

Guida al backup

1. Introduzione al backup

Backup dei dati – una parte necessaria nella gestione dei rischi

Con l'aumentare dei rischi associati a virus, attacchi informatici e rotture hardware, implementare una procedura di backup sistematico è una parte necessaria per ogni strategia aziendale di gestione del rischio.

La perdita dei dati può avvenire per una moltitudine di motivi, quali cancellazione accidentale di file, che può restare ignorata per giorni se non settimane. Una buona strategia di backup deve permettere di poter ripristinare i dati da diverse istanze di un certo lasso di tempo.

La scelta del sistema di backup va ponderata accuratamente, e l'investimento necessario va confrontato con il costo di un eventuale perdita dei dati. Molte volte si sottovaluta l'effettiva perdita economica dovuta alla perdita o all'indisponibilità dei dati. Si prenda ad esempio la perdita di un singolo file (progetto, foglio elettronico, etc.) a cui si è lavorato magari per decine di ore, la sua ricostruzione da zero implicherà l'utilizzo di un numero identico di ore e la sua indisponibilità per tutto il tempo necessario a ricostruirlo.

Backup su nastro – media ideale

Il nastro è un media ideale per le sue notevoli capacità di immagazzinamento, per il basso costo, e la possibilità di archiviare i nastri in luoghi protetti.

Organizzare un numero di nastri in una efficiente strategia di backup permette inoltre di ripristinare i dati da diversi punti temporali, e di archivarli.

Backup su disco – giusto complemento

Un giusto complemento al backup su nastro è il backup su disco, esso può esser fatto sui dischi già presenti sulla macchina o collegati direttamente ad essa (DAS), su sistemi di dischi disponibili in rete (NAS) e strutture di rete progettate per l'immagazzinamento di dati (SAN). Il backup su disco permette di solito di avere una maggiore velocità di esecuzione, consentendo di ridurre la finestra temporale che deve essere resa disponibile al backup di file aperti o altamente utilizzati.

I formati nastro

Esiste una moltitudine di formati nastro. Alcuni tra i più usati sono:

Formato nastro	Capacità (non compressa)	Velocità di trasferimento	Utilizzo
Travan	1 - 20Gb	1Mb/sec	Uso domestico, piccoli server
DAT / DDS / 4mm (Digital Data Storage on Digital Audio Tape)	2 - 20Gb	2.75Mb/sec	Server piccoli/medi,
LTO (Linear Tape Open)	200 - 1600Gb	40-320Mb/sec	Server medi/grandi e mainframe

Le organizzazioni piccole e medie troveranno che un nastro Travan o 4mm fornirà la soluzione ideale in termini di capacità di immagazzinamento e costo. Sarà di solito possibile immagazzinare tutti i dati in un unico nastro, in questo modo sarà sufficiente acquistare una singola unità a nastro al posto di un più costoso caricatore di nastri.

Quando vanno fatti i backup?

Il backup va fatto idealmente al di fuori dell'orario di lavoro, quando il traffico di rete è al minimo. Schedulare il backup in un orario notturno è la soluzione migliore per gran parte delle organizzazioni. Eseguire il backup una volta al giorno (dopo ogni giorno lavorativo) fornisce una buona protezione contro la perdita di dati.

I differenti tipi di backup

All'interno del software di backup sono disponibili diversi tipi di backup. Ognuno di essi potrà immagazzinare una differente quantità di dati, e differenti tipi di file come possiamo vedere nella tabella sottostante:

Tipo di backup	File immagazzinati sul nastro
Completo	Tutti i file, dati di sistema, etc.
Differenziale	Tutti i file aggiunti o modificati dall'ultimo backup completo
Incrementale	Tutti i file aggiunti o modificati dall'ultimo backup completo, differenziale o incrementale
Giornaliero	Tutti i file aggiunti o modificati durante lo stesso giorno del backup

Un backup completo salverà tutti i file e i dati di sistema sul nastro. Questo permetterà il ripristino completo di tutti i dati da un unico nastro.

I backup differenziali, incrementali e giornalieri sono backup parziali e servono a ridurre la quantità di dati salvati sul nastro e la velocità di esecuzione del backup stesso. Per ripristinare i dati da uno di questi backup verrà richiesto anche l'ultimo backup completo, così come tutti gli altri backup parziali eseguiti dall'ultimo backup completo.

Per esempio: se il backup completo viene eseguito al lunedì, e backup incrementali durante gli altri giorni, per ripristinare i dati dell'ultimo giovedì sono necessari 4 nastri (lunedì completo + martedì incrementale + mercoledì incrementale + giovedì incrementale).

Il problema con i backup parziali è la necessità di più nastri durante il ripristino dei dati. Se uno di questi nastri è rovinato, non è possibile garantire che il ripristino proceda correttamente.

Chiaramente, se la totalità dei dati può essere immagazzinata in un singolo nastro, eseguire il backup completo ogni volta è la strategia più sicura.

Il software di backup

Esistono moltissimi software che aiutano ad eseguire il backup; ognuno di essi ha caratteristiche e costi differenti. La scelta del software va fatta tenendo conto delle esigenze aziendali e del prezzo che si è disposti a pagare.

2. I sistemi di rotazione dei nastri

In un sistema di rotazione dei nastri, più nastri sono organizzati in una libreria, in modo da fornire un completo sistema di salvataggio dati, con la possibilità di mettere i nastri in una posizione remota per una maggiore sicurezza. Nastri differenti sono usati in giorni differenti seguendo una specifica strategia.

Rotazione con 5 nastri – uno al giorno

Lo schema di rotazione più semplice è quello di avere un nastro per ogni giorno lavorativo. Se la settimana lavorativa va dal lunedì al venerdì avremo 5 nastri così etichettati: lunedì, martedì, mercoledì, giovedì, venerdì. Ogni giorno della settimana andrà sostituito il nastro. Per esempio: se il backup viene eseguito alle ore 22:00 di ogni giorno, durante la giornata dovrà essere inserita la cassetta del giorno stesso (il lunedì quella del lunedì, il martedì quella del martedì, e così via).

Con questo sistema sono necessari solo 5 nastri, ma si possono ripristinare solamente i dati dell'ultima settimana.

Rotazione dei nastri con archiviazione traslata

Questo sistema, a differenza del precedente, consente di avere uno storico dei dati per un periodo più lungo. Il sistema prevede che il nastro di un preciso giorno della settimana venga archiviato in luogo sicuro e NON riutilizzato la settimana successiva, così per le settimane successive traslando di un giorno il nastro che viene archiviato. Esempio:

	Lun	Mar	Mer	Gio	Ven	Sab	Dom
Settimana 1	31 Nastro 1	1 Nastro 2	2 Nastro 3	3 Nastro 4	4 Nastro 5	5 -	6 -
Settimana 2	7 Nuovo Nastro	8 Nastro 1	9 Nastro 2	10 Nastro 3	11 Nastro 4	12 -	13 -
Settimana 3	14 Nastro 5	15 Nuovo Nastro	16 Nastro 1	17 Nastro 2	18 Nastro 3	19 -	20 -
Settimana 4	21 Nastro 4	22 Nastro 5	23 Nuovo Nastro	24 Nastro 1	25 Nastro 2	26 -	27 -
Settimana 5	28 Nastro 3	29 Nastro 4	30 Nastro 5	1 Nuovo Nastro	2 Nastro 1	3 -	4 -

Con questo sistema a seconda del numero di nastri disponibili si possono archiviare i backup di un certo numero di settimane precedenti (con 20 nastri si hanno a disposizione i dati dell'ultima settimana e di un giorno specifico per ognuna delle 15 settimane precedenti). Naturalmente va tenuto in considerazione che i nastri che ruotano tutte le settimane vanno sostituiti con maggior frequenza. Quando non si avranno più nuovi nastri a disposizione, si inizierà a riutilizzare i nastri archiviati iniziando dal più anziano.

Nonno – Padre – Figlio (NPF)

Lo schema nonno-padre-figlio è un altro metodo molto utilizzato; esso utilizza il seguente schema di backup:

- giornaliero – sui nastri "figlio"
- settimanale – sui nastri "padre"
- mensile – sui nastri "nonno"

Il sistema è molto più potente della rotazione settimanale, ma richiede un maggior numero di nastri.

Per esempio, considerando il calendario sottostante:

Lunedì	Martedì	Mercoledì	Giovedì	Venerdì	Sabato	Domenica
	1 Figlio 1	2 Figlio 2	3 Figlio 3	4 Figlio 4	5 -	6 -
7 Nonno 1	8 Figlio 1	9 Figlio 2	10 Figlio 3	11 Figlio 4	12 -	13 -
14 Padre 1	15 Figlio 1	16 Figlio 2	17 Figlio 3	18 Figlio 4	19 -	20 -
21 Padre 2	22 Figlio 1	23 Figlio 2	24 Figlio 3	25 Figlio 4	26 -	27 -
28 Padre 3	29 Figlio 1	30 Figlio 2				

Questa strategia permette di ripristinare i dati dell'ultima settimana, di tutti i lunedì delle ultime 5 settimane, di tutti i primi lunedì di ogni mese a seconda di quanti nastri "nonno" sono in nostro possesso.

3. Implementazione di un sistema di backup

Cose da evitare in una buona strategia di backup

Ci sono svariati errori che possono ridurre l'efficacia di una strategia di backup:

- **Nastri fallati** – Se vengono utilizzati gli stessi nastri per un tempo troppo lungo, la probabilità che il nastro si degradi a tal punto da rendere illeggibili i dati è molto elevata. In ogni caso il software di backup è in grado di rilevare i nastri fallati nel momento in cui verifica i dati appena scritti.

- **Errori umani** – se viene utilizzato il nastro errato, la strategia risulterà inefficace. Per minimizzare questo tipo di errori può essere implementata una procedura scritta a cui attenersi strettamente ed utilizzare strumenti integrati nel software per istruire il personale addetto su quale nastro va inserito.
- **Archiviazione non sicura dei nastri** – I nastri devono essere posizionati in un luogo sicuro, lontano da fonti di calore e campi magnetici; i backup mensili dovrebbero essere portati in un luogo diverso, in modo da evitare ogni possibilità di perdita dovuta ad eventi catastrofici (se i nastri vengono archiviati nello stesso luogo in cui è posto il server, e questo luogo subisce un evento catastrofico avrò perso qualsiasi possibilità di recupero dei dati).

I passi per implementare un sistema di backup

Ora che si conoscono le basi, qual è il modo migliore ed economico per proteggere i dati? Ecco i 3 passi fondamentali:

1 – Scegliere e comprare l'unità di backup

La quantità di dati da salvare, nella maggioranza dei casi, necessita di un singolo nastro. Come prima cosa si dovrà calcolare la quantità di dati che dovranno essere salvati, aumentarla di una congrua percentuale e scegliere il sistema appropriato (vedi tabella a pagina 1).

Successivamente vanno acquistati un numero sufficiente di nastri a seconda della strategia di backup scelta. Lo schema Nonno-Padre-Figlio richiede un minimo di 10 nastri.

2 – Implementare il processo di backup, usando il software

Il prossimo passo è definire il calendario dei backup, etichettare i nastri, e configurare il software di backup in modo che i backup vengano eseguiti automaticamente all'orario selezionato. A seconda del software scelto avremo funzionalità più o meno evolute, che ci permettono di semplificare questa attività.

3 – Eseguire e controllare i backup continuativamente

I backup, per essere efficaci, vanno eseguiti e controllati quotidianamente. Un monitoraggio costante dell'attività di backup attraverso l'invio di mail con i 'log' del backup da parte del software agli operatori addetti, la loro lettura e una sollecita azione di correzione del problema sono fondamentali per un corretto funzionamento della strategia di backup. Per esempio: se il 'log' presenta degli errori nella verifica dei file salvati dovrà essere sostituito immediatamente il nastro incriminato.

4 – Eseguire la manutenzione dell'unità a nastro.

Una pulizia regolare e l'utilizzo del supporto corretto sono gli elementi fondamentali di una buona conservazione delle unità DDS e dei vostri dati. Non solo riducono le possibilità di guasto dell'unità, ma possono inoltre migliorare le prestazioni in fatto di velocità di trasferimento e l'affidabilità dell'unità, garantendo in tal modo la disponibilità dei dati in ogni momento

Le operazioni di pulizia sono semplici e richiedono pochissimo tempo. E' sufficiente inserire una cartuccia di pulizia all'interno dell'unità. L'unità carica automaticamente la cartuccia, pulisce le testine ed espelle la cartuccia.

- Pulire le testine con cadenza settimanale, utilizzando solo cartucce di pulizia consigliate. Non utilizzare panni, alcool isopropilico o altro, per pulire le testine.
- Sostituire la cartuccia dopo 50 cicli di pulizia oppure se l'unità espelle immediatamente la cartuccia senza effettuare un ciclo di pulizia, oppure se sul display a cristalli liquidi del caricatore automatico viene riportata la dicitura "Clean Fail" (pulizia non riuscita). Sull'etichetta della cartuccia di pulizia è presente un grafico con le modalità di registrazione.
- Per i caricatori automatici, includere una cartuccia di pulizia nel contenitore. Si consiglia di effettuare tale operazione come procedura di routine nell'ambito delle attività di backup.
- Oltre alle normali operazioni di pulizia, utilizzare una cartuccia di pulizia ogni volta che sul pannello anteriore dell'unità viene indicata la necessità di pulire le testine.
- Unità HP StorageWorks DAT 72: Se la cartuccia di pulizia non viene espulsa, è probabile che sia scaduta. In questo caso, premere il pulsante di espulsione, gettare la cartuccia di pulizia e ripetere l'operazione con una nuova cartuccia.

5 – Eseguire periodicamente un test di ripristino dei dati.

Inoltre consigliamo di effettuare periodicamente (circa ogni sei mesi) una prova di ripristino dati, in modo tale da verificare la qualità e l'affidabilità dei supporti usati; e a fine anno di sostituirli completamente in modo da evitare una eccessiva usura nel caso di backup intensivi.

Un ripristino di prova può evidenziare problemi dell'hardware che non vengono messi in luce durante la verifica Software.

Si ricorda infine che la legge 196/03 prevede espressamente l'obbligo di adozione di procedure per la custodia di copie di sicurezza dei dati, e prevede sanzioni per chi non adotta tali strumenti.