

Una Federazione di Storage S3?

M. Carboni

Costruzione di una infrastruttura condivisa

29/05/2025



BY

Outline

- 1 Esigenza
- 2 Attività
- 3 Tecnologia
- 4 Considerazioni

Esigenza



- ➡ Il vero storage si vede quando lo storage smette di funzionare
- ➡ (**no HTStorage**) Non stiamo cercando un sistema ad alte prestazioni
- ➡ Andare oltre **CEPH** e **MinIO**, che funziona nel sito, nel multi-sito
 - ➡ funzionamento non rispondente alle nostre esigenze

Perchè una federazione di Storage

I vantaggi di una soluzione storage basata sulla federazione di risorse geograficamente distribuite, ma basate su un approccio tecnologico comune, come l'accesso a oggetti (s3), sono molteplici. Le principali individuate sono:

- ➡ Ottimizzazione delle Risorse
- ➡ Scalabilità e Flessibilità
- ➡ Facilità di Accesso ai Dati
- ➡ Sicurezza e Conformità
- ➡ Riduzione dei Costi
- ➡ Supporto alla Collaborazione e alla Ricerca Condivisa
- ➡ Resilienza e Continuità Operativa
- ➡ Integrazione con Infrastrutture di Calcolo Distribuite
- ➡ Possibilità di Innovazione e Sperimentazione

Possibili Beneficiari

- ➡ Sistemi Informativi di Ateneo, per gli *obblighi di tutela dei dati*
- ➡ Gruppi Scientifici
 - ➡ Non metterei i **RAW data** di un esperimento come LHC
- ➡ Possono ospitare l'accesso ai dati FAIR

Interesse da parte della comunità

- ➡ Interesse “sparso” da parte degli Enti GARR a costruire un modello di mutuo “supporto”, Continuità Operativa, Disaster Recovery, ecc.
- ➡ Come GARR abbiamo presentato l’idea al gruppo ICT della CRUI che ha portato alla formalizzazione dell’esigenza

Interesse da parte della comunità

- ➡ Interesse “sparso” da parte degli Enti GARR a costruire un modello di mutuo “supporto”, Continuità Operativa, Disaster Recovery, ecc.
- ➡ Come GARR abbiamo presentato l’idea al gruppo ICT della CRUI che ha portato alla formalizzazione dell’esigenza
- ➡ Tra gli obiettivi:
 - ➡ **Autonomia Digitale:** *dati scientifici su provider commerciali*
 - ➡ **Ridurre la Delega** alla gestione a soggetti terzi garantendo la **Localizzazione fisica** dei dati
 - ➡ **Gestione a Norma (ACN)** limitata ai soli dati **ordinari** e **critici**
 - ➡ no dati **strategici**

Interesse da parte della comunità

- ➡ Interesse “sparso” da parte degli Enti GARR a costruire un modello di mutuo “supporto”, Continuità Operativa, Disaster Recovery, ecc.
- ➡ Come GARR abbiamo presentato l’idea al gruppo ICT della CRUI che ha portato alla formalizzazione dell’esigenza
- ➡ Tra gli obiettivi:
 - ➡ **Autonomia Digitale:** *dati scientifici su provider commerciali*
 - ➡ **Ridurre la Delega** alla gestione a soggetti terzi garantendo la **Localizzazione fisica** dei dati
 - ➡ **Gestione a Norma (ACN)** limitata ai soli dati **ordinari** e **critici**
 - ➡ no dati **strategici**

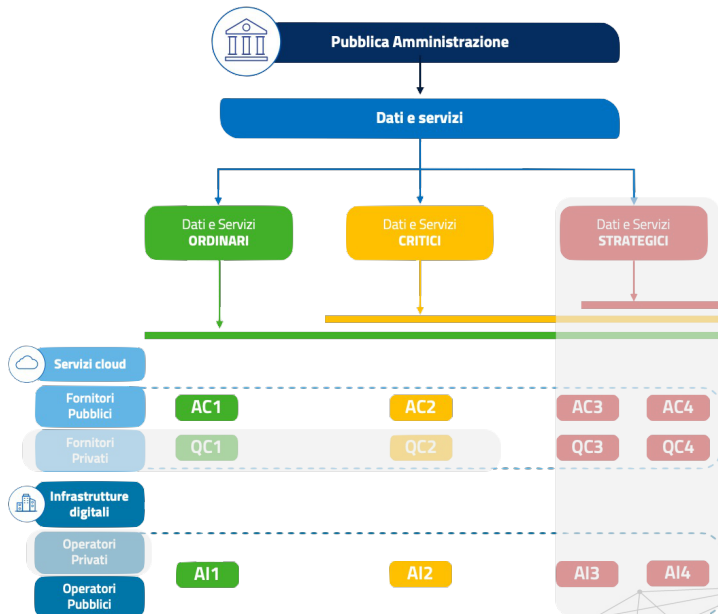
Rischio

Mettere tutti i dati nella medesima infrastruttura

Sintesi del Regolamento Unico Cloud per la PA

- ➡ Definisce:
 - ➡ Modalità per **classificazione**, **migrazione** e **qualificazione** dei servizi cloud per la PA.
 - ➡ Requisiti minimi per **sicurezza**, **capacità elaborativa**, **risparmio energetico** e **affidabilità**.
 - ➡ Caratteristiche di **qualità**, **performance**, **scalabilità**, **sicurezza** e **portabilità**.
- ➡ Decreto Direttoriale n. 21007/24 - **valido dal 1 agosto 2024**.
- ➡ Regola anche infrastrutture di **housing** e servizi **edge**.

Classificazione Dati e Servizi



Soggetti con hanno mostrato Interesse

- ➡ **Università di Bologna**
- ➡ Istituto Nazionale di Astrofisica - INAF
- ➡ **Università degli Studi di Milano-Bicocca**
- ➡ Libera Università di Bolzano
- ➡ Scuola Superiore Sant'Anna di Pisa
- ➡ Università di Trento
- ➡ Politecnico di Torino

Attività



Obiettivo

- ➡ Creare un servizio federato di Object Storage conforme alle normative
- ➡ Basato sul protocollo **S3**
- ➡ Supportato e Gestito insieme agli enti (Università e Centri di Ricerca)
- ➡ In grado di Garantire autonomia digitale, sicurezza e riduzione della dipendenza da cloud commerciali

Requisiti per un servizio di storage I

Caratteristiche del Servizio

- ➡ **Disponibile:** del dato anche in caso di malfunzionamento di una o più parti. In grado di gestire anche la mancanza di un intero sito
- ➡ **Affidabile:** in caso di fallimento di una o più componenti secondo le metologie RAID o equivalenti
- ➡ **Resiliente:** Geografica, in quanto quella locale non è sufficiente

Controllo agli Utenti

- ➡ **Gestione:** in grado di garantire livelli di delega su base Organizzazione, Tenant, ecc.
- ➡ **Multi Organizzazione:** in grado di fornire “risorse” e gestione delle stesse su base organizzazione con deleghe gerarchiche
- ➡ **Multi Tenant:** supportare la creazione di contesti funzionali indipendenti con livelli di ridondanza indipendenti su base sito

Requisiti per un servizio di storage II

- ➔ **Multi Utente:** a tutti i livelli sia di gestione che utilizzo, anche garantendo la gestione di gruppi sia almeno su base TENANT
- ➔ **Sicura:** dell'infrastruttura, dei dati, ma anche dell'accesso (es. RANSOMWARE) copia immutabile

Noto ed estendibile

- ➔ **Scalabile:** in grado di crescere da **pochi PB** fino a poter arrivare a **100PB+**, e di fornire una prestazione in linea con la crescita del volume dati
- ➔ **Federabile o Federata:** è necessario definire il livello della federazione:
 - ➔ Identità, Risorse, Altro?
- ➔ **API Based:** l'interfaccia di accesso ai dati oltre che essere "WEB-Based" deve garantire un accesso secondo gli Standard S3 attraverso coppie di chiavi (API Keys) da associare ad un connettore S3

Requisiti per un servizio di storage III

Compromesso Costi/Benefici

- ➡ **Sostenibile:** la spesa connessa (**TCO**) con questo tipo di soluzione deve essere almeno equivalente alle soluzioni di mercato alle quali si potrà aggiungere il valore della gestione "In House"
- ➡ **Autonomia Digitale:** nel conto economico vanno anche considerati il valore che la gestione diretta dei dati garantisce

Caratteristiche

del modello Implementativo

- ➡ Architettura **on-premise federata**
- ➡ Controllo locale su backup, geo-replica e sicurezza
- ➡ Accesso tramite **protocollo S3**
- ➡ Gestione policy con **identità federata**
- ➡ Supporto a data lake, archiviazione, analisi, aree collaborative

del modello Organizzativo

- ➡ **Modello PROSUMER**: ogni partecipante è produttore e consumatore
- ➡ **GARR**: coordinamento tecnico e infrastruttura
- ➡ **Comitato di indirizzo**: CRUI, GARR, rappresentanti PROSUMER

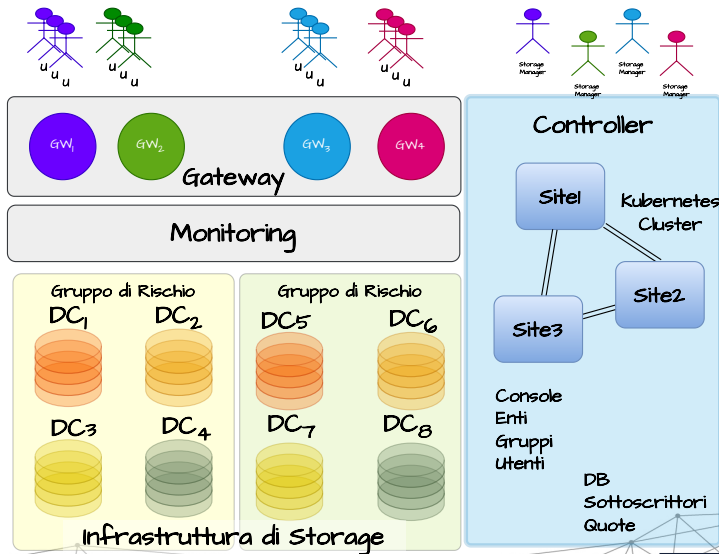
Sperimentazione Tecnologica

- ➡ Pilota avviato a febbraio 2025 con 2x750 TB da GARR, corrispondenti a due siti distinti
- ➡ Obiettivo: avere almeno 2 PB iniziali
- ➡ Tecnologie valutate: MinIO, Ceph, Dell ECS, Cloudian, Cubbit

A valle delle azioni preliminari verranno integrate le risorse dell'Università di Milano Bicocca e dell'Università di Bologna

HL Architecture

- ➡ Orchestratore e federazione delle risorse
- ➡ sicurezza e ridondanza con “polverizzazione” e cifratura



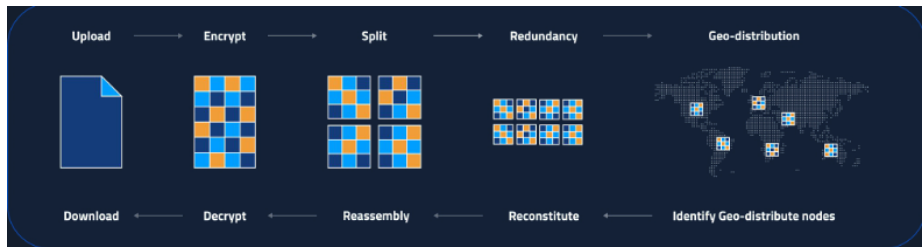
Tecnologia



DS3: Cambiamento del Paradigma Funzionale

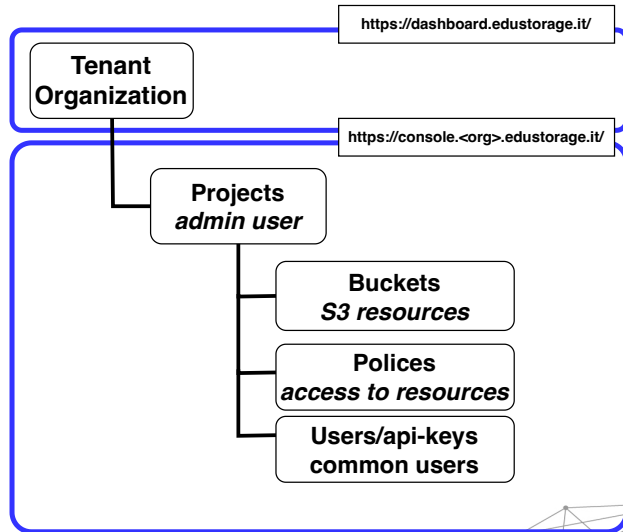
**Sicuro,
Resiliente,
Conveniente**

- ➡ **DS3** è l'acronimo di **Distributed S3**. Un'innovativa soluzione di archiviazione compatibile con S3
- ➡ Invece di memorizzare i dati in un'unica posizione, i dati vengono crittografati, suddivisi in frammenti, ridondanti e distribuiti in una rete geo-distribuita, garantendo ai clienti pieno controllo e proprietà dei propri dati



Tenant e swarm

- ➡ L'Organizzazione e il monitoraggio dell'utilizzo di spazio è demandata ai Tenant
- ➡ dashboard per le organizzazioni (resellers) e console per gli utilizzatori finali (utenze, client, etc.)
- ➡ Uno user può avere più progetti



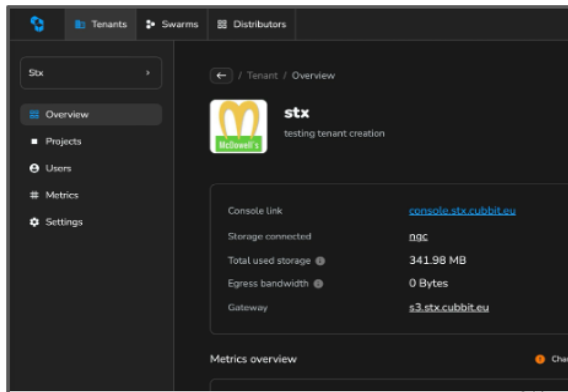
Dashboard

<https://dashboard.edustorage.it/>

Tenant Organization

Dashboard consente di:

- ➡ Legare il tenant (e tutti i suoi progetti), ad uno (ed un solo) storage/sciame specifico
- ➡ Creare nuove utenze admin
- ➡ Monitorare/fatturare il consumo di storage/sciame specifico



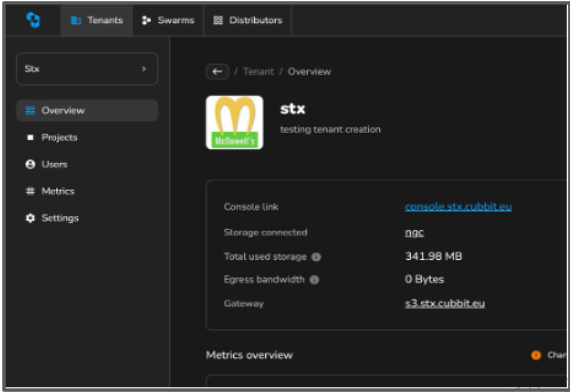
Console

Console consente di:

- ➡ Creare bucket
- ➡ Creare nuove utenze/api-keys
- ➡ Gestire permessi di accesso

<https://console.<org>.edustorage.it/>

Projects
admin user

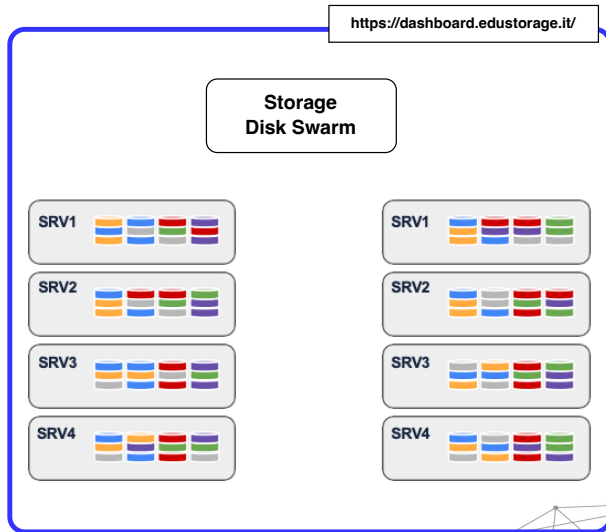


The screenshot displays the STX console interface. At the top, there are tabs for 'Tenants', 'Swarms', and 'Distributors'. The 'Tenants' tab is active, showing a list of tenants. The selected tenant is 'stx', which has a logo featuring a yellow 'M' and the text 'stx testing tenant creation'. Below the tenant name, there is a table with the following data:

Console link	console.stx.cubbit.eu
Storage connected	ngc
Total used storage	341.98 MB
Egress bandwidth	0 Bytes
Gateway	s3.stx.cubbit.eu

At the bottom of the console, there is a 'Metrics overview' section with a 'Chart' button.

- ➡ Swarm permette di federare più risorse distribuite



- ➡ Swarm permette di federare più risorse distribuite.

<https://dashboard.edustorage.it/>

Storage Disk Swarm

The screenshot shows a web interface for 'Storage Disk Swarm'. On the left is a sidebar with a menu: 'Demo1', 'Panoramica', 'Nexus' (selected), 'Classi di ridondanza', 'Fornitori', and 'Impostazioni'. The main content area has a breadcrumb trail: '/ Swarm / Nexus / Nodi / Crea Nodi in blocco'. Below this is the title 'Crea nodi in blocco' and a description: 'Creare ora i nodi in blocco, con un nodo per disco per server. Ogni server deve avere lo stesso numero di nodi coerente.' There are two input fields: 'Numero di server' with a value of 12 and 'Numero di dischi per server' with a value of 12. Below these is a 'Provider' section with a text description: 'Scegli un provider di archiviazione che sarà responsabile della gestione di questo nodo. Un provider di archiviazione è un'entità fisica che ha uno o più nodi in gestione. Se intendi eseguire un nodo da solo, non è necessario modificare questo parametro. Se, d'altra parte, stai lanciando un nodo per conto di un provider di terza parte, selezionalo'.

<https://dashboard.edustorage.it/>

Storage Disk Swarm

➡ Decide dei livelli di ridondanza

Classe di ridondanza

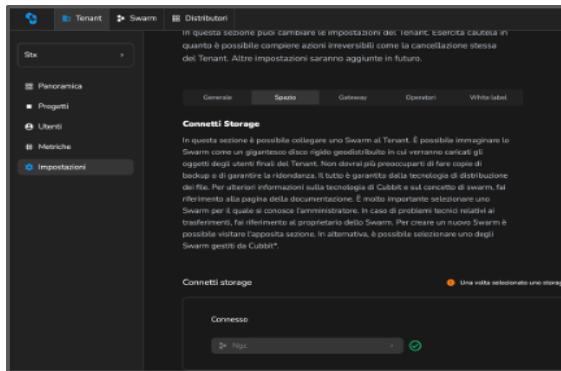
Una classe di ridondanza è una policy di protezione dei dati altamente strutturata e specializzata definita da una quintupla unica di parametri. Questi parametri sono progettati specificamente per ottimizzare la resilienza della rete e l'integrità dei dati nei sistemi distribuiti che utilizzano il modello di correzione degli errori Reed-Solomon.

default	
Default redundancy class	
Livello del Nexus	2 + 1
A livello Ring	12 + 4 + 4
Dimensione Ring	0 Bytes
Fattore di ridondanza	x2

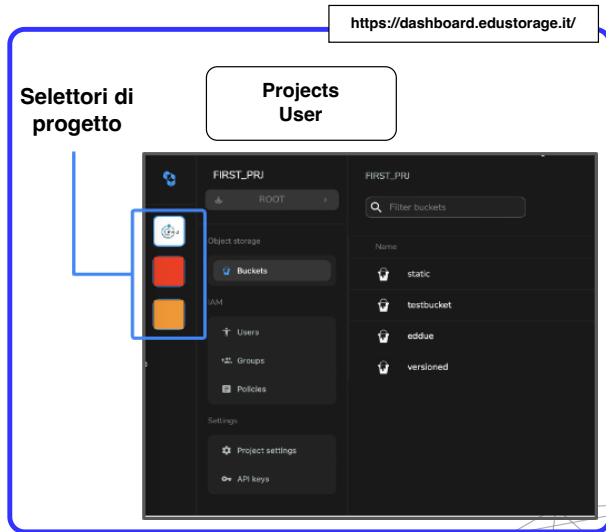
- ➡ Un tenant è connesso ad uno storage/swarm specifico

<https://dashboard.edustorage.it/>

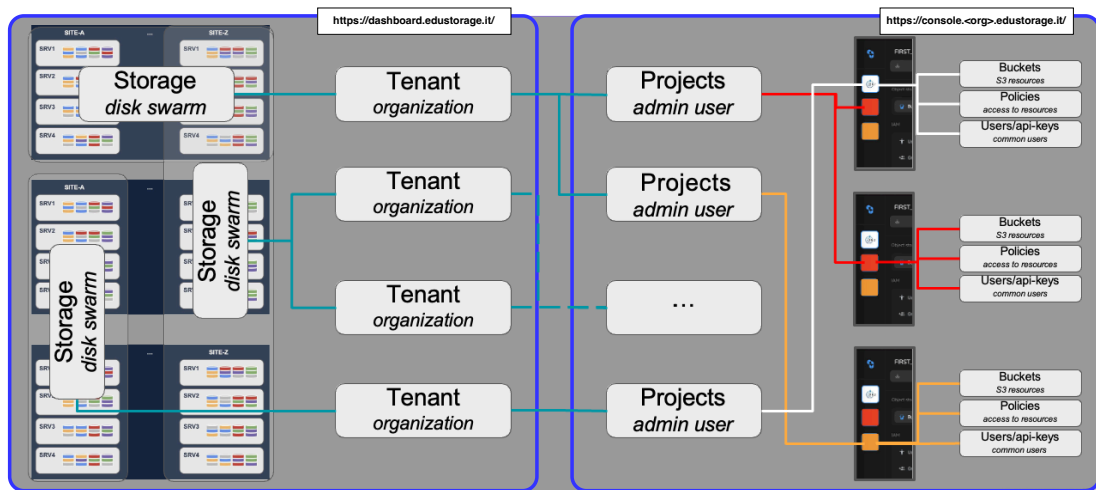
Tenant Organization



- ➡ Un'utenza può avere in console progetti da uno o più tenant



Compressivamente



Roadmap

➡ Fase1: Q1-**Q2** 2025

- ➡ Avvio del progetto pilota in collaborazione con università e centri di ricerca e implementazione della rete in **Gennaio 2025**
- ➡ definizione LLD della componente **GARR Coordinator** da mettere in funzione di HA su 3 siti distinti
- ➡ Definizione dei requisiti di partecipazione alla federazione: caratterizzazione dell'infrastruttura di storage
- ➡ Attività di onboarding dei sistemi di storage (6 server) presenti nei siti di Bologna e di Torino
- ➡ valutazione dei diversi scenari di malfunzionamento (perdita di un sito, nodo, ecc.)
- ➡ prototipare il modello di autenticazione mista, IDEM + homeless

➡ Fase2: Q2-**Q3** 2025

- ➡ Espansione verso altre università e finalizzazione del modello operativo per il sistema a regime
- ➡ Costruzione del sistema di monitoring dell'infrastruttura: Coordinator e Sistemi Storage
- ➡ Definire i modelli di migrazione dati per temporanea disconnessione o per il rilascio delle risorse

➡ Fase3: Q3-Q4 2025, **Q1 2026**

- ➡ Implementazione operativa della rete federata secondo il modello definitivo.

Considerazioni



Federazione

Questioni Aperte, necessità di Contributi

- ➡ modelli hardware supportati, interlocuzione con CRUI
- ➡ modello di accesso alla rete
- ➡ modello economico e scalabilità con Cubbit
- ➡ processi di federazione, ingresso di un partner prosumer
- ➡ espansione e riduzione delle risorse
- ➡ distacco regolamentato
- ➡ gestione degli incidenti e della sicurezza
- ➡ modello di supporto utenti e secondo livello
- ➡ monitoraggio e notifiche alert



Si accettano contributi



Si accettano contributi

This work is licensed under a Creative Commons “Attribution 4.0 International” license.



Strumenti OpenSource

$\text{\LaTeX}$ - Draw.IO - GNU.Makefile

Abstract

- ➡ In questo intervento presenteremo la proposta di un nuovo servizio comunitario.
- ➡ Il progetto di Federazione Storage S3 mira a creare un servizio di storage federato qualificato ACN basato sul protocollo S3, gestito da Università e Centri di Ricerca. Questo servizio offrirà un controllo completo sui dati, riducendo la latenza di accesso e migliorando la sicurezza e la continuità del servizio. La proposta include un modello collaborativo e un'architettura on-premise federata, con l'obiettivo di garantire l'autonomia digitale e ridurre la dipendenza dai cloud provider commerciali.
- ➡ Nell'intervento descriveremo i requisiti sul servizio, gli obiettivi della fase pilota in corso e le azioni che stiamo intraprendendo con CRUI per rendere il servizio sostenibile.