System Administration

User Management

UNIX

User Management

- *"A user is any entity that can execute programs or own files."*
  - system user list defined by several files
    - *user list is contained in /etc/passwd*
    - *also involves /etc/group*
      - a user can be a member of multiple groups
    - *(perhaps also /etc/shadow)*
    - *more about these files when we look at security*
  - may like to distinguish between 'normal' user and 'pseudo-users'
    - *UNIX doesn't, however…*
    - *pseudo-users can't login*
      - the password field contains an illegal value
      - root can 'su' to them, however
        - needed for administration purposes
    - *only exist to provide an owner for some system*
      - lp, daemon, ftp, etc.

Password & Group Files

⌘ *(see p.194, Frisch)*

/etc/passwd:
account:password:UID:GID:GECOS:directory:shell

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
bob:x:500:500:Bob Brown,,,,:/home/bob:/bin/tcsh
pcguest:x:502:502::/home/pcguest:/bin/false
```

/etc/group
group_name:passwd:GID:user_list

```
root::0:root
bin::1:root,bin,daemon
daemon::2:root,bin,daemon
sys::3:root,bin,adm
adm::4:root,adm,daemon
tty::5:
disk::6:root
lp::7:daemon,lp
mem::8:
kmem::9:
wheel::10:root
mail::12:mail
news::13:news
uucp::14:uucp
man::15:
games::20:
gopher::30:
dip::40:
ftp::50:
nobody::99:
users::100:bob
floppy:x:19:
bob::500:bob
pcguest:x:502:
guest:x:503:
ppp:x:504:
pppusers:x:230:
popusers:x:231:
slipusers:x:232:
```

Adding A New User

- several steps
  - *(see p.144, Frisch)*
- useradd

```
# useradd -s /bin/tcsh -G ftp,mail,news newnwadmin
```

  - creates a new user with an invalid password
    - *use passwd to give the user a legal one*
  - automates *some of* the work required to add a new user
    - used to have to do everything by hand
      - *vipw needed to control problems with concurrent editing*
    - *uses a number of default settings*
      - as defined in /etc/default/useradd
    - *often need to do lots more site-specific things*
      - register the user with specialized databases, applications, set up a web page for the user, etc.
      - *(see p.174 & p.186, Frisch)*
  - adding a user is often one of the first things that an administrator will automate
  - *(see p.177, Frisch)*

The User Login Environment

- the login shell obtains a number of options from various files
  - default
    - */etc/profile, /etc/csh.cshrc, /etc/bashrc, etc.*
      - the various shells look at these files when they startup but before they look at the user's files
      - sysadmin may want to customize these
  - user
    - *.login, .cshrc, .profile, .xinitrc, etc.*
      - *user's configuration files in their home directories*
    - (see p.165, Frisch)
    - useradd *may populate a new user's home with files from /etc/skel*
      - "The system administrator is responsible for placing the default user files in the /etc/skel directory."
- once a user is set up, it's account should be tested
  - can test with su

```
# su - newuser
```

    - *best to do a complete login, to be 'sure'...*

Removing A User

- **userdel**

```
# userdel -r oldnwadmin
```

- **'undo' the addition procedure's actions**
  - needs care
    - *best to back up the user's files first!*
  - it may never be possible to completely remove a given user from a system
    - *may be associated with locally-developed applications, may need to remain as a mail destination, etc.*
      - leave a disabled entry in the password file
- **the user may have files on the system outside his/her home directory. To find these:**

```
# find / \( -group usergroup -o -user username \) -print
```

- **removing a user is typically the second thing that is automated ;-)**
- **usermod command may be used to modify an account's settings**

Standard Users And Groups

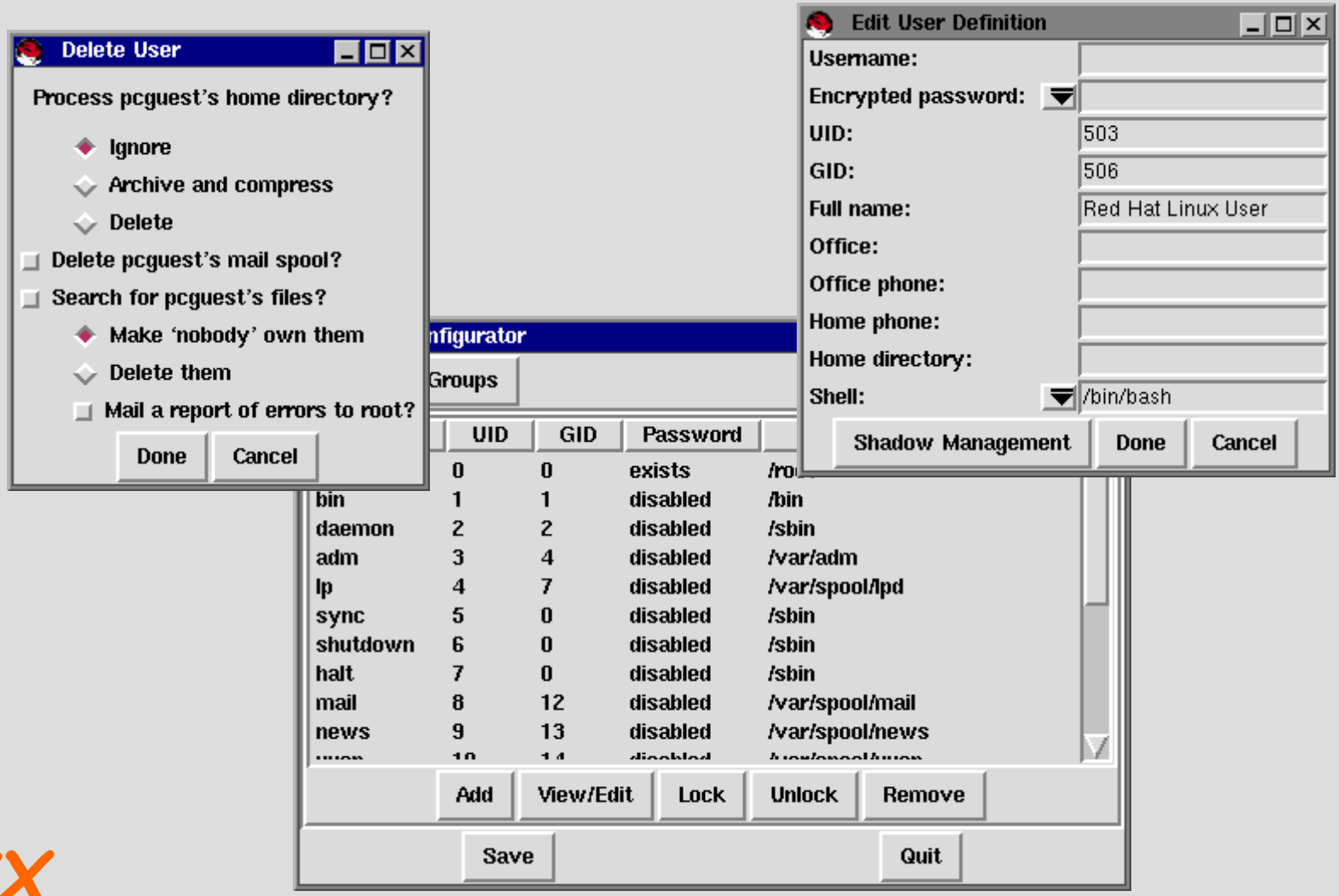
- this is the Redhat list; most systems provide most of these by default
  - most are pseudo-users
    - *can't login; simply support system functionality*
  - most important user is *root* (UID 0, GID 0)
    - *note: the account's **values** are important not the **name***
      - allows duplicate root accounts when a site has multiple administrators
        - potentially possible to track a given administrator's actions...
    - *has no restrictions placed on its activities*
      - maintaining strong security is VITAL for this user!

Group	GID	Members
root	0	root
bin	1	root,bin,daemon
daemon	2	root,bin,daemon
sys	3	root,bin,adm
adm	4	root,adm,daemon
tty	5	
disk	6	root
lp	7	daemon,lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	ftp
nobody	99	
users	100	

User	UID	GID	Home Directory	Shell
root	0	0	/root	/bin/bash
bin	1	1	/bin	
daemon	2	2	/sbin	
adm	3	4	/var/adm	
lp	4	7	/var/spool/lpd	
sync	5	0	/sbin	/bin/sync
shutdown	6	0	/sbin	/sbin/shutdown
halt	7	0	/sbin	/sbin/halt
mail	8	12	/var/spool/mail	
news	9	13	/var/spool/news	
uucp	10	14	/var/spool/uucp	
operator	11	0	/root	/bin/bash
games	12	100	/usr/local/games	
gopher	13	30	/usr/lib/gopher-data	
ftp	14	50	/usr/rhs/ftp	
nobody	99	99	/root	

RedHat's *usercfg* Tool

- in keeping with RedHat's philosophy of making Linux easier to use



sudo

```
# sudo mount /mnt/cdrom
Password:
```

- *(see p.9 Frisch)*
- **free tool downloadable from the internet**
  - *http://www.courtesan.com/sudo/*
  - distributed as source code: allows examination
- **lets a permitted user run commands as another user**
  - allows defined users perform selected superuser activities
    - *administer printers, (un)mount disks, shutdown systems, etc.*
  - don't need to distribute the root password around
    - *sudo only asks for a user's own password for verification*
  - allows a person to be trained one step at a time
    - *first printers, then shutdown; then…*
- **sudo determines who is an authorized user by consulting the file /etc/sudoers**
  - allows for a large amount of configuration
    - *who can do what, on what machine*
- **maintains a log of its activity**
  - via syslog (sysklogd) and/or to a file

Sample /etc/sudoers

```
# User alias specification
User_Alias      FULLTIMERS=millert,mikef,dowdy
User_Alias      PARTTIMERS=bostley,jwfox,mccreary

# Runas alias specification
Runas_Alias     OP=root,operator

# Cmnd alias specification
Cmnd_Alias       DUMPS=/usr/etc/dump,/usr/etc/rdump,/usr/etc/restore,\
                                  /usr/etc/rrestore,/usr/bin/mt
Cmnd_Alias      KILL=/usr/bin/kill
Cmnd_Alias      PRINTING=/usr/etc/lpc,/usr/ucb/lprm
Cmnd_Alias      SHUTDOWN=/usr/etc/shutdown
Cmnd_Alias      HALT=/usr/etc/halt,/usr/etc/fasthalt
Cmnd_Alias      REBOOT=/usr/etc/reboot,/usr/etc/fastboot
Cmnd_Alias      SHELLS=/usr/bin/sh,/usr/bin/csh,/usr/bin/ksh,\
                       /usr/local/bin/tcsh,/usr/ucb/rsh,\
                       /usr/local/bin/zsh
Cmnd_Alias      SU=/usr/bin/su
Cmnd_Alias      VIPW=/usr/etc/vipw,/etc/vipw,/bin/passwd

# Host alias specification
Host_Alias      SUN4=bruno,eclipse,moet,anchor
Host_Alias      SUN3=brazil,columbine
Host_Alias      DECSTATION=wilkinson,soma,dendrite,thang
Host_Alias      DECALPHA=widget,thalamus,foobar
Host_Alias      CSNETS=128.138.243.0,128.138.204.0,128.138.242.0

# User specification
# root and users in group wheel can run anything on any machine as any user
root                            ALL=(ALL) ALL
%wheel                          ALL=(ALL) ALL

# full time sysadmins can run anything on any machine without a password
FULLTIMERS      ALL=NOPASSWD:ALL
# part time sysadmins may run anything except root shells or su
PARTTIMERS      ALL=ALL,!SU,!SHELLS

# rodney may run anything except root shells or su on machines in CSNETS
rodney                          CSNETS=ALL,!SU,!SHELLS

# operator may run maintenance commands and anything in /usr/oper/bin/
operator        ALL=DUMPS,KILL,PRINTING,SHUTDOWN,HALT,REBOOT,/usr/oper/bin/
```