www.sunrisetechnology.it

BACKUP SENZA SORPRESE

Backup su cloud avanzato

Versionamento · Sync · Restore · Sicurezza

Backup non testato = rischio

...dal file al ripristino

Introduzione

Un backup cloud efficace non è un semplice salvataggio remoto: richiede trasmissione cifrata, archiviazione ridondata e verifiche periodiche. Questo allegato raccoglie parametri operativi e cautele di sicurezza per proteggere i dati.

1 · Capire il backup

Un vero backup cloud cifra i file in transito con TLS/HTTPS e li conserva in archivi ridondati. Il versionamento mantiene gli stati incrementali, così si può tornare a una versione integra.

Dati al sicuro

[DUE PILASTRI]

TLS

Cifra i file in transito, di solito con TLS/HTTPS, per evitare intercettazioni.

Versionamento

Conserva i singoli stati incrementali, a differenza di un mirror che sovrascrive il file modificato.

Restore

Dopo un attacco ransomware si ripristina la versione integra dal pannello del provider.

Anti-ransomware

Gli stati incrementali precedenti restano disponibili nel pannello di controllo del provider.

[IN PRATICA]

Un mirror in tempo reale sovrascrive il file modificato; il versionamento no e permette di tornare indietro.

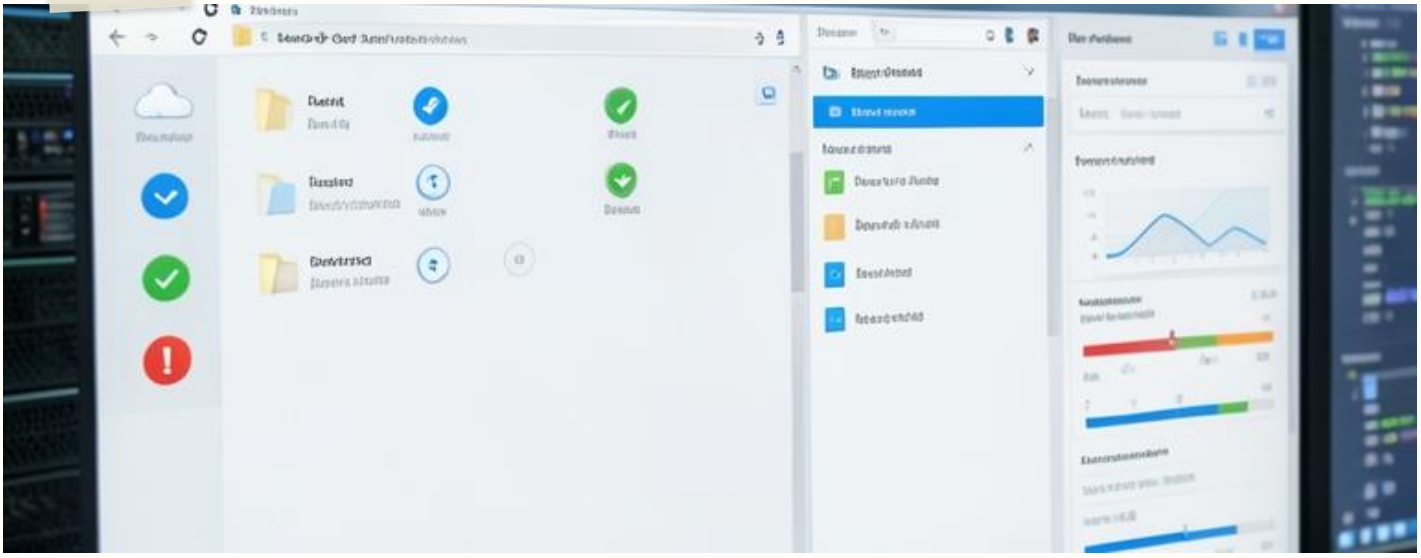
Cosa escludere

Cache e temporanei

Vanno esclusi cache dei browser e file temporanei come Pagefile.sys e Hiberfil.sys: non hanno valore.

File intermedi

Directory di build e file intermedi di compilatori o software di montaggio video non vanno salvati.



Cosa sincronizzare

Database attivi

Rischio

I database in uso (.mdf o .sqlite aperti) rischiano di risultare corrotti durante la scrittura.

VSS

Volume Shadow Copy: i software di backup che lo supportano gestiscono i database anche mentre sono in uso.

Dump dedicati o VSS

Per i database attivi servono dump dedicati o backup con supporto VSS, non la semplice sincronizzazione.

> *Regola pratica: escludi cache, temporanei e build, proteggi i database con dump o VSS, sincronizza solo ciò che serve davvero.*

3 · Sincronizzazione

La configurazione del client bilancia comodità d'accesso e limiti fisici dell'hardware locale: spazio su disco e banda vanno gestiti con cura.

[MODALITÀ]

On-Demand

Mostra l'intero albero delle cartelle senza occupare byte sul disco; i file si scaricano solo all'apertura.

Sync totale

Scarica localmente tutti i file: occupa spazio sul disco rigido del dispositivo.

Banda

Limiti di upload e download evitano che la sincronizzazione saturi la connessione negli orari di lavoro.

Sincronizzazione sotto controllo

Le regole d'oro della sync

Banda: *limiti di upload e download.*

Modalità virtuale: *i file si scaricano al momento dell'apertura e possono essere rilasciati automaticamente dopo l'uso.*

Orari di lavoro: *evita che il sync continuo saturi la connessione aziendale o domestica.*

[SINCRONIZZAZIONE CONTINUA]

Il motore monitora il file system tramite hook del sistema operativo (ReadDirectoryChangesW in Windows, inotify in Linux). I file grandi vengono divisi in chunks con hash e si carica solo ciò che cambia.

5 · Test di ripristino

Il test di restore è l'unico modo per validare l'integrità della catena di backup: senza prove periodiche, una copia che sembra corretta può rivelarsi illeggibile quando serve.

Test trimestrale

Ogni trimestre: scarica file critici su un dispositivo pulito o alternativo.

Monitoraggio

Molti client falliscono in silenzio: controlla spesso il log errori.

Restore: valida la catena di backup

[COSA VERIFICARE NEL RESTORE]

Un campione significativo, come archivi contabili o database, va scaricato e controllato per leggibilità e integrità strutturale dei dati.

Cartella di test pulita

Si crea la cartella su un dispositivo pulito o alternativo, dove scaricare i file di prova.

Campione di file critici

Si scarica un campione significativo, ad esempio archivi contabili o database, scegliendo i dati davvero critici.

Apri e verifica file

Si verifica che i file scaricati siano leggibili e integri: il backup è...

6 · Accessi sicuri

La sicurezza del cloud dipende dalla rigorosità delle policy d'accesso: protezione della dashboard del provider e permessi limitati riducono il danno di un account compromesso.

MFA / 2FA
TOTP / FIDO2
per la dashboard, mai via SMS.

Minimo privilegio
Sola lettura
o accesso a sottocartelle: un account compromesso non cancella tutto.

Autenticazione forte

TOTP o chiavi FIDO2/WebAuthn

L'accesso alla dashboard web va protetto con TOTP tramite app authenticator o, preferibilmente, con chiavi di sicurezza fisiche.

SMS esclusi: SIM swapping

Gli SMS vanno esclusi per il rischio di SIM swapping: l'autenticazione basata su TOTP o su chiavi FIDO2/WebAuthn resta la scelta più solida per la dashboard del provider.

Una dashboard senza 2FA non è una politica di sicurezza.

7 · Checklist iniziale

Prima di affidarti al backup, controlla che sia configurata l'esclusione di file temporanei, cache e database attivi. Imposta limiti di banda di upload e download per non penalizzare la rete e attiva la modalità File On-Demand per ottimizzare lo spazio sui dischi locali. Una mappatura errata delle directory rischia di compromettere le performance del client.

7 · Verifiche avanzate

Gli ultimi controlli chiudono il cerchio: dopo configurazione, sincronizzazione e restore, restano da verificare la conservazione delle versioni, la cadenza dei test e la protezione delle credenziali.

Dati sotto controllo

CHECKLIST FINALE

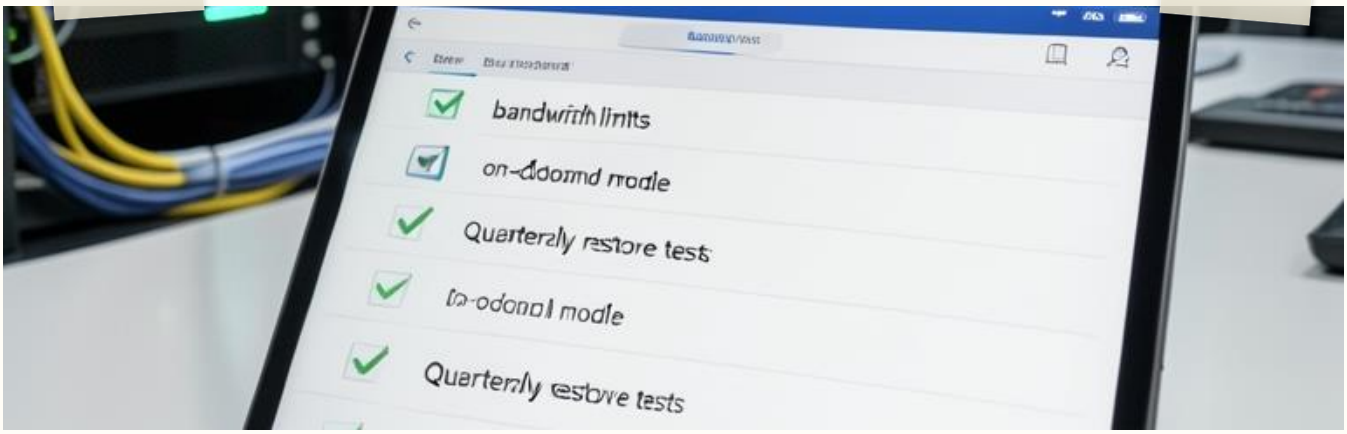
Verifica quanti giorni o quante versioni passate conserva il piano, programma a calendario il test trimestrale e usa 2FA con app o hardware.

***Versioni** — controlla quanto storico conserva il piano.*

***Restore** — test di ripristino a calendario ogni trimestre.*

***Accessi** — password master complessa e 2FA su app o hardware.*

Risultato: dati ripristinabili al bisogno.



Un backup che si testa è un backup affidabile

Esplora altri trucchi e tutorial su

www.sunrisetechnology.it →

Creato con il supporto di strumenti IA | © Sunrise Technology