

INFN Cloud - un anno di operatività: esperienze di gestione infrastrutture e utenti

INFN Cloud TEAM
(see last slide)



Introduzione



- *Descrizione generale WP e compiti*
- *Highlight dell'attività svolta durante il primo anno di produzione*
- *Considerazioni, lessons learned, cosa abbiamo fatto bene, male*

Architecture, Operations and Service Portfolio - WP1 -





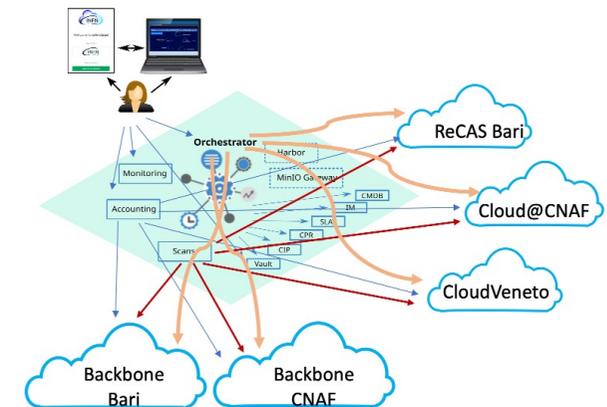
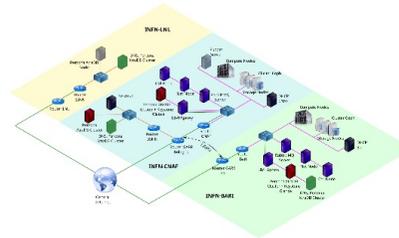
Task ed obiettivi di WP1

- Gestione operativa dell'infrastruttura del backbone di INFN Cloud
 - Hardware
 - Sistema di gestione dell'infrastruttura cloud del backbone – Openstack
- Gestione dei servizi core di INFN Cloud presenti sul backbone, con particolare attenzione alla continuità operativa
- Gestione di servizi di tipo SaaS
- Gestione dell'infrastruttura di storage S3 di INFN Cloud, in continua evoluzione
- Supporto agli altri WP
- Supporto di secondo livello agli utenti

Architettura vari livelli



- IaaS
- PaaS
- Infrastrutture federate





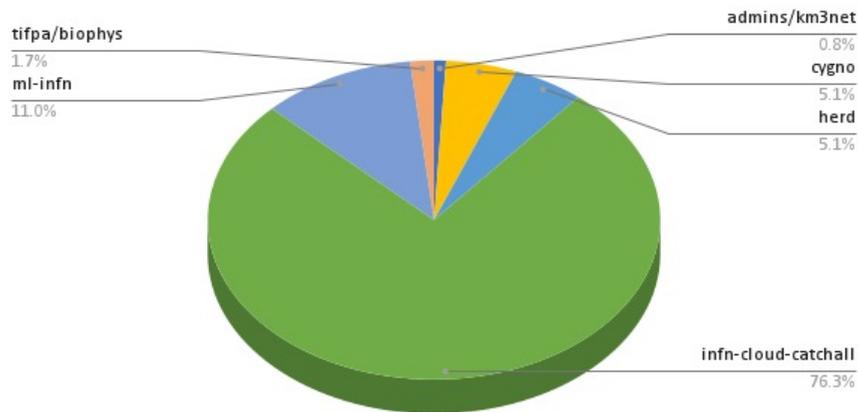
Numeri

- 23 Hypervisor sul Backbone di INFN Cloud
 - ~ 2K VCPU, 15 TB RAM
- Storage sul Backbone di INFN Cloud
 - ~ 1.5 PB raw HDD
 - ~ 100TB raw SSD

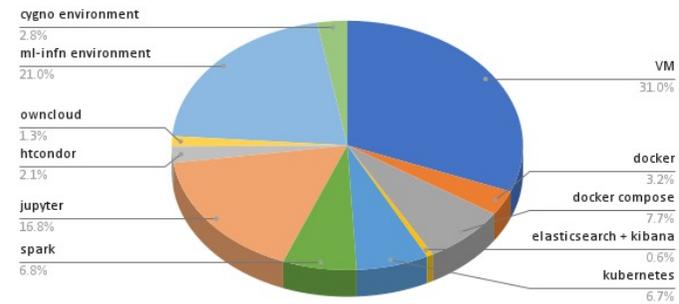
Deployments (1)



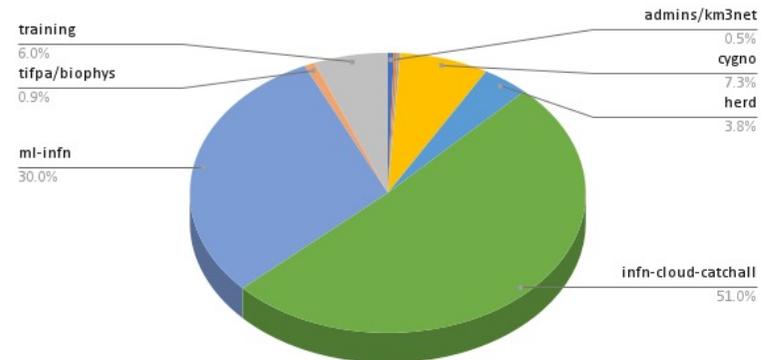
Currently Active Deployments per IAM Group: Total 118



Fraction of Deployment per solution. Total 810



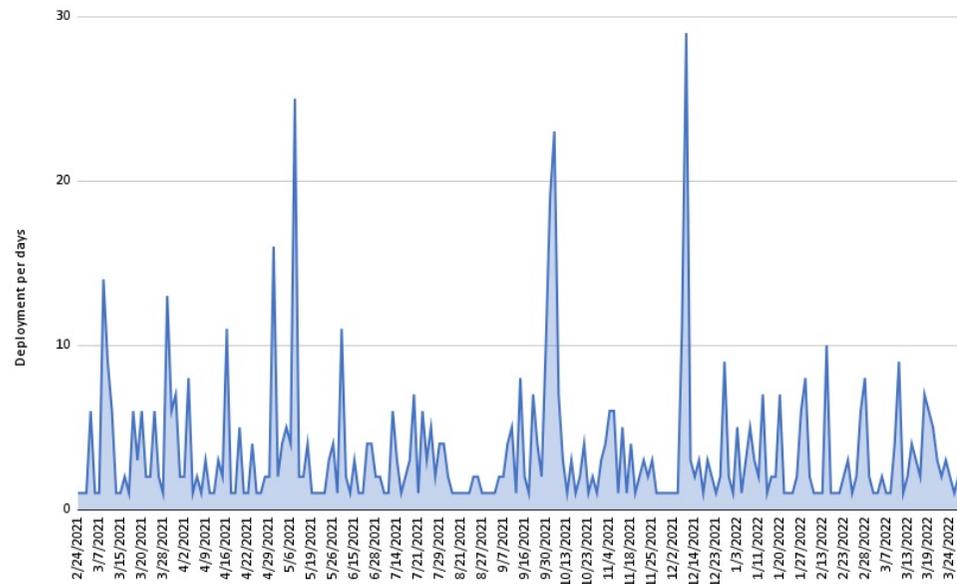
Deployment per IAM Group: Total 810



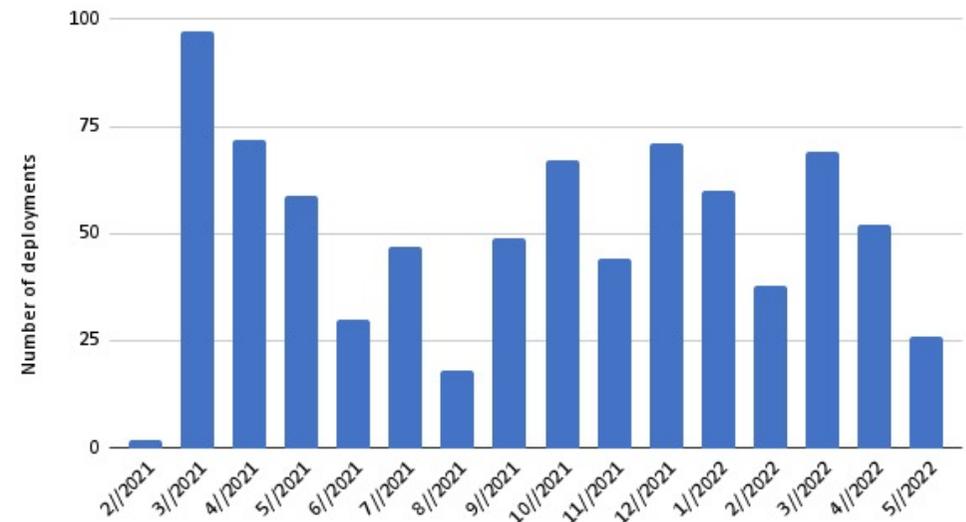
Deployments (2)



Deployment per days



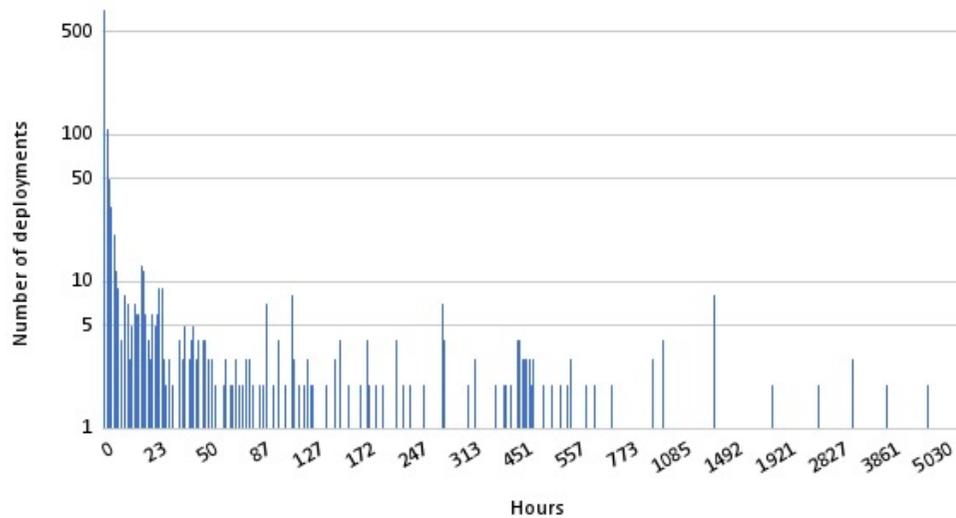
Number of deployments per month



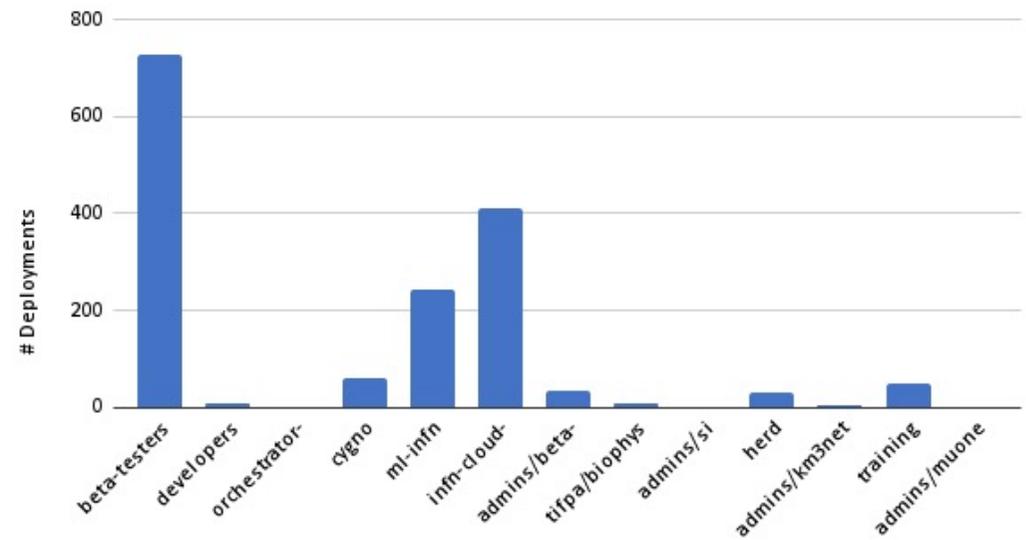
Deployments (3)



Deployments lifetime in hours (production and testing)



Deployments by groups



Highlights



- Ottimizzazione e fine tuning dei servizi di storage, sia di tipo block device che object
 - performance tuning
 - risoluzione di problemi
 - consolidamento dell'infrastruttura
 - realizzazione e gestione del servizio di storage S3 basato su MinIO gateway
- Supporto agli altri WP:
 - infrastruttura per CI/CD
 - infrastruttura per scansioni di sicurezza
- Gestione di nuovi servizi:
 - Notebook as a Service
 - Docker repository



Riflessioni

- Le risorse umane sono sempre il punto più critico
 - manca il tempo per affrontare i problemi con la necessaria tranquillità e per studiare approfonditamente nuove soluzioni e strategie
 - difficoltà a trovare persone che siano disponibili a gestire nuovi servizi o ad intraprendere nuove attività
 - lentezza nel portare a termine attività articolate
- Ottimo coordinamento tra i WP rende il lavoro più facile



Documentation and User Support, Communication and Training - WP2 -





Task ed obiettivi di WP2

Documentazione e supporto utenti

➤ Documentazione:

- Guide **utente** per i servizi offerti
- guide **amministrative** per la gestione operativa di IaaS e PaaS per gli amministratori di sito
- Guide **tecniche** per l'implementazione delle «regole di ingaggio» (vedi WP4)

➤ Supporto utenti e di casi d'uso:

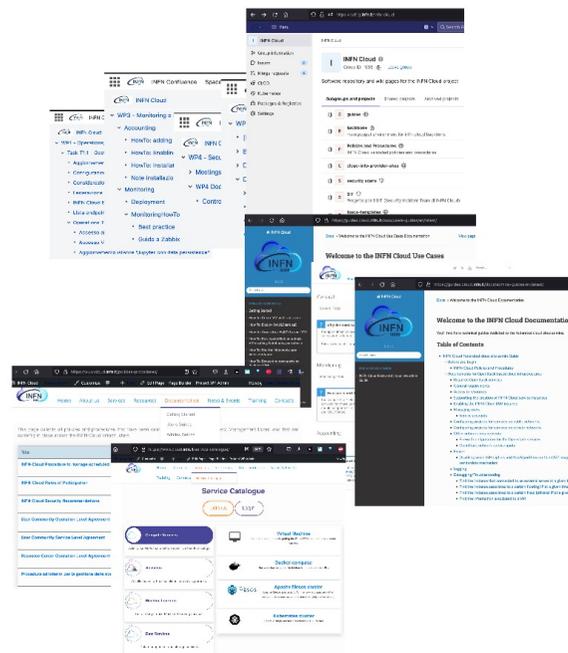
- Definizione e implementazione del **sistema di supporto utenti**: Service Desk, livelli di support
- Raccolta dei **requirement e supporto di nuovi casi d'uso**: best practices e documentazione tecnica per l'implementazione (ad esempio: come usare e scrivere TOSCA templates o i TOSCA types)

Comunicazione e training

- Creazione e organizzazione di materiale per dissemination, presentazioni, organizzazione eventi, partecipazione ad eventi esterni.
- Attività di comunicazione interna (CSN, altre componenti INFN) ed esterna.
- Organizzazione di eventi di training a livello sia utente che amministratore su argomenti correlati alle attività di INFN Cloud.

Documentazione

- Knowledge Base interna + Code Repositories:
 - Confluence: <https://confluence.infn.it/display/INFNCLOUD/INFN+Cloud>
 - GitLab: <https://baltig.infn.it/inf-n-cloud>
- End-Users:
 - Guide: <https://guides.cloud.infn.it/docs/users-guides/en/latest/>
 - FAQs: <https://www.cloud.infn.it/faq/>
- Admins cloud federate:
 - Guide: <https://guides.cloud.infn.it/docs/admins-guides/en/latest/>
- Politiche e Procedure
 - <https://www.cloud.infn.it/policies-procedures/>
- Service Catalogue:
 - <https://www.cloud.infn.it/service-catalogue/>



• **Good & Bad: ricca “libreria” basata sulla forte collaborazione tra i vari WP, condivisione conoscenze, esperienze MA l’effort e limitato (5WP + le stesse persone) => serve molto tempo avere documentazione adatta a essere pubblicata**



Supporto

- ServiceDesk:

- Modalità di contatto:

- <https://servicedesk.cloud.infn.it>
 - cloud-support@infn.it

- Tipi di richieste

- RegISTRAZIONI – uso risorse e soluzioni, personale o collaborazione
 - Problemi tecnici & Sugerimenti di miglioramento
 - Training

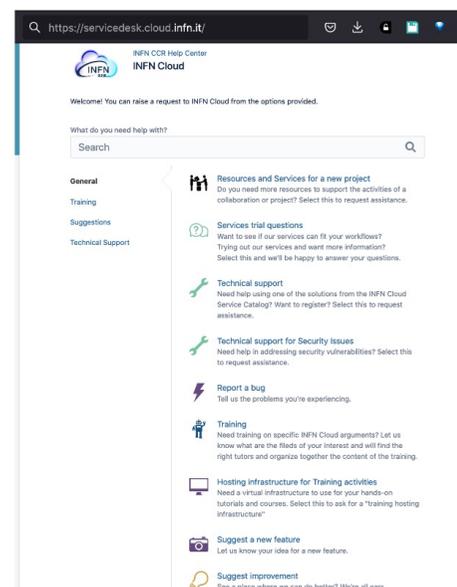
- Supportare i supporter:

- Guide, template
 - Checkpoint settimanali

- **Good & Bad: sistema di supporto organizzato a livelli e con turni, ma**

Internamente: Primo livello di supporto /turni coperto solo da ~4 persone

Esternamente (utenti): Evidente la non lettura delle guide, in particolare “Getting Started”

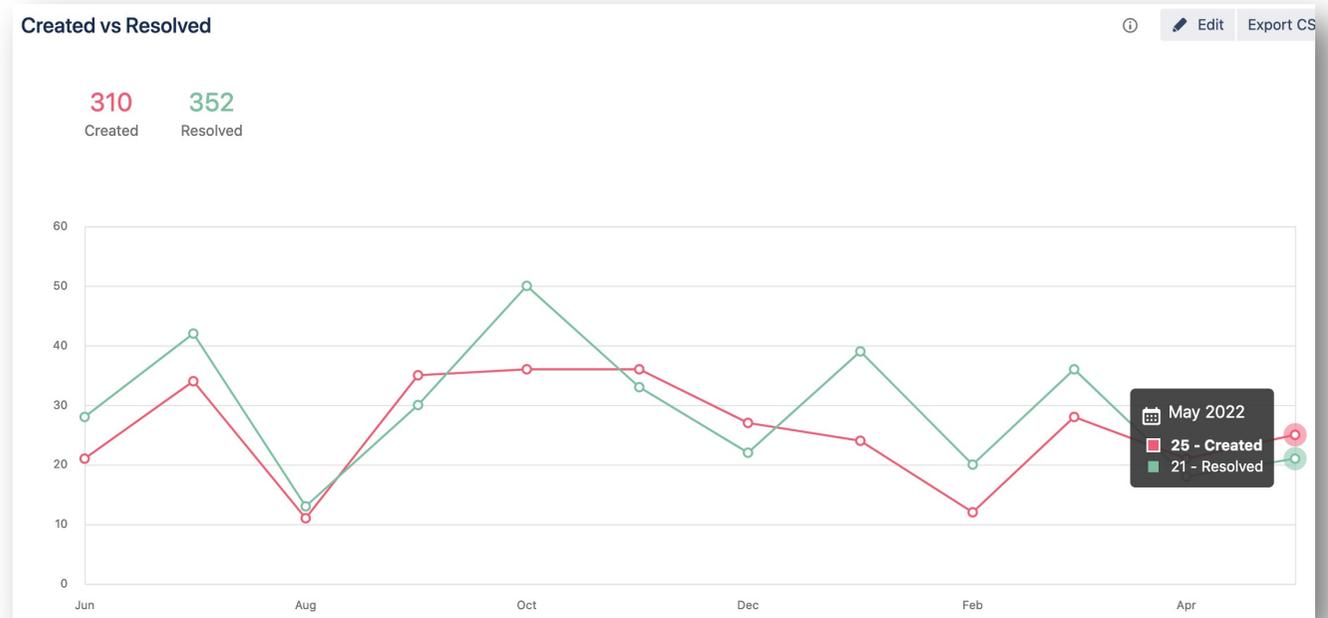
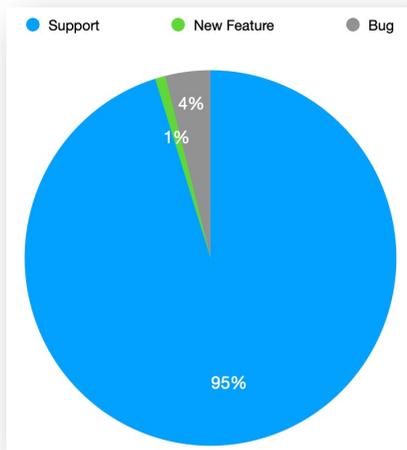


Supporto – alcuni numeri



- Numero totale ticket aperti: **561**
- Attualmente aperti: **21**

- Richieste registrazione: **322**
- Attualmente aperte: **7**



- **Molto da migliorare: SLA, corretta classificazione delle richieste**

Comunicazione

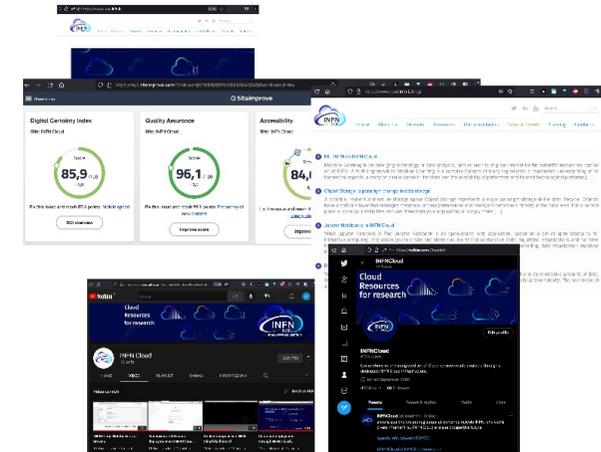


- Sito web: <https://www-cloud.infn.it>
 - Accessibilità = WCAG 2.1
 - Blogs
 - Canali Social: [Twitter](#), [YouTube](#), [Linkedin](#)
 - Eventi – partecipazione a conferenze
 - GARR 2020, 2021
 - EGI Conference 2020
 - CCR 2020, 2021
 - [ISGC 2022](#)
 - Workshop AI@INFN

- **Good & Bad:**

Grande aiuto, molto professionale dal Ufficio Comunicazione INFN

Dopo la spinta iniziale, stiamo soffrendo di mancanza di contributi per la sezione Blog





Formazione (1)

- Corsi:
 - 2022
 - New: [Uso e sviluppo di applicazioni e servizi su INFN Cloud](#)
 - [Docker e orchestrazione di container - II edizione](#)
 - [DataScience con Python: dalle Stringhe all'Intelligenza artificiale – II edizione](#)
 - 2021
 - [Second ML-INFN Hackathon: Starting Level](#)
 - [DataScience con Python: dalle Stringhe all'Intelligenza artificiale](#)
 - [Tutorial Days CCR : Amministrazione di risorse erogate attraverso INFN Cloud](#)
 - [Big Data E Machine Learning](#)
 - [First ML-INFN Hackathon](#)
 - [Docker e orchestrazione di container](#)
 - 2020
 - Tutorial Days CCR:
 - [Tutorial days di CCR : INFN Cloud - Utenti e Use cases](#)
 - [Tutorial days di CCR: INFN Cloud - Federated cloud sysadmins](#)
- **Good & Bad: Infrastruttura e le soluzioni di INFN Cloud usate con successo per corsi sia organizzati da noi che da “esterni”**

Tuttavia – alla mancanza di personale si aggiungono anche difficoltà provocate da vincoli normativi interni non chiari



Formazione (2)

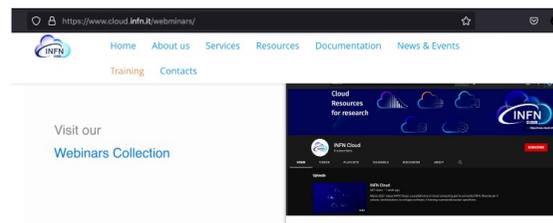
- **Webinars:**

- Tutte le guide hanno un webinar

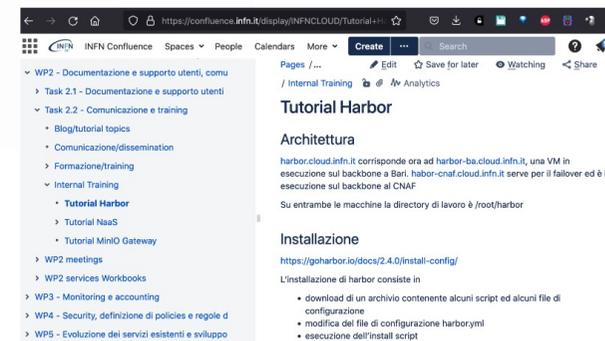
- **NEW – Formazione Interna**

- Come parte del processo di messa in **produzione** di **nuovi servizi** vengono organizzati seminari interni per i gruppi di **gestione operativa** e **supporto**
- Fino ad ora: Harbor, NaaS, MinIO Gateway

- **Good & Bad: Ogni servizio deve avere almeno 3 gestori => molto difficile trovarli**



- Available webinars:
- Introduction to INFN Cloud
 - Getting Started
 - HowTos
 - Ssh key deployment
 - VM with persistent storage
 - Kubernetes
 - Deployment di Spark + Jupyter su INFN Cloud
 - Container deployment through INFN Cloud dashboard
 - Docker compose via INFN Cloud dashboard
 - Elasticsearch + Kibana deployment via INFN Cloud dashboard
 - INFN Cloud Notebook as a Service
 - ...and much more on the youtube channel
 - Use Cases : Cygno (Giovanni Mazzetti)



Monitoring and Accounting - WP3 -





Obiettivi e task di WP3

- Monitoraggio
 - Infrastruttura (BACKBONE) e relativi servizi ancillari
 - Servizi cloud (PaaS)
 - Risorse per Cloud Federata
 - Servizi utente
- Dashboard di Progetto
 - Visualizzazione di metriche di performance
- Notifiche di malfunzionamenti, degrado di performance, esaurimento risorse
- Pagina di stato con avvisi di downtime/maintenance
- Bollettino informativo periodico su stato risorse e notifiche
- Accounting
 - collezione dati su uso delle risorse (per utenti e per gruppi)

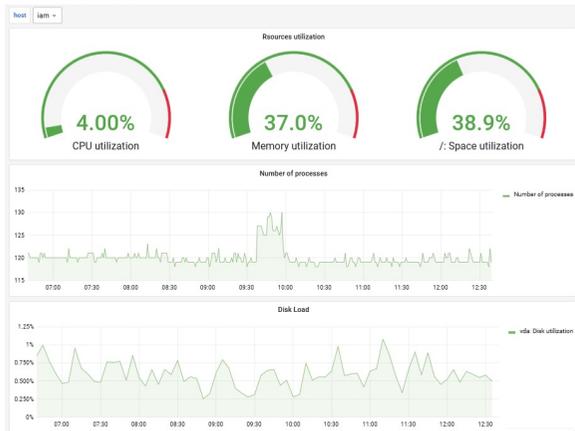
Monitoring



<https://monitoring.cloud.infn.it:3000>

<https://status.cloud.infn.it/>

Stato servizi



2022-05-21->2022-05-25 Cloud@VENETO power cut and OpenStack upgrade Maintenance due to start in 2 days

2022-05-23->2022-05-27 Cloud@CNAF at risk because of OpenStack upgrade Maintenance due to start in 4 days

1. INFN Cloud

Object Storage	Operational
Backbone - Cloud Compute (Bari)	Operational
Backbone - Cloud Compute (CNAF)	Operational
Authentication	Operational

2. Federated Cloud - CloudVeneto

CloudVeneto - Cloud Compute	Operational
-----------------------------	-------------

3. Federated Cloud - ReCaS-Bari

ReCaS-Bari - Cloud Compute	Operational
----------------------------	-------------

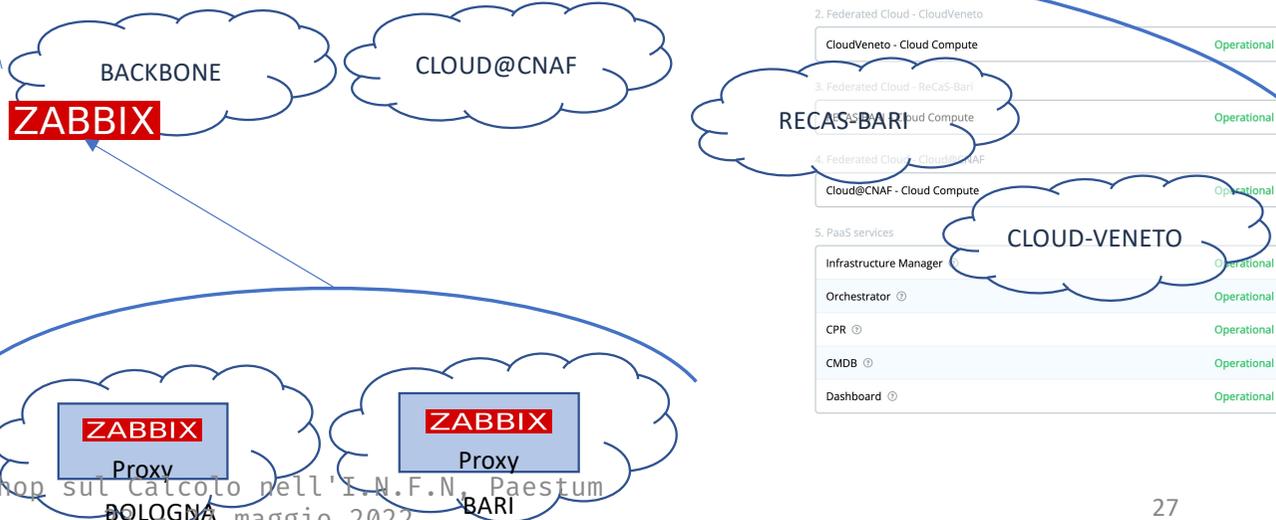
4. Federated Cloud - Cloud@CNAF

Cloud@CNAF - Cloud Compute	Operational
----------------------------	-------------

5. PaaS services

Infrastructure Manager	Operational
Orchestrator	Operational
CPR	Operational
CMDB	Operational
Dashboard	Operational

Risorse cloud di progetto



Workshop sul calcolo nell'I.N.F.N., Paestum
23-27 maggio 2022

INFN Cloud Accounting

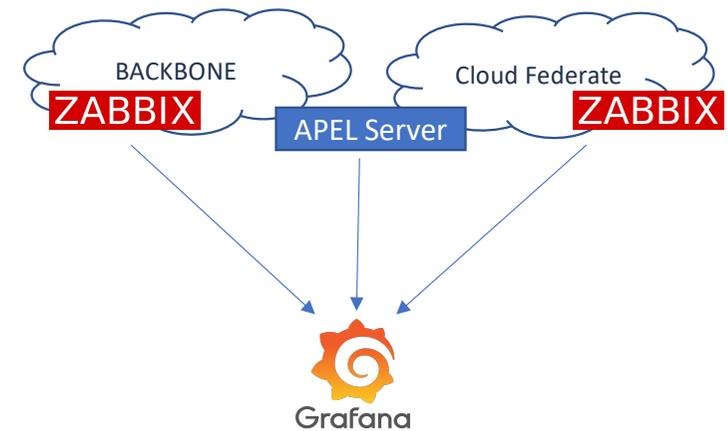


• Architettura

- Ibrida basata su
 - servizi di accounting già in produzione in EGI
 - Server: APEL (database e aggregazione dei dati), RabbitMQ (message broker)
 - Client: Collectd/cASO per la collezione delle metriche
 - ZABBIX di infrastruttura

• Visualizzazione

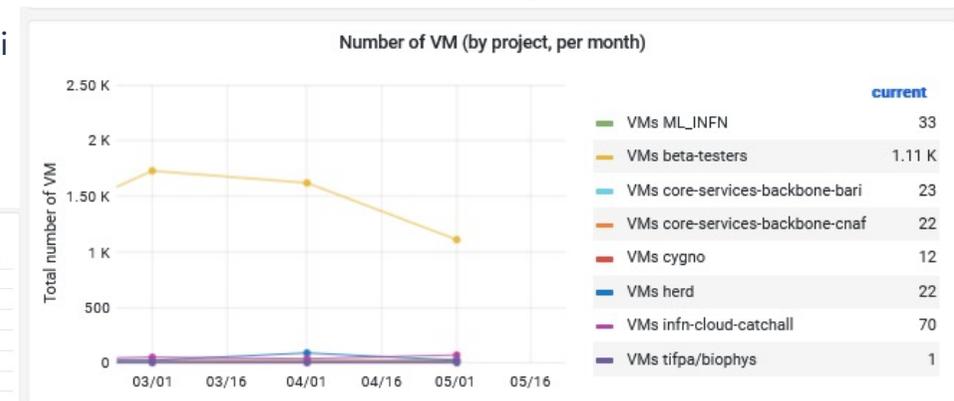
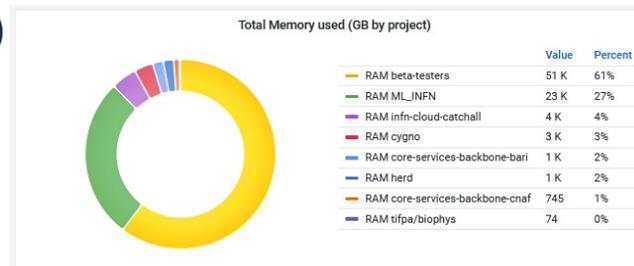
- Grafana
 - Data source: APEL (DB) + ZABBIX
 - Autenticazione via INDIGO-IAM
 - Accesso selettivo alle Dashboard
 - dati aggregati per provider (cloud federate), gruppi, utenti



<https://accounting.cloud.infn.it:3000>

• Metriche

- CPUtime, RAM, disk, numero istanze
- Volumi, IP (**new**)
- GPU (**Coming soon**)





Attività future

- Installazione in HA dell'infrastruttura di monitoring (Zabbix 6.0)
- Messa in produzione di un servizio di monitoring per le applicazioni degli utenti
- Monitoring di Availability/Reliability
- Definire e implementare un servizio di accounting user level

Security, Policies and Rules of Participation

- WP4 -



Obiettivi e task di WP4

Coordinare la sicurezza di INFN-Cloud

Stabilire le politiche di utilizzo e comportamento accettabile su INFN-Cloud

Gestire gli incidenti e monitorare la sicurezza

Design (in collaborazione con gli altri WP) di soluzioni che rispettino i requisiti di sicurezza



Risultati

- Definiti diversi documenti di policy e procedure, che vengono regolarmente aggiornati: AUP, ROP, privacy policy, regole di utilizzo.
 - Target: end user, amministratori di servizio, amministratori di siti federati
- Definite procedure per la gestione delle vulnerabilita` e degli incidenti di sicurezza (istituito a tal scopo il "Security Incident Team")
- Coordinamento degli aspetti di sicurezza e policies wrt nuovi sviluppi (es. deployment su reti private).



In collaborazione con Harmony e CCR

Accesso non privilegiato alla INFN Cloud per utenti esterni



- Contratto o Convenzione:
 - l'utente sia stato opportunamente identificato, attraverso un identity provider riconosciuto dall'INFN (es. attraverso un sistema di identity federation come quelli usati nelle infrastrutture WLCG o EGI);
 - l'utente sia membro della Virtual Organization (VO) a cui i servizi di INFN Cloud vengono dati in uso in base alla convenzione/accordo/contratto, e ne abbia accettato la relativa AUP;
 - l'utente abbia già seguito un corso di formazione adeguato presso l'ente di appartenenza, ovvero abbia seguito il corso base sulla sicurezza informatica INFN
 - l'utente abbia accettato le AUP e i Terms of Use di INFN Cloud

Non e' necessaria la registrazione degli utenti nella INFN AAI se negli accordi di collaborazione da stipulare con le Istituzioni di provenienza siano inclusi i requisiti di riconoscimento di livello almeno equivalente al nostro (Loa2) e la garanzia di aver effettuato una formazione di base sulla sicurezza informatica

Accesso privilegiato alla INFN Cloud su risorse istanziate su rete privata per utenti esterni



Ipotesi:

- risorsa istanziata su rete privata (come da quesito)
- risorsa ad esclusivo uso personale: non deve cioè essere concesso l'accesso ad altri utenti
- risorsa che deve trattare dati di tipo tecnico-scientifico: il trattamento di dati personali non deve essere significativo

la Commissione ritiene che:

- **L'utente** deve aver seguito un corso di istruzione di livello intermedio presso l'INFN o la sua home organization.
- L'identificazione dell'utente dovrà essere LoA2.
- La risorsa dovrà essere istanziata con un meccanismo di trasmissione dei log verso un server esterno, che l'utente si impegna a non modificare. I log dovranno essere adeguatamente protetti e conservati per almeno sei mesi
- A carico del **gestore cloud**
 - La risorsa dovrà essere costantemente monitorata dall'esterno e sottoposta a scansioni alla ricerca di vulnerabilità.
 - Dovrà essere mantenuto e tenuto aggiornato un elenco degli utenti che hanno avuto accesso alla risorsa.

Security Incident Team (SIT)



- Team di 6 persone che opera in shift
- Monitoraggio (via scansioni continue e automatiche) dello stato di INFN-Cloud
- Valutazione delle vulnerabilita' segnalate da qualunque fonte e relativa gestione del problema
 - In modo da sanare i deployment attivi
 - In modo che non vengano creati nuovi deployment vulnerabili
- Gestione degli incidenti (finora non ce ne sono stati)
 - In collaborazione con lo CSIRT di INFN

Service Evolution and New Developments - WP5 -





Obiettivi e task di WP5

Sviluppo, porting e co-design e R&D di soluzioni tecniche user-level per utenti e comunità scientifiche, finalizzate a facilitare l'accesso alle risorse di computing e di storage, incluso eventualmente accesso ad hardware specializzato (i.e. GPU ...)

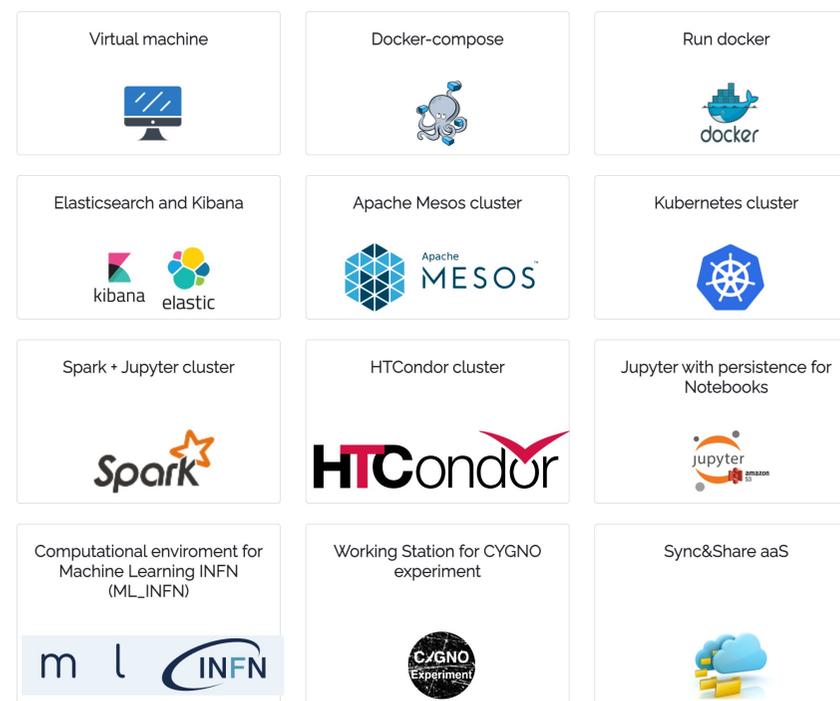
Le attività sono organizzate in due macro aree: **evoluzione dei servizi core** della PaaS e allo **sviluppo dei servizi di alto livello**

- **Forte sinergia con gli altri WP** per coordinare: onboarding di nuovi use-case/comunità, preparazione della documentazione dei servizi di alto livello, monitoraggio dello stato dei servizi core e delle vulnerabilità dei servizi di alto livello, gestione degli aggiornamenti della PaaS e dei servizi di alto livello, etc.
- **Manutenzione dei servizi implementati:** bug fixing, vulnerabilità, ed estensione di funzionalità
- **Documentazione: testing e sviluppo di documentazione, benchè meno appealing, sono di fondamentale importanza!**

Risultati: il catalogo dei servizi



- Abbiamo sviluppato e messo a disposizione **12 servizi** di alto livello tra cui:
 - **ambienti di sviluppo interattivi, dinamici, multi-utente, basati su Jupyter Notebook**
 - Facilmente customizzabili in base alle esigenze
 - Soluzioni integrate pre la persistenza dei dati
 - **ambienti di calcolo per l'esecuzione di job in modalità batch** (basati su cluster HTCondor)
 - Integrazione con soluzioni di data access
 - **accesso allo storage con modalità diverse** (posix, S3) a seconda degli use-case
- Abilitato un notebook as a service
 - Esempio di sinergia tra WPs



Il catalogo è costruito a partire da componenti modulari altamente configurabili.

Risultati: nuove funzionalità



- L'Orchestrator e gli altri componenti della PaaS sono stati modificati ed estesi per **migliorare le capacità di federazione dei siti e di scheduling dei deployment.**
- Highlights:
 - **Disk QoS:** È possibile richiedere volumi di diverso tipo (p.e. in base alla replica, performance, etc.);
 - **Acceleratori:** è possibile scegliere il modello per le GPU;
 - **Networking:** è possibile configurare le porte aprendole solo verso subnet o ip specifici;
 - **Security:** è possibile creare deployment su rete private (accessibile tramite VPN con autenticazione IAM)
- Dashboard evolution:
 - Obiettivo è semplificare l'interazione utente-PaaS nella gestione di parametri di configurazione dei template (TOSCA) i.e. prendendo automaticamente authN information, etc.



Lessons learnt

- Stiamo facendo attività di co-design con le prime comunità/sigle. In particolare CSN2 -> CYGNO, HERD (ma anche AMS, FERMI); CSN5 : ML_INFN. Questo è di estremo valore e va potenziato perchè
 - Permette di guidare lo sviluppo focalizzandolo alle esigenze di esperimento (priorità)
 - Consente di implementare una "code base" generica
 - Specializzando solo l'ultimo miglio
 - Facilita il riuso di componenti e soluzioni già disponibili
 - Facilita il knowledge transfer (in ambo i sensi!)
- Ovviamente questo ha un costo e richiede effort su entrambe i fronti. Non ultimo la creazione di documentazione tecnica fruibile
 - A tendere pensiamo sia il modo più per costruire una comunità che contribuisce allo sviluppo e alla manutenzione del portfolio. In tal senso contributi e interessati, anche nello sviluppo, è assolutamente benvenuto!
 - Fornire **feedback da parte degli utenti** richiede effort, tuttavia è cruciale per migliorare l'offerta di servizi!



Lessons learnt (cont)

- E' stato implementato un ambiente (gemello) dedicato allo sviluppo e il testing di nuove soluzioni ma anche di patch, fixes etc. Questo ci permette di abilitare la fase di beta testing senza nessuna interferenza con le attività di produzione:
- Il **beta-testing**, in particolare durante questo primo anno, è stato di fondamentale importanza per migliorare i servizi offerti
 - Spesso i contributi arrivati dai power users sono stati fondamentali e molto ben ricevuti. Vanno stimulate sempre più queste interazione. Contributi sono BENVENUTI
- La **gestione delle vulnerabilità** sui servizi offerti nel catalogo è sicuramente un task non banale
 - Al momento i test vengono fatti in maniera manuale, ma stiamo mettendo a punto un sistema (basato su Jenkins) che li automatizzi il più possibile

Prossimi passi



➤ INFN Cloud: visione futura e prossime attività

INFN Cloud: visione futura e prossime attività

🕒 17:00 - 17:25

📍 Sala Saturno (Hotel Ariston)
Via Laura, 13 - Capaccio-Paestum (SA)

Presenter Davide Salomoni



Last BUT not least - People

- Bari
 - Marica Antonacci
 - Giacinto Donvito
 - Nadina Foggetti
 - Alessandro Italiano
 - Vincenzo Spinoso
 - Roberto Valentini
- CNAF
 - Alessandro Costantini
 - Andrea Ceccanti
 - Vincenzo Ciaschini
 - Doina Cristina Duma
 - Barbara Martelli
 - Diego Michelotto
 - Davide Salomoni
 - Francesco Sinisi
 - Riccardo Veraldi
 - Stefano Zani
- Padova
 - Federica Fanzago
 - Sergio Traldi
 - Massimo Sgaravatto
 - Marco Verlato
- Perugia
 - Diego Ciangottini
 - Mirco Tracolli
 - Daniele Spiga
- Bologna
 - Gianluca Peco
 - Paolo Veronesi
- LNGS
 - Stefano Stalio
- LNS
 - Emidio Giorgio
- Torino
 - Luciano Gaido
- Trieste
 - Lucio Strizzolo

A big **thank you** also to the INFN Cloud users, scientific collaborations, to the INFN management and to all those who provided very useful feedbacks. Keep them coming!