Posteitaliane

Disaster Recovery e Business Continuity

Seminario generale sulle architetture e sulle tecnologie adottate nelle soluzioni di

Disaster Recovery e Business Continuity

Maggio 2013

Posteitaliane

Calogero Gandolfo

Responsabile Service Assurance

Maggio 2013

Il contesto Poste Italiane

➢Poste Italiane è l'infrastruttura logistica e tecnologica più grande e capillare dell'Italia che fornisce, oltre ai servizi postali, prodotti integrati di comunicazione, logistici, finanziari, assicurativi e di telefonia mobile su tutto il territorio nazionale a cittadini, imprese e pubblica amministrazione.

➢ Con la propria rete capillare di uffici postali, presenti in tutta Italia, garantisce i propri servizi a oltre 32 milioni di clienti. La presenza sul territorio, la grande esperienza e l'uso delle nuove tecnologie hanno permesso a Poste Italiane di assumere un ruolo da protagonista nel processo di sviluppo economico e sociale dell'Italia e la rendono partner naturale della pubblica amministrazione nei servizi al cittadino.

➢Il tasso di redditività colloca oggi il Gruppo Poste Italiane ai primi posti tra i grandi operatori postali d'Europa.

Il Gruppo Poste Italiane

Postel

Poste mobile

SDA EXPRESS COURIER Gruppo Posteitaliane

PosteEnergia

Postevita GruppoAssicurativoPostevita

Postetutela

PostEcom

Europa gestioni immobiliari

PosteShop

Posteassicura GruppoAssicurativoPostevita

MISTRALAIR Gruppo Posteitaliane

BANCA del MEZZOGIORNO

BancoPostaFondi SGR

Diventare un'azienda di servizi ad alto valore aggiunto che, valorizzando al massimo i suoi asset fondamentali ed in particolare la presenza capillare sul territorio, soddisfi le specifiche necessità della clientela tutta, nelle sue molteplici articolazioni, con una ampia ed integrata offerta di servizi costruiti sulle proprie competenze logistico/postali, finanziarie, di gestione dei processi di "outsourcing".

Strumento fondamentale per il conseguimento di questi obiettivi è l'uso di tecnologie Informatiche e di Telecomunicazione (ICT) all'avanguardia dirette alla costituzione del sistema "a rete" tra i più avanzati, completi e capillari del Paese

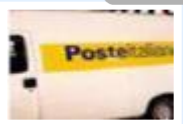
Per adempiere alla propria missione aziendale, Poste Italiane ha intrapreso un turn-around culturale, tecnologico e di processo che l'ha portata ad una significativa evoluzione del proprio modello di business

L'infrastruttura di Posteitaliane

RETE FISICA

- Circa 14.000 Uffici postali
- 2.771 Uffici di recapito
- 21 centri meccanizzati

RETE LOGISTICA



- 10 aerei e 10 voli giornalieri
- 38.000 veicoli
- 4.500 corrieri
- 3 hub logistici automatizzati

INFRASTRUTTURA ICT

- 11.000 uffici postali collegati in banda larga ad oltre 2Gbps
- Rete di trasmissione IP ad elevata capacità best in class
- 600 Terabyte di capacità di memoria in 5 Data Center
- Datawarehouse con 21 mln di clienti retail e quasi 2 mln business
- Monitoraggio in tempo reale h24 dei servizi erogati

RETE DI ACCESSO MULTICANALE

- 60.000 postazioni di lavoro
- Contact Center con oltre 900 operatori
- Canale web con oltre 70 milioni di pagine visualizzate ogni mese
- 6850 ATM (distributori di monete)
- 700 chioschi multimediali
- Digitale terrestre
- Telefono cellulare (tecnologia NFC)

Il più moderno sistema integrato di reti e piattaforme per l'erogazione di servizi

Agenda

- **Introduzione**
  - *Terminologia e Standard*
  - *Normative Internazionali*
- **I fondamenti del Disaster Recovery e della Business Continuity**
  - *Panoramica delle soluzioni disponibili*
  - *Descrizione delle tecnologie abilitanti*
  - *I piani e le procedure organizzative*
- **L'evoluzione della soluzione di Disaster Recovery in Poste Italiane**
  - *2006. Soluzione con Nastri a freddo*
  - *2007. Soluzione con Replica asincrona dei dati*
  - *Oggi. Soluzione SRDF-Star*

Il Disaster Recovery

Quale danno al Business Aziendale può derivare dall'indisponibilità prolungata delle Applicazioni e/o dalla perdita dei Dati Aziendali?

Il **Disaster Recovery (DR)** è l'insieme di…

…**Tecnologie** e **Processi** predisposti per ripristinare le ..

…**Applicazioni** e i **Dati** necessari all'erogazione dei…

… **Servizi di Business**, interrotti a seguito di…

…**Gravi Eventi Dannosi** (**Disastri**).

Business Continuity e Disaster Recovery

- **Business Continuity Management** è un processo strategico e tattico che permette ad un'organizzazione di avere una risposta a qualunque avvenimento e interruzione del Business che può avere impatto sui processi aziendali che contribuiscono al “core business” dell'azienda, garantendo un livello di servizio minimo accettabile predefinito.

- **Disaster Recovery** è l'insieme di processi e tecnologie atti a **ripristinare sistemi, dati e infrastrutture** necessarie all'erogazione di servizi “core business” a fronte di gravi emergenze (disastri).

Disastro

- Un disastro è la conseguenza dell'attuarsi di una minaccia non dovuta ad una aggressione intenzionale
  1. Disastri naturali: terremoto,alluvione, tornado, eruzione vulcanica
  2. Disastri dovuti all'uomo e alla tecnologia: incendio, esplosione, rottura delle condutture dell'acqua, mancanza di corrente, di linee di telecomunicazioni e di condizionamento ambientale
- Solo a causa degli uragani negli ultimi 10 anni si sono verificati in USA oltre 100 emergenze nazionali :nel 2012, l'uragano Sandy ha interessato 24 stati, tra cui l'intera costa est dalla Florida al Maine e ovest nel Michigan e Wisconsin, con danni particolarmente gravi in New Jersey e New York. La tempesta ha colpito New York il 29 ottobre, inondando strade, tunnel e linee della metropolitana e togliendo l'elettricità in giro per la città. I danni negli Stati Uniti sono stimati a più di 63 miliardi di dollari.
- Una società USA su 4 ha dichiarato di aver sperimentato un disastro negli ultimi 5 anni
- In California si verifica un intenso terremoto ogni 3 anni circa : si attende il famoso Big One
- Nel Settembre 2003 si è verificato il peggior black-out elettrico in Italia
- Il recente terremoto in Emilia ha colpito molte aziende presenti sul territorio

""Le cose che non speri accadono più spesso di quelle che speri.
Plauto(245-184 A.C.), Mostellaria""

""Se una cosa può andare storta, lo farà
Assioma di Murphy""

Alcuni termini ricorrenti

- **Rischio**: esposizione di una organizzazione a perdite o danni. Risultato della combinazione della probabilità del verificarsi di un evento e dell'impatto(gravità) prodotto dall'evento stesso
- **Minaccia**: è l'elemento che rappresenta un pericolo per l'organizzazione
- **Vulnerabilità**: una debolezza nota nel sistema rispetto a una minaccia
- **Attacco**: tentativo deliberato di creare un danno (es. attacco informatico, attacco terroristico)

Standard ISO 22301 ISO 22313

- La rilevanza sempre maggiore assunta dalle problematiche relative al processo di gestione della Business Continuity ha portato recentemente alla pubblicazione di alcuni standard specifici:

  ISO 22301:2012, "Societal security - Business continuity management systems -- Requirements" pubblicata a Maggio 2012

  ISO 22313:2012, "Societal security - Business continuity management systems – Guidance pubblicata a Dicembre 2012

- La prima norma specifica i requisiti per implementare, gestire e migliorare un sistema documentato di Business Continuity Management (BCMS) per preparare l'azienda a fronteggiare gli eventi distruttivi quando essi si verificano.
- La seconda norma fornisce una guida generale basata su best practices mondiali per la pianificazione, la implementazione, la gestione e il miglioramento costante di un sistema documentato di gestione della Business Continuity.

Standard BS25999

- Prima della pubblicazione degli standard ISO 22301 e ISO 22313 lo standard di riferimento per il processo di gestione della Business Continuity era lo standard **BS25999**
- Tale standard è composto da due parti:

  BS25999-1:2006 *Business Continuity Management. Code of practice*

  BS25999-2:2007 *Specification for Business Continuity Management*
- La prima parte rappresenta una guida generale e stabilisce processi, principi e terminologia per la gestione della Business Continuity
- La seconda parte specifica i requisiti per implementare, gestire e migliorare un sistema documentato di Business Continuity Management (BCMS)
- Con l'avvento delle nuove norme ISO la BS25999-2 sarà a breve ritirata.

ISO: International Organization for Standardization

BSI : British Standard Institution

Standard BS7799/ISO17799/ISO27002

- **BS7799** e **ISO17799** sono lo Standard per le politiche e le procedure di Sicurezza delle informazioni
- Lo standard è stato inizialmente conosciuto come standard inglese BS7799 pubblicato dal British Standards Institution(1995)
- Più tardi (2000) con diverse revisioni è stato adottato dal comitato tecnico internazionale ISO IEC diventando ISO17799 (Information Technology- Code of practice for information security management)
- Di recente lo standard ISO17799 è stato rivisto ulteriormente ed è diventato ISO27002 (Luglio 2007)

Lo standard fa esplicito riferimento alla Business Continuity:

•Business Continuity (BS7799):To counteract interruptions to business activities and to protect crtitical business processes from the effects of major failures or disaster

ISO: International Organization for Standardization

IEC: International Electrotechnical Commission

Standard BS7799/ISO17799/ISO27002

- A differenza di altri standard più tecnologici, questo, utilizza un approccio di tipo organizzativo e si rivolge ai livelli più alti della organizzazione.
- Lo standard è una 'guida' per l'organizzazione verso una profonda conoscenza dei propri processi, flussi informativi e sistemi a supporto del business
- Vengono indicate delle best practices per l'attivazione dei controlli che l'organizzazione deve implementare, sia dal punto di vista organizzativo che tecnologico, per poter realizzare un processo di messa in sicurezza dei sistemi che hanno il maggior peso nella generazione del valore
- Principali controlli presi in considerazione per la Business Continuity sono:
  - ✓ Il processo di gestione della Business Continuity
  - ✓ L'analisi di impatto sulle attività dell'azienda
  - ✓ La redazione e la implementazione dei piani di Business Continuity
  - ✓ Il monitoraggio, il testing e la revisione dei piani di Business Continuity

- Da un punto di vista più tecnologico il NIST(National Institute of Standards and Technology) ha redatto delle raccomandazioni che forniscono indicazioni e strategie relativamente ai seguenti tipi di sistemi:
  - *Desktop e portatili*
  - *Server*
  - *Siti WEB*
  - *LAN/WAN*
  - *Sistemi Distribuiti*
  - *Mainframe*

- Il documento del NIST *"Contingency Planning Guide for Information Technology Systems"* fornisce le linee guida per la predisposizione del contingency plan per i sistemi informativi
- Il *contingency plan* si riferisce alle misure da applicare durante il verificarsi di una emergenza per ripristinare al più presto le funzionalità più rilevanti dei sistemi informativi
- Il NIST identifica i seguenti passi principali:
  - *realizzazione della BIA(Business Impact Analysis)*
  - *identificazione dei controlli preventivi*
  - *sviluppo delle strategie di recupero*
  - *progettazione, testing e esercizio del contingency plan*
  - *manutenzione e aggiornamento del piano*

Il NIST identifica le seguenti fasi da seguire nel caso di evento catastrofico:

1. **Attivazione**

l'evento si è verificato, è stato rilevato, il personale preposto deve essere avvertito e i danni prodotti devono essere stimati

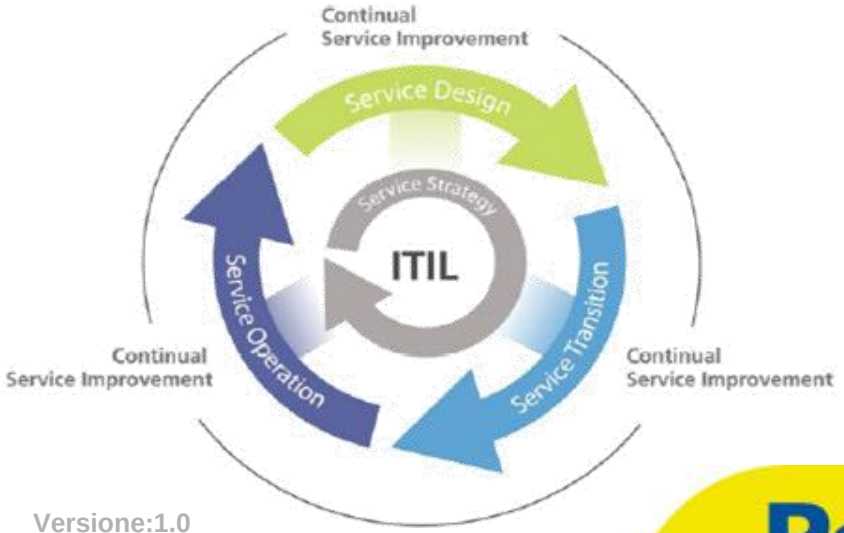
2. **Recupero**

le azioni che ciascun gruppo preposto deve compiere a fronte dell'evento rilevato

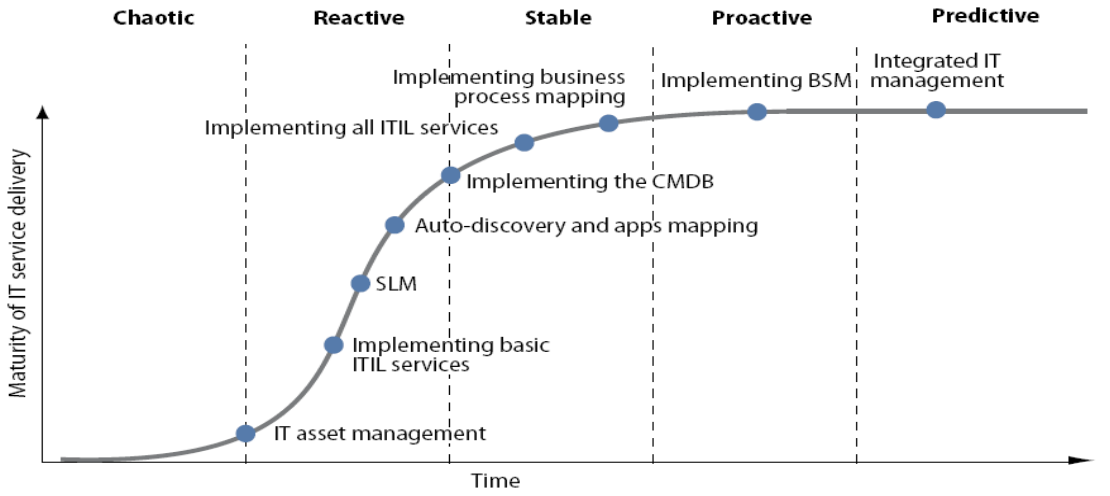
3. **Ricostituzione**

le azioni che devo essere messe in atto per ripristinare la normale operatività

- Molte organizzazioni di Information Technology hanno adottato per la gestione dei servizi la metodologia ITIL
- L'Information Technology Infrastructure Library (ITIL), sviluppata dall'UK Office of Government Commerce (OGC) a partire dalla fine degli anni '80, fornisce una raccolta completa e integrata di best practices per i processi IT.
- Essendo un framework, ITIL propone delle linee guida per la strutturazione dei processi IT e ne individua gli obiettivi, le attività generali, input e output, senza scendere nel dettaglio delle singole attività.



- Grazie a tale approccio è possibile inserire all'interno di un contesto strutturato le metodologie e le attività già in uso presso un'organizzazione, contribuendo in tal modo alla codifica delle interrelazioni tra i processi e favorendo la cooperazione tra le differenti funzioni.
- L'adozione di ITIL come standard di processo, permette di passare da una gestione reattiva dei servizi e delle infrastrutture IT ad una gestione proattiva, che previene l'insorgere dei problemi limitando così l'impatto sulla continuità e sull'efficienza dei servizi.



Source: Forrester Research, Inc.

Adempimenti di ordine legislativo - 1

- Il decreto legislativo n. 196 del 30 Giugno 2003 ‘ Codice in materia di protezione dei dati personali impone alcune misure di sicurezza dei dati.
- In particolare l’allegato B Disciplinare Tecnico in materia di misure minime di sicurezza indica che deve essere riportata nel Documento Programmatico della Sicurezza: *“…la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento…”* E nel caso di dati sensibili o giudiziari: *“…sono adottate idonee misure per garantire il ripristino dell’accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni…”*

Adempimenti di ordine legislativo - 2

- Il decreto legislativo n. 82 del 7 Marzo 2005 ‘ Codice dell’Amministrazione Digitale’ contiene l’articolo 50 bis che si riferisce esplicitamente al tema della continuità operativa e del Disaster Recovery.
- In particolare prescrive :”In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.”
- A tali fini, le pubbliche amministrazioni definiscono:
- *a)* il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
- *b)* il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

- Con ‘Basilea 2’ si intende il nuovo accordo internazionale (2001) sui requisiti patrimoniali delle Banche
- Le banche dei paesi aderenti dovranno accantonare quote di capitale proporzionali al rischio derivante dai vari rapporti di credito assunti
- Tra i rischi da prendere in considerazione vi sono anche i rischi operativi (frodi e indisponibilità sistema informativo)
- Le Banche Centrali dovranno vigilare sul rispetto dei criteri previsti
- Il **Disaster Recovery** e la **Business Continuity** rientrano quindi tra le attività di adeguamento a Basilea 2

Sarbanes – Oxley Act

- Emesso dal governo americano nel 2002 riguarda i controlli che devono essere presenti nelle aziende quotate sulla Borsa USA
- L'intento è quello di garantire la trasparenza e la tracciabilità delle operazioni compiute, a salvaguardia dei diritti degli azionisti
- Anche le aziende italiane quotate a Wall Street devono implementare i controlli previsti
- Sebbene il **Disaster Recovery** e la **Business Continuity** non siano citati esplicitamente è invece chiaro il richiamo alla implementazione dei backup e alle modalità per il recupero dei dati

Agenda

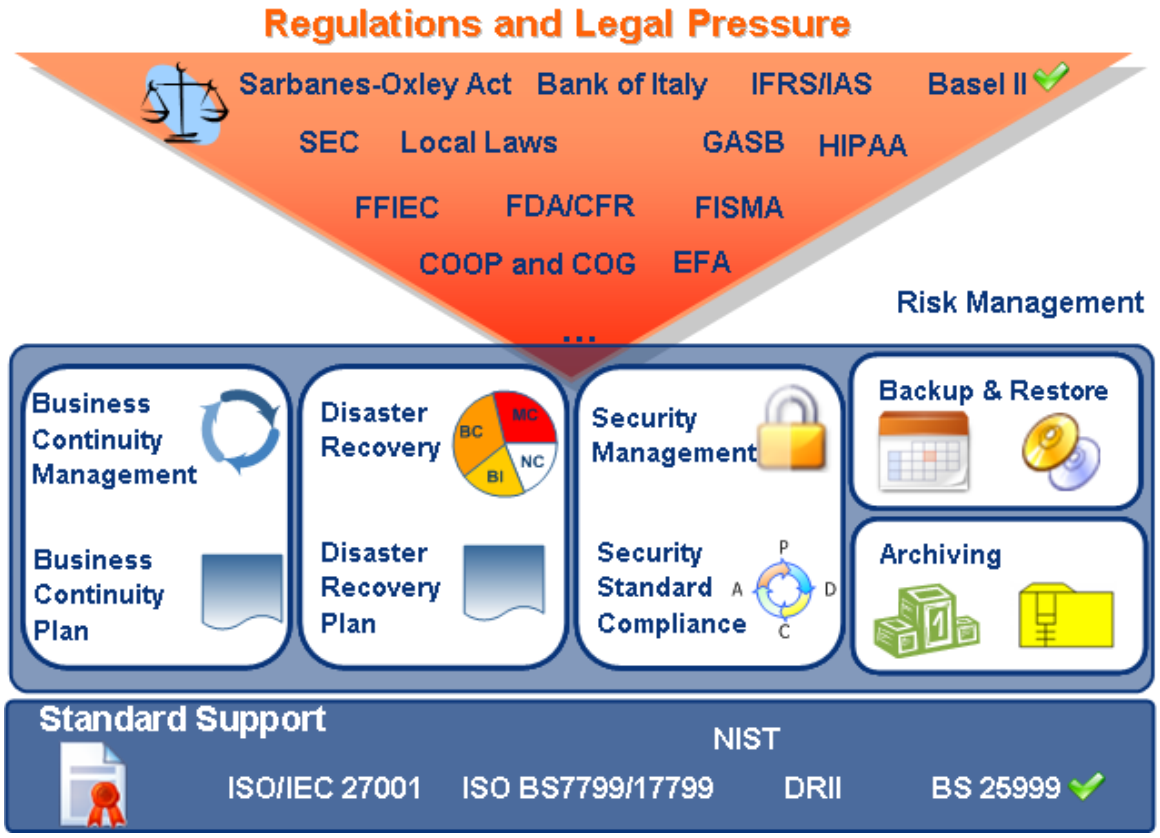
- **Introduzione**
  - *Terminologia e Standard*
  - *Normative Internazionali*
- **I fondamenti del Disaster Recovery e della Business Continuity**
  - *Panoramica delle soluzioni disponibili*
  - *Descrizione delle tecnologie abilitanti*
  - *I piani e le procedure organizzative*
- **L'evoluzione della soluzione di Disaster Recovery in Poste Italiane**
  - *2006. Soluzione con Nastri a freddo*
  - *2007. Soluzione con Replica asincrona dei dati*
  - *Oggi. Soluzione SRDF-Star*

Perchè il Disaster Recovery?

- Limitare le perdite dovute a riduzione di revenue o ad altri costi
- Minimizzare l'interruzione di Processi Business Critical
- Soddisfare ai requisiti imposti da obblighi di compliance 
- Evitare di compromettere la reputazione e la solidità della azienda
- Definire dei processi semplificati di decisione e di azione per fronteggiare una situazione imprevista
- Preservare le business operations e "sopravvivere" in caso di possibili failures
- Prevedere un ritorno "controllato" alla normale operatività

The Business Problem

La metodologia per la Business Continuity aiuta le aziende nel proteggere il loro business e nell'ottenere la compliance con le leggi internazionali e le regolazioni, riducendo i rischi e migliorando il rapporto prestazioni/costi.



Basilea II è il nuovo accordo sui requisiti patrimoniali delle banche; è un programma obbligatorio al fine di ridurre:

- **Credit Risk**. Le banche sono tenute a immagazzinare in maniera più strutturata i dati sensibili e storici.
- **Rischio operativo**, che è stato definito come "il rischio di perdita derivante dai processi interni inadeguati o in fault, dalla gente e dai sistemi o dagli eventi esterni". La banca deve valutare il loro grado del rischio operativo.

Prepararsi al Disaster Recovery

Presupposti per rispondere efficientemente ad una situazione di emergenza:

- **Criteri** per riconoscere una **Condizione di "Disastro"** e attivare le **Politiche d'Intervento**
- **Conoscenza** della **Criticità** dei **Dati**, delle **Applicazioni** e la loro **Priorità**
- **Obiettivi Misurabili** per il **Ripristino del Servizio**

Prepararsi al Disaster Recovery

- **Valutare** il potenziale **danno al business** derivante dall'indisponibilità prolungata delle **Applicazioni** e/o dei **Dati Aziendali**.
- **Pianificare** contromisure tecnologiche e organizzative per prevenire o gestire le **Emergenze**
- **Progettare** risorse e processi per prevenire e fronteggiare le emergenze
- **Implementare** sistemi e procedure operative di supporto
- **Eseguire** le procedure operative ordinarie di custodia dei **Dati** e della **Configurazione**
- **Verificare** periodicamente e sistematicamente l'efficacia e l'efficienza di tutte le procedure di gestione delle emergenze
- **Intervenire** sulle **Non-Conformità**
- **Pianificare** il miglioramento continuo dell'intero sistema

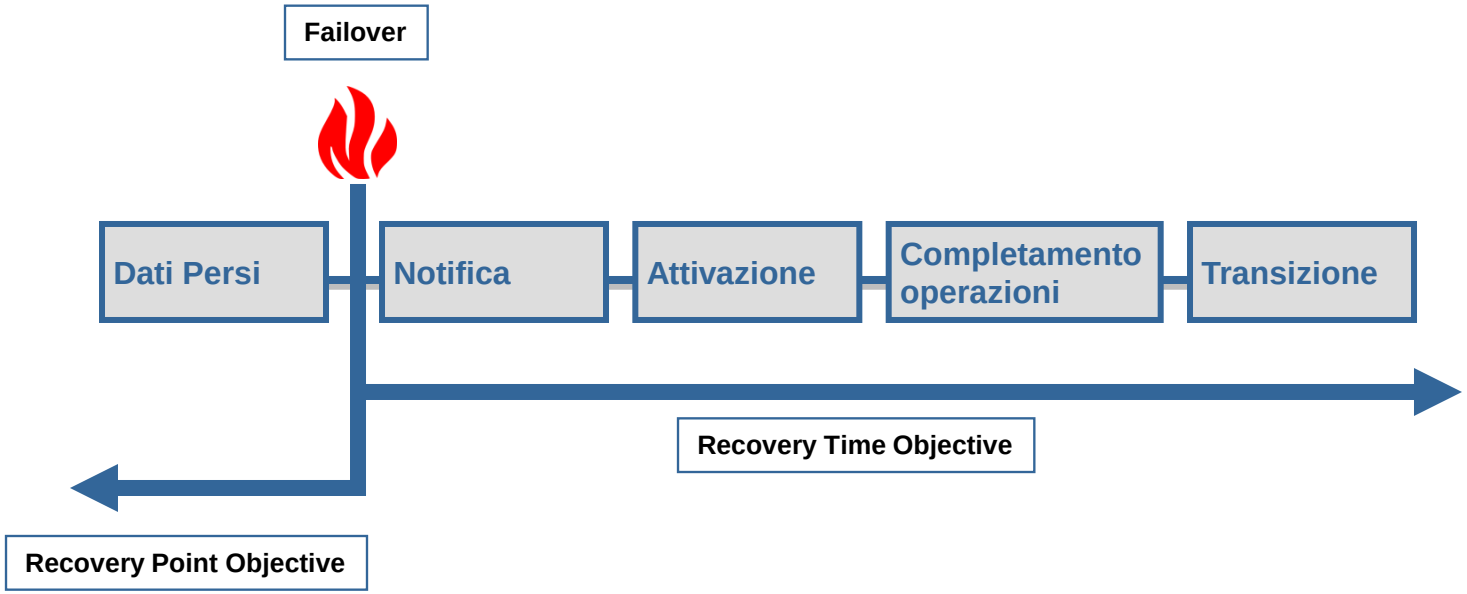
Non è un intervento "una tantum" ma un

Processo Operativo/Gestionale continuo

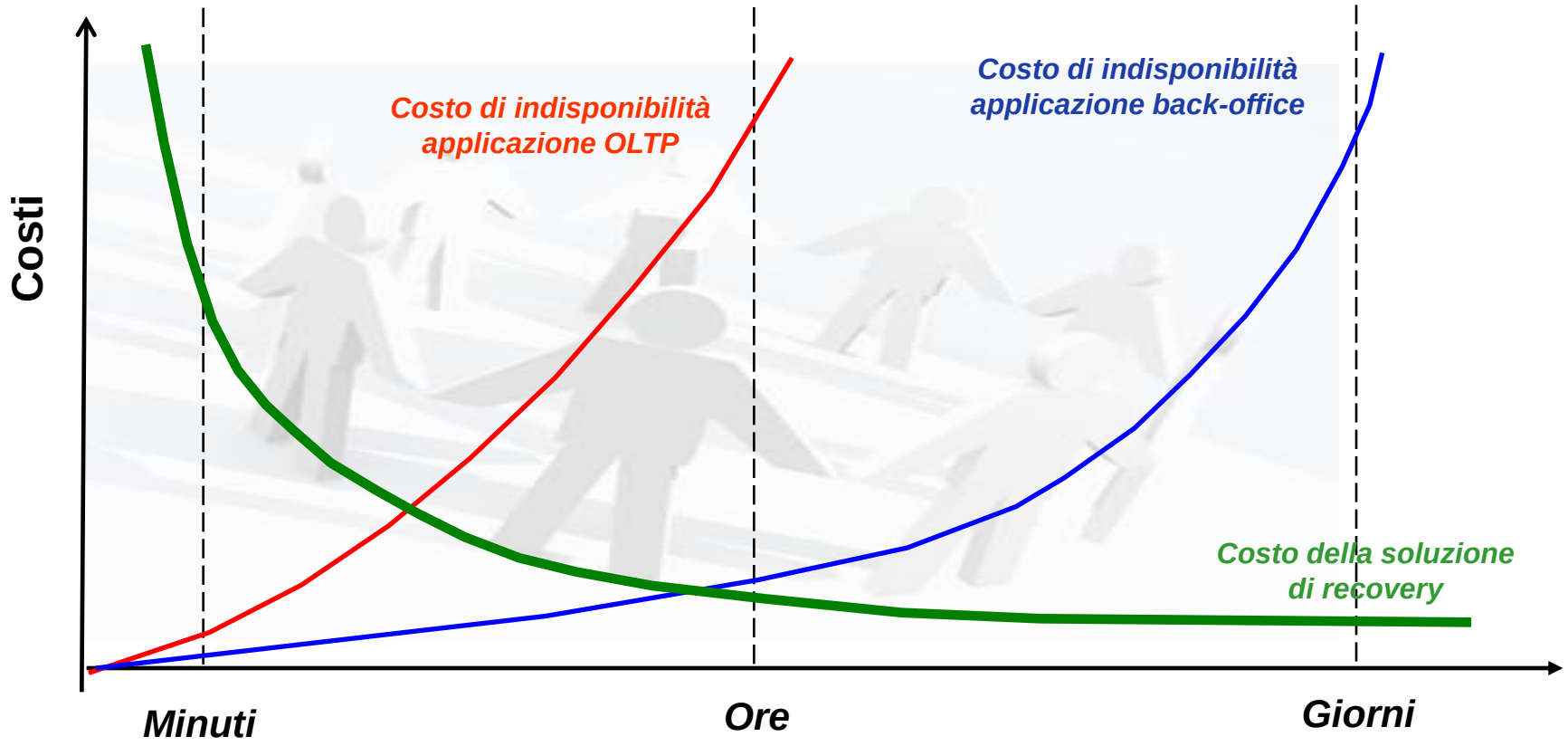
Prepararsi al Disaster Recovery

I requisiti di Business si traducono in requisiti Tecnologici, le cui metriche sono:

- **RTO** (Recovery Time Objective) = esprime in unità di tempo, l'intervallo temporale ammissibile di indisponibilità dei sistemi in seguito ad un disastro.
- **RPO** (Recovery Point Objective) = esprime in unità di tempo, l'ammontare massimo di dati che possono essere persi in seguito ad un disastro.



➔ Costi e benefici delle soluzioni di Recovery



- Anche per il parametro **RPO i costi aumentano sensibilmente al diminuire del suo valore**
- Esso è associato alla importanza del dato, e cioè quante informazioni siamo disposti a perdere a fronte di un disastro.
- Dipende dalla distanza esistente tra i vari Data Center
- Esso inoltre dipende dalla struttura organizzativa della azienda e dalla capacità di recuperare i dati persi attraverso procedure specifiche

"In ogni progetto di Disaster Recovery occorre tenere sempre presente che l'elemento più importante è sempre il dato perché talvolta non recuperabile"

Valutazione RTO e RPO

- Da un punto di vista metodologico la modalità largamente adottata per la determinazione dei parametri RTO e RPO è quella basata su:

  - **Business Impact Analysis (BIA)**
  - **Risk Assessment (RA)**

Business Impact Analysis

- Tecnica per l'identificazione degli asset critici di un determinato processo di business aziendale
- Analizza la criticità degli asset (personale, sedi, strumenti di lavoro, sistemi IT) in relazione all'impatto sul funzionamento del processo
- Valuta le potenziali perdite economiche derivanti dalla interruzione o dal grave degrado nel funzionamento di un processo
- I processi vengono analizzati nella loro completezza (end-to end) tenendo in considerazione non soltanto gli asset interni ma anche quelli esterni all'azienda

In particolare per i sistemi IT costituiscono obiettivi della BIA:

- identificazione delle applicazioni business critical e della infrastruttura tecnologica(Data Center,Linee TLC, server, storage, ecc.) su cui sono installate
- identificazione delle vulnerabilità degli ambienti tecnologici e analisi per le aree a maggior rischio dei Sigle point of failure(SPOF) e dei corrispondenti tempi di recupero

- Il processo di Risk Assessment (RA) non considera soltanto le vulnerabilità esistenti ma anche le minacce che gravano sui processi critici e le conseguenze che ne potrebbero derivare
- Vengono analizzati i controlli previsti a contenere gli effetti delle minacce incombenti
- I metodi più comunemente utilizzati per eseguire il RA sono due:
  - metodo quantitativo
  - metodo qualitativo

Nell'utilizzare il **metodo quantitativo** vengono presi in considerazione due elementi fondamentali:

- La probabilità che un evento si verifichi
- L'impatto, cioè la perdita economica che Il verificarsi dell'evento produrrebbe

- Si definisce quindi un parametro, detto Costo Stimato Annuale, ottenuto per ciascun evento come prodotto della perdita potenziale per la probabilità che si verifichi
- Tale metodo non è molto preciso principalmente perché la probabilità è stimata su base statistica

Risk Assessment – Metodo qualitativo

Nell'utilizzare il **metodo qualitativo** vengono valutati i seguenti elementi:

- Minacce
- Vulnerabilità
- Controlli:
  - *Deterrenti*
  - *Preventivi*
  - *Detettivi*
  - *correttivi*
- Vengono definiti degli scenari e per essi vengono eseguiti dei test di accettabilità confrontando i risultati con i requisiti attesi
- Si definiscono quindi delle decisioni di salvaguardia per colmare i livelli tra il rischio misurato e quello accettabile
- Si ricicla sui test di accettabilità fino a che il rischio misurato non risulti entro i criteri di accettabilità

Determinazione RTO e RPO

- I risultati ottenuti mediante BIA e RA vengono presi in considerazione nell'ambito di una analisi costi benefici per determinare i corretti valori di RTO e RPO che guideranno la implementazione della soluzione di Disaster Recovery
- Vengono inoltre individuate le dipendenze e le priorità da seguire nel ripristino dei sistemi e delle applicazioni
- Tutto confluisce nel documento fondamentale del Disaster Recovery che è il DRP(Disaster Recovery Plan)

È il documento che formalizza i parametri di RTO e RPO ottimali per il contesto di business in esame

ESEMPIO

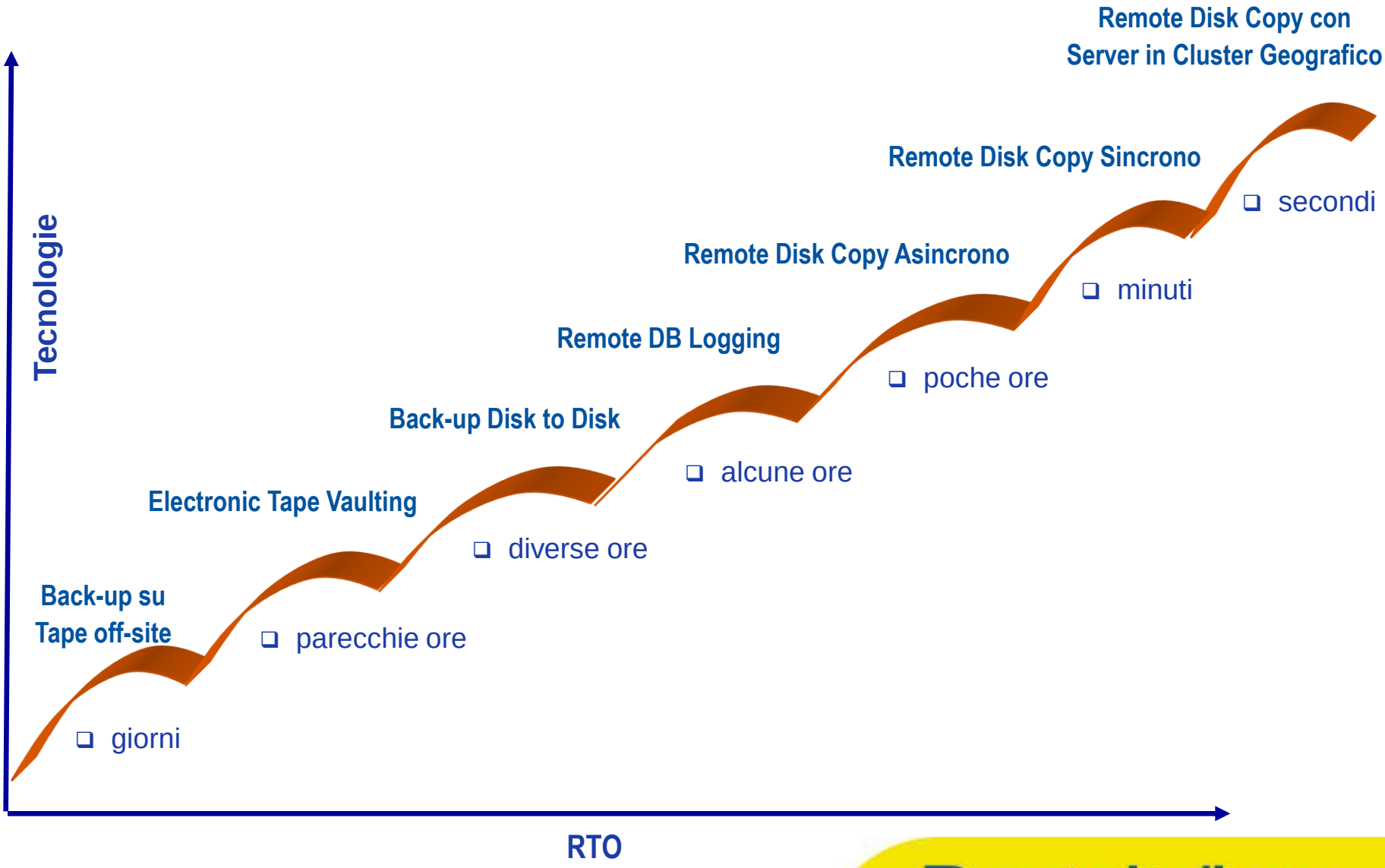
Tempo di Ripristino	Basso	Medio	Alto
Riduzione Perdite	M€	M€	K€
Costo del Ripristino	10M€	100K€	K€
Delta Benefici-Costi	negativo	**Positivo**	nessuno

Il parametro di RTO deve essere mediato tra il valore delle perdite economiche prodotte durante il tempo che intercorre tra il disastro e la ripartenza del servizio e i costi della soluzione necessaria a garantire la ripartenza del servizio

Disallineamento Dati	Basso	Medio	Alto
Incremento Perdite	K€	100K€	M€
Costo Allineamento	10M€	M€	100K€
Delta Benefici-Costi	negativo	negativo	**Positivo**

Il parametro di RPO deve essere mediato tra il valore delle perdite economiche prodotte dal disallineamento dati e i costi della soluzione necessaria a garantire l'allineamento tra il sito di DR e quello di produzione

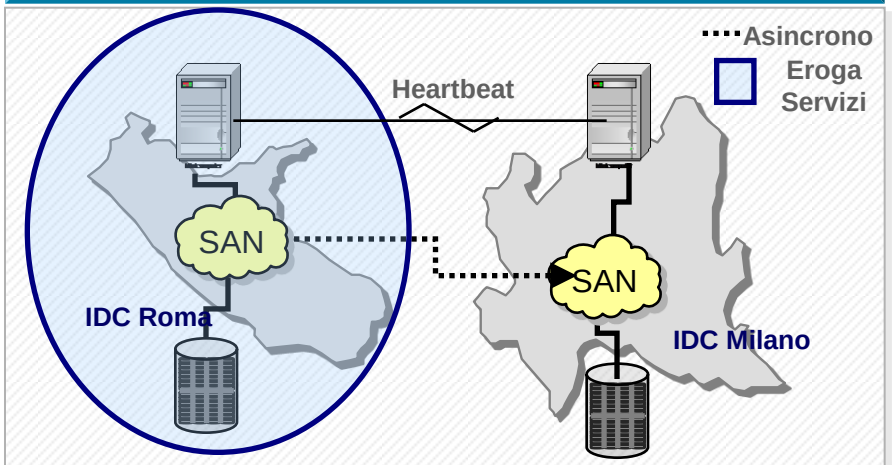
➔Tecnologie e tempi di RTO



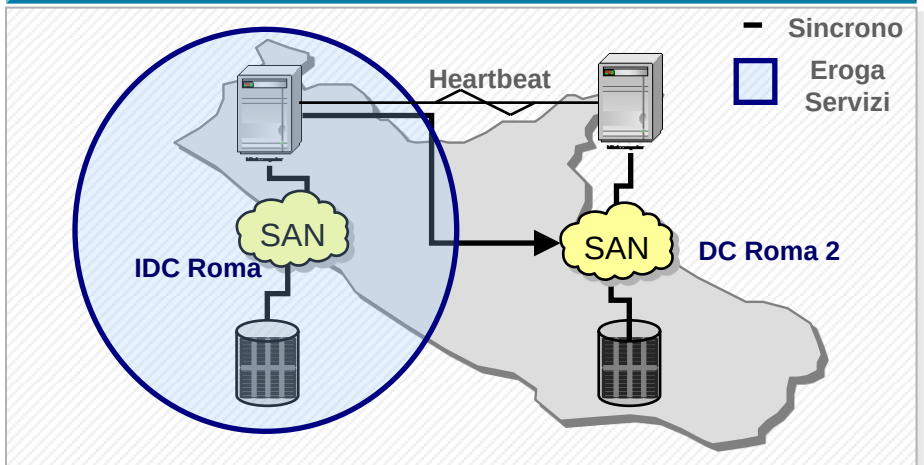
Cluster geografico e metropolitano

Il valore di RTO può essere significativamente ridotto mediante l'utilizzo di configurazioni di cluster geografico o metropolitano

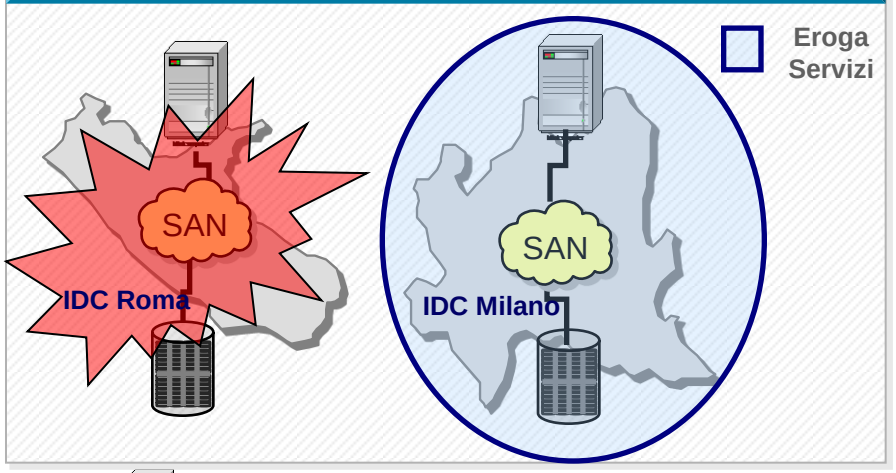
Ambito DR - Cluster Geografico



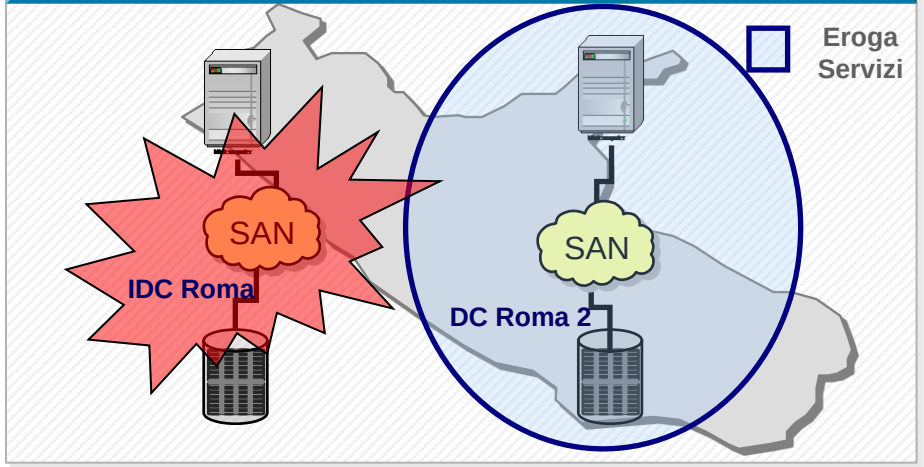
Ambito BC - Cluster Metropolitano



Ambito DR - Risposta al disastro



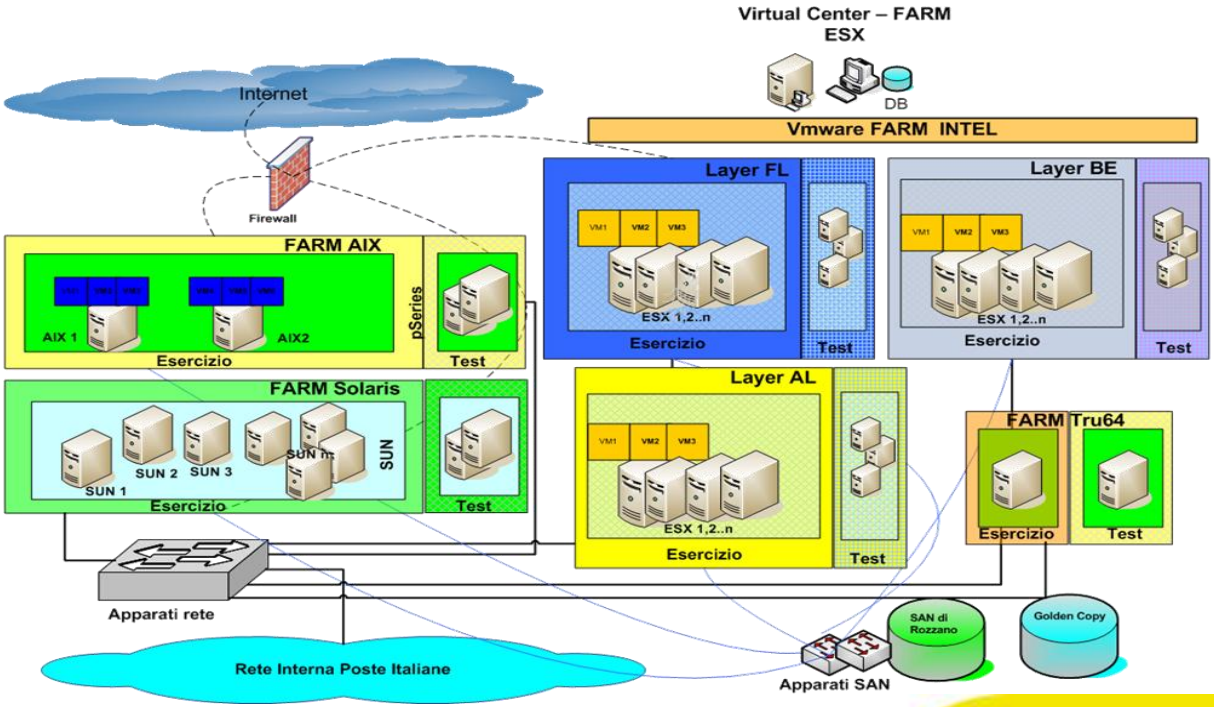
Ambito BC - Risposta al disastro



Server Storage

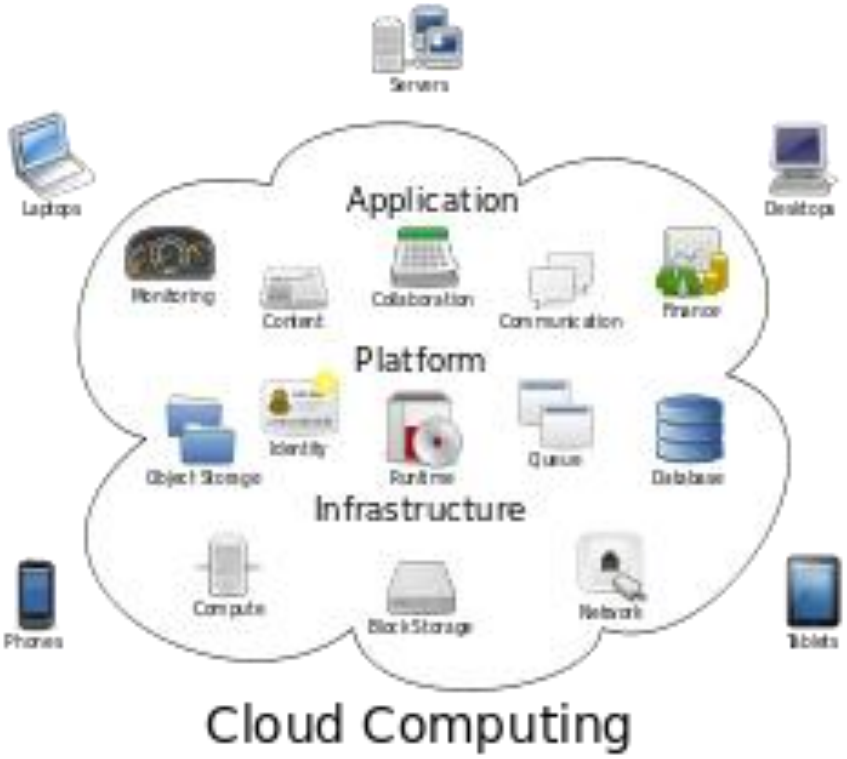
Sistema di consolidamento e virtualizzazione server per DR

- Virtualizzazione e Consolidamento dei Server
  - Flessibilità, Efficacia e Convenienza Economica della Soluzione
  - Per IBM RISC con AIX viene usata la tecnologia IBM POWER Virtualization
  - Per INTEL viene usata la tecnologia VMWARE
- Replica Fisica dei Server e procedure di Clonazione (solo nei casi indispensabili)
  - Risorse pronte per ripartire tempestivamente

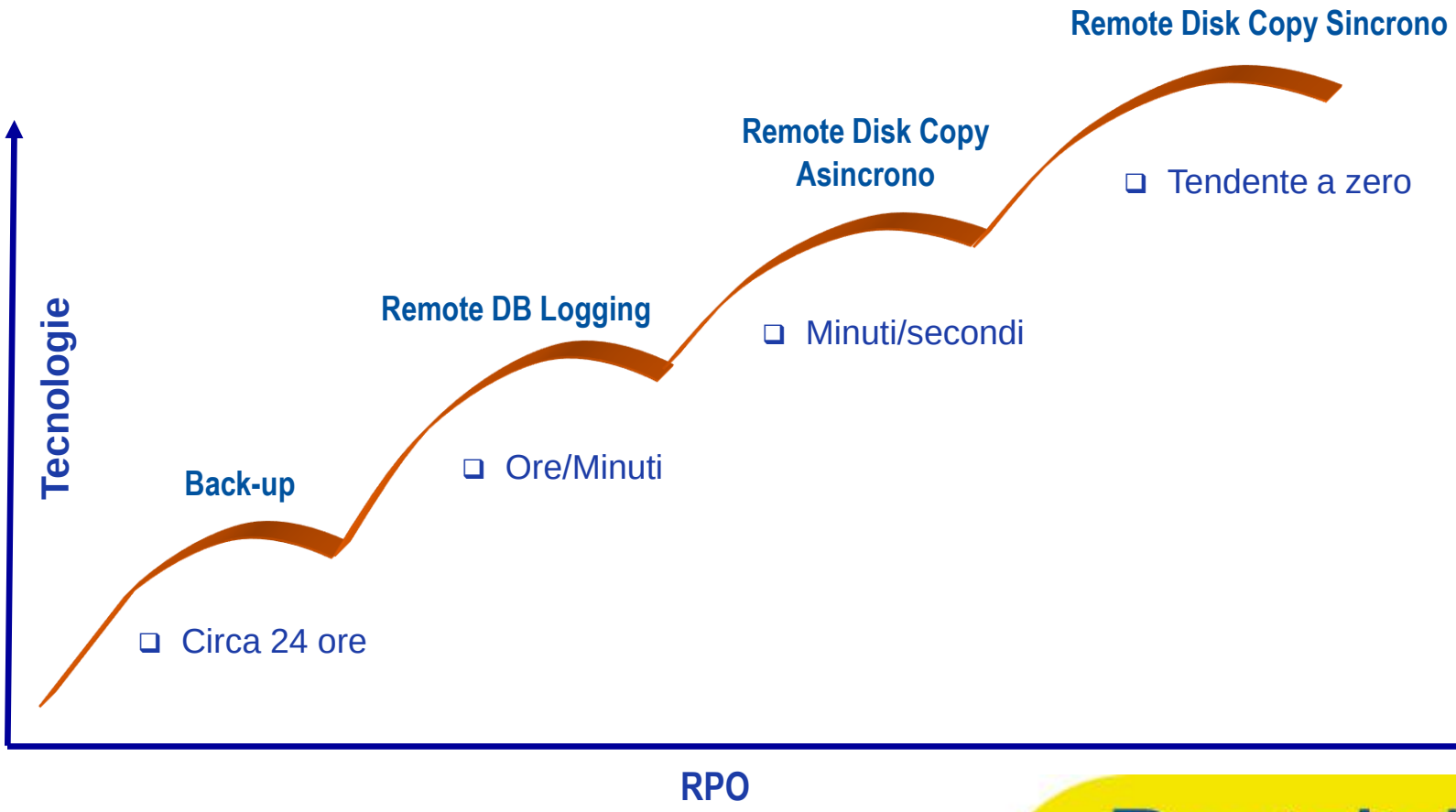


Il cloud Computing

- Cos'è il Cloud Computing ?
  - Il cloud computing è un modello per abilitare ubique,comode e on demand reti di accesso a pool condivisi di risorse computazionali configurabili (es. network, servers, storage, applicazioni e servizi) che possono essere ottenute rapidamente con minimo sforzo di gestione ed una limitata interazione con il service provider (NIST sp800-145)
- 3 Modelli di Servizio
  - IaaS Infrastructure as a Service
  - PaaS Platform as a Service
  - Saas Software as a Service
- La continuità operativa è un obbligo
  - Tutti i provider di servizi in modalità cloud computing devono dotarsi di soluzioni di Business Continuity



➔Tecnologie e tempi di RPO



Il salvataggio dei dati

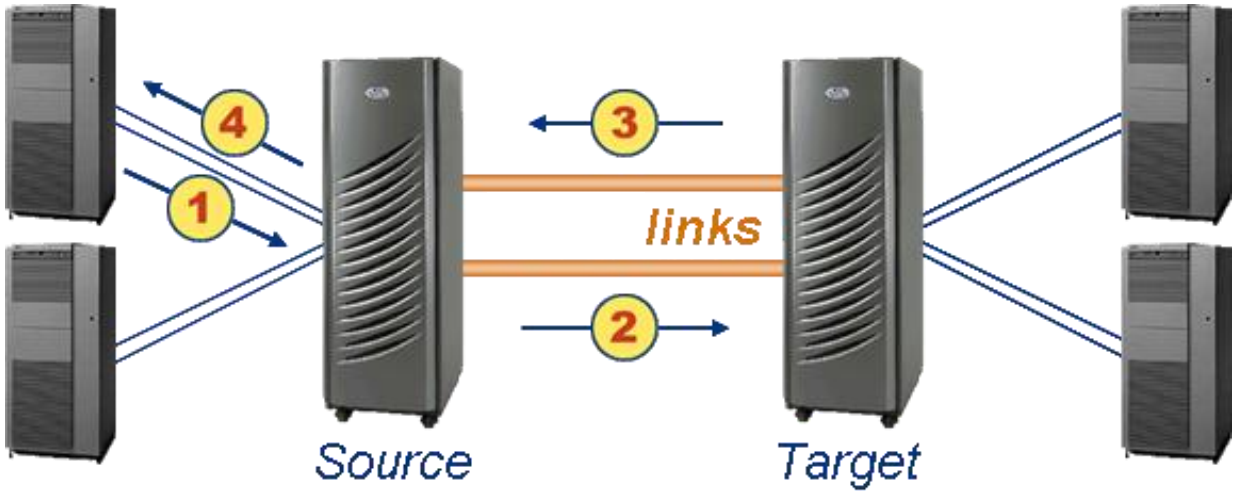
- L'elemento più critico è costituito dai dati in quanto rappresentano l'asset più fragile e quello completamente irrecuperabile
- L'informazione associata al dato è spesso quella fondamentale per l'erogazione dei servizi
- Storicamente il dato viene salvato mediante back-up su nastro
- Le evoluzioni tecnologiche dei dischi e la loro riduzione di costo consentono di realizzare delle soluzioni di back-up Disk to Disk
- Tuttavia anche i nastri hanno subito una importante evoluzione tecnologica che ne ha migliorato le prestazioni e la capacità(> 1TB)
- Le soluzioni di DR basate sul back-up dei dati presentano valori di RTO e RPO molto alti

La duplicazione dei dati

- Per ottenere un sensibile miglioramento del parametro RPO è necessario adottare una tecnica di duplicazione remota dei dati
- E' possibile replicare i dati in modo continuo e completo (mirroring geografico) oppure inviare soltanto le variazioni delle basi dati (Remote DB logging)
- In relazione alla distanza e alle caratteristiche del sito di DR è possibile attivare la replica sincrona o asincrona dei dati
- La replica può essere ottenuta utilizzando delle funzionalità proprie dei sottosistemi storage (Vendor dependent) oppure mediante funzionalità di software specifici di Data mirroring (Server dependent)

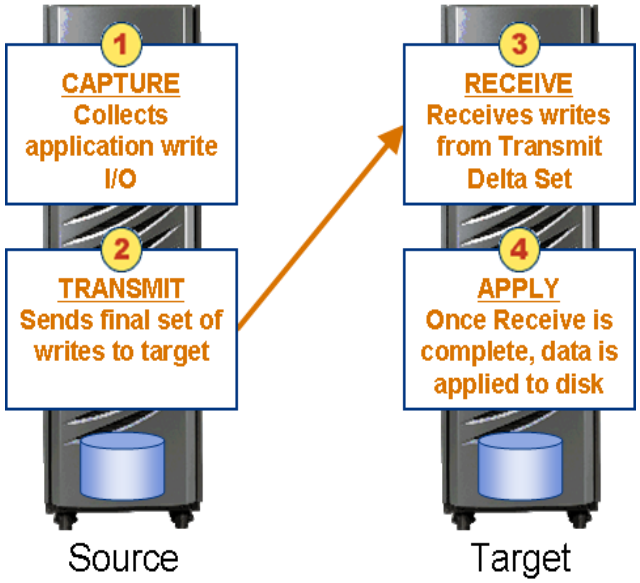
➔ Sincrono

1. L’operazione di scrittura viene ricevuta nelle cache dello storage Source,
2. L’operazione di I/O viene trasmessa alla cache del Target,
3. Un acknowledgment è inviato dal Target alla cache del Source,
4. Un status di fine operazione viene presentato al server.



➔Asincrono

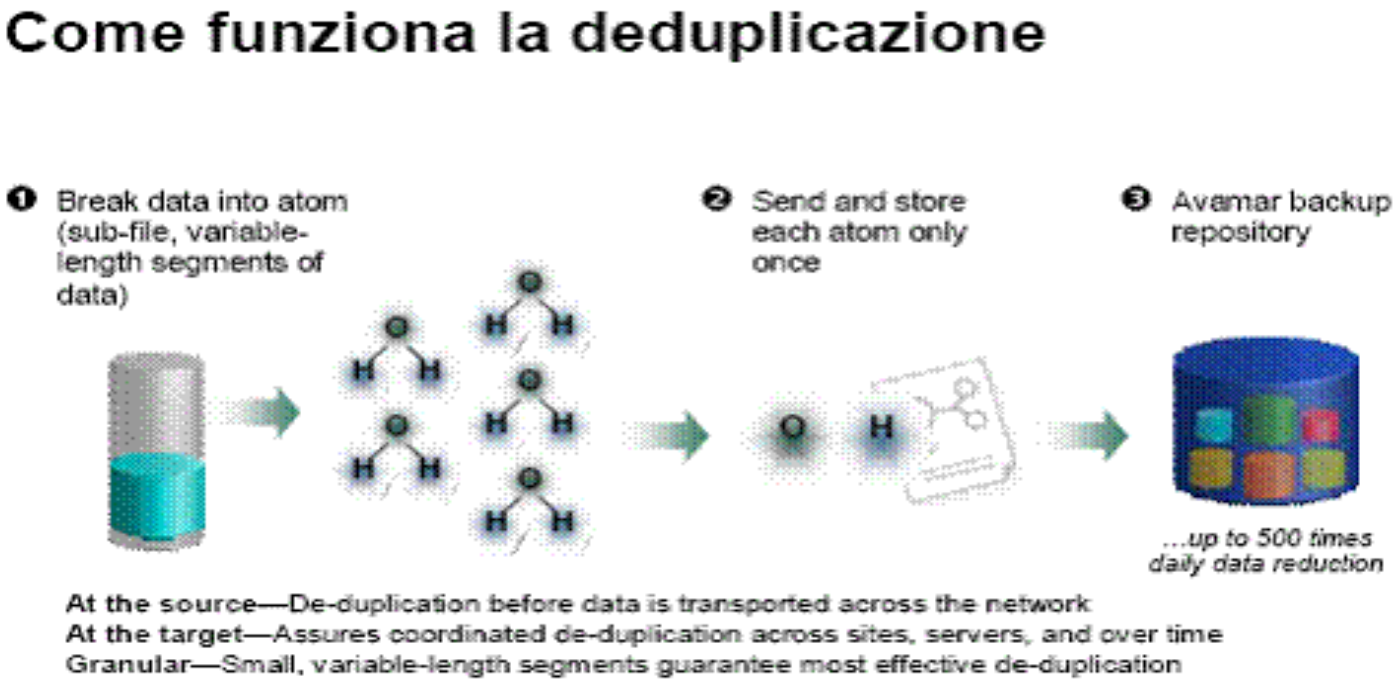
- Le operazioni di scrittura vengono catturate dall'unità 'Source' in cache nel (**Capture**). Al completamento del ciclo il 'Delta set' viene consolidato (**Transmit**), in modo da remotizzare sul sito secondario solo l'ultimo aggiornamento associato ad uno specifico blocco di una traccia. I dati trasmessi sono ricevuti dall'unità 'Target' Symmetrix (**Receive**). Se la trasmissione viene completata con successo, i dati vengono promossi (**Apply**) e da qui trasferiti su disco.



La de-duplicazione dei dati

- Negli ultimi tempi si sta affermando sul mercato una nuova tecnologia di memorizzazione dei dati detta de-duplicazione
- Questa tecnica consiste essenzialmente nel fattorizzare sequenze di dati identiche presenti su file o porzioni di file diversi memorizzandole una sola volta
- In questo modo e' possibile ridurre drasticamente lo spazio fisico necessario per memorizzare grandi quantità di dati soprattutto quelli del back-up
- Queste funzionalità sono spesso integrate direttamente nei sottosistemi di storage che inoltre possono replicare i dati in modo continuo sul sito alternativo di DR risparmiando sulla capacità della banda di rete necessaria

La de-duplicazione è un processo in cui ogni elemento di un dato è confrontato con un record di un dato memorizzato precedentemente al fine di identificare sequenze ripetute o ridondanti
Gli opportuni algoritmi di compressione provvedono a memorizzare soltanto una delle sequenze ripetute e a creare gli indici per la ricostruzione del dato completo



Il sito di Disaster Recovery

Se l'azienda predispone un sito dedicato al Disaster Recovery esso può essere classificato in:

Hot Site se il sito è completamente attrezzato con i sistemi, le linee TLC e con tutti i servizi necessari pronti ad essere attivati immediatamente

Warm Site se il sito è parzialmente attrezzato o presenta dei servizi la cui attivazione richiede del tempo

Cold Site se il sito dispone soltanto delle infrastrutture di base e di aklcuni servizi ridotti

Il sito di Disaster Recovery

Se l'azienda stipula degli accordi con altre organizzazioni per il sito dedicato al Disaster Recovery si possono avere le seguenti opzioni:

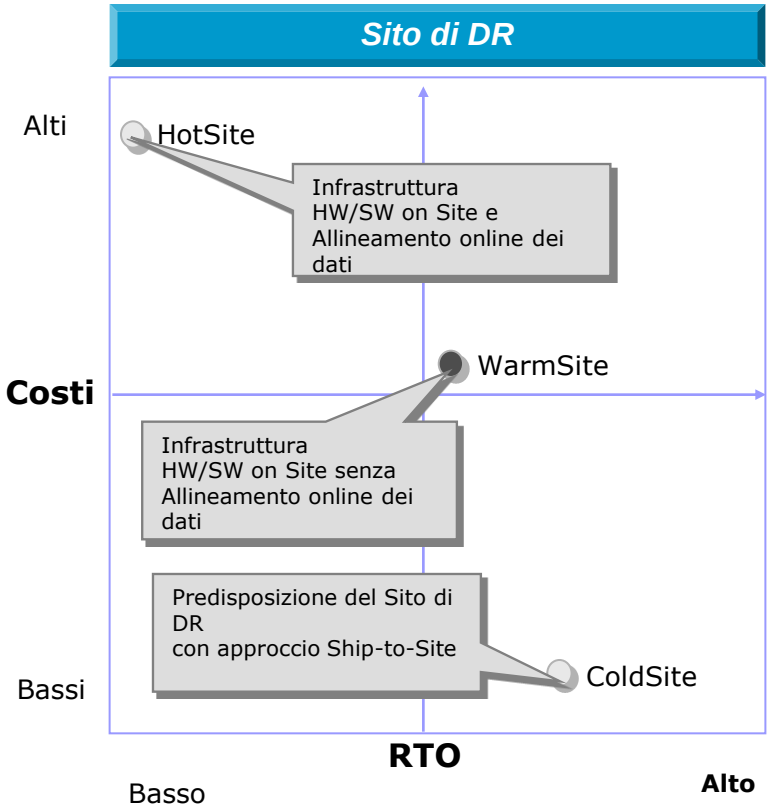
Timeshares se il sito è destinato a fornire servizi a diverse aziende mediante risorse che saranno approntate al bisogno

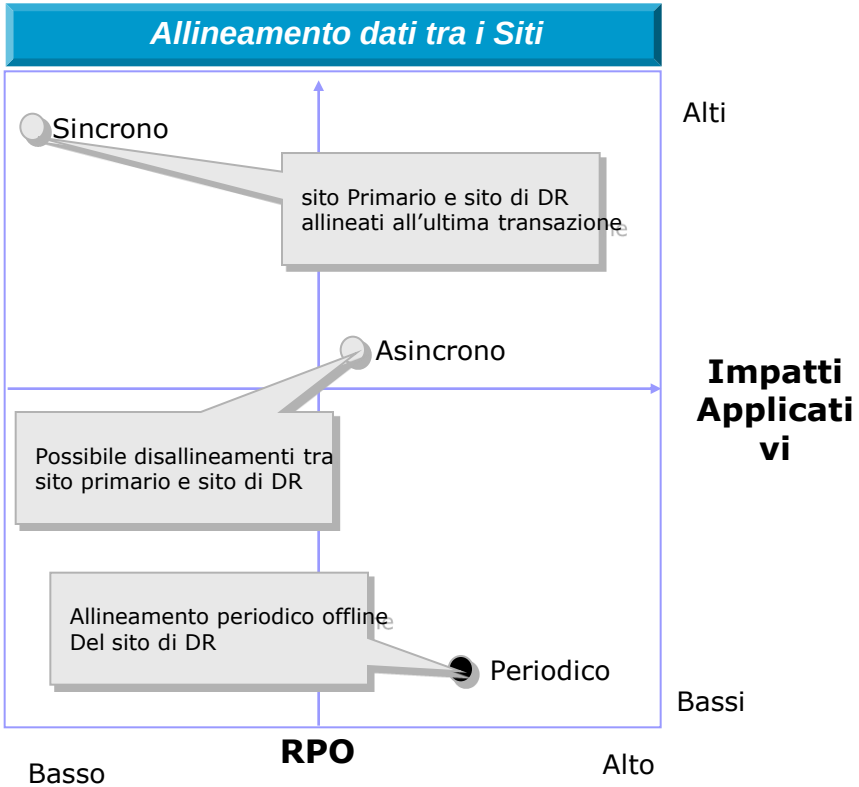
Accordi interaziendali quando aziende con tipologie di applicazioni e/o architetture simili si impegnano a fornire reciprocamente il sito di DR in caso di necessità

Rolling Mobile sites siti cioè realizzati utilizzando mezzi mobili quali TIR o altro specificatamente attrezzati per le necessità di Disaster Recovery

La valorizzazione dei parametri di RTO (Recovery Time Objective) e RPO (Recovery Point Objective) influenza i costi di realizzazione e gli impatti applicativi di una strategia di DR

ESEMPIO

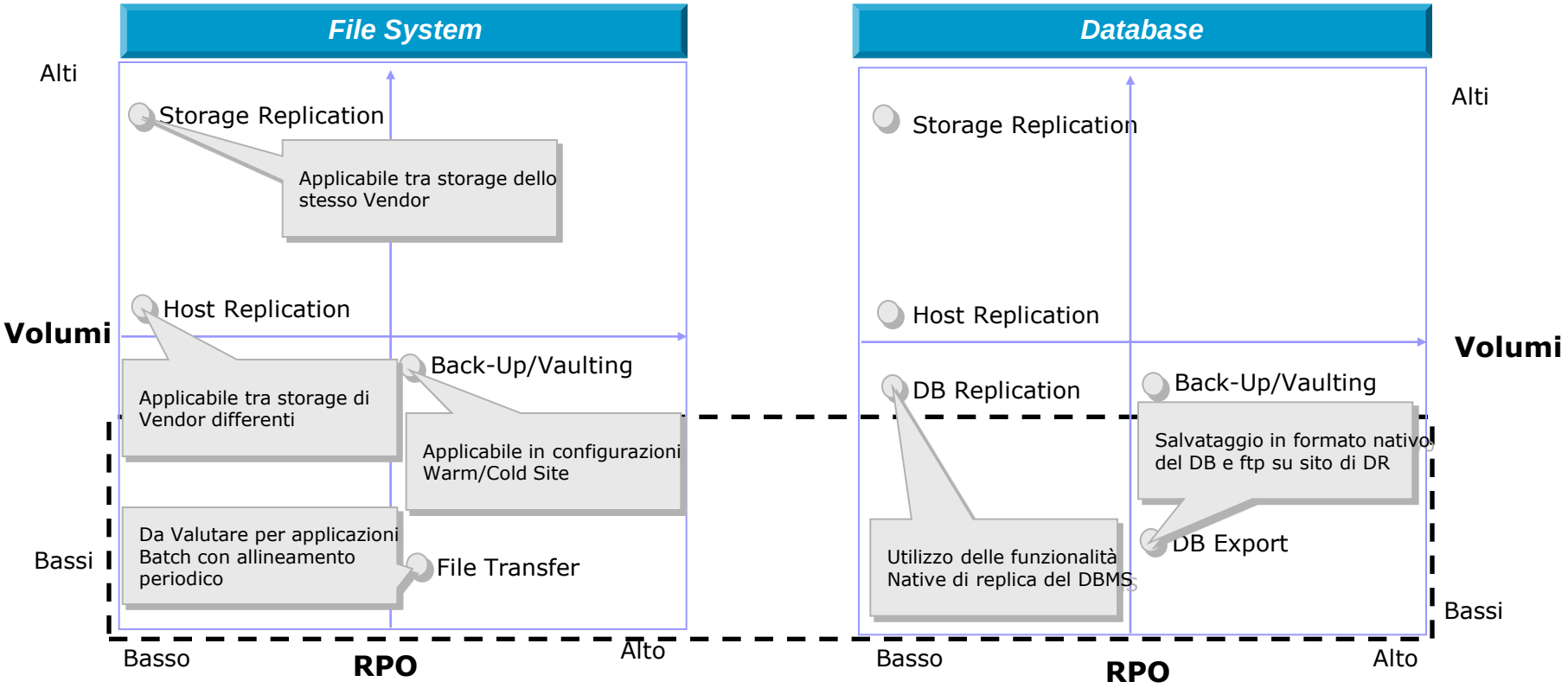




Possibili soluzioni tecnologiche ai requisiti del DRP

L'analisi dell'architettura Applicativa e Tecnologica dei sistemi coinvolti dalla strategia di DR, determina la scelta delle tecnologie opportune per la replica dei dati applicativi

ESEMPIO

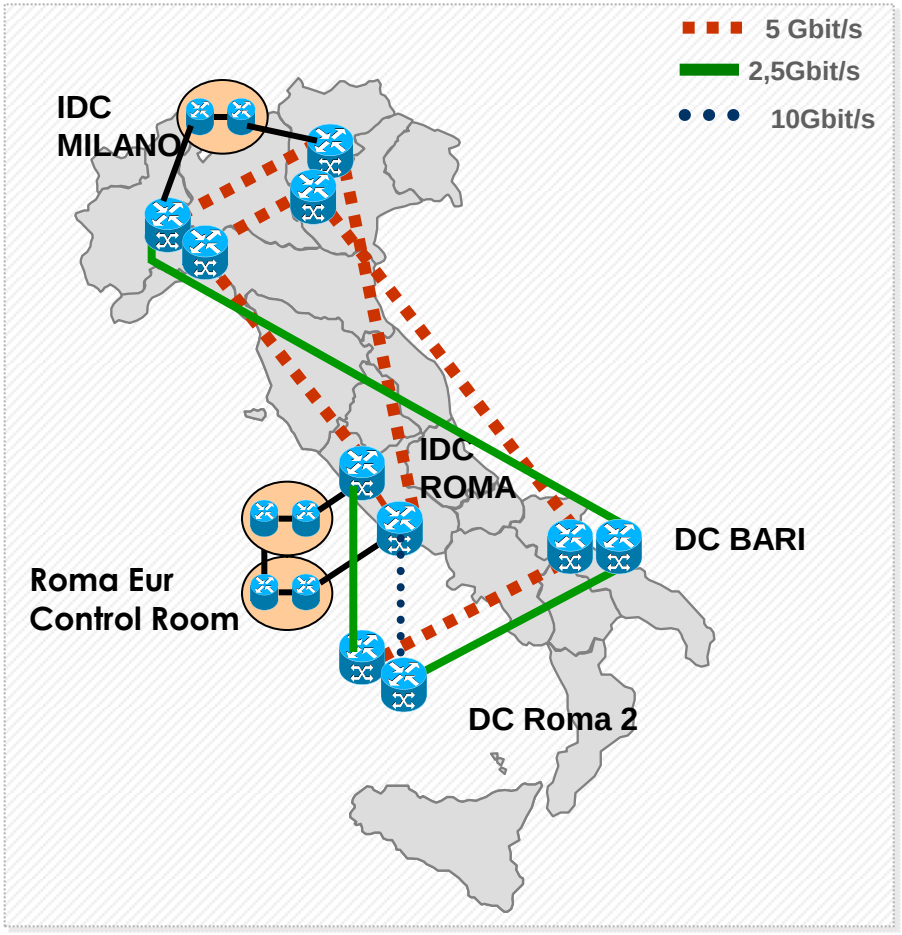


Possibili soluzioni tecnologiche ai requisiti del DRP

Le soluzioni di BC e DR devono poter contare su una rete TLC di caratteristiche adeguate

ESEMPIO

Rete di Interconnessione tra i Data Center (VDCN)



VDCN: Virtual Data Center Network

Rete ad alta velocità per il trasporto del traffico sul territorio nazionale e l'implementazione di servizi a valore aggiunto

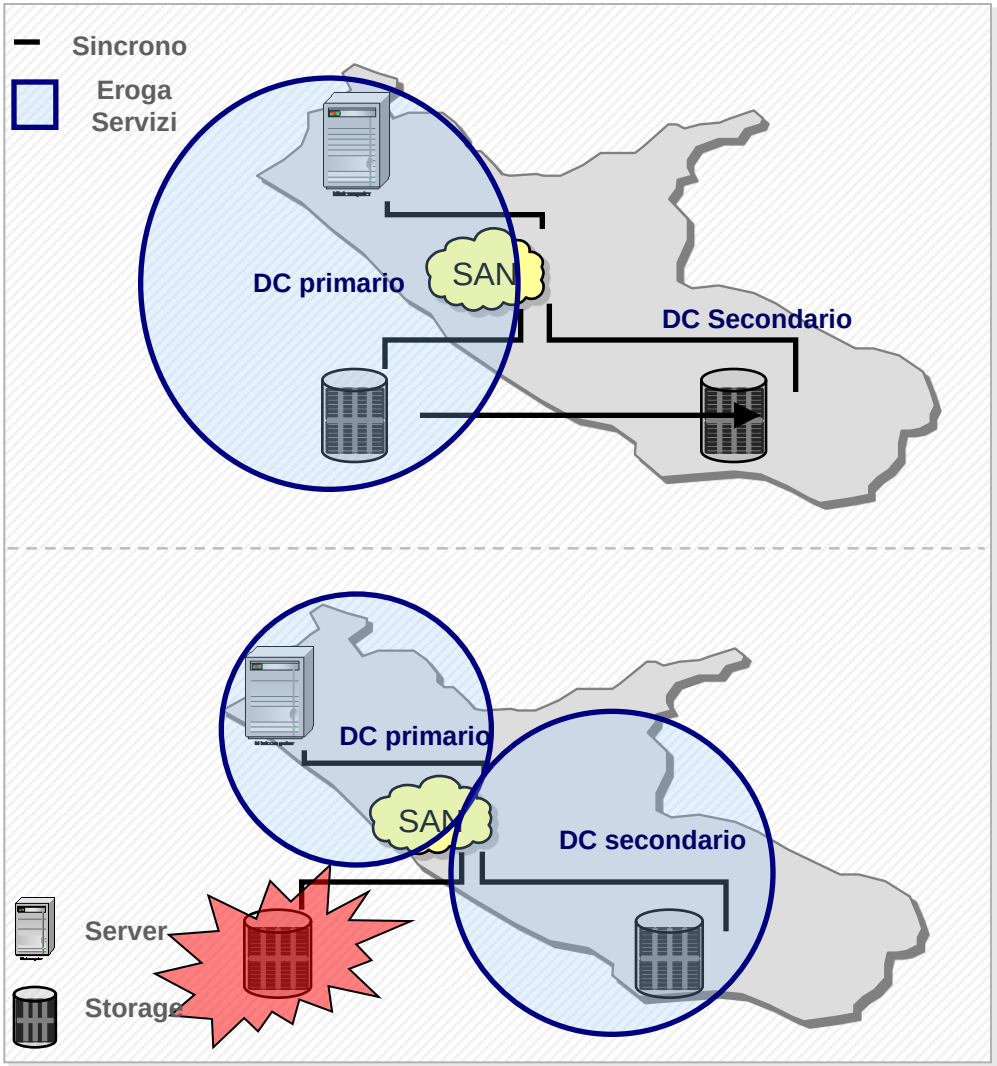
Infrastruttura in alta affidabilità capace di garantire la ridondanza del percorso fisico e logico

Permette l'erogazione di servizi di interconnessione diversi in funzione del Data Center

Infrastruttura di supporto per le soluzioni di DR e BC

BC con SAN Metropolitana

Architettura Logica



Allineamento dei Dati

1

Allineamento sincrono dello storage tra il sito primario e il sito secondario

Allineamento dei Server

1

Non in ambito

Risposta al disastro localizzato nel DC Primario

1

Ripartenza dello storage sul sito secondario senza perdita di dati, i server utilizzati per erogare i servizi rimangono quelli nel DC primario

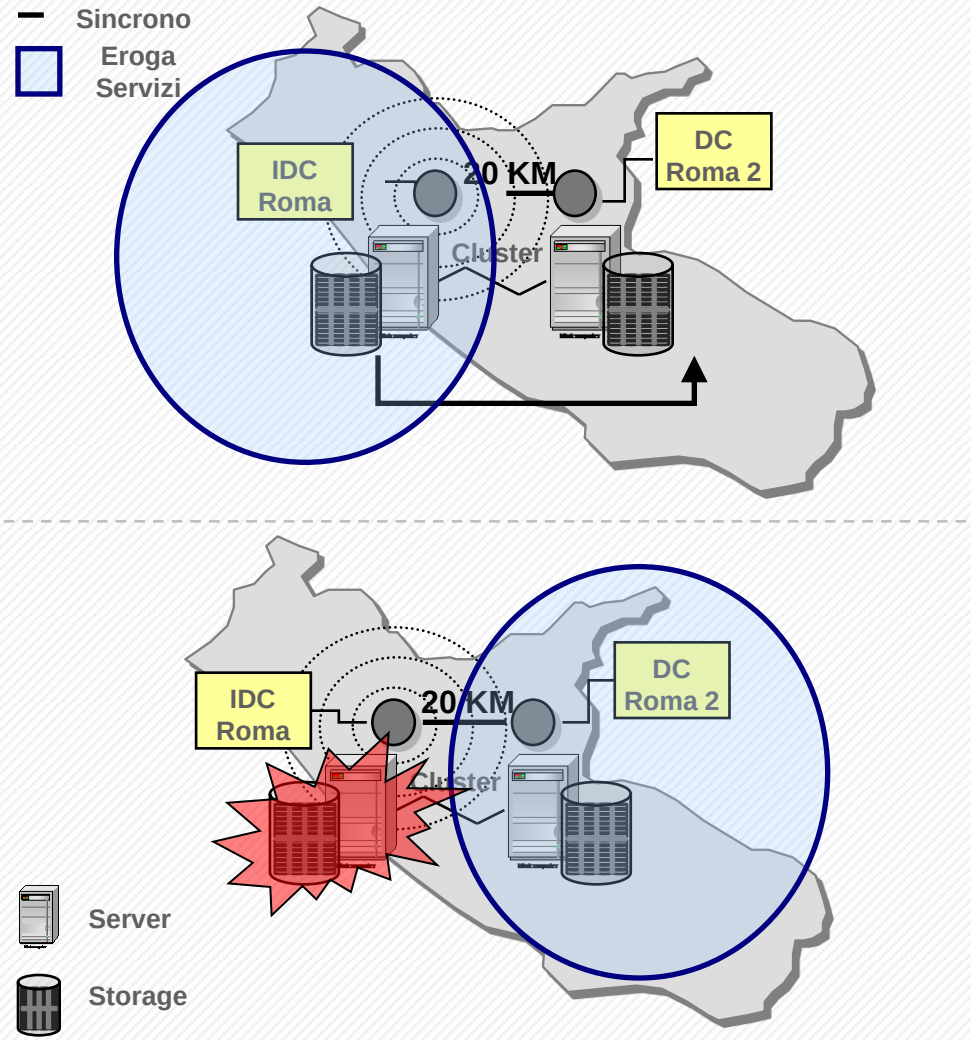
Risposta al disastro esteso

1

Non disponibile

BC con Cluster Metropolitano e Replica Sincrona

Architettura Logica



Allineamento dei Dati

1

Allineamento sincrono dello storage tra il sito primario IDC Roma e DC Roma 2

Allineamento dei Server

1

I server devono essere configurati in Modalità Hot e in Cluster Metropolitano

Risposta al disastro Localizzato nel IDC Roma

1

Ripartenza dei sistemi nel sito di BC (DC Roma 2) senza perdita di dati

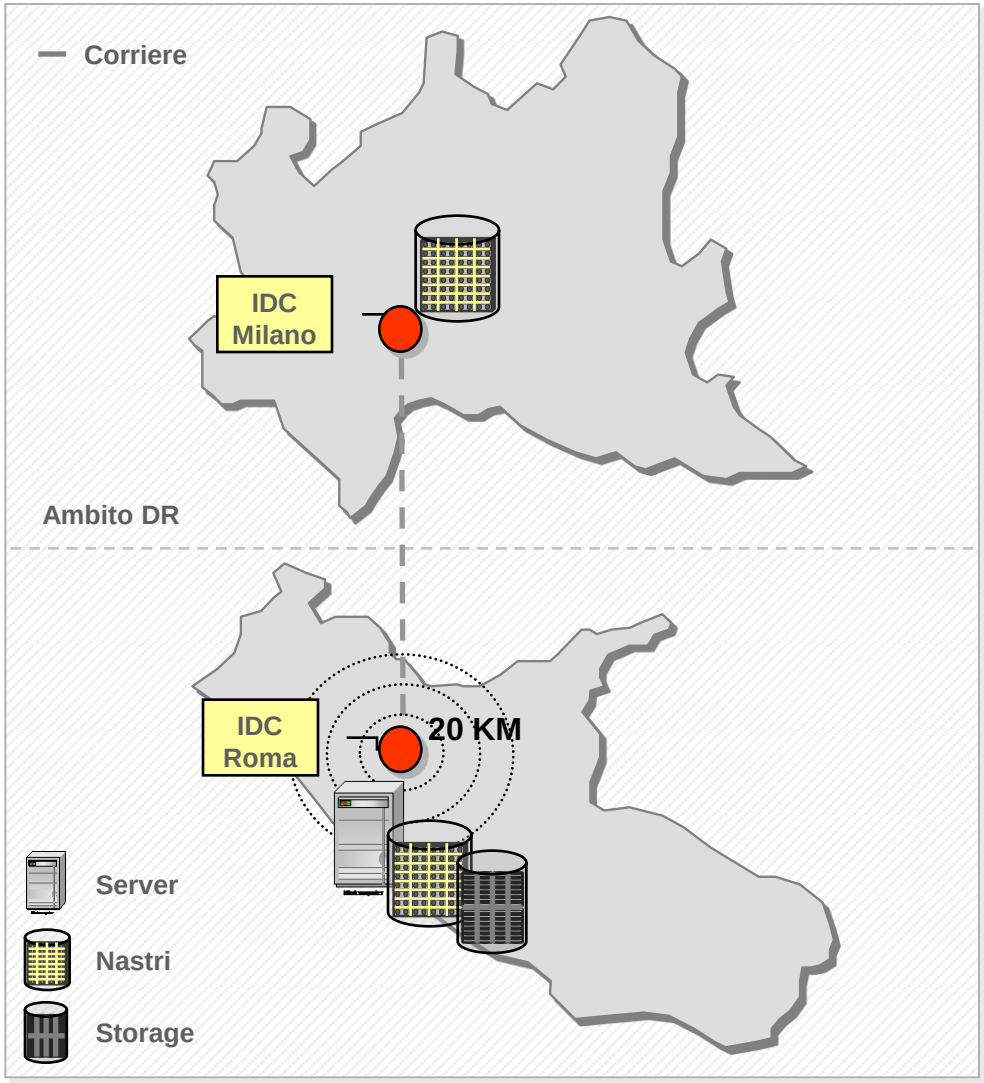
Risposta al disastro Esteso nell'area romana

1

Non disponibile

DR con Backup Remote Vaulting

Architettura Logica



Allineamento dei Dati

1. Il SW di gestione del backup crea i duplicati dei nastri oggetto di remote vaulting
2. I Nastri sono spediti nel sito remoto con la frequenza necessaria a soddisfare i requisiti di RPO

Allineamento dei Server

1. I server possono essere configurati in modalità
   - Hot
   - Warm
   - Cold

Risposta al disastro Localizzato nel IDC Roma

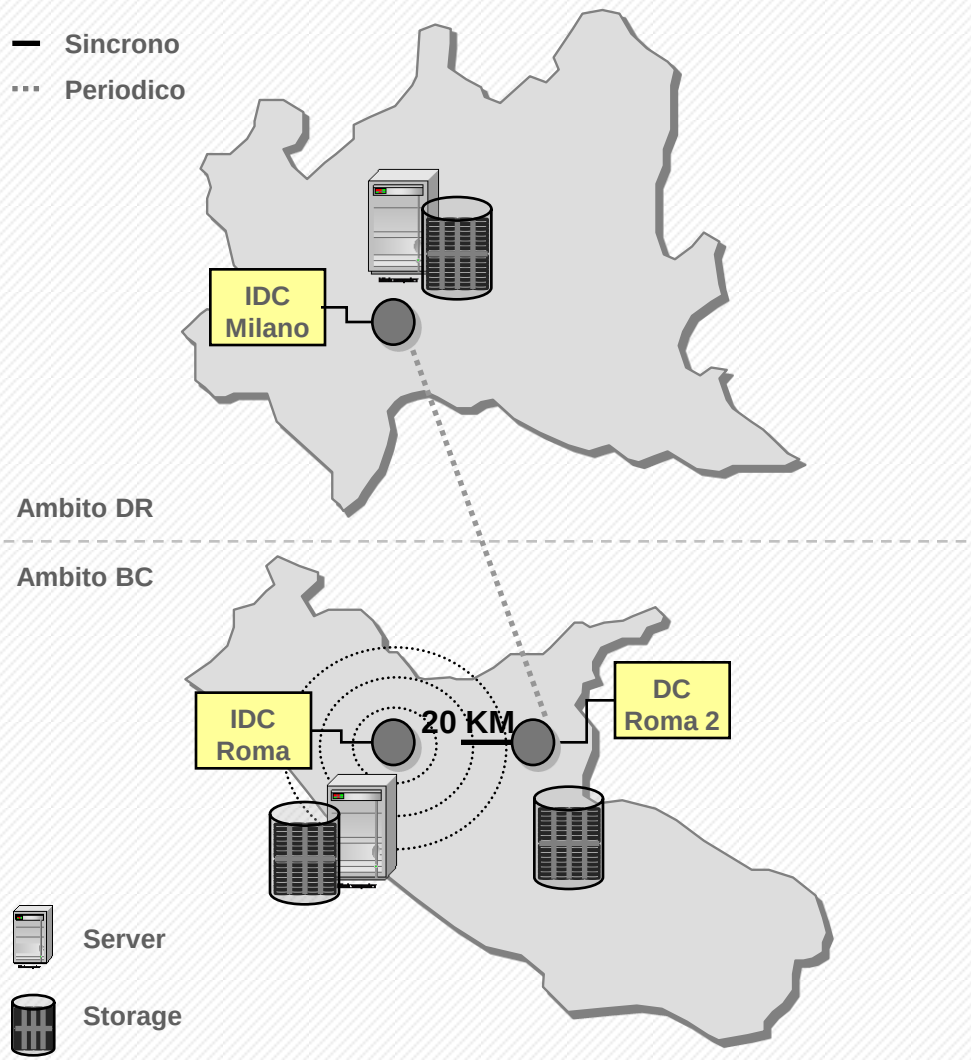
1. Ripartenza dei sistemi nel sito di DR

Risposta al disastro Esteso nell'area romana

1. Ripartenza dei sistemi nel sito di DR

DR con replica a cascata dei dati

Architettura Logica



Allineamento dei Dati

1. Allineamento sincrono dello storage tra il sito primario IDC Roma e DC Roma 2
2. Allineamento periodico dello storage tra il sito DC Roma 2 e il sito IDC Milano

Allineamento dei Server

1. I server possono essere configurati in modalità
   - Hot
   - Warm
   - Cold

Risposta al disastro Localizzato nel IDC Roma

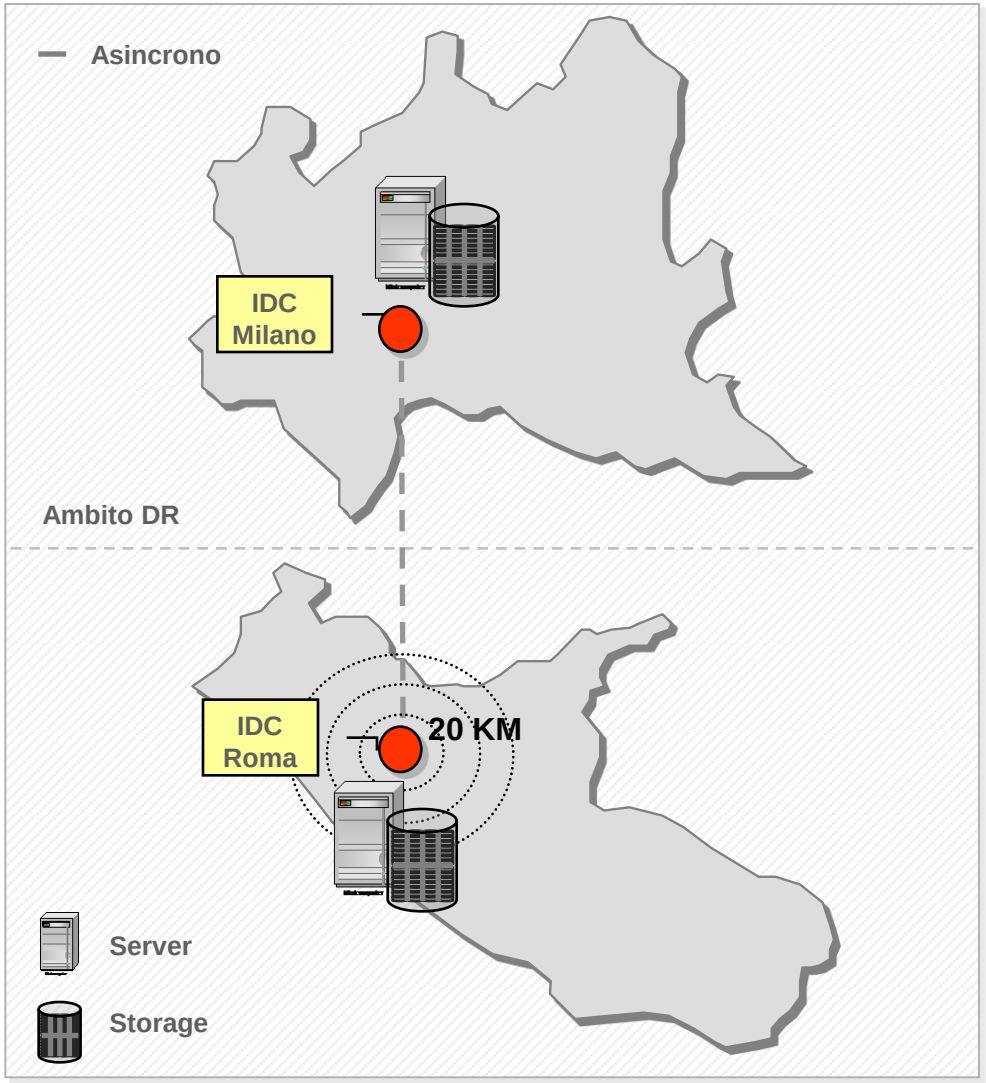
1. Allineamento dei dati necessari a sincronizzare lo storage del DC Roma 2 con quello dei DC di Milano
2. Ripartenza dei sistemi nel sito di DR (DC Milano) senza perdita di dati

Risposta al disastro Esteso nell'area romana

1. Ripartenza dei sistemi nel sito di DR con perdita dei dati proporzionale alla frequenza dell'allineamento periodico

DR con replica Asincrona dei dati

Architettura Logica



Allineamento dei Dati

1 Allineamento asincrono dello storage tra il sito primario IDC Roma e IDC Milano

Allineamento dei Server

1 I server possono essere configurati in modalità

- Hot
- Warm
- Cold

Risposta al disastro Localizzato nel IDC Roma

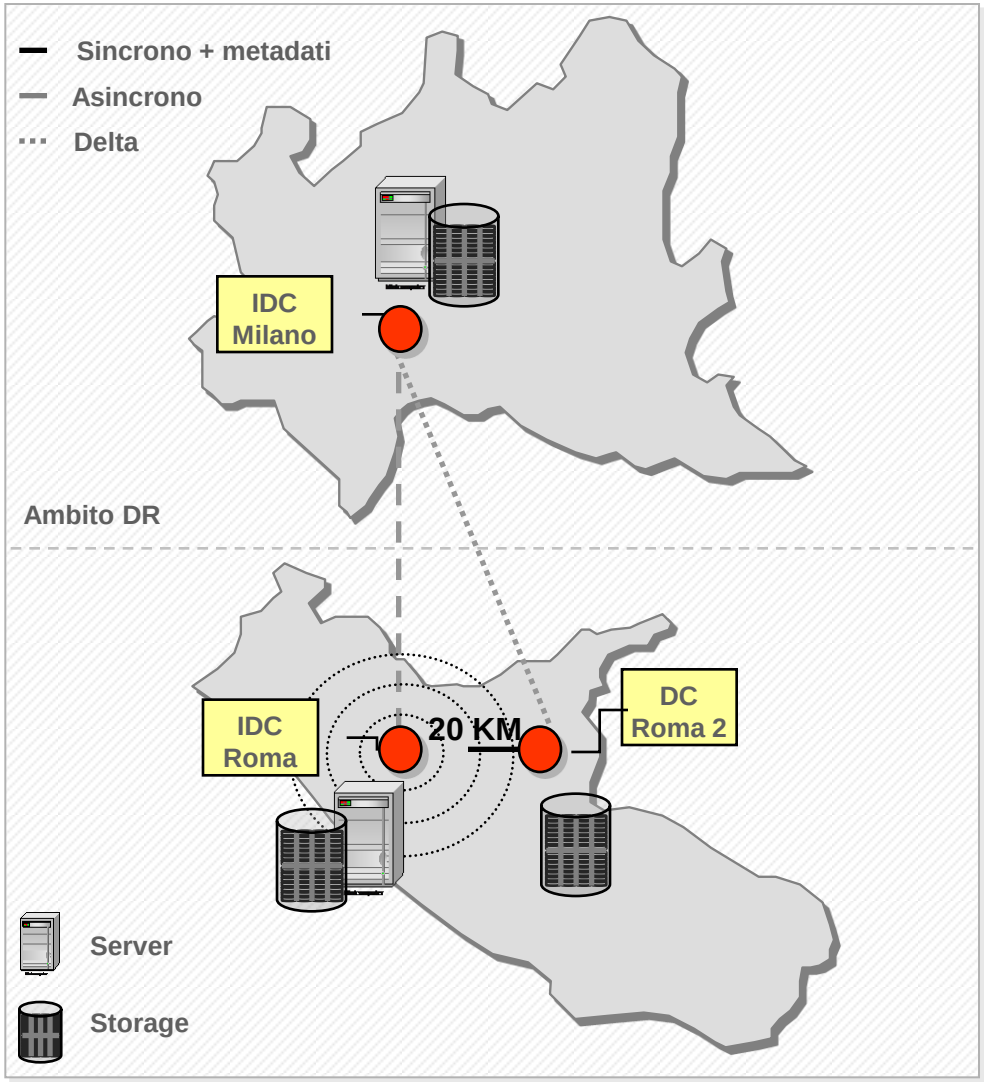
1 Ripartenza dei sistemi nel sito di DR (IDC Milano) con perdita dei dati

Risposta al disastro Esteso nell'area romana

1 Ripartenza dei sistemi nel sito di DR (IDC Milano) con perdita dei dati

DR con replica Star dei dati

Architettura Logica



Allineamento dei Dati

1. Allineamento asincrono dello storage tra il sito primario IDC Roma e IDC Milano

   Allineamento sincrono dello storage tra IDC Roma e DC Roma 2, contestualmente sono inviati anche i metadati necessari a tracciare lo stato di avanzamento dell'allineamento asincrono tra IDC Roma e IDC Milano

Allineamento dei Server

1. I server possono essere configurati in modalità
   - Hot
   - Warm
   - Cold

Risposta al disastro Localizzato nel IDC Roma

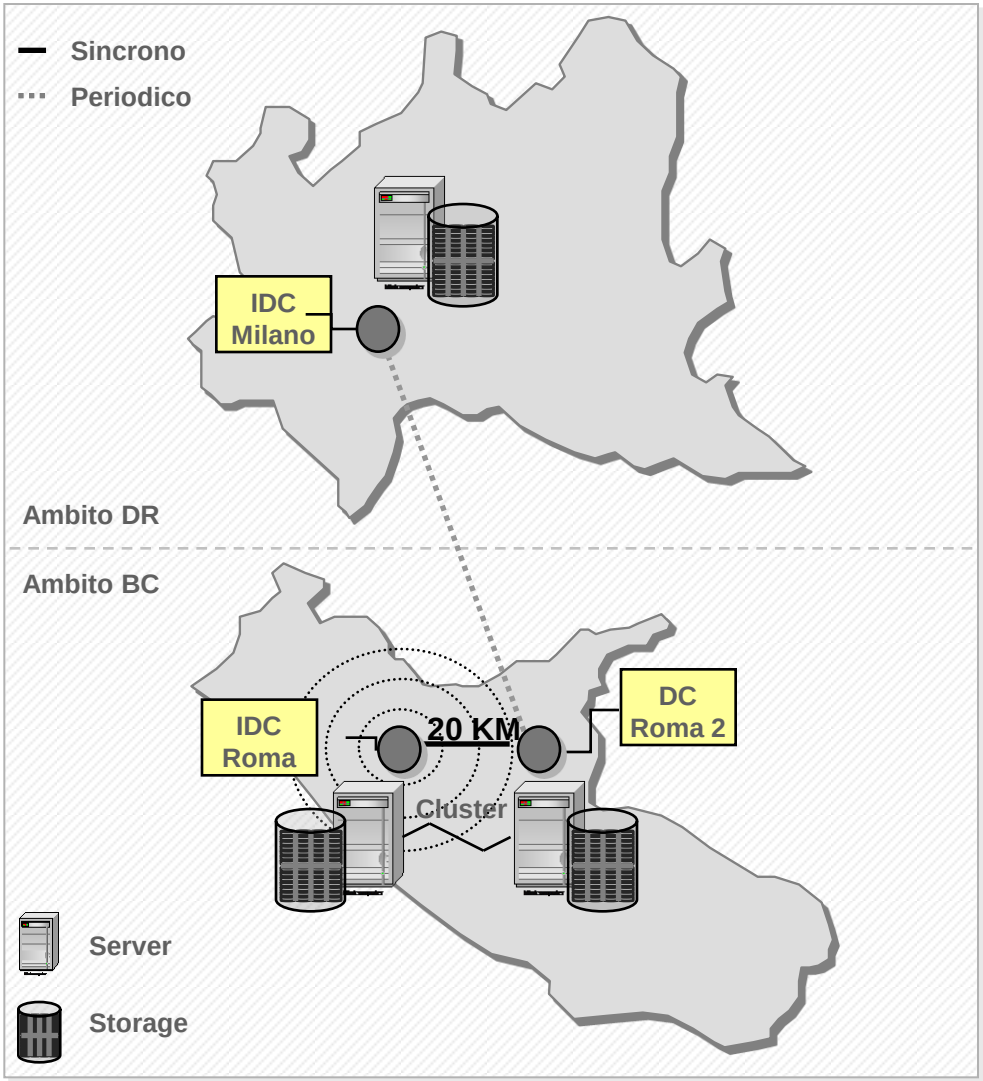
1. Allineamento del delta dei dati necessari a sincronizzare lo storage del DC Roma 2 con quello dei DC di Milano
2. Ripartenza dei sistemi nel sito di DR (DC Milano) senza perdita di dati

Disastro Esteso nell'area romana

1. Ripartenza dei sistemi nel sito di DR con perdita minimale dei dati

DR e BC con replica a Cascata dei dati

Architettura Logica



Allineamento dei Dati

1. Allineamento sincrono dello storage tra il sito primario IDC Roma e DC Roma 2
2. Allineamento periodico dello storage tra il sito DC Roma 2 e il sito IDC Milano

Allineamento dei Server

1. I Server in ambito BC devono essere configurati in Modalità Hot e in Cluster Metropolitano

I server in ambito DR possono essere configurati in modalità

- Hot
- Warm
- Cold

Risosta al disastro Localizzato nel IDC Roma

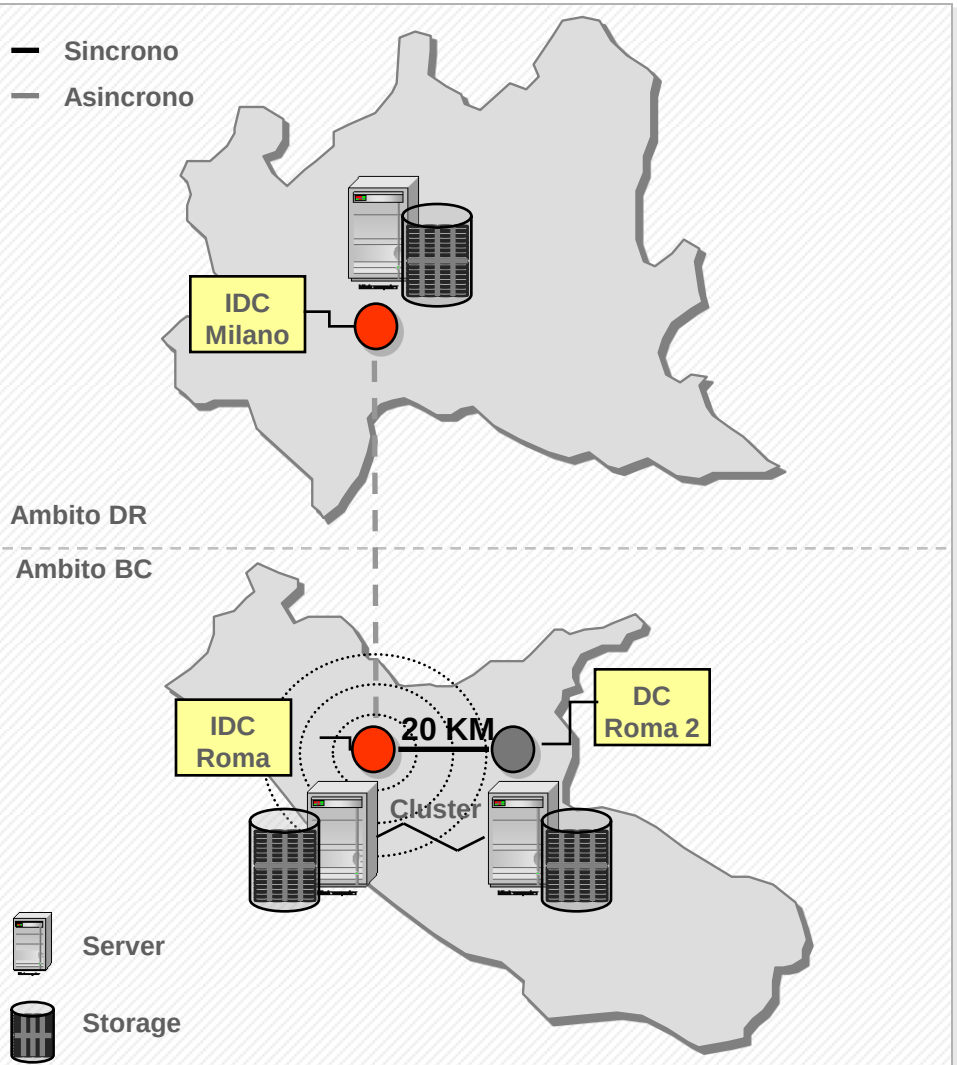
1. Ripartenza dei sistemi nel sito di BC (DC Roma 2) oppure allineamento dei dati necessari a sincronizzare lo storage del DC Roma 2 con quello dei DC di Milano e successiva ripartenza dei sistemi nel sito di DR (DC Milano) senza perdita di dati

Risposta al disastro Esteso nell'area romana

1. Ripartenza dei sistemi sui siti di DR con perdita dei dati proporzionale alla frequenza dell'allineamento periodico

DR e BC con replica Parallela dei dati

Architettura Logica



Allineamento dei Dati

1. Allineamento sincrono dello storage tra il sito primario IDC Roma e DC Roma 2

   Allineamento asincrono dello storage tra il sito primario IDC Roma e IDC Milano

Allineamento dei Server

1. I server in ambito BC devono essere configurati in Modalità Hot e in Cluster Metropolitano

   I server in ambito DR possono essere configurati in modalità
   - Hot
   - Warm
   - Cold

Risposta al disastro Localizzato nel IDC Roma

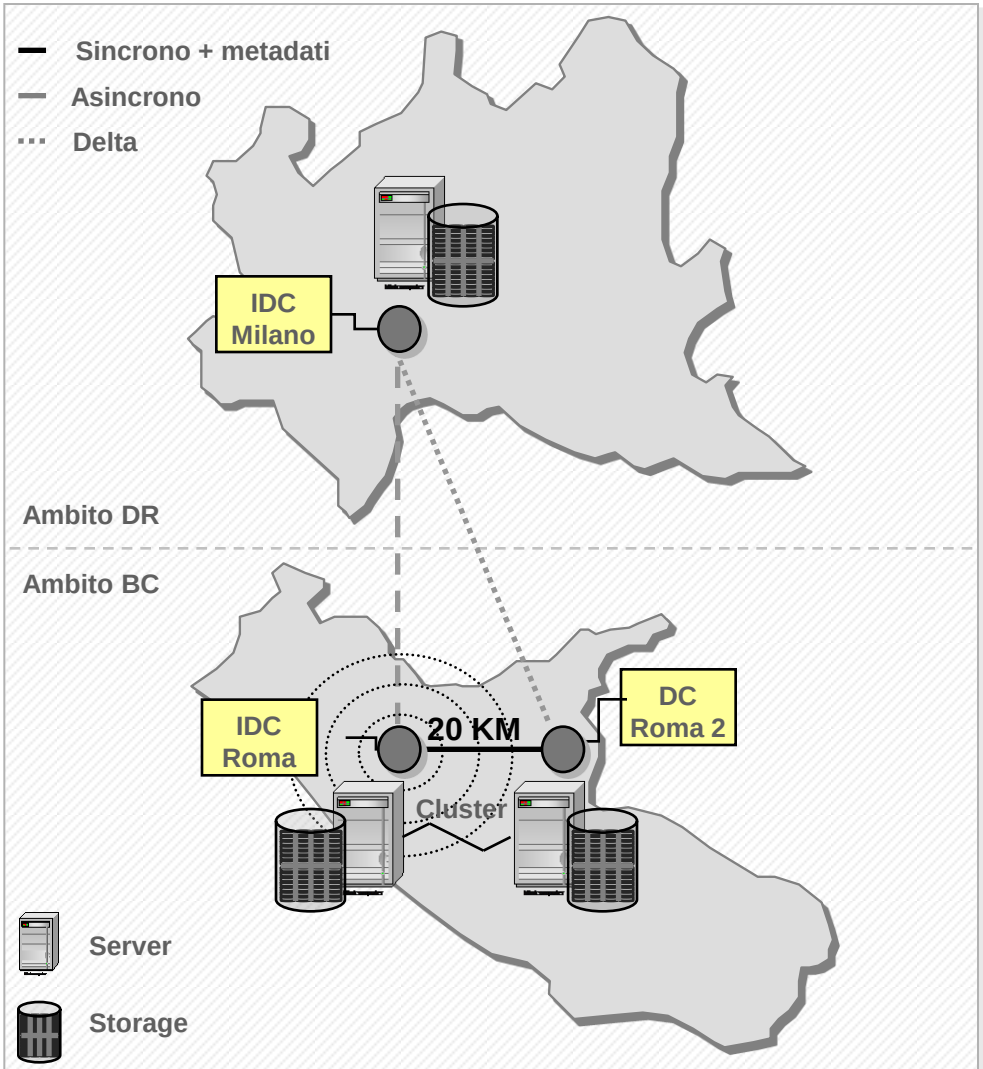
1. Ripartenza dei sistemi nel sito di BC (DC Roma 2) senza perdita di dati oppure sul sito di DR (IDC Milano) con perdita dei dati

Risposta al disastro Esteso nell'area romana

1. Ripartenza dei sistemi nel sito di DR (IDC Milano) con perdita minimale dei dati

DR e BC con replica Star dei dati

Architettura Logica



Allineamento dei Dati

1. Allineamento asincrono dello storage tra il sito primario IDC Roma e IDC Milano

   Allineamento sincrono dello storage tra IDC Roma e DC Roma 2, contestualmente sono inviati anche i metadati necessari a tracciare lo stato di avanzamento dell'allineamento asicrono tra IDC Roma e IDC Milano

Allineamento dei Server

1. I Server in ambito BC devono essere configurati in Modalità Hot e in Cluster Metropolitano

   I server in ambito DR possono essere configurati in modalità
   - Hot
   - Warm
   - Cold

Risposta al disastro Localizzato nel IDC Roma

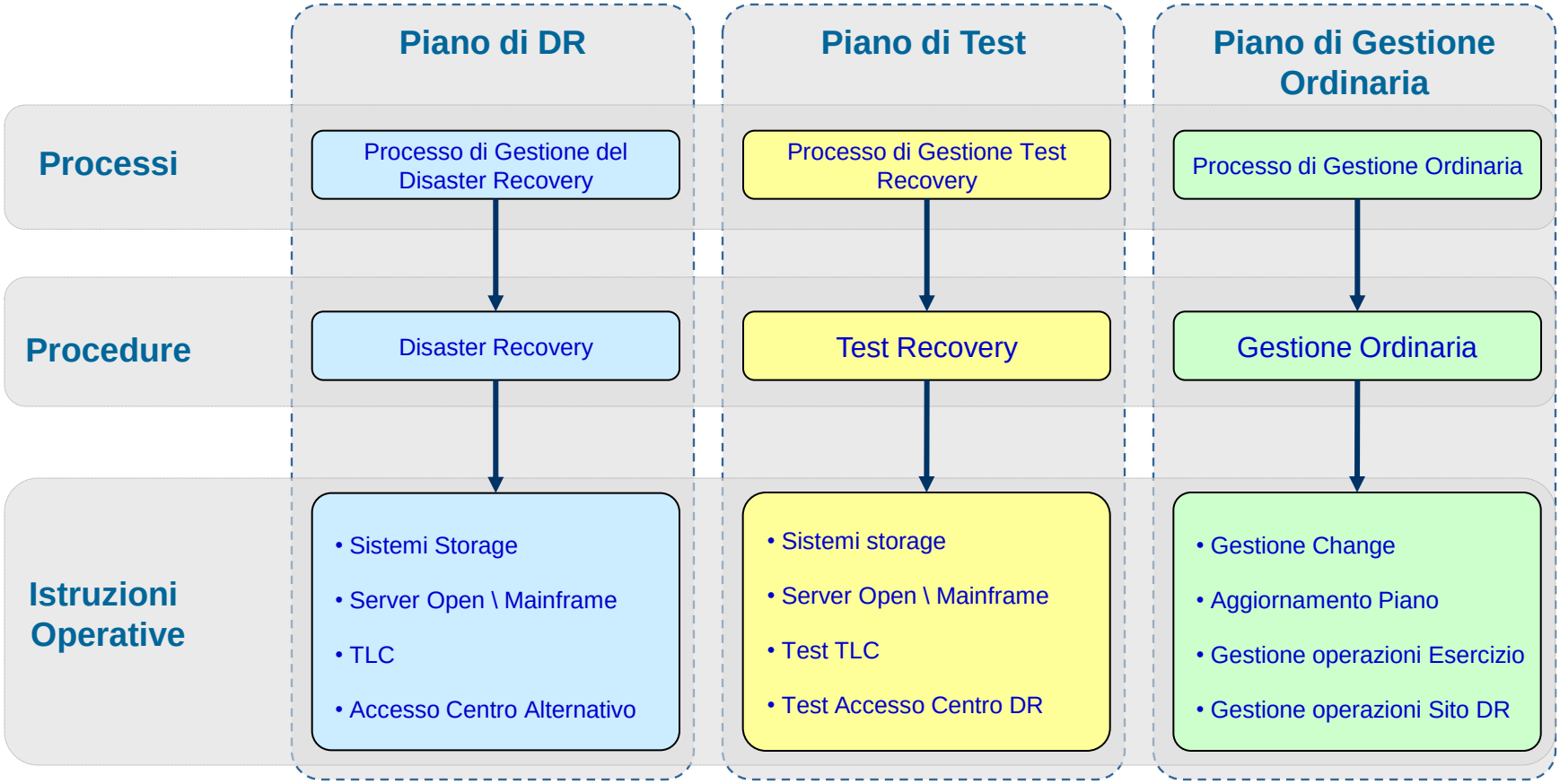
1. Ripartenza dei sistemi nel sito di BC (DC Roma 2) oppure nel sito di DR (IDC Milano) senza perdita di dati.

Disastro Esteso nell'area romana

1. Ripartenza dei sistemi sui siti di DR con perdita minimale dei dati

La documentazione completa del Piano di Continuità per il DR

- Piano di DR, per la gestione della situazione di reale emergenza;
- Piano di Test, per la simulazione periodica del recovery e verifica dell'efficacia della soluzione;
- Piano di Gestione Ordinaria, per la quotidiana manutenzione e controllo della soluzione.



Agenda

- **Introduzione**
  - *Terminologia e Standard*
  - *Normative Internazionali*
- **I fondamenti del Disaster Recovery e della Business Continuity**
  - *Panoramica delle soluzioni disponibili*
  - *Descrizione delle tecnologie abilitanti*
  - *I piani e le procedure organizzative*
- **L'evoluzione della soluzione di Disaster Recovery in Poste Italiane**
  - *2006. Soluzione con Nastri a freddo*
  - *2007. Soluzione con Replica asincrona dei dati*
  - *Oggi. Soluzione SRDF-Star*

Il progetto di Poste Italiane

- **BancoPosta** raggruppa tutti i servizi finanziari offerti da Poste Italiane, secondo le nuove direttive di Basile 2, il disaster recovery e la business continuity diventano un punto centrale per l'erogazione dei servizi.

- L'architettura BancoPosta di Poste Italiane è distribuita sia su sistemi mainframe che su sistemi open, la parte open prevede l'esecuzione di 40 applicativi distribuiti su 171 server e una quantità di dati memorizzati di 81.957 GB

➔ 2006. Sistema di Distaster Recovery “cold”

La prima soluzione di DR in Poste Italiane consisteva nella replicare dei dati in modalità **cold**. Una volta al giorno, normalmente alle ore 2,00, tutti dati venivano replicati su cartucce magnetiche e conservati su di un sito bunker situato ad una distante maggiore di 100 km; in caso di disastro i nastri venivano trasferiti sul sito di Settimo Milanese per eseguire il ripristino e far ripartire i sistemi. Questa soluzione prevedeva il recupero dei dati per i soli sistemi Mainframe.

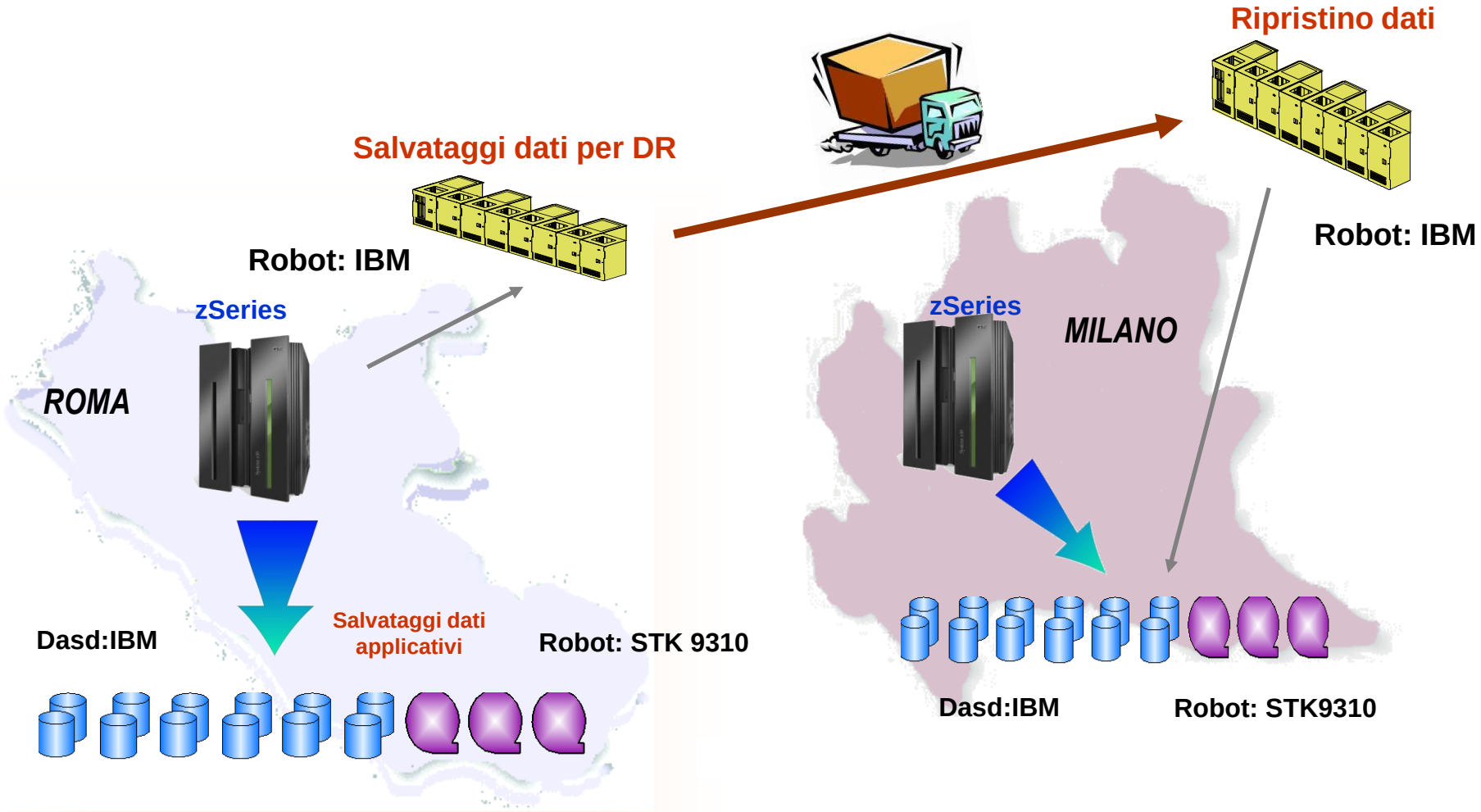
Caratteristiche della soluzione:

- ✓ Perdita dati (RPO)= 24 ore
- ✓ Ripristino della funzionalità (RTO) = 48/72 Ore

Criticità:

- ✓ Tempi di produzione dei nastri (circa 10 ore)
- ✓ Ripristino dei soli dati su disco
- ✓ Breve interruzione delle attività per consentire la copia consistente

Il progetto di Poste Italiane



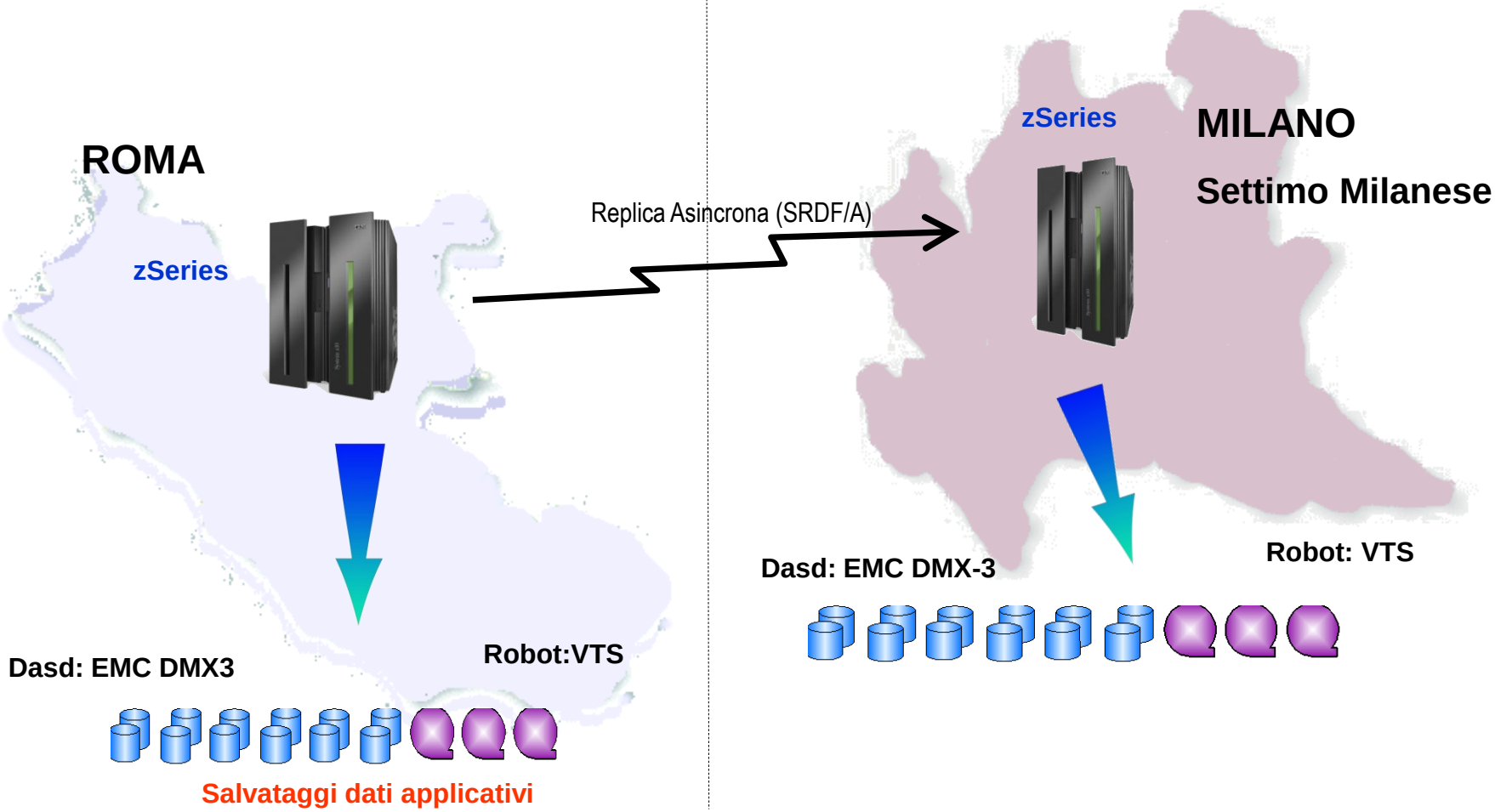
- 2007. Architettura con replica asincrona

Nel dicembre 2006, Poste Italiane implementa una nuova soluzione di Disaster Recovery; questa architettura prevede la creazione di due siti, Roma come sito di produzione e Milano come sito di DR. Le repliche dei dati vengono eseguite attraverso un protocollo asincrono SRDF/A (Symmetric Remote Data Facility / Asyncronous) . *Questa soluzione viene implementata sia per il mondo Mainframe che per i sistemi Open.*

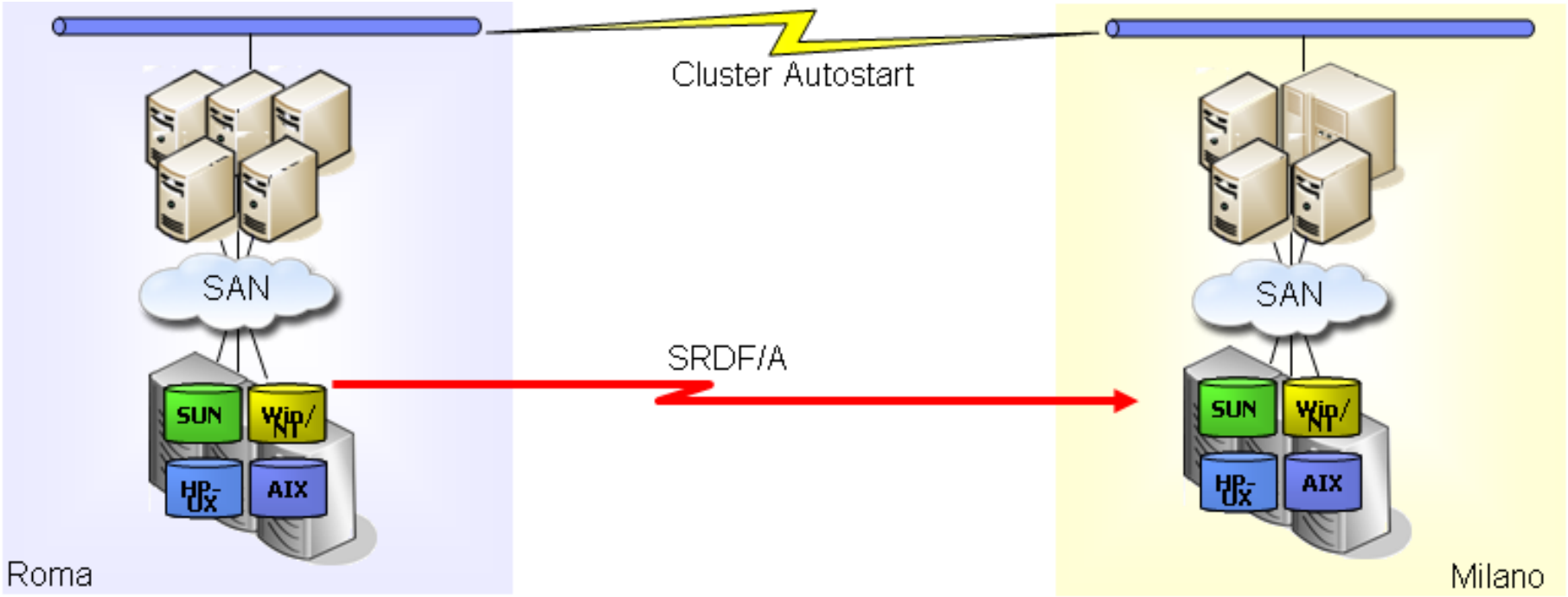
Caratteristiche della soluzione:

- Perdita dati (RPO)= circa 30 sec
- Ripristino della funzionalità (RTO) = 4 Ore
- Eliminazione dei nastri di DR con relativo trasporto e stoccaggio
- Sostituzione Robot con VTS per replica nastri (attiva da Marzo 2007)

➔ Replica Asincrona Mainframe



- Replica Asincrona su Sistemi Open (“Architettura a due siti”)



2008. Architettura in modalità SDRF/ Star

La situazione attuale di Poste italiane in ambito DR, prevede un'architettura denominata a "tre siti" . Questa configurazione permette di ottenere Tempi di RPO pari a zero, in quanto vengono utilizzati tre differenti siti: Roma, Pomezia e Milano, questa architettura protegge il sistema sia da catastrofi metropolitane, inferiori ai 100 km che da catastrofi geografiche, superiori a 100 km.

Caratteristiche della soluzione:

- Perdita dati (RPO)= 0
- Ripristino della funzionalità (RTO) = 2 Ore
- Replica asincrona dei dati su nastro memorizzati su VTS

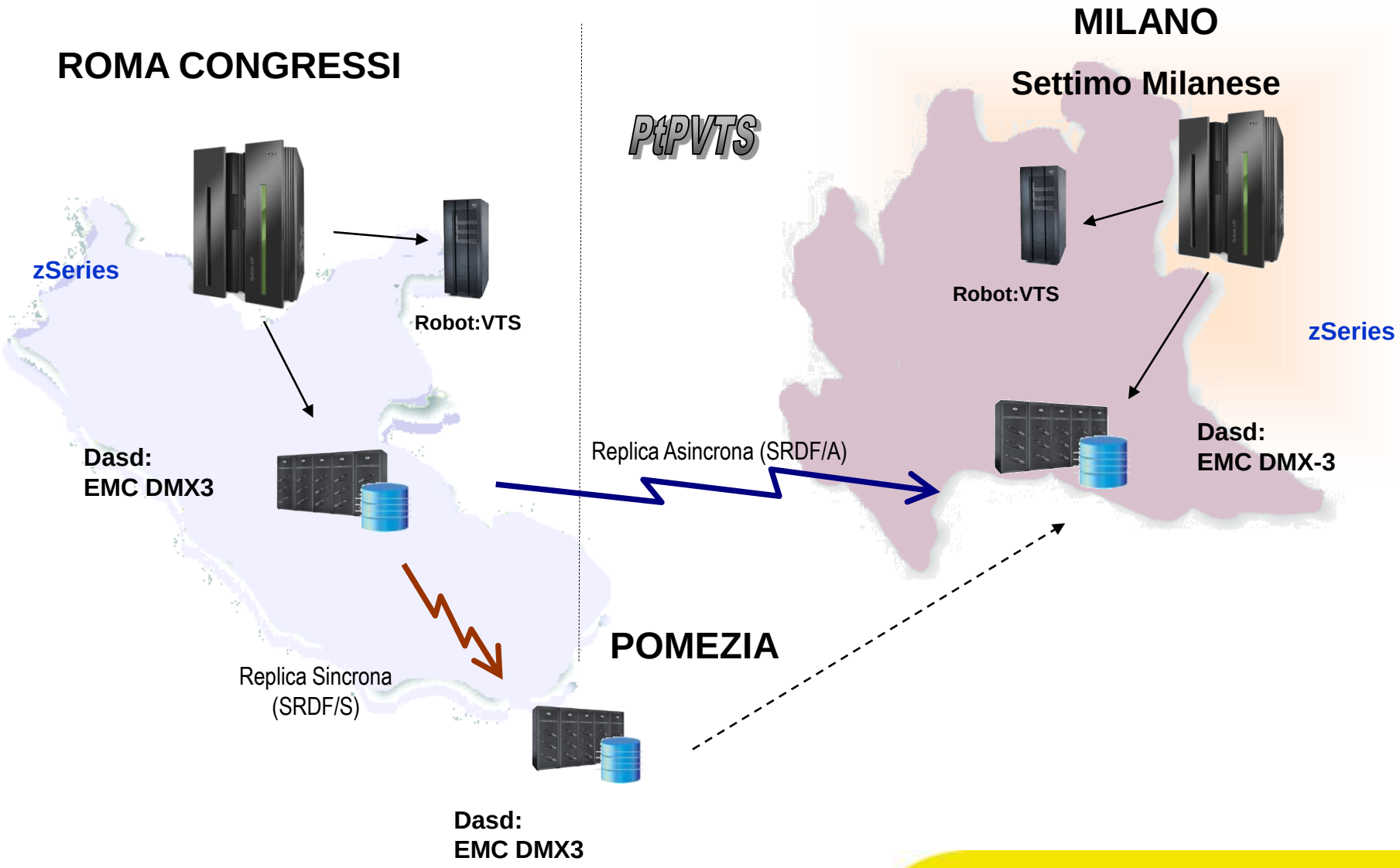
Criticità:

- Impatto sulle prestazioni del sito primario a causa della copia sincrona.
- Soluzione tecnologicamente avanzata e pertanto contenente elementi di complessità gestionale

Azioni di contenimento:

- Monitoraggio costante di tutta la infrastruttura a supporto della soluzione tecnologica di Disaster Recovery
- Esecuzione periodica dei test di ripartenza

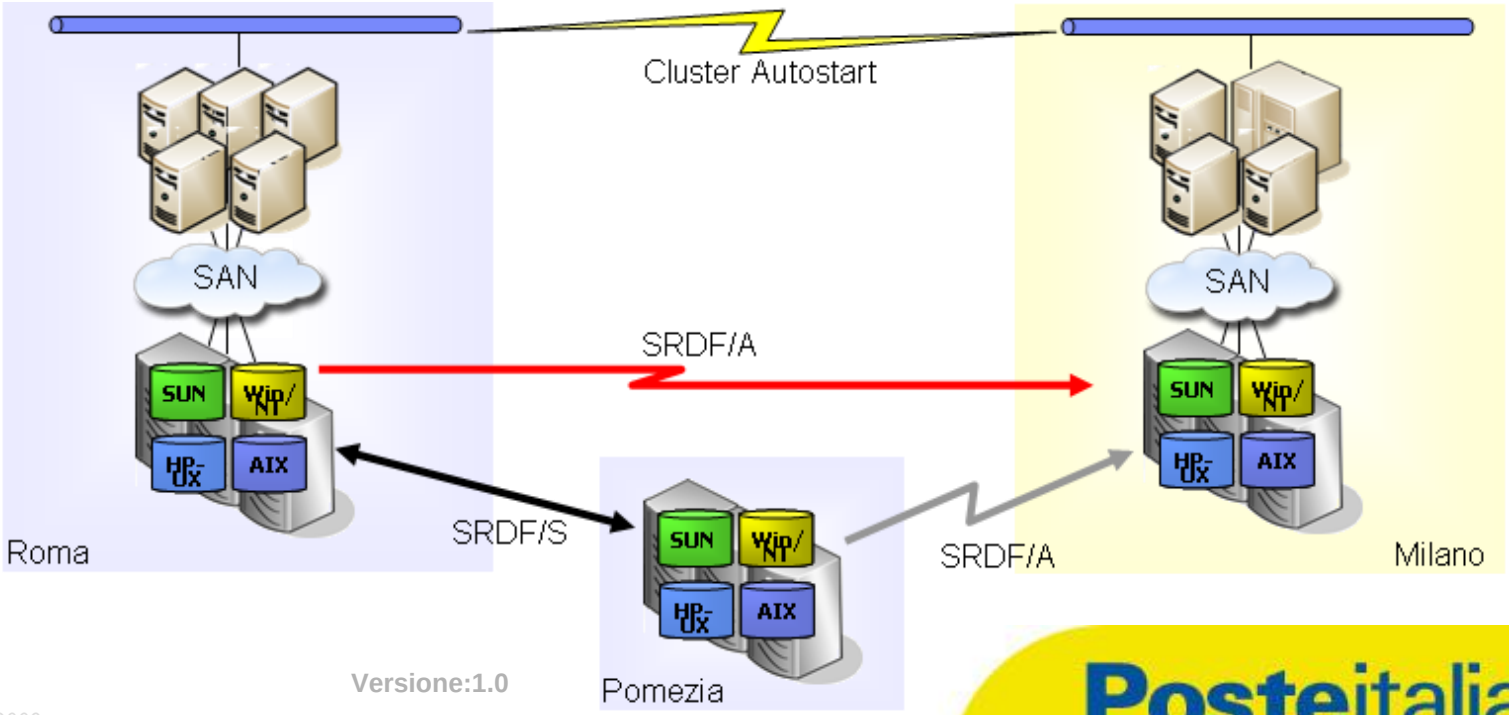
➔ Sistema Mainframe



➔ Sistemi Open (architettura a tre siti)

Architettura a tre siti: Questa architettura viene utilizzata per le applicazioni che prevedono requisiti di RPO pari a zero, ovvero quantità di dati perdi a fronte di un disastro nulli.

L'architettura viene realizzata mediante la creazione di tre siti, Il sito di produzione e il sito bunker che comunicano in transazioni atomiche attraverso un protocollo sincrono (SRDF/S), e un terzo sito utilizzato solo per DR collegato in modo asincrono con il sito di produzione.



➔ Situazione Attuale

Poste Italiane grazie alla propria architettura di DR può soddisfare i requisiti di "BASILEA 2".

Ad oggi, tutti i servizi BancoPosta sono coperti da una soluzione Disaster Recovery, in particolare sono state create due classi di servizi in funzione dall' esigenze di business e dei relativi livelli di servizio (SLA).

Applicazioni sotto Disaster Recovery	Numero
Applicazioni BancoPosta con RPO=8	80
Applicazioni BancoPosta con RPO=0	29

Oltre a BancoPosta è stato già avviato la copertura dei servizi di posta Exchange in DR.

Poste Italiane sta provvedendo a creare una lista di priorità per inserire in DR alcuni dei servizi di maggior rilievo.

Stato attuale delle architetture e dei servizi in DR

Il progetto, nel suo complesso, ha avuto una durata di circa 24 mesi (Kick-off progetto Ottobre 2006; Go-Live Star Dicembre 2008) **ed ha permesso di porre sotto DR il sistema Mainframe ed i sistemi Open dei servizi Bancoposta.**

- Per le applicazioni che risiedono su **Mainframe** sono stati rispettati i requisiti
  - **RPO = 0 e RTO = 2 ore**
- Per le applicazioni residenti su sistemi **Open**, sono stati rispettati i requisiti definiti singolarmente in relazione alle caratteristiche dell'applicazione:
  - **RPO = 0;8 ore e RTO = 2,4,6,8 ore**

  Complessivamente sono sotto Disaster Recovery i sistemi Mainframe di oltre 30000 MIPS e oltre 70 TB di dati e per la parte Open, 41 applicazioni, 171 server con oltre 80 TB di dati.

Le maggiori criticità che il progetto ha dovuto affrontare, data la sua complessità, sono state riscontrate nella fase di integrazione delle differenti tecnologie nonché nella risoluzione dei problemi legati alla diversa collocazione geografica delle componenti infrastrutturali.

Il progetto di Poste Italiane : possibili evoluzioni

- *La comparazione tra i livelli di continuità attuali e quelli possibili evidenzia le aree di miglioramento in termini di business continuity*

			CONTINUITÀ ATTUALE	CONTINUITÀ POSSIBILE
COMPONENT RECOVERY	server	server mainframe	"trasparente", l'utente non ha evidenza del problema	"trasparente" per l'utente
		cluster A/P	tempo di ripartenza su altro nodo, 5-15 minuti	
		cluster A/A	"trasparente", l'utente non ha evidenza del problema	"trasparente", l'utente non ha evidenza del problema
	unità dischi	dischi mainframe	tempi di riparazione ed eventuale ripopolamento o soluzione disaster recovery	"trasparente", ma con condizioni: ▪ avvicinamento dei dischi sincroni ▪ virtualizzazione storage per UNIX Wintel
		dischi UNIX Wintel		
DISASTER RECOVERY	edificio	indisponibilità prolungata del CED e/o della sede di viale Europa/Congressi	RTO: ripristino servizi IT entro 2 ore RPO: perdita dati max tendente a zero	tendente a "trasparente" (5-15 minuti per cluster A/P), la somma delle misure di component recovery offre la migliore protezione in caso di totale indisponibilità del sito primario
	area metropolitana	indisponibilità prolungata area metropolitana	RTO: ripristino servizi IT entro 2 ore RPO: perdita dati max tendente a zero	RTO: ripristino servizi IT entro 2 ore RPO: perdita dati max tendente a zero