each new user account

Flere kontoer gjennom et script

- La oss anta at vi har en fil med alle nye brukere på formen fornavn etternavn
  - Vi skal gi hver bruker en konto på formen etternavn + forbokstav i fornavn. Eks Tore Engen blir brukernavn “engent”

```
#!/bin/bash
while read first last; do
        name="$first $last"
        username="$last${first:0:1}"
        useradd –c "$name" –m $username
done
```

Se “” brukt rundt $name etter -c

Hva om vi har to brukere med samme ettnavn “Engen” og Den ene heter “Tore” og den andre heter Tom” ?

Vi skal oppdatere skriptet og sjekke i /etc/passwd for om det aktuelle brukernavnet vi tenker å bruke er benytter før. Er det brukt, legger vi til et tall.

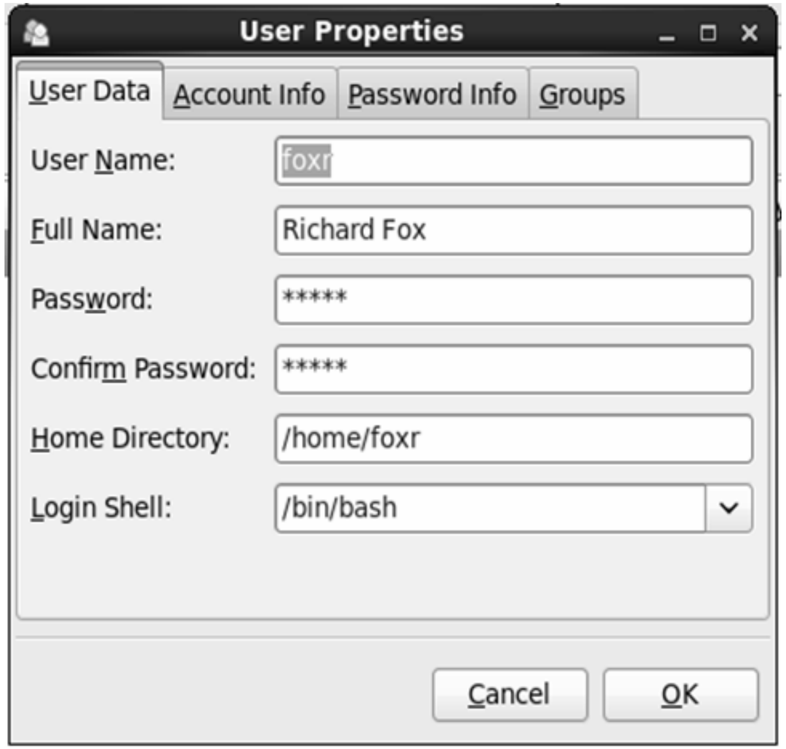
Flere kontoer gjennom et script

- Modifisert skript
  - Vi sjekker antallet som har “etternavn + første forbokstav i fornavn” likt, og legger til et tall på dette brukernavnet

```
#!/bin/bash
while read first last; do
        name= "$first $last"
        username="$last${first:0:1}"
        n=`egrep –c $username /etc/passwd`
        n=$((n+1))
        username=$username$n
        useradd –c "$name" –m $username
done
```

Vedlikehold av brukere og grupper

- Vi kan bruke "User Manager GUI" for å endre brukere og grupper
- Finnes den ikke? – installer med "yum install system-config-users". Start deretter med kommandoen "system-config-users &" som root.



User Properties

User Name: foxr

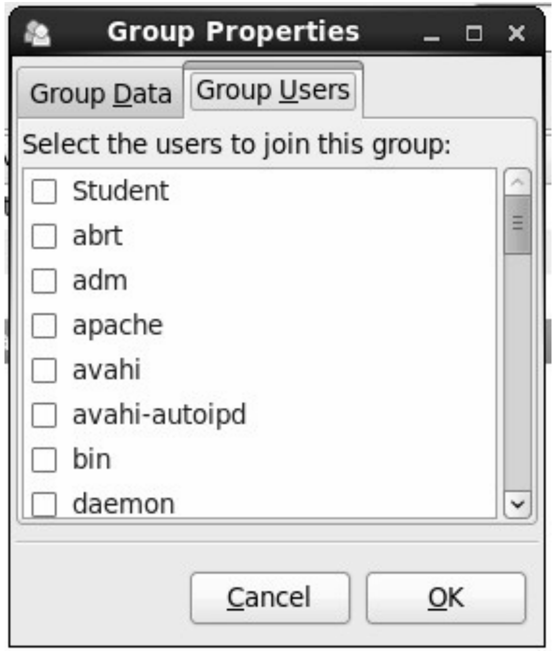
Full Name: Richard Fox

Password: *****

Confirm Password: *****

Home Directory: /home/foxr

Login Shell: /bin/bash



Group Properties

Select the users to join this group:

- ☐ Student
- ☐ abrt
- ☐ adm
- ☐ apache
- ☐ avahi
- ☐ avahi-autoipd
- ☐ bin
- ☐ daemon

Vedlikehold av brukere og grupper

- usermod – similar options to useradd
  - -l newname – changes user’s username to newname
  - -L, -U – lock and unlock the account
  - -m dir – change home directory to dir
- groupmod – similar options to groupadd
  - –n newname – changes group name go newname
- userdel and groupdel – delete users and groups
  - for userdel, -f forces deletion even if user is logged in or has processes running
  - -r – deletes user’s home files (home directory, email directory) but other files owned by the user outside of the home directory remain

Passord: /etc/shadow

- chage kontrollerer informasjonen lagret i /etc/shadow om utløp på en brukers passord
  - /etc/shadow lagrer brukernavn og kryptert password for hver bruker på følgende form:
    - days since January 1, 1970 that the password was last changed
    - days before the password may change again
    - days before the password must be changed
    - days before warning is issued
    - days after the password expires that the account is disabled
    - days since January 1, 1970 that the account will become disabled
  - Hvor tegnet :: betyr ikke noen verdi mellom de forskjellige elementene ::
    - zappaf:…:15558:1:35:25:20:365:
    - foxr:…:15558:1:28:21:10::

Passord: chage (kommando)

- For å endre informasjon i /etc/shadow som kontrollerer brukerens passord (bortsett fra å endre passordet), use
  - chage [options] username

Option	Meaning
-d day	Set number of days when password was last changed (automatically set once password is changed, if never changed, this date is the number of days since the epoch)
-E day	Set day on which user's account will become inactive (will expire), specified as a date (YYYY-MM-DD) or the number of days since the epoch
-I day	Set number of days of inactivity after a password has expired before the account becomes locked. Using –I -1 removes any previously established inactivity date.
-l	Show this user's password date information
-M days	Number of days remaining before user must change password, use with –W.
-m days	Minimum number of days between which a user is allowed to change passwords, 0 means user free to change password at any time
-W days	Number of days prior to when a password must be changed that a warning is issued

Passord: passwd (kommando)

- passwd kommando er brukt for å endre en brukers passord
  - passwd [options] username
- Mange opsjoner som overlapper kommandoen chage

Option	Meaning
-d	Disable the password (make the account password-less)
-i day	Same as chage –I day
-k	Only modify the password if it has expired
-l	Lock the account (user cannot login until unlocked)
-n day	Same as chage –m day
-S	Output status of password for the given account, similar to chage -l
-u	Unlock the locked account
-x day	Same as chage –M day
-w day	Same as chage –W day

Nyttig info: /etc/skel

- /etc/skel katalogen inneholder filer som vil bli kopier til NYE brukeres hjemmeområde
  - Systemansvarlig vil sette opp denne strukturen basert på hva han tror brukerne trenger:
  - Eksempler er filer som .bashrc, .bashrc_profile, .bash_logout and kataloger som .gnome and .mozilla

Nyttig info: /etc/bashrc

- When a user opens a Bash shell, the /etc/bashrc is executed
  - This allows the system administrator to establish default settings for all users' Bash settings
- There is also /etc/profile for all user logins irrelevant of shell
  - These scripts will establish environment variables like
    - EDITOR – for default editor (/bin/vi or /bin/vim)
    - PATH – an initial PATH variable
    - PS1 – user prompt
    - umask – initial umask value for file and directory permissions

sudo

- The sudo command allows a user to execute an instruction as another user
  - The most common use is to let a user execute root-level commands
  - This is of course dangerous so we must be careful with who we provide sudo access with and what they can do with it
- The sudo command looks like this:
  - sudo [-u username|uid] [-g groupname|gid] command
  - Thus, you specify the command you want to execute and the user that the command should execute under
  - If you omit user/group, the default is to execute it as root
  - In order to use sudo, the user must have an entry in the /etc/sudoers file (see next slide)

sudo: /etc/sudoers

- This file, accessible only by root, lists all of the users who have sudo access along with the commands that they have access to
  - Format: username(s)   host=command
    - where username(s) is the list of users or groups, groups are indicated using %group as in %users for all users, or the word ALL
    - host is the hostname which can be localhost, the specific machine’s host, or the word ALL
    - command is the Linux command including any options or parameters that the command needs

sudo: Example

- Let’s imagine that we want all users to have the ability to add groups to the system
  - %users localhost=/usr/sbin/groupadd
    - notice the need for the full path because sudo operates as root and we are not assured that root will have /usr/sbin in its PATH
- Now a user can create a new group through
  - sudo groupadd my_new_group
  - The user is asked to log in using their own password
  - An error message will arise warning the user that this occurrence is being logged if groupadd is not available to this user in the sudoers file

sudo: Discussion

- The sudo command can be very powerful
  - You will want to restrict its usage as you don't want just anyone to have access to root commands
  - One command that users of a workstation might need is shutdown
  - You can also give users access to view files that they might otherwise not have access to
    - %users   localhost=/bin/ls /usr/local/protected
- To edit the sudoers file, use visudo
  - This command launches vi and lets you edit sudoers (only root can edit suoders)
  - This is better than directly editing sudoers in vi because visudo will syntactically check your sudoers file before you exit