EURO SERVIZI Srl

Disaster Recovery

Piano di ripristino del sistema

DEFINIZIONE E TECNICHE DI DISASTER RECOVERY

Per **Disaster Recovery** (brevemente DR) si intende l'insieme di misure tecnologiche e organizzative/ logistiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.

Il **Disaster Recovery Plan** (DRP) (in italiano, Piano di disaster recovery) è il documento che esplicita tali misure. Il piano d'emergenza deve prevedere il ripristino di tutte le funzioni dell'ente. Per la definizione del DRP devono essere valutate le strategie di ripristino più opportune. La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.

TECNICHE DI DISASTER RECOVERY

Allo stato attuale, la tecnologia offre la possibilità di realizzare varie soluzioni di continuità e Disaster Recovery, fino alla garanzia di fatto di un'erogazione continua dei servizi necessaria per i sistemi definiti *mission critical*. In pratica i sistemi e i dati considerati *importanti* vengono ridondati in un "sito secondario" o "sito di Disaster Recovery" per far sì che, in caso di disastro (terremoto, inondazione, attacco terroristico, ecc.) tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività sul sito secondario nel più breve tempo e con la minima perdita di dati possibile.

Chiaramente quanto più stringenti saranno i livelli di continuità tanto più alti saranno i costi di implementazione della soluzione.

In particolare, i livelli di servizio sono usualmente definiti dai due parametri Recovery Time Objective (RTO) e Recovery Point Objective (RPO).

Replica sincrona

La replica sincrona garantisce la specularità dei dati presenti sui due siti poiché considera ultimata una transazione solo se i dati sono stati scritti sia sulla postazione locale che su quella remota. In caso di evento disastroso sulla sede principale, le operazioni sul sito di Disaster Recovery possono essere riavviate molto rapidamente (basso RTO e RPO praticamente nullo).

Replica asincrona

Per far fronte al limite di distanza tra i due siti imposto da tecniche sincrone, si ricorre spesso alla tecnica di copia asincrona. In questo caso il sito che si occuperà della replica può trovarsi anche a distanze notevoli. In questo modo è possibile affrontare anche disastri con ripercussioni su larga scala (come ad esempio forti scosse sismiche) che altrimenti potrebbero coinvolgere entrambi i siti (se questi si trovano nelle vicinanze).

Tecnica mista

Per garantire la disponibilità dei servizi anche in caso di disastro esteso e al tempo stesso ridurre al minimo la perdita di dati vitali si può ricorrere ad una soluzione di tipo misto: effettuare una copia sincrona su un sito intermedio relativamente vicino al primario e una copia asincrona su un sito a grande distanza.

Disaster Recovery

Piano di ripristino del sistema

CARATTERISTICHE DEL PRODOTTO/SERVIZIO

Il prodotto è una vera e propria soluzione di **disaster recovery** con **replica asincrona** che prevede il ripristino su un ambiente perfettamente funzionante in modo da garantire dei **livelli bassi di RTO e RPO**.

Il prodotto offre un servizio di backup con sincronizzazione direttamente sui nostri server e viene impostato in fase di startup sulla base delle condizioni ambientali presenti nell'ente (caratteristiche dei server, mole dei dati da trattare, velocità della linea, etc.). In questa fase verrà definita anche la frequenza della replica e di conseguenza il livello di RPO.

Vengono presi in considerazione solo i dati più critici dell'ente, ovvero il sistema gestionale, il database, le applicazioni ed il sistema documentale.

Garanzia dei dati

Il backup viene garantito su uno spazio dedicato su server in alta affidabilità situati presso DataCenter di primaria importanza nazionale con banda illimitata; la velocità della replica dipende quindi solo ed esclusivamente dalla banda dell'Ente.

Massima riservatezza.

I dati (documentale e database) vengono posizionati in un area dedicata al cliente, alla quale può accedere unicamente lo stesso tramite utente, password e filtro sull'IP chiamante.

Area di ripristino

Il ripristino avviene in un server Windows dove sono presenti, già installate ed attive, tutte le applicazioni costantemente aggiornate.
In una macchina, dunque, che è già perfettamente funzionante (con i suoi IP etc.), per effettuare il ripristino sarà sufficiente:

- importare il database
- collegare l'ambiente documentale

Il tutto verrà eseguito in caso di disastro mediante un script completamente automatico ed avrà una durata di qualche decina di minuti, garantendo quindi un basso livello di RTO.

ASPETTI ORGANIZZATIVI E RISULTATI ATTESI

Il prodotto prende in considerazione solo l'ambiente gestionale, pertanto è necessario che l'uso della *funzione documentale* sia quanto più possibile estesa. Questo infatti, oltre a semplificare il lavoro degli utenti, offre maggiori garanzie sull'integrità dei documenti. Infatti, un documento presente su un *sistema documentale*, a differenza di una cartella di rete non può, ad esempio per errore, essere spostato in una cartella differente

Lo spazio garantito, accessibile solo ed esclusivamente mediante credenziali specifiche e dagli indirizzi IP dell'Ente attraverso un normale sistema di sincronizzazione (anch'esso definito sulla base delle condizioni ambientali del cliente) salva:

- database, esportato con le cadenze desiderate (una o più volte al giorno),
- sistema documentale.

La applicazioni invece vengono costantemente mantenute aggiornate dalla scrivente.

Viene complessivamente garantito :

- *il ripristino in tempi molto rapidi (qualche decina di minuti)*
- *il buon esito del ripristino*
- *l'allineamento dei dati all'ultimo aggiornamento, quindi nella peggiore delle ipotesi alla notte precedente.*

In fase di attivazione del servizio, è prevista una simulazione e già in quella sede vengono comunicate tutte le informazioni per l'accesso in caso di disastro.

COMPARAZIONE CON ALTRI PRODOTTI

Il mercato oggi, offre diverse soluzioni che rispondono alla voce Disaster Recovery.
Andando però a valutarle nel dettaglio, ci si accorge subito che non lo sono nel vero senso del termine e che comunque offrono tempi di RTO decisamente lunghi.
Si tratta infatti, di sistemi di backup su server presso qualche "data farm" (backup on cloud), dove vengono copiati i file e l'immagine di uno o più server.

Queste soluzioni pur offrendo una minima garanzia sull'integrità delle informazioni salvate, lasciano molti dubbi circa i tempi e le modalità di ripristino al verificarsi dell'evento (disastro).

Significa, ad esempio, che in caso di evento disastroso, per il ripristino in un sito alternativo, dovranno essere previste le seguenti attività manuali:

1. recuperare l'immagine corretta del server
2. installare ed avviare la macchina
3. cambiare tutti i parametri di rete (che ovviamente è impostata per lavorare all'interno della rete del cliente)
4. verificare le impostazioni di ambiente e delle varie applicazioni
5. verificare ed eliminare eventuali connessioni ad altre unità della rete (del cliente)
6. verificare (e sperare) che tutto funzioni e sia raggiungibile dal sito alternativo

Come si può intuire sono operazioni tutt'altro che semplici, aggravate magari dall'agitazione del momento, che possono, se non eseguite correttamente, essere fonte di rilevanti problemi, poi difficilmente gestibili.

Il nostro prodotto, invece, ha un approccio diverso perchè prende in considerazione globalmente tutti gli ambiti che compongono l'ambiente gestionale, ovvero il cuore dell'Ente (database, sistema documentale, applicazioni). Evitando così, non una ma, tutte le operazioni manuali che sarebbero necessarie a garanzia del buon esito dell'operazione e dei bassi livelli di RTO e RPO.

CONCLUSIONI

La scelta di un prodotto D.R., può essere difficile per un Ente, di conseguenza sintetizziamo le principali caratteristiche del nostro prodotto rispetto alle classiche soluzioni:

- garanzia di buon esito del ripristino
- tempi rapidissimi di ripristino
- massiva riservatezza delle informazioni.
- mole dati contenuta a garanzia del buon esito della sincronizzazione dei dati

Il risultato è, quindi, che in caso di evento (disastro,) sarà reso disponibile nell'arco di pochi minuti un ambiente Terminal Server accessibile in desktop remoto da uno o più utenti, con l'ambiente gestionale perfettamente funzionante.