Soluzioni di continuità operativa

Federico Calò
Direttore Dipartimento Datacenter & Cloud

Soluzioni di continuità operativa nei datacenter Lepida

Argomenti

- Infrastruttura fisica: misure di sicurezza e continuità del singolo datacenter
- Infrastruttura di rete geografica: resilienza della rete geografica
- Tecnologie di alta affidabilità attive nel singolo datacenter
- Soluzioni di continuità operativa multi datacenter
- Business Continuity
- Disaster Recovery
- Backup immutabile
- Criticità da considerare
- Scenari reali

Infrastruttura fisica

Tutti i datacenter Lepida sono costruiti secondo le linee guida Tier III dell'Uptime Institute
Le misure di sicurezza fisica di ogni singolo datacenter prevedono:

- ridondanza 2N degli impianti di alimentazione elettrica, con due linee totalmente separate ed indipendenti a partire dalla fornitura in media tensione
- ciascuna linea elettrica è dotata di un UPS a servizio degli apparati IT, gli UPS sono modulari, internamente ulteriormente ridondati in modalità N+1 e individualmente dimensionati sul carico totale degli apparati IT
- le linee elettriche indipendenti arrivano separatamente ad ogni armadio rack, ciascuno dotato di due PDU e alimentano tutti gli apparati IT che sono sempre dotati di alimentazione 2N
- alimentazione di emergenza garantita da gruppi elettrogeni diesel dotati di almeno 24 ore di autonomia (2N a Ferrara e Modena, N a Ravenna e Parma)
- ridondanza 2N degli impianti di condizionamento, con due circuiti indipendenti di raffreddamento e di distribuzione dell'acqua fredda all'interno delle sale
- impianti di rilevazione e spegnimento incendi, impianti antiallagamento, antintrusione, controllo accessi, videosorveglianza e presidio H24
- impianto di supervisione degli impianti con allarmistica collegata ai tecnici reperibili
- attività di manutenzione periodica programmata di tutti gli impianti, atta a garantire il corretto funzionamento di tutti i sistemi, con test delle ridondanze

Rete geografica

- Ogni datacenter Lepida costituisce un POP della rete geografica
- Il core router del datacenter è totalmente ridondato in modalità 2N
- Le connessioni di rete del core router verso l'esterno sono effettuate tramite 3 distinti link 100Gb
- Due link 100Gb su fibra spenta Lepida con percorsi geografici distinti, anche internamente al datacenter
- Il terzo link 100Gb fornito da un gestore terzo in modalità IP che garantisce la connettività Layer 3 anche in caso di fault contemporaneo dei due link in fibra
- Presente anche una connettività offline di emergenza per l'accesso in manutenzione agli apparati Lepida
- In corso di realizzazione progetto per garantire la resilienza del singolo datacenter anche al fault completo del core router

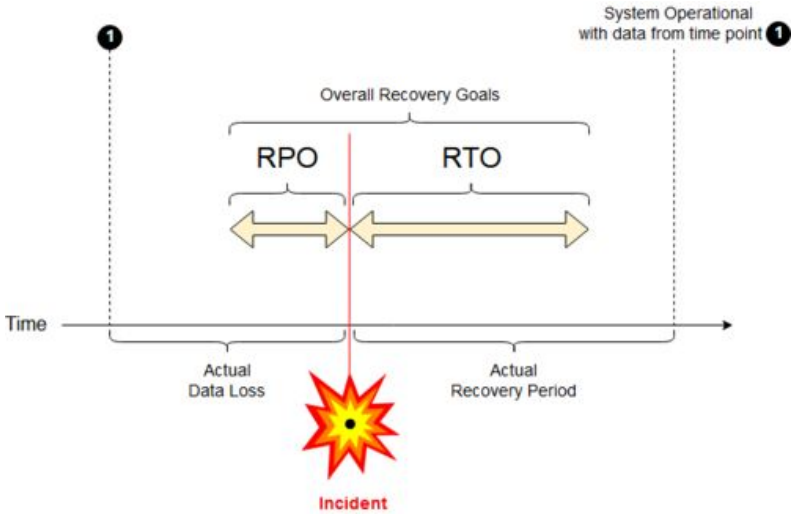
Tecnologie di alta affidabilità interne ai datacenter

- Tutti gli apparati IT interni al datacenter sono comunque configurati in modalità HA
- Gli apparati di rete di distribuzione interna sono sempre configurati in modalità 2N
- La SAN è costruita con due fabric distinte ed indipendenti che connettono tutti gli apparati, sia storage che server
- Tutti gli storage sono completamente ridondati e su qualsiasi componente può essere effettuata la manutenzione a caldo in caso di guasto
- Tutti gli storage di tipo SAN sono presentati ai server attraverso un virtualizzatore storage (Vplex o Metronode), che, tra le altre cose, garantisce la possibilità di sostituire lo storage fisico a caldo senza disservizio per gli enti
- Il virtualizzatore storage permette anche di effettuare configurazioni in HA su più storage
- Tutti i server sono dotati di ridondanze interne che garantiscono la possibilità di intervenire a caldo in caso di guasti alle componenti principalmente soggette ad usura (alimentatori, ventole, dischi)
- I server virtuali messi a disposizione da Lepida nel listino IaaS sono ospitati su cluster di virtualizzazione in alta affidabilità, che garantiscono la resilienza al fault del singolo nodo compute
- Le infrastrutture fisiche messe a disposizione degli enti permettono di realizzare architetture di clustering no single point of failure

Disaster recovery - pianificazione e definizione delle strategie

La pianificazione della gestione di un evento passa attraverso la **Business Impact Analysis**, che si occupa, partendo dall'analisi dei rischi, di definire per ogni servizio due parametri fondamentali, che guidano la scelta delle strategie di disaster recovery:

- **Recovery Time Objective (RTO)**: tempo in cui il sistema deve essere ripristinato a seguito di un incidente
- **Recovery Point Objective (RPO)**: tempo massimo di cui si tollera la perdita di dati in caso di incidente



Piani di continuità operativa

Business continuity plan: l'insieme di procedure documentate che guidano le organizzazioni nel rispondere, recuperare, riprendere e ripristinare a un livello pre-definito le attività a seguito di un'interruzione. Include la pianificazione di aspetti non correlati all'IT come strutture, crisi di comunicazione e protezione della reputazione.

Disaster recovery plan: l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi a fronte di gravi emergenze. E' parte del business continuity plan e ne tratta gli aspetti tecnologici. In Lepida è tipicamente gestito a livello di piattaforma (ognuna ha il suo piano specifico).

Strategie di Disaster Recovery

- **Business continuity**
  - RPO = 0 e RTO prossimo allo 0
  - totalmente automatica, non richiede intervento umano per il failover
- **Disaster recovery**
  - RPO ed RTO >0, da definire in funzione del servizio, tipicamente RPO tra 1 ora e 24 ore, RTO tra 30 minuti e 6 ore
  - richiede un processo decisionale per essere attivato, in quanto comporta una perdita di dati, e un'intervento umano
- **Backup immutabile**
  - RPO elevato, funzionale alla frequenza dei backup, tipicamente 12-24 ore
  - RTO elevato, necessità di ripartire da zero con tempi lunghi nell'ordine dei giorni
  - protegge da eventi gravi quali ransomware, errori umani, eventi disastrosi

Non esiste una soluzione unica che metta al sicuro da qualsiasi evento. La scelta della strategia da applicare deve essere effettuata sulla base di una valutazione dei rischi e della criticità del singolo servizio e normalmente comporta un mix delle varie soluzioni possibili.

Business continuity vs disaster recovery vs backup

Le tre strategie assolvono a scopi differenti, gestiscono scenari di guasto differenti e non sono mutualmente esclusive.

Guasto	Business Continuity	Disaster Recovery	Backup
Corruzione dei dati			X
Errore umano		X*	X
Guasto sulla rete di accesso		X	X
Guasto hardware ai sistemi	X	X	X
Indisponibilità del sito	X	X	X

* : se opportunamente configurato ed entro certi limiti

lepida

Business Continuity

Aspetti di dettaglio

- Pro
  - Automatica, non richiede intervento umano per l'attivazione
  - RPO = 0 ed RTO prossimo allo 0
  - Gestita a livello infrastrutturale normalmente trasparente alle applicazioni
  - Protegge da guasti hardware o infrastrutturali fino all'indisponibilità di un intero datacenter
- Contro
  - Introduce latenza in scrittura tra 3 e 6 ms, va valutato attentamente l'impatto sulle performance degli applicativi
  - non protegge da problemi sui dati (corruzione, cancellazione accidentale, ransomware, ….) in quanto i dati sono replicati in maniera sincrona tra i due data center
  - non protegge da problemi logici a livello di networking/firewall in quanto tali componenti sono condivise tra i due data center
  - gli automatismi di funzionamento della soluzione sono essi stessi soggetti a possibili guasti
- Campo di applicazione
  - Servizio IaaS basato su VM gestito da Lepida
  - Servizio storage a blocco, richiede attività di configurazione e gestione da parte dell'ente
  - Servizio storage file based (CIFS/NFS)
  - Servizio object storage S3

Disaster recovery

Aspetti di dettaglio

- Pro
  - se opportunamente gestita e configurata può proteggere da guasti su qualsiasi livello dell'infrastruttura (hardware, facilities, networking, …) fino alla corruzione del dato (se identificata nella finestra di RPO definita)
  - diversi scenari e modelli di implementazione coprono tutte le soluzioni applicative
- Contro
  - può essere invasiva a livello applicativo se si vuole avere una protezione completa
  - necessita di una attività spesso complessa per l'esecuzione, che deve essere il più possibile automatizzata e comunque totalmente proceduralizzata
  - per rendere la procedura efficace in caso di reale disastro gli enti devono essere autonomi nella sua esecuzione
  - richiede una decisione per l'avvio della procedura (in quanto comporta perdita di dati) e di un intervento umano per l'esecuzione, per quanto automatizzata.
  - l'RTO atteso parte sempre dall'avvio della procedura, va quindi considerato in aggiunta il tempo necessario per la decisione e l'intervento
  - necessita di test periodici di verifica
  - nella definizione della procedura di disaster recovery va considerato che le operazioni devono essere eseguite in condizioni di emergenza

Soluzioni tecnologiche disponibili nei listini Lepida

Business continuity

- Disponibili solo nella coppia di data center Ferrara/Ravenna
- VM IaaS in HA
- Replica sincrona dello storage blocco, utilizzabile dall'ente per la configurazione di cluster VMWare "Stretched"
- Replica sincrona dello storage File Based (CIFS/NFS) solo su storage Unity
- Replica geografica dello storage Object di tipo S3 solo su storage ECS
- Networking L2/L3 stretched
- Servizio Firewall in HA

Soluzioni tecnologiche disponibili nei listini Lepida

Disaster recovery

- Disponibili su qualsiasi data center
- replica asincrona dello storage file based (CIFS/NFS) su storage Unity e PowerScale/Isilon
- replica asincrona dei dati per il servizio Oracle as a Service basata su tecnologia Oracle DataGuard
- replica asincrona delle VM IaaS
- per gli enti che utilizzano i servizi BaaS e Storage la costruzione del disaster recovery è a carico dell'ente, Lepida mette a disposizione infrastrutture separate su data center differenti che possono essere utilizzate per la predisposizione

Soluzioni tecnologiche disponibili nei listini Lepida

Backup immutabile

- Disponibile presso i datacenter di Modena e Ravenna
- Storage Dell Data Domain con funzionalità di Retention Lock che garantisce l'impossibilità anche da parte degli amministratori con accesso fisico allo storage di cancellare i backup per la durata della retention impostata
- Tutte le VM IaaS in gestione Lepida utilizzano già questa tecnologia per i backup
- Utilizzabile come target per i backup di tutti i software che lo supportano, sia per servizi forniti da Lepida che per servizi utilizzati dal singolo ente
- Disponibile anche per il servizio Backup as a Service a listino Lepida basato su tecnologia Commvault

Soluzioni di continuità operativa

Criticità da considerare

- Dipendenze dei servizi
  - Nei piani di DR devono essere valutate le interdipendenza tra i servizi e l'effettiva fruibilità del sistema per gli utenti finali
  - Networking e firewall sono spesso comunque condivisi ed un guasto a quel livello può impattare diversi siti
- Interazioni tra servizi
  - in caso di DR è garantita la disponibilità dell'applicativo WEB, ma tutte le integrazioni esterne, sia in ingresso che in uscita?
- Separazione fisica dei servizi su siti differenti
  - criticità di performance ad avere sistemi fortemente correlati tra loro erogati da siti differenti
- Servizi infrastrutturali
  - DNS, NTP, Autenticazione, monitoraggio
- Test periodici necessari per verificare l'efficacia delle soluzioni implementate e per garantire il miglioramento continuo

Scenari reali 1

Evento del 11 novembre 2023

- il disservizio ha causato lo spegnimento della sala network del data center di Ravenna. Tutti i server e gli storage sono rimasti accesi, ma hanno perso connettività sia network che storage tra loro. Si sono inoltre spenti gli apparati di rete core, sia di routing geografico che firewall
- i servizi in business continuity sarebbero ripartiti automaticamente nel sito di Ferrara, in quanto il guasto è previsto negli scenari di recovery. Non ci sarebbe stata perdita di dati in quanto la replica sincrona avrebbe riacceso i server con i dati che erano presenti nel momento dello spegnimento. Tuttavia ci sono state due condizioni specifiche che avrebbero reso parzialmente inefficace l'operazione:
  - i server erano rimasti accesi e isolati, alla ripartenza si sarebbe potuta creare una condizione anomala di server contemporaneamente accesi in entrambi i siti, anche se per poco tempo in quanto i sistemi avrebbero provveduto a spegnere quelli di ferrara
  - al riavvio dei servizi gli apparati di rete geografica hanno avuto uno stato inconsistente per un periodo di tempo, cosa che avrebbe comunque causato l'indisponibilità dei servizi anche a Ferrara in quanto la componente di networking geografico è in comune
- I servizi in disaster recovery si sarebbero potuti attivare in quanto il sito di Dr non era impattato

lepida

Scenari reali 2

Evento del 24 aprile 2024

- il disservizio ha causato l'isolamento network del data center di Ferrara
- l'attivazione automatica della Business Continuity in ambiente VMWare non viene gestita se non attivando delle procedure manuali
- i servizi in business continuity potevano essere attivati manualmente nel sito di Ravenna, in quanto il guasto è previsto negli scenari di recovery, senza alcun impatto sui dati e con i tempi di ripristino previsti dalla BC
- Sono in corso di analisi le configurazioni degli ambienti VMWare per valutare l'automatismo di attivazione della BC in caso di isolamento network
- I servizi in disaster recovery si sarebbero potuti attivare in quanto il sito di Dr non era impattato

Scenari reali 3

Eventi di criptazione dei dati

- Nei casi di criptazione dei dati, a qualsiasi livello, la business continuity non è utile in quanto i dati vengono criptati in maniera sincrona tra i due siti
- I servizi in disaster recovery si possono attivare se il sito di DR non è coinvolto dalla criptazione dei dati e se l'evento si scopre entro i tempi di replica dei dati tra i due siti
- Il backup immutabile è l'unica soluzione certa a scenari di questa natura

www.lepida.net