

INGEGNERIA DEI DATI

La Regola del 3-2-1

3 copie • 2 supporti • 1 copia off-site • Verifica



Architettura di backup resiliente



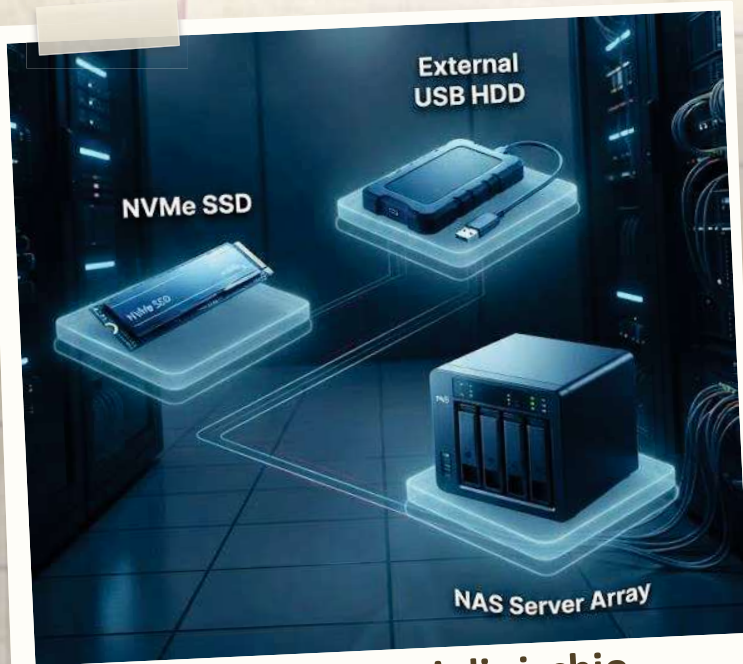
Anti-perdita dati

Introduzione

Questo documento espande i concetti della guida di base, fornendo specifiche tecniche, metriche di disaster recovery e considerazioni architetturali avanzate per blindare l'infrastruttura dati contro qualsiasi vettore di perdita.

1 • Tre copie

Il concetto di triplicazione dei dati non nasce da un principio di ridondanza superflua, ma dalla necessità di isolare i dati rispetto a vettori di rischio eterogenei.



Analisi dei vettori di rischio

[RISCHIO]

Copia 1

Risiede sul volume principale e costituisce il file di lavoro quotidiano soggetto a potenziali corruzioni.

Copia locale

Supporto indipendente che mitiga i guasti meccanici o i crash di filesystem del volume principale.

Terza copia

Isolamento definitivo per prevenire la propagazione di ransomware e comandi di cancellazione massiva.

Immutabilità

Architettura air-gapped o WORM per impedire che un attacco informatico comprometta i backup remoti.

[ISOLAMENTO LOGICO]

I malware fileless e le minacce silenti possono propagarsi ai dischi secondari se rimangono costantemente montati e accessibili in scrittura dal sistema operativo.

Parametri e supporti

RPO—Recovery Point

Quantità massima di dati tollerabile che può andare persa a causa di un causa di un incidente, determinata dalla frequenza.

RTO—Recovery Time

Il tempo necessario per ripristinare i sistemi operativi e i dati a seguito di seguito di un guasto con storage ad alta velocità.



Eterogeneità dei supporti

Memorie

SSD NVMe

Disco primario interno ad alte prestazioni per la gestione rapida dei dati di dei dati di lavoro quotidiani.

NAS

Array RAID di dischi meccanici NAS-grade per variare la tecnologia di scrittura e ridurre i guasti.

Nastro / USB — Off-site

Sistema di archiviazione esterno utile per la delocalizzazione geografica e la continuità aziendale.

*Regola pratica: **SSD NVMe** per il lavoro quotidiano, **NAS RAID** per la **RAID** per la copia locale, **Cloud o disco esterno** per la delocalizzazione delocalizzazione off-site.*

2 • Due supporti

L'eterogeneità dei supporti di memorizzazione previene il rischio di rischio di single point of failure tecnologico o legato all'usura dovuta al tempo di produzione.

[ARCHITETTURA]

Hardware

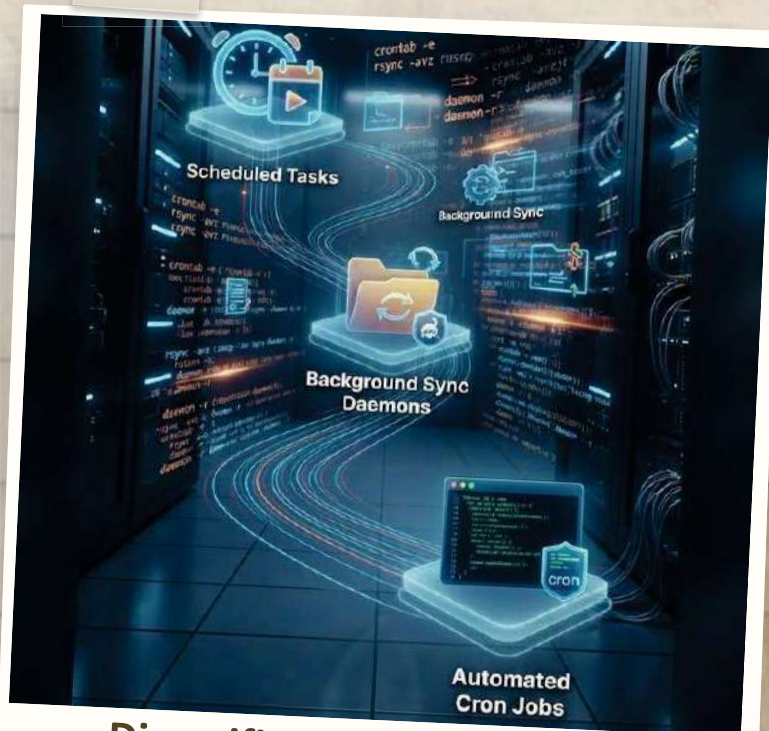
Affiancare al disco primario interno un supporto di tipo differente significa variare la tecnologia di scrittura.

File system diversi

NTFS/APFS per il client e ext4/ZFS su NAS Linux per proteggere contro la corruzione logica dei metadati.

Bit-rot

Prevenzione contro errori di bit-rot silenziosi e anomalie del controller SATA o NVMe locale.



Diversificazione dei supporti

Le regole d'oro del backup

Eterogeneità: tecnologie differenti.

Separazione: adottare file system differenti per prevenire la corruzione logica dei metadati.

Delocalizzazione: garantire sempre una copia off-site contro incendi o furti fisici.

[ERRORI RICORRENTI IN AZIENDA]

Affidarsi a una sola copia di sicurezza, mantenere i dischi di backup sempre montati e accessibili, oppure ignorare la verifica periodica dei dati salvati.

3 • Copia fuori sede

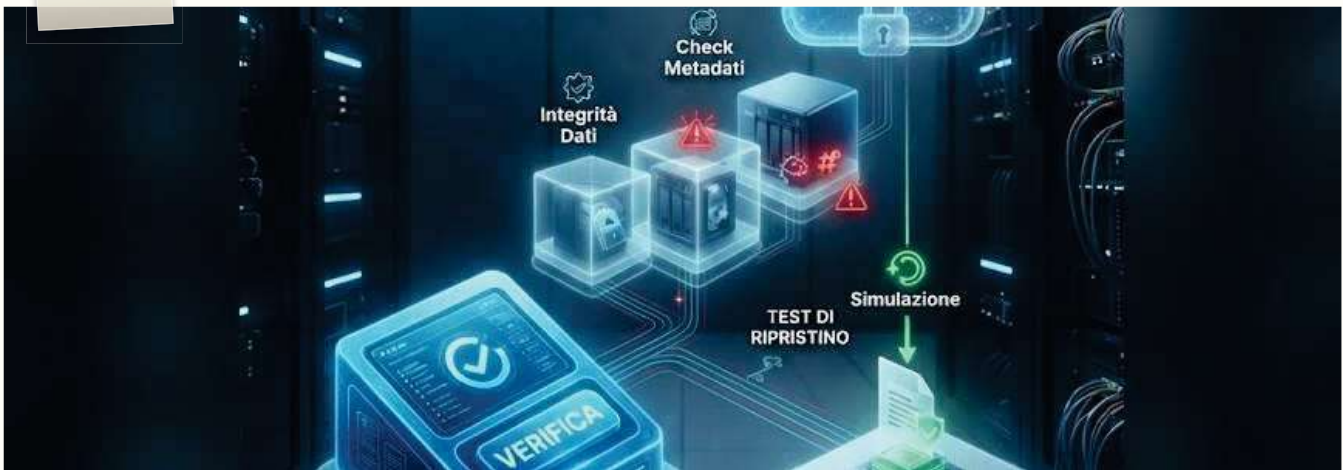
La delocalizzazione geografica è l'unico baluardo contro i disastri fisici totali e le compromissioni perimetrali dell'infrastruttura locale aziendale.

Copia Off-Site

Cloud storage criptato o disco cifrato ruotato fisicamente in un'altra locazione.

Continuity

Garantisce la continuità aziendale a fronte di eventi catastrofici locali.



Delocalizzazione geografica della copia di sicurezza

[MITIGAZIONE RISCHI AMBIENTALI]

Eventi come incendi, sbalzi di tensione catastrofici, furti fisici dell'hardware o eventi alluvionali azzerano l'operatività locale e richiedono una strategia remota.

Incendi e alluvioni — Sede

Distruzione totale dell'hardware locale e dei supporti di memorizzazione memorizzazione primari presenti in ufficio.

Cloud Criptato — Off-site

Storage remoto sicuro accessibile via rete per il ripristino rapido dei dati critici dei dati critici aziendali.

Rotazione Dischi — Backup

Dischi cifrati trasportati fisicamente in altra locazione per garantire un un isolamento totale.

4 • Script

L'intervento umano è statisticamente l'anello più debole di qualsiasi qualsiasi procedura di sicurezza informatica: l'automazione elimina le elimina le dimenticanze.

Task manuali

0%

affidati alla memoria umana: rischio rischio elevato di errori e dimenticanze.

Task schedulati

100%

gestiti da servizi di sistema operativo e script incrementali silenziosi.

Eccezioni

Notifiche e Webhook

Segnalazione tempestiva di fallimenti nell'esecuzione dei task, esaurimenti di esaurimenti di spazio o errori di permessi.

Daemon in background

Esecuzione programmata tramite Task Scheduler su Windows o cron jobs su ambienti Unix/Linux per garantire continuità.

Un backup non automatizzato è un backup dimenticato.

5 • Verifica periodica

Un backup non testato è, dal punto di vista logico, un non-backup. L'illusione di sicurezza porta spesso a scoprire l'inefficacia del sistema solo nel momento della massima emergenza, rendendo indispensabile un protocollo di test mensile su ambiente di staging.



www.sunrisetechnology.it

6 • Protocollo di test

Il processo di verifica deve simulare un ripristino reale estraendo estraendo campioni di dati significativi come file di database, archivi archivi contabili complessi e immagini di sistema.



Simulazione ripristino dati

VERIFICA INTEGRITÀ

È necessario verificare periodicamente che i client di backup non abbiano interrotto la sincronizzazione a causa di token scaduti.

***Token scaduti** — bloccano la sincronizzazione.*

***Modifiche policy** — variazioni storage.*

***Saturazione disco** — esaurimento esaurimento spazio.*

Risultato: dati sempre ripristinabili in in caso di emergenza.



La sicurezza dei dati è un processo continuo

Esplora altri trucchi e tutorial su
www.sunrisetechnology.it →