Convegno

Business Continuity e Disaster Recovery

Normative, processi e tecnologie

Ing. Mario D'Ettorre

17/06/2022

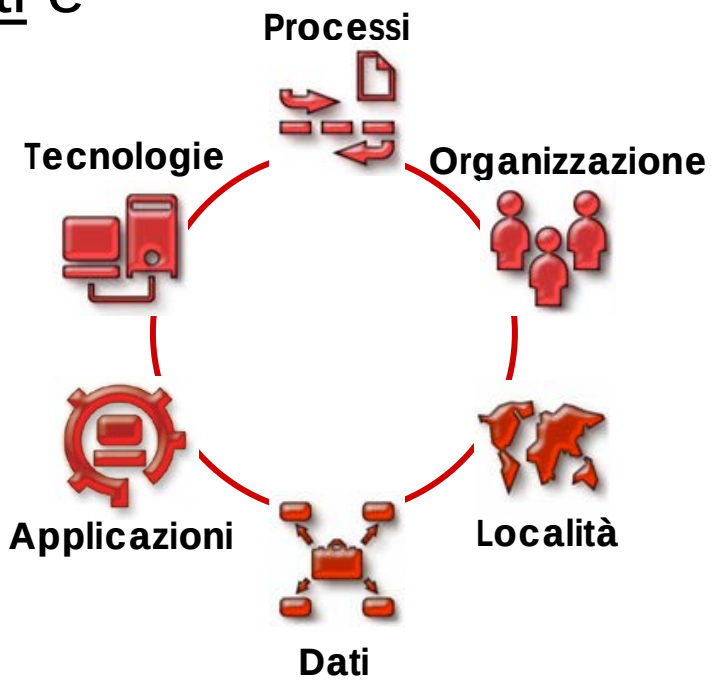
AGENDA

- **Introduzione**
  - *Terminologia e Standard*
  - *Normative e Linee Guida*
- **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 delle soluzioni di Disaster Recovery**
  - *Soluzione con Nastri a freddo*
  - *Soluzione con Replica asincrona dei dati*
  - *Soluzione SRDF-Star*

Disaster Recovery: IL PROBLEMA

Come evitare che eventi dannosi possano provocare l'indisponibilità prolungata delle applicazioni e/o la perdita dei dati, creando gravi danni al Business Aziendale ?

Occorre mettere in atto un insieme di misure tecnologiche per replicare i dati e i sistemi critici in un sito distante, che si presume non venga impattato dal disastro e misure organizzative per rendere disponibile nel sito distante il personale tecnico in grado di attivare i sistemi



COME 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

Business Continuity Management

Il Disaster Recovery rientra nella categoria molto più vasta del Business Continuity Management

Business Continuity Management:

insieme di piani e procedure che permettono 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.

Normative e Linee Guida

STANDARD ISO 22301 e ISO 22313

- **ISO 22301:2019,** "Societal security - Business continuity management systems -- Requirements" pubblicata a Maggio 2012 – recepita da UNI come UNI EN ISO 22301
- **ISO 22313:2020**, "Security and resilience - Business continuity management systems – Guidance to the use of ISO 22301" 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 in accordo con i requisiti definiti nella ISO 22301.

Normative e Linee Guida

ISO/TS 22317:2021 Security and resilience – Business continuity management systems – Guidelines for business impact analysis (BIA)

ISO/TS 22318:2021 Security and resilience – Business continuity management systems – Guidelines for supply chain continuity

ISO/TS 22330:2018 Security and resilience – Business continuity management systems – Guidelines for people aspects on business continuity

ISO/TS 22331:2018 Security and resilience – Business continuity management systems – Guidelines for business continuity strategy

ISO/TS 22332:2021 Security and resilience – Business continuity management systems – Guidelines for developing business continuity plans and procedures

ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

ISO 31000 Risk management – Guidelines

ISO 31010 Risk management – Risk assessment techniques

La complessità della Business Continuity Management è evidente !!

Normative e Linee Guida

NIST

NIST Special Publication 800-34 Rev 1: **Contingency Planning Guide for Federal Information Systems ***

Il NIST(National Institute of Standards and Technology) in USA, ha redatto delle raccomandazioni e linee guida per la predisposizione del **Contingency Plan** per i sistemi informativi.

Il **Contingency Plan** riguarda le misure da applicare al verificarsi di una emergenza per ripristinare al più presto le funzionalità più rilevanti dei sistemi informativi

Il NIST identifica i seguenti processi 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 documento è liberamente scaricabile da Internet

Normative e Linee Guida

NIST

Il contingency plan del sistema informativo riguarda un ampio ambito di attività e quindi per rappresentare questo aspetto il NIST prevede i seguenti piani dedicati:

- **Business Continuity Plan (BCP)**
- Continuity of Operations (COOP) Plan
- Crisis Communications Plan
- Critical Infrastructure Protection (CIP) Plan
- Cyber Incident Response Plan
- **Disaster Recovery Plan (DRP)**
- Information System Contingency Plan (ISCP)
- Occupant Emergency Plan (OEP)

Normative e Linee Guida

NIST

Il NIST identifica le seguenti fasi come essenziali per un contingency plan:

1. **Attivazione e Notifica**

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

2. **Ripristino**

   identifica la sequenza e 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 quali ad esempio verifiche sui dati e sulle funzionalità o predisposizione di un nuovo sito

Normative e Linee Guida

BASILEA 2

Con ‘Basilea 2’ si intende il nuovo accordo internazionale (2004 entrato in vigore nel 2007) sui requisiti minimi di capitale patrimoniale delle Banche.

Le banche dei paesi aderenti dovranno accantonare quote di capitale per coprire le perdite inattese dovute a tre categorie di rischio:

- Rischio di credito
- Rischio di mercato
- Rischio operativo

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

ADEMPIMENTI A LIVELLO LEGISLATIVO

Il **CODICE DELL'AMMINISTRAZIONE DIGITALE** (CAD) è un atto normativo della Repubblica Italiana, precisamente il decreto legislativo 7 marzo 2005, n. 82.

Esso costituisce un corpo organico di disposizioni che presiede all'uso dell'informatica come strumento privilegiato nei rapporti tra la pubblica amministrazione e i cittadini dello Stato.

L'articolo 50bis si riferiva esplicitamente al tema della continuità operativa e del Disaster Recovery.

Con successive normative tale articolo è stato abrogato perché è stato emanato dall'**AGID** il documento:

LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI

che pone enfasi su :

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa.

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.

ADEMPIMENTI DI ORDINE LEGISLATIVO

il **regolamento generale sulla protezione dei dati** (***General Data Protection Regulation***), ufficialmente **regolamento (UE) n. 2016/679** e meglio noto con la sigla **GDPR**, è il regolamento che l'Unione Europea ha emanato in materia di trattamento di dati personali e della privacy.

L'Articolo 30 "*Sicurezza del trattamento*" del GDPR non cita esplicitamente il **Disaster Recovery** e la **Business Continuity** ma la capacità indicata al punto *c)* ne implica la presenza

Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

- *a) la pseudonimizzazione e la cifratura dei dati personali;*
- *b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;*
- ***c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;***
- *d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

AGENDA

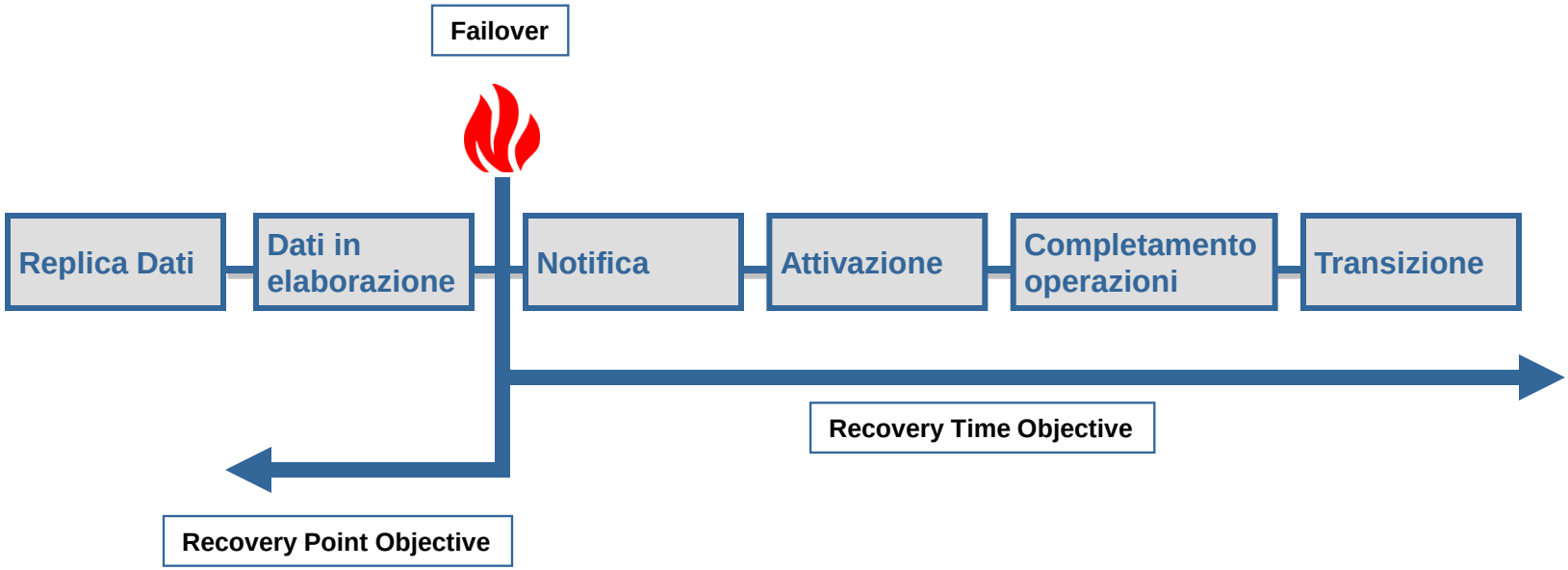
- **Introduzione**
  - *Terminologia e Standard*
  - *Normative e Linee Guida*
- **I fondamenti del Disaster Recovery e della Business Continuity**
  - *Parametri di Base RPO e RTO*
  - *Descrizione delle tecnologie abilitanti*
- **L'evoluzione delle soluzioni di Disaster Recovery**
  - *Soluzione con Nastri a freddo*
  - *Soluzione con Replica asincrona dei dati*
  - *Soluzione SRDF-Star*

REQUISITI TECNICI PER IL DR

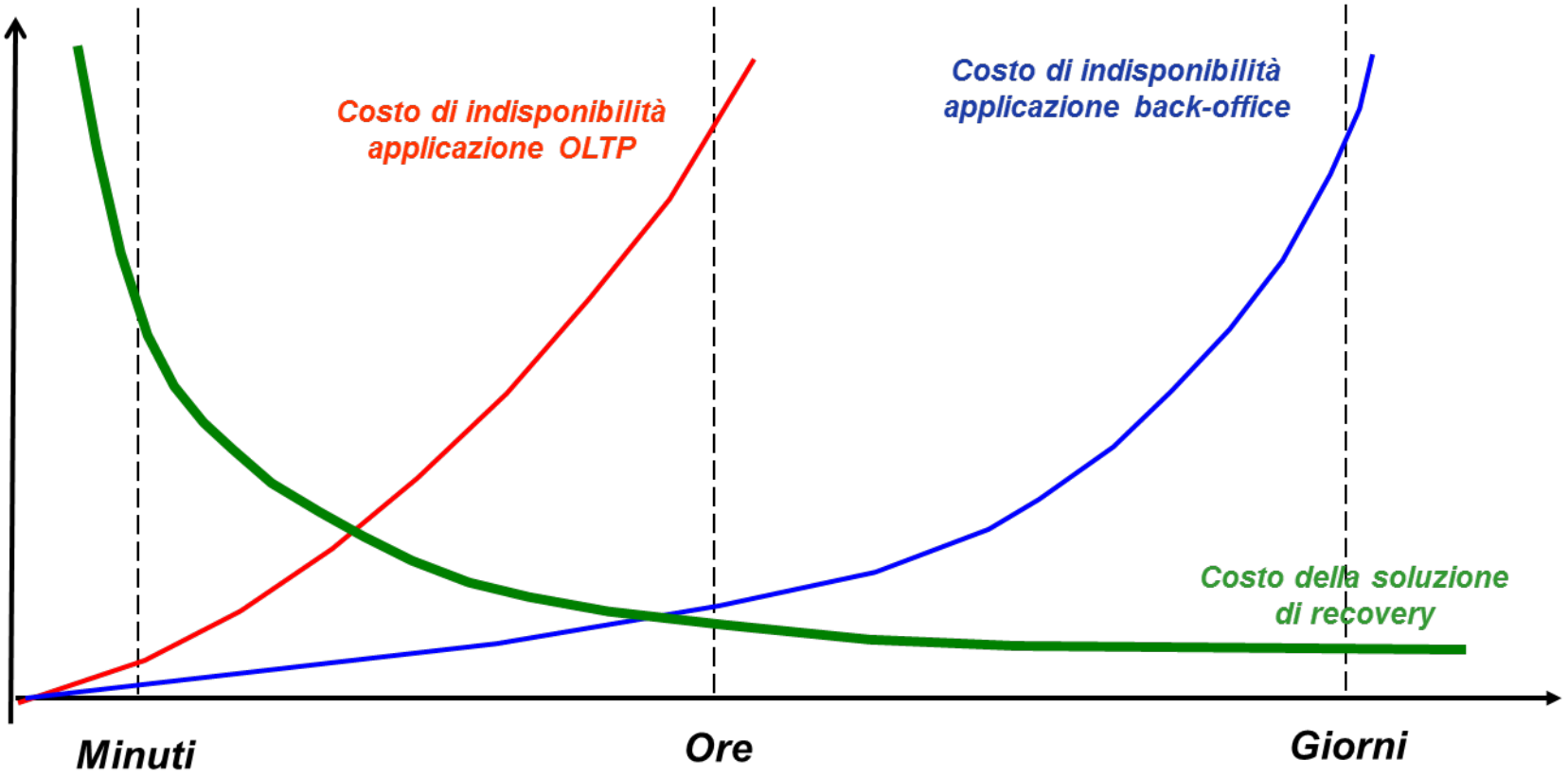
I requisiti di Business si traducono in requisiti Tecnologici, le cui metriche sono:

- **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) = indica il tempo trascorso dall'ultima replica dei dati fino all'accadere del disastro e corrisponde al massimo di dati che possono essere persi. L'RPO è legato alla frequenza di replica dei dati al sito remoto.

La continuità di servizio implica RPO e RTO ~ 0



RTO versus Costi



RPO versus Costi versus Importanza del Dato

Anche per il parametro **RPO i costi della soluzione di DR 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 per via del tempo di allineamento dei dati
- 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 non recuperabile”

COME DETERMINARE RPO e RTO

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)

Analizza la criticità degli asset (personale, sedi, strumenti di lavoro, sistemi IT) in relazione all'impatto sul funzionamento del processo

In particolare per i sistemi IT che costituiscono obiettivi della BIA:

- identificazione delle applicazioni business critical e della infrastruttura tecnologica (Data Center,Linee TLC, server, storage, ecc.) di cui hanno bisogno
- identificazione delle vulnerabilità della infrastruttura come la presenza di Single Point of Failure (SPOF) e dei corrispondenti tempi di recupero

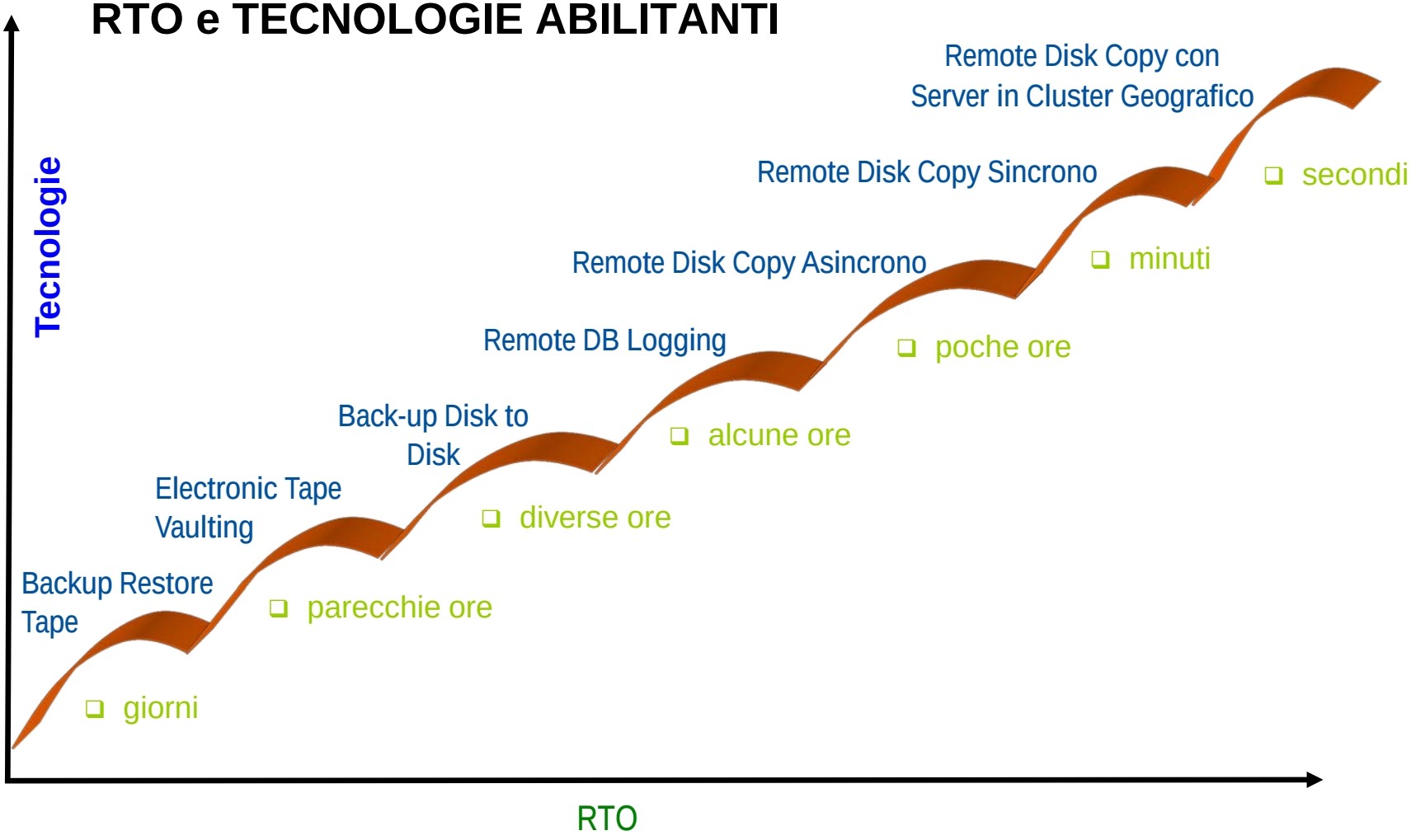
Risk Assessment (RA)

Il processo di Risk Assessment (RA) considera le minacce che gravano sui processi critici al fine di minimizzare il loro verificarsi od il loro impatto.

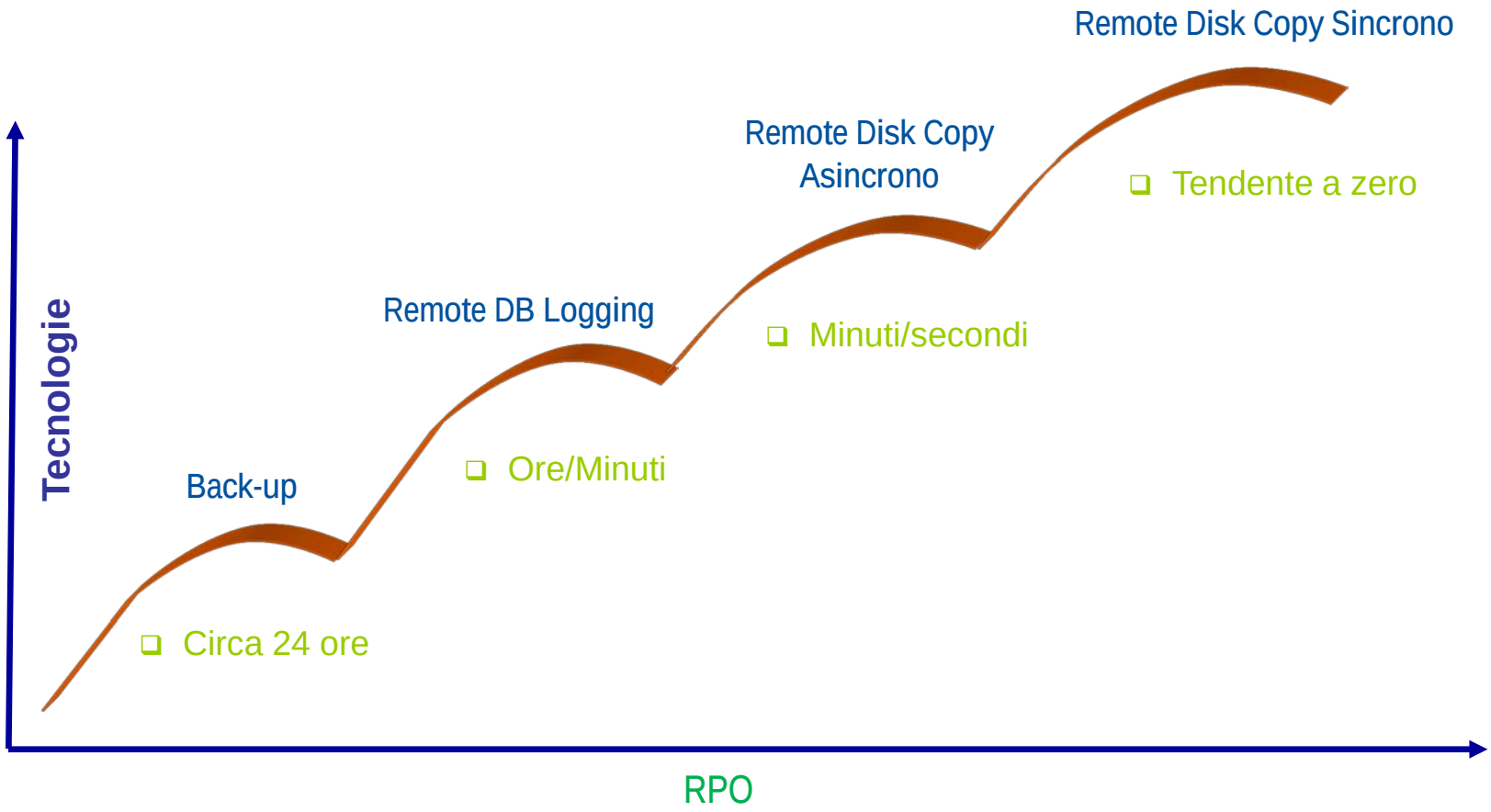
Il RA è basato sulla probabilità che un evento minaccioso si verifichi e l'impatto economico o di altra natura derivante dal verificarsi dell'evento. Sono usati due metodi:

- **metodo qualitativo**: si identificano i rischi e si stimano la probabilità e l'impatto di ciascuno secondo un «giudizio esperto» senza l'uso di metodi statistici
- **metodo quantitativo**: in questo caso si fa una analisi più approfondita usando metodi statistici e anche dati storici. Questo metodo viene usato per approfondire i rischi principali individuati con l'altro metodo. Il limite di questo tipo di analisi è tuttavia la bontà del modello utilizzato.

RTO e TECNOLOGIE ABILITANTI



RPO e TECNOLOGIE ABILITANTI



LA SALVAGUARDIA DEI DATI

Storicamente il dato veniva 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 perché bisogna ripristinare l'intero set di dati

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

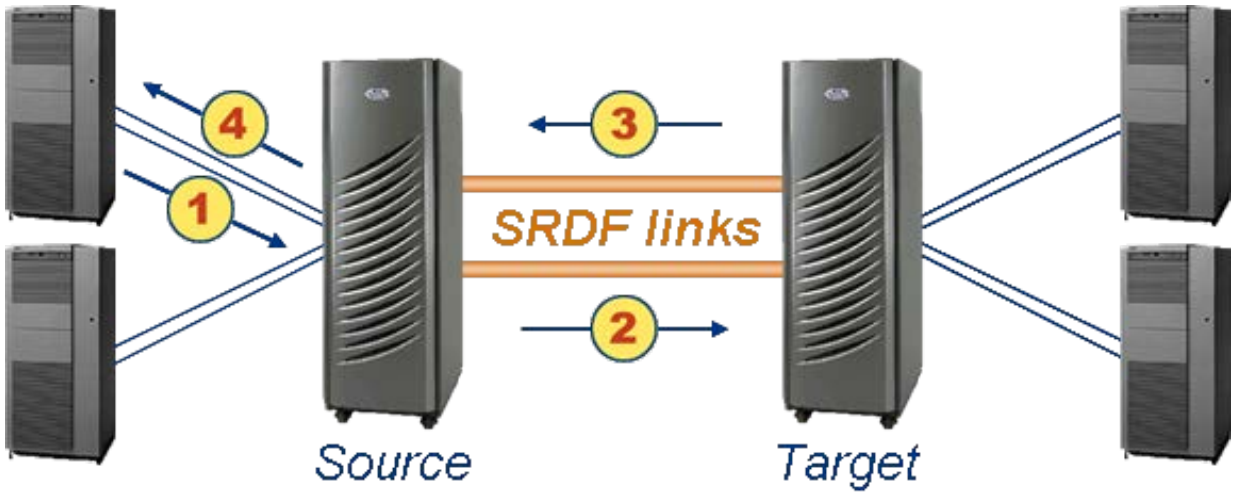
La replica può essere ottenuta in vario modo:

- software di data mirroring tra computer adatto per piccole realtà e poco efficiente poiché utilizza tempo e risorse di sistema
- allineamento automatico dei dati tra gli apparati di storage (in genere con protocolli di tipo proprietario)
- virtualizzazione dello storage che consente di aggregare gli apparati di storage di diversa provenienza in un unico pool di risorse consentendo la migrazione dei dati

SISTEMI PER LA DATA REPLICATION

Replica Sincrona

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



LA DEDUPLICAZIONE DEI DATI

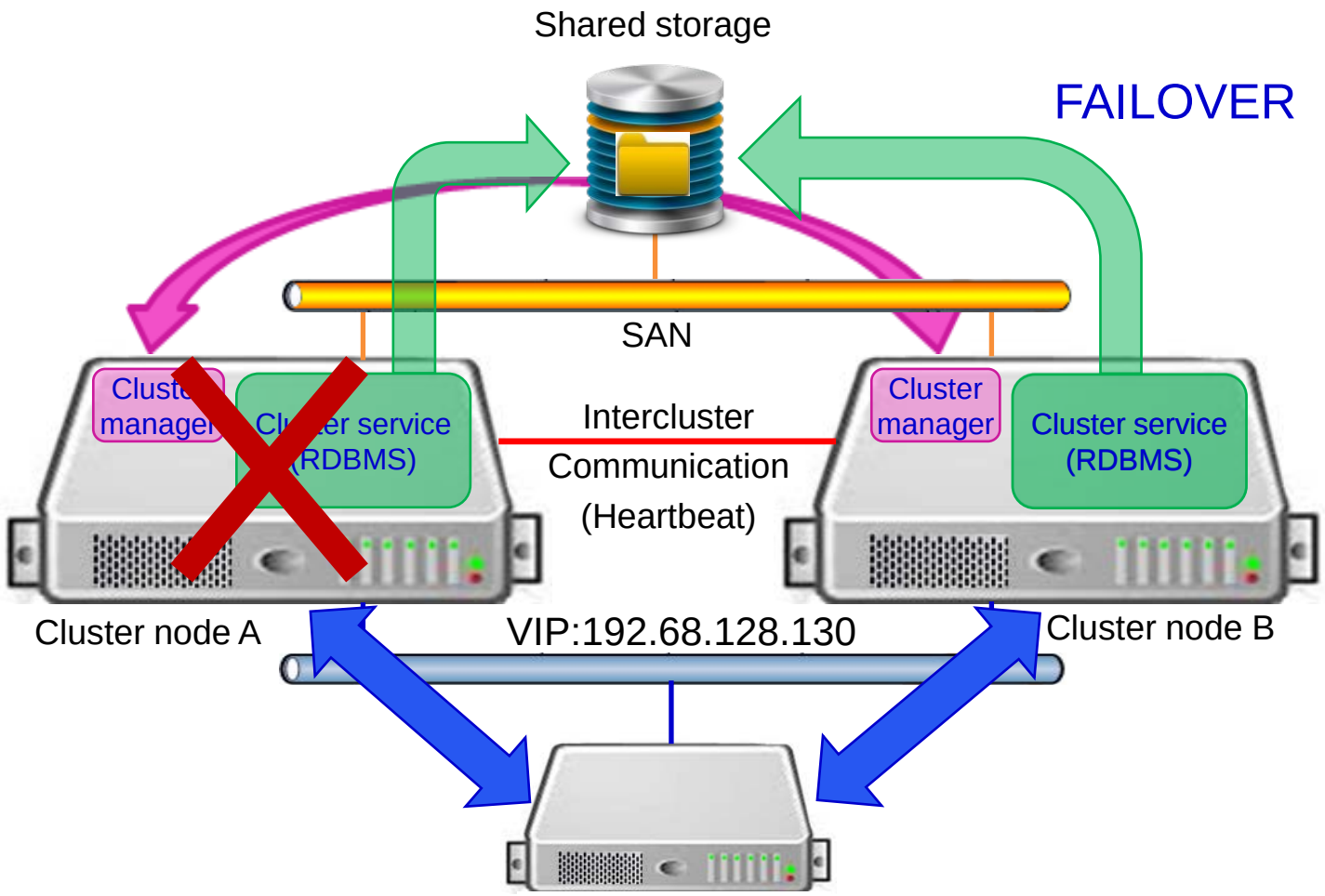
La De-duplicazione consiste essenzialmente nel fattorizzare sequenze di dati identiche presenti su file o porzioni di file diversi memorizzandole una sola volta

In questo modo è 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

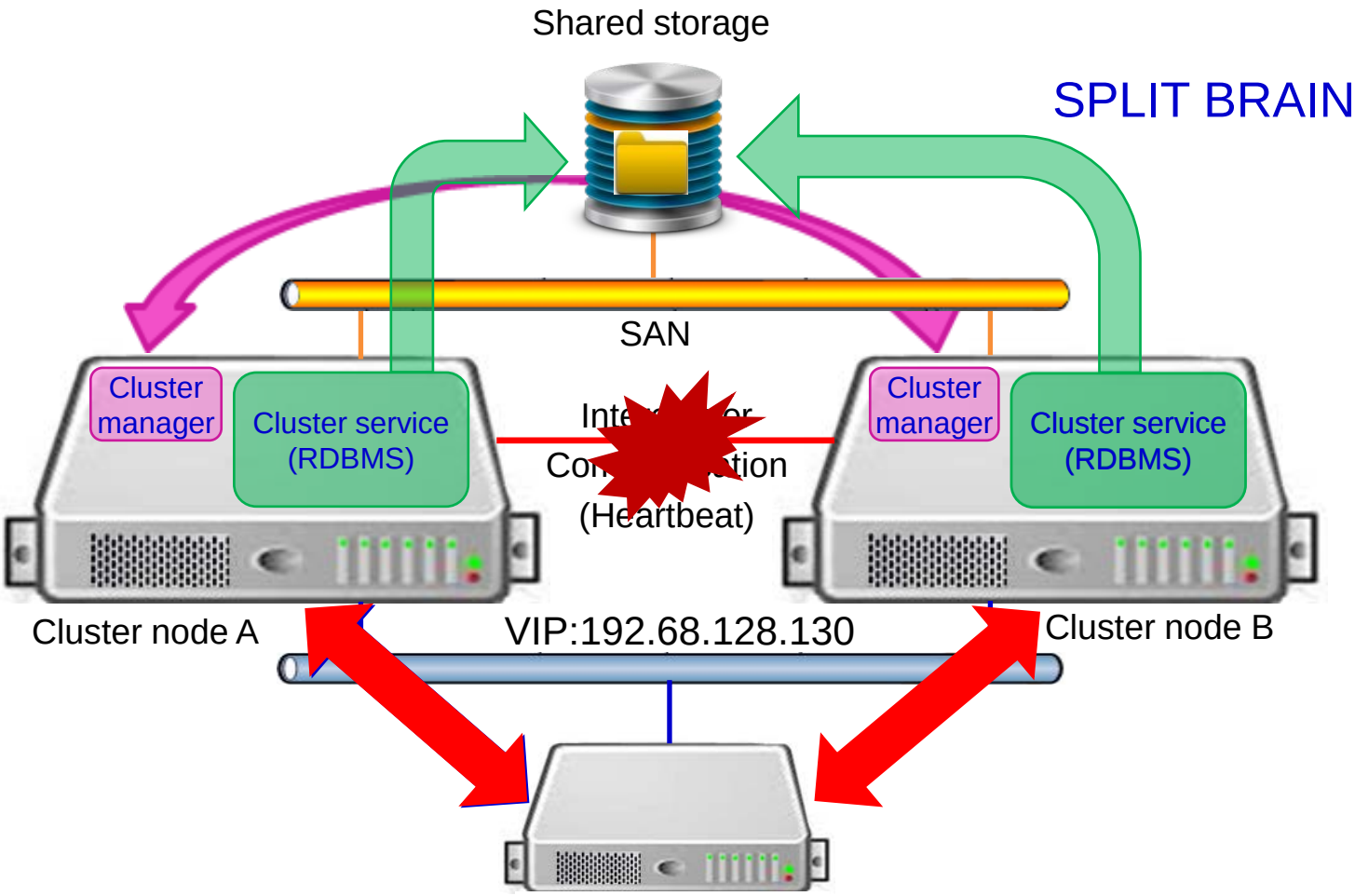
HIGH AVAILABILITY CLUSTER

Il valore di RTO può essere significativamente ridotto mediante l'utilizzo di configurazioni in cluster e storage condiviso

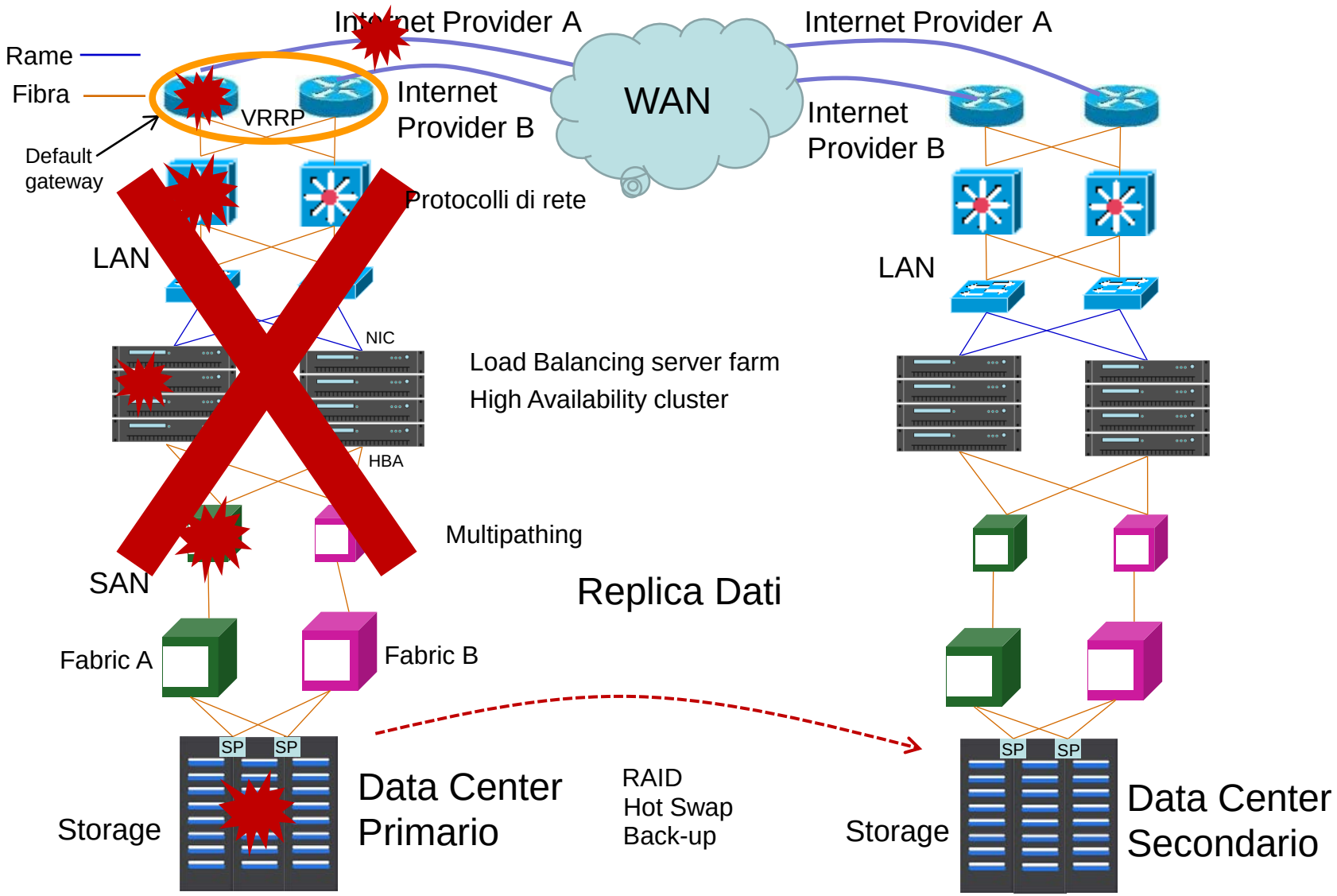


HIGH AVAILABILITY CLUSTER

L' interconnessione tra i nodi del cluster è molto importante !!



TECNOLOCIE DI FAILOVER

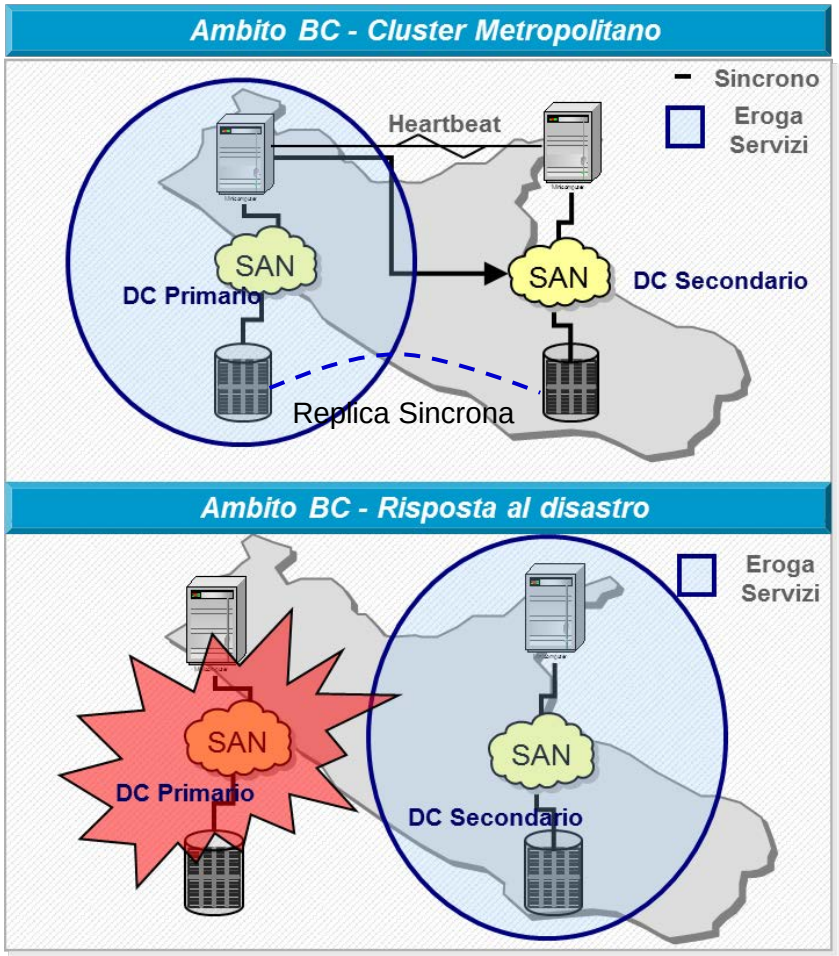


CLUSTER GEOGRAFICO

Il cluster può essere realizzato in ambito geografico o metropolitano aggiungendo un secondo sistema di storage che viene allineato con il principale mediante replica dati sincrona.

In questo caso l'Alta Disponibilità diventa Business Continuity, in quanto il servizio continua ad essere erogato anche se il DC Primario decade

Il vincolo principale è la velocità delle transazioni dovuta alla replica sincrona



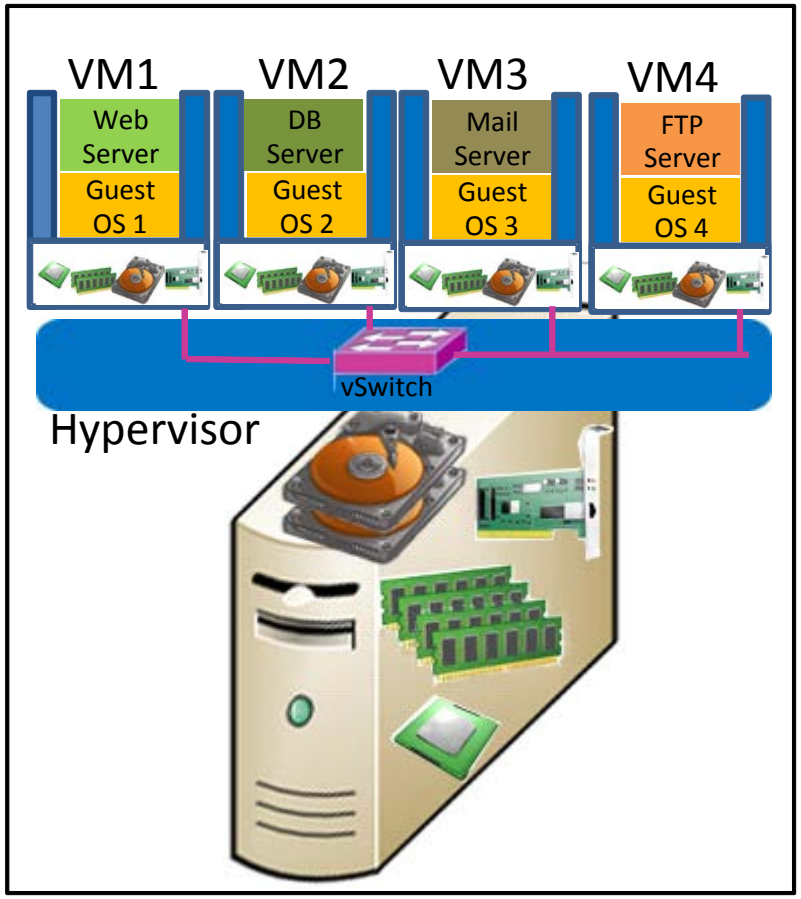
VIRTUALIZZAZIONE

Con il software posso creare delle risorse hardware virtuali (CPU, memoria, HDD, rete) **ed utilizzarle per far girare sistemi operativi** (OS) **e applicazioni** (App) **in modo equivalente ad un server fisico.**

Il programma che consente la virtualizzazione viene chiamato **HYPERVISOR** e le risorse virtualizzate macchine virtuali o **VM.** Un server fisico può sostenere il carico di molte VM.

Le VM sono costituite da un insieme di file sull'Hard Disk del server fisico.

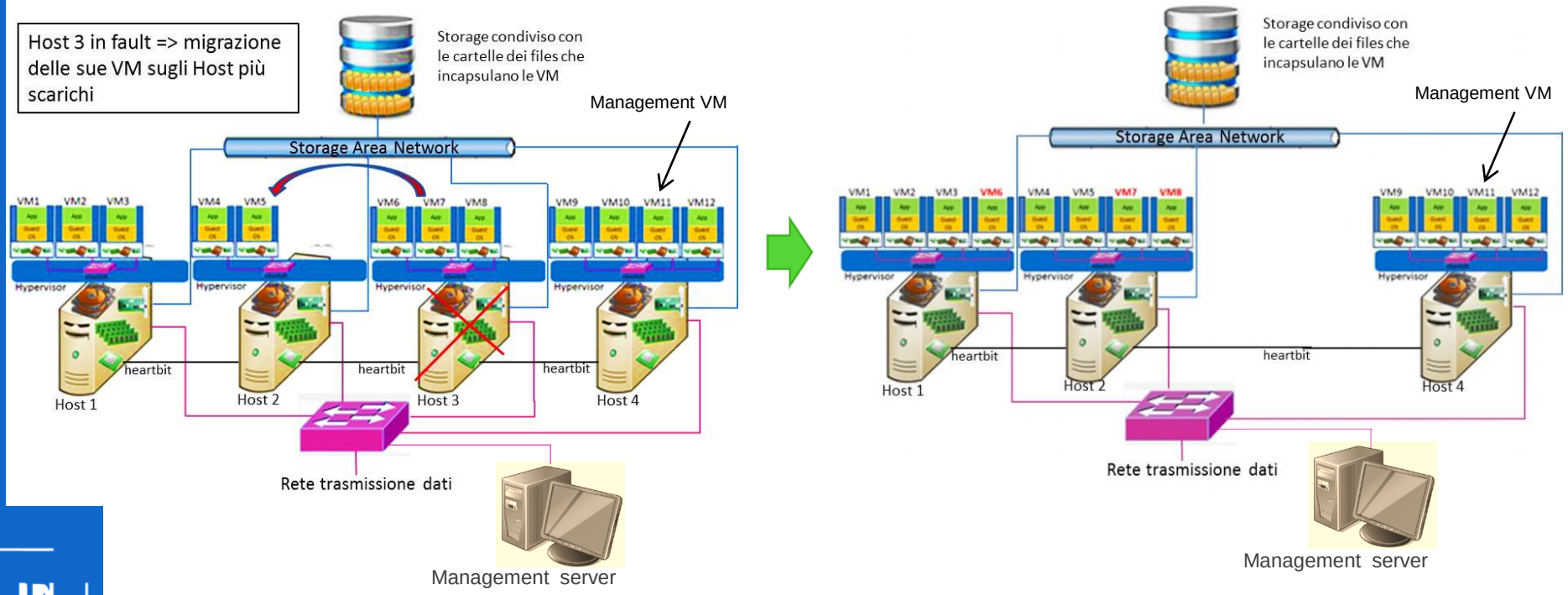
Le caratteristiche «fisiche» che la VM possiede sono liberamente configurabili ovviamente all'interno delle risorse hardware effettive del server fisico



Failover in virtualizzazione

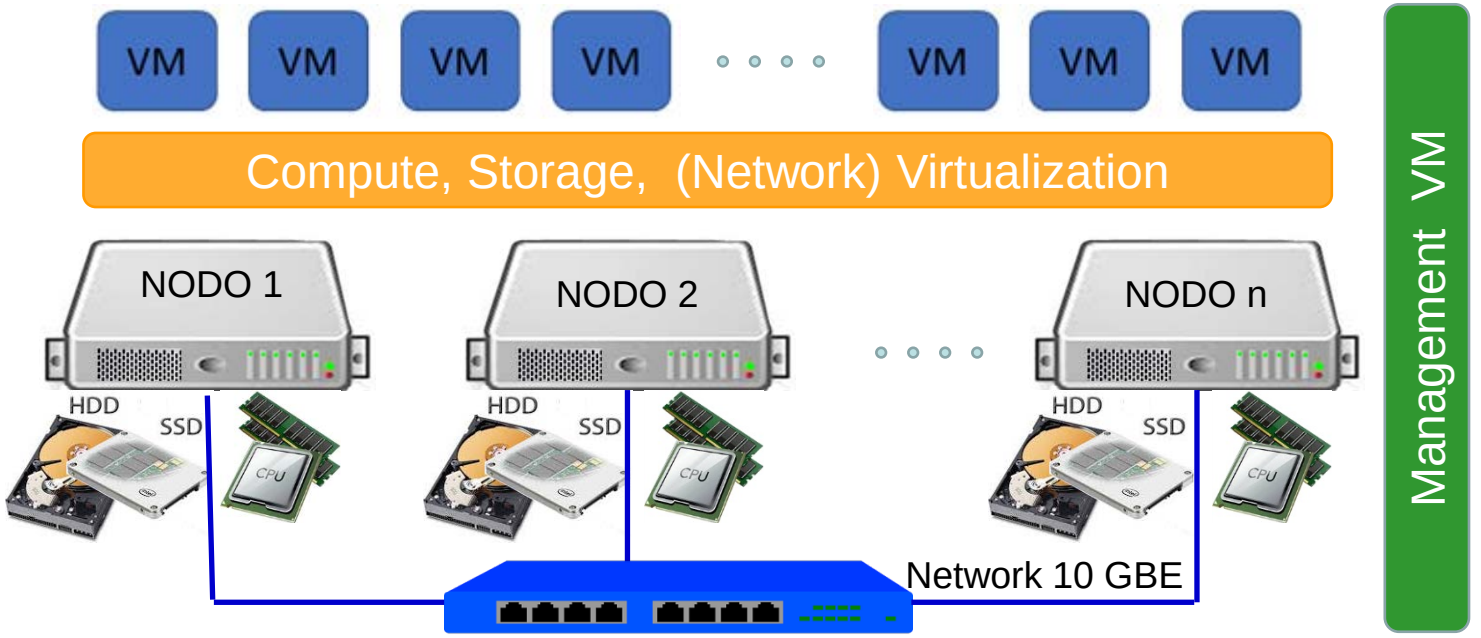
Se il server fisico si guasta cosa succede alle Virtual Machines ?!?

La soluzione si basa sulla disponibilità dello storage condiviso tramite la rete SAN oppure in replica sincrona



Il futuro oggi: Iperconvergenza

Le scritture sono **replicate** o **distribuite** su più nodi (***redundancy factor***) – No data locality



Necessità di una **comunicazione dedicata ad alta velocità** fra i nodi del cluster, per distribuire dati e metadati

CLOUD COMPUTING

Il cloud computing è un nuovo concetto di erogazione di servizi IT, forniti on demand utilizzando risorse computazionali virtualizzate.

Il modello di servizio prevede la continuità operativa attraverso le zone di disponibilità o Availability Zones.

Ogni zona di disponibilità è costituita in effetti da uno o più Data Center completamente indipendenti connessi da una rete ad alte prestazioni in modo da fornire bassa latenza.

Si possono quindi implementare soluzioni in Cloud ad alta disponibilità replicando la configurazione che eroga i servizi IT (risorse di calcolo, archiviazione e networking) in zone diverse.

Tra le zone di disponibilità la replica dei dati avviene in maniera sincrona garantendo la Business Continuity.

Le zone di disponibilità sono aggregate in regioni (Region), e si può richiedere un servizio di DR (DRaaS) nel quale i dati vengono replicati in maniera asincrona su una Region diversa.

AGENDA

- **Introduzione**
  - *Terminologia e Standard*
  - *Normative e Linee Guida*
- **I fondamenti del Disaster Recovery e della Business Continuity**
  - *Parametri di Base RPO e RTO*
  - *Descrizione delle tecnologie abilitanti*
- **Soluzioni di Disaster Recovery**
  - *Scelte di progetto*
  - *Soluzioni disponibili*

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:

Time shares 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

DISASTER RECOVERY PLAN

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

ESEMPIO

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

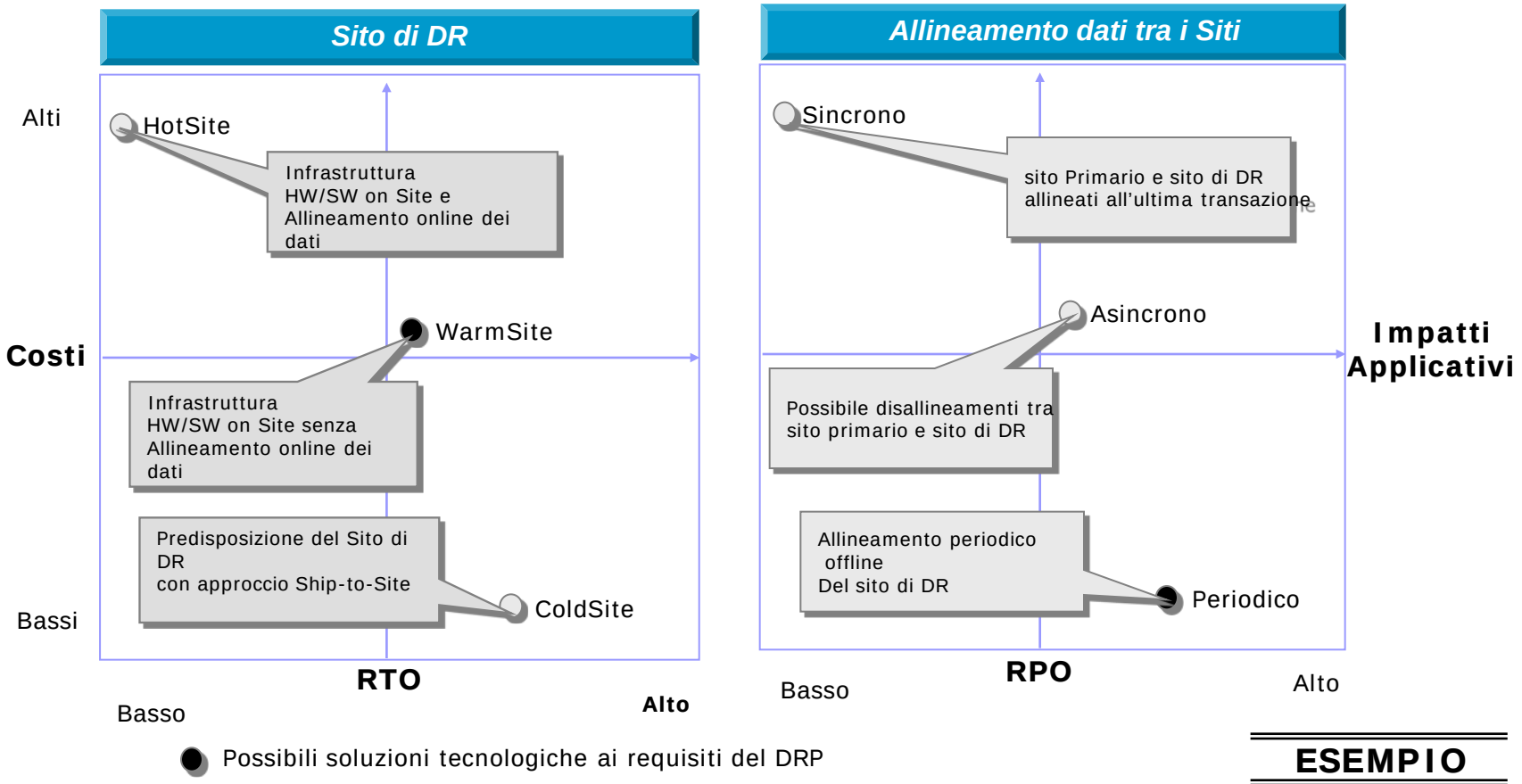
Tempo di Ripristino	Basso	Medio	Alto
Riduzione Perdite	M€	M€	K€
Costo del Ripristino	10M€	100K€	K€
Delta Benefici-Costi	negativo	**Positivo**	nessuno

Il parametro di 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

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

TIPOLOGIA SITO DI DR versus RTO e RPO

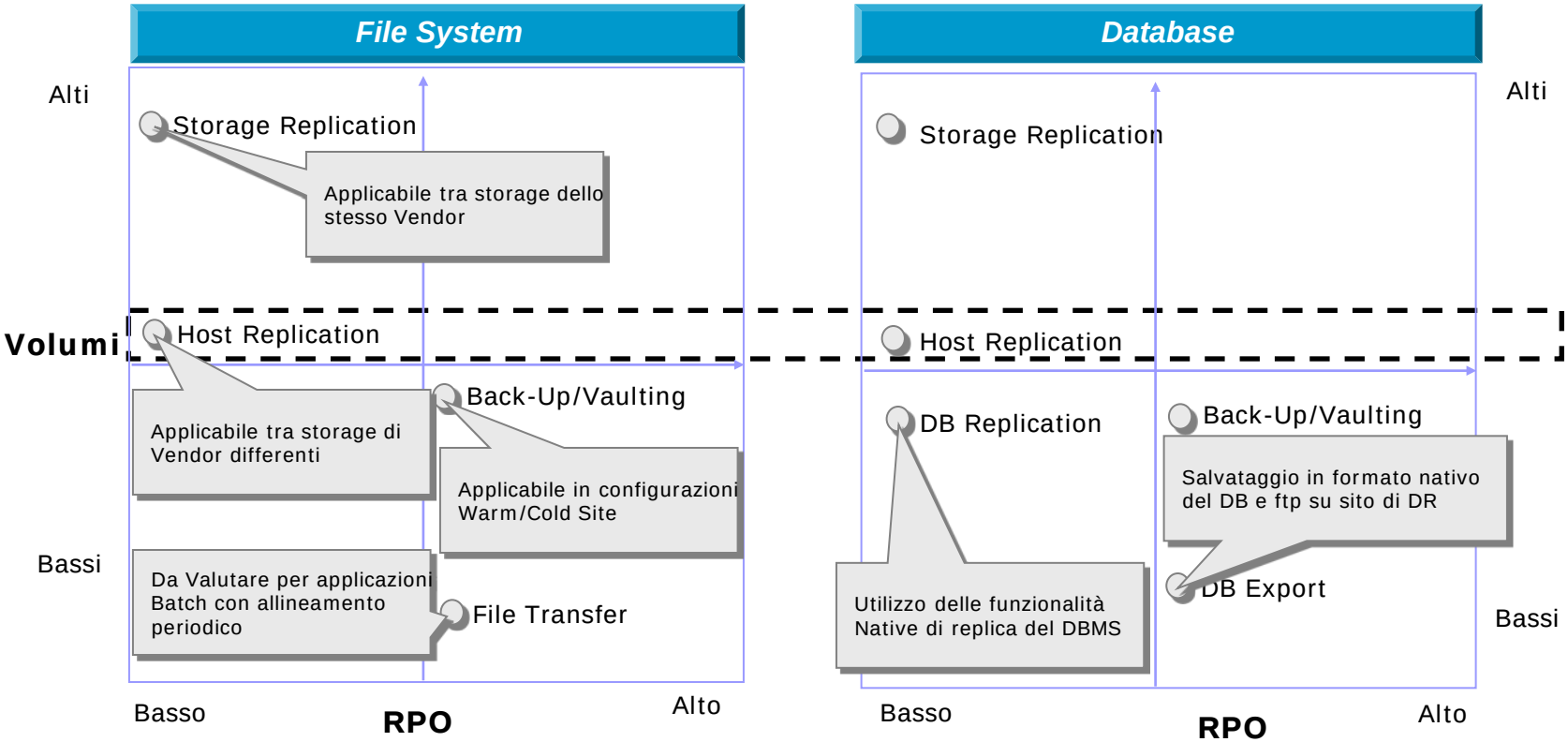
La valorizzazione dei parametri di RTO (Recovery Time Objective) e RPO (Recovery Point Objective) influenza i costi di realizzazione e gli impatti applicativi di una strategia di DR



ESEMPIO

RPO e VOLUMI

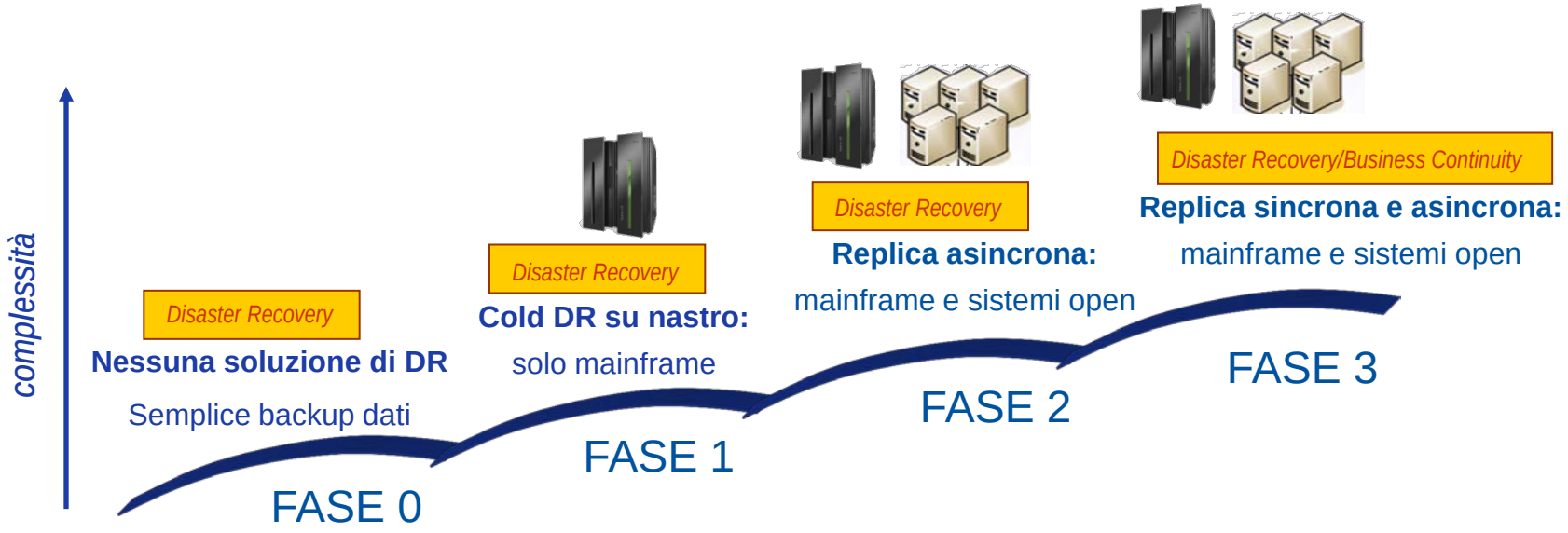
L'architettura Applicativa e Tecnologica dei sistemi coinvolti dalla strategia di DR, determina le scelte tecnologiche adeguate per la replica dei dati applicativi



EVOLUZIONE SOLUZIONI DR

Per le aziende che erogano servizi finanziari, con l'avvento delle direttive di Basile 2, il disaster recovery e la business continuity sono diventate diventate un punto centrale per l'erogazione dei servizi.

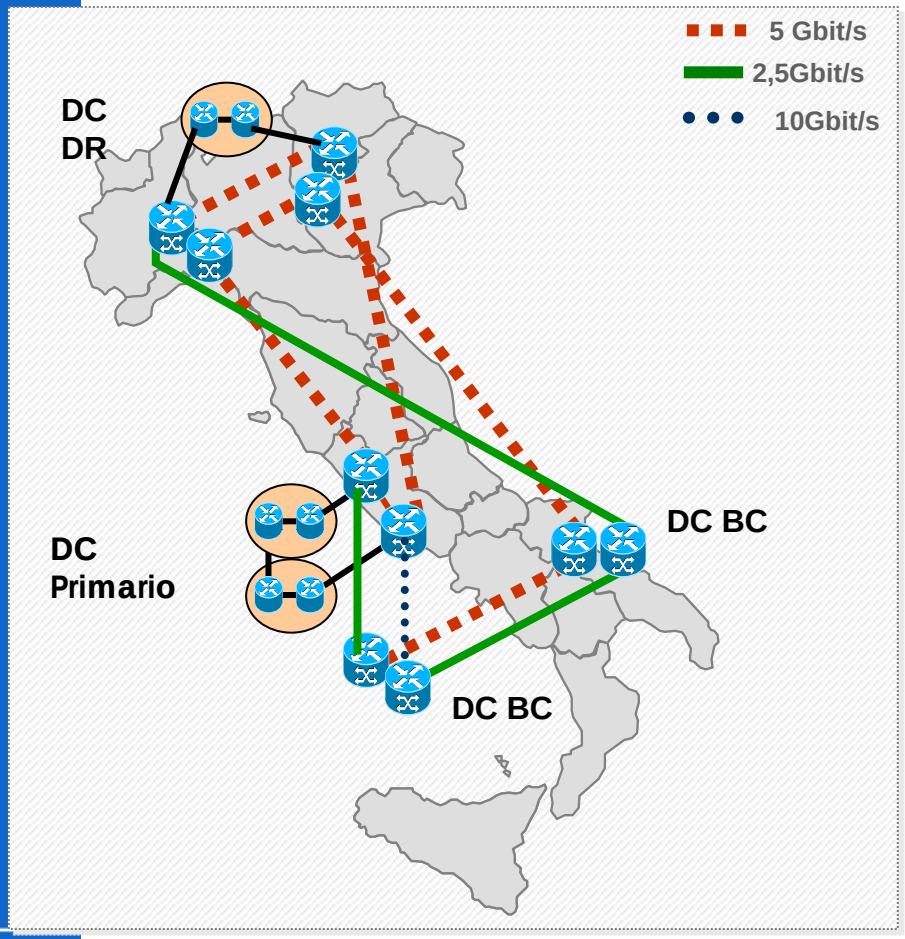
- La soluzione deve comprendere sia le applicazioni che risiedono su sistemi mainframe sia quelle sui sistemi open
- Una tipica roadmap di evoluzione della soluzione è la seguente:



L'IMPORTANZA DELLE TLC

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

Rete di Interconnessione tra i Data Center



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

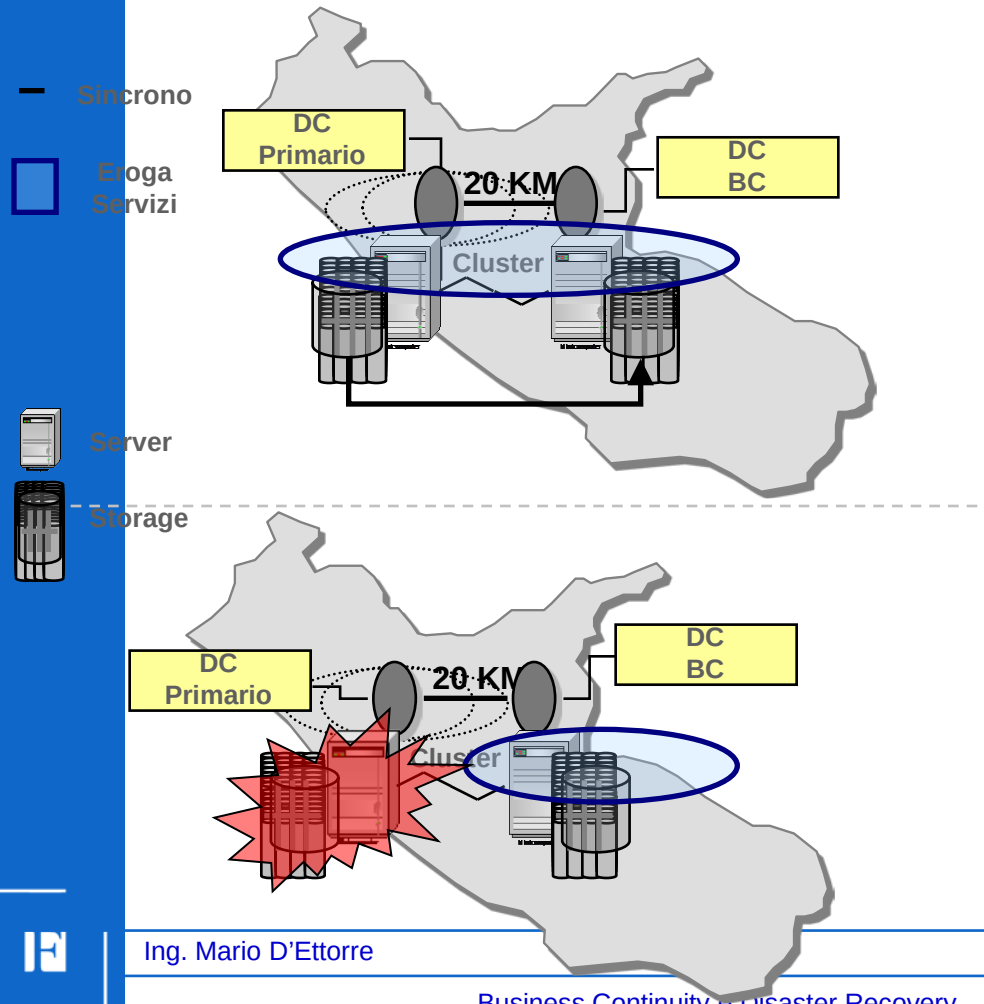
Permette l'erogazione di servizi di interconnessione diversi in funzione del Data Center

Infrastruttura di supporto per le soluzioni di DR e BC

ESEMPIO

CONFIGURAZIONE BC con CLUSTER GEOGRAFICO

Architettura Logica



Allineamento dei Dati

Allineamento sincrono dello storage tra il sito primario e DC Business Continuity

Allineamento dei Server

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

Risposta al disastro Localizzato nel DC Primario

Ripartenza dei sistemi nel sito di BC senza perdita di dati

Risposta al disastro Esteso nell'area geografica

Non disponibile

ARCHITETTURA MULTISITE O STAR

La soluzione più avanzata e largamente adottata in questi ultimi anni, 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: un sito primario di produzione, un secondo sito, detto bunker, a circa 20 km e un terzo sito, per il DR, ad oltre 100 km dal sito primario. Questa architettura protegge 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 Virtual Tape (VTS)

Criticità:

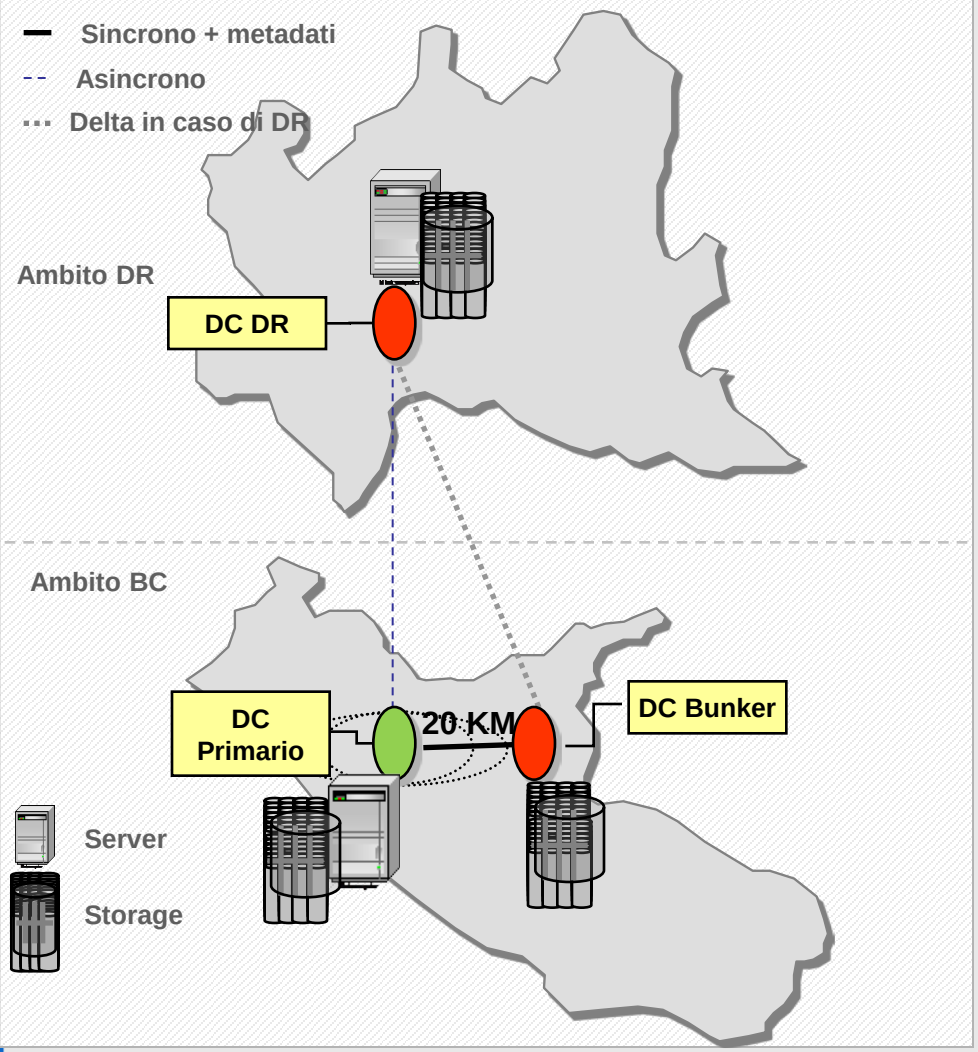
- ✓ Impatto sulle prestazioni del sito primario a causa della copia sincrona.
- ✓ Soluzione tecnologicamente avanzata e pertanto contenente elementi di complessità gestionale

Azioni di contenimento:

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

ALCUNE CONFIGURAZIONI DI ESEMPIO: REPLICA MULTISITE

Architettura Logica- Replica Multisite



Allineamento dei Dati

Allineamento asincrono dello storage tra il sito primario e il DC di DR

Allineamento sincrono dello storage tra DC Primario e DC Bunker, contestualmente sono inviati anche i metadati necessari a tracciare lo stato di avanzamento dell'allineamento asincrono tra DC Primario e DR

Allineamento dei Server

I server possono essere configurati in modalità

- Hot
- Warm
- Cold

Risposta al disastro Localizzato nel DC Primario

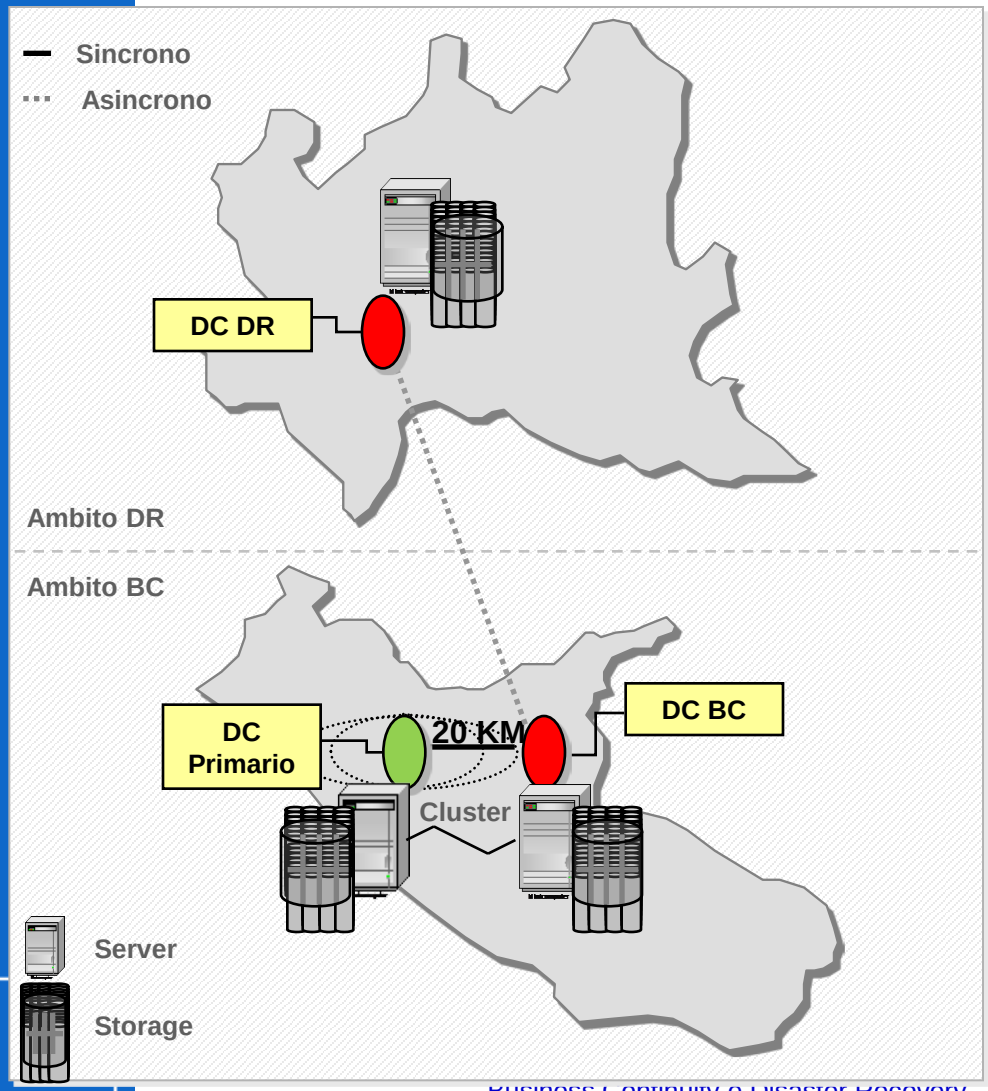
Allineamento del delta dei dati necessari a sincronizzare lo storage del DC di DR con quello Bunker

Ripartenza dei sistemi nel sito di DR senza perdita di dati (RPO=0)

Disastro Esteso nell'area romana

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

Architettura Logica- Replica in cascata



Allineamento dei Dati

Allineamento sincrono dello storage tra il sito primario e DC di BC

Allineamento asincrono dello storage tra il sito DC BC e il sito di DR

Allineamento dei Server

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 DC Primario

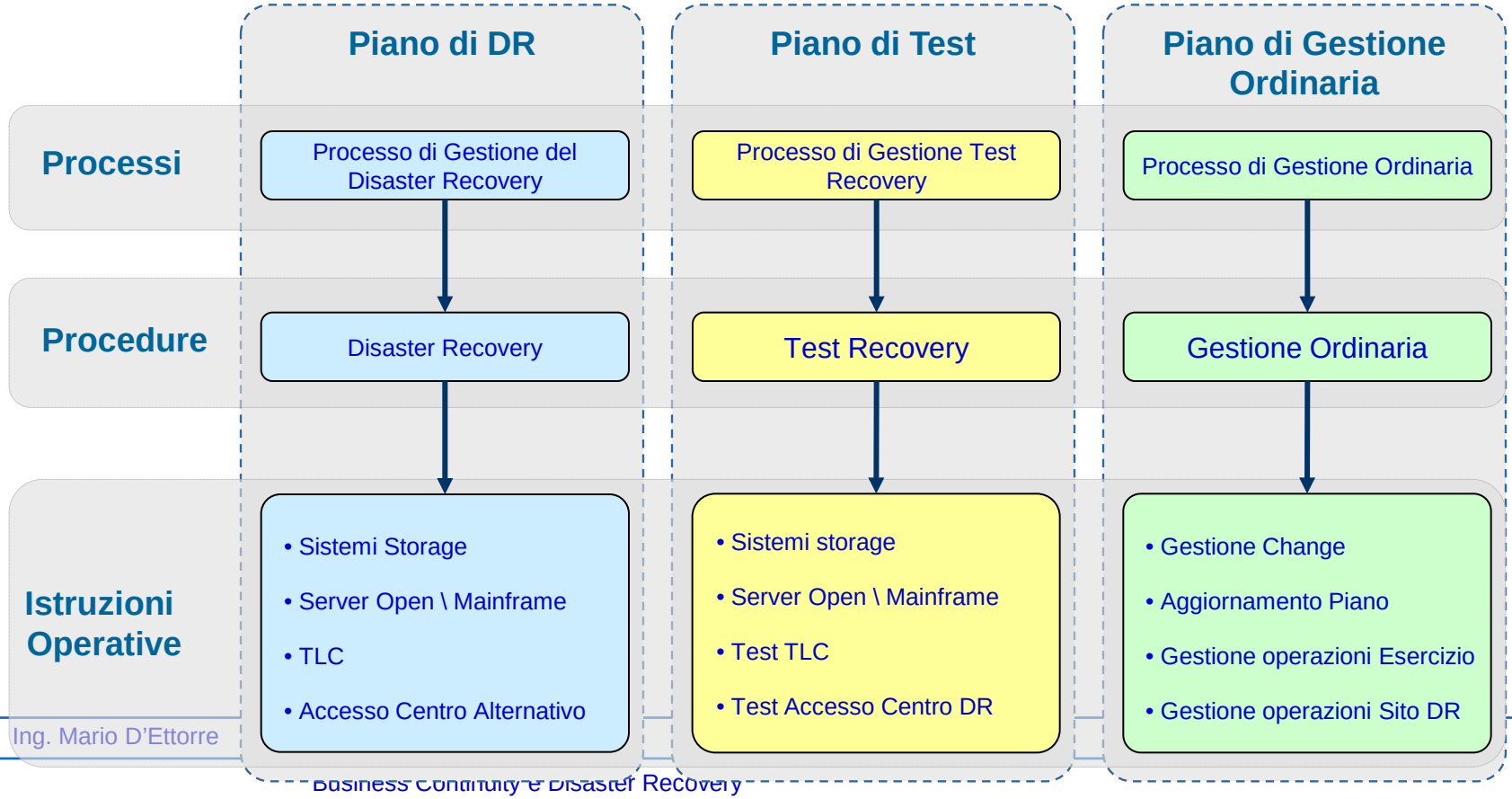
Ripartenza dei sistemi nel sito di BC sulla copia allineata oppure nel caso di replica bidirezionale nessun impatto sul servizio

Risposta al disastro Esteso nell'area geografica

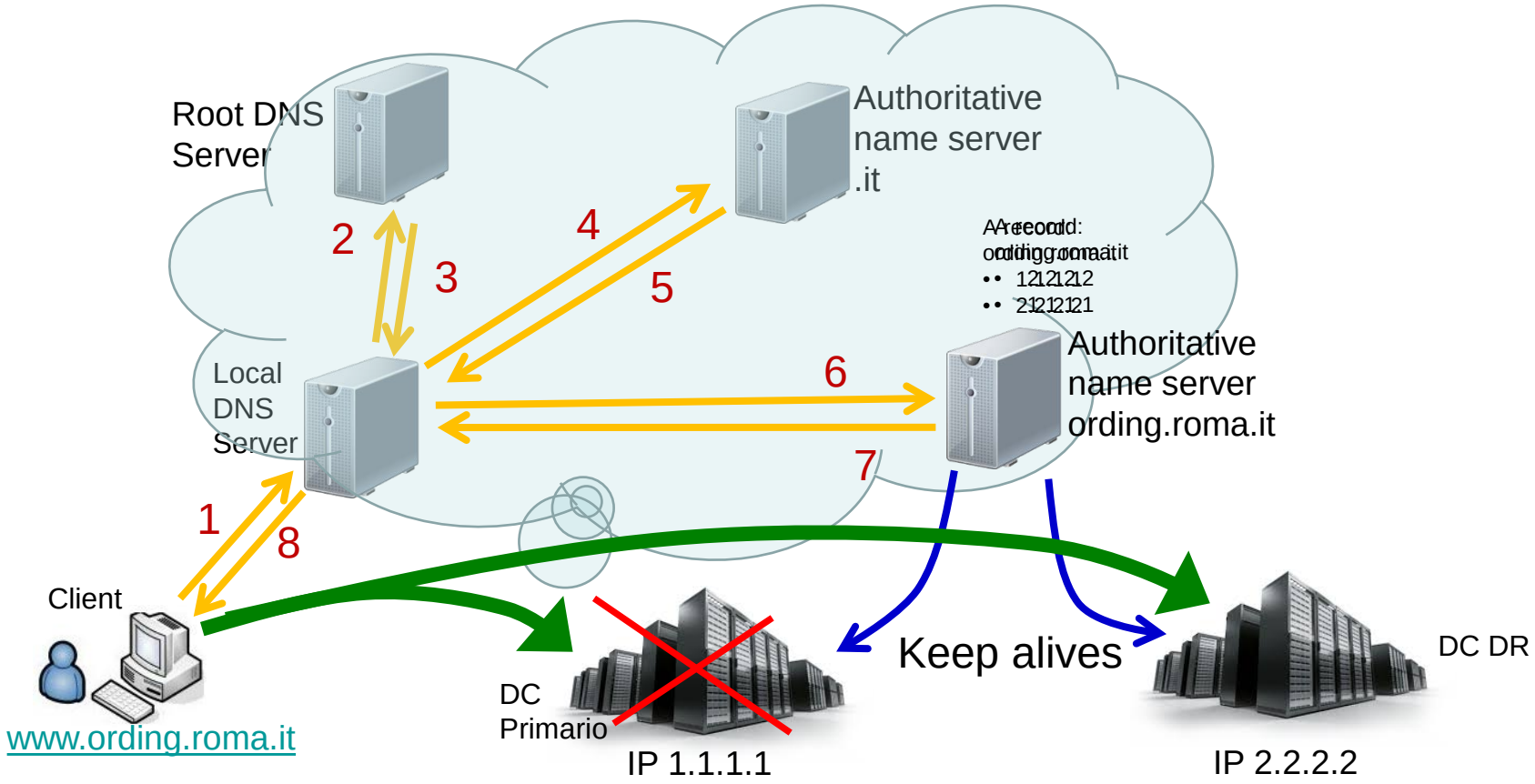
Ripartenza dei sistemi sul sito di DR con perdita dei dati proporzionale alla frequenza dell'allineamento periodico

DOCUMENTAZIONE

- 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.



SELEZIONE TRAMITE DNS



Il Domain Naming System (DNS) consente di utilizzare i "nomi di dominio" al posto degli indirizzi IP. Il sistema è realizzato tramite i server DNS (nodi) che conservano le corrispondenze IP <> nomi di dominio di cui sono responsabili e si rivolgono ai nodi successivi per trovare informazioni di altri domini.

GRAZIE

per L’ATTENZIONE

email to : dettorremario@gmail.com