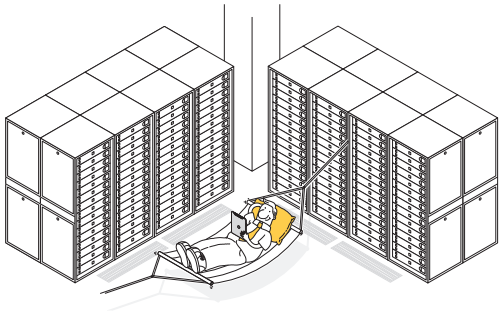
Disaster Recovery vs Business Continuity: facciamo chiarezza



seeweb
THINK CLOUD

Indice

Premessa

Come Seeweb abbiamo avuto occasione di notare come sia prassi comune fare confusione tra il concetto di *business continuity* e quello di *disaster recovery*.

Non di rado, clienti preoccupati di subire guasti tecnici o perdita di dati, al momento del progetto della propria infrastruttura Cloud richiedono, senza avere sempre un'idea precisa, una continuità di servizio che spesso associano al concetto del "nessun fermo, mai" e alla disponibilità dei server su più data center. Sempre non di rado, chiedono di avere i servizi online in maniera continuativa e allo stesso tempo "tutti i dati replicati dall'altra parte".

Non sapendo che così stanno puntando a una continuità di servizio che non ha però a che fare con il "recovery" e che con quest'ultimo spesso non è conciliabile.

In cosa consiste il disaster recovery (DR)

Si tratta del processo che rende possibile recuperare i dati in caso di disastro.
Adottare una politica di "disaster recovery" vuol dire avere un sito secondario in cui salvare tutti i dati, potendo quindi recuperare i propri database in caso di catastrofi naturali (incendi, uragani, terremoti, o qualsiasi evento naturale o doloso possa mettere a rischio la funzionalità di un data center).

Ma il DR non riguarda solo i dati, esso riguarda anche il resto dei sistemi. Un piano di DR deve quindi includere sia i dati salvati sia anche tutto quanto serve per ripristinare il servizio in caso di disastro.

Nel caso di un progetto di disaster recovery, molta importanza riveste la pianificazione di *come* i dati verranno recuperati affinché, in caso di disastro, siano nuovamente accessibili.
Da notare che, in caso di effettivo disastro, **al momento del suo verificarsi i dati non saranno accessibili, ma dovranno prima essere recuperati**, e la velocità alla quale verranno recuperati dipende esclusivamente dalla pianificazione dell'infrastruttura e dai processi che ne sono alla base, e che saranno stati preventivamente testati.

> Obiettivo primario della disaster recovery è quindi assicurare che i dati non vadano persi, lasciando in secondo piano la possibilità che siano, per un determinato lasso di tempo, inaccessibili.

La preoccupazione principale del cliente che implementa un piano di disaster recovery è l'**RTO** o "recovery time objective" ossia la durata massima del fermo, che va stabilita al momento della pianificazione: in tal modo, l'azienda sa già in anticipo a quanto tempo di disagio va incontro avendo progettato la DR in modo da tollerare una certa durata massima di downtime.

L'**RPO** o "recovery point objective" stabilisce invece la quantità massima di dati a cui un'azienda è disposta a rinunciare a seguito di un problema.
Anche se RPO si riferisce a una quantità di dati si misura in unità di tempo, come l'RTO, quindi l'ammontare dei dati persi dipende da quanti se ne producono per unità di tempo.

Le suddette definizioni in accordo con quanto definito dalla norma ISO 22300, che formalizza il vocabolario utilizzato dalla norma ISO 22301, relativa alla business continuity

Oltre che stabilire durante il progetto RTO ed RPO è necessario, al fine di realizzare un DR geografico, dislocare i servizi ICT in nodi geograficamente distribuiti con una certa distanza l'uno dall'altra. La distanza minima del sito secondario non è stabilita in maniera netta, e più che delle regole ci sono delle "best practise".

Come indica il *Disaster Recovery Journal**, "*there is no rule of thumb when it comes to the appropriate distance between your data center and your recovery site*."
Una "best practise" di DR prevede tra i 50 ed i 100 km di distanza per repliche asincrone (bassi RPO); oltre i 100km di distanza per repliche batch (RPO più alti).

(*) http://www.drj.com/2011-articles/winter-2011-volume-24-issue-1/the-state-of-disaster-recovery-preparedness.html

In cosa consiste la business continuity (BC)

La business continuity è una pratica definita dalla norma **ISO 22301**, che stabilisce i requisiti necessari a pianificare, stabilire, attuare, rendere funzionante un sistema di gestione documentato, e per monitorare, mantenere attivo e migliorare in continuo il sistema di gestione finalizzato a proteggere, ridurre le possibilità di accadimento, preparare, dare risposte e ripristinare eventi destabilizzanti per un'organizzazione, quando questi abbiano a manifestarsi.

La business continuity può essere assimilata a uno "0 downtime" sull'infrastruttura tecnologica e si riferisce alla possibilità di progettare l'architettura Cloud in modo da garantire una continua operatività della stessa in caso di disastro o grave danno ai sistemi.
A differenza del disaster recovery, un piano di business continuity prevede che, *durante il verificarsi del disastro, i sistemi continuino ad essere attivi e funzionanti*: senza interruzioni. Per realizzare questo obiettivo, è necessario mettere a punto un progetto in cui i dati siano sincronizzati su due data center diversi grazie a strategie sia lato hardware che software. I dati e l'applicazione presenti su un server in business continuity sono in un rapporto di *failover* con un secondo sistema che si trova in un data center diverso. Generalmente, l'utente che utilizza l'applicativo su un sistema di BC, in caso di guasto sperimenterà solo una breve pausa ma senza accorgersi che si era verificato un problema. Come si può realizzare un progetto di business continuity? Sicuramente, attraverso un sistema in *cluster*. La replica su più sistemi consentirà di accedere ai dati da una fonte secondaria, come nel caso del clustering in modalità *active/active*: in questo modo, gli utenti di un servizio continueranno a lavorare per esempio sul loro mail server anche nel caso in cui l'applicativo mail vada in down sul server di produzione, e questo perché l'applicazione viene riavviata sul secondo server.

> Diversamente dal programma di DR, obiettivo primario è la possibilità di continuare a fruire del sistema durante il fermo.

Conditio sine qua non della BC è la distribuzione dei servizi ICT su più data center (2 o più server farm) che però non distino tra loro oltre 20 km di distanza. Infatti, maggiore è la distanza, maggiori saranno anche i tempi di recovery. In particolare, tra 5 e 50 km, aumentando la distanza si riduce il rischio ma si rallentano progressivamente le prestazioni delle transazioni da eseguire in BC.

DR: se funziona, migliora anche la BC

Vediamo ora come il concetto di continuità di servizio possa intersecarsi con quello di business continuity e in qualche modo lo determini. In caso di infrastrutture che fanno capo a progetti "business critical", l'obiettivo del cliente è molto più spesso la continuità di servizio rispetto al "semplice" recupero dei dati.
Nella maggior parte dei casi, in presenza di un'architettura cloud progettata secondo una disaster recovery, le aziende si preoccupano del tempo che il recupero dei dati richiederà e proprio questa questione implica una domanda precisa:

- Quali sono i dati che si desidera recuperare prima degli altri?
- Quali i costi in caso di un certo downtime?

E' fondamentale infatti **stabilire delle priorità**. E le priorità vengono stabilite dalle relazioni commerciali e dal tipo di business: quanto perdiamo in termini economici? Chi sono i nostri partner, cosa perdono in caso di disastro, quali sono i dati che non compromettono la nostra collaborazione con loro?

Ovviamente, anche se disaster recovery e business continuity sono due cose differenti, che richiedono misure differenti, se l'infrastruttura è stata ben progettata a livello di affidabilità e scalabilità e quindi la "visione" di disaster recovery è stata adeguata, ci saranno anche migliori opportunità di far fronte con maggiore successo anche alla questione della continuità (pur in assenza di un piano specifico di business continuity ma solo di disaster recovery). Se invece il progetto di recovery è più debole, allora sicuramente in caso di disastro la continuità del business verrà penalizzata.

DR e BC: insiemi e sottoinsiemi

Il disaster recovery si può definire un sottoinsieme della Business Continuity.
Fattori essenziali sono la disponibilità di un secondo sito dove effettuare il backup (off-site) e la velocità di restore.
A seconda della criticità del business, il disaster recovery, che è "data-centrico", potrà essere effettuato integrando l'architettura cloud con un backup remoto, soluzione a bassissimo costo, oppure pensare a un *mirroring* completo dell'infrastruttura.

La business continuity, invece, ha un focus più ampio, e obiettivi più ambiziosi: con essa si mira a continuare a lavorare durante il disastro stesso. Tutti i processi devono essere attivi anche in caso il sistema nel sito di produzione venga compromesso per via di errori umani o catastrofi naturali. Un corretto piano di BC deve prevedere anche la piena consapevolezza, da parte dei dipendenti dell'azienda coinvolta, di cosa fare e come in caso si verifichi il problema.

Disaster recovery: un riassunto

A seguire uno schema sulle caratteristiche di un piano di DR:

- prevede la pianificazione di come reagire al malfunzionamento/rottura dei servizi ICT rispetto al recupero di dati e servizi;
- prevede di analizzare come prima cosa il rischio;
- valuta RTO ed RPO ossia, rispettivamente, l'obiettivo temporale di recupero del business e la massima finestra temporale entro la quale il sistema deve essere riattivato;
- i suoi costi sono direttamente proporzionali a quanto saranno ambiziosi RTO ed RPO;
- implica l'allocazione dei servizi ICT su due (o anche più) data center distanti geograficamente a una distanza in km ragionevolmente elevata;
- una "best practise" di DR prevede tra i 50 ed i 100km di distanza per repliche ascincrone (bassi RPO); oltre i 100km di distanza per repliche batch (RPO più alti).

Business continuity: un riassunto

A seguire uno schema sulle caratteristiche di un piano di BC:

- prevede la pianificazione di come continuare a lavorare senza interruzioni al verificarsi di un malfunzionamento/rottura dei servizi ICT;
- prevede di analizzare come prima cosa il rischio;
- implica l'allocazione dei servizi ICT su due (o anche più) data center non troppo distanti geograficamente al fine di non incidere troppo sulle prestazioni;
- in particolare, prendendo in considerazione l'intervallo tra 5 e 50 km, aumentando la distanza si riduce il rischio ma rallentano progressivamente le prestazioni.

DR e BC: cosa può fare Seeweb

Come Cloud Provider con sedi distribuite tra Lazio e Lombardia e parte del network di aziende europee DHH, Seeweb è in grado di fornire infrastrutture ridondate e di contribuire alla realizzazione di progetti di Business Continuity.

Certificata ISO22301 dal 2021, Seeweb consente di **garantire dati in Disaster Recovery** già a partire dalle infrastrutture che abbiano solo un semplice servizio di backup: quest'ultimo, infatti, copia e alloca i dati su una sede diversa (sede Seeweb) da dove si trovano i servizi (infrastruttura di produzione). Di qui, basta attivare un backup settimanale o giornaliero per sapere i propri file al sicuro.

Seeweb consiglia comunque anche **l'esecuzione di un Backup Recovery Test**, finalizzato alla verifica dell'efficacia della procedura di recupero dei dati: dalla tempistica necessaria al restore, al controllo dell'effettiva integrità di tutte le informazioni, verifiche fondamentali per le infrastrutture critiche soprattutto ogni qualvolta si apportino aggiornamenti hardware, software, firmware.

La progettazione di architetture cloud o dedicate che, oltre a un backup remoto, siano replicate off-site con un **Disaster Recovery geografico** di tutti gli asset, va pianificata a seconda degli obiettivi del cliente: in base alla latenza che è in grado di "accettare", al tipo di dati cui dare priorità, etc.
Fondamentale, quindi, mettersi in contatto con uno specialista per d**isegnare il tipo di architettura in DR o BC in linea con i propri obiettivi**.

Conclusioni

- Essenziale è sottolineare che le soluzioni non sono sostitutive tra loro: ognuna ha delle funzioni ed esclude l'altra.
- In entrambi i casi, è molto importante valutare il rischio: identificando quali funzioni, processi aziendali e dati siano più importanti di altri.
- Valutare la vulnerabilità di apparati e applicazioni.
- E, quindi, affidarsi a un partner tecnologico che sia in grado di gestire tutto questo: dalla dislocazione geografica dei servizi alla possibilità di un supporto tecnico veloce e continuativo.

Fonti:
http://www.netstandard.com/far-far-enough-disaster-recovery-site/
http://www.datacenterknowledge.com/archives/2013/01/04/disaster-recovery-is-not-business-continuity/
http://www.oneneck.com/news-events/blog/posts/2016/7/19/disaster-recovery-vs-business-continuity-what-s-the-difference

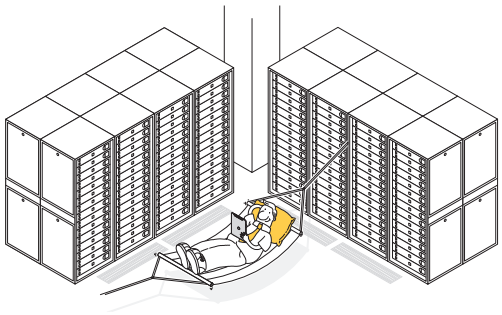
Seeweb srl
Via Armando Vona 66
03100, Frosinone

Via Caldera, 21 - edificio B
20153 Milano

https://www.seeweb.com
info@seeweb.com
https://www.facebook.com/seeweb.it
https://twitter.com/seeweblive

Autrice White Paper:
Chiara Grande
chiara.g@seeweb.it

Disaster Recovery vs Business Continuity:
facciamo chiarezza



14dicembre2023

seeweb
THINK CLOUD