Utenti e gruppi

Utenti e gruppi

- Ogni utilizzatore di UNIX ha associato:
  - Un identità univoca
    - Nomeutente nome alfanumerici
    - UID identità numerica
  - Uno o più gruppi
    - Nomegruppo nome alfanumerico
    - GID identità numerica

Utenti speciali e pseudoutenti

- **root** root è il superutente
- **daemon** per la sicurezza del sistema, i processi che non necessitano di privilegi di root vengono assegnati all'utente daemon
- **sys** utente per la gestione della memoria e del kernel
- **nobody** utente fittizio per gestire i permessi soprattutto in protocolli di rete: nobody non dovrebbe possedere file

Sicurezza

- Gestione utenti e gruppi
- Password utenti
- Permessi dei file
- Controllo accessi locali (in particolare per l'utente root e/o comandi *su, sudo*)
- Gestione servizi di rete (sshd, telnet, sendmail, ftp o web server, etc. etc.)

Sicurezza

- *who* per controllare gli accessi in tempo reale
- *last* per controllare gli ultimi accessi
- *passwd -f* forza cambio password utente al successivo login
- *logins -p* per controllare utenti senza password
- *finger* informazioni sugli utenti
- /var/adm/loginlog file che contiene i login errati (spesso va creato, per esempio con *touch /var/adm/loginlog*)
- /var/adm/sulog file con gli accessi con il comando *su* (si deve vedere anche il file /etc/su per vedere se è messa la riga SULOG=/var/adm/sulog)

Diventare root: *su* & *sudo*

- *su*
  - *su* in realtà permette di sostituire qualunque utente.
    - *su* si chiede di diventare root
    - *su nomeutente* si chiede di diventare l'utente nomeutente
    - Ovviamente verrà richiesta la password
    - *su -* effettua un cambio utente come se si fosse in una shell di login, quindi cambiando anche l'ambiente (shell, PATH, variabili, etc. etc.)
- *sudo* (non su solaris10)
  - Accesso a root limitato per un solo comando
  - /etc/sudoers imposta utenti che possono usare *sudo* e definisce i comandi possibili per ciascuno
  - *visudo* per modificare con accesso esclusivo sudoers

Aggiungere un utente

- Nome
- Password
- Cartella home e shell utente
- Gruppi di appartenenza
- File /etc/passwd
- Password → /etc/shadow
- Permessi della cartella home!
- Skel
- UID e GID

/etc/passwd

```
root:x:0:0:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
smmsp:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
ale:x:100:1::/export/home/ale:/bin/sh
```

- Nome di login
- Password crittografata
- UID
- GID
- Informazioni sull'utente
- Home
- shell

/etc/shadow

(obbligatorio in Solaris)

```
root:irULkDPbhgMfg:6445::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
smmsp:NP:6445::::::
listen:*LK*:::::::
gdm:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
ale:ir0twHl.9AU4M:14385::::::
```

- Nome di login
- Password crittografata
- Data ultima modifica password
- Numero minimo di giorni tra modifiche successive
- Numero massimo di giorni tra modifiche successive
- Giorni di avviso scadenza password
- Giorni massimi di inattività
- Data scadenza account

/etc/group

```
root::0:
other::1:root
bin::2:root,daemon
sys::3:root,bin,adm
adm::4:root,daemon
uucp::5:root
mail::6:root
tty::7:root,adm
lp::8:root,adm
nuucp::9:root
staff::10:
daemon::12:root
sysadmin::14:
smmsp::25:
gdm::50:
webservd::80:
postgres::90:
nobody::60001:
noaccess::60002:
nogroup::65534:
users::100:_
```

- Nome del gruppo
- Password crittografata
- GID
- Elenco membri del gruppo

N.B. Ci sono gruppi vuoti, senza utenti. A cosa possono servire?

Rimuovere un utente

- Rimozione delle righe da passwd e shadow
- Rimozione home
- Rimozione file nelle cartelle temporanee
- Rimozione dei processi di stampa eventuali
- Rimozione degli eventuali processi in crontab
- Terminazione dei processi in esecuzione
- Azzeramento quota disco

Gestire gli utenti

- *useradd* aggiunge un utente
- *userdel* elimina un utente
- *usermod* modifica le proprietà di un utente
- *groupadd* aggiunge un gruppo
- *groupdel* elimina un gruppo
- *groupmod* modifica le proprietà di un gruppo
- *logins* riepilogo utenti

Permessi dei file

- *chown* cambio proprietario
- *chmod* cambio permessi
- *chgrp* cambio gruppo
  - *chown* lavora anche per i gruppi (al posto di *chgrp*)
    - Es*: chown root:users file*
- *Permessi:*
  - *r* lettura (in ottale 4)
  - *w* *scrittura* (in ottale 2)
  - *x* *eseguibile* (in ottale 1)

Permessi dei file

- Due possibili modi di cambiare i permessi:
  - Ottale:
    - *$ chmod 0111 nomefile* → --x--x--x
- Esplicita:
  - *$ chmod a+x nomefile*
  - *$ chmod a-x nomefile*
  - *$ chmod a=x nomefile*

Differenze?

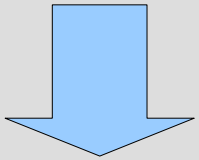
Permessi dei file: *umask*

- *umask* imposta i permessi predefiniti dei file di un utente (per l'esattezza imposta quelli che NON verranno dati)

- *umask nnn*:
  - In genere i permessi di default sono
    - *umask 022* rw-r--r--

Setuid & Setgid

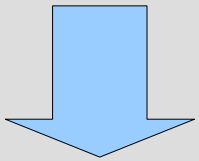
- Esempio pratico: *passwd* deve scrivere sui file /etc/passwd e sui file /etc/shadow che però non possono essere accessibili agli utenti “normali”



- *passwd* quindi ha impostati i permessi setuid e setgid (6555)

Setuid & Setgid

- Quindi il setuid (ed eventualmente il setgid) associano al processo l'identità del proprietario del file (o del gruppo del file) e non dell'utilizzatore del comando (si veda UID E EUID).



- Il processo può avere permessi superiori all'utente, anche se solo limitatamente a quel compito.

Sticky

- Il bit sticky serve a mantenere il processo in memoria anche al termine dell'esecuzione
  - Accesso più rapido
  - Maggior consumo di risorse
- Ormai, vista la quantità di memoria disponibile, è praticamente in disuso

Controllo degli utenti: *who, finger*

- *who opzioni*
  - -b ora dell'ultimo reeboot
  - -H intestazione delle colonne
  - -l terminali di login
  - -m informazioni solo sul terminale corrente
  - -p processi attivi
  - -q risposta breve
  - -r mostra il runlevel
  - -s nome, terminale e dettagli sul tempo di log
  - *who am i* per controllare con quale userid si sta lavorando
- *finger utente*
  - Campi predefiniti:
    - nome utente, nome completo, mome del terminale
    - tempo di inattività e di login
    - Luogo e telefono ufficio

Controllo occupazione degli utenti: *quot*

- *quot opzioni nomeutente*
  - *-a* per tutti i fs montati
  - *-c* Output a 3 colonne con dimensione file, numero file, occupazione totale dei file più piccoli
  - *-f* Per ogni utente mostra il numero dei blocchi, il numero dei file e username

Gestione spazio utenti

- Creare un file quotas nella radice del fs
- *edquota* gestisce il file delle quote per il fs
- *quota* informazioni spazio disponibile
  - *quota -v nomeutente*
- *quotacheck* controllo consistenza quota per ufs
- *quotaon* attiva le quote per un fs
- *quotaoff* disattiva le quote per un fs
- Può essere necessario impostare alcune opzioni in /etc/fstab