Corso GNU/Linux

9 febbraio 2010

<jb007@netstudent.polito.it>

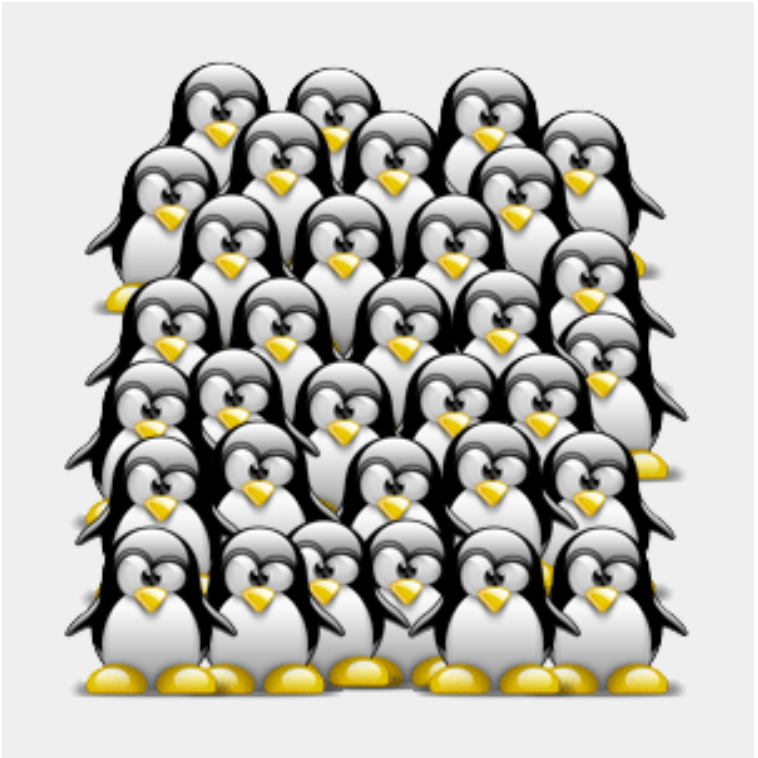
http://netstudent.polito.it

Gestione utenti

Dove osano le password

Della pigrizia e dell'immobilità

Permessi



Gestione utenti

Unix ha permesso, fin dalle prime versioni, ad utenti differenti di operare simultaneamente sul sistema, ed anche **GNU/Linux** è un sistema **multiutente**, pertanto i permessi e le restrizioni dei singoli utenti e dei gruppi sono molto più rigorose che su altri sistemi proprietari per l'utenza domestica e molto simili a quanto codificato per i sistemi di classe enterprise.

In sintesi, **i dati di un utente non sono modificabili e visionabili da altri utenti se non nel caso che questo sia esplicitamente permesso** (ovviamente l'utente root non ha limitazioni).

Gestione utenti

Anche le operazioni che si possono eseguire su di un sistema GNU/Linux sono soggette a questo sistema di permessi, che di fatto rende anche molto più difficile la creazione ed il diffondersi di virus su sistemi GNU/Linux.

Per accedere ad un sistema GNU/Linux, salvo rari casi, è necessario **loggarsi** sul sistema immettendo **username e password**.

Gestione utenti

adduser/useradd: quando viene invocato senza l'opzione **-D**, il comando **useradd** crea un nuovo account di utente usando i valori specificati sulla linea di comando ed i valori predefiniti dal sistema. Il nuovo account di utente verrà aggiunto ai file di sistema che lo necessitano, verrà creata la home directory, e lì verranno copiati i file iniziali, a seconda delle opzioni sulla linea di comando.

Le principali opzioni che si applicano al comando **useradd** sono

-d *home_dir*

Il nuovo utente verrà creato usando *home_dir* come valore per la directory di login dell'utente.

Gestione utenti

-e *data_scadenza*

La data di disattivazione dell’'account dell'utente (*MM/GG/AA)*.

-f *giorni_inattività*

Il numero di giorni dopo la scadenza della password fino a quando l'account verrà permanentemente disabilitato. 0 disabilita l'account immediatamente, mentre -1 disabilita questa caratteristica.

-g *gruppo_iniziale*

Nome o GID del gruppo utente, che deve esistere.

Gestione utenti

segue **adduser/useradd**

-G *gruppo,[...]*

Altri gruppi di cui l'utente è membro. Devono essere immessi separati da virgola, senza spazi.

-s *shell*

Il nome della shell di login dell'utente.

Gestione utenti

-u *uid*

Il valore numerico dell'ID dell'utente. Questo valore deve essere univoco, a meno che non venga usata l'opzione *-o*. Il valore deve essere non-negativo. Il comportamento predefinito è di usare il minimo valore di ID superiore a 999 e superiore a quello di ogni altro utente. Valori tra 0 e 999 sono tipicamente riservati per account di sistema.

File di riferimento:

/etc/passwd - informazioni sugli account di utenti

/etc/default/useradd - informazioni predefinite

/etc/skel - directory contenente i file predefiniti

Gestione utenti

Con l'opzione **-D**, **useradd** mostra i valori predefiniti correnti, ed è possibile modificare tali parametri

-b *home_predefinita*

Il prefisso del percorso per la home directory del nuovo utente. Il nome dell'utente verrà aggiunto alla fine di *home_predefinita* per creare il nome della nuova directory.

-e *data_scadenza_predefinita*

Data di disabilitazione dell’account utente.

Gestione utenti

***-f** inattività_predefinita*

Numero di giorni dopo la scadenza pwd prima della disattivazione account.

***-g** gruppo_predefinito*

Il nome o ID del gruppo iniziale per un nuovo utente.

***-s** shell_predifinita*

Il nome della shell di login per un nuovo utente

*Senza opzioni, **useradd** mostra i valori predefiniti.*

Gestione utenti

chsh: *permette di variare la shell dell'utente*

chsh [-s shell] [-l] [nome_utente]

le uniche shell valide sono quelle elencate nel file **/etc/shell**

Opzioni: -s, --shell -l, --list-shells

Gestione utenti

Usermod: *questo comando permette di modificare l'account di un utente*

Opzioni:

-c *commento:* Il campo commento del nuovo utente nel file password.

-d *home_dir:* nuova directory di login. Con l'opzione -m viene traslato il contenuto dell'home corrente.

-e *data_scadenza:* data di disabilitazione dell'utente.

-f *giorni_inattività:* giorni di inattività prima della disabilitazione dell'account.

Gestione utenti

passwd: *permette di modificare la password di login di un utente*

passwd [utente [password]]

La nuova password deve essere lunga almeno sei caratteri e può essere composta sia da maiuscole che da minuscole o da caratteri non alfabetici. Ovviamente non è possibile usare il nome dell'utente come password.

Nel caso di utilizzo del comando da parte di root, le regole per la password non sono applicate e non viene richiesta preventivamente la vecchia password.

gpasswd: permette di inserire delle password per i gruppi ed amministra i file **/etc/group** ed eventualmente anche **/etc/gshadow**

Gestione utenti

Sintassi:

gpasswd gruppo

gpasswd -a utente gruppo

gpasswd -d utente gruppo

gpasswd -R gruppo

gpasswd -r gruppo

gpasswd [-A utente,...] [-M utente,...] gruppo

Gestione utenti

groupadd: *- Crea un nuovo gruppo*

groupadd [**-g** *gid* [**-o**]] *gruppo*

-g *gid*

valore numerico dell'identificatore (ID) del gruppo. Valori tra 0 e 99 sono tipicamente riservati per account di sistema.

Gestione utenti

groupdel: - Elimina un nuovo gruppo

groupdel *gruppo*

Non è possibile eliminare gruppo primari di utenti esistenti, l'esecuzione del comando non modifica in alcun modo il GID dei file esistenti che dovrà essere variato manualmente.

newgrp: - logga in un nuovo gruppo : questo comando permette di variare il GID di un utente. Condizione necessaria è che l'utente faccia parte del gruppo il cui GID vuole ottenere.

Gestione utenti

Dove osano le password

Della pigrizia e dell'immobilità

Permessi

… le password

/etc/passwd contiene tutto il database degli utenti dei sistema, racchiuso in un normale file di testo. Talvolta viene anche definito come il file delle password, anche se di fatto, con l'introduzione di /etc/shadow tale file non contiene più le password.

1. Username.
2. Password, in forma criptata, oppure x in presenza di /etc/shadow.
3. ID utente numerico.
4. ID del gruppo numerico.
5. Nome completo o descrizione dell'account.
6. Home directory.
7. Shell di login.

… le password

Il file /etc/passwd è leggibile da tutti gli utenti del sistema, in modo da permettere la ricerca di un altro utente, ma questo vuole anche dire che un sistema privo di /etc/shadow conterrebbe in questo file anche le password, seppur in forma criptata.

… le password

/etc/group contiene tutto il database dei gruppi abilitati sul sistema, in forma di file di testo ed ha una struttura dei record molto semplice:

gruppo*:*password*:*GID*:*lista degli utenti

gruppo

Si tratta del nome che identifica il gruppo, assieme al suo GID.

password

Se utilizzata, la password di gruppo sarebbe memorizzata in questo file in forma criptata, e sussistono per questo file tutte le limitazioni presenti in /etc/passwd. L'utilizzo della password di gruppo non è però molto diffuso.

… le password

GID

È il numero identificativo del gruppo: è il valore inserito all'interno di /etc/passwd per indicare il gruppo predefinito di un utente. Un utente può ovviamente appartenere a più gruppi distinti, ma può avere un solo gruppo predefinito.

lista degli utenti

L'insieme di tutti gli utenti di un gruppo.

… le password

Purtroppo la criptazione delle password presente in /etc/passwd, soprattutto in presenza di password deboli, ovvero prive di ragionevoli criteri di sicurezza (troppo corte o banali) può essere decodificata in breve tempo con i sistemi moderni.

Da qua la necessità di memorizzare le password in un altro file, **/etc/shadow**, appunto, leggibile solo da root ed in cui le password sono comunque salvate in forma criptata: nessun amministratore deve poter conoscere le password degli utenti.

Per maggior sicurezza, infine, solo i programmi di autenticazione e di gestione degli possono aver accesso ad /etc/shadow, che ha questa forma:

username:password:lastchange:min:max:warn:inactive:expire:

… le password

username: nome dell'utente.

password: password criptata oppure * (utente disabilitato) e !! (nessuna password).

lastchange: numero di giorni dall'ultima modifica di password (espresso in modo Unix, quindi dal 1 gennaio 1970).

min: giorni minimi prima di poter cambiare la password.

max: durata massima della password (sempre in giorni);

warn: numero di giorni di preavviso per la password.

inactive: numero di giorni di inattività concessi all'utente

expire: data di disabilitazione dell'account.

… le password

E’ importante ricordare che normalmente l’inattività e la “data di scadenza” non vengono impostate di default con i comandi standard di configurazione degli utenti.

Gestione utenti

Dove osano le password

Della pigrizia e dell'immobilità

Permessi

Della pigrizia...

L'utilizzo della shell permette di poter operare in **modalità remota**, ovvero attraverso la la rete esattamente come se si agisse localmente.

In realtà l'accesso remoto è molto più corrente di quello che non si creda nell'utilizzo dei sistemi: è tipico infatti che i server siano dislocati in aree apposite che non sono accessibili normalmente ed amministrati in modalità remota.

Il metodo più utilizzato per accedere a tali macchine era il **telnet**: con questo termine si indica sia il programma di terminale che il protocollo di comunicazione.

Della pigrizia...

Telnet serve per stabilire connessioni con sistemi remoti ed utilizzare la shell, ma ha un grosso limite di sicurezza: ***username e password vengono trasmesse senza criptazione*** *e sono quindi facilmente identificabili.*

Ecco perché è stato creato il **protocollo SSH** che prevede l'utilizzo di una connessione criptata per tutte le procedure di autenticazione e di gestione.

Gestione utenti

Dove osano le password

Della pigrizia e dell'immobilità

Permessi

Permessi

Tutti i file, directory, link, etc sono dotati di permessi

I permessi (o ACL) sono degli attributi che limitano l'accesso degli utenti ai file

Si basano sull'identificazione dell'utente e di gruppi di utenti, e sull'impostazione di privilegi di lettura, scrittura ed esecuzione

Permessi

Ogni utente che accede al sistema e` caratterizzato da un numero uid

Tale numero puo` non essere univoco

Inoltre ogni utente appartiene ad uno o piu` gruppi, indicati con il numero gid

Di solito root ha uid 0

Ogni file appartiene ad un utente e ad un gruppo

Permessi

Il permesso di lettura (r) indica l'accesso in sola lettura del contenuto del file

Il permesso di scrittura (w) permette la modifica e cancellazione del file

Il permesso di esecuzione (x) permette l'esecuzione di un file

Tutti i programmi (anche i comandi base visti) hanno il permesso di esecuzione

Il permesso di esecuzione per una directory si traduce nella possibilita` di accedervi (per esempio con 'cd NOMEDIR')

Permessi

Gli eseguibili non sono quindi caratterizzati dall'estensione ma dal permesso 'x'

I permessi r, w, x, l'utente ed il gruppo di un file possono essere visti con 'ls -l'

Il primo gruppo di 10 caratteri si compone di:

Un carattere che indica il tipo di file, che non puo` essere cambiato (e` deciso alla creazione)

'-' indica file normale, 'd' directory, 'l' un link, 's' socket, ...

Permessi

Tre gruppi di 3 caratteri nella forma 'rwx'

Il primo gruppo si riferisce ai permessi del proprietario (u – user)

Il secondo gruppo indica i permessi del gruppo di appartenenza (g -group)

Il terzo gruppo indica i permessi degli altri utenti e gruppi (o -others)

Se la lettera del permesso e` presente, il privilegio e` concesso, altrimenti e` presente un '-'

Permessi

Segue poi l'indicazione del proprietario del file, la dimension e l'ora di creazione

Per esempio la stringa '-rw-r--r--' indica un file normale che puo` essere letto da tutti e scritto solo dal proprietario

Una directory con permesso di lettura ma non di esecuzione ('drw-rw-rw-') permette a tutti di elencare e modificare i file contenuti, ma non permette di accedervi (per esempio con 'cd')

Permessi

I permessi e proprietari possono essere modificati con tre comandi base

'**chown** NOMEUTENTE NOMEFILE' permette di cambiare il proprietario di un file

Solo root puo` impostare arbitrariamente la proprieta` dei file

Un utente normale non puo` “regalare” un suo file ad un altro utente

'**chgrp** NOMEGRUPPO NOMEFILE' permette di impostare il gruppo del file

Permessi

'**chmod**' permette di cambiare la sequenza di permessi di un file

Ha due modalita` di utilizzo

Tramite indicazione esplicita dei permessi r, w, x per le utenze u, g, o

E` possibile assegnare, togliere o aggiungere permessi per l'utente o gruppo

Esempio 'chmod go-w NOMEFILE'

Nel caso l'utenza sia omessa, si intende tutti e tre (es 'chmod +rw NOMEFILE')

Permessi

Per assegnare esattamente i permessi 'chmod u=rw,go=r NOMEFILE'

La seconda modalita` consiste nel rappresentare la terna rwx su 8 numeri:

0 = ---, 1 = --x, 2 = -w-, 3 = -wx, 4 = r--, 5 = r-x, 6 = rw-, 7 = rwx

Impostare 'chmod 777 NOMEFILE' e` quindi equivalente a permettere qualsiasi operazione a tutti ('rwxrwxrwx')

Permessi

E` poi presente un programma che si occupa di gestire i permessi di default quando si crea un file. '**umask**' senza argomenti riporta la maschera attualmente utilizzata

La maschera e` nel formato numerico di chmod, ma rovesciata

Per esempio 022 indica che una directory verra` creata con permessi 755, ovvero 'rwxr-xr-x'

I file normali, che di default non sono eseguibili, sono normalmente privati di 'x'

Copyleft

Quest'opera, per volontà degli autori, è rilasciata sotto la disciplina della seguente licenza

Creative Commons Public License

Attribuzione-Condividi allo stesso modo 2.5 Italia

Tu sei libero:


di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera


di modificare quest'opera

Alle seguenti condizioni:


Attribuzione. Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.


Condividi allo stesso modo. Se alteri o trasformi quest'opera, o se la usi per crearne un'altra, puoi distribuire l'opera risultante solo con una licenza identica o equivalente a questa.

Ogni volta che usi o distribuisci quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza. In ogni caso, puoi concordare col titolare dei diritti utilizzi di quest'opera non consentiti da questa licenza. Questa licenza lascia impregiudicati i diritti morali. Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

Questo è un riassunto in linguaggio accessibile a tutti del codice legale (la licenza integrale) che è disponibile alla pagina web:

http://creativecommons.org/licenses/by-sa/2.5/it/legalcode

Copyleft

Quest'opera, per volontà degli autori, è rilasciata sotto la disciplina della seguente licenza

Creative Commons Public License

Attribuzione-Condividi allo stesso modo 2.5 Italia

Tu sei libero:


di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera


di modificare quest'opera

Alle seguenti condizioni:


Attribuzione. Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.


Condividi allo stesso modo. Se alteri o trasformi quest'opera, o se la usi per crearne un'altra, puoi distribuire l'opera risultante solo con una licenza identica o equivalente a questa.

Ogni volta che usi o distribuisci quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza. In ogni caso, puoi concordare col titolare dei diritti utilizzi di quest'opera non consentiti da questa licenza. Questa licenza lascia impregiudicati i diritti morali. Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

Questo è un riassunto in linguaggio accessibile a tutti del codice legale (la licenza integrale) che è disponibile alla pagina web:

http://creativecommons.org/licenses/by-sa/2.5/it/legalcode

Copyleft

Quest'opera, è stata realizzata grazie al contributo di molte persone. La prima versione è stata realizzata a partire dalle slide realizzate da Silvio Colloca distribuite con licenza Creative Commons sul sito http://linuxhelp.it. Successivamente sono state modificate dai molti docenti che hanno prestato il loro servizio gratuito nelle lezioni dei corsi Netstudent. In ordine sparso (e sperando di non dimenticare nessuno): Giovanni Berton Giachetti, Daniele Lussana, Alessandro Ugo, Emmanuel Richiardone, Andrea Garzena, Stefano Cotta Ramusino, Roberto Preziusi, Marco Papa Manzillo, Puria Nafisi Azizi, Luca Necchi, Luca Barbato, David Putzer, Alberto Grimaldi, Nicola Tuveri, Stefano Colazzo, Laura De Martini, Luca Bruno, ecc...