

An illustration depicting a data backup process. At the top, three yellow folders are shown. On the left, a laptop with a blue screen is positioned next to a hard drive. In the bottom right, there is a blue cloud icon and a stack of silver database cylinders. Two large, light blue curved arrows indicate the flow of data: one from the folders down to the cloud, and another from the cloud back up towards the laptop and hard drive. The word 'BACKUP' is written in large, bold, red letters with a black outline across the center of the image.

**BACKUP**



# I Dati

- I **dati** sono la principale ricchezza di qualsiasi azienda che utilizza un sistema informativo.
- Tutte le aziende di piccolo/medio/grosso calibro di solito hanno un sistema informatico → **tutte le aziende hanno nei dati una criticità fondamentale.**
- Si anche il DAIS e Ca'Foscari, pensate ad esempio, ai soli dati relativi alle iscrizioni degli studenti di ogni singolo anno...
- Anche se non sembra, i dati sono una risorsa costantemente in pericolo...

# Dati – Nemici/Pericoli

- I principali nemici che insidiano i dati sono:
  - **Guasti all'hardware**
    - Hard disk e ram guasti causano corruzione e/o perdita di dati.
  - **Bachi nel software**
    - Qualche simpaticone che sbaglia la clausola where in una query di cancellazione in un database:  

```
delete from <importantissima tabella non replicata> where 1=1;
```
  - **Azione umana**
    - Utente che legge libri proibiti su sql e poi ti sgancia un:  

```
mysql> drop database <importantedatabase che sostiene il mondo>
```
    - Utente che passando per la sala server appicca un incendio....
    - Sistemista distratto da  bionda carina  che scrive:  

```
# rm -rf /
```
    - Svariati tecnici che fanno manutenzione di svariate cose (condizionatori, centraline ecc) che staccano/attaccano spine e interruttori a casaccio.
  - **Disastri vari**: terremoti, **incendi**, **allagamenti**, cavallette, carestie,...

# BACKUP

- È **fondamentale** avere una o più copie dei dati:
  - I **dati sono preziosi**, crearli, estrapolarli è più costoso in termini di tempo e denaro che proteggerli.
  - È necessario quindi applicare delle politiche per la protezione dei dati stessi.
- Creare, mantenere, gestire e amministrare le copie dei dati è una operazione chiamata **Backup**.
- L'operazione di estrazione dei dati da un **backup** è detta **Restore**. Ogni tanto è opportuno provare un restore di qualche dato per verificare che il backup sia **consistente**.
- Il **backup dei dati** ci salva spesso da situazioni altrimenti disastrose.

# BACKUP - supporto

- Il **backup dei dati** è una delle maggiori applicazioni delle unità di storage!
- **Deve essere effettuato** su unità di storage diverse da quelle contenute all'interno del server/pc che contengono i dati da proteggere.
- La scelta del **supporto di backup** è fondamentale e deve tenere conto dei seguenti punti:
  - Costo.
  - Affidabilità.
  - Velocità.
  - Disponibilità.
  - Conservazione.
- Esempi di supporto: DAT, DLT, TAPELIB, HD, DVD, BLURAY, SAN, NAS, vecchi server inusati con dischi grossi ecc....

# BACKUP – old style

- Prima dell'avvento di **NAS** e **SAN** le risorse di storage erano connesse direttamente a un server (soluzioni **SAS** e **DAS**) e l'unico modo per effettuare il backup all'interno della rete prevedeva che i dati venissero trasferiti all'unità di backup attraverso la LAN:
  - **DAT, DLT, TAPELIB e altre unità a nastro**: erano connesse a dei server che si occupavano di fare il backup tramite software client/server (amanda, bakula, ntbackup).
  - **Dischi usb/firewire, cd, dvd, bluray**: come sopra.
  - **USB PEN**: non è una valida soluzione di backup!!! Come lo erano i floppy.
- Questo approccio, usato a volte anche oggi, ha degli inconvenienti... Quali?

# BACKUP – old style, inconvenienti

- **Traffico elevato sulla LAN:** spesso i backup devono girare solo di notte se si ha una sola LAN per via del consumo di banda.
- I server di backup sono collocati nel percorso dei dati... si **consumano quindi risorse server** che dovrebbero essere destinate ai calcoli.
- La **sicurezza informatica spesso viene meno**, in quanto, spesso, i dati da salvare viaggiano in chiaro sulla LAN usata anche dagli utenti. (ad esempio: AMANDA).

# BACKUP: SAN E NAS

- Con l'avvento di **SAN** e **NAS**, anche l'approccio al backup è cambiato!
- **Sostanzialmente questi sistemi permettono, tramite una buona progettazione di eseguire backup di qualsiasi tipo senza intasare la banda della LAN (hanno ad esempio schede Gb e/o LAN dedicate) e senza limitare preziose risorse di calcolo.**
- Quello che risparmiate sulla CPU, sulla RAM, ecc.. di un server dedicato al backup lo potete investire in tanti dischi cicciosi da usare per collezionare e proteggere i vostri dati :).



# BACKUP – Ruolo del Sysadmin

- Il Sys Admin spesso **è un paranoico maniacale**... e la paranoia è essenziale per una gestione responsabile del backup!!!!
- È meglio salvare più volte gli stessi dati che dimenticarsi qualcosa....
- Per questo è utile avere un backup del backup e...
- **Backup del sistema di backup.**
  - Es: amanda: se crashava il server amanda addio backup.
  - Se il pc va in crash che fine fa il backup?
  - Pensare a un sistema di backup ridondato.
- **Il sistemista deve pensare e prevedere tutte queste cose.**

# BACKUP – Tipologie/Strategie

- Vi sono tre **strategie o tipologie** di backup che si distinguono principalmente per la mole di dati da salvare ad ogni esecuzione:
  - **Completo.**
  - **Differenziale.**
  - **Incrementale.**
- A seconda dell'importanza e della frequenza di variazione dei dati da salvare un backup può essere:
  - Eseguito ogni minuto...
  - **Orario.**
  - **Giornaliero.**
  - **Settimanale.**
  - **Mensile.**

# Backup Completo

- Un **backup completo** effettua, periodicamente la **copia completa di tutti i dati da salvare**.
  - Se avete 1Tb di dati da salvare ogni notte, ogni giorno il backup completo occuperà 1Tb sul supporto di storage scelto.
- È una soluzione ottimale solo per piccole quantità di dati e/o cicli di backup lunghi (1 volta alla settimana?).
- L'esempio più semplice di backup completo è il backup che potreste fare della vostra home linux tramite il comando `tar`:

```
# tar cvf faromano.tar /home/faromano
```

Per il restore:

```
# tar xvf faromano.tar
```

# BACKUP - Incrementale

- Un **backup incrementale** salva solo i dati modificati successivamente all'orario in cui è stato effettuato l'ultimo backup (completo o incrementale).
- Si parte ovviamente da un **backup completo** che deve essere rinnovato (rifatto) periodicamente.
- Il vantaggio principale è la velocità di esecuzione del backup.
- Lo svantaggio è che spesso il ripristino di uno o più file richiede l'analisi di uno o più backup incrementali, a volte fino al completo di riferimento.
  - In caso di ripristino di un filesystem intero è necessario recuperare l'ultimo backup completo e poi tutti gli incrementali successivi.

# BACKUP - Differenziale

- I **backup differenziali** sono simili a quelli incrementali: **salvano solo i file modificati dall'ultimo backup**. Tuttavia, i **backup differenziali sono cumulativi**: in altre parole, con uno schema differenziale, **una volta che un file viene modificato** esso continua ad essere **incluso in tutti i backup differenziali successivi** (fino ovviamente al successivo backup completo).
- **Ogni backup differenziale contiene tutti i file modificati dall'ultimo backup completo**, rendendo possibile l'esecuzione di un ripristino completo con solo l'ultimo backup completo e l'ultimo backup differenziale.
- Anche la strategia dei backup differenziali prevede di partire da un backup completo che deve essere rinnovato (rifatto) periodicamente.

# BACKUP – Esempio LAB DAIS

- Per il backup su Windows utilizziamo un software gratuito nella sua forma base di nome **Uranium Backup**. Uranium effettua tutte le notti un **backup completo** delle **Home (Z)** verso un area condivisa.

- Per Linux usiamo/usavamo **bakula** che effettuava un **backup incrementale** tutte le notti. Ora usiamo `rsnapshot`:

`rsnapshot` effettua tutte le notti un **backup differenziale** delle Home su un volume esportato da un NAS e si occupa di creare periodicamente un **backup completo**.

# BACKUP – Esempio LAB DAIS

BROOT:  
Autenticazione/Home  
Windows



Uranium Backup:  
backup completo delle  
Home su Area  
condivisa

Obelix: NAS di Backup

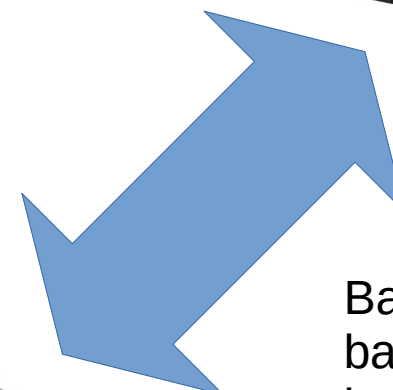


BAU: replica di BROOT



ROAR: Home Linux

Bakula/rsnapshot:  
backup  
incrementale



# BACKUP – Rsnapshot

- **rsnapshot** è una applicazione in grado di effettuare il **backup differenziale** di porzioni di file system.
- Sfruttando **rsync** è in grado di conservare diverse copie di backup, realizzate in diversi istanti di tempo, minimizzando la quantità di dati trasferiti e lo spazio occupato nel disco.
- Se utilizzato in concomitanza con **ssh** può effettuare il backup anche di sistemi remoti.
- Vedremo installazione e configurazione in laboratorio!



# Avete il backup!!!



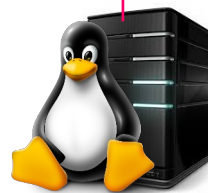
192.168.100.0



Nas dati



.10



.12



.13



192.168.1.50



192.168.1.100



Nas per il backup dei dati

