

Sistemi Linux

Corso di Informatica Forense - OIG
Facoltà di Giurisprudenza
Università degli studi di Bologna

dr. Stefano Fratepietro

m@il: fratepietro@cirsfid.unibo.it
skype: stefano.fratepietro



CIRSFID



stevolab.net



Contenuti

- Storia di Linux
- Distribuzioni
- Live cd Linux
- Struttura del file system
- Principali caratteristiche
- Principali locazioni dati

Storia I

- Linux nasce nel 1991 da un' idea di Linus Torvalds
- Linux non è altro che un kernel "unix-like" creato da zero
- Nel 1994, con la presentazione "al mondo" della versione 1.0, nascono Red Hat e Suse, aziende leader nel settore delle distribuzioni commerciali
- Nel 1996 viene rilasciata la versione 2.0 con notevoli passi avanti in termini di prestazioni e supporti hardware



Storia II

- Nel 1999 viene rilasciata la versione 2.2
- Nel 2001 viene rilasciata la versione 2.4 con notevoli passi avanti in termini di prestazioni e supporti hardware
- Nel 2005 viene rilasciata la versione 2.6, prima versione del kernel con supporti e miglioramenti per l'utilizzo del sistema lato utente





Contenuti

- Storia di Linux
- **Distribuzioni**
- Live cd Linux
- Struttura del file system
- Principali caratteristiche
- Principali locazioni dati



Distribuzioni I

- Una distribuzione Linux è una distribuzione software che include un kernel Linux e un insieme variabile di altri strumenti e applicazioni software, siano esse freeware, open source o commerciali.
- Le distribuzioni sono distribuite gratuitamente (Licenza GPL)
- Esistono distribuzioni a pagamento, in questo caso non si paga il software ma servizi correlati alla distribuzione fornita



Distribuzioni II

- Ogni distribuzione mira a raggiungere determinati obiettivi e a soddisfare una parte delle esigenze informatiche
 - Distribuzioni lato user (Ubuntu, Mandrake)
 - Distribuzioni lato server (Debian, Suse, Red Hat)
 - Distribuzioni ibride (Knoppix, Gentoo)



Distribuzioni III

- Non esiste uno standard nell'organizzazione delle directory
- Può capitare che a seconda della distribuzione possa cambiare la locazione dei file e delle directory di configurazione e o addirittura il nome con cui esse sono chiamate



Distribuzioni IV

Esempio: file di configurazione della rete

- in Debian è in `/etc/network/interfaces`
- in Red Hat è in `/etc/sysconfig/network`



Contenuti

- Storia di Linux
- Distribuzioni
- **Live cd Linux**
- Struttura del file system
- Principali caratteristiche
- Principali locazioni dati



Live cd Linux I

- Un Live CD è un CD-ROM (anche dvd) contenente un sistema operativo in grado di essere avviato ed eseguito senza doverlo installare su un hard disk
- Si utilizza per scopi dimostrativi, didattici o **per avere a disposizione un sistema operativo completo da usare su un computer altrui**



Live cd Linux II

- Tutti i dati vengono caricati nella memoria volatile (RAM) del sistema dove vengono eseguite tutte le operazioni ove vi è necessità di memorizzare dati
- Le unità di memoria non volatile (hard disk, dispositivi esterni di memoria) non vengono per alcun motivo alterate a meno che non vi sia la volontà dell'utente



Live cd Linux III



Ne parleremo più avanti



Contenuti

- Storia di Linux
- Distribuzioni
- Live cd Linux
- **Struttura del file system**
- Principali caratteristiche
- Principali locazioni dati



File system Linux I

- I sistemi Unix oriented (Linux, BSD e similari) hanno a disposizione un'ampia gamma di tipi di file system da poter utilizzare indipendentemente dal tipo di distribuzione usata, unica limitazione consiste nelle versioni di kernel obsolete.
- In alcuni casi è possibile l'utilizzo di file system sviluppati per altri sistemi operativi
(ad esempio Windows)



File system Linux II

- Nei sistemi Unix un inode è una struttura dati sul file system che archivia le informazioni base dei file, delle cartelle o di qualsiasi altro oggetto. Le informazioni includono:
 - la dimensione del file e la sua locazione fisica (se risiede su un dispositivo a blocchi come, ad es., un hard disk)
 - il proprietario e il gruppo di appartenenza
 - le informazioni temporali di creazione, modifica e ultimo accesso



File system Linux III

- Ogni inode ha associato un numero univoco all'interno del dispositivo e ogni file presente è identificato come un link hardware all'inode tramite il suo numero
- Il sistema operativo, quando un programma cerca di accedere ad un file tramite un nome (es. documento.txt), cerca l'inode corrispondente e recupera tutte le informazioni sopra descritte per operare correttamente con il file



File system Linux IV

Principali caratteristiche di un file system Linux sono:

- superblock: contiene informazioni sulla partizione come il numero di blocchi complessivo, il numero di inode, il numero di blocchi liberi, un'indicazione di quando è avvenuta l'ultima verifica della struttura, etc. L'informazione contenuta nel superblock è così importante che viene duplicata in varie zone del disco in modo che possa più facilmente essere recuperata in caso di errore



File system Linux V

- block bitmap: tabella in cui ad ogni bit è associato un blocco di dati. Lo stato del bit indica se il relativo blocco è libero o allocato ad un file
- inode bitmap: tabella in cui ciascun bit è associato ad un "inode". Lo stato del bit indica se il corrispondente inode è libero o in uso



File system Linux VI

- Ogni dispositivo a blocchi formattato, viene visto come una raccolta di inode, ciascuno con un numero che lo individua all'interno di quel dispositivo. Ogni inode contiene:
 - Tipo del file: File, directory ecc...



File system Linux VII

- Codice gruppo proprietario (group), numero che individua un gruppo di utenti, lo si trova in `/etc/group`
- Permessi `rwx` per l'user, gruppo e altri: illustrano se un processo appartenente a quell'user o a quel gruppo può leggere/scrivere/ eseguire il file
- Data di ultimo accesso all'inode, modifica dell'inode, modifica del file



Contenuti

- Storia di Linux
- Distribuzioni
- Live cd Linux
- Struttura del file system
- **Principali caratteristiche**
- Principali locazioni dati



Principali caratteristiche I

- architetture a 32 e 64 bit
- multi piattaforma: supporto per architetture diverse da quelle x86
- multitasking: più programmi funzionano contemporaneamente
- multiuser: più utenti nella stessa macchina contemporaneamente
- protezione della memoria tra processi, in modo che un programma non possa mandare in crash l'intero sistema



Principali caratteristiche II

- memoria virtuale con paginazione su disco: in una partizione separata o in un file del filesystem o in entrambi, con la possibilità di aggiungere nuove aree durante il funzionamento (sono chiamate aree di swap)
- demand loads eecutables: Linux legge dal disco solo le parti di un programma che sono attualmente usate
- console virtuali multiple: sessioni di login indipendenti attraverso la console, scambiabili premendo una combinazione di tasti dedicati
- supporto per quasi tutti i file system



Principali caratteristiche III

- Un programma in esecuzione si chiama processo
- Un processo ha un user-id e un group-id che sono quelli dell'utente che lo ha lanciato e un process-id (pid) univoco
- Ogni file e directory hanno un user-id, un group-id (che sono quelli del loro proprietario) e un insieme di diritti
- I diritti di un file/directory regolano indipendentemente la possibilità per i processi di leggere, scrivere e eseguire/consultare il file/directory in base all'uguaglianza o meno degli user-id e dei group-id del processo e del file



Assegnazione dei permessi

- I permessi vengono identificati nel seguente modo:
 - lettura definito dal flag r che tradotto in numero assume il valore 4
 - scrittura definito dal flag w che tradotto in numero assume il valore 2
 - esecuzione definito dal flag x che tradotto in numero assume il valore 1
 - nessun permesso che tradotto in numero assume il valore 0

Esempio: `chmod 755 nomefile`

- 7 -> lettura scrittura esecuzione al proprietario
- 5 -> lettura esecuzione al gruppo
- 5 -> lettura esecuzione agli altri utenti



Gestione delle memorie di massa I

- All'interno della directory `/dev` sono presenti diversi file speciali chiamati file di device che si comportano in modo diverso dai file normali
- Questo tipo di file sono un'interfaccia per i driver (che fanno parte del kernel Linux) che si occupano del reale accesso all'hardware



Gestione delle memorie di massa II

- null: rende nullo un output
- zero: device virtuale con tutti i bit settati a zero
- fd0: Primo lettore di dischetti
- fd1: Secondo lettore di dischetti
- hda: Disco fisso o lettore CD IDE presente sulla prima porta IDE (Master)
- hdb: Disco fisso o lettore CD IDE presente sulla prima porta IDE (Slave)
- hdc: Disco fisso o lettore CD IDE presente sulla seconda porta IDE (Master)
- hdd: Disco fisso o lettore CD IDE presente sulla seconda porta IDE (Slave)



Gestione delle memorie di massa III

- hda1: Prima partizione del primo disco fisso IDE
- hdd15: Quindicesima partizione del primo disco fisso IDE
- sda: Il disco fisso SCSI con l'ID SCSI più basso (p.e. 0)
- sdb: Il disco fisso SCSI con l'ID SCSI successivo (p.e. 1)
- sdc: Il disco fisso SCSI con l'ID SCSI ulteriore (p.e. 2)
- sda1: Prima partizione del primo disco fisso SCSI
- sdd10: Decima partizione del primo disco fisso SCSI
- sr0: Il lettore CD SCSI con l'ID SCSI più basso
- sr1: Il lettore CD SCSI con l'ID SCSI successivo
- ttyS0: Porta seriale 0, COM1 sotto MS-DOS
- ttyS1: Porta seriale 1, COM2 sotto MS-DOS



Contenuti

- Storia di Linux
- Distribuzioni
- Live cd Linux
- Struttura del file system
- Principali caratteristiche
- **Principali locazioni dati**



Principali locazioni dati

- /: radice del sistema
- /bin: programmi "di base" del sistema (mkdir ad esempio è qui)
- /home: profili utente e tutti i file dei profili dei software
- /lib: librerie di sistema
- /media: usato per gestire le periferiche esterne in automatico
- /proc: informazioni dettagliate sul sistema in tempo reale
- /usr: librerie, eseguibili e documentazione
- /var: log, file di lavoro del sistema
- /sbin: file essenziali per permettere l'avvio e il recupero del sistema
- /etc: file di configurazione del sistema - *.conf



Struttura albero del FS



