

Corso di Informatica Forense

Facoltà di Giurisprudenza – Operatore informatico giuridico

File system

Argomenti trattati

- Introduzione al file system
- File system Windows
- File system Linux/Unix
- File system Mac

Introduzione al file system

Un file system è l'insieme dei tipi di dati astratti necessari per la memorizzazione, l'organizzazione gerarchica, la manipolazione, la navigazione, l'accesso e la lettura dei dati

- memorizzazione: allocazione di un dato nel fs
- organizzazione: allocazione in un determinato settore del dato
- manipolazione: alterazione e modifica del dato
- navigazione: “sfogliare” il fs
- accesso i/o: accesso ai file memorizzati

Introduzione al file system

I file system tipicamente hanno tabelle che associano i nomi dei file con i file, collegando il nome di un file ad un indice in una tabella di allocazione (file allocation table) dove è specificato l'indirizzo di allocazione del file in memoria.

Compito del file system è quello di semplificare la complessità di utilizzo dei diversi “media” creando una interfaccia per i sistemi di memorizzazione.

Introduzione al file system

I file system generalmente usano dispositivi di archiviazione che offrono l'accesso ad un array di blocchi di dimensione fissa, generalmente in settori di 512 byte l'uno.

Il file system è responsabile dell'organizzazione di questi settori e tiene traccia di quali settori appartengono a quali file, e quali invece non sono utilizzati.

Introduzione al file system

Dal punto di vista dell'utente un file system è composto da due elementi:

- File: una collezione di informazioni correlate composte da
 - Nome: Stringa di caratteri che identifica un file nel file system
 - Tipo: Associazione di un file ad un software per la sua lettura/utilizzo (non in tutti i sistemi operativi)
 - Locazione e dimensioni: Dimensioni e posizionamento del file all'interno del file system
 - Data ed ora: Informazioni relative alla data della creazione del file e alla sua ultima modifica
- Directory: un insieme di informazioni per organizzare e fornire informazioni su file che compongono il file system (armadio di file)

Introduzione al file system

Un disco fisico può essere composto da più partizioni che a loro volta possono essere formate da diversi tipi di file system

- Il primo settore del disco è il master boot record (MBR) ed è utilizzato per fare il boot del sistema.
 - Contiene la partition table (tabella delle partizioni)
 - Contiene l'indicazione delle partizioni attive
- Ogni partizione inizia con un boot block
- Il MBR carica il boot block della partizione attiva e lo esegue

Introduzione al file system

Generalmente il file system è composto da:

- Superblock: Contiene informazioni sul tipo di file system
- Tabelle per la gestione dello spazio libero
- Tabelle per la gestione dello spazio occupato (non su tutti i FS)
- Root directory: Directory radice del file system (/)
- File e directory

Introduzione al file system

File system più diffusi:

- Amiga File Systems - OFS, FFS1 e 2, International, PFS, SFS usati su Amiga
- BFS - il Be File System usato su BeOS
- DFS , ADFS - file system della Acorn
- EFS (IRIX) - un vecchio file system a blocchi usato su IRIX
- Ext2 - Extended filesystem 2, diffuso su sistemi GNU Linux
- Ext3 - Extended filesystem 3, diffuso su sistemi GNU Linux (ext2+journaling)
- FAT - Usato su DOS, Microsoft Windows e su molti dispositivi dedicati, dispone di tabelle a 12 e 16 bit
- FAT32 - versione con tabelle a 32 bit di FAT
- FFS - Fast File System, usato in vecchi sistemi BSD
- HFS - Hierarchal File system, usato su vecchie versioni di Mac OS
- HFS+ - Hierarchal File system Plus, usato sulle versioni recenti di Mac OS e su Mac OS X
- HPFS - High Performance File system, usato su OS/2

Introduzione al file system

File system più diffusi:

- ISO 9660 - Usato su dischi CD-ROM e DVD-ROM (anche con estensioni Rock Ridge e Joliet)
- JFS - Journaling File system, disponibile su sistemi GNU Linux, OS/2, e AIX
- LFS - Log-structured file system
- Minix - Usato su sistemi Minix
- NTFS - Usato su sistemi basati su Windows NT
- ReiserFS – File system journaling, diffuso su sistemi GNU Linux
- UDF - File system a pacchetti usato su supporti WORM/RW, CD-RW e DVD
- UFS - Unix File system, usato su vecchi sistemi BSD
- UFS2 - Unix File system, usato su nuovi sistemi BSD
- UMSDOS - file system FAT esteso con permessi e metadata, usato su GNU Linux
- XFS - Usato su sistemi IRIX, ottimo file system per Linux (consigliato)

Introduzione al file system

Esempi di file system di rete sono:

- AFS (Andrew File System)
- AppleShare
- CIFS (conosciuto anche come SMB o Samba)
- Coda
- GFS
- InterMezzo
- Lustre
- NFS

Introduzione al file system

Tipi di file:

- MS-Dos: Massimo 8 caratteri per il nome del file e massimo 3 per l'estensione
- Windows 9x e derivati da tecnologia NT: Nomi ed estensioni di lunghezza variabile con associazione dell'estensione del file al relativo software che permette la lettura/esecuzione del file
- Linux, Unix e Mac OS X: Nomi di lunghezza variabile, manca completamente il concetto di estensione del file.

(Vedremo nel dettaglio prossimamente)

Introduzione al file system

Problema:

Ogni volta che avviene una modifica sui file, il file system corregge le proprie tabelle che rappresentano lo stato dei file stessi: nome, lunghezza, posizione, privilegi di sicurezza ecc... nel momento in cui avviene una improvvisa interruzione di corrente o un crash di sistema, può verificarsi anche una discrepanza tra lo stato dei nostri file e le relative tabelle di descrizione che non riflettono più l'ultima "fotografia" del disco: il blocco improvviso del sistema ha bloccato anche l'ultimo aggiornamento delle tabelle di descrizione.

Introduzione al file system

Problema:

Al reboot, il file system deve controllare tutto il disco e deve fare del suo meglio per correggere le tabelle di descrizione in modo da sincronizzarle con lo stato reale dei nostri file. Se i dischi sono grandi e se ci sono molti file, questa operazione può richiedere molto tempo, e inoltre non è detto che sia sempre accurata!

Introduzione al file system

Soluzione

Per aiutare questa fase di ripristino dell'operatività è stato implementato il **journaling**: si tratta di una sorta di diario delle operazioni, un vero log delle operazioni in corso. Prima il file system scrive nel log quello che vuole fare, poi lo fa, ed in fine cancella il log

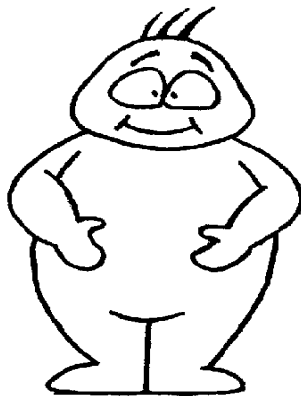
Pro:

- niente più attese al reboot
- vengono minimizzati i possibili guai ai nostri file

Contro:

- leggero degrado delle prestazioni

File system FAT



File system FAT

La struttura del file system classico dei sistemi DOS, che permane anche nei sistemi Windows 95/98/NT/Xp (Windows NT supporta anche un diverso tipo di file system chiamato NTFS) viene chiamata FAT dal nome della sua componente principale. La FAT32 costituisce una variante a 32 bit introdotta con la release B di Windows 95 per consentire la gestione di partizioni di dimensioni maggiori di 2 Gbytes.

File system FAT

Le principali caratteristiche sono:

- FAT: File Allocation Table --> Tabella di allocazione dei blocchi
- Root directory: La directory di livello gerarchico più elevato
- Sotto directory: Le directory di livello inferiore alla radice.
- Clusters: blocchi che contengono i dati dei file

File system FAT

Gli elementi della FAT sono di lunghezza fissa, pari a 16 bit, non è possibile indirizzare più di 65535 cluster e poiché un cluster non può essere maggiore di 32768 byte, il file system ha un limite massimo superiore di 2 Gbyte per la dimensione della partizione.

Soluzione!

Una delle novità della release B del sistema operativo Windows 95, fu quella dell'introduzione della nuova versione a 32 bit della FAT (FAT32) che sostanzialmente mantiene la stessa struttura, ma utilizza elementi a 32 bit, anziché a 16, consentendo di definire cluster non superiori a 4 Kbyte anche per dischi di grandi dimensioni.

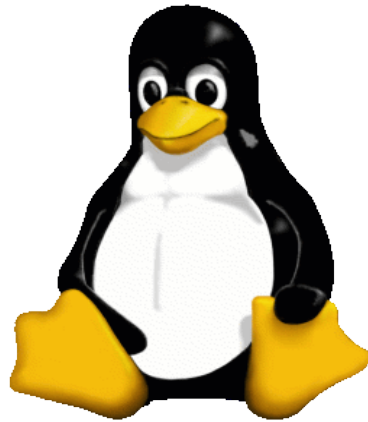
(Scoperta dell'acqua calda!!!)

File system FAT

L'albero del file system FAT di una partizione, ad esempio c:/ (dove c sta per il nome della partizione), è composto da una root directory “/” dove sono contenute tutti i file e le directory del sistema.

I file vitali del sistema operativo sono contenuti nella cartella Windows di default (fortunatamente durante l'installazione è possibile scegliere il nome della directory) mentre i file dei software installati generalmente sono contenuti nella directory Programmi (Program Files). Documenti e file utente sono contenuti nella cartella “Documents and settings” (solo nelle versioni sviluppate con tecnologia NT)

File system Linux/Unix



File system Linux/Unix

I sistemi Unix oriented (Linux, BSD e simili) hanno a disposizione un'ampia gamma di tipi di file system da poter utilizzare indipendentemente dalla versione della 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/Unix

L'inode contiene tutte le informazioni relative ad un file e quelle necessarie a reperire i dati effettivamente contenuti nel file. E' il tramite per l'accesso ai dati di ciascun file memorizzati nei "data blocks". Ogni inode contiene una tabella di 15 puntatori, i primi 12 sono i puntatori "diretti", ciascuno di essi contiene l'indirizzo di un blocco di dati appartenente al file, dal tredicesimo puntatore in poi, troviamo i puntatori indiretti di primo,secondo e terzo livello ovvero essi puntano ad un altro blocco di puntatori, ciascuno dei quali a sua volta contiene l'indirizzo di un blocco di dati.

La sua struttura è tale da conciliare due esigenze opposte:

- Garantire un accesso veloce ai dati
- Consentire la gestione di file di dimensioni variabili

File system Linux/Unix

Le principali caratteristiche di un file system per sistemi Linux/Unix sono:

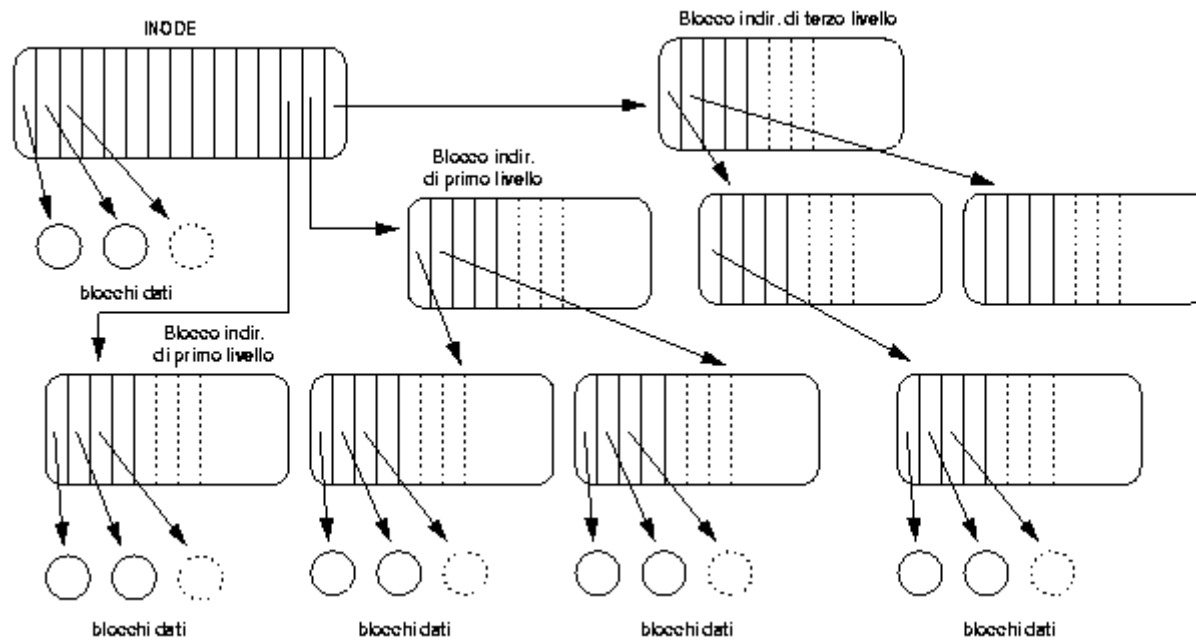
- **superblock:** contiene informazioni sulla partizione come il numero di blocchi complessivo, il numero di inode, il numero di blocchi liberi, un'indicazione di quando è avvenuta l'ultima verifica della struttura, etc. L'informazione contenuta nel superblock è così importante che viene duplicata in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

Le principali caratteristiche di un file system per sistemi Linux/Unix sono:

- **inode table:** Ogni elemento di questa tabella corrisponde ad un singolo file.
- **data blocks:** la porzione di disco dove sono effettivamente memorizzati i dati. Ogni blocco di dati (blocco logico) ha una dimensione multipla della dimensione del blocco fisico secondo una potenza di due. La dimensione del blocco logico viene stabilita al momento della formattazione. Allo scopo di ottimizzare l'allocazione dello spazio disco il file system è in grado di gestire "frammenti" di blocco nella parte finale del file, ovvero ogni file è costituito da 0 o più blocchi logici e da un frammento finale.
- **directory:** tabella che associa nomi arbitrari agli inode.

File system Linux/Unix



File system Linux/Unix

Ogni dispositivo a blocchi formattato, viene visto come una raccolta di inode, ciascuno con un numero che lo individua all'interno di quel dispositivo.

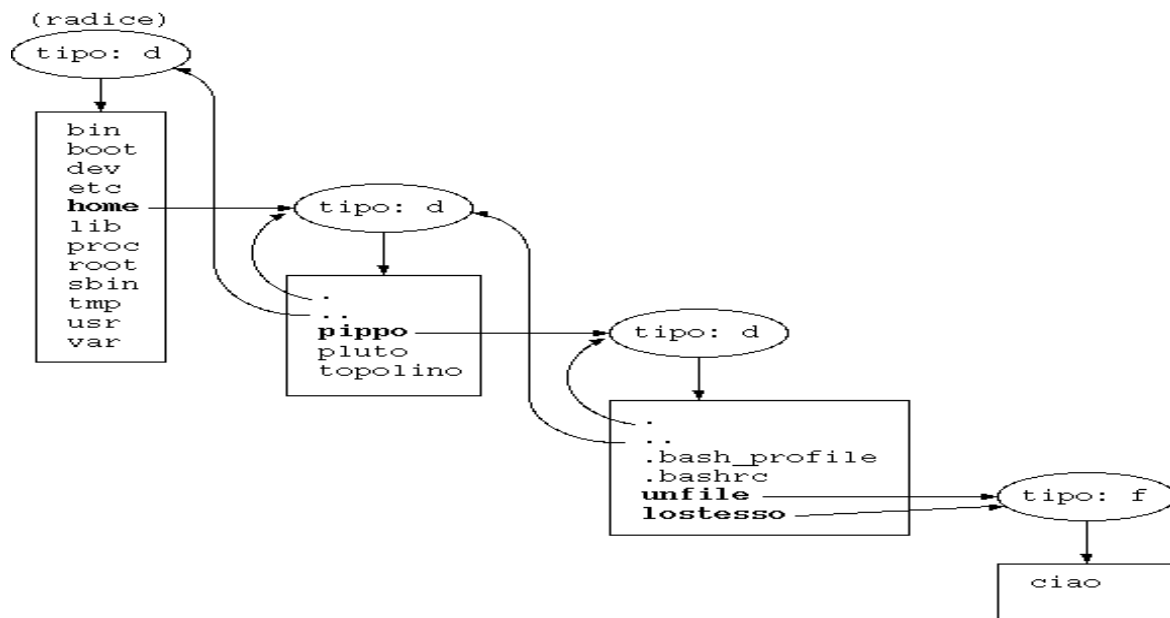
Ogni inode contiene questi dati:

- **Tipo del file:** File, directory ecc...
- **Codice utente** proprietario (user), numero che individua un utente, lo si trova in /etc/passwd
- **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 che può leggere/scrivere/eseguire il file.
- **Data** di ultimo accesso all'inode, modifica dell'inode, modifica del file

File system Linux/Unix

Ogni inode contiene questi dati:

- **Numero di link a questo inode:** Numero di directory che contengono l'inode e di processi che lo stanno usando. Quando questo numero scende a zero, il file viene cancellato in modo irrecuperabile dal sistema
- **Lunghezza del file in byte:** la lunghezza max dipende dal tipo di formattazione.
- **Tabella dei blocchi del file:** elenco dei blocchi che compongono il file.



File system Linux/Unix

Il file nei sistemi unix/linux è una struttura che si apre con una testa e una coda contenente dei meta dati quali:

- Payload (contenuto del file)
- Proprietario (UID)
- Gruppo (GID)
- Data creazione
- Data dell'ultima modifica

File system Mac



Link di riferimento

- <http://it.wikipedia.org>
- <http://it.tldp.org/HOWTO/Filesystems/>
- <http://www.macosx.it/>
- <http://www.google.it>
- <http://www.stevelab.net/steve>

DOMANDE?

