

27 Novembre 2004
LINUX DAY 2004

Recuperare dati da un hard-disk parzialmente danneggiato

GIAN PAOLO GHILARDI

Il caso Carapax

- Carapax è il nome di un nostro piccolo server interno su cui sono pubblicati documenti, appunti, ... degli studenti del Polo di Crema.
- circa un mese fa, a seguito di una riaccensione forzata dovuta ad un blackout, la macchina non torna online.
- l'hard-disk emette suoni nefasti, che non annunciano nulla di buono.
- questa (breve) presentazione ha lo scopo di illustrare la sequenza di passi compiuti per recuperare i dati dal sopra-citato hard-disk.

Prima analisi con Knoppix

- Carapax dispone di diverse partizioni formattate con Reiserfs v3, un filesystem di tipo journaling.
- per accertare il problema si è proceduto tramite la “solita” Knoppix.
- effettuato il boot, si è provato a montare la partizione di root (/) in una opportuna directory.

```
mount -t reiserfs /dev/hda1 /mnt/RESCUE
```
- ovviamente il mount non ha avuto esito positivo ed il fallimento è stato seguito da un vistoso aumento del rumore dell’hard-disk (ossia si sente “grattare”).

Check del filesystem 1/2

- la valutazione del livello di danno inizia con una verifica sul filesystem.
- come detto le partizioni di Carapax sono state formattate con Reiserfs v3, conseguentemente si usano i relativi tool, i `reiserfsprogs`.
- si decide di trascurare momentaneamente il rumore di fondo prodotto dall'hard-disk e si procede:
 - verificando l'integrità del filesystem, eventualmente forzando un controllo completo (non solo il normale log-replay dei filesystem journaling come Reiserfs)
 - testando l'eventuale danneggiamento dei soli superblocchi (ossia di quei blocchi contenenti le informazioni fondamentali del filesystem utilizzato)
 - forzando la ricostruzione del "tree" di Reiserfs: in pratica si chiede di riscrivere la struttura e le informazioni fondamentali del filesystem rileggendo tutti i dati utili direttamente dal disco/partizione che li contiene.

Check del filesystem 2/2

- Il programma usato per verificare lo stato del filesystem è `reiserfsck`. Si decide di procedere per gradi, verificando ed eventualmente correggendo le varie parti del filesystem danneggiate.
- le opzioni di `reiserfsck` provate su Carapax sono, nell'ordine:
 - `--check`: richiede una verifica rapida dell'integrità del filesystem
 - `--fix-fixable`: richiede un controllo ed un'eventuale correzione delle anomalie trovate sul filesystem
 - `--rebuild-sb`: richiede la ricostruzione dei superblocchi del filesystem
 - `--rebuild-tree`: richiede la ricostruzione completa del "tree" del filesystem
- ciascun test sul disco incriminato ha avuto esito negativo: è terminato prematuramente intorno al 50% dell'analisi preliminare. Il tutto è stato accompagnato da una lunga attesa (i tools tentano più volte la lettura prima di segnalare il fallimento) e da un significativo aumento del rumore molesto dell'hard-disk.

Test dei cluster danneggiati

- verificato che il problema si trova a monte del filesystem, ossia si tratta di un problema hardware, decidiamo quindi di controllare lo stato dei cluster: usando il programma `badblocks`.
- a seconda delle opzioni `badblocks` può effettuare dei test distruttivi (ossia effettua dei test di lettura e scrittura sui blocchi erronei) o meno (sola lettura).
- nel nostro caso scegliamo di effettuare un controllo in modalità read-only, con rapporto dettagliato (verbose mode) e log su file.
`badblocks -v /dev/hda1 -o badblocks.log`
- il log su file dei cluster danneggiati ci permette di ripetere i controlli sul filesystem tramite `reiserfsck` informando però il tool della presenza di cluster danneggiati.
- sfortunatamente nemmeno la conoscenza dei cluster danneggiati ha permesso di ripristinare il normale funzionamento del disco.

Considerazioni

- l'hard-disk appare danneggiato ma non interamente: benchè non sia stato possibile montare le partizioni, `reiserfsck` ha comunque potuto operare su una parte significativa dei dati prima di terminare con un messaggio di errore.
- rimane quindi da accertare se i dati siano effettivamente persi o sia comunque possibile recuperarne una porzione.

Un primo tentativo di recupero dei dati

- per recuperare i dati dall'hard-disk una prima idea è l'utilizzo di `dd` (data dumper), programma UNIX utilizzabile per effettuare una copia bit-a-bit dei dati di una partizione su un altro hard-disk.
- sfortunatamente `dd` non è ottimizzato per operazioni di rescue di dati: in presenza di gravi errori di I/O (quali possono essere grossi insiemi di cluster danneggiati), `dd` termina con un codice di errore.

Il mini-howto

- un'immediata ricerca su Internet ci ha permesso di recuperare un'interessante pagina con un *mini-howto* che spiega come tentare un recupero dati da un hard-disk danneggiato in situazioni analoghe alla (per non dire peggiori della) nostra.
- Il documento è disponibile su:
http://home.arcor.de/florianlang/writing/hd_failure/

Il tool consigliato

- la soluzione presentata nel documento si è rivelata soddisfacente anche nel nostro caso.
- il tutto si riconduce all'utilizzo di una versione modificata di *dd*, *dd_rescue*, appositamente ottimizzata per tentare il recupero di tutti i dati anche in presenza di grandi quantità di errori di I/O.
- Il tool (ovviamente gratuito) è disponibile presso <http://www.garloff.de/kurt/linux/ddrescue/>

Recupero dei dati 1/2

- l'idea base è veramente semplice:
- si usa `dd_rescue` sulle partizioni danneggiate, ottenendo immagini contenenti tutti i dati recuperabili/recuperati (ovviamente le immagini sono poste su un qualche medium affidabile, come un altro disco).

```
# dd_rescue /dev/hda1 /mnt/smb_remote/hda1_saved.img
```
- si montano le immagini in loopback

```
# mount -t reiserfs -o rw,loop=/dev/loop0  
/root/hda1_saved.img /mnt/RESCUE
```
- se tutto procede (estremamente) positivamente il filesystem dovrebbe essere montato direttamente e dovrebbe essere possibile recuperare i dati senza ulteriori passi (come è fortunatamente avvenuto nel nostro caso).

Recupero dei dati 2/2

- qualora il filesystem montato in loopback dovesse risultare danneggiato (es: alcuni superblocchi critici non sono stati recuperati correttamente), è ora possibile utilizzare *reiserfsck* ed invocare la ricostruzione del “tree” (stavolta il tutto avviene su un medium affidabile!).
- se tutto procede correttamente sarà ora possibile recuperare i dati (nel nostro caso, una porzione significativa comprensiva dei dati per noi fondamentali).
- nel nostro caso tutto si è risolto positivamente. :)

Conclusioni

- spero che questa stringata presentazione vi sia piaciuta.
- morale della fiaba: mai dare per morto un hard-disk prima di aver cercato il giusto tool sulla Rete :)
- that's all, folks! ;)