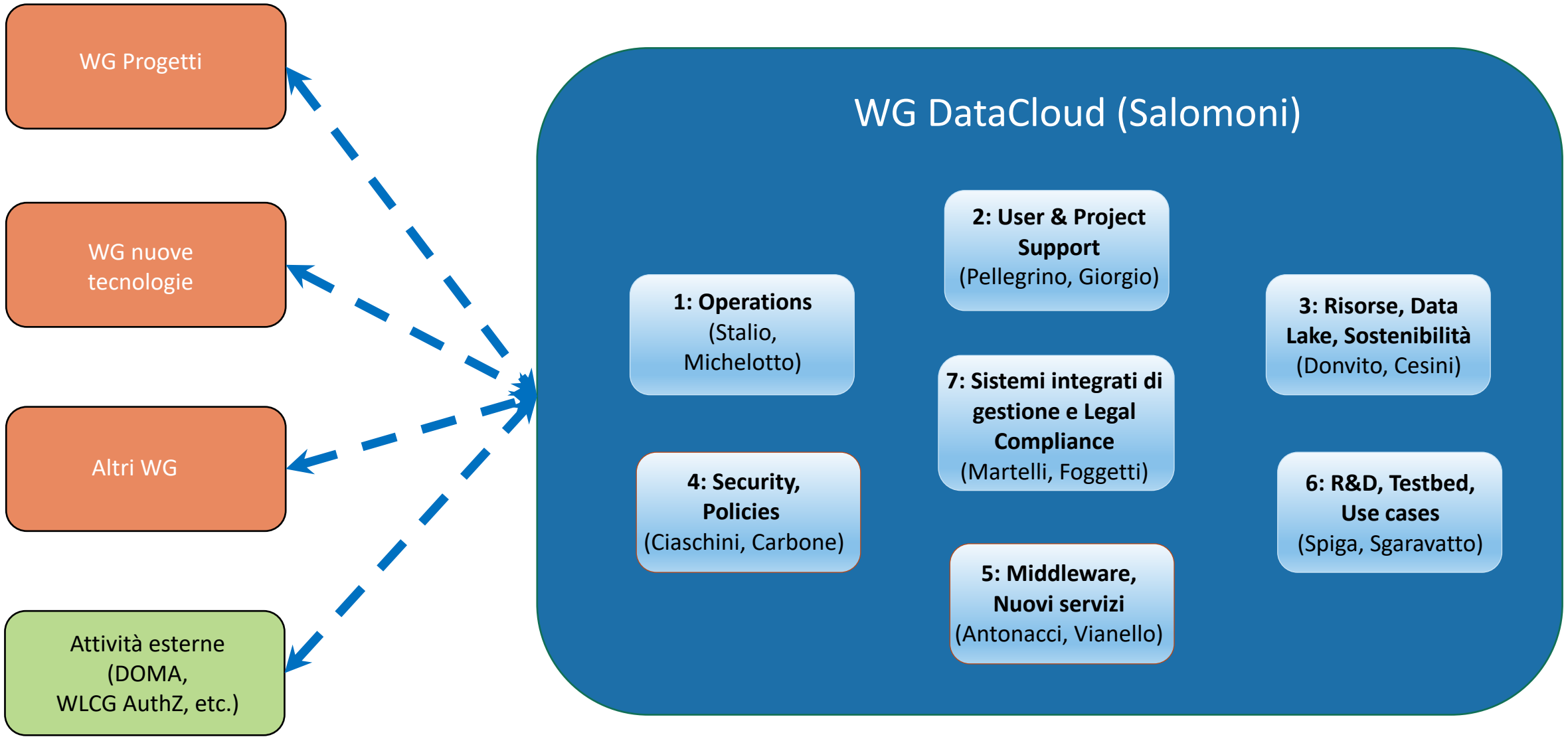
Integrazione in DataCloud delle nuove risorse ed evoluzione dei servizi connessi

Giacinto Donvito
On behalf of “DataCloud team”
23/5/2023

La struttura del WG DataCloud



Le attività dei progetti PNRR (e non solo) e i WPs Data Cloud

- **Tutte le attività legate anche ad iniziative esterne (PNRR, EU, Nazionali) devono sempre trovare una collocazione/riferimento nei WP di Data Cloud**
  - Le operation del ICSC e TERABIT ➔ **WP1**
  - Lo user support delle nuove comunità di utenti di ICSC ➔ **WP2**
  - Il planning dell'allocazione delle risorse (IT e personale) ➔ discusso nel contesto di **WP3**
    - È già partita una attività di pianificazione, di concerto con i responsabili locali delle varie sedi, per ottimizzare la distribuzione delle nuove persone sulle vari attività in corso e necessarie per l'infrastruttura distribuita DataCloud
  - La security e il supporto a use case con dati sensibili, i problemi per l'accesso alle risorse da persone esterne a INFN ➔ **WP4/WP7**
  - Le attività di R&D per l'implementazione di nuovi servizi, use case dei progetti, sviluppo/supporto middleware ➔ **WP5/WP6**

DataCloud-related contributions

- Developing an automated ATLAS analysis workflow on the INFN Cloud facility (Caterina Marcon), 22/5
- Esperienza di un'analisi dati CMS nell'INFN "Analysis Facility" framework (Tommaso Diotalevi), 22/5
- evoluzione datacenter INFN attraverso le gare (Daniele Cesini), 23/5
- integrazione in datacloud delle nuove risorse ed evoluzione dei servizi connessi (Giacinto Donvito), 23/5
- requisiti da parte delle comunità mediche e life science e loro impatto sull'infrastruttura distribuita (Barbara Martelli), 23/5
- Deployment dell'ambiente di calcolo per ML-INFN su INFN Cloud sfruttando le GPU (eventualmente partizionate) (Gioacchino Vino), 23/5
- Evoluzione e utilizzo della PaaS nell'infrastruttura distribuita INFN Cloud: focus sui nuovi sviluppi e servizi per gli utenti (Marica Antonacci), 23/5
- Dynamic K8S for HPC Applications on Cloud (Ahmad Alkhansa), 23/5
- S3 Storage Accessed Via POSIX: a CEPH-STS Solution Provided For Research Communities (Ahmad Alkhansa), 23/5
- Il progetto interTwin e le sue sinergie tecnologiche per l'INFN (Daniele Spiga), 23/5
- Federare lo storage distribuito nazionale: la prima esperienza in Datacloud verso il DataLake (Diego Ciangottini), 23/5 + Demo 24/5
- INDIGO-IAM: sviluppi futuri e federazioni OIDC (Roberta Miccoli), 23/5
- Un approccio RESTful per la gestione di file richiamati da tape in StoRM (Federica Agostini), 23/5
- Democratizzare la distribuzione del software: un pilot basato su CVMFS e storage a oggetti (Giada Malatesta), Demo 24/5
- A Block Chain based Distributed App (DApp) for GDPR informed consent management (Ana Velimirovic), Demo 24/5
- Monitoring and Accounting on DATA Cloud infrastructure (Alessandro Pascolini), Demo 24/5
- Matlab as a Service su INFN Cloud (Federico Fornari), Demo 24/5
- IAM as a Service su INFN Cloud (Federico Fornari), Demo 24/5
- Cyber security EU legal Framework and the open-source scenario (Nadina Foggetti), 25/5
- Gestione delle vulnerabilità nella rete INFN e test di Greenbone Enterprise TERA (Cristian Greco), 25/5
- Il SOC dell'INFN: fare tesoro delle esperienze locali per costruire un SOC nazionale - Endpoint Detection and Response all'INFN (Gianluca Peco), 25/5
- Supporto ad utenti e progetti in INFN Cloud e loro casi d'uso (Francesco Sinisi), 26/5
- MATLAB as a Service su INFN Cloud (Federico Fornari), 26/5

Operation status & activities

- Gestione dell'infrastruttura del «Backbone» (infrastruttura distribuita storage S3)
- Coordinamento gestione infrastrutture distribuite
- Gestione dei «core services» DataCloud
- Gestione dei «servizi SaaS» di INFN DataCloud
- Monitoring
- Sicurezza dell'infrastruttura
- Supporto di secondo livello per gli utenti

Futuro

- Coordinamento della gestione dei centri di calcolo anche Grid (Tier2)
- Coordinamento della gestione delle HPC-Bubble distribuite
- Riunioni previste con tutti i tier2 per pianificare le attività future nell'ambito dei progetti PNRR et al.

User support e training

- Supporto di primo livello per gli utenti della cloud federata (sia backbone che il resto)
- Organizzazione di turni per il supporto
- Organizzazione di training e corsi
  - Particolarmente intensa l'attività per l'organizzazione dei corsi per i nuovi assunti (progetti PNRR)

Futuro

- Organizzazione per il supporto a utenti delle comunità dei progetti PNRR

Resource planning e sostenibilità

- Discussione dello stato delle infrastrutture di base dei data center INFN (Tier2-1)
- Necessità di ammodernamenti e upgrade delle infrastrutture
- Necessità di allocazione risorse (Calcolo & storage) agli esperimenti, e valutazione dei «tipi di servizi» necessari

Futuro

- Organizzazione per il supporto a utenti delle comunità dei progetti PNRR

Security and policy

- Collaborazione con la CCR
- CSIRT+SOC
- Lavoro (in collegamento con il gruppo Harmony) sulle policy di accesso
- Coordinamento della gestione della sicurezza sulla infrastruttura nazionale di DataCloud
  - SCANSIONI: armonizzazione/unificazione attività per strutture e cloud;

Futuro

- Supportare la gestione degli accessi da utenti esterni all'ente
- Unificazione delle procedure e delle policy di sicurezza

Middleware e Sviluppo servizi

- Sviluppo di: IAM, PaaS, Dashboard per seguire i requisiti delle comunità di utenti che li usano (INFN-Cloud, WLCG, altri progetti/esperimenti)
- Sviluppi perfettamente sinergici con quanto promesso per i progetti PNRR

Futuro

- Coinvolgere i nuovi sviluppatori e continuare ad armonizzare le attività per supportare in modo sinergico i nuovi use case (Progetti PNRR e altri)
  - Non è semplice: la «learning curve» è piuttosto ripida nella fase inziale

R&D, Testbed, Use cases

- Testbed per le soluzioni di gestione del software
- Testbed per la distribuzione delle task di analisi su infrastrutture di calcolo eterogenee e distribuite
- Testbed per realizzare il data-lake nazionale

Futuro

- Valutazione di use case provenienti da una base di utenti più ampia e adattamento dei modelli di implementazione
  - Per esempio il progetto: DARE

Sistemi integrati di gestione e Legal Compliance

- Attività per l'estensione delle policy di accesso a utenti
  - non amministratori di sistema
  - «non INFN»
- Gap analysis e implementazione di una cloud «ISO certified» estesa fra CNAF, Bari e Catania
  - ➔ Nuova certificazione ISO **Ottobre 2023**
- Individuate le policy da scrivere e implementare e individuato il WP responsabile per ciascuna

Futuro

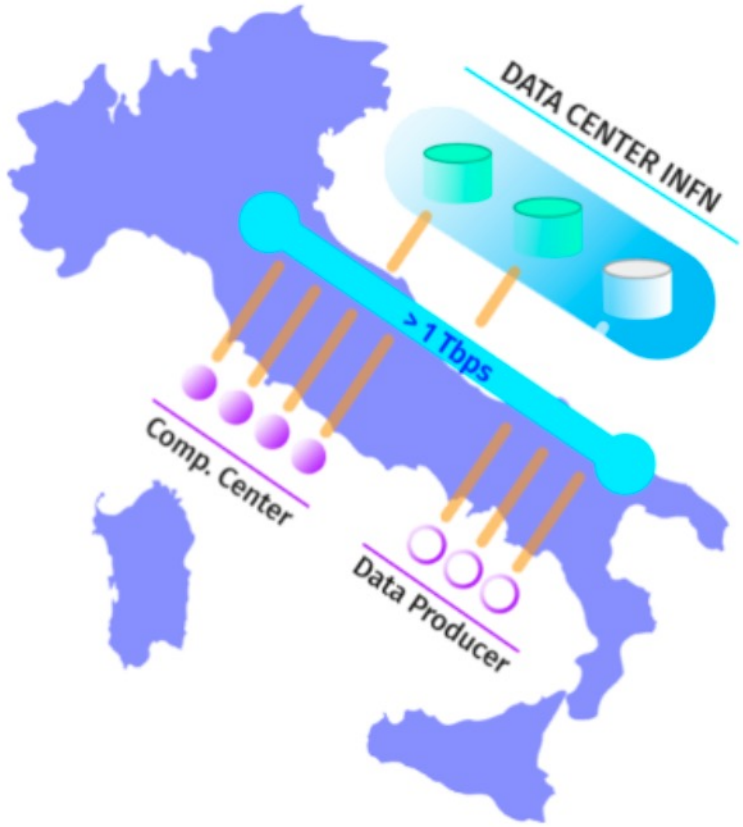
- Valutazione dei nuovi use-case e comunità di utenti che portano esigenze ancora più stringenti di quelle a cui siamo abituati
  - DARE, ICSC Spoke8, ma ci sono anche i POS
- Monitoring delle normative e standard ISO a cui dobbiamo fare riferimento

Federation

INFN CLOUD IS DESIGNED AS A FEDERATION OF PRE-EXISTING INFRASTRUCTURES

- The **Backbone** of the INFN Cloud is made up of two closely linked federated sites, BARI and CNAF.
- A scalable set of **satellite sites**, geographically distributed across Italy and loosely coupled, expand the resources offered by the backbone.

INFN Cloud core services and some centralised, fully managed, high-level services are hosted on the Backbone. This allows us to leverage **high-availability** and **disaster recovery** capabilities to ensure that these critical services are always available and operating at peak efficiency.

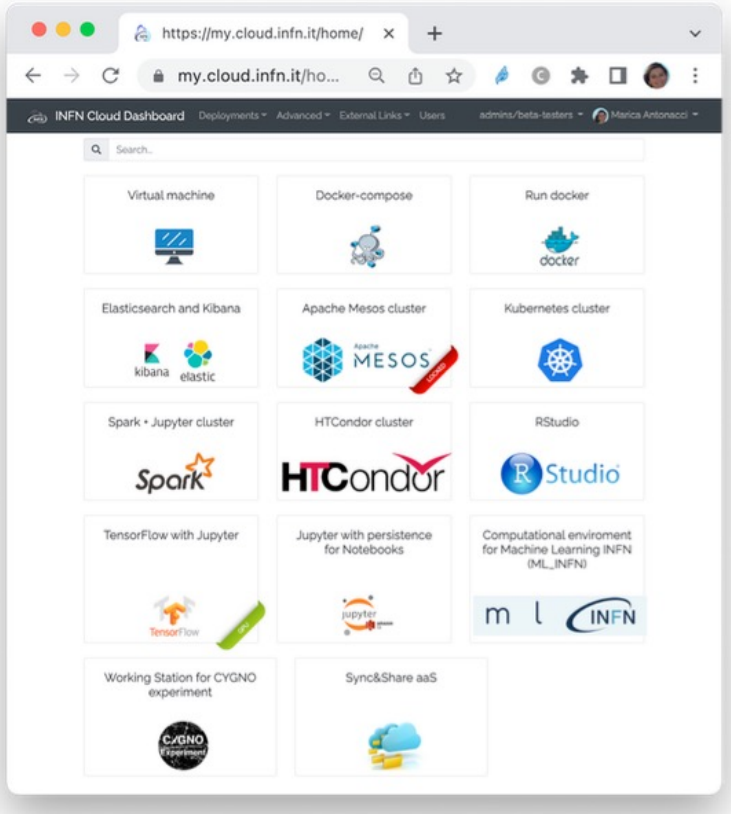


Front-ends

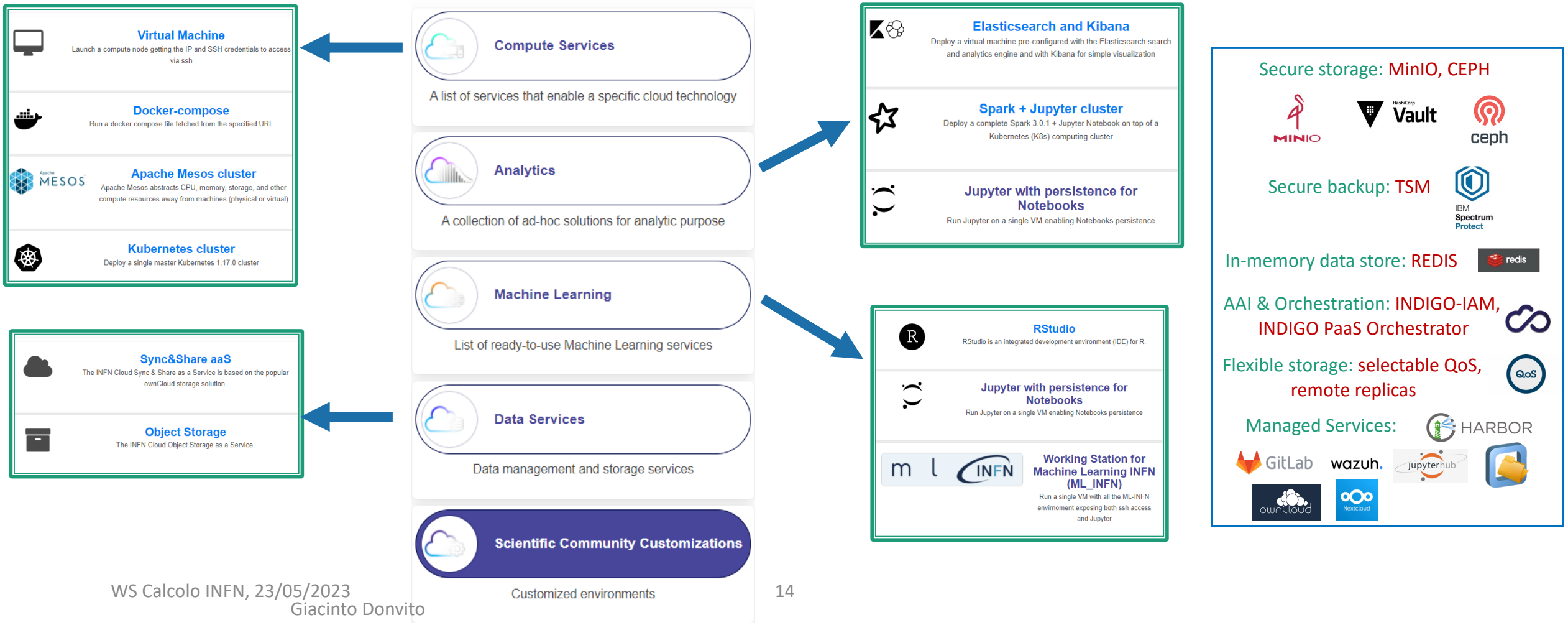
THE PAAS DASHBOARD

The INDIGO PaaS Dashboard is a web-based user interface that enables users to manage and monitor their deployments without requiring any TOSCA knowledge.
The dashboard hides all technical details and provides an intuitive interface for managing service deployments.

- OpenID-Connect Authentication
- Multi-tenancy
- Secrets management (via Vault integration)
- Dynamic view of service catalog (depending on the user group membership)



Dal portafoglio di INFN Cloud



L’infrastruttura del DTE

INDIGO-IAM
oppure EGI Check-IN

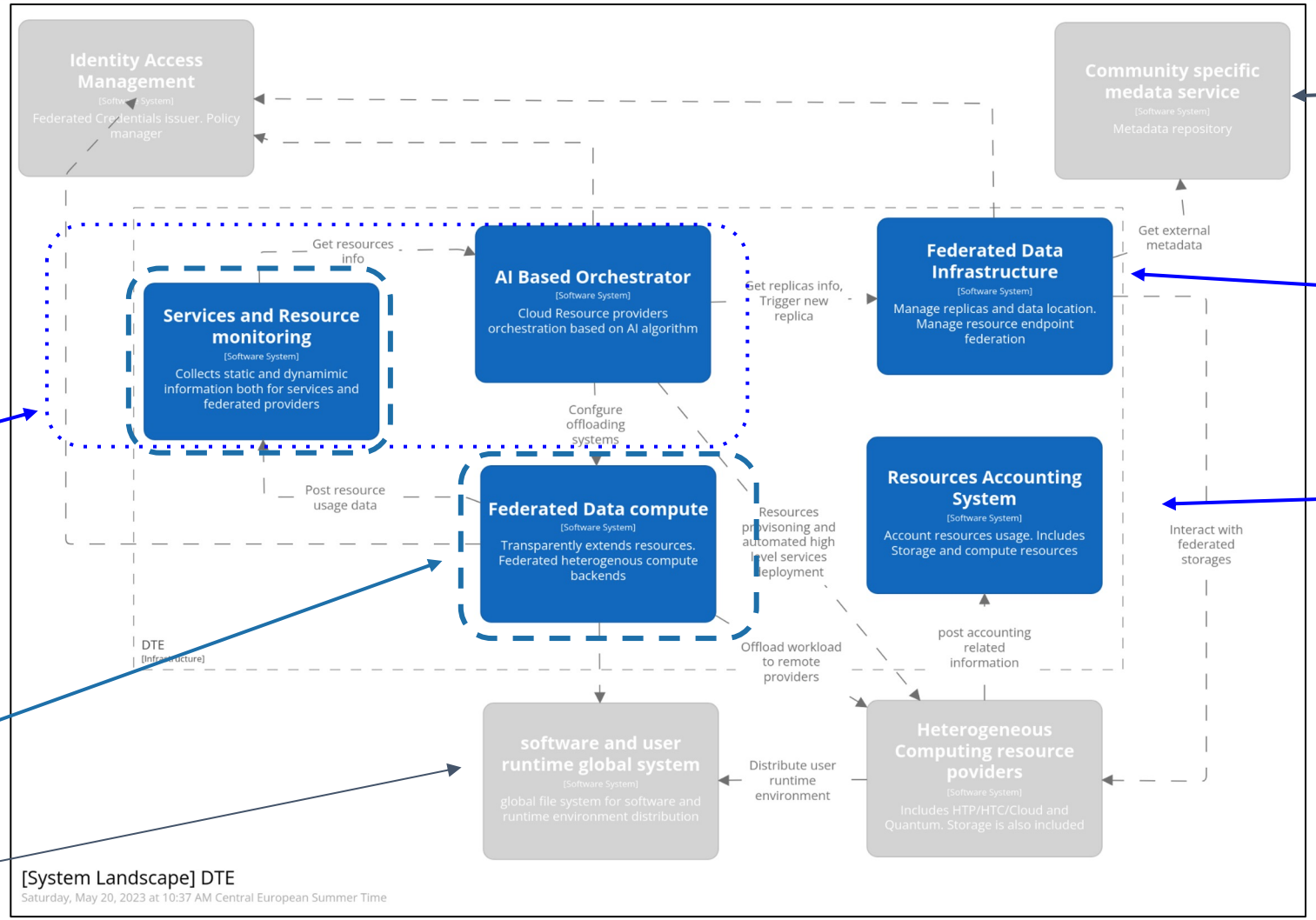
Ovvero quell’insieme di servizi che da accesso alle risorse

Non partiamo da zero!! Ma evolviamo quanto già fatto

INDIGO PaaS Orchestrator

Sistema per l’offloading (vedi presentazione InterTwin)

CVMFS



Cataloghi di comunità

Rucio + FTS

APEL

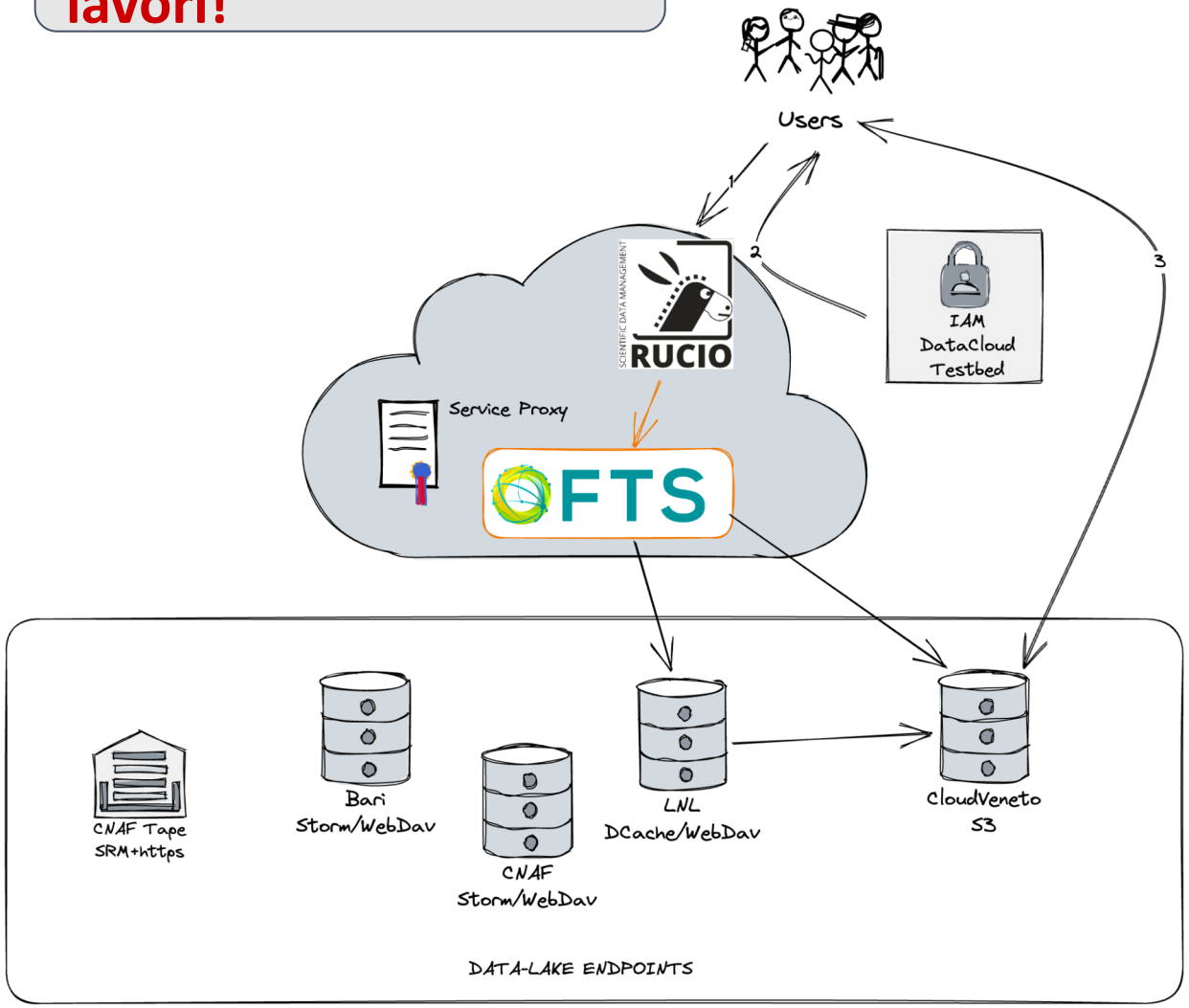
daniele.spiga@pg.infn.it

Dove siamo

~6 mesi da inizio lavori!

- **Instanziato su risorse cloud i server IAM, FTS e RUCIO dedicati al testbed DataCloud**
  - FTS può essere mantenuto “centralmente” e servire istanze di RUCIO multiple
  - IAM per AuthZ fine gestita centralmente, vedi dopo
- **Federato 5 siti con storage eterogenei:**
  - Uno storage con protocollo S3 su ceph @CloudVeneto
  - Tre storage con protocollo WebDav
    - Due basati su STORM (CNAF, Bari)
    - Uno su dCache (LNL)
  - Un endpoint tape @CNAF
- **Automatizzato la registrazione e la gestione degli utenti via IAM**
  - AuthZ gestita centralmente, i siti autorizzano sulla base dei token rilasciati

Dopo un periodo di configurazione siamo ad una situazione dove **il sistema e in linea con quello che ci eravamo prefissati** (vedi dopo e demo Massimo)



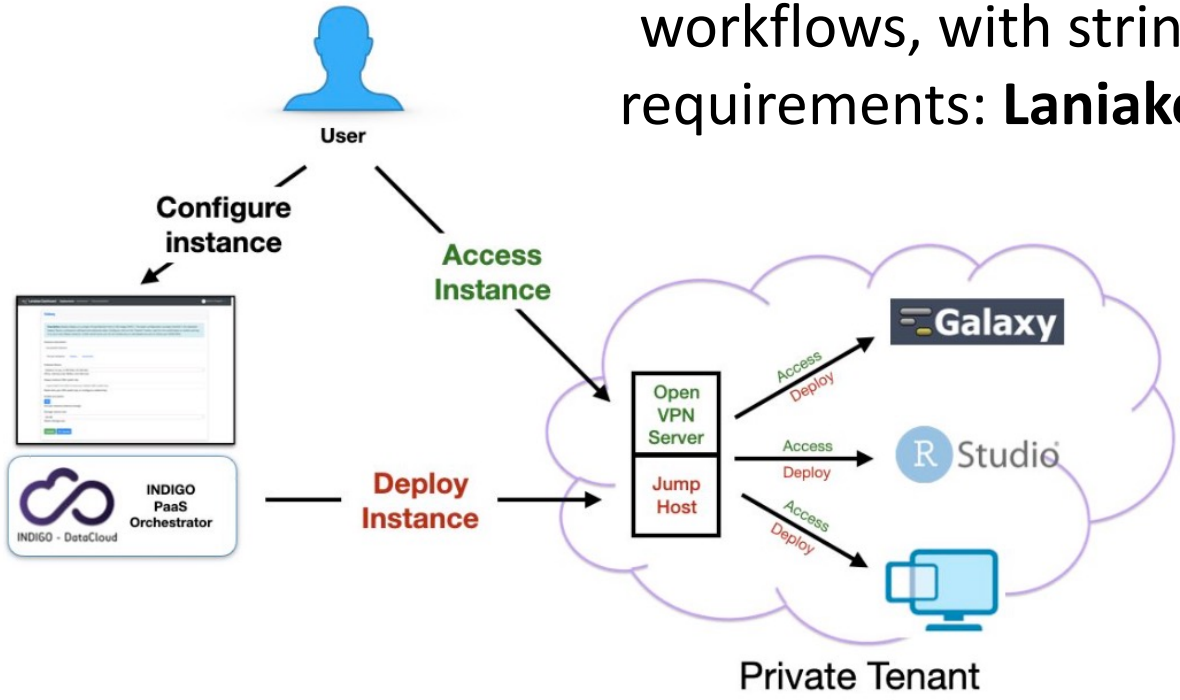
Security: multiple isolation levels

Deployments under VPN

VPN isolated environments - Automatic deployments of virtual environments on private networks.

Isolation is reached using Tenant and security groups properties, granting the access only through VPN authentication.

User authentication to the VPN using the same Laniakea credentials.



An *example* of the **Service Composition** approach: extending INFN Cloud to support complex workflows, with stringent security requirements: **Laniakea** (Elixir Italy)

41

EPIC Cloud

Enhanced Privacy and Compliance Cloud – The INFN Cloud partition for personal and confidential data processing

- The GDPR states that Clinical and medical data (for instance, genomic) is personal data; i.e., it fits in the Art.9 special categories of personal data.
  - Genomic data is mostly impossible to be anonymized → GDPR shall always be applied
  - ISO/IEC 27001 is the main certification mechanism compliant with GDPR requirements (Art. 43, 58, 63)
- In order to comply with the requirements of health research projects INFN is involved in, we created **a region of the INFN Cloud infrastructure**, applied specific organizational and technical security measures, and certified it ISO/IEC 27001, 27017, 27018.
  - This is **EPIC Cloud**: a reference Cloud implementation for the treatment of sensitive data at INFN.

From the Data Controller side, the fact that EPIC Cloud is ISO-certified is a way to demonstrate that processing is performed in accordance with the GDPR.

Come saranno costruite le HPC Bubbles

- Stiamo acquisendo risorse “HPC” che renderemo disponibili su INFN Cloud in diverse sedi dell’INFN
- **Cluster di nodi CPU** con significativa RAM (> 1.5TB / server) e di core (> 200 core / server), connessi via InfiniBand
- **Cluster di nodi CPU+GPU** con almeno 4 x GPU [h100] / server, connessi via InfiniBand
- **Cluster di nodi CPU+FPGA** (previste FPGA di più produttori), con possibilità di realizzare FPGA-mesh
- **Cluster di fast storage** con taglia minima 1 PB + storage sui nodi delle Bubbles

- Caratteristiche di servizio
- Integrazione con e accesso a **tutti i servizi di INFN Cloud**
- Integrazione **tra le HPC Bubbles** (Virtual HPC Bubbles)
- Integrazione **tra le HPC Bubbles e centri HPC tradizionali** (es. Leonardo, PRACE-Italy, ma anche VEGA e altri)

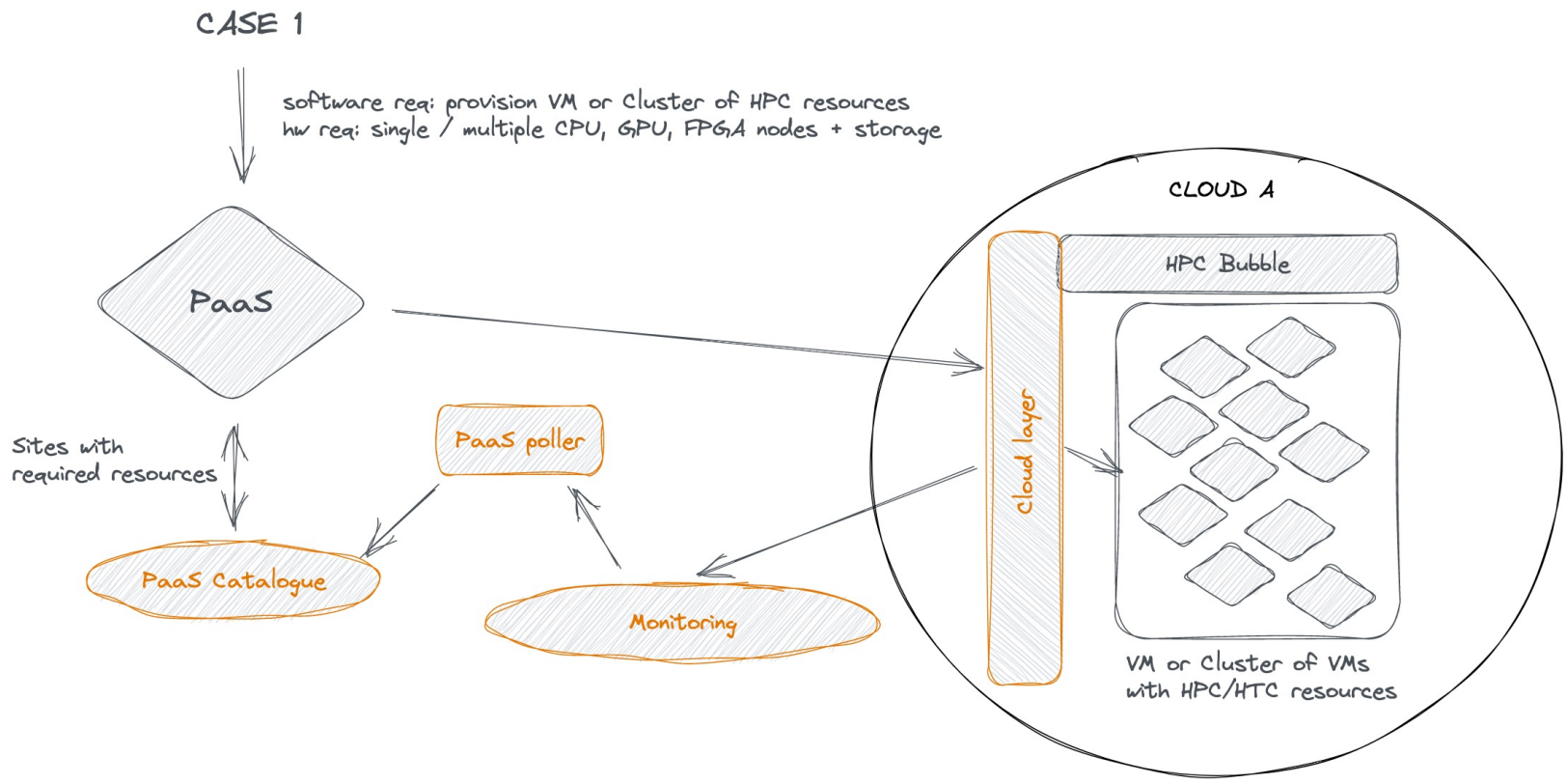
Le “HPC Bubbles” dunque…

- Saranno regioni, distribuite sul territorio nazionale e accessibili in modalità Cloud Computing che espanderanno l’infrastruttura INFN HPC-BD-AI e su cui sarà possibile eseguire calcoli ad altissime prestazioni (HPC).

- Forniranno cluster e soluzioni flessibili con risorse di tipo CPU, GPU, FPGA e storage veloce, saranno **combinabili tra di loro** e si **integreranno con i grandi centri HPC nazionali**, come Leonardo o PRACE-Italy @ CINECA, **con il Centro Nazionale ICSC** e con altre Cloud o centri HPC internazionali.

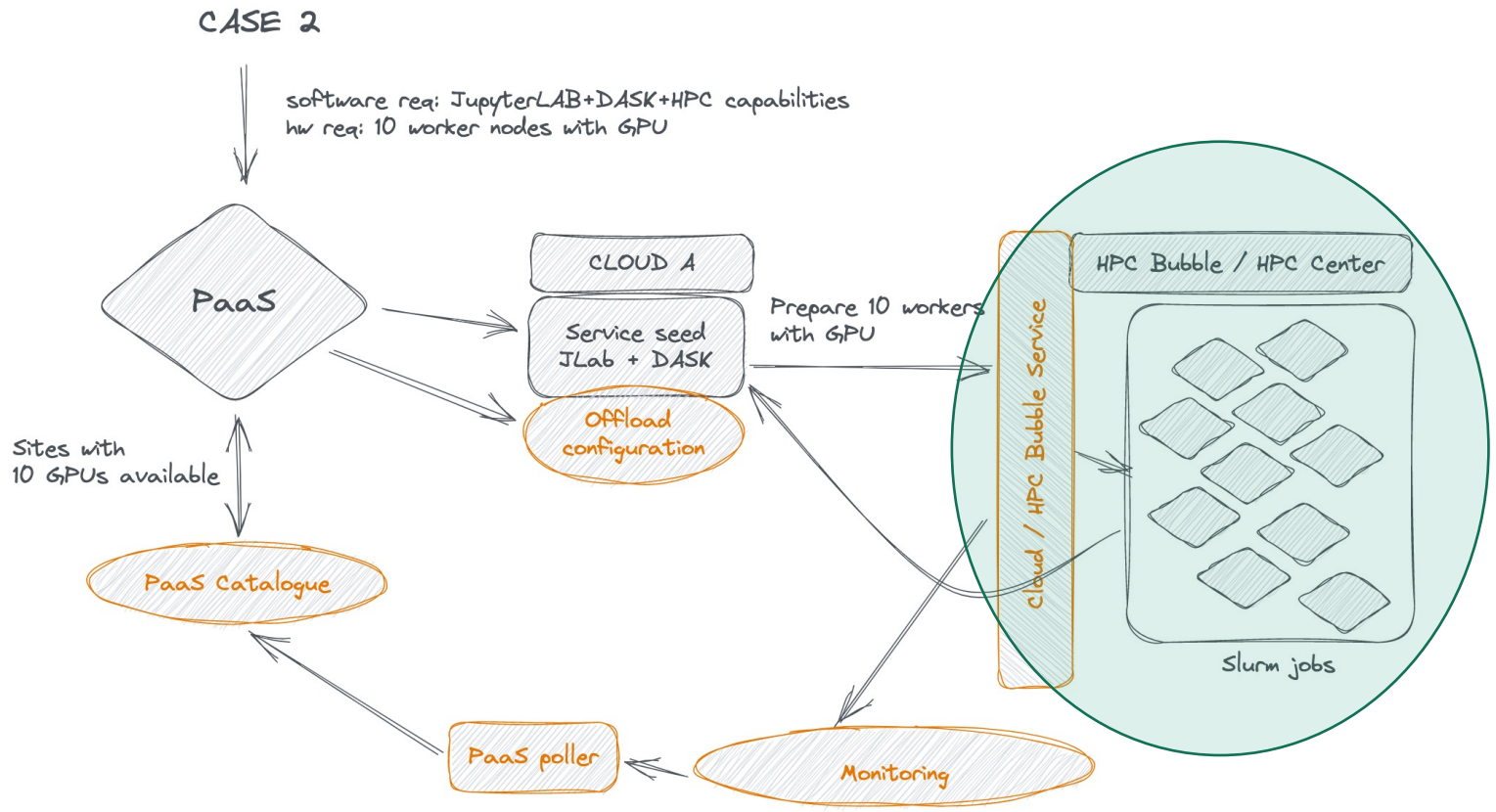
Integrazione tra Cloud tradizionale e HPC Bubbles

- **Obiettivo 1**: utilizzo delle risorse HPC Bubbles direttamente **da Cloud**



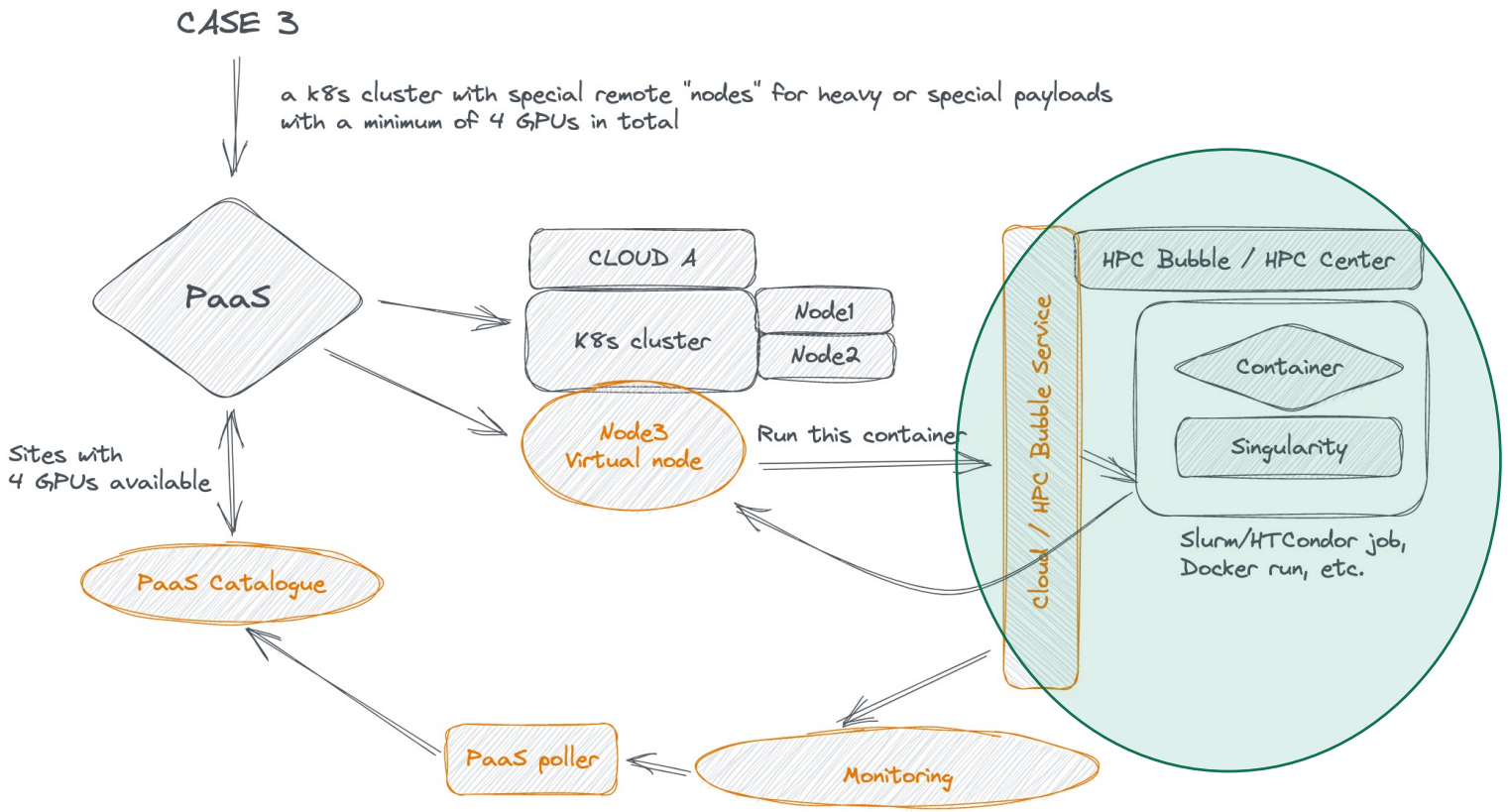
Integrazione tra Cloud tradizionale e HPC Bubbles

- **Obiettivo 2**: offloading di DASK tasks per **analisi interattiva**



Integrazione tra Cloud tradizionale e HPC Bubbles

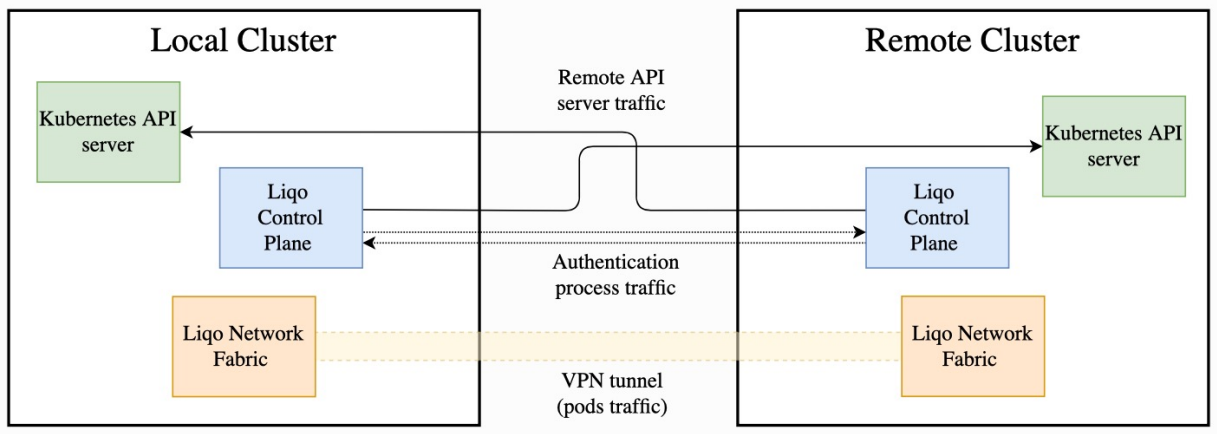
- **Obiettivo 3**: offloading di pod Kubernetes per **pipeline di ML / data science**



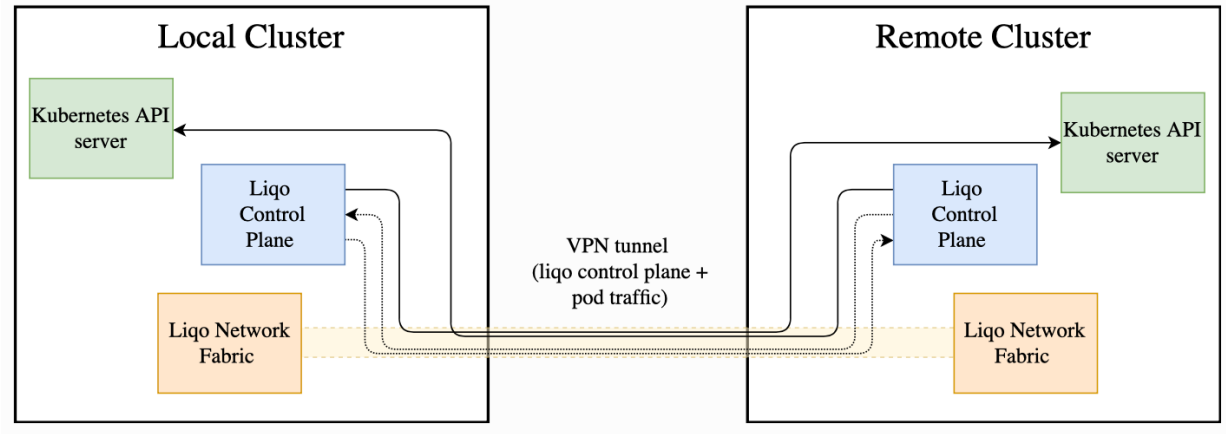
Integrazione tra HPC Bubbles e con altre risorse HPC (es. da ICSC)

- **Obiettivo 4**: creazione di **Virtual HPC Bubbles**

- Pensiamo di valutare due differenti approcci di peering del control plane tra le Bubbles:
  out-of-band e *in-band*



Out-of-band control plane



In-band control plane

Source: https://liqo.io

Integrazione in infrastrutture certificate ISO

- Dal testo del WP4 di TeRABIT:

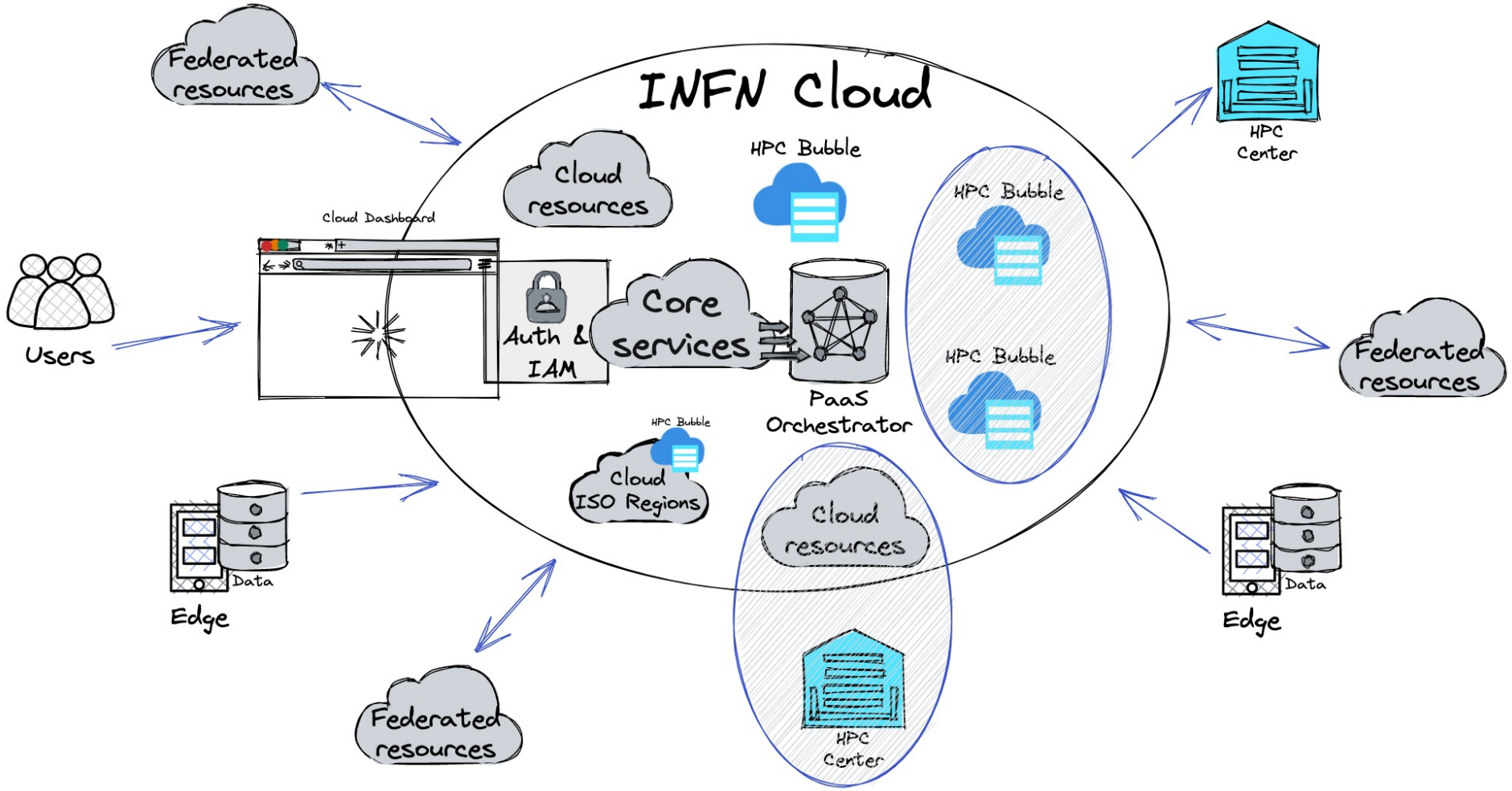
[…] a key aspect that will be covered by this WP is the provisioning of HPC bubbles installed also in **federated Cloud HPC centres that are ISO 27001, 27017 and 27018 certified**.
This will allow not only to support full edge-to-cloud-to-HPC integration in general, but also to expand it to cover the **case where ingestion, storage and processing of sensitive data is needed**, such as all the cases that require management of health-related data.

- HPC Bubbles su EPIC Cloud:

INFN Cloud contiene già una regione certificata ISO chiamata **EPIC** (Enhanced Privacy and Compliance) Cloud, dedicata specificamente al trattamento in Cloud di dati sensibili. Con TeRABIT, **istanzieremo una HPC Bubble anche su EPIC**.

- Inoltre, nel contesto di ICSC, EPIC Cloud verrà estesa per realizzare altre due regioni certificate in INFN Cloud. Un obiettivo di TeRABIT è di portare le HPC Bubbles in almeno una di queste due nuove regioni.

The *continuum* from Edge, to Cloud, to HPC



Ipotesi di distribuzione delle risorse PNRR (HPC-Bubbles + Risorse ICSC)

Sito	Nodi CPU	Nodi GPU	Nodi FPGA	Storage (PBN EC)
CNAF	16	14	2	4
CNAF-ISO27001	8	8	0	2
BA	7	3	0	3
MI-BI	0	0	2	0
PI	8	0	0	0
TO	6	4	0	0
LNGS	4	0	0	0
NA	8	0	2	0
RM1	8	0	0	0
PD/LNL	6	6	0	0
TOTAL	**60**	**35**	**6**	**9**

SEDE	Numero sistemi
BARI	19
NAPOLI	19
CATANIA	7
ROMA1	8
FRASCATI	8
TORINO	9
MILANO	8
PISA	9
LEGNARO	8

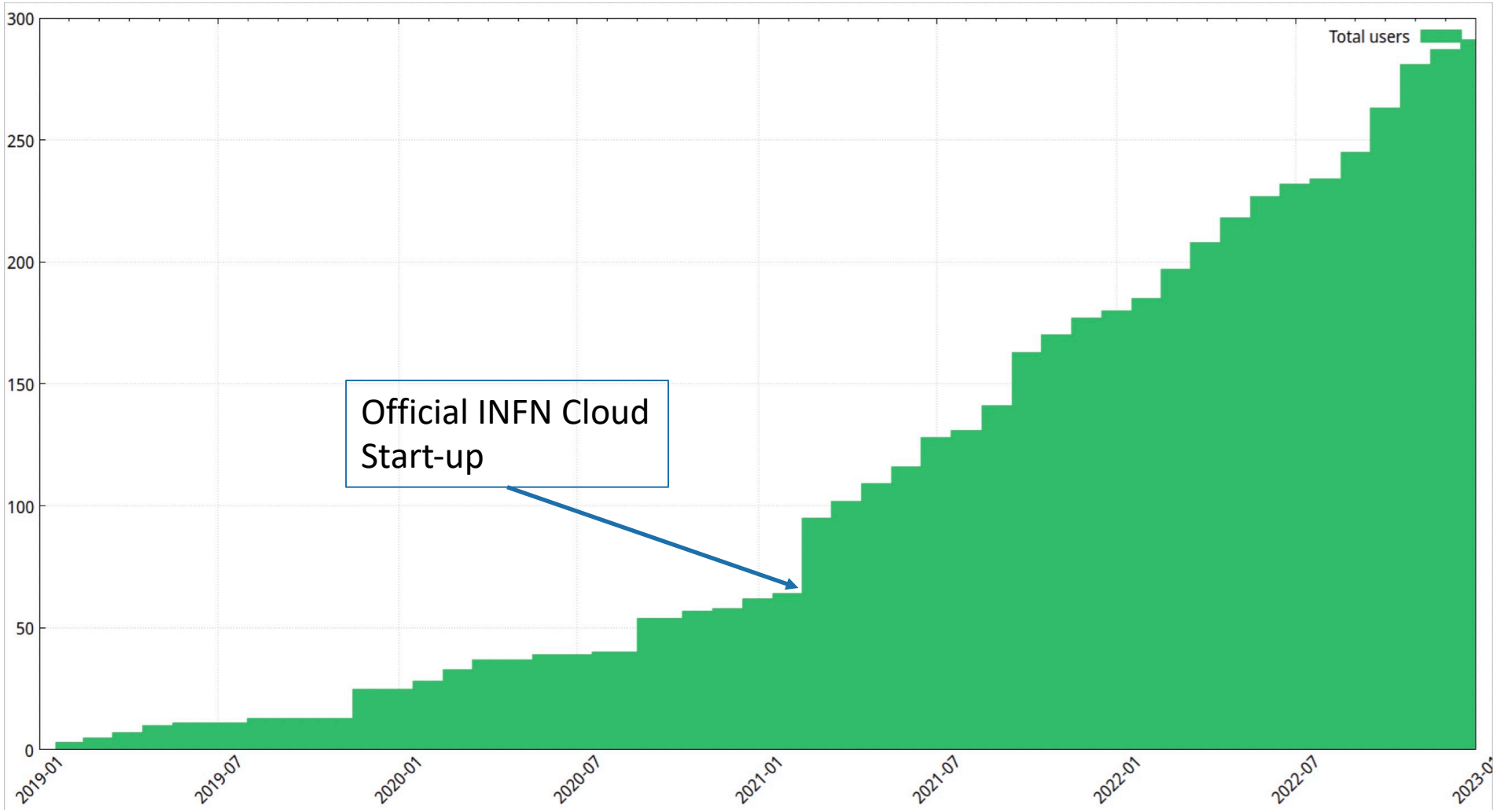
- Attualmente solo 3 siti fra questi hanno una risorsa federata in INFN-Cloud
- La «distribuzione» dello storage cloud e «poco distribuita»
  - Questo richiede che l'accesso sia trasparente alla distanza fisica

Punti aperti per la discussione

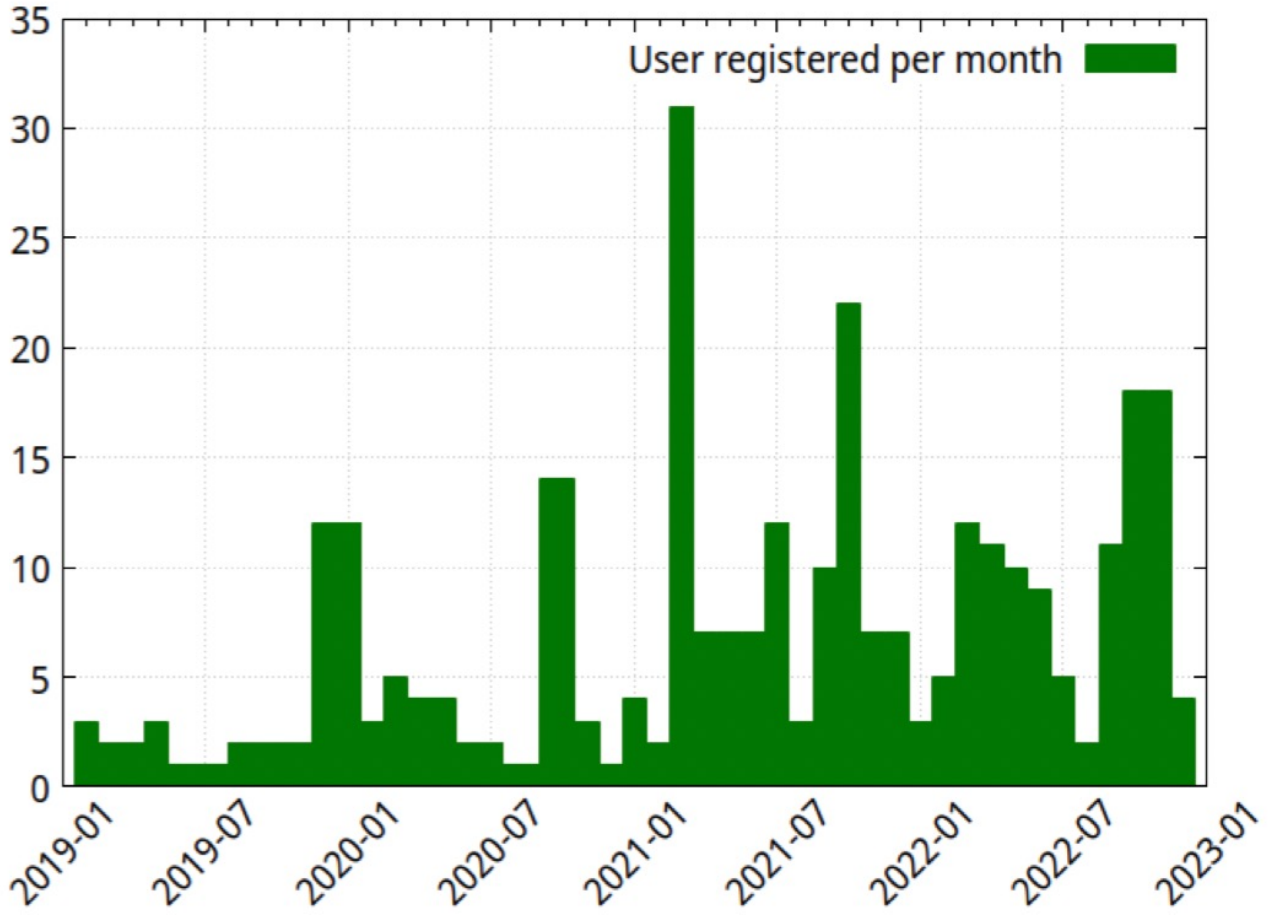
- Governance di DataCloud
  - Vedi «non conformità» sull'audit INFN-Cloud
- Coordinamento con le sedi
  - Soprattutto circa i nuovi assunti e il loro coinvolgimento nelle attività Nazionali
- Steering di allocazione delle risorse (Pledged/non pledged) sui vari servizi (Cloud/Grid)
  - in discussione un foglio con il mapping di tutti gli assunti (tecnici e tecnologi) PNRR tra progetti vs. wp di datacloud
- Nella maggior parte dei siti che sono potenziati con risorse PNRR non c'è sufficiente expertise per realizzare Cloud-Bubbles
  - In alcuni siti non c'è neanche la Cloud
  - Gli utenti (PNRR in particolare) chiedono sempre più accesso a questo tipo di risorse
- Molti dei vincitori dei concorsi stanno rinunciando, in qualche sito questo è particolarmente grave
  - Anche con 0 prese di servizio
- **È necessario sostituire il coordinatore del WG di DataCloud ☹**

Backup slides

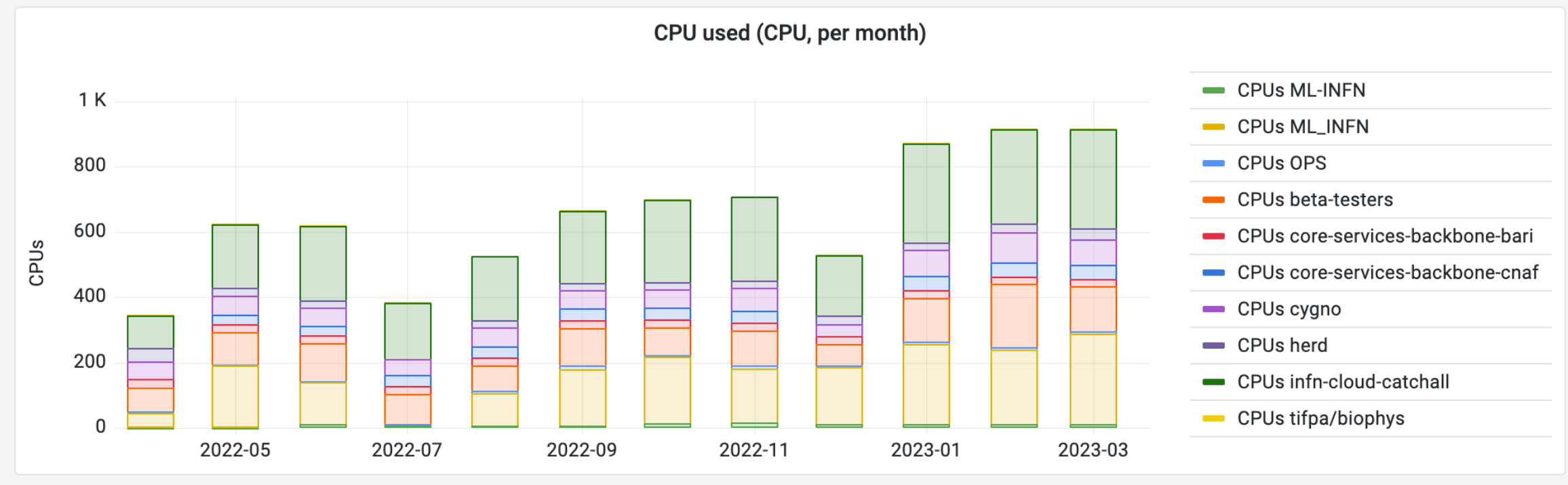
Crescita degli utenti



Iscrizioni per mese (dall'inizio)



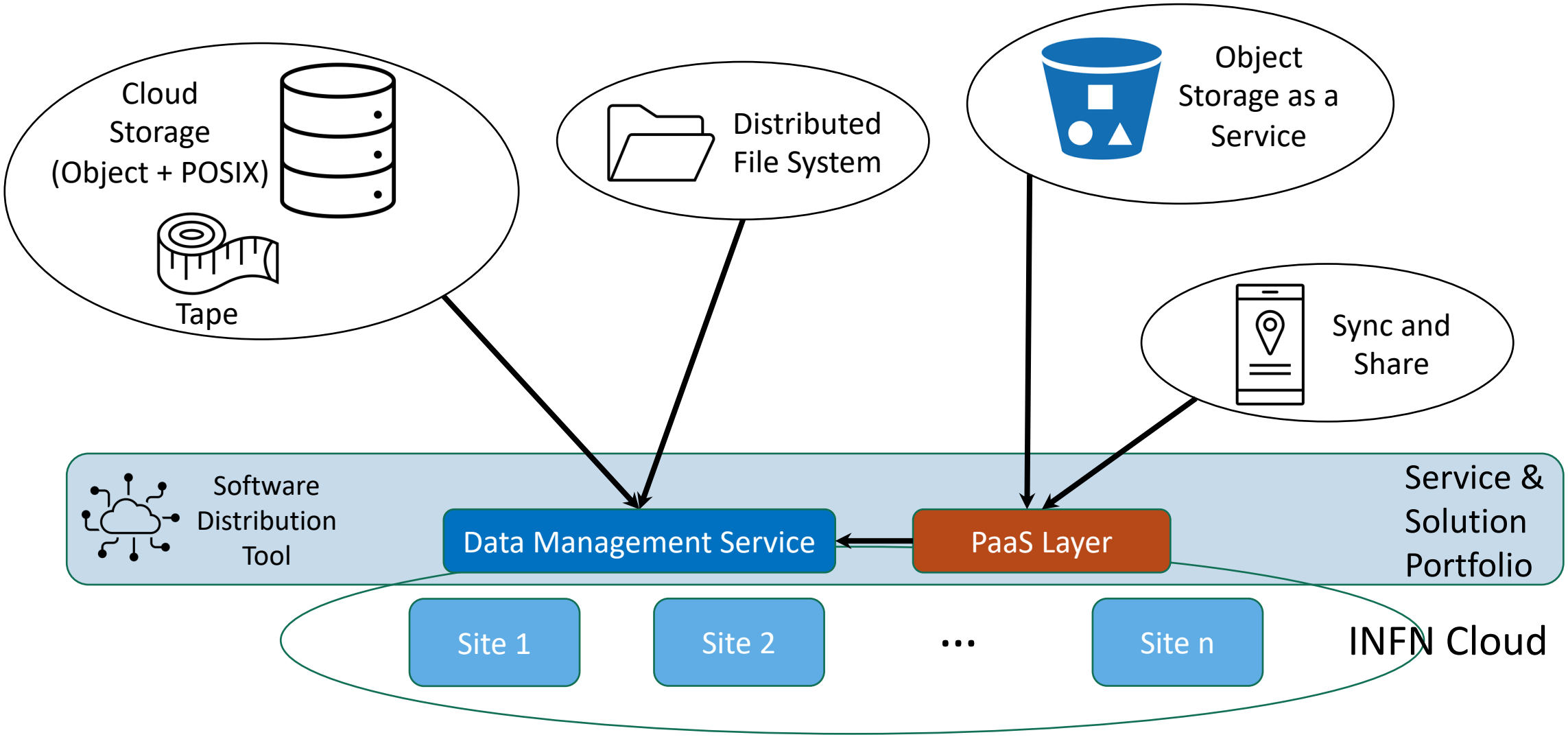
CPU usata per mese



The INFN Cloud Data Services

- Data Management Service
- Distributed File System
- Object Storage [also “as a Service”]
- Sync and Share
- Software Distribution Tool

Architectural overview



INFN Cloud Data Management Service

- This service decouples physical storage from the logical layer, i.e., the user-level view.
  - The service handles files upload / download from the datalake or in general from remote storage.
- Configure data copy policies among cloud sites or between edge and cloud, with the option to possibly replicate data among multiple sites.
- Configure data policies to replicate data among different storage classes (es. HDD vs. SSD).
- Create a metadata catalog from scratch for your data.
- Plug in your own catalog to the INFN Cloud Data Management Service.

INFN Cloud Distributed File System

- This service provides persistent and resilient storage (i.e., backed up).
- Access your own files via Posix from cloud-based resources such as VMs, or for example mounting them from your own laptop.
- Use it to create your own cloud-based “home directory”, accessing it from everywhere.
- Supports:
  - Client-side caching.
  - Data Management–driven replicas.
- Not suitable to host large amount of data (> 5 TB). Use object storage for this and for high I/O requirements.

INFN Cloud Object Storage

- This service provides scalable data storage using S3-compatible storage.
- Storage is also visible via Posix mount (but the performance is in this case lower than the dedicated distributed Posix service)
- Supports:
  - Tenant segregation
  - At-rest encryption
  - Secure transfer via https
  - Data Management-driven replicas
- An “object storage as a service” can also be provided, if the requirement is to get a self-managed, S3-compatible storage service.

INFN Cloud Software Distribution Tool

- This managed service allows to distribute your software or configurations to the datalake by just committing it to some gitlab-area or by copying it to some S3-compatible bucket.
- The software can then be automatically mounted by any of your resources in INFN Cloud.
- Supports:
  - Automated integration with the INFN Cloud Gitlab Service and with INFN Cloud S3-compatible buckets.
  - Automated deployment of a CVMFS hierarchy
  - Automated POSIX mount in containers or VMs deployed over INFN Cloud

INFN Cloud Sync and Share

- Store files in INFN Cloud, so they are available on any of your devices and can be shared with a few clicks.
- Not suitable to store large amounts of data (> 5TB), no built-in high-availability. Custom configurations may be discussed with the INFN Cloud Management.
- Available implementations:
  - Owncloud
  - Nextcloud
- Supports:
  - Self-instantiation for yourself or your group
  - File versioning
  - Collaborative text editing
  - Clients for Windows, MacOS, Linux, Android, iOS

What we are working on

- All the items shown before…
  - Four MD thesis dedicated to compute/data services have just been started at CNAF on:
    - CVMFS extensions
    - DASK-based workload multi-site offloading
    - Use of microVMs
    - Creation of a prototype blockchain as a service
- **We must adopt a consistent process for the definition of the services**. This is defined in the DataCloud WPx meetings and documents. This is where the discussions take place → **please do participate**.
- Adaptation of the services shown for:
  - Tecnopolo (CNAF Reloaded)
  - INFN Cloud
  - ICSC Spokes, starting from Spoke 2, Spoke 3, Spoke 8
  - InterTwin (data management with HPC support and external catalogs)
  - DARE, in collaboration with Istituti Ortopedici Rizzoli / AlmaHealthDB
  - Health Big Data
  - Sant'Orsola

Data services: summary table (with some internals, still under discussion)

Service Name	Managed Service	Self-provisioning	Storage Limit (Default)	Automated Replicas	QoS Support	S3 REST API	Web Frontend	POSIX Access	File Versioning	Internal
Data Management Service	Yes	No (for now)	N/A	Yes	Yes	N/A	Yes	N/A	N/A	Rucio, FTS
Distributed File System	Yes	No	5 TB (1TB)	Yes	No	No	No	Yes (high throughput)	No	CephFS + StoRM-WebDAV Other solutions?
Object Storage	Yes	Yes (if requested)	Subject to negotiations	Yes	Yes	Yes	Yes	Yes (low throughput)	No	Ceph
Software Distribution Tool	Yes	Yes	1 TB	Yes	N/A	No	No	Yes	No	cvmfs + extensions
Sync and Share	No	Yes	5 TB (1 TB)	No	No	No	Yes	Yes (low throughput)	Yes	Owncloud Nextcloud