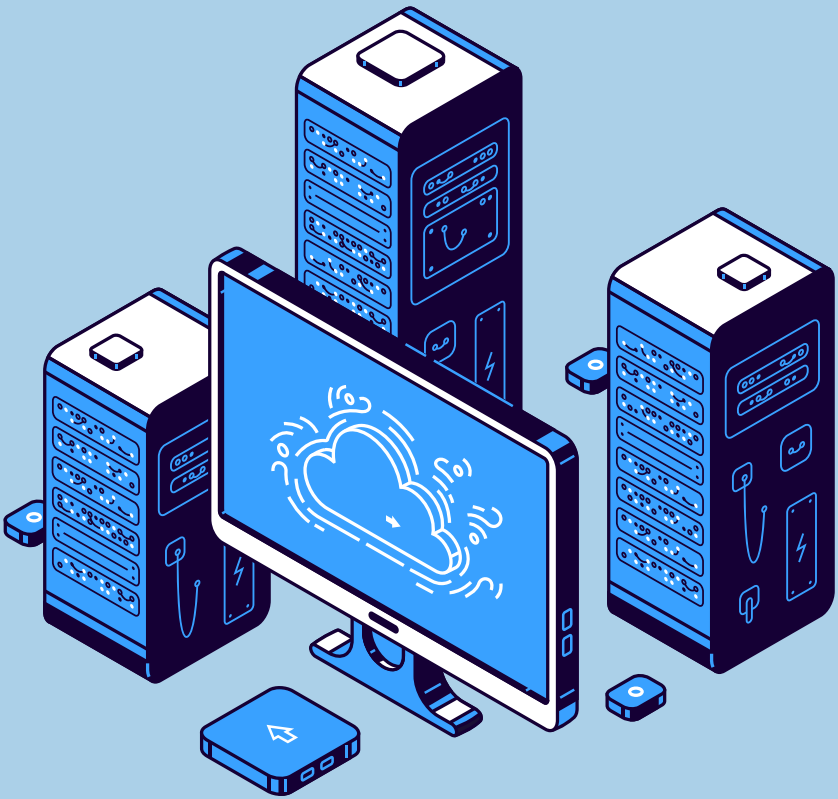
( )register.it

COME METTERE IL PROPRIO
SERVER IN SICUREZZA



Indice

1. Introduzione.

2. L'importanza di mettere in sicurezza il proprio server
   2.1 Disastri aziendali e prevenzione
   2.2 La protezione dei dati critici

3. La protezione dei dati critici
   3.1 Tipologie di backup e scelta del migliore
   3.2 Come attivare un backup efficiente

4 Come attivare un backup efficiente
   4.1 Cos'è il RAID e perché è importante
   4.2 Verificare lo stato del RAID

5 Verifica dello stato dei dischi
   5.1 Intervenire tempestivamente in caso di problemi

6. Conclusioni

1

Introduzione

In un'epoca in cui la tecnologia gioca un ruolo cruciale nella nostra vita quotidiana, **assicurarsi che le informazioni siano al sicuro è diventato un aspetto fondamentale** per la sopravvivenza e il successo di qualsiasi azienda.

Disastri e incidenti aziendali possono verificarsi in qualsiasi momento, spesso in modo inaspettato e improvviso. La corretta **gestione del proprio server e il corretto salvataggio dei dati** tramite un efficiente sistema di backup sono strumenti essenziali per garantire la continuità operativa, minimizzare le perdite di dati e ridurre i tempi di ripristino dell'operatività.

In questo eBook esploreremo insieme l'importanza di **mettere in sicurezza il proprio server**, le **strategie per attivare un backup efficace** e come monitorare lo **stato del RAID e dei dischi** del proprio server.

2

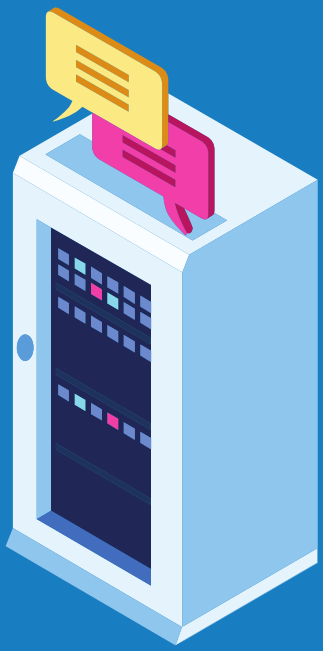
Mettere in sicurezza il proprio server

In un mondo digitale in continua evoluzione, le minacce informatiche sono all'ordine del giorno e possono compromettere la sicurezza delle informazioni custodite nei server delle aziende.

Questo capitolo tratta proprio dell'importanza di mettere in sicurezza il proprio server e si concentra su come evitare disastri aziendali e proteggere i dati critici.

Disastri aziendali e prevenzione

I disastri aziendali possono accadere in qualsiasi momento e possono causare danni significativi ai dati e ai sistemi IT. Per **ridurre il rischio** di disastri e garantire la continuità delle operazioni aziendali, è importante adottare misure di prevenzione, ecco le più importanti da seguire:



- Pianificare un Piano di Ripristino del Disastro (DRP).
- Implementare misure di sicurezza per proteggere i server e le infrastrutture IT.
- Effettuare test e audit periodici della sicurezza del server.

Un DRP è un documento che definisce le azioni da intraprendere nel caso si verifichi un disastro. Il DRP dovrebbe includere la valutazione delle possibili minacce, l'identificazione dei sistemi critici da proteggere, la definizione di processi e procedure di ripristino e la formazione del personale su tali processi.

Disastri aziendali e prevenzione

Le misure di sicurezza possono aiutare a **proteggere i server e le infrastrutture IT** dall'accesso non autorizzato e dai rischi ambientali.

Alcune delle misure di sicurezza più comuni includono l'utilizzo di f**irewall, software antivirus e anti-malware**, l'aggiornamento costante dei sistemi operativi e delle applicazioni, la gestione delle autorizzazioni degli utenti e la protezione dei server attraverso soluzioni di rilevazione delle intrusioni e di crittografia.

È importante effettuare test e audit periodici della sicurezza del server e delle misure di prevenzione adottate, al fine di verificare l'efficacia delle soluzioni implementate e individuare eventuali aree di miglioramento.

Adottando queste misure di prevenzione, le aziende possono ridurre il rischio di disastri e garantire la continuità delle operazioni aziendali.

La protezione dei dati critici

La protezione dei dati critici è fondamentale per garantire la continuità delle operazioni quotidiane della tua azienda o organizzazione. I dati critici sono quelle informazioni che, se perse o compromesse, potrebbero causare gravi problemi operativi, legali e finanziari.

Ecco alcuni suggerimenti per proteggere i dati critici:

- **Identifica e classifica i dati critici:** Devi sapere quali sono le informazioni più importanti, dove sono archiviate e come vengono utilizzate all'interno della tua infrastruttura IT.

- **Valuta i rischi che riguardano la sicurezza dei dati**: Ciò include sia le minacce esterne, come gli attacchi informatici e il furto di dati, sia quelle interne, come la perdita accidentale di informazioni o l'errore umano.

- **Implementa misure di sicurezza per proteggere i dati critici:** Alcune delle misure più efficaci includono backup regolari, crittografia dei dati, controllo degli accessi, formazione degli utenti e aggiornamenti e patch di sicurezza.

Seguendo questi suggerimenti, potrai minimizzare i rischi associati alla protezione dei dati critici, garantire la sicurezza delle informazioni e assicurare la continuità operativa della tua attività.

La protezione dei dati critici

Ecco alcuni dettagli aggiuntivi su ciascuna misura di sicurezza:

- **Backup regolari:** Eseguire backup regolari dei dati critici è essenziale per garantire che sia possibile ripristinare le informazioni perdute o compromesse. È consigliabile adottare una politica di backup combinata, che preveda sia backup locali che in cloud, in modo da avere più punti di ripristino in caso di problemi.

- **Crittografia dei dati:** Crittografare i dati critici garantisce che, anche se venissero intercettati da terzi non autorizzati, questi rimangano inutilizzabili.

- **Controllo degli accessi:** Limitare l'accesso ai dati critici solo alle persone autorizzate riduce il rischio di perdita accidentale o intenzionale di informazioni. Implementa politiche di controllo degli accessi basate sulle esigenze specifiche del tuo contesto aziendale.

- **Formazione degli utenti:** Gli errori umani sono una delle principali cause di perdita di dati. Formare adeguatamente il personale sulla gestione sicura delle informazioni può ridurre significativamente rischi e problemi.

- **Aggiornamenti e patch di sicurezza:** Mantieni sempre aggiornati i sistemi operativi, le applicazioni e il firmware del tuo server, per proteggere i dati critici dalle vulnerabilità note.

3

Backup per proteggere e preservare i tuoi dati

Il backup dei tuoi dati è fondamentale per **garantire la sicurezza delle informazioni** e per prevenire possibili perdite dovute a errori umani, guasti hardware, attacchi informatici o eventi imprevisti.

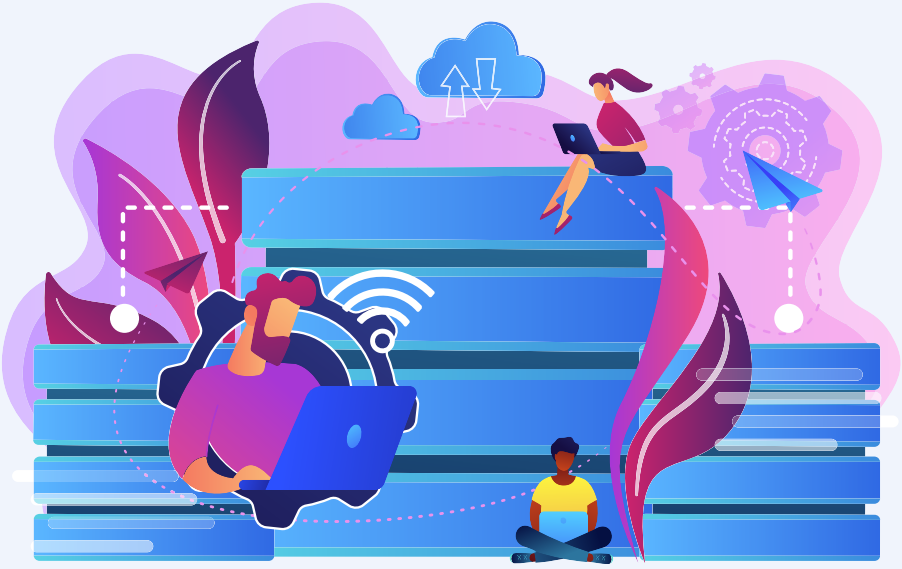
Negli scenari più disastrosi, la mancanza di un adeguato backup può portare alla **perdita di dati vitali** e influire negativamente sulla continuità delle operazioni aziendali.

In questo capitolo, esploreremo le diverse tipologie di backup, come scegliere il migliore in base alle tue esigenze e come attivarlo in modo efficiente.

Tipologie di backup e scelta del migliore

Quando si tratta di mettere in sicurezza i dati del tuo server, è fondamentale conoscere le diverse tipologie di backup disponibili e scegliere quella più adatta alle tue esigenze. In questo modo, potrai assicurarti di avere una copia aggiornata e sicura dei tuoi dati, pronta per essere ripristinata in caso di necessità.

Le tipologie di backup più comuni sono le seguenti:



- **Backup completo:** È una copia di tutti i dati presenti sul server. Richiede più tempo e spazio di archiviazione rispetto ad altri tipi di backup, ma offre il vantaggio di avere una copia completa di tutti i dati.

- **Backup incrementale:** È una copia solo dei dati che sono stati modificati dall'ultimo backup completo o incrementale. Richiede meno tempo e spazio di archiviazione rispetto a un backup completo, ma può rallentare il processo di ripristino dei dati, poiché è necessario ripristinare l'ultimo backup completo e tutti i backup incrementali successivi.

- **Backup differenziale:** È simile al backup incrementale, ma copia solo i dati modificati dall'ultimo backup completo. Richiede più tempo di un backup incrementale, ma il processo di ripristino è più rapido, poiché è necessario ripristinare solo l'ultimo backup completo e l'ultimo backup differenziale.

La scelta del tipo di backup più adatto dipende dalle esigenze specifiche dell'azienda, tra cui le dimensioni del server, la frequenza delle modifiche ai dati e la velocità di recupero richiesta in caso di problemi. Per scegliere il metodo di backup più adatto alle tue esigenze, considera i seguenti aspetti:

- **Budget:** Quanto sei disposto a investire nella soluzione di backup?

- **Frequenza delle modifiche ai dati:** Se i dati sul tuo server cambiano frequentemente, potresti optare per backup incrementali o differenziali.

- **Velocità di ripristino:** Se la velocità è un fattore fondamentale, potresti optare per una combinazione di backup completi e differenziali.

In ogni caso non esiste una soluzione di backup "perfetta" per tutte le situazioni, l'importante è selezionare il metodo più adatto alle tue necessità specifiche e monitorarlo costantemente per garantire la protezione dei tuoi dati.

Come attivare un backup efficiente

Per attivare un backup efficiente dei tuoi dati, è essenziale seguire alcune linee guida e adottare le migliori pratiche.
Ecco alcuni passi fondamentali:

1. **Valuta le tue esigenze:** prima di tutto, devi capire quali dati sono critici per la tua attività e quanto spesso necessitano di essere sottoposti a backup.
2. **Scegli il dispositivo di backup:** è importante selezionare un dispositivo di backup che sia affidabile e sufficientemente capiente per archiviare tutti i dati che desideri proteggere.
3. **Utilizza un software di backup:** per rendere l'intero processo di backup più semplice ed efficiente, è consigliabile utilizzare un software di backup affidabile e facile da usare.
4. **Pianifica i backup:** per assicurarti che i tuoi dati siano sempre protetti, è fondamentale pianificare regolarmente i backup. Ricorda che più spesso esegui il backup dei tuoi dati, minore sarà il rischio di perdita di dati in caso di evento catastrofico.
5. **Verifica l'integrità dei backup:** non basta eseguire i backup, è altrettanto importante assicurarsi che siano integri e funzionanti.
6. **Proteggi i tuoi backup:** per garantire la sicurezza dei tuoi dati, è essenziale proteggerli con cifratura e password. Inoltre, è altamente raccomandabile conservare una copia dei backup in una posizione geograficamente diversa.

Seguendo questi consigli, sarai in grado di attivare un backup efficiente e affidabile per proteggere i tuoi dati e garantire la continuità operativa della tua attività.

4

Controllare lo stato del RAID del server

IUn elemento cruciale per garantire la sicurezza del tuo server e la protezione dei dati e delle informazioni in esso contenute è il controllo e la gestione dello stato del RAID del server.

In questo capitolo, ci concentreremo sul RAID, sulla sua importanza e su e come verificare il suo stato in maniera corretta.

Cos'è il RAID e perché è importante

Il **RAID, acronimo di Redundant Array of Independent Disks,** è una tecnologia di storage che ti permette di unire più dischi rigidi in un'unica unità logica, migliorando così le prestazioni del sistema e garantendo una maggiore protezione dei dati.

- **RAID 1 (mirroring):** crea una copia esatta dei dati su due dischi rigidi, garantendo una maggiore affidabilità in caso di guasto di uno dei due dischi.
- **RAID 5 (striping con parità):** distribuisce i dati e le informazioni di parità su tutti i dischi del sistema, garantendo sia una maggiore velocità di accesso ai dati sia una ridondanza per proteggerli.
- **RAID 10 (minimo 4 dischi):** crea 2 o più coppie di dischi in RAID 1 in modo da aumentare la capacità totale e le prestazioni, senza perdere la ridondanza.

Cos'è il RAID e perché è importante

Avere un sistema RAID attivo sul tuo server è fondamentale per due motivi principali:

- **Sicurezza dei dati:** Il RAID ti permette di proteggere i dati memorizzati sul tuo server, riducendo il rischio di perdite di dati in caso di guasto di un disco rigido. La perdita di dati può avere gravi conseguenze per la tua attività, come interruzioni delle operazioni, costi di recupero e potenziali azioni legali da parte di clienti o partner.

- **Prestazioni del sistema:** Il RAID migliora le prestazioni del tuo server, garantendo tempi di accesso ai dati più rapidi e un migliore bilanciamento del carico tra i dischi rigidi. Questo si traduce in una maggiore efficienza nell'elaborazione dei dati e nella gestione delle applicazioni, con conseguente migliore qualità del servizio per i tuoi clienti e utenti.

Scegliere il livello RAID più adatto alle tue esigenze dipende da diversi fattori, tra cui il budget, la quantità di dati da archiviare, le prestazioni richieste e la tolleranza al rischio.

Se stai cercando un sistema RAID che offra una maggiore protezione dei dati, il RAID 1 è la soluzione migliore. Se stai cercando un sistema RAID che offra prestazioni migliori, il RAID 5 o il RAID 10 sono le soluzioni migliori.

Verificare lo stato del RAID

Per verificare lo stato del RAID del tuo server e mantenerlo il in perfette condizioni, è fondamentale seguire alcune linee guida e procedure, vediamo insieme quali sono:

Innanzitutto, è importante **effettuare verifiche regolari sul RAID**, preferibilmente ogni settimana o almeno una volta al mese. In questo modo si può individuare tempestivamente eventuali anomalie o guasti e intervenire prontamente per risolverli.

Inoltre, è consigliabile **tenere sotto controllo le informazioni sullo stato dei dischi rigidi** che compongono il sistema RAID, tramite appositi software di monitoraggio che consentono di verificare il grado di usura e di prevenire eventuali malfunzionamenti.

Ogni produttore di server fornisce anche il software per Linux e Windows per la gestione e il montoraggio di RAID, hardware e firmware.

Una volta intallato il software è possibile verificare lo stato del raid e del controller raid con i seguenti comandi, da eseguire nella shell in caso di linux o in una powershell aperta come amministratore nel caso sia Windows:

Verifica del controller raid:

Comando:

omreport storage controller

Output:

Controller
ID : 0
Status : Ok
Name : PERC H730 Mini
Slot ID : Embedded
State : Ready
Firmware Version : 25.5.6.0009
.....

Importante controllare lo Status.

Verifica del RAID:

Comando:

omreport storage vdisk controller=0

Output:

List of Virtual Disks in the System

Controller PERC H730 Mini (Embedded)
ID : 0
Status : Ok
Name : Virtual Disk0
State : Ready
Hot Spare Policy violated : Not Assigned
Encrypted : No
Layout : RAID-1
Size : 278.88 GB (299439751168 bytes)
.....

Controllare che lo "Status" sia Ok e che lo "State" sia Ready. un'altra buona pratica è quella di tenere sempre aggiornati i firmware e i driver dei componenti del server, per migliorare le prestazioni e la stabilità del sistema RAID.

5

Verifica dello stato dei dischi

Oltre a un buon sistema di backup e alla verifica dello stato del RAID, è importante prestare attenzione anche allo stato dei dischi del tuo server.
Per la verifica dello stato dei dischi è possibile lo stesso software usato per la verifica del RAID. Anche in questo caso i comandi sono da eseguire nella shell in caso di linux o in una powershell aperta come amministratore nel caso sia Windows:

Comando:

```
omreport storage pdisk controller=0
```

Output:

```
List of Physical Disks on Controller PERC H730 Mini (Embedded)

Controller PERC H730 Mini (Embedded)
ID                : 0:1:0
Status            : Ok
Name              : Physical Disk 0:1:0
State             : Online
Power Status      : Spun Up
Bus Protocol      : SAS
Media             : HDD
.....
```

Nell'output ci saranno tutti i dischi del server, controllare per ognuno di essi che lo "Status" sia Ok e lo "State" Online.

Intervenire tempestivamente in caso di problemi

Ora che hai configurato il monitoraggio dello stato del disco, è fondamentale agire prontamente nel momento in cui si presentano problemi con uno dei dischi del server.
Ricorda che **agire tempestivamente può fare la differenza** per proteggere i dati e garantirne la disponibilità.

Se il monitoraggio del pannello rileva un problema, questi sono alcuni passi che puoi seguire per affrontare ed eventualmente risolvere il problema:

1. Valuta l'entità del problema: È importante capire se il problema è temporaneo o se è il sintomo di un problema più grave.
2. Effettua un backup immediato dei dati: Se noti che uno dei dischi presenta problemi, assicurati di eseguire un backup immediato dei dati presenti sul server.
3. Contatta il supporto tecnico: Non appena individui un problema, contatta il nostro supporto tecnico. I nostri operatori potranno aiutarti a identificare la causa del problema e adottare le misure necessarie per risolverlo.
4. Esegui la manutenzione del disco: A seconda dell'entità del problema e delle indicazioni del supporto tecnico, potresti dover eseguire operazioni di manutenzione sul disco.
5. Monitora attentamente i progressi: Una volta risolto il problema, continua a monitorare lo stato del disco per assicurarti che il problema non si ripresenti in futuro. Il monitoraggio costante ti aiuterà a prevenire eventuali problemi futuri e a mantenere il tuo server e i tuoi dati al sicuro.

6

Conclusioni

In queste ebook abbiamo esplorato l'importanza di mettere al sicuro il proprio server e le informazioni che ospita.

Ora che sei arrivato alla conclusione tocca a te mettere in pratica tutti i suggerimenti che ti abbiamo dato nel corso dei vari capitoli.

Ricorda, **mettere al sicuro il tuo server e le informazioni che ospita è fondamentale per la protezione e il successo della tua attività**. Ora sei equipaggiato con gli strumenti e le conoscenze per affrontare queste sfide e assicurarti la massima protezione dei tuoi dati e la continuità delle tue operazioni.

Non aspettare che sia troppo tardi: metti subito in pratica questi preziosi suggerimenti per proteggere il tuo server e i tuoi dati, garantendo un futuro più sicuro e sereno per la tua azienda.


( )register.it