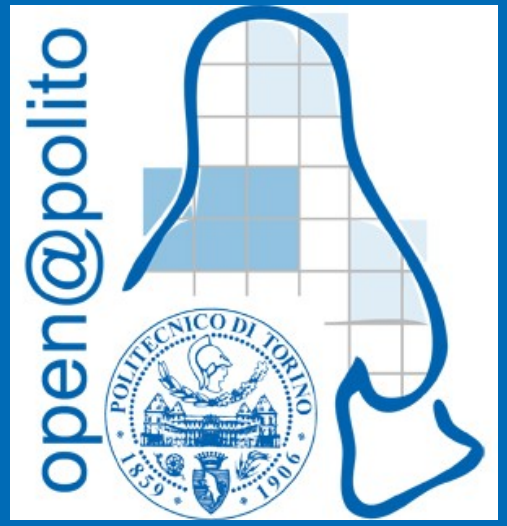
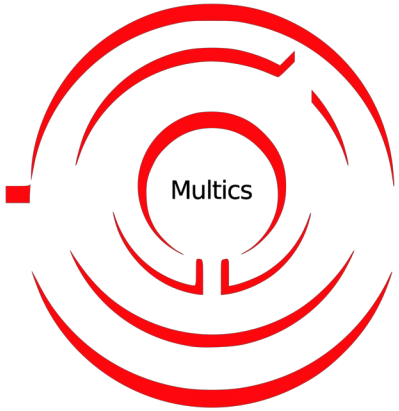
Utenti, gruppi e super-utente

Di Davide Nicolini, Rosario Antoci, Christian Piazzolla e Andrea Artuso

Con il supporto di:



Un po' di storia



Multics (1969)

By VectorVoyager - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=116207801

Terminale IBM 3279 (1979)

By Jonathan Schilling - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=59714790

Mainframe IBM 7090 (~1960)

By NASA Ames Research Center / Emerson Shaw - This image or video was catalogued by Ames Research Center of the United States National Aeronautics and Space Administration (NASA) under Photo ID: ARC-1961-A-28284., Public Domain, https://commons.wikimedia.org/w/index.php?curid=2878809

- Accesso simultaneo al mainframe
- Isolamento delle risorse

Utenti e gruppi in GNU/Linux

Linux eredita la caratteristica di essere **multi-user** da UNIX.

Gli utenti sono un modo per **separare le risorse** e per garantire **maggiore sicurezza** del sistema.

In GNU/Linux la gestione degli utenti è basata sul **Principle of Least Privilege (PoLP)**: ogni utente ha i permessi necessari ad interagire solo con una specifica applicazione/file/dispositivo. Esempio: l'utente `www-data` è l'utente che gestisce i processi legati ai *web server*.

Utenti e gruppi in GNU/Linux

In GNU/Linux esistono 2 tipi di utenti:

1) Utenti **standard** (UID ≥ 1000): sono gli utenti che vengono utilizzati dalle *persone fisiche* che utilizzano il sistema. Sono caratterizzati da:
   - Accesso interattivo alla shell
   - Presenza della home directory
2) Utenti **di sistema** (UID < 1000): sono utenti creati automaticamente dall'OS o da applicazioni installate. Sono caratterizzati da:
   - Non hanno una shell interattiva
   - Non hanno una home directory
   - Permessi specifici solo per eseguire il servizio che gestiscono

Super-utente

In GNU/Linux esiste un utente speciale, l'utente **root**.

Viene creato automaticamente durante l'installazione del sistema ed è l'utente che si occupa di tutti i processi privilegiati del sistema. È caratterizzato dall'UID=0.

L'utilizzo dell'utente root dovrebbe essere limitato alle operazioni che operano su file privilegiati del SO.

Alcune volte è necessario eseguire comandi privilegiati.

Eseguire comandi privilegiati

Per eseguire comandi privilegiati dal nostro utente standard abbiamo 2 possibilità:

su

Il comando su ci permette di impersonare l'utente root.

Aspetto nel terminale:

```
user@hostname: $
```

```
root@hostname: #
```

Dall'utente root, possiamo usare `su <nome utente>` per impersonare un altro utente del sistema.

sudo

Il comando sudo ci permette di eseguire, come utenti standard, un singolo comando in modo privilegiato.

Sintassi:

```
$ sudo comando parametri
```

Per poter usare sudo il nostro utente deve essere nel file dei "sudoers".

Il file /etc/sudoers

Il file /etc/sudoers, chiamato anche “file dei sudoers”, è un file di sistema in cui vengono specificati i permessi che ogni utente ha di eseguire comandi privilegiati.

Per modificare questo file è necessario eseguire il comando `visudo` dall’utente root. Questo comando aprira l’editor predefinito del sistema e creerà una copia modificabile del file /etc/sudoers. Una volta salvate le modifiche il file /etc/sudoers verrà sovrascritto dalla copia creata con visudo.

Il file /etc/sudoers

Ogni riga del file /etc/sudoers ha questo formato:

```
[utente/%gruppo] [host]=([exec_as_user]:[exec_as_group]) [opzioni] [comando]
```

Esempi:

- `%[nome gruppo]` per indicare un gruppo
- `[host]` permessi quando l'utente è connesso in remoto
- `[exec_as_user]:[exec_as_group]` permessi di eseguire comandi come altro utente/gruppo
- `NOPASSWD:` password non richiesta

Eseguire comandi privilegiati: 2 metodi

1) Il primo metodo che ci permette di eseguire comandi privilegiati dal nostro utente standard è quello di aggiungerlo al **gruppo sudo**. Facendo questo il nostro utente potrà eseguire *tutti* i comandi in modo privilegiato.

2) Il secondo metodo è quello di inserire *esplicitamente* l'utente nel file dei sudoers. In questo caso è possibile definire permessi specifici per l'utente, per esempio possiamo permettere solo l'installazione dei pacchetti.

Creazione utente

Per creare un utente possiamo eseguire il seguente comando:

```
$: sudo useradd <nome utente>
```

Questo comando si occupa della creazione dell'utente, dell'assegnazione dei permessi, dell'assegnazione del UID, configurazione della shell, ecc.

Di default però non crea la home directory (/home/<nome utente>). Per farlo è possibile utilizzare l'opzione `-m`. Se si vuole creare una home directory in una posizione diversa da quella di default è possibile usare l'opzione `-d <path>`.

In alternativa è possibile usare uno script Perl denominato `adduser`.

Modifica utente

Per modificare un utente esistente è possibile usare il binario usermod.

Sintassi:

```
$: sudo usermod [opzioni] <utente>
```

Opzioni comuni:

- `-a`: aggiungi l'utente ad un gruppo/i
- `-r`: rimuovi l'utente da un gruppo/i
- `-G`: lista dei gruppi a cui aggiungere l'utente (da usare insieme ad -a)
- `-d`: nuova login directory

Rimozione utente

Per rimuovere un utente è possibile usare il binario userdel.

Sintassi:

```
$: sudo userdel [opzioni] <utente>
```

Opzioni comuni:

- `-f`: forza la rimozione (necessario quando l'utente è ancora loggato o ha dei processi in esecuzione)
- `-r`: rimuove anche tutti i file nella home directory dell'utente

In alternativa è possibile usare uno script Perl denominanto `deluser`.

Cambio password

Per cambiare la password di un utente viene utilizzato il comando `passwd`.

Sintassi:

```
$: sudo passwd [opzioni] <utente>
```

Il comando chiederà di inserire la nuova password dell'utente e di confermarla. Le opzioni del comando permettono anche di far scadere istantaneamente la password dell'utente, di cancellarla, di impostare una data di scadenza, ecc.

È possibile usare il comando `chage` per impostare la data di scadenza della password per un utente o per verificare l'ultimo cambio password.

/etc/passwd e /etc/shadow

Il file /etc/passwd contiene tutti gli utenti presenti nel sistema, uno per riga.

```
utente:x:1021:1020:Nome Cognome:/home/utente:/bin/bash
```

Ogni riga è formata da 7 campi separati da due punti:

1) Nome utente
2) x → la password è crittografata nel file /etc/shadow
3) UID dell'utente
4) GID del gruppo principale dell'utente
5) Nome completo dell'utente
6) Home directory
7) Default shell

[1]

/etc/passwd e /etc/shadow

Il file /etc/shadow contiene le password cifrate di ogni utente, una per riga.

Ogni riga è formata da:

```
utente:$1$bfdnfd$7a9f6e24c4445f05043ff26b78cc0d58: …
```

1) Nome utente
2) Tipo di algoritmo di cifratura
3) Password cifrata + salt
4) Altri parametri

[2]

Visualizzare i gruppi

- **groups** elenca i gruppi di cui l'utente attivo ($USER) fa parte
- **id -gn <username>** mostra il gruppo principale dell'utente
- **groups <nome utente>** indica i gruppi di cui l'utente passato al comando fa parte
- **getent group <nome gruppo>** elenca tutti gli utenti che fanno parte del gruppo indicato
- **getent group** elenca tutti i gruppi esistenti
- **less /etc/group** mostra i contenuti del file /etc/group

Gestire i gruppi

- **groupadd <nome gruppo>** crea un nuovo gruppo
- **usermod -aG <gruppo1>,<gruppo2> <nome utente>** aggiunge l'utente a uno o più gruppi
- **gpasswd -d <nome utente> <gruppo>** rimuove l'utente dal gruppo
- **usermod -g <gruppo> <nome utente>** cambia il gruppo principale dell'utente
- **groupdel <nome gruppo>** elimina il gruppo

Bibliografia

Approfondimenti

[1] https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/

[2] https://www.cyberciti.biz/faq/understanding-etcshadow-file/

Copyleft

Quest'opera, per volonta' degli autori, e' rilasciata sotto la disciplina della seguente licenza

Creative Commons Public License
Attribuzione - Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0)

Tu sei libero:

Condividere — riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare questo materiale con qualsiasi mezzo e formato

Modificare — remixare, trasformare il materiale e basarti su di esso per le tue opere per qualsiasi fine, anche commerciale.

Il licenziante non puo' revocare questi diritti fintanto che tu rispetti i termini della licenza.

Alle seguenti condizioni:

Attribuzione — Devi riconoscere una menzione di paternita' adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare cio' in qualsiasi maniera ragionevole possibile, ma non con modalita' tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.

StessaLicenza — Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

Divieto di restrizioni aggiuntive — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare

Questo e' un riassunto in linguaggio accessibile a tutti del codice legale (la licenza integrale) che e' disponibile alla pagina web:
https://creativecommons.org/licenses/by-sa/4.0/legalcode.it