Fault-tolerant - Tolleranza ai guasti

Fault significa guasto. I sistemi fault-tolerant restano operativi anche con un componente non utilizzabile per guasto. Per arrivare a questo risultato si installano elementi **ridondanti** (supplementari) che garantiscono la funzionalità in attesa della riparazione del dispositivo danneggiato. **Hot swap** indica che la riparazione (scambio del componente guasto) può essere fatta a caldo senza spegnere il sistema. Si tratta di tecnologie applicate soprattutto sui server che utilizzati da numerosi utenti hanno costi per il fermo macchina elevati.

Statisticamente in un PC le parti più soggette a guasti sono quelle con parti in movimento: hard disk, ventole e alimentatori soggette ad usura per attrito. Ci sono parti in movimento anche in DVD e floppy ma il loro uso è occasionale e quindi la probabilità di guasto diminuisce notevolmente.

RAID

Gli Hard Disk sono un elemento critico di un sistema informatico, hanno una probabilità di guasto relativamente elevata. Con un **MTBF** (mean time between failure - tempo medio di funzionamento tra due guasti) pari a 876.000 ore, pari a 100 anni (24 * 365 * 100), si ha la probabilità che un hard disk su cento si danneggi durante il primo anno di funzionamento.

Se la sostituzione del componente danneggiato è semplice, non lo è altrettanto il ripristino dei dati e dei programmi contenuti in esso. Si sono perciò studiati i sistemi RAID (Redundant Array of Independent Disks) in cui più hard disk sono collegati fra di loro per realizzare anche configurazioni fault-tolerant. Le configurazioni più comuni sono: RAID 0, 1 e 5.

Raid 0. Non si tratta di una configurazione fault-tolerant, due o più HD sono configurati per formare un unico HD di capacità maggiore e con migliori prestazioni in quanto possono lavorare in parallelo le testine delle due unità.

Raid 1 Mirror. E' una configurazione fault-tolerant. Per ogni HD ne esiste uno di mirror in cui sono duplicati i dati. In caso di guasto di un HD quello rimasto è sufficiente per il funzionamento del sistema. In scrittura è equivalente ad un HD singolo. In lettura ha una maggior velocità rispetto ad un HD singolo per la possibilità di usare la testina che si trova nella migliore posizione per l'accesso ai dati. Per mantenere le maggiori prestazioni anche in caso di guasto si ricorre all'unità **hot-spare**, un disco di riserva che sostituisce automaticamente quello danneggiato. Per i dati lo spazio utilizzabile è la metà della capacità totale.

Raid 5. E' una configurazione fault-tolerant. Si usano minimo 3 HD di cui uno riservato per la parità, opportuni algoritmi sono in grado di recuperare i dati in caso di guasto di un singolo HD. Anche in questo caso si possono utilizzare unità hot-spare. Con N dischi lo spazio per i dati è pari alla somma della capcità di N-1 HD.

Raid 0 e 1 sono già disponibili su molte schede madri configurando due HD SATA. Per sistemi ad alte prestazioni si usano unità SCSI.

Alimentatore ridondate

Nel cabinet del server si trova lo spazio per il montaggio di due o più alimentatori. In caso di guasto quelli rimasti sono in grado di alimentare comunque il sistema.

Ventole ridondanti.

Per garantire il raffreddamento adeguato si montano più ventole rispetto al minimo indispensabile.

RAM ECC

Esiste una probabilità minima ma diversa da zero che un bit memorizzato in una RAM possa cambiare valore. Per rilevare questi malfunzionamenti si ricorre, nelle RAM ECC, a bit supplementari di parità che possono:

- Rilevare l'errore bloccando il sistema
- Correggere automaticamente l'errore con opportuni algoritmi di calcolo.

Si tratta di dispositivo più costosi delle memorie installate nei PC di uso comune.

Server gemello

Se l'azienda vuole che il sistema informativo non si fermi per qualunque guasto si ricorre ad un secondo server con le stesse caratteristiche del primo e che è aggiornato in tempo reale con le modifiche del server principale. In caso di guasto il secondo sistema subentra automaticamente al primo senza creare interruzioni del servizio.

UPS – Gruppo elettrogeno

Garantisce il funzionamento del sistema anche in mancanza di energia elettrica. Per avere ore di autonomia è necessario ricorrere ad un gruppo elettrogeno sincronizzato con l'UPS che garantisce l'energia nel tempo necessario per l'avvio del motore.

Backup - Copia di sicurezza

L'utilizzo del sistema più affidabile che esista non esonera l'amministratore dall'impostare un adeguato programma di backup e di **disaster recovery**.

Si devono effettuare periodicamente copie dei dati memorizzate nel sistema. La frequenza e il numero di copie dipendono dall'importanza dei dati. Per valutare l'importanza dei dati la domanda da porsi è quanto tempo è necessario per ricaricare i dati in caso di perdita? Per alcune applicazioni **mission critical** non è ammessa la perdita di nessun dato.

La copia può essere fatta in tempo reale, giornalmente, settimanalmente, ecc…

I supporti possono essere:

- Server gemello per copie in tempo reale
- Replica su un secondo PC
- DVD fino a 5 GB
- Chiavi USB per archivi fino a 10 GB
- Hard disk esterni con interfaccia SATA o Ethernet Gigabit per archivi fino a un TB. L'uso dell'USB per grandi quantità di dati non è consigliabile per la sua lentezza.
- Nastri di backup per archivi oltre i 100 GB
- Spazio in una server farm accessibile tramite Internet.

Per evitare inutili ripetizioni di copia di dati già memorizzati si utilizza la funzionalità di **backup incrementale** che duplica solo i dati variati rispetto all'ultima copia.

Visto che anche la copia si può danneggiare i backup dovrebbero essere almeno due da usare alternativamente in modo indipendente.

Per aumentare la sicurezza almeno una copia dovrebbe essere conservata in locali diversi da quello in cui è installato il sistema informativo, **vaulting**.