

# Utenti

- Il cuore del sistema di gestione degli utenti si trova nei file
    - /etc/passwd
    - /etc/group
    - /etc/shadow
  - Anche altri file sono (più o meno) importanti in questo processo:
    - /etc/skel/
    - /etc/motd
    - ...
- 
-

# */etc/passwd*

- Formato:
    - account:passwd:UID:GID:GECOS:homedir:shell
  - **nome di login, username**
    - storicamente, fino a 8 caratteri.
  - **password** (cifrata)
    - se viene utilizzato shadow, contiene solo una “x”.
  - **UID (User IDentifier):** identificativo dell'utente.
    - su GNU/Linux, solitamente gli UID < 100 sono riservati per gli utenti di sistema.
    - UID ormai a 32 bit.
- 
-

# */etc/passwd*

- **GID (Group IDentifier)**: identificativo del gruppo.
    - il gruppo primario dell'utente.
  - UID 0: utente root
  - GID 0: gruppo root.
  - **GECOS (General Electric Comprehensive Operating System)**
    - Storicamente, le informazioni dell'utente: nome completo, numero di ufficio ed edificio, telefono di ufficio, telefono di casa.
- 
-

# */etc/passwd*

- **homedir**
  - la directory home dell'utente.
- **shell**
  - la shell di login dell'utente. Se vuoto, viene utilizzata quella standard ( /bin/sh ). Se punta ad un programma non esistente, l'utente non potrà avere accesso alla macchina tramite login.

# */etc/group*

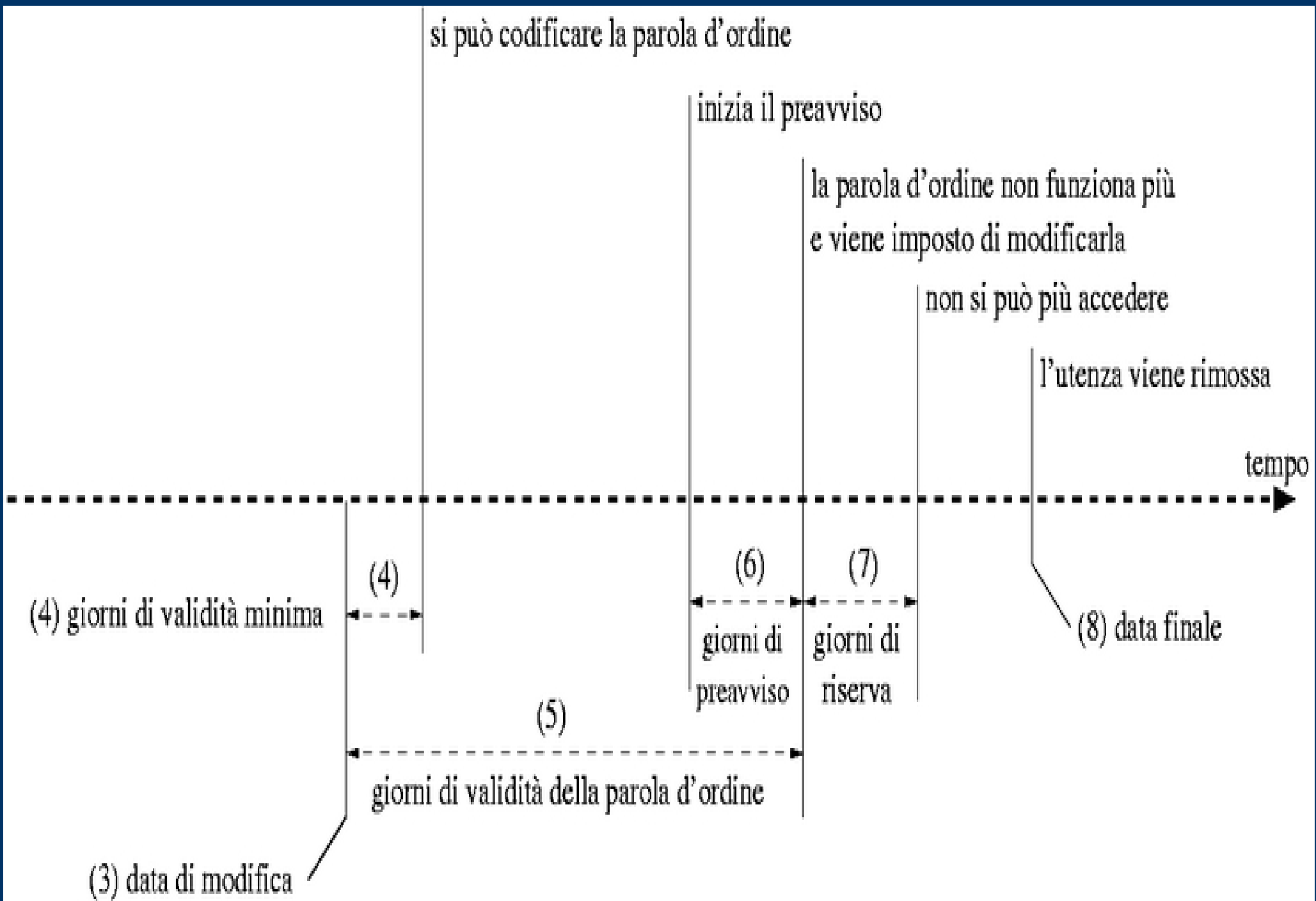
- Formato:
    - group\_name:passwd:GID:user\_list
  - **group\_name**
  - **password**
    - in pratica, mai utilizzata.
  - **GID (Group Identifier)**
    - su GNU/Linux, solitamente i GID < 100 sono riservati per i gruppi di sistema.
  - **user\_list:**
    - lista degli utenti che fanno parte del gruppo
- 
-

# */etc/shadow*

- Presente da tempo in tutte le distribuzioni, contiene le informazioni relative alle password (cifrate) degli utenti, tra cui quelle relative alla loro scadenza (aging). La configurazione globale è in `/etc/login.defs`.
  - Campi:
    - 1.nome di login
    - 2.password cifrata
      - in formato md5
    - 3.data di ultima modifica della password.
      - espressa come il numero di giorni trascorsi a partire dal 1 gennaio 1970.
- 
-

# */etc/shadow*

- 4.giorni prima che la password possa essere modificata
  - 5.giorni dopo i quali la password deve essere modificata.
  - 6.giorni prima della scadenza della password in cui l'utente viene avvertito
  - 7.giorni dopo la scadenza della password in cui l'account viene disabilitato
  - 8.giorni a partire dal 1 gennaio 1970 dopo i quali l'account viene disabilitato.
- Se la password non viene modificata entro il numero di giorni specificato dopo la scadenza della password, l'account viene disabilitato.
- 
-



# *Gestione degli utenti*

- Aggiungere utenti: **useradd**
    - tutti i campi di /etc/passwd possono essere passati come parametri. Se alcuni non sono specificati, vengono inseriti valori di default
    - parametro -m per creare la directory home dell'utente.
  - Aggiungere utenti: **adduser**
    - frontend interattivo per useradd (meno utile per gli script)
  - Modificare utenti: **usermod**
  - Eliminare utenti: **userdel**
    - con -r, sono rimossi i relativi file.
- 
-

# Gestione degli utenti

- Cambio delle informazioni di aging (campi di /etc/shadow):
    - chage
  - Modifica della password:
    - passwd
    - con il parametro -l, l'account viene bloccato (in pratica, inserendo un “!” all'inizio del campo relativo alla password). Si può sbloccare (mantenendo la password) con -u.
    - passwd -S visualizza lo stato dell'account.
    - Attenzione alla scelta della password!
- 
-

# *Gestione degli utenti*

- Quando viene creato un nuovo utente, il contenuto della directory `/etc/skel/` viene copiato (con i permessi appropriati) nella directory personale dell'utente.
- `/etc/motd` contiene il messaggio che viene mostrato agli utenti subito dopo il login.



# *Gestione dei gruppi*

- Aggiungere gruppi: **groupadd**
    - tutti i campi di /etc/group possono essere passati come parametri. Se alcuni non sono specificati, vengono inseriti valori di default.
    - Utile per gli script
  - Aggiungere gruppi: **addgroup**
    - frontend interattivo per groupadd.
  - Modificare gruppi: **groupmod**
  - Eliminare gruppi: **groupdel**
    - non si possono rimuovere gruppi che siano primari per qualche utente.
- 
-

# Quota

- Se il sistema (ed il tipo di filesystem) supporta la quota sui file, è possibile impostare due tipi di limiti, sia sulle dimensioni che sugli inode:
    - un limite logico (o “soft”), superabile temporaneamente durante la sessione di lavoro, ma che blocca l'account se superato a lungo (oltre un tempo di grazia “grace time”).
    - un limite fisico (o “hard”).
  - Limiti separati per ogni partizione (vedi fstab)
    - È importante impostare anche i limiti per gli inode utilizzati, per evitare blocchi del sistema (numero inode è legato al numero dei file...).
- 
-

# Quota

- È possibile impostare la quota per gli utenti (e per i gruppi) tramite il comando `edquota`
    - `edquota nomeutente`
      - apre un editor interattivo per impostare la quota per l'utente `nomeutente`. È possibile cambiare l'editor modificando il valore della variabile d'ambiente `VISUAL`.
    - `edquota -p utentemodello altroutente`
      - imposta la quota dell'utente `altroutente` utilizzando quella di `utentemodello` come modello.
    - `edquota -t`
      - modifica il tempo di grazia, per dimensioni e inode
- 
-

# Comandi vari

- **passwd, chsh, chfn,**
    - permettono di modificare rispettivamente password, shell e GECOS.
  - **quota**
  - **id [nomeutente]**
    - informazioni sull'utente (UID, GID e gruppi).
  - **groups [nomeutente]**
    - i gruppi dell'utente specificato .
  - **last [nomeutente]**
    - informazioni su login/logout.
- 
-

# Shell

- La shell di Linux ( /bin/bash ) prevede due modalità di funzionamento:
    - *non interattiva*; quando viene richiamata con un nome di file come parametro, la shell tenta di eseguirlo come uno script.
    - *interattiva*; viene richiamata direttamente, e presenta all'utente il prompt (contenuto della variabile d'ambiente PS1). Specificando -i, la shell avviata è interattiva.
  - Ulteriore suddivisione (per shell interattive):
    - shell di login
    - shell non di login
- 
-

# Shell

- Shell di login: normalmente invocata quando si conclude la procedura di accesso, o comunque quando viene specificato il parametro `-l`.
- Differenze: i file di configurazione utilizzati.
- Shell di login interattiva: all'avvio, prova ad eseguire i comandi contenuti in
  - `/etc/profile`,
  - `~/.bash_profile`, `~/.bash_login`, e `~/.profile`
- All'uscita, se presente, legge ed esegue il file
  - `~/.bash_logout`

# Shell

- Shell interattiva non di login: vengono letti ed eseguiti (se presenti) i file:
    - /etc/bash.bashrc e ~/.bashrc
  - Shell non interattiva: il nome del file di configurazione viene ricavato dalla variabile d'ambiente BASH\_ENV (storicamente ENV)
  - Quando viene richiamata come /bin/sh, la bash cerca di emulare le vecchie implementazioni di sh, con un occhio verso POSIX.
    - Ad es., in caso di shell non interattiva di login, vengono ignorati i file di configurazione.
- 
-

# *Cambiare utente*

- Cambiare utente: `su`
    - `su [opzioni] [-] [username [argomenti]]`
  - Invocato senza parametri, avvia il processo per diventare superutente (viene richiesta la password). Altrimenti, può specificare un qualsiasi utente.
  - Se viene specificato il `-`, viene avviata una shell di login.
  - Ogni ulteriore parametro viene passato come comando alla nuova shell (che può anche non essere quella di default, con il parametro `-s`)
- 
-

# *sudo*

- Permette di eseguire comandi con i permessi di un altro utente.
  - Configurazione: `/etc/sudoers`, modificabile tramite `visudo` (evita modifiche simultanee).
  - Permette di definire quattro tipi di alias:
    - User\_Alias USERALIAS = utente1, utente2, ...
    - Runas\_Alias RUNASALIAS = utente1, utente2, ...
    - Host\_Alias HOSTALIAS = host1, host2, ...
    - Cmnd\_Alias CMNDALIAS = cmd1, cmd2, ...
- 
-

# *sudo*

- Configurazione del tipo
  - `utente/i macchina/e = [(esegui come)] comando/i`
  - dove
    - `utente/i` può essere un utente, una serie di utenti, un `USERALIAS`, o semplicemente `ALL`;
    - `macchina/e` può essere una macchina, una serie di macchine, un `HOSTALIAS`, o semplicemente `ALL`;
    - `esegui come` può essere un utente, una serie di utenti, un `RUNASALIAS`, o semplicemente `ALL`;
    - `comando/i` può essere un comando, una serie di comandi, un `CMNDALIAS`, o semplicemente `ALL`;
- 
-

# ***PAM (Pluggable Authentication Module)***

- Struttura generalizzata per la gestione dei metodi di autenticazione.
  - Permette di configurare, in base al contesto, la politica di autenticazione.
  - Disponibile da tempo con tutte le distribuzioni GNU/Linux.
  - Le applicazioni devono essere predisposte per utilizzare questo sistema.
  - Moduli localizzati in `/lib/security/pam_*.so`.
- 
-

# ***PAM (Pluggable Authentication Module)***

- Configurazione in `/etc/pam.d/nomeservizio`.
  - Per ogni servizio di autenticazione, viene letto il corrispondente file di configurazione (oppure quello di default, `/etc/pam.d/other`), e richiamati i relativi moduli PAM. A secondo del risultato, l'autenticazione avrà successo o verrà restituito un errore.
  - Vantaggi: permette di impostare condizioni aggiuntive senza toccare i programmi (pluggable...)
- 
-