Shutdown

E' importante seguire le procedure corrette quando si spenge un sistema Linux. Se non lo fate, il filesystem probabilmente si corromperà e i file diventeranno illeggibili.

Questo perché Linux utilizza una cache su disco, che non scrive sul disco tutto insieme, ma solo ad intervalli; un comportamento del genere migliora moltissimo la performance, ma sta anche a significare che se spengete semplicemente il computer d'improvviso la cache può contenere molti dati, e quello che si trova sul disco può non essere un filesystem che funziona perfettamente

Un'altra ragione per non spengere direttamente l'interruttore è che in un sistema multitasking ci possono essere molti processi attivi in background. Usando la corretta sequenza di shutdown vi assicurate che tutti i processi in background possano salvare i propri dati.

Il comando per spengere correttamente un sistema Linux è *shutdown*. Normalmente può essere usato in due modi.

Shutdown

Se vi trovate su un sistema dove siete l'unico utente, il modo normale di usare *shutdown* è uscire da tutti i programmi, scollegarsi da tutte le console virtuali, collegarsi come root su una di esse, passare nella directory root per evitare problemi nell'unmount dei filesystem e

dare il comando

> shutdown -h now

Se il vostro sistema ha molti utenti, usate il comando

> shutdown –h +tempo messaggio,

dove tempo è il tempo in minuti prima che il sistema venga fermato, e message è una breve spiegazione del perché il sistema viene spento.

L'avviso viene visualizzato su tutti i terminali su cui c'è un utente collegato e viene ripetuto automaticamente alcune volte prima dello spegnimento, ad intervalli sempre più brevi.

Quando comincia il vero shutdown viene fatto l'unmount di tutti i filesystem (eccetto quello di root), i processi utente (se qualcuno è ancora collegato) vengono uccisi, ed i demoni vengono fermati

Shutdown

Fare il reboot significa avviare di nuovo il sistema, e si può ottenere facendo shutdown, togliendo la corrente e poi rimettendola. Un metodo più semplice è usare l'opzione -r di shutdown, ad esempio dando il comando

> shutdown -r now.

La maggior parte dei sistemi Linux fanno shutdown -r now quando si preme *ctrl-alt-canc* sulla tastiera, in modo da riavviare il sistema. L'azione di ctrl-alt-canc è però configurabile, e spesso è preferibile inserire un ritardo in sistemi multiutente.

Per sistemi accessibili a chiunque si può configurare *ctrl-alt-canc* in modo che non abbia nessun uso

Init e runlevel

Un runlevel è uno stato di init e dell'intero sistema che definisce quali servizi del sistema sono operativi. I runlevel sono identificati da numeri. Non c'è un parere comune per come usare i runlevel definiti a livello utente (dal 2 al 5): alcuni amministratori di sistema usano i runlevel per definire quali sottosistemi funzionano, cioè se gira X, se la rete è operativa e così via. Altri hanno tutti i sottosistemi che girano sempre, o li avviano e li fermano individualmente senza cambiare runlevel, perché i runlevel sono uno strumento troppo grezzo per controllare il sistema. Potete decidere da voi, ma può essere più semplice seguire come fa la vostra distribuzione di Linux.

0	Ferma il sistema
1	Modalita' utente singolo
2-5	Definiti dall'utente
6	Reboot

Single user mode

Un runlevel importante è la modalità utente singolo (runlevel 1), in cui solo l'amministratore di sistema usa la macchina e girano il minor numero possibile di servizi di sistema.

La modalità a utente singolo è necessaria per portare avanti dei compiti di amministrazione

Gli script di avvio che init usa faranno entrare automaticamente in modalità utente singolo se fsck automatico al boot fallisce, in modo da evitare che il sistema usi un filesystem talmente rovinato da non poter essere riparato da fsck.

I servizi associati ai runlevel sono definiti nel file /etc/inittab

Login nel dettaglio

Login si occupa di autenticare l'utente e di inizializzare la shell.

Parte della configurazione iniziale consiste nel mandare in output il contenuto del file /etc/motd (message of the day") e controllare la posta elettronica.

Queste fasi possono essere disabilitate creando il file .hushlogin nella home directory dell'utente.

Se esiste il file /etc/nologin, i login sono disabilitati. Un file del genere viene di solito creato da shutdown e da comandi simili. login controlla la presenza di questo file, e se esiste non accetterà i login. Se esiste, login manderà in output il suo contenuto al terminale prima di uscire.

login tiene un log di tutti i tentativi di login falliti in un file di log di sistema (usando syslog). Tiene anche un log di tutti i login di root; entrambi possono essere utili per rintracciare gli intrusi

Login in dettaglio

Gli utenti collegati al momento sono elencati in /var/run/utmp; questo file è valido solo fino al prossimo reboot o shutdown del sistema, ed elenca ogni utente ed il terminale (o la connessione di rete) che sta usando, oltre ad altre informazioni utili.

I comandi ***who, w*** e simili usano utmp per vedere chi è collegato.

Tutti i login che hanno avuto successo sono registrati in /var/log/wtmp. Questo file crescerà senza limite, quindi deve essere ripulito regolarmente, ad esempio usando un job di cron settimanale.Le buone distribuzioni di Linux lo fanno senza dover configurare niente. Il comando last legge wtmp.

Sia utmp che wtmp sono in formato binario (consultate la pagina man di utmp); non conviene esaminarli senza usare programmi speciali.

La shell

Dopo l'autenticazione di login, all'utente viene presentato il prompt della shell

Alla partenza la maggior parte delle shell eseguono prima un file globale di configurazione e poi uno specifico per l'utente che esegue il login.

Generalmente il primo e' /etc/profile il secondo .profile nella home dell'utente; mentre il file globale serve all'amministratore di sistema per assegnare un ambiente comune di lavoro (PATH), quello specifico permette agli utenti di personalizzare il proprio ambiente.

Il controllo degli accessi

Tradizionalmente il database degli utenti e' tenuto nel file /etc/passwd.

Il database degli utenti non contiene soltanto le password criptate, ma anche altre informazioni sugli utenti, come il loro vero nome, le home directory e le shell di login (es. csh,tcsh,bash).

Il database dei gruppi degli utenti viene tenuto in /etc/group

La gestione degli account

Il file /etc/passwd ha una linea per ogni nome utente, e viene diviso in sette campi delimitati da due punti:

Username:Passwd:UID:GID:Dati:Home:Shell

Username ' è il nome di login

Password è la parola d'ordine cifrata. Se questa indicazione manca, l'utente puo' accedere al sistema senza indicare alcuna parola d'ordine.Se questo campo contiene un asterisco (*) l'utente non puo' accedere al sistema.

Dati contiene, ad es., l'indicazione del nominativo completo dell'utente (nome e cognome)

Home definisce la directory assegnata all'utente.

Shell definisce il tipo di shell assegnata all'utente

La gestione degli account

Esempio
rossi:724AD9dGbG25k:100:502:M. Rossi:/home/rossi:/bin/bash

L'utente **'rossi**' corrisponde al numero UID 100 e al numero GID 502; si chiama M. Rossi; la sua directory personale è '/home/rossi'; la sua shell è '/bin/bash'.

Di questo utente non si conosce niente altro che il nome e il cognome.

La gestione degli account

Qualsiasi utente sul sistema può leggere il file delle password, in modo da poter, ad esempio, sapere il nome di un altro utente.

Ciò significa che anche la password (il secondo campo) è disponibile per tutti.

Il file delle password contiene le password in forma criptata, quindi in teoria non ci sono problemi; comunque, la criptazione può essere decodificata, specialmente se le password sono deboli (brevi o che si trovano nel dizionario

Molti sistemi Linux usano le shadow password: un modo alternativo per tenere le password, che vengono immagazzinate criptate in un file separato, /etc/shadow, leggibile solo da root.

Il file /etc/passwd contiene solo un indicatore speciale nel secondo campo.

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Il file /etc/group contiene l'elenco dei gruppi di utenti.
La struttura delle righe di questo file è molto semplice.

gruppo:*parola_d'ordine_cifrata*:*GID*:*lista_di_utenti*

***gruppo*: è** il nome utilizzato per identificare il gruppo.

***parola_d'ordine*:** Di solito non viene utilizzata e di conseguenza non viene inserita. Se è presente una parola d'ordine, questa dovrebbe essere richiesta quando un utente tenta di cambiare gruppo attraverso **'newgr**p'.

***GID*: è** il numero identificativo del gruppo.

***lista_di_utenti*:** elenco di nomi di utente separati da virgole.

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Esempi

tizio::502:tizio

Si tratta di un caso molto semplice in cui il gruppo **'tizi**o' non ha alcuna parola d'ordine e ad esso appartiene solo un utente omonimo ('**tizi**o' appunto).

users::100:tizio,caio,sempronio

In questo caso, gli utenti **'tizi**o', **'cai**o' e **'sempron**io' appartengono al gruppo **'user**s'.

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Alcune versioni di Linux hanno dei comandi per aggiungere un utente (adduser o simili)

Per creare invece a mano un account occorre seguire questi passaggi:

Modificate il file /etc/passwd con *vipw* e aggiungete una nuova linea per il nuovo account.

vipw blocca il file, in modo che altri comandi non provino a modificarlo nello stesso tempo. Il campo della password dovrebbe essere impostato a (*)', in modo che sia impossibile collegarsi.

Nello stesso modo, modificate /etc/group con *vigr*, se dovete anche creare un nuovo gruppo.

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Create la home directory dell'utente con *mkdir e* copiate i file da /etc/skel nella nuova home directory.

Aggiustate l'owner e i permessi con *chown* e *chmod*:
l'opzione -R (discesa ricorsiva) è utilissima in questo caso

Impostate la password con *passwd*.

Dopo aver impostato la password nell'ultimo passaggio, l'account sarà funzionante. Non dovreste impostarla finché non avete fatto tutto il resto, altrimenti l'utente si potrebbe collegare inavvertitamente mentre state ancora copiando i file.

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Modifica delle proprietà degli utenti

Ci sono alcuni comandi per modificare le varie proprietà di un account (cioè il campo relativo in /etc/passwd):

chfn Cambia il campo del nome completo.
chsh Cambia la shell di login.
passwd Cambia la password.
Il superutente può usare questi comandi per cambiare le proprietà di qualsiasi account; gli utenti normali possono modificare solo quelle del proprio.

Altri compiti vanno fatti a mano; ad esempio, per modificare il nome dell'utente va modificato /etc/passwd direttamente (ricordatevi, con vipw); ugualmente, per aggiungere o togliere l'utente da altri gruppi va modificato /etc/group (con vigr).

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Rimozione di un utente
Per rimuovere un utente prima vanno rimossi tutti i suoi file, i file e gli alias della posta, i job di stampa, di cron e at, e tutti i riferimenti all'utente.

Poi si rimuovono le linee rilevanti dai file /etc/passwd e /etc/group (ricordatevi di rimuovere l'utente da tutti i gruppi di cui faceva parte). Può essere una buona idea disabilitare prima l'account (vedi sotto), prima di cominciare a rimuovere tutto, per evitare che l'utente usi l'account mentre lo state rimuovendo.

Ricordate che gli utenti possono avere dei file al di fuori della home directory. Li potete trovare con il comando *find*:
find / -user username

Alcune distribuzioni di Linux hanno dei comandi speciali per farlo: cercate *deluser* o *userdel*; ma è facile anche farlo a mano, e i comandi possono non fare tutto.

Dipartimento di Informatica e Scienze dell'Informazione

La gestione degli account

Disabilitazione temporanea di un utente
Talvolta è necessario disabilitare temporaneamente un account, senza rimuoverlo. Ad esempio, l'utente può non aver pagato l'abbonamento.

Il modo migliore di disabilitare un account è cambiare la shell con un programma speciale che stampa solamente un messaggio. Così, chiunque provi a collegarsi nell'account non ci riuscirà e saprà il perché. Il messaggio può dire all'utente di contattare l'amministratore in modo da risolvere qualsiasi problema.

Sarebbe anche possibile cambiare lo username o la password in qualcos'altro, ma allora l'utente non saprebbe cosa sta succedendo. Un modo semplice di creare il programma speciale è scrivere degli `script tail':

#!/usr/bin/tail +2
Questo account è stato chiuso per un problema di sicurezza.
Chiamate il 555-1234