Gestione degli Utenti e Gruppi in Linux

Samuele Cacchiarelli

6 novembre 2004

Sommario

Appunti della IV lezione del Corso Linux di Base organizzato dal GLM[1]. Negli appunti che seguono, per brevità, non sono riportati i confronti con il sistema Windows che sono stati esposti durante la lezione.

Parte I
Lista degli Utenti e dei Gruppi

La gestione degli utenti e dei gruppi, intesa in senso stretto come creazione e modifica degli stessi, in un sistema Linux è un operazione relativamente semplice e veloce. Può essere svolva in maniera completamente *manuale*, andando ad intervenire su pochi file o direttamente con un semplice editor di testi, o indirettamente attraverso l'ausilio di appositi comandi, testuali o grafici. In questa prima parte mostreremo quali sono i file che sono interessati a tali modifiche. Nella seconda vedremo quali comandi utilizzare per velocizzare le operazioni.

1 Lista degli Utenti

In un sistema Linux la lista degli utenti riconosciuti dal sistema è memorizzata nel file */etc/passwd*. Il sistema consulta tale file al momento del *Login*, per controllare l'esistenza dell'utente che si accinge a loggarsi e verificarne la password.

Ogni riga di questo file rappresenta un Utente ed è divisa in sette campi separati dal carattere ":" . I sette campi contengono le seguenti informazioni:

1. Nome Utente
2. Password criptata[2]
3. Numero dell'utente (UID)
4. Numero del gruppo (GID) principale di appartenza

[1] Da LINUX ADMINISTRATION HANDBOOK di E.Nemeth. G.Snyder, T.R.Hein -2002 Prentice Hall PTR

[2] Negli attuali sistemi Linux, le password criptate degli utenti non vengono più registrate in questo file ma nel file /etc/shadow, che vedremo nel prossimo paragrafo.

5. Informazioni generali separate da virgole, quali Nome completo, Indirizzo, Numero telefonico aziendale e privato (GECOS)

6. Home directory

7. Indicazione della shell predefinita per l'utente

Ad esempio il contenuto di tale file può assomigliare al seguente:

```
root:x:0:0:root,,,:/root:/bin/bash
sam:x:1000:100:Samuele Cacchiarelli,,,:/home/sam:/bin/ksh
```

Possiamo vedere ad esempio che la prima riga si riferisce all'utente root, la cui passwd è "x"[3], il cui numero UID è 0 il GID di appartenenza è 0, il vero nome è root, la sua home directory è /root e infine la sua shell di login è /bin/bash. Non sono indicate informazioni relative a indirizzo e numeri telefonici. La seconda riga si riferisce all'utene sam, il cui vero nome è Samuele Cacchiarelli, la cui home directory è /home/sam e la sua shell di login è /bin/ksh.

Vediamo più in dettaglio i vari campi.

Nome Utente

Il nome utente (o username) deve essere unico e non può avere una lunghezza superiore a 32 caratteri. Può contenere maiuscole o minuscole, ma per ragioni di compatibilità con un eventuale server di posta presente nella macchina (che usualmente non fa distinzione tra maiuscole e minuscole) si consiglia di utilizzare solo username formati da caratteri minuscoli.

Password criptata

Questo campo un tempo conteneva la password criptata dell'utente. Nei sistemi moderni, per motivi di sicurezza, le password degli utenti sono registrate nel file /etc/shadow. Al suo posto, il file /etc/passwd conterrà una semplice "x".

Ogni qualvolta si voglia disabilitare l'accesso di un utente al sistema, è sufficiente sostituire la "x" con un "*". Per consentire l'accesso di un utente senza password, basterà invece cancellare completamente ogni carattere presente (sia x o * o qualsiasi altro carattere).

Da notare come, nonostante si faccia uso del sistema delle shadow password, rimanga possibile inserire a mano in tale campo la password criptata. La presenza della password direttamente su tale file[4], avrà la precedenza su quella eventualmente presente in /etc/shadow, che pertanto verrà ignorata [5].

[3]Nei sistemi Linux che fanno uso del sistema delle shadow password, viene messa, in questo campo, al posto della password criptata dell'utene una semplice "x". La "x" indica al sistema che la vera password criptata dell'utente va ricercata in un ulteriore file chiamato */etc/shadow*.

[4]Ciò non è consigliabile, essendo comunwue il file /etc/passwd leggibile da tutti gli utenti. Con l'ausilio di appositi software infatti, si da in questo modo la possibilità ad utenti locali della macchina di scoprire le password altrui.

[5]Per generare la password a mano e copiarla in tale campo, o nell'equivalente in /etc/shadow si può utilizzare il comando *mkpasswd*.

Numero dell'utente (UID)

L'utente in un sistema Linux è identificato principalmente dal suo UID poi dal nome. Per convenzione all'utente root è assegnato il numero UID 0. È possibile, anche se non consigliabile, assegnare a più utenti il numero UID 0, ciò consentirà agli stessi di essere considerati dal sistema come utenti amministratori alla pari di root. Sempre per convenzione e prassi, agli utenti non di sistema è solito assegnare UID elevati, almeno da 100 in su, ciò eviterà di confondere gli utenti normali dagli utenti di sistema.

Numero del gruppo (GID) principale di appartenza

Ogni utente può appartenere fino a ben 32 gruppi diversi. L'indicazione in questo campo del gruppo di appartenenza principale ha rilevanza soltanto nella creazione di file o directory da parte dell'utente. I nuovi file o directory creati da un utente saranno di proprietà dell'utente stesso e del suo gruppo principale di appartenenza.

GECOS

Costituiscono le informazioni generali dell'utente. Non è necessario che vengano indicate e non è necessario che abbiamo una particolare forma o contentuo. Tuttavia per compatibilità con alcuni programmi come *fuser*, in tale campo vengono registrate quattro strighe separate dalla virgola: la prima indica il nome reale dell'utente, la seconda il suo indirizzo, la terza il numero telefonico dell'ufficio, la quarta il numero telefonico personale.

Home directory

Costituisce la directory personale dell'utente, dove viene a trovarsi lo stesso immediatamente dopo essersi loggato.

Shell di login

Indica la shell di default che viene assegnata all'utente appena loggato.

2 Lista delle Password

Nei sistemi che fanno uso delle shadow password (ormai tutti), l'elenco delle password viene registrato in un file separato leggibile solo dall'utente root, chiamato /etc/shadow. In tal modo si evita che le password seppur criptate vengano liberamente lette da tutti gli utenti del sistema[6].

Anche in questo caso il file contiene in chiaro una serie di righe, ognuna delle quali si riferisce ad un utente presente in /etc/passwd. Più precisamente ogni riga contiene i seguenti 9 campi separati dal carattere ":"

1. Nome utente, indica il nome dell'utente a cui si riferisce
2. Password criptate, contiene la password dell'utente criptata

[6]Il file /etc/passwd infatti per permettere il corretto login al sistema deve essere leggibile da tutti gli utenti.

3. La data dell'ultima modifica della password
4. Il numero minimo di giorni amesso tra un cambio di password e l'altro
5. Il numero massimo di giorni amesso tra un cambio di password e l'altro
6. Il numero di giorni di preavviso di scadenza della password
7. Il numero di giorni consentiti oltre la data di scadenza della password
8. Il giorno di scadenza dell'account[7]
9. Un ulteriore campo rivervato, tuttora generalmente non utilizzato

Di questi campi, quelli necessariamente non vuoti devono essere i primi due, gli altri devono comunque essere presenti anche se vuoti e sempre separati dai ":"

Ad esempio:

```
sam:$1$b1/EEd6W$yuEF/uI2jZ8oM1joatV/x0:::::::
```

Il contenuto di tale file deve essere coerene, quanto meno per ciò che riguarda il numero e l'identificativo degli utenti presenti, con il contenuto del file /etc/passwd. Un utile programma per riconciliare i due file è *pwcon*. Questo comando crea, se non presente, il file /etc/shadow, vi trasferisce eventuali password presenti in /etc/password nell'analogo campo presente in /etc/shadow, cancella le righe di /etc/shadow che non fanno riferimento a utenti presenti in /etc/password (che ricordiamo sono i soli utenti riconosciuti dal sistema) e ne crea di nuove qualora vi sia bisogno.

3 Lista dei Gruppi

Come anticipato, ogni utente può appartenere a ben 32 gruppi diversi. In quanto tale può vantare permessi e diritti di gruppo relativamente ad un file o cartella. Ad esempio un utente che non abbia permessi di lettura su un determinato file di proprietà di un altro, può vantare ugualmente permessi di lettura sullo stesso purchè l'utente faccia parte del gruppo proprietario del file e su tale file siano stati concessi i permessi di lettura per il gruppo.

Anche in questo caso l'elenco dei gruppi presenti nel sistema sono contenuti in un semplice file di testo chiamato */etc/group*. Ogni riga del file identifica un determinato gruppo e contiene le seguenti quattro informazioni separate dal carattere ":"

1. Il nome del gruppo, che può essere anche uguale al nome di un utente (ciò non implica che l'utente debba per forza appartenere al gruppo che reca il suo nome, anche se ciò è conveniente oltre che logico)
2. La password del gruppo, normalmente omessa in quanto non utilizzata dalla maggior parte delle distribuzioni Linux[8].
3. Il Numero del Gruppo (GID)

[7] calcolato come numero di giorni dal 1/1/1970.

[8] La presenza di una password di gruppo è rilevante solo in determinati contesti, ad esempio qualora si utilizzi il comando *newgrp*.

4. I membri del gruppo, costituiti da un elenco di nomi di utenti separati da virgole.

Parte II
Creazione e Gestione di Utenti e Gruppi

La creazione di un utente o di un gruppo consiste essenzialmente nell'inclusione, nei file visti sopra, delle informazioni necessarie. Si può pertanto decidere di effettuare tale operazione completamente a mano con un semplice editor di testi o attraverso l'ausilio di comandi appositi come *useradd*, *groupadd*.

4 Complichiamoci la vita :)

Qualora si decidesse di intervenire a mano sui file /etc/password per creare un utente o modificarne alcune informazioni si consiglia fortemente di utilizzare, specie in una situazione di reale multiutenza, il comando *vipw*.

vipw altro non fa che aprire il file /etc/passwd con il vostro editor preferito (impostato nella variabile EDITOR[9]) e al contempo blocca il file stesso unitamente al file /etc/shadow, impedendo agli altri utenti o amministratori della vostra macchina di apportarvi modifiche. Gli utenti perciò saranno inabilitati, nel frattempo, a modificare la propria password.

La creazione di un utente tramite *vipw* deve poi essere completata quanto meno con la creazione della directory home attraverso il comando *mkdir* e con l'assegnazione della proprietà e del gruppo proprietario, all'utente stesso ed al suo gruppo principale, utilizzando i comandi *chown* e *chmod*.

Ad esempio, per creare l'utente tony con UID 1001, GID 100, volendo intervenire direttamente sul file /etc/passwd, si può seguire i seguenti passaggi:

inserire la seguente riga nel file /etc/passwd

```
tony:*:1001:100::/home/tony:/bin/bash
```

facendo attenzione a che nel file /etc/group esista il gruppo con GID 100, altrimenti va creato inserendovi ad esempio la seguente riga[10]

```
users:x:100:tony
```

La presenza dell'asterisco nel campo della password in /etc/passwd fa si che, l'utenza rimanga disabilitata.

Per assegnare una password all'utente è sufficiente inserirla già criptata[11] nel campo della password al posto dell'asterrisco e successivamente, nel caso si faccia uso delle shadow password, invocare il comando *pwcon* per generare

[9] L'editor di default è *vi* pertanto prima di usare *vipw*, imparate ad usare l'editor *vi* o potreste avere dei problemi ;-)

[10] Analogamente per intervenire direttamente sul file /etc/group per creare, cancellare o modificare un gruppo, si utilizzi il comando *vigr*.

[11] Vedi nota 5 a pag. 2

automaticamente la rispettiva riga in /etc/shadow. Oppure si potrà intervenire, anche in questo caso, direttamente su file /etc/shadow inserendo la riga con nome utente, password criptata e eventualmente le altre opzioni. In questo ultimo caso bisognerà ricordarsi di inserire a mano nel secondo campo del file /etc/passwd una *x*.

A questo punto va creata la home directory dell'utente e vanno assegnati i giusti permessi e attributi con i comandi seguenti:

```
mkdir /home/tony
chown tony.users /home/tony
chmod 700 /home/tony
```

5 Semplifichiamoci la vita

Ovviamente esiste un modo più semplice per creare un utente o gruppo. Ogni distribuzione Linux ha con sè una serie di comandi per una facile e veloce gestione degli utenti. Vediamone alcuni.

Per creare un utente è sufficiente utilizzare il comando *useradd*.

Ad esempio per creare l'utente tony come sopra:

```
useradd -m -u 1001 -g 100 -d /home/tony tony
```

L'opzione *-m* è fortemente consigliata perchè oltre a creare automaticamente la directory home qualora non venga specificata, fa sì che vi vengano copiati i file di configurazione di default per l'utente.
L'opzione *-u* indica il numero di utente che si vuole assegnare all'ultente.
L'opzione *-g* indica il GID (o il nome del gruppo) che si vuole assegnare di default all'utente.
L'opzione *-d* indica la directory home dell'utente.

Per creare un gruppo è invece sufficiente utilizzare il comando *groupadd*.

Ad esempio per creare il gruppo users con GID 100:

```
groupadd -g 100 users
```

Per creare o modificare la password di un utente si può usare il comando *passwd*.

```
passwd tony
```

Per modificare la propria è sufficiente dare il comando *passwd* senza alcun argomento (ovviamente solo root può modificare la password di altri utenti con il comando visto sopra, mentre un utente normale può solo modificare la propria).

Per cancellare un utente o gruppo vi sono poi i rispettivi comandi, *userdel* e *groupdel*.

```
userdel tony
groupdel users
```

Una volta cancellato un utente è bene cancellare anche i file ad esso appartenuti. Un modo veloce per trovarli è dare il comando:

```
find / -nouser
```

il quale restituirà la lista dei file o directory che non risultano appartenere a nessun utente del sistema.

Un ulteriore comando utile per gestire alcune informazioni dell'utente è *chfn*. Tale comando permette di modificare in maniera semplice ed interattiva solo le informazioni presenti nel campo GECOS del file /etc/passwd. Un comando di amministrazione più completo per modificare e rifinire i dati dell'utente è invece *usermod*.

Con *usermod* è possibile modificare praticamente tutto ad esclusione della password: ovvero i dati nel campo GECOS, la home directory la data di scadenza dell'account, il nome utente stesso, i gruppi di appartenenza, il gruppo di default, la shell di default e il numero UID.