Corso Di Linux

Liceo Fermi, Bologna - Marcello Galli, novembre 2009

Utenti e Gruppi

Solo con Windows XP, la Microsoft si e' decisa a permettere a piu' utenti di usare il PC, ognuno con le sue configurazioni, ed il suo spazio disco, ottenendo un rudimentale sistema multi-utente. Ma Linux, ed Unix prima di lui, sono **veri** sistemi multi-utente. Con Linux piu' persone possono lavorare contemporaneamente allo stesso computer. Ovviamente il video e la tastiera sono una sola, ma utenti diversi possono essere collegati allo stesso computer via rete, o, nello stesso schermo, ci possono essere finestre diverse che appartengono ad utenti diversi. Questo modo di lavorare e' comune nei server.

In Linux (ed in Unix prima di lui) ci sono tanti utenti. E tanti gruppi di utenti, un utente puo' appartenere a piu' gruppi.

Ogni utente e' identificato da un numero detto uid od User-ID (ID sta per: user identifier). Anche ogni gruppo e' identificato da un numero, detto gid o Group-ID (sta per group identifier).

C'e' un solo utente che puo' fare tutto sulla macchina, e' l'utente di gestione, che si chiama root, gli altri possono solo fare operazioni limitate, definite dalla loro appartenenza ai diversi gruppi. Il meccanismo per le autorizzazioni e' molto semplice, ma funzionale:

- tutte le componenti del computer, files. directory, ed anche le device, come: video, audio, masterizzatore, floppy etc., sono viste come files.
- ad ogni file (sia quelli veri che le devices) e' associato ad un utente e ad un gruppo. Quindi un file appartiene ad un utente, ed un gruppo, suoi proprietari.
- il file ha 3 tipi di permessi per il proprietario (owner): lettura, scrittura, esecuzione. Il permesso di esecuzione vale se il file e' un programma, e permette al proprietario di eseguire il programma. Se il file e' una directory il permesso di esecuzione diventa il permesso di entrare nella directory.
- il file ha 3 tipi di permessi anche per il gruppo cui appartiene,
- il file ha poi 3 tipi di permessi che si applicano a tutti gli altri (others), quelli che non sono ne' il proprietario del file, ne' appartengono al gruppo che possiede il file.

Poniamo ora che si voglia dare possibilita' di usare il CD solo ad alcuni utenti: si fa un gruppo, ad esempio chiamato "cdusers", poi al CD, che e' la device /dev/cdrom, si associa il gruppo "cdusers". Si da alla device il permesso di lettura per il gruppo, ma nessun permesso per gli altri. A questo punto solo gli utenti che appartengono al gruppo cdusers possono usare il CD. Quando si vuole far usare il CD ad un utente lo si mette nel gruppo "cdusers". In questo modo si puo' impedire ad alcuni di sentire la musica, al altri di usare CD e floppy, ed anche di usare video e tastiera. Si puo'fare quello che si vuole, basta fare i gruppi giusti ed assegnare gli utenti ai gruppi.

Il proprietario di un file ne decide i permessi (a parte l'utente root che puo' fare tutto). E decide se gli altri possono leggere i suoi files, scriverci, eseguirli, od entrare nelle sue cartelle.

Ogni distribuzione ha il suo modo di definire i gruppi e gli accessi alle parti del sistema, ma il principio generale e' sempre quello: si fa un gruppo che possiede i files che rappresentano certe risorse e si mettono nel gruppo gli utenti cui si vuole dare accesso. I gruppi sono elencati nel file /etc/group,

gli utenti nel file /etc/passwd. Ci sono comandi appositi per aggiungere o modificare utenti e gruppi, oggi spesso anche comode interfacce grafiche. Si puo' anche andare direttamente a scrivere nei files /etc/passwd ed /etc/group, ma bisogna stare attenti, si rischia di sbagliare qualcosa e qualche utente non riesce piu' ad ad entrare nel computer.

Esisteno in Linux anche altri sistemi per regolare l'accesso alla macchina, piu' precisi. Ad esempio si puo' decidere in che ore si possono fare certe cose, permettere cose diverse a chi usa il computer via rete o a chi si collega dalla tastiera e video etc. Sono un po' come le ACL (access control list) che ci sono in Windows, o che c'erano nei vecchi computers della Digital. Questi sistemi sono pero' piu' complicati da gestire e sono poco usati.

I diversi utenti entrano nel sistema utilizzando una password. hanno una loro cartelle riservata, di loro proprieta', nella directory /home. L'utente root entra anche lui con una password, e la sua cartella riservata e' in /root. Non conviene usare molto l'utente root. Prendetevi la briga di fare tanti utenti nel vostro sistema ed usate il vostro sistema come un utente normale, non come root, che va usato solo per gestire il sistema, e con una certa attenzione.

Un utente normale puo' fare pasticci solo nella sua cartelle, non puo' danneggiare il sistema, ne' le cose degli altri. Root puo' fare tutto, quindi, se fate sbagli quando siete root, potete distruggere il vostro Linux. C'e' stata parecchia gente esperta, che a sera, stanca, ha dato un comando di distruzione files e si e' accorta troppo tardi che era nella cartelle sbagliata .... Unix e' un sistema scarno, non sta tanto a dare avvisi, esegue quello che gli dite senza pieta'. Ma la gente, abituata a windows, essenzialmente mono-utente, tende ad usare anche Linux come root. Questo non va bene, tanto e' vero che certe distribuzioni, per evitare la cosa, hanno disattivato l'utente root, e si deve usare un comando particolare (comando: 'sudo') per fare le operazioni che dovrebbero essere fatte come root.