WORKSHOP GARR 2026

NET MAKERS

Un anno di EduStorage

Fabio Farina

GARR

Le esigenze della comunità

Storage come servizio

- Indipendente dalle VM
- Object storage Ceph di GARR Cloud al limite

Autonomia e costi

- Meno lock-in
- Nessuna sorpresa sull'egress
- Pronti per GDPR e NIS2

Geo-resilienza

- Sopravvivere alla perdita di un sito
- Copie immutabili

Da dove nasce esigenze emerse dalla comunità, riprese nei documenti per il CTS e nel Piano Triennale

Né comprare né costruire: federare

COMPRARE

Hyperscaler

- Scala immediata, nessun investimento iniziale
- Sovranità delegata a provider extra-UE
- Costi imprevedibili, legati all'egress

LA TERZA VIA DELLE NREN

FEDERARE

Federazione NREN

- **Si cresce mettendo in comune le risorse**
- **I dati restano cifrati e sovrani**
- **Costi condivisi: nessuno li sostiene da solo**

COSTRUIRE

On-premise

- Pieno controllo e residenza dei dati
- Pochi possono permettersi la geo-ridondanza da soli
- DR e operatività su un solo ente

EduStorage federa l'infrastruttura, poi dati e servizi

Possedere l'hardware ≠ accedere ai dati

Gli enti mettono in comune dischi, siti e banda: i dati restano cifrati e sovrani

Identità federata, per tenant

WORKSHOP GARR 2026

NET MAKERS

Tre concetti, una tecnologia

CONCETTO	COSA SERVE	COME LO FA CUBBIT
Aggregazione software-defined dello storage	Unire dischi di enti diversi in un'unica risorsa, su hardware di ciascun ente	Swarm di Nexus · un agente per disco
Controllo di dove stanno i dati e con quale ridondanza	Decidere dove stanno i dati e quanto sono protetti	Classi di ridondanza
Cifratura e resilienza geografica	Nessun sito vede i dati; la perdita di un sito non li compromette	dati polverizzati e cifrati · EC geografico × locale

Prima i requisiti, poi la scelta tecnologica Cubbit è la tecnologia che realizza un'idea che avevamo già chiara

DS3 COMPOSER

The components, and the level each one sits at

LAYER 04

Orchestration

One control plane for every Swarm.

Composer

Configuration, topology and policy. Runs inside the Coordinator.

Coordinator

Data path, metadata and consensus. Optionally cloud-hosted.

LAYER 03

File services

POSIX-style access, layered on S3.

DittoFS file gateway

separate server

Sits on top of the S3 gateway. Can run remote, away from the storage sites.

LAYER 02

Access

How applications reach the data.

DS3 S3 gateway

S3-compatible endpoint. Authentication, tenancy and access enforcement.

DFS gateway

in development

Native file services in parallel to S3, for workloads that need them.

LAYER 01

Storage

Where the bytes actually live.

Storage node

Holds encrypted fragments on your disks. Serves reads and rebuilds.

Geo-distribution

Erasure-coded fragments spread across sites. Loss of a site loses no data.

Redundancy Class: Geographical and Local Resiliency

LAYER 1 — GEOGRAPHICAL EC

Across sites

Each object is split into data + parity shards, spread across independent sites.



Data + parity shards spread across sites — e.g. 1 per site

LAYER 2 — LOCAL EC

Inside one site

Within each site, a second EC layer protects data across its nodes and drives.

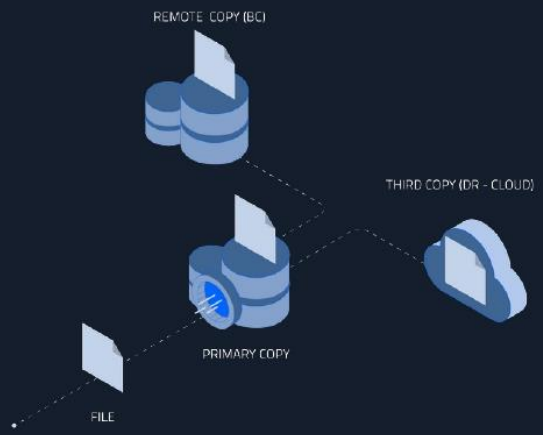


Shards spread across nodes and drives a drive or node can fail and rebuild locally.

A GEO-NATIVE PARADIGM

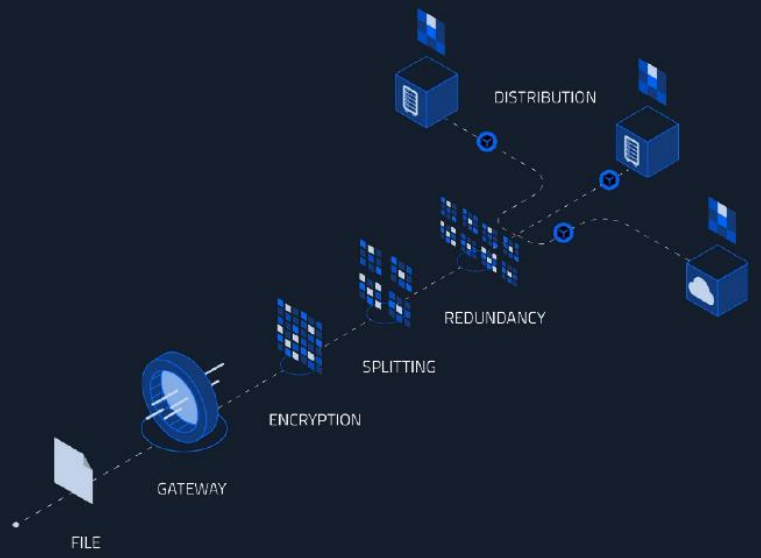
Not copies. Encrypted shards, distributed geo-natively.

TRADITIONAL GEO-REDUNDANCY



- ✕ Up to 4.5x Storage Footprint
- ✕ Up to 2.5x network traffic
- ✕ **3** data silos to manage

CUBBIT — GEO-NATIVE



- ✓ **Up to 1.8x storage footprint**
- ✓ **Up to 1.8 Network traffic**
- ✓ **1** global namespace · encryption at shard level

Secure. Resilient. Space-efficient. It's like RAID — but for your infrastructure, across sites.

FAILURE SCENARIO

Resiliency in action: 5 sites data protection

Geographical EC 3+2 across five sites, the same local EC 4+2 inside each one.



✓ **Object still reads**

SITES LOST	UNITS LOST PER SURVIVING SITE	READ
2 of 5	**2 of 6**	**succeed**

Dal fisico al tenant: uno Swarm, molti ProSumer

Internet — client S3 → **Proxy pair** — edge pubblico → **VRF EduStorage** — privata

DNS GARR · TLS HARICA — nomi e certificati

CONTROLLO per tenant	**Progetti** per gruppo di lavoro	**Bucket e policy** IAM · ACL · versioning	**Utenti e API key** per tenant	**Controllo delegato** al referente ProSumer
LOGICO tenant isolati	**Tenant GARR** 4 gateway S3	**Tenant UniBo** 2 gateway S3	**Tenant UniMiB** 2 gateway S3	**Nuovi tenant** per ogni ProSumer
CLASSI redundancy class	**ring-0-garr** GARR	**ring-1-unibo** UniBo	**classe dedicata** UniMiB	**più classi** sullo stesso Swarm
FISICO Composer	SWARM	**Nexus GARR** Palermo · Napoli · Bologna	**Nexus UniBo** Bologna	**Nexus UniMiB** Milano

Hardware condiviso, gestione separata

ATTIVO

Login federato: l’identità resta all’ente

LA CATENA

IdP IDEM
SAML istituzionale

→

Satosa
SAML → OIDC

→

Keycloak
claim aggiuntivi

→

Console EduStorage
login OIDC

COSA CAMBIA PER L’ENTE

Nessuna password custodita

GARR e Cubbit non gestiscono le credenziali degli utenti

MFA e policy restano all’ente

valgono le regole del proprio IdP

Solo il personale dell’ente

allowlist di dominio; account creato al primo accesso

Lato Cubbit IdP configurabile per tenant (SAML 2.0 / OIDC) · account creato al primo accesso, con la mail come chiave

A CHE PUNTO SIAMO

Automazione e visibilità

Sinergie di automazione

ATTIVO

Le catene di automazione GARR pilotano l'Ansible nativo di Cubbit per i nuovi siti

Inventario breve
nomi e IP · utente SSH · lsblk

→

GARR + Cubbit
playbook concatenati

→

Nexus in esercizio
storage · gateway · monitoraggio

NOVITÀ

Visibilità per ogni ProSumer

Dashboard di audit

Uso dello storage per progetto e tenant, per ogni ProSumer e per GARR

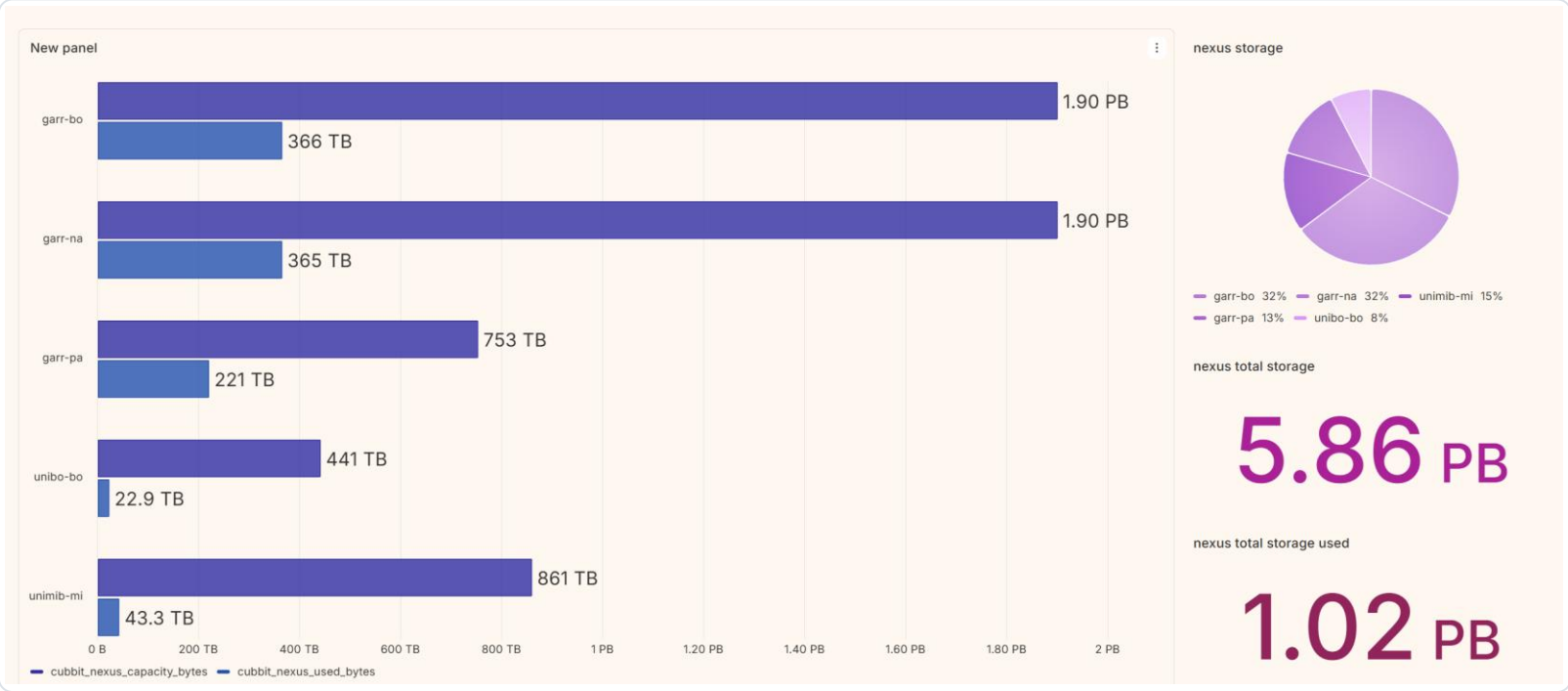
IN FINALIZZAZIONE

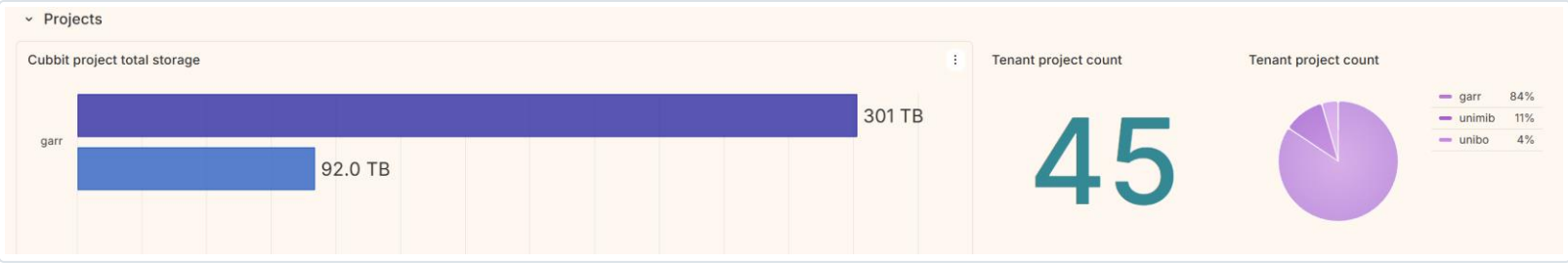
Logging centralizzato

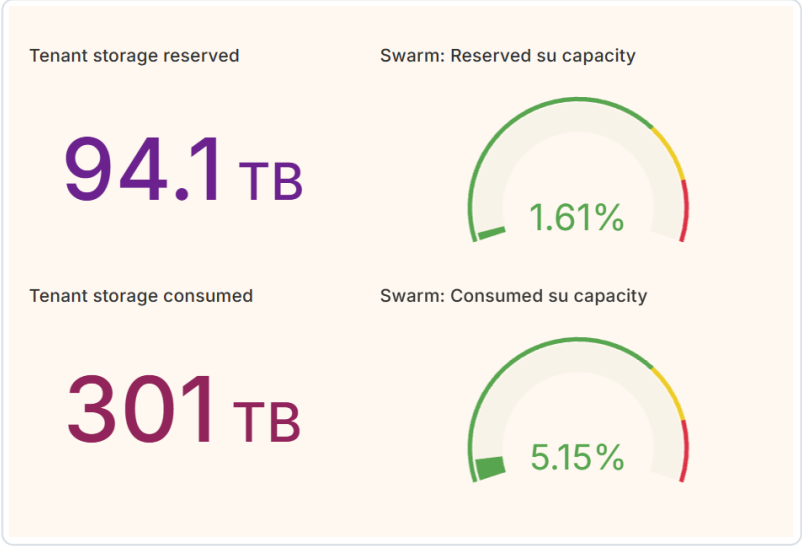
Log di gateway e nodi in un unico punto: troubleshooting più rapido tra i siti

IN IMPLEMENTAZIONE

La dashboard di EduStorage







COSA MOSTRA

- Capacità e uso per Nexus
- Spazio riservato e consumato per tenant
- Progetti per tenant

A CHE PUNTO SIAMO

I numeri di EduStorage

CAPACITÀ RAW OGGI

5,86 PB

da 3,56 PB · +4 server GARR

1,02 PB usati · 45 progetti
GARR 84% · UniMiB 11% · UniBo 4%

302 TB di dati nel tenant GARR
throughput 671 vs 375 MiB/s su Ceph (≈ 1,8×)

- **GARR** — Palermo · Napoli · Bologna · 13 nodi — **4,56 PB** — ATTIVO
- **Università di Bologna** — primo ProSumer — **441 TB** — ATTIVO
- **Università di Milano-Bicocca** — ProSumer · nuovo hardware — **861 TB** — ATTIVO
- **3 organizzazioni** — in ingresso — ONBOARDING
- **Altri atenei ed enti** — manifestazioni di interesse

EduStorage al lavoro: i casi d'uso GARR

I CARICHI GRANDI

Telemetria di rete, osservabilità e log



≈ 144,8 TB

Backup



≈ 118,9 TB

CRESCITA MEDIA

0,57 TB/g
giorni feriali

0,33 TB/g
weekend

MOLTI CARICHI DIVERSI

AI: hosting di modelli

1,85 TB

→ **F. Lombardo** mer 4/11 · AI

Sensing delle fibre

467 GB · primo Consumer puro

→ **P. Bolletta** a seguire

Sicurezza e servizi verticali

≈ 8 GB · analisi VA/PT

→ **L. Fava** mer 4/11 · Sicurezza

Totale ≈ 266 TB · dati al 26/10 · progetti di test personali esclusi

Diventare ProSumer

Questa fase si concentra esclusivamente sui ProSumer: chi conferisce hardware usa capacità. I Consumer arriveranno in seguito.

PERCHÉ ADERIRE

Storage geo-distribuito
federato, oltre il proprio data center

Valore all'hardware
server e dischi non pienamente utilizzati

Ruolo nella governance
tecnica e nell'evoluzione del progetto

Più controllo sui dati
ridondanza, accesso e gestione

IL PROSUMER

Conferisce un Nexus locale
e usa la capacità della federazione

Regola: chi mette risorse usa risorse, in proporzione a quota e classe

→

COSA CI METTE GARR

Nexus fondatore e federatore neutrale

DNS e certificati TLS
gestiti da GARR

Componenti distribuite
le prime, operate da GARR

Attivazione automatizzata
dei nuovi siti

Classi di ridondanza e requisiti essenziali

In ogni sito EC locale almeno 4+2: tollera 2 dischi su nodi diversi oppure un nodo intero

BASE

Copie secondarie, DR, lungo termine

1 sito · nessun sito perso tollerato

Su 500 TB raw: **≈ 330 TB netti** (1,5 : 1)

RAFFORZATO

Backup primari, dataset costosi da rigenerare

3 siti, geo 2+1 · tollera 1 sito

Su 500 TB raw: **≈ 220 TB netti** (2,25 : 1)

MASSIMA PROTEZIONE

Dati critici, ricerca attiva, output HPC

6 siti, geo 4+2 · tollera 2 siti

Su 500 TB raw: **≈ 220 TB netti** (2,25 : 1)

GARR è più ridondante: 3 siti, geo 2+1, EC locale 10+4 · la classe si sceglie in onboarding; cambiarla significa un nuovo tenant

REQUISITI ESSENZIALI

Server e dischi

≥ 3 server bare metal per sito · 12–36 HDD per nodo, in JBOD · da 500 TB a 2 PB raw

Adiacenza PoP GARR

uplink verso la rete GARR 2×10 GbE

VRF dedicata

in DMZ, con indirizzamento privato fornito da GARR

Il percorso di adesione e chi fa cosa

1 → **Contatto**
manifestazione di interesse

2 → **Analisi**
capacità, classe di ridondanza, rete

3 → **Predisposizione**
server, VRF dedicata, Ubuntu 24.04

4 → **Deploy**
automatizzato, da un inventario breve

5 → **In esercizio**
tenant, login IDEM, dashboard

CHI FA COSA

In arrivo audit e logging centralizzati

L1 Referenti dell'ente
nodo, accessi, utenze, quote e configurazioni locali

L2 GARR
ciclo di vita della federazione, adesioni, variazioni del pool, disconnessioni

L3 Cubbit e GARR
aggiornamenti critici, bachi bloccanti, escalation sistemiche

Impegni di permanenza: perché servono

IL MOTIVO: IL RIBILANCIAMENTO

Sui dischi di ogni ProSumer ci sono frammenti dei dati di tutta la federazione.

Un'uscita senza preavviso abbassa la ridondanza per tutti.

Il preavviso dà il tempo di ribilanciare i frammenti sugli altri siti, senza esporre i dati.

24

mesi

Permanenza minima

nodi in federazione per almeno 24 mesi, con manutenzione hardware (NBD)

6

mesi

Preavviso di uscita

per la disconnessione programmata: il tempo di ribilanciare i dati senza ridurre la protezione

Lezioni apprese e prossimi obiettivi

Cosa abbiamo imparato

- **Ruoli privacy da affinare**
  quando i dati non passano dai nodi GARR
- **Scritture con un sito giù**
  comportamento da confermare: in valutazione il 3+1
- **DR del Coordinator**
  da valutare: RPO non nullo
- **Onboarding e competenze**
  percorso di formazione in preparazione

Prossimi obiettivi

- Federare le risorse degli atenei pilota e accogliere nuove organizzazioni
- Backup remoto e DR come building block
- Archivio immutabile e backup immutabile con copia indipendente
- Consolidamento nazionale
- Servizi verticali, es. GARRbox
- Pilota multi-NREN

Come partecipare

CHI PUÒ ADERIRE OGGI

Università ed enti di ricerca

- Connessi alla rete GARR
- ≥ 500 TB raw su ≥ 3 server
- Referenti locali per il livello L1

CONSUMER: NELLA FASE SUCCESSIVA

1 **Scriveteci**
risorse e casi d'uso

→

2 **Analisi congiunta**
capacità, classe, rete

→

3 **Onboarding**
formazione, fino all'esercizio

PUNTI IMPORTANTI

I tempi dell'adesione dipendono soprattutto da

Hardware
gara di acquisizione e tempi di fornitura

Rete in DMZ
studio e predisposizione della VRF dedicata

Decisioni interne
negoziazione e approvazioni nell'ente

WORKSHOP GARR 2026

NET MAKERS

Grazie

edustorage@garr.it
Fabio Farina · GARR

Backup · Requisiti tecnici completi

Server e dischi

- ≥ 3 server bare metal omogenei per sito
- 12–36 HDD per nodo, JBOD senza RAID
- ≥ 80 IOPS e 150 MB/s per disco
- 1 vCore + 2 GB RAM per disco
- Gateway: 4 vCore + 4 GB per 1 Gbps

Rete

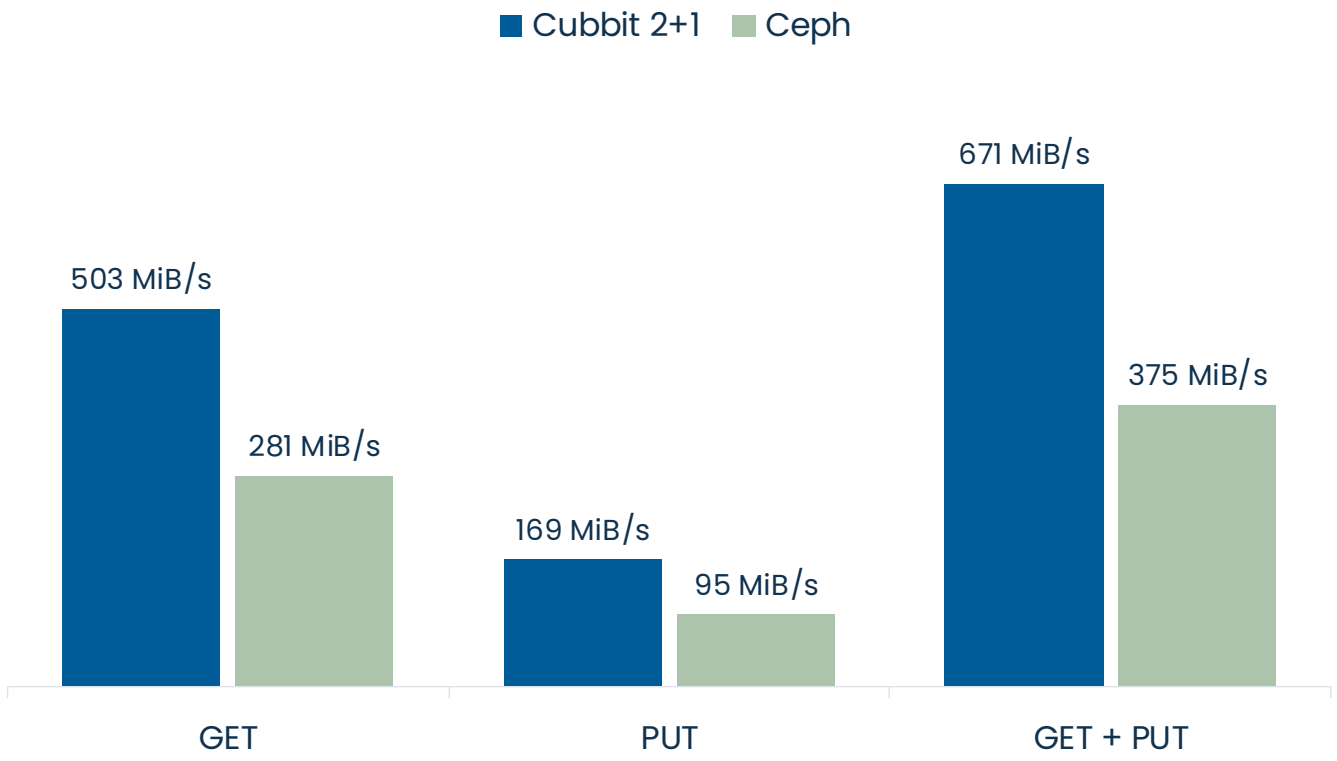
- 2 NIC in bonding
- 10 GbE locale (meglio 25 GbE)
- Uplink GARR ≈ 2×10 GbE, ridondato
- VRF dedicata in DMZ, indirizzi privati da GARR
- RTT ≤ 10 ms verso il Coordinator per file piccoli

Sistema e sicurezza

- Ubuntu 24.04 LTS su dischi OS separati
- TLS ≥ 1.2
- SSH con chiavi / MFA
- Firewall limitato alle porte necessarie
- Continuità del sito

Backup · Benchmark Cubbit DS3 vs Ceph GARR Cloud

Throughput · MiB/s, più alto è meglio



Latenza media

secondi per oggetto da 100 MiB, più basso è meglio

GET

5,3 s vs 10,3 s Ceph

PUT

2,9 s vs 3,1 s Ceph

MinIO Warp · 32 client concorrenti
oggetti da 100 MiB
run migliore 748 MiB/s