giornale delle Assicurazioni
Mensile
Ketchum
Data 06-2013
Pagina 70/72
Foglio 1 / 2

STORAGE Nuove strategie

Quando il processo si esternalizza

Conservazione dei dati, ritorno alla normalità in caso di fermo, coinvolgimento degli agenti. Ecco che cosa cambia se la compagnia affida il controllo dell'archivio a terzi.

Alberto Mazza

L'outsourcing entra nel mondo assicurativo dalla porta dello storage e della business continuity. Alcune compagnie (essenzialmente di medie e piccole dimensioni) sperimentano, infatti, l'esternalizzazione della tecnologia partendo proprio dalla gestione dell'archivio e della ripartenza in caso di disastro. Altre, invece, affidano in blocco i processi a un fornitore esterno. Ecco i casi di Reale Mutua e di Assimoco.

Reale Mutua «Nei primi mesi del 2012, Reale Mutua assicurazioni ha spostato il data centre in un sito diverso dalla storica sede di via Corte d'appello», spiega **Alfredo Robusto**, responsabile sicurezza e continuità del business del gruppo torinese. «Questa operazione ha comportato anche un cambio di fornitore per il servizio di disaster recovery. Infatti, il contratto con il nuovo outsourcer (Cedacri, *ndr*) prevede l'*housing* dell'infrastruttura primaria a Collecchio. Ma anche l'erogazione dei servizi di disaster recover da un sito secondario, di proprietà dello stesso fornitore. A oggi la situazione è consolidata». Dove si trova la seconda struttura? «A Castellazzo Bormida, presso il data centre Cedacri specializzato per quell'attività».

In quanto tempo assicurate il ritorno alla normalità in caso di fermo? E ogni quanto tempo organizzate test? «Grazie alla predisposizione del piano di disaster recovery, l'erogazione del servizio è garantita in caso di danno grave al sito primario», risponde Robusto. «In questo caso, i tempi di ripristino sono quelli concordati con l'utente di business, (per i casi più critici, il *recovery time objective* è di 24 ore). I dati sono replicati in modalità asincrona (il ritardo massimo possibile è di 10 millisecondi), con tecnologia *Hp continuous access*; esiste inoltre un punto di consistenza dei dati consolidato ogni sera alle 21:00 (tecnologia *Hp business copy*). Le modifiche infrastrutturali sono gestite in maniera continuativa attraverso un processo di *change management* tecnologico, che ha il compito di mantenere aggiornato il sito secondario sia nell'hardware, sia nel software», puntualizza Robusto. «Tutto l'impianto di disaster recovery viene periodicamente testato (il contratto con il fornitore prevede quattro prove annuali) per gli aspetti funzionali delle singole componenti interessate, ma anche per gli aspetti organizzativi».

Cluster a più nodi
«Per gli ambienti (sia di test, sia di produzione) a più alta criticità, sono previsti cluster di server a più nodi che, in caso di fault di uno di questi, garantiscono la continuità del servizio», afferma Alfredo Robusto, responsabile sicurezza e continuità del business del gruppo Reale Mutua.

In che modo coinvolgete gli agenti nella disaster recovery? «Tutte le architetture di rete per la raccolta dei siti periferici, come agenzie, quartier generali di outsourcer e sedi direzionali (Cld, altre compagnie del gruppo Reale Mutua e uffici distaccati) sono ridondate. Per queste strutture è previsto, infatti, un collegamento con il sito principale di Collecchio, ed esistono connessioni dedicate per il sito secondario di disaster recovery. Tutte le architetture che garantiscono la connettività dei siti periferici, realizzate con i principali *carrier* telefonici italiani, si basano su tecnologia Mpls (Telecom Italia e Fastweb) e sono realizzate con criteri di business continuity. Non tutti i sistemi sono stati inseriti nel piano di disaster recovery con le stesse modalità e tempistiche per il ripristino», aggiunge Robusto: «questo, infatti, dipende dai risultati della Bia (*business impact analisys*) che viene effettuata ogni anno. In questo modo vengono identificati due diversi perimetri ("a caldo" e "a freddo") a seconda delle criticità, con modalità di salvataggio dati diverse e Rpo e Rto differenti».
I server prevedono connessioni di rete e storage ridondate? «Sì. Per gli ambienti (sia di test, sia di produzione) a più alta criticità, sono previsti *cluster* di server a più nodi che, in caso di *fault* di uno di questi, garantiscono la continuità del servizio. Le procedure di backup per i database prevedono sia backup fisici (attraverso strumenti specifici della suite *Sql Backtrack*, di Bmc software), sia salvataggi periodici degli export dei dati, replicati con tecnologia storage *Ca* di Hp. Le modifiche ai sistemi non replicati (a carico di Rma) avvengono insieme alla modifica dei sistemi di produzione, in accordo con il processo di change management tecnologico». Le connessioni degli utenti, conclude Robusto, «vengono trasferite dal sito tradizionale a quello di emergenza, effettuando variazioni al *routing* (il protocollo utilizzato è Ospf/Bgp) delle nuvole di raccolta dei siti periferici, tramite procedure appositamente descritte e documentate. Queste operazioni, che devono essere effettuate sull'hardware di rete poste nel sito secondario, possono essere eseguite sia dal personale Rma, sia da quello del fornitore del servizio di disaster recovery (oggi Cedacri), in possesso, all'occorrenza, delle opportune credenziali».

Assimoco Anche Assimoco ha scelto di affidare lo storage all'esterno. In che modo è organizzato questo processo? «Lo storage dei principali dati di compagnia», dice **Dani-**

giornale delle Assicurazioni

Mensile

Ketchum

Data 06-2013
Pagina 70/72
Foglio 2 / 2

Due localizzazioni
«L'outsourcer ha predisposto due localizzazioni distinte per i siti di recovery in caso di disastro», spiega Michele Montagnini, responsabile tecnologie e gestione operativa. «La prima fa riferimento a tutte le componenti che riguardano il sistema mainframe, e quindi del Db2. Lo storage, in particolare, viene replicato dal sito primario in tempo reale». A fianco, il team It di Assimoco. Da sinistra a destra: Michele Di Grazia, Danilo Ughetto, Enrico Morani, Walter Fontana, Michele Montagnini, Claudio Fischetti e Fabrizio Caputo.

lo Ughetto, responsabile It di Assimoco, «è ripartito su diversi sistemi di archiviazione. Queste architetture funzionano con la tecnologia utilizzata dalle applicazioni che gestiscono il sistema informativo di compagnia. I dati sono, quindi, memorizzati su sistemi *Dbrms Db2 for z/os, Oracle enterprise*».
All'interno del primo sistema di archiviazione, prosegue Ughetto, «trovano posto tutti i dati relativi ai portafogli di compagnia e alla gestione delle componenti contabili legate agli intermediari. Nel secondo, invece, sono memorizzate le informazioni relative alla gestione dei sinistri, al sistema di datawarehouse e a quelli legati al sistema Sap».
Di che cosa si occupa l'outsourcer? «Di tutte le operazioni di backup in funzione di policy, concordate con la compagnia», risponde **Michele Montagnini**, responsabile tecnologie e gestione operativa di Assimoco. Che prosegue: «l'outsourcer ha predisposto due localizzazioni distinte per i siti di *recovery* in caso di disastro. La prima fa riferimento a tutte le componenti che riguardano il sistema mainframe, e quindi del Db2. Lo storage, in particolare, viene replicato dal sito primario in tempo reale».
Come? «In pratica, si effettua una scrittura "in doppio" dei dati. attraverso un software specializzato». E la seconda localizzazione? «Riguarda la componente dipartimentale, cioè Oracle», dice Montagnini. «In questo caso, i dati vengono replicati a cadenza settimanale in modalità *full backup*. Mentre gli *archive log* sono salvati durante i giorni della settimana, dal lunedì al sabato. E, quindi, trasmessi in deduplica dall'unità di recovery situata sul sito primario alla struttura secondaria».
Quanto tempo ci vuole per il ritorno alla normalità? «Il ripristino, inteso come Rto, avviene in maniera differenziata, a seconda che si faccia riferimento al sistema mainframe o a quelli dipartimentali», risponde Montagnini. «In quest'ultimo caso possiamo tornare operativi in meno di un'ora. Mentre, per quanto riguarda il mainframe, la ripartenza è stimata intorno alle 12 ore». ■