



INFN/TC-00-09

1 Giugno 2000

Ba.Se.: idee per un backup semplificato

Giovanni Barbagallo¹, Massimo Carboni², Davide Cobai³, Roberto Ferrari⁴,
Francesco Ferrera¹, Michele Gambetti⁵, Francesco Prelz⁶,
Ivo Saccarola⁴, Claudio Strizzolo⁷, Lucio Strizzolo⁷

¹⁾ *INFN, Laboratori Nazionali del Sud*, ²⁾ *INFN, Laboratori Nazionali di Frascati*,
³⁾ *INFN, Gruppo collegato di Udine*, ⁴⁾ *INFN, Sezione di Padova*,
⁵⁾ *INFN, Sezione di Ferrara* ⁶⁾ *INFN, Sezione di Milano* ⁷⁾ *INFN, Sezione di Trieste*

Riassunto

I prodotti commerciali di backup non forniscono una copertura completa delle esigenze di backup identificate all'interno dei servizi calcolo dell'INFN. L'integrazione di componenti esistenti di pubblico dominio con una struttura di storage estremamente semplificata (e resa possibile dal basso costo delle unità a disco in ambiente PC) sembra fornire un'alternativa pratica ed accessibile. Presentiamo le caratteristiche di un simile sistema.

PACS:89.80

*Published by SIS-Pubblicazioni
Laboratori Nazionali di Frascati*

1 Perché non affidarsi ad un prodotto commerciale?

- Nel corso delle prove effettuate dal gruppo di lavoro INFN sui backup, è emerso che nessuno dei prodotti commerciali disponibili sul mercato italiano soddisfa *tutti* i requisiti stabiliti preventivamente dallo stesso gruppo.
- I prodotti commerciali tendono a soddisfare le esigenze delle installazioni commerciali (tipicamente gestione di database ad alta disponibilità). Dal punto di vista dei requisiti formulati per le sezioni INFN, questo rappresenta un costo aggiuntivo in termini di complessità di comprensione del sistema. Secondo la logica di diversificazione commerciale, poi, il formato di backup dei singoli prodotti è proprietario sia in termini di compressione che in termini di organizzazione interna delle aree di stage e dei nastri.
- Nessun prodotto commerciale prevede la possibilità, oggi del tutto accessibile per i ridotti costi degli hard disk, di avere l'intero saveset di backup aggiornato disponibile in linea, in modo da poter effettuare un'operazione di restore nel modo più semplice possibile, utilizzando i normali comandi di gestione dei file.
- Esistono componenti software di pubblico dominio per UNIX generico, largamente adottate e stabili (ad es. prodotti GNU come *gtar* *gzip*, oppure *Samba*, oppure database per la gestione dell'archivio), che fanno sì che la realizzazione di uno strumento di backup *semplificato*, con server su UNIX generico, diventi un esercizio di integrazione piuttosto semplice (si vedano le specifiche più sotto).
- Una soluzione costruita con componenti pubbliche risulta più facilmente scalabile, ad esempio per la realizzazione di stazioni (“chioschi”) di backup che possono essere usati per backup occasionali da parte di singoli utenti.
- Uno strumento di pubblico dominio, che comprenda strumenti modulari di accesso e gestione dei dati su tutti i filesystem identificati nei requisiti per l'INFN, può anche supplire alle carenze di qualunque pacchetto software commerciale adottato che, ad esempio, non sia in grado di gestire particolari filesystem (ad es. *AFS*).
- Può essere utile una soluzione di contingenza se emergono problemi nella manutenzione, commercializzazione o supporto a lungo termine di un qualunque prodotto commerciale.

2 Schema funzionale (Figura 1)

Partendo dai requisiti sviluppati dal gruppo di lavoro INFN sui “Tool di interesse generale”, ipotizziamo un *server di backup* su UNIX generico, preferibilmente su architettura PC (Linux). Per semplificare al massimo l’organizzazione dei dati sul server, e considerando il costo decrescente dello storage su disco (indicativamente: 230 Euro IVA inclusa per 18 GB EIDE alla data di stesura del presente documento), supponiamo di avere a disposizione un’*area di stage* sul server di dimensioni pari al saveset di backup. Le esigenze di archiviazione storica dei dati di backup vengono gestite da un’*unità di archiviazione a nastro* (singola o robotizzata) collegata direttamente al server di backup.

I dati oggetto del backup risiedono in linea di principio su un numero imprecisato di host accessibili via rete (che da questo momento in poi verranno definiti *clienti di backup*). I dati di backup vengono in generale identificati univocamente dal protocollo di accesso ai dati, dal nome di rete del cliente di backup e dalla directory radice del filesystem che li ospita (ad esempio nel formato `base://nome.xx.infn.it/directory1/directory2`). La funzione di *cliente di backup* può al limite essere svolta anche dal server stesso, ma rimane logicamente distinta. Le funzioni del server di backup sono sostanzialmente due:

1. Scheduling del trasferimento dei dati dai clienti di backup all’area di stage. Può essere richiesto il backup (cioè la sua sincronizzazione con la copia nell’area di stage) di un dato filesystem (identificato come sopra), su base oraria, giornaliera, settimanale, mensile, oppure in modo asincrono su richiesta. La programmazione di questa attività deve essere in grado di tenere conto delle risorse di rete locale disponibili (ad esempio, deve essere in grado di interrompersi nelle ore diurne).
2. Trasferimento programmato dei dati presenti nell’area di stage verso l’unità di archiviazione. Essendo l’unità di archiviazione collegata direttamente al server, questa attività può utilizzare la massima capacità di I/O dell’unità di archiviazione stessa.

Queste due funzioni possono svolgersi in modo indipendente. L’attività di archiviazione genera informazioni di log (quali file, con quali caratteristiche, quando sono stati archiviati su nastro, dove...) che è utile vengano salvate in modo organizzato (database ?) per facilitare le operazioni di restore. Per garantire la consistenza di questo archivio, l’archivio stesso viene salvato su tutti i nastri prodotti dall’unità di archiviazione.

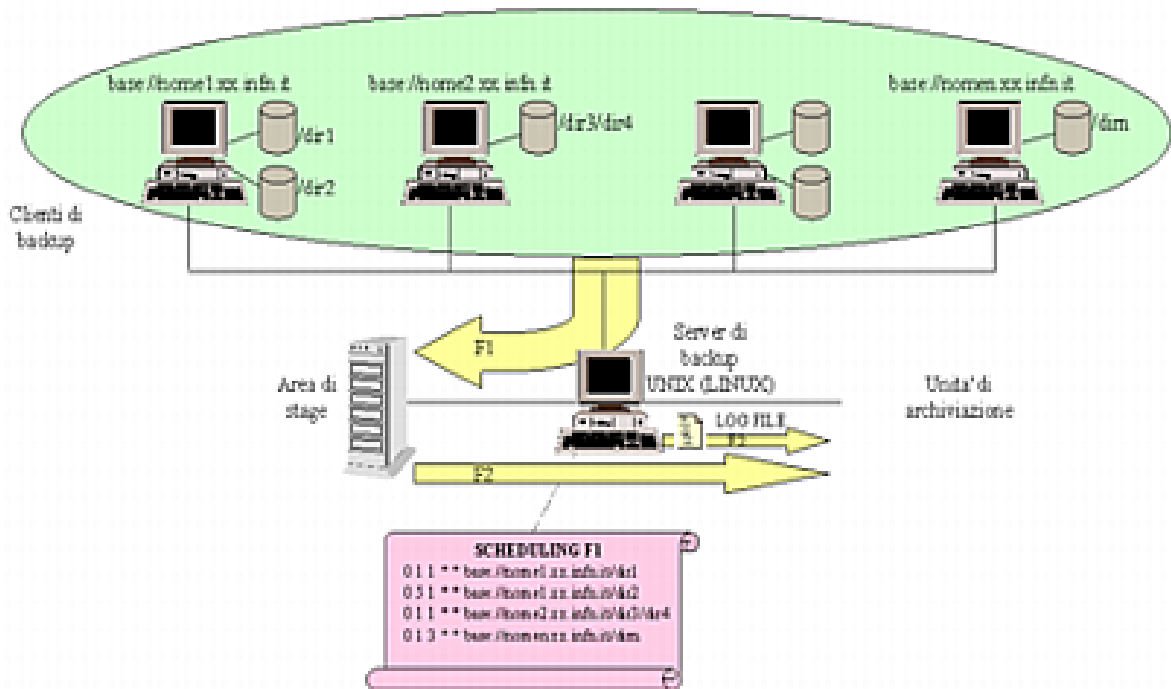


Figura 1: Schema funzionale di un sistema di backup semplificato.

3 Accesso ai dati sui clienti di backup

I requisiti elaborati dal gruppo di lavoro INFN sui “Tool di interesse generale” identificano la possibile provenienza dei dati stessi come segue:

1. Filesystem montati su Unix generico
2. Filesystem Unix esportati via NFS
3. Filesystem Unix esportati via AFS
4. Filesystem Windows esportati via Netbios
5. Filesystem Windows NT montati localmente

Il server di backup deve essere integrato con componenti adatte a trasferire file con queste caratteristiche da e per i clienti, ed a ripristinare quelle caratteristiche che non possono essere mappate in modo naturale sulle caratteristiche di un file Unix. In particolare, si possono utilizzare i seguenti accorgimenti:

3.1 Filesystem montati su Unix generico (Figura 2)

I file vengono richiesti ad un applicativo di servizio appositamente installato sulla macchina (inetd), in grado di autenticare l'utente/host di backup remoto e di inviare i dati relativi.

3.2 Filesystem Unix esportati via NFS (Figura 3)

Vengono montati sul server di backup, provvisto di cliente NFS.

3.3 Filesystem Unix esportati via AFS (Figura 4)

I file vengono copiati dal server di backup seguendo il loro albero logico (e non la collocazione fisica in volumi AFS). Per le directory viene inoltre salvata (in un file ausiliario collocato nell'area di stage, e salvato su nastro con tutto il resto) la ACL, per consentirne il ripristino in fase di restore. Da questo discende che il server di backup deve essere configurato come cliente di AFS, e che deve essere in possesso di autenticazioni sufficienti per leggere i file (utente di sola lettura), e almeno dell'autenticazione dell'utente proprietario dei file per il loro ripristino. Il ripristino non comprende la ri-creazione e la ri-configurazione dei volumi AFS, la cui manipolazione è riservata all'amministratore AFS.

UNIX GENERICO

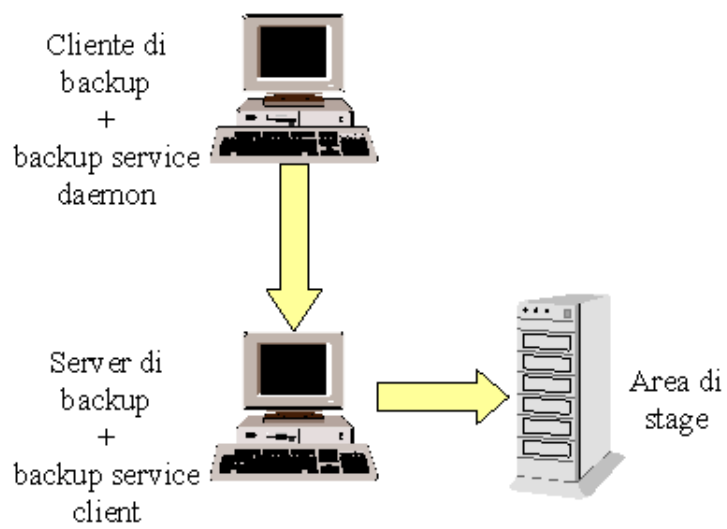


Figura 2: Accesso ai filesystem montati su Unix generico.

UNIX NFS

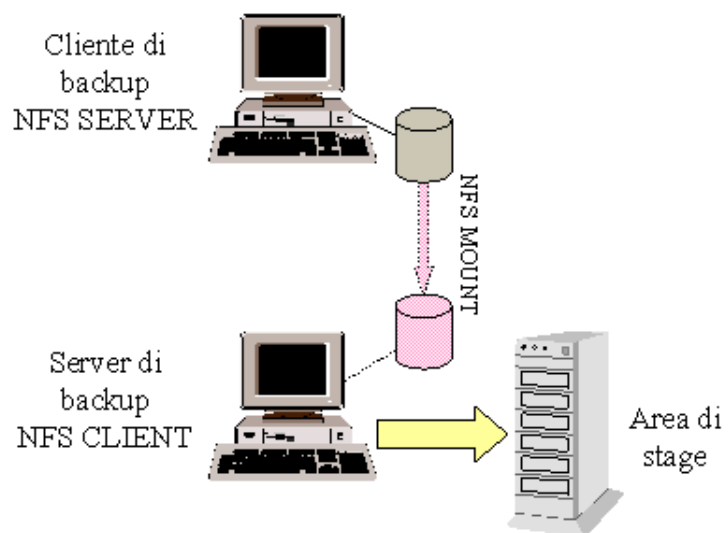


Figura 3: Accesso ai filesystem Unix esportati via NFS.

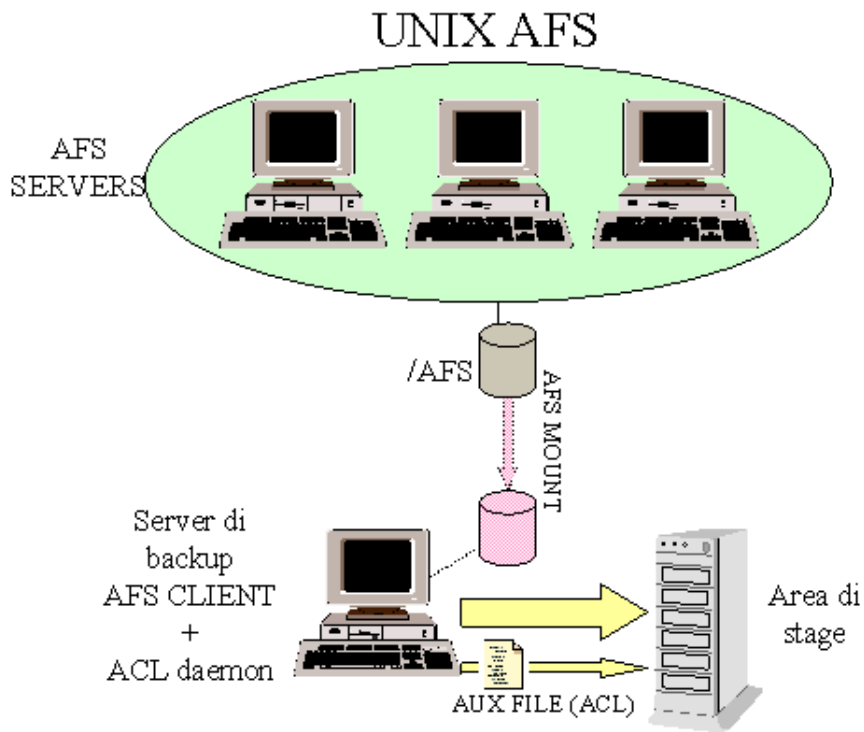


Figura 4: Accesso ai filesystem Unix esportati via AFS.

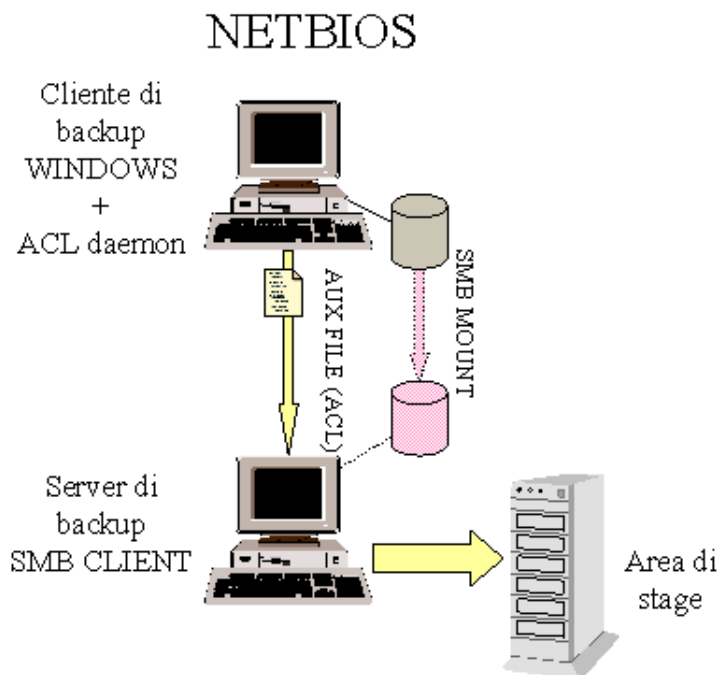


Figura 5: Accesso ai filesystem Windows/NT esportati via Netbios.

3.4 Filesystem esportati via Netbios (Figura 5)

Vengono copiati sul server di backup via smbmount o smbtar (Samba). In questo caso devono essere ottenute e salvate le ACL di protezione dei singoli file. È necessario un applicativo di servizio sul cliente Windows in grado di ottenere le ACL dei file (output del comando di sistema "cacls"), in modo che queste possano essere salvate in un file ausiliario nell'area di stage, e quindi eventualmente ripristinate.

3.5 Filesystem locali montati su Windows NT (Figura 6)

È necessario un accesso ai file (che ad ordine zero potrebbe essere fornito da un server FTP), e lo stesso applicativo di cui al punto precedente per ottenere (ed eventualmente ripristinare) le informazioni sulle ACL.

La comunicazione con questi filesystem diversi si presta bene ad essere incapsulata in moduli collegati al server di backup, e che implementano le seguenti funzioni:

- copia di un filesystem remoto nell'area di stage (con codici di errore che definiscano in modo inequivocabile il successo o l'insuccesso dell'operazione). Questa

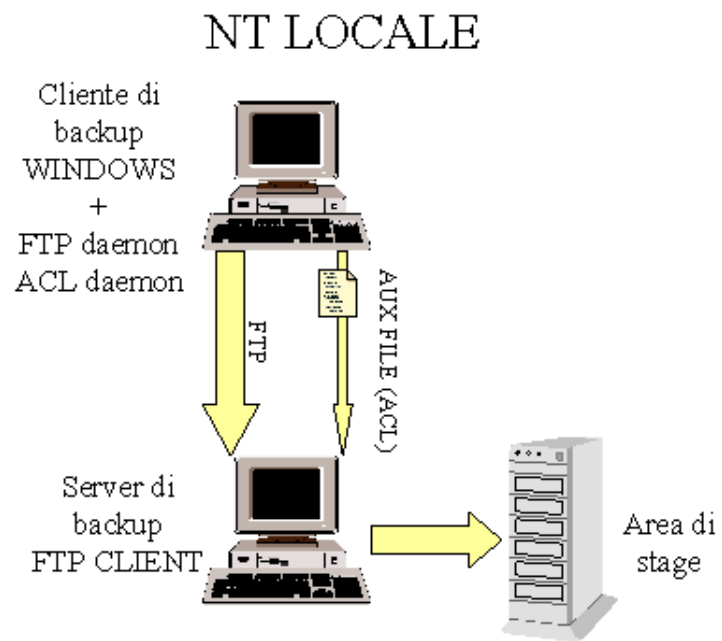


Figura 6: Accesso ai filesystem locali montati su Windows NT.

funzione codifica anche (ove necessario) le informazioni accessorie sui file (ACL o altro) e le salva in opportuni file accessori nell'area di stage.

- ripristino di un filesystem presente nell'area di stage verso il cliente di backup (ed eventuale ripristino di informazioni accessorie come le ACL).
- copia e ripristino come sopra di singoli file.

I metodi che implementano queste funzioni all'interno dei moduli possono essere riassunti in soli due:

```
Status Backup_Module::save(String filesystem);  
Status Backup_Module::restore(String filesystem);
```