WORKSHOP GARR 2025

NET MAKERS

Infrastruttura di Business Continuity e Disaster Recovery dell'INFN

Stefano Longo

Istituto Nazionale di Fisica Nucleare - CNAF

Domande?

Fatele quando volete

Per le domande potete usare: wooclap.com con codice WSGARR25

Ora però iniziamo 😉

Introduzione

L'INFN è un ente distribuito sul territorio italiano. Sono presenti

- 20 Sezioni
- 6 Gruppi collegati
- 4 Laboratori Nazionali (LNF, LNS, LNGS, LNL)
- 3 Centri Nazionali (CNAF, GGI, TIFPA)

Ogni sito offre una serie di servizi ai propri utenti.
Alcune esigenze della nostra utenza sono comuni a tutte le sedi.

Introduzione

I Servizi forniti all'intera comunità INFN vengono erogati principalmente da due siti:

- CNAF
- Laboratori Nazionali di Frascati

Motivo della centralizzazione è l'economia di gestione:

- Infrastrutturale (Affidabilità, disponibilità, monitoraggio, backup, DR, etc.)
- Personale

(Ad un incremento di SLA corrisponde un aumento non lineare in termini di costi e di complessità di gestione)

Introduzione

I due siti hanno implementato infrastrutture in Alta Affidabilità (HA) in grado di massimizzare la disponibilità dei servizi e dei dati.

Nella progettazione è stato considerato uno SLA che assicurasse continuità di servizio anche in presenza dei problemi più comuni.

Considerando il CNAF come esempio sono state implementate:

SAN che garantiscano l'accesso ai dati anche in presenza di malfunzionamenti HW (dischi e controller). Nel tempo poi si è garantita la disponibilità dei dati anche in termini di velocità di accesso, mediante sistemi in grado di bilanciarsi automaticamente

Sistemi di virtualizzazione «managed», in grado di resistere ai malfunzionamenti più comuni (rottura sistemi di alimentazione, schede di rete o di accesso alla SAN) o comunque in grado di reagire autonomamente alla rottura di un certo numero di server.

Backup in grado di garantire la presenza di una seconda copia dei dati

Infrastruttura di Business Continuity

Data la pervasività dei servizi offerti sia dalla CCR che dalla DSI, ad inizio 2017 viene sollevata dal management la richiesta di assicurare - per i servizi essenziali - la disponibilità senza dover attendere i tempi lunghi di un potenziale «recovery manuale», anche in presenza di una «major failure» in uno dei siti impiegati per l'esecuzione dei servizi (Business Continuity).

Nasce il progetto BC che ha portato all'infrastruttura attualmente impiegata per l'erogazione dei servizi

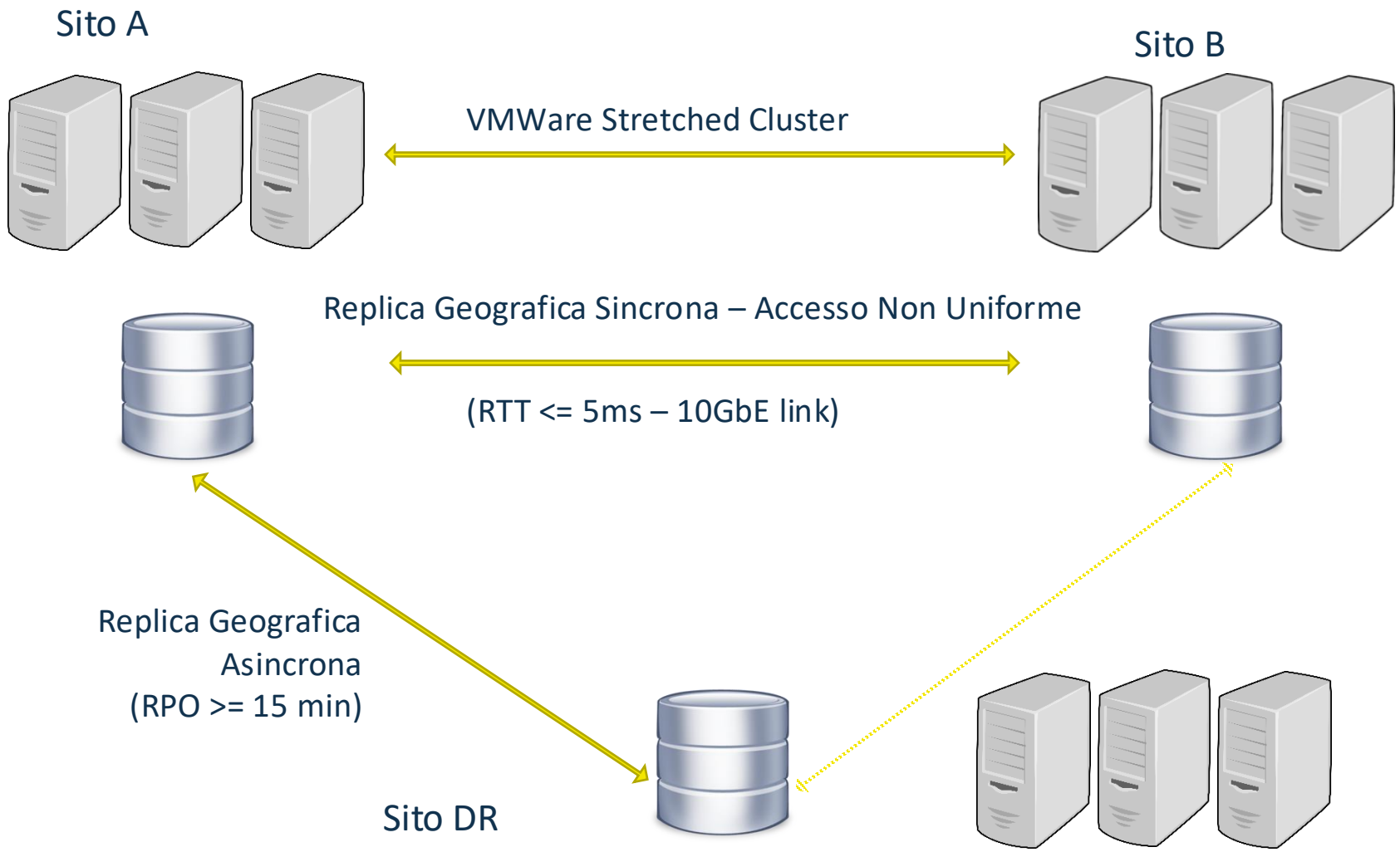
Il progetto prevede il coinvolgimento di tre siti: il CNAF, un sito a distanza medio-bassa per la Business Continuity ed un sito a grande distanza per il DR

Infrastruttura di Business Continuity

I requirements per aumentare affidabilità e disponibilità di dati e applicazioni prevedevano:

- Servizi fruibili anche in caso di indisponibilità di uno dei centri impiegati per l'esecuzione
- Un Recovery Point Objective ~ 0
- Un Recovery Time Objective -> 0
- Nessuna introduzione di particolari requisiti a livello applicativo
- Alta Affidabilità implementata a livello infrastrutturale
- Implementazione comprensiva di DR per adempiere alla corrente normativa e per facilitare recovery di eventuali disastri

Infrastruttura di Business Continuity

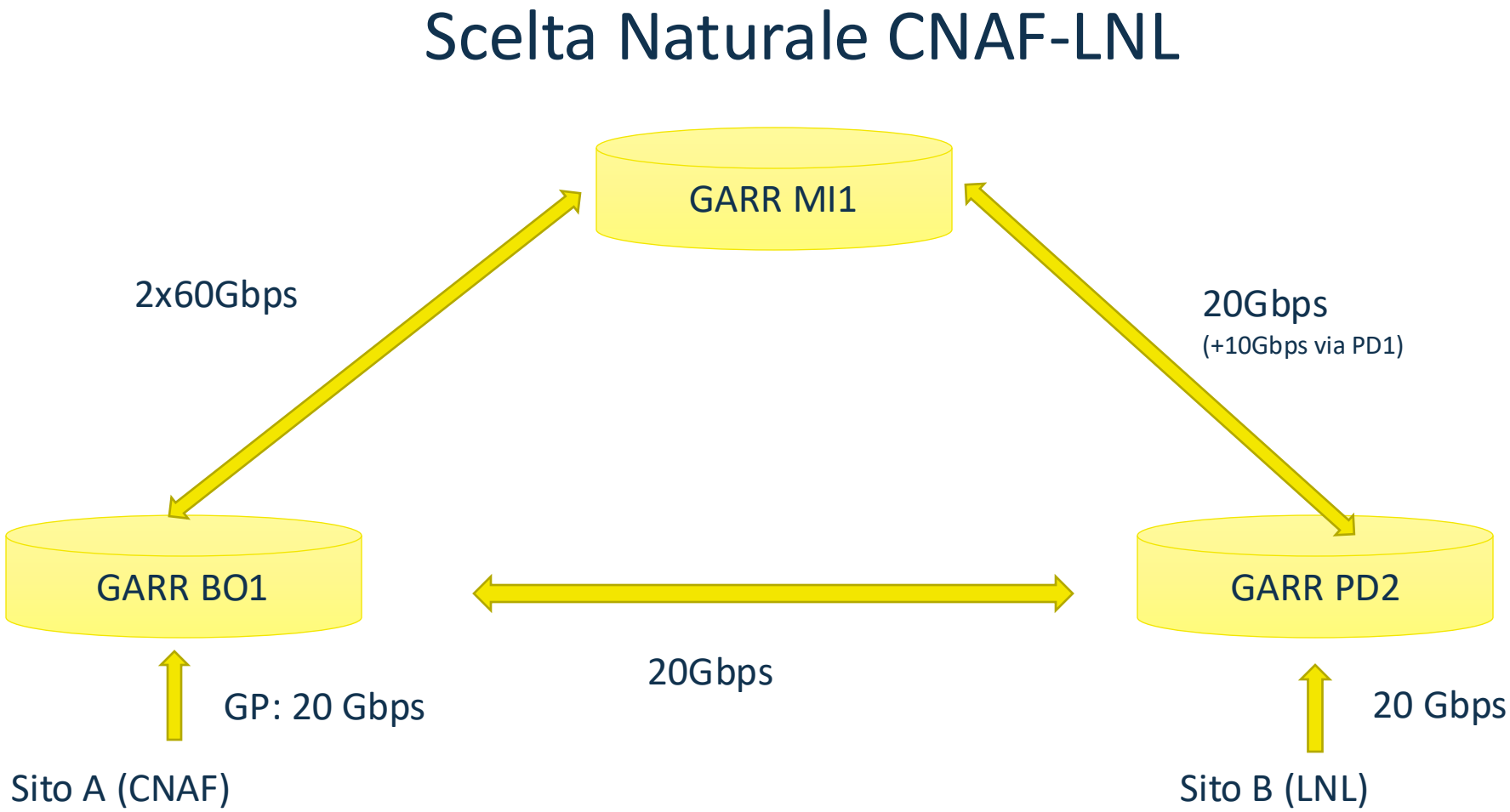


Infrastruttura di Business Continuity

Ricerca per un secondo sito

- Ad un RTT ragionevole (inferiore a 5ms)
- Con un datacenter già in essere
- In grado di fornire continuità elettrica e di raffreddamento
- Che disponga di un path alternativo per la connettività geografica

Infrastruttura di Business Continuity



Infrastruttura di Business Continuity

Qualche dettaglio implementativo:

- VPN con estensione L2 tra CNAF e LNL
- Stretched cluster Attivo/Attivo con accesso NON uniforme, SAN FC
- RTT CNAF-LNL ≈ 2ms
- Routing verso WAN gestito via VRRP
- Reti servizi annunciate da entrambi i siti con pesi diversi: durante il normale funzionamento il routing è gestito dal CNAF, in caso di inaccessibilità del data center, il routing converge su LNL (tempo necessario ≈ 1 minuto).
- RPO = 0, RTO nel range dei minuti (in funzione del fallimento)
- Failover VMware gestito mediante SAN (PDL); implementati controlli aggiuntivi (APD, DRS, placement e soglie di ingresso)
- Split-brain gestito con witness installato a LNF (sito DR)

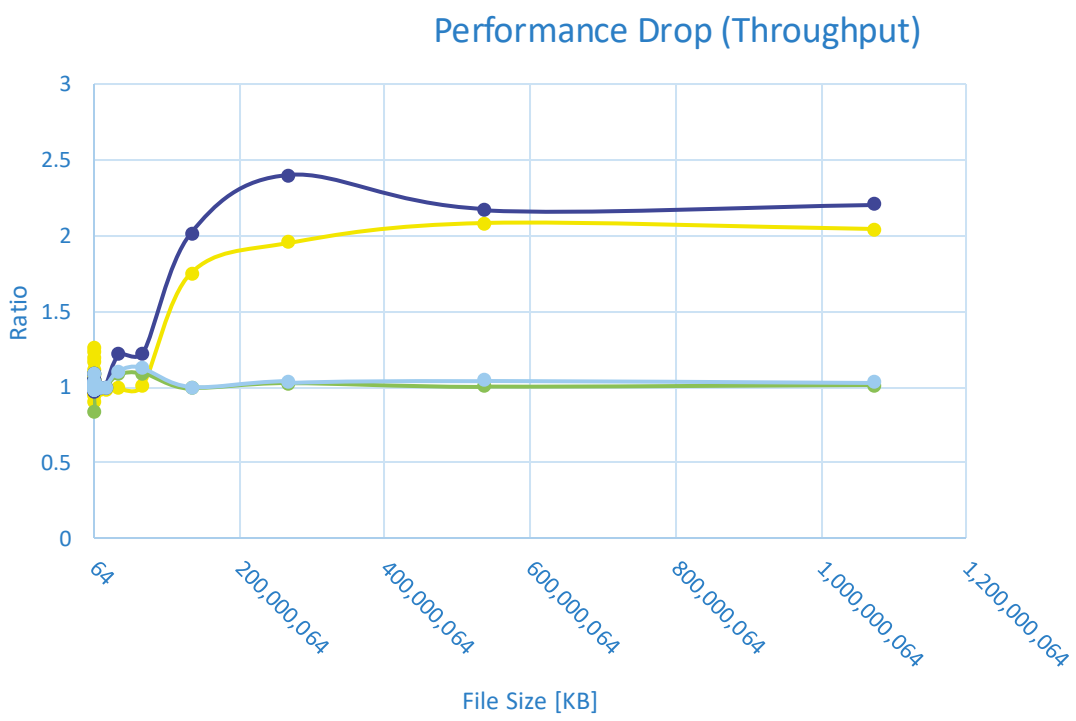
BC – Stato Attuale

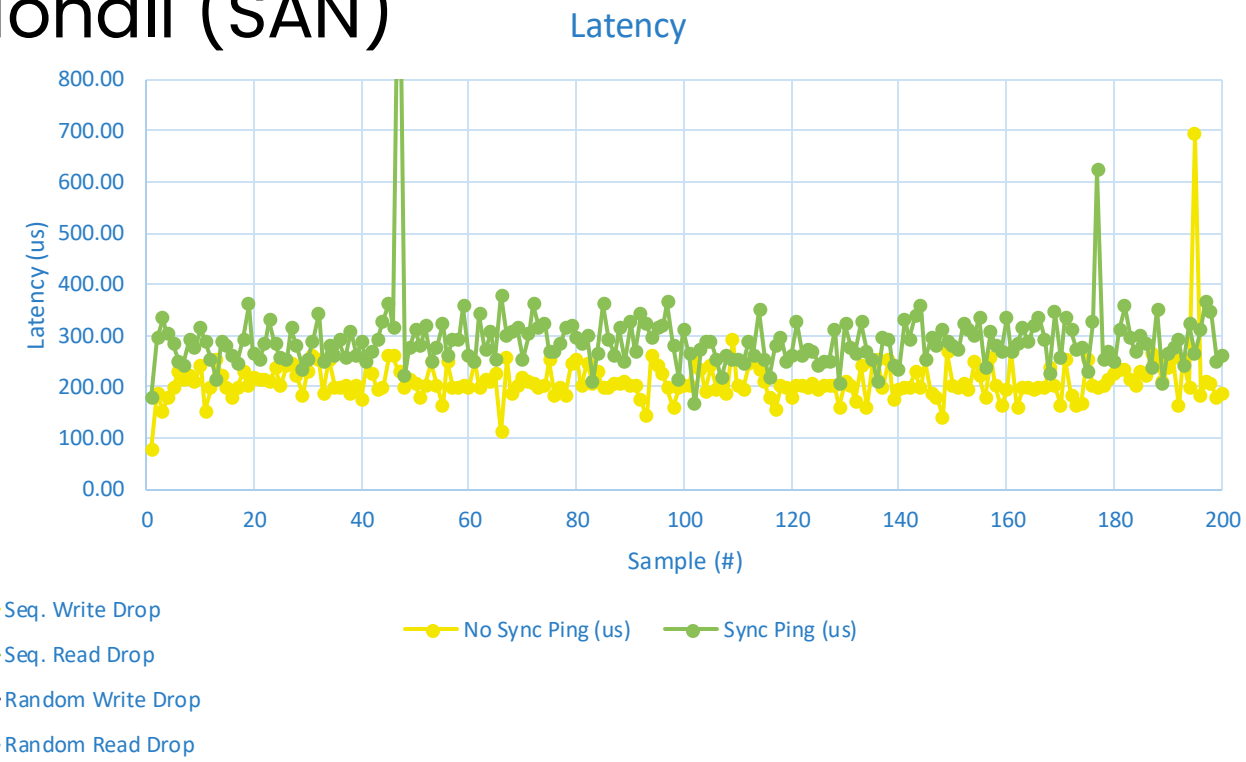
Alcuni risultati:

- SAN: Blocco ≈ 125TB, in replica geografica sincrona, accesso simultaneo da 4 controller, NAS ≈ 200TB in replica geografica sincrona con failover automatico dei server NAS
- 36 Hypervisor in funzione (DELL M640, MX750 e MX760)-> ≈ 15TB RAM, 1440 core
- 514 VM in esecuzione su 10 reti gestite sul link CNAF-LNL
- Infrastruttura fornita essa stessa come servizio ad altri gruppi
- Manutenzioni senza necessità di down programmati
- Continuità operativa assoluta (RTO->0) per alcuni servizi

BC – Stato Attuale

Costo RPO nullo in termini prestazionali (SAN)





BC – Stato Attuale

Assieme ai risultati positivi, qualche rovescio della medaglia:

- Infrastruttura molto dipendente dalla stabilità della rete -> Buon funzionamento infrastruttura dipende dalla frequenza degli «incidenti» sulla rete geografica
- Innesco failover a 5,5ms
- Alcuni servizi legacy mal tollerano il riavvio
- Alcuni utenti mal tollerano i riavvi delle VM 😉
- Durante alcune manutenzioni possibile innesco di incidenti multipli. L'infrastruttura converge autonomamente ma è possibile un incremento significativo del RTO

BC – Prossimi Passi

L’infrastruttura si sta avviando al settimo anno di esercizio, alcuni componenti approssimano l’EOS, in particolare la SAN.

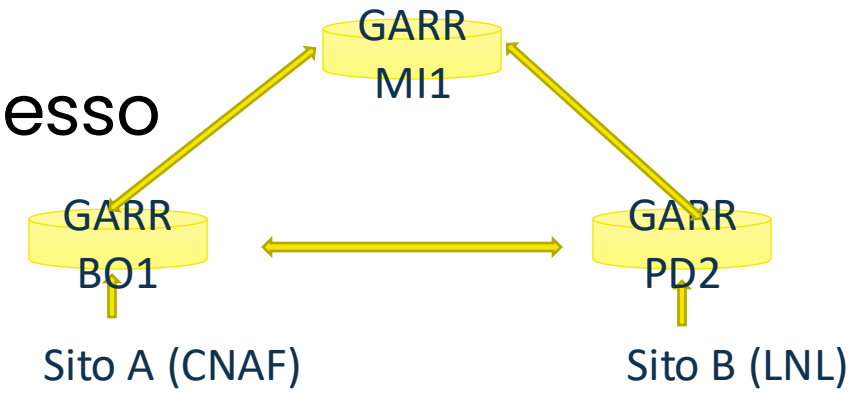
La sostituzione dell’hardware è l’occasione per riprogettare alcune componenti dell’infrastruttura, per risolvere o ridurre le criticità riscontrate durante questi anni di funzionamento

- Failover innescati da «brevi» fluttuazioni sul link CNAF-LNL
- Necessità riavvio servizi su sito superstite
- Possibili sequenze con più ripristini/riavvi dei servizi dovute al timing con cui tornano disponibili i vari componenti di rete

BC – Prossimi Passi

Il nuovo progetto prevede:

- Implementazione replica geografica sincrona in grado di supportare RTT di 10ms
- Migrazione SAN da FC ad iSCSI
- Passaggio ad uno stretched cluster con accesso uniforme
- Configurazione multipath con priorità su accesso locale
- Ottimizzazione di un secondo path su Milano usabile sia per la replica geografica sincrona che come path iSCSI…in condizioni di emergenza



Conclusioni

Un dovuto ringraziamento a tutto il Team:

Servizi Nazionali@CNAF:
- Stefano Antonelli
- Ettore Cesarini
- Marco Corvo
- Stefano Longo
- Felice Rosso

Calcolo@LNL:
- Massimo Biasotto
- Sergio Fantinel
- Michele Gulmini
- Marco Roetta

NET@CNAF:
- Lorenzo Chiarelli
- Donato De Girolamo
- Mariangela Longo
- Stefano Zani

Calcolo@LNF:
- Sandro Angius
- Dael Maselli
- Lorenzo Napoleoni
- Ramon Orrù
- Claudio Soprano
- Dario Spigone
- Tommaso Tonto
- Michele Tota

Domande?

Potete contattarci alle seguenti mail:

Stefano Longo: Stefano.Longo@cnaf.infn.it

Servizi Nazionali INFN: servnaz@lists.infn.it

WORKSHOP GARR 2025

NET MAKERS

Backup Slides

Hardware BC

2 Huawei Oceanstor 5500 v5

- 19 HD SSD da 1.92TB
- 36 HD SAS 10k da 1.8TB
- 24 HD NL-SAS da 4TB
- NAS: 24 HD NL-SAS da 12 TB + 6 SSD da 1.92 TB

2+2 Huawei SN2224

- 24 porte FC@16Gbp (12 ottiche)

2x Enclosure DELL M1000E

- 4+4 DELL PowerEdge M640
  - CPU: 2xIntel Xeon 6132 (14 cores@3,7GHz)
  - RAM: 384GB RDIMM 2667MT/s
  - HD: 2xSSD 200GB (RAID1 via H330)
  - Eth: 4 Broadcom BCM57840
  - FC: 2 Emulex LPe16002
- 2+2 Switch Ethernet Force10 MXL
- 2+2 Switch FC Brocade M6505

Hardware BC

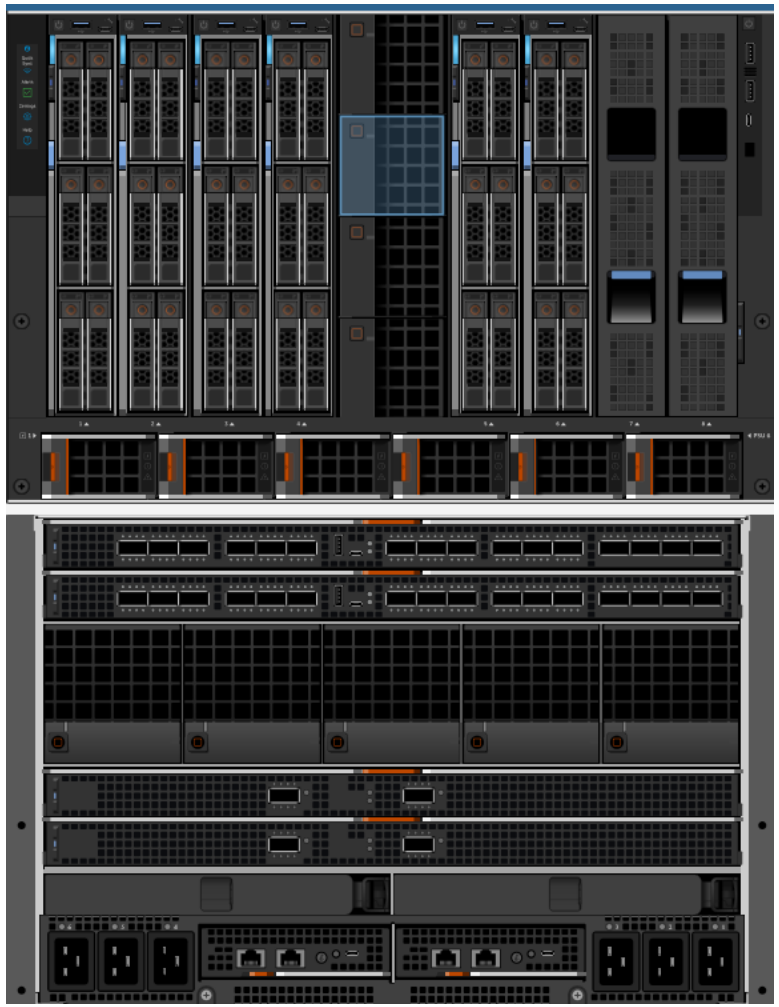
2+2 Switch Ethernet Force10 MXL

- 32 porte interne@10Gb
- 2 porte QSFP+ per connessione switch-switch
- 2 porte QSFP+ con breakout cables
- 4 porte SFP+ con ottiche impiegate per storage e uplinks

2+2 Switch FC Brocade M6505

- 16 porte interne 16GbsFC
- 8 porte esterne
- 4 ottiche montate

Hardware BC



2 x Enclosure DELL EMC PowerEdge MX 7000

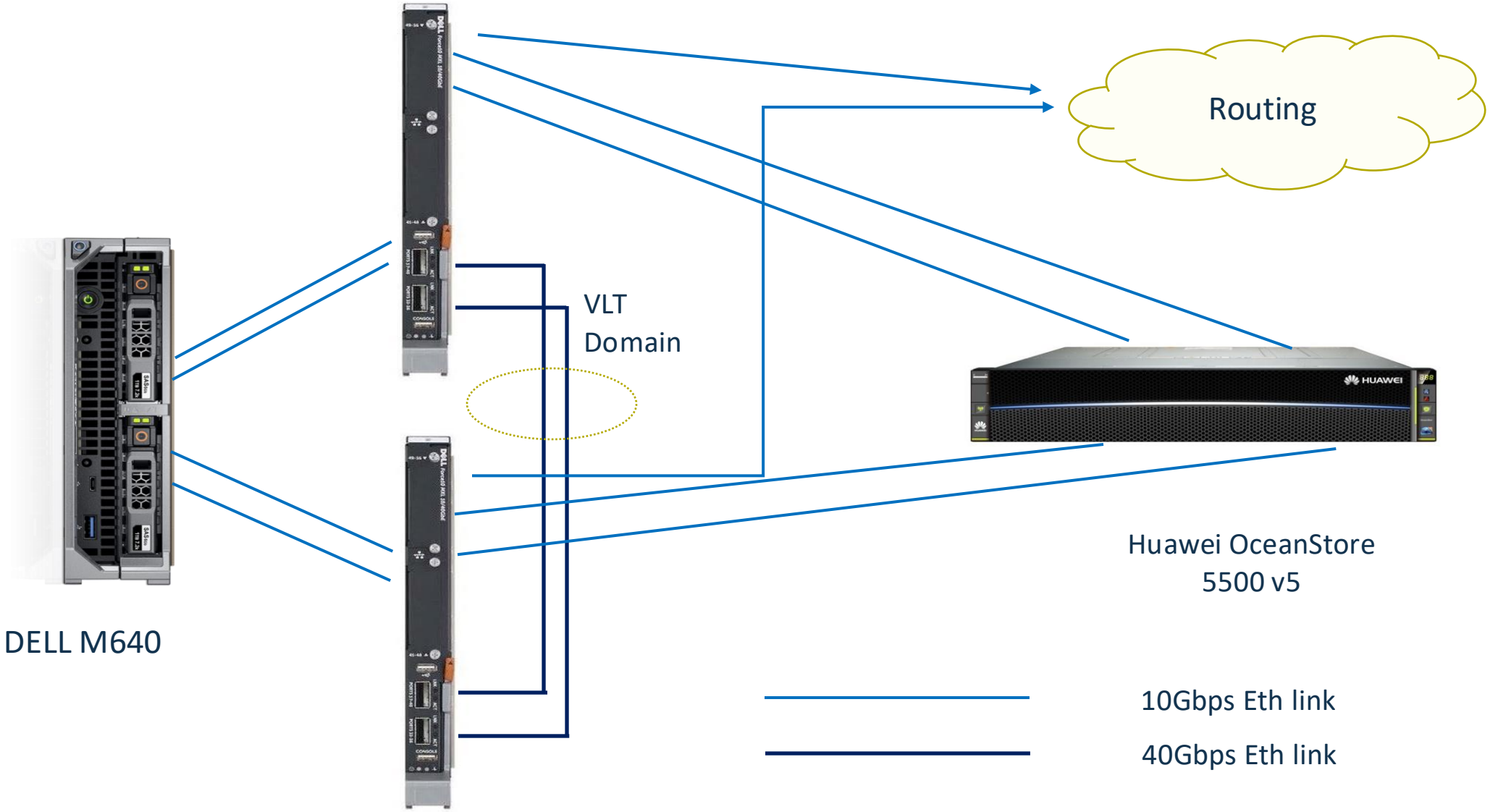
Ognuno è dotato di 3 lame PowerEdge MX 750c e 3 MX 760c con

- 2 CPU Intel Xeon Gold 6342/6542Y
- 512 GB di RAM (espandibile a 1TB)
- 2 HD SSD da 446GB con controller RAID PERC H745P (RAID 1)
- 2 Schede di rete Qlogic CNA, ognuna con 2 porte a 25Gbps

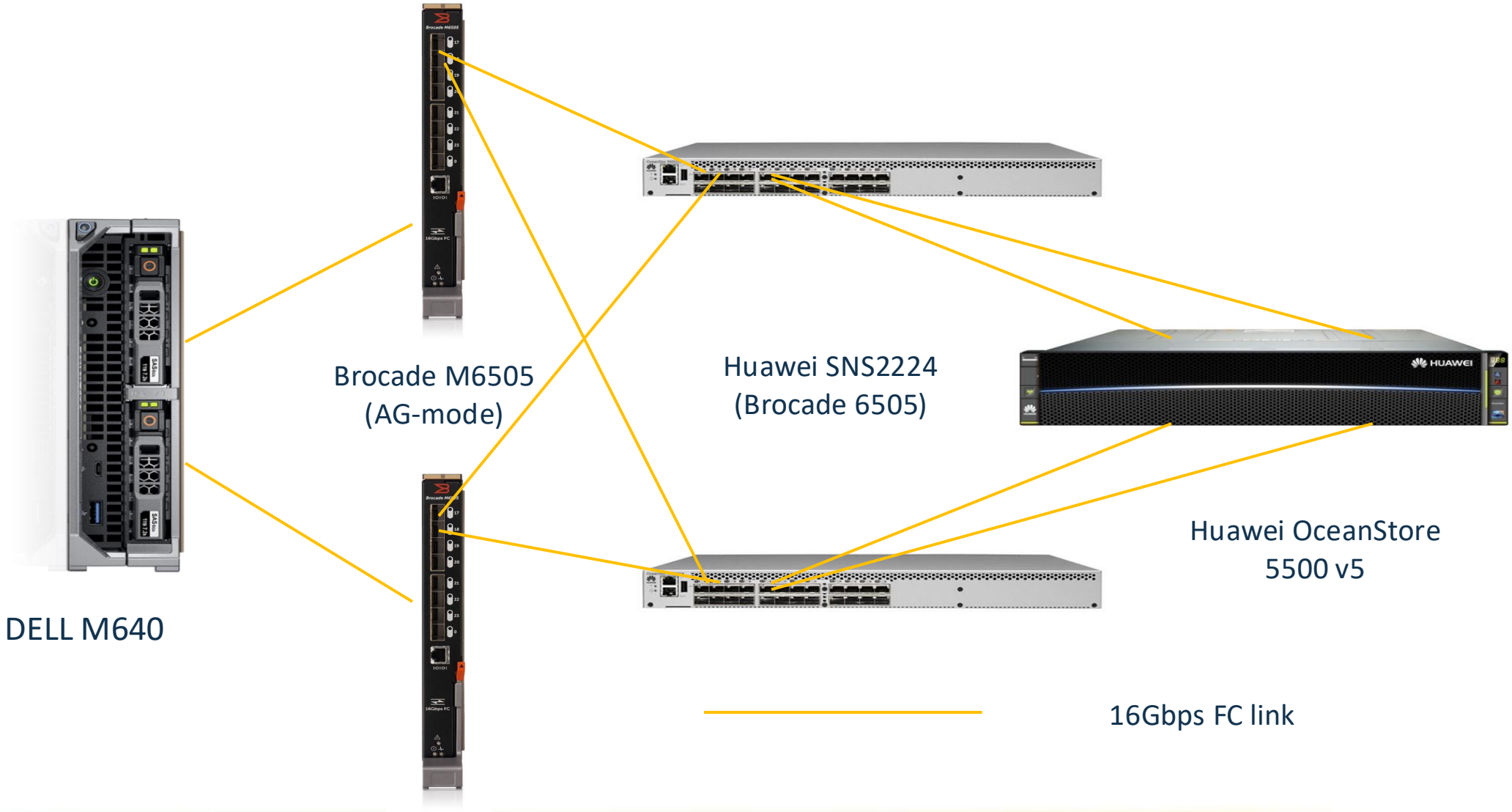
Connettività:

- 2 Fabric Engine MX 9116n
- 2 Fabric Expander Module MX7116n
- Uplink: 4x10GbE per FE
- SAN: 4x16/32Gbps FCoE per FE

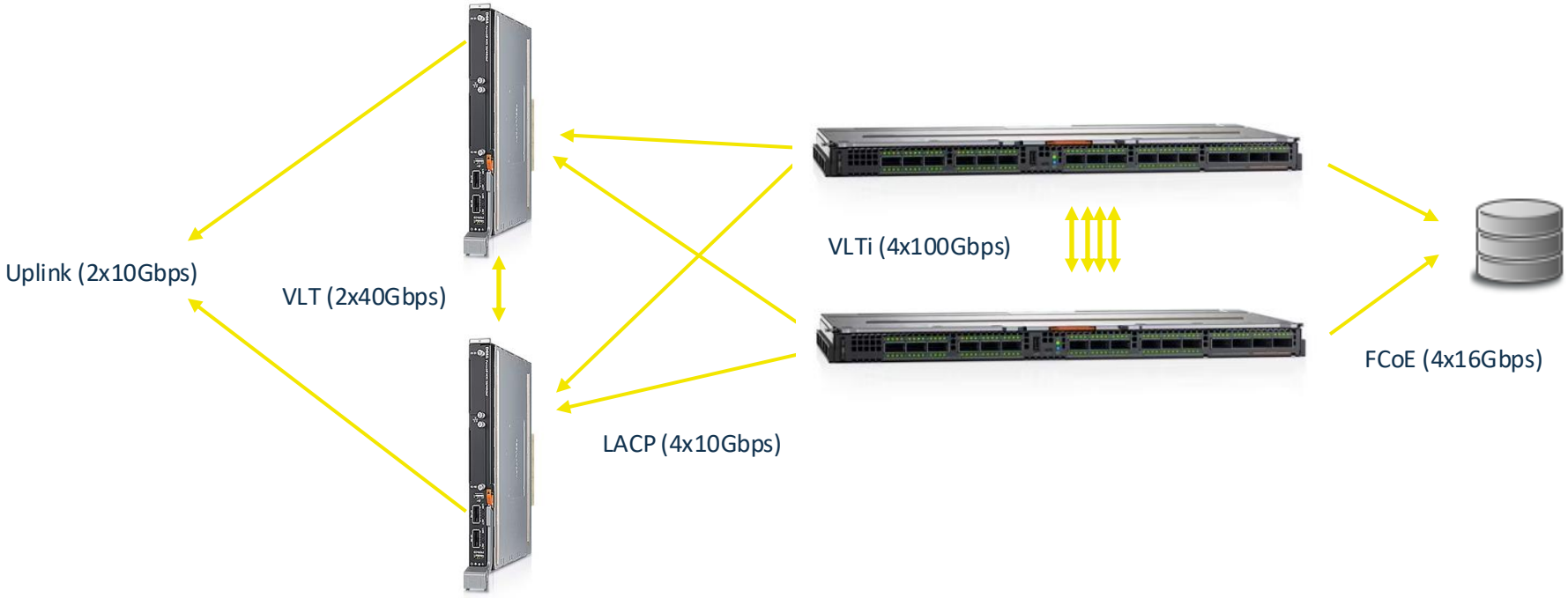
Hardware BC – LAN M1000e



Hardware BC – SAN M1000e



Hardware BC - MX



MX9116n configurati in modalità Fabric

Connettività SAN realizzata via FCoE

Uplink attualmente verso Force10 MXL 10/40, pianificata connettività diretta al gateway