Informatica

Quando a morire è l'hard disk

di Nicola Bortolotti

È un evento traumatico che spesso offre qualche indizio: i sintomi preoccupanti possono consistere in rumori strani, soprattutto all'accensione, episodiche perdite di dati che si manifestano con errori inspiegabili, un improvviso spegnimento del motore (e, magari, subitanea riaccensione) durante il normale funzionamento, un rallentamento delle operazioni di scrittura.

Nella maggior parte dei casi, tuttavia, quando si hanno le prime avvisaglie è già troppo tardi per intervenire e, in un numero non raro di casi, il decesso – anche di esemplari con poche ore di vita – avviene di colpo, senza alcun avvertimento.

Di malattie che si manifestino in modo così silente, insidioso e pernicioso la medicina, per fortuna, non ne annovera molte. Questo *modus moriendi*, invece, rappresenta la norma per uno dei componenti essenziali di una qualsiasi computer: il disco rigido, ossia “hard disk”, più spesso tradotto come “disco fisso” anche se – a rigore – tale componente è sempre più spesso rimovibile e trasportabile.

Dove sono custoditi i dati

Sebbene, in senso stretto, un calcolatore elettronico non abbia bisogno della cosiddetta “memoria di massa” per il suo funzionamento – fatta eccezione per una memoria a sola lettura che contenga il sistema operativo – salvo particolarissimi casi e applicazioni (PC ad uso industriale, ad esempio, o dispositivi elettronici “dedicati” di uso sempre più comune) è ovviamente improponibile pensare a un Personal Computer (o – peggio – a un server, che spesso è deputato a fare solo quello!) sul quale non sia possibile memorizzare nulla, ossia che “perda” tutti i dati sui quali si sta lavorando al suo spegnimento. La memoria di lavoro di un computer (la RAM) è infatti, per sua natura, velocissima ma “volatile”, ossia non sopravvive alla mancanza di alimentazione; per contro la “memoria di massa” (hard disk, USB pen drive, memory card, nastri magnetici, CD/DVD e così via) ha tempi di accesso enormemente più elevati (quantunque quasi inavvertibili per un normale utilizzatore, salvo utilizzi intensivi) ma può serbare le informazioni intatte per

vi) ma può serbare le informazioni intatte per periodi di tempo elevatissimi, che – nel caso dei nastri magnetici correttamente conservati – può anche raggiungere i decenni.

Gli hard disk, che oggi offrono comunemente e a bassissimo costo quantità davvero cospicue di dati memorizzabili, dell'ordine di diversi Terabyte (pari a mille miliardi di “caratteri”), hanno un funzionamento mirabilmente raffinato e delicato, e ruotano incessantemente a velocità che, allo stato attuale, vanno dai 5.400 (sui portatili) ai 15.000 (sui server) giri al minuto. I dischi rigidi sono, di norma, moderatamente resistenti agli urti soltanto quando sono spenti e le testine automaticamente “parcheeggiate” (una procedura essenziale e critica che, una volta, doveva essere decisa dall'utente alla fine del lavoro); diventano, invece, assai vulnerabili alle sollecitazioni meccaniche durante il funzionamento, specie in fase di lettura e scrittura e di accensione e spegnimento. Soffrono, inoltre, le temperature elevate. Un periodo delicato della loro vita è costituito dalle prime ore di funzionamento (il cosiddetto “burn in”, il momento della “bruciatura” nel quale si verifica – cosa tipica per i dispositivi elettronici – una frequenza anomala di malfunzionamenti), superate le quali si può ragionevolmente ritenere che – prescindendo da eventi “traumatici” e surriscaldamenti – la vita del disco potrà statisticamente procedere senza troppe “scosse”.

Parametri che possono fuorviare

Ma quanto può valere la vita di un hard disk? Un dato che veniva usualmente riportato nelle “specifiche tecniche” è il cosiddetto MTBF (Mean Time Between Failures, tempo medio tra guasti), che è di norma superiore a 500.000 ore ed è un indicatore sovente male interpretato, tanto che alcuni costruttori – anche tra i più noti – oggi preferiscono non indicarlo più, privilegiando altri parametri meno equivocabili. MTBF, infatti, non indica l'aspettativa di vita media di un singolo disco (in tal caso si potrebbe fare affidamento su un hard disk moderno per 57 anni!) ma deve sempre

essere valutato assieme al “tempo di servizio” dichiarato dal costruttore o – laddove non specificato – al tempo di “garanzia limitata”. MTBF è infatti valutato – entro il “*service life*” – su un grande numero di hard disk dello stesso tipo e rappresenta il numero medio di ore totali di funzionamento (sommando quelle di *tutti i dischi*, non di uno singolo!) prima che si sia manifestato il guasto di *uno di loro*. Da ciò discende che, effettivamente, è lecito attendersi che un HD con MTBF di un milione di ore sia più affidabile di uno con 500.000 ore, ma sarebbe gravissimo errore aspettarsi una vita utile anche solo di 100.000 ore.

Un parametro ben più realistico, rilevante e inquietante è il numero di “load/unload cycles” dichiarato dai costruttori, in genere variante da alcune decine ad alcune centinaia di migliaia di cicli. Tale numero rappresenta – grossolanamente – il numero minimo di attivazioni delle testine (non di accensioni e spegnimenti dell’hard disk) garantite. Si pensi al fatto che, anche solo scrivendo un documento senza salvarlo (pratica censurabile), il numero di load/unload cycles (invisibili all’utente) può facilmente raggiungere il centinaio in un’ora. In tal modo il numero di cicli “garantiti” può essere esaurito in un anno di vita, il che, ovviamente, non implica il fatto che dopo un anno il guasto sia quasi assicurato, ma ridimensiona non di poco le aspettative di affidabilità nei confronti di questo preziosissimo componente del computer, unico depositario della memoria (e del lavoro) di chi lo utilizza.

Obbligo di Legge

È bene ricordare che, nel caso un professionista o un’azienda tratti dati personali (ed è quasi impossibile che ciò non avvenga), l’esigenza di prevenire la perdita delle informazioni memorizzate non è solo consigliabile ma rappresenta un vero e proprio obbligo, sancito dalla Legge 196/2003. Le strategie utilizzabili a tal fine sono molteplici ma, sostanzialmente, si possono così sintetizzare: l’effettuazione regolare di copie di backup dei dati, da conservare in luoghi sicuri, e l’utilizzo di particolari configurazioni di più dischi rigidi in grado di supplire al guasto di uno di essi senza perdita di informazioni.

Questa ultima tecnologia, che i bassissimi costi attuali dell’hardware suggeriscono di adottare anche a livello domestico e personale, è racchiusa nell’acronimo RAID (Redundant Array of Inexpensive Disks, oggi reinterpretato in Independent, ossia insieme ridondante di dischi indipendenti). Nella sua forma più semplice, detta RAID1 (implementabile a costo zero, a parte quello del disco aggiuntivo, in tutte le schede madri moderne), è sinonimo del cosiddetto “mirroring”, e consiste nell’installare due dischi identici che sono gestiti automaticamente in modo da contenere in ogni momento gli stessi dati; tale coppia viene percepita come un unicum dall’utilizzatore: qualora se ne guasti uno, l’altro continua a funzionare dando il tempo di

fare un backup e rimpiazzare l’hard disk guasto, sul quale verrà “specchiato” nuovamente l’intero contenuto dell’altro.

L’aumento di affidabilità conseguente al mirroring è eccezionale, a fronte di un costo risibile. A tale tecnologia, per ovvie ragioni di spazio e consumi, si è obbligati a rinunciare solo nei computer portatili, ma è del tutto privo di significato, nelle altre tipologie di prodotti, rinunciare alla tranquillità del RAID1 in favore di un risparmio minimo, dell’ordine dei 50 euro nel caso di un PC ad uso domestico o workstation per Office Automation.

Non a caso, nel numero 1-2009 di questa rivista, si indicavano delle soluzioni software gratuite per realizzare dei “NAS – Network Attached Storage”, sostanzialmente dei file server dedicati, dotati di funzionalità RAID1 e 5.

Quando l’hard disk muore

Ma cosa fare quando un hard disk muore?

Qualora non si sia in precedenza agito “con la cura del buon padre di famiglia” il disco potrebbe contenere dati preziosi. In tal caso si può tentare un recupero, pur consapevoli che si tratta di impresa pressoché disperata. Se il guasto è realmente meccanico le strategie possono andare dalla rozza (ma, con i modelli del passato, sovente efficace) “sculacciata” alla partenza e successivo backup tombale fino allo spegnimento definitivo, alla installazione su interfaccia (anche un adattatore esterno) molto più lenta, fino al tentativo di recupero dei dati in “camera bianca” (senza polvere), ad opera di aziende specializzate e costosissime, che si rivela – tuttavia – quasi sempre inutile. Nel caso di perdita dei dati per problemi non (o non esclusivamente) hardware, la via migliore è il recupero mediante una distribuzione Linux “live” su CD come SystemRescueCD, un ausilio gratuito e quasi insostituibile per i tecnici, in grado di riportare in pochi minuti alla salute partizioni corrotte Windows (e non solo), comprese quelle che utilizzano il file system NTFS, o di consentire l’accesso via rete a supporti difettosi.

Un aspetto quasi sempre sottovalutato dopo la dipartita di un disco (ma anche dopo la semplice dismissione di un PC obsoleto), tuttavia, è la necessità di distruggerlo prima dello smaltimento, soprattutto qualora esso contenga dati sensibili.

Tale operazione, formalmente equivalente al passare documenti al trituratore, è diventata un poco visibile obbligo di Legge (la citata 196/2003) ma viene sovente dimenticata, in particolare quando viene smaltito un hard disk guasto.

La domanda, infatti, è: che senso ha distruggere un hard disk se è guasto? Se il disco è in salute si può avere la falsa illusione che sia sufficiente “formattarlo” per eliminare le informazioni ivi contenute, mentre occorrerebbero operazioni ben più lente e critiche (il

cosiddetto “wiping”) per rendere impossibile il recupero da parte di eventuali malintenzionati ipertecnologici. Ma se il disco addirittura è inutilizzabile, la necessità di distruggerlo (o custodirlo in luogo protetto) sembra una beffa che si aggiunga al danno; eppure, poiché la probabilità di recuperare qualcosa non è rigorosamente nulla, in presenza di dati sensibili è bene seguire protocolli di smaltimento simili a quelli utilizzati da sempre dalle autorità militari. Come fare, dunque?

Come “triturare” un disco

Un metodo speditivo ed efficace, anche e soprattutto per hard disk in salute, che potrebbero facilmente cadere nelle mani sbagliate, è la distruzione fisica della memoria mediante smagnetizzazione. È ovvio che il servirsi di appositi e costosissimi strumenti (come, ad esempio, i “degausser” di tipo professionale come quello al link <http://www.ontrackdatarecovery.it/degausser/>) è del tutto fuori luogo. Una strada percorribile, quindi, può essere quella di aprire l’hard disk (operazione che, se eseguita in un ambiente normalmente polveroso, di per sé potrebbe danneggiarlo) e avvicinare moltissimo ai “piatti”, fin quasi a toccarli, un potente magnete permanente. Si noti che ripetute prove hanno dimostrato che effettuare una tale operazione su un disco sigillato non sortisce alcun effetto, in quanto, per superare l’effetto schermante dell’involucro metallico e la distanza, occorrono campi magnetici molto intensi, quali quelli prodotti dai citati degausser. A smagnetizzazione ultimata è consigliabile, senza ironia, completare l’operazione con un danneggiamento meccanico delle superfici del disco.

Tali operazioni possono sembrare frutto di disturbi paranoici, ma è davvero sorprendente constatare quanto il rispetto di alcuni dettagli formali obbligatori per Legge (come, ad esempio, stesura e aggiornamento del DPS) si accompagnino a comportamenti fin troppo disinvolti e inconsapevoli in presenza dello smaltimento delle memorie digitali. Non a caso i tritadocumenti di ultima generazione sono quasi sempre provvisti di una finestrella trita-CD/DVD (utilizzabile anche per gli obsoleti floppy).

Prevenire è meglio di curare

Dopo essersi soffermati sulla eliminazione dei resti, è bene focalizzare l’attenzione sulla conservazione dei dati. Le strategie realmente e sempre efficaci (nonché economiche), come già preannunciato, consistono quasi esclusivamente nella prevenzione, mediante una buona politica di backup, l’utilizzo sistematico del mirroring (RAID1) anche sulle macchine non critiche (il maggior costo si ripaga anche solo evitando una giornata di fuori servizio), una politica di manutenzione preventiva e il salvataggio di “immagini” dei propri

dischi su altri hard disk rimuovibili; una via assai interessante è costituita anche dalla virtualizzazione.

Qualche anno fa aveva destato grande interesse e speranza la tecnologia S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology), che – grazie a un costante monitoraggio di alcuni parametri vitali e sulla base di alcuni modelli statistici di autodiagnosi – prometteva che gli hard disk di nuova generazione sarebbero stati in grado di annunciare in anticipo di essere prossimi a guastarsi. Tale tecnologia, a dire il vero, rappresenta una delle maggiori promesse non mantenute lato utente (alzi la mano chi ha ricevuto nella sua vita uno S.M.A.R.T. warning prima di vedere defungere il proprio prezioso disco...), anche se ha fornito e continua a fornire ai costruttori preziosissime informazioni *post-mortem* sui prodotti ritornati in garanzia: una miriade di dati che hanno permesso la progettazione di supporti sempre più affidabili.

Una clonazione (gratuita) come assicurazione

Il salvataggio di “immagini” delle partizioni dei propri dischi (o dell’intero hard disk) consente, in caso di “crash” o di qualsiasi altro evento nefasto, di recuperare la situazione esattamente com’era al momento della “istantanea”, senza dovere reinstallare nulla. Se si utilizza uno strumento potente e totalmente gratuito come il maturo Clonezilla, poi, è possibile clonare in un sol colpo diversi sistemi operativi installati sul proprio computer, in modo semplice e veloce.

Clonezilla, la cui immagine ISO da masterizzare su CD è scaricabile dal sito ufficiale <http://clonezilla.org/>, è una particolare distribuzione Linux appositamente personalizzata al fine di consentire la copia da disco o partizione a un file immagine (e viceversa), ma anche direttamente da disco a disco e da partizione a partizione. Il riconoscimento dell’hardware (sia esso un disco esterno connesso tramite porta USB o un “depository” in rete) è eccellente e – in taluni casi – superiore a quello di pur giustamente blasonati prodotti commerciali (come, ad esempio, Symantec Ghost). La creazione delle immagini di partizioni NTFS è velocissima, mentre è più lenta quella delle partizioni FAT32; oltre che per i filesystem Microsoft, il supporto è totale per Linux e Mac: ext2, ext3, reiserfs, xfs, jfs, hfs+. Una particolarità notevolissima in ambito aziendale della “Server Edition” (anch’essa gratuita) è quella di potere effettuare una clonazione simultanea in rete su più computer: si pensi al tempo risparmiato potendo ricreare lo stesso ambiente di lavoro su un massimo di quaranta macchine nel giro di pochi minuti.

Clonezilla opera egregiamente anche nel caso in cui il disco di origine presenti problemi di lettura (cosa tipica per hard disk che stanno per defungere): è sufficiente attivare l’apposita opzione “avanzata” e la copia procede inesorabile anche in presenza di errori di lettura.