INFN Cloud: l'infrastruttura

Stefano Stalio - Diego Michelotto

06/03/2025

Indice

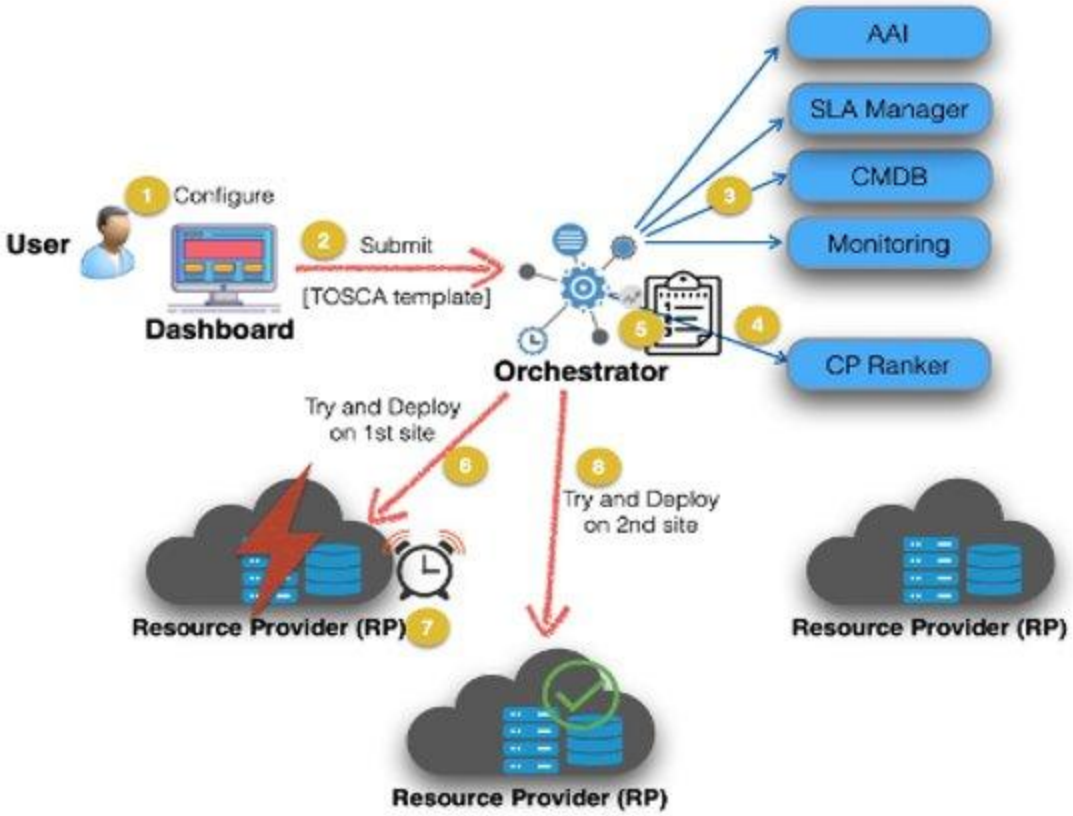
- INFN Cloud
  - Backbone
  - Provisioning
  - Monitoring
  - Accounting
- Federazione siti cloud

- Servizi
  - IAM
  - PaaS
  - FTS + Rucio
  - S3
  - NaaS
  - Container Registry
  - Monitoring
  - DNS
  - Healthchecks

INFN Cloud / Un modello federato

INFN Cloud nasce nel 2021 basandosi su un modello federato dove l'orchestratore di Indigo DataCloud rappresenta il punto di accesso unico a risorse eterogenee distribuite sui data center dell'INFN e dove lo IAM di Indigo DataCloud è lo strumento che accentra le funzionalità di autenticazione ed autorizzazione degli utenti.

Questo modello si estende oggi, in **INFN DataCloud** ai progetti ICSC e TeraBit, ed a data center di istituzioni diverse



INFN Cloud

- Infrastruttura Cloud distribuita che si basa sul Backbone
  - Core Services e SaaS
- Federa le infrastrutture cloud dei vari siti INFN
  - PaaS, con gestione Quote, SLA, ecc…
- Base per il DataLake INFN
  - Offre storage per storage personale a staff INFN
  - Mette a disposizione gli strumenti per il data management per i dati di esperimento

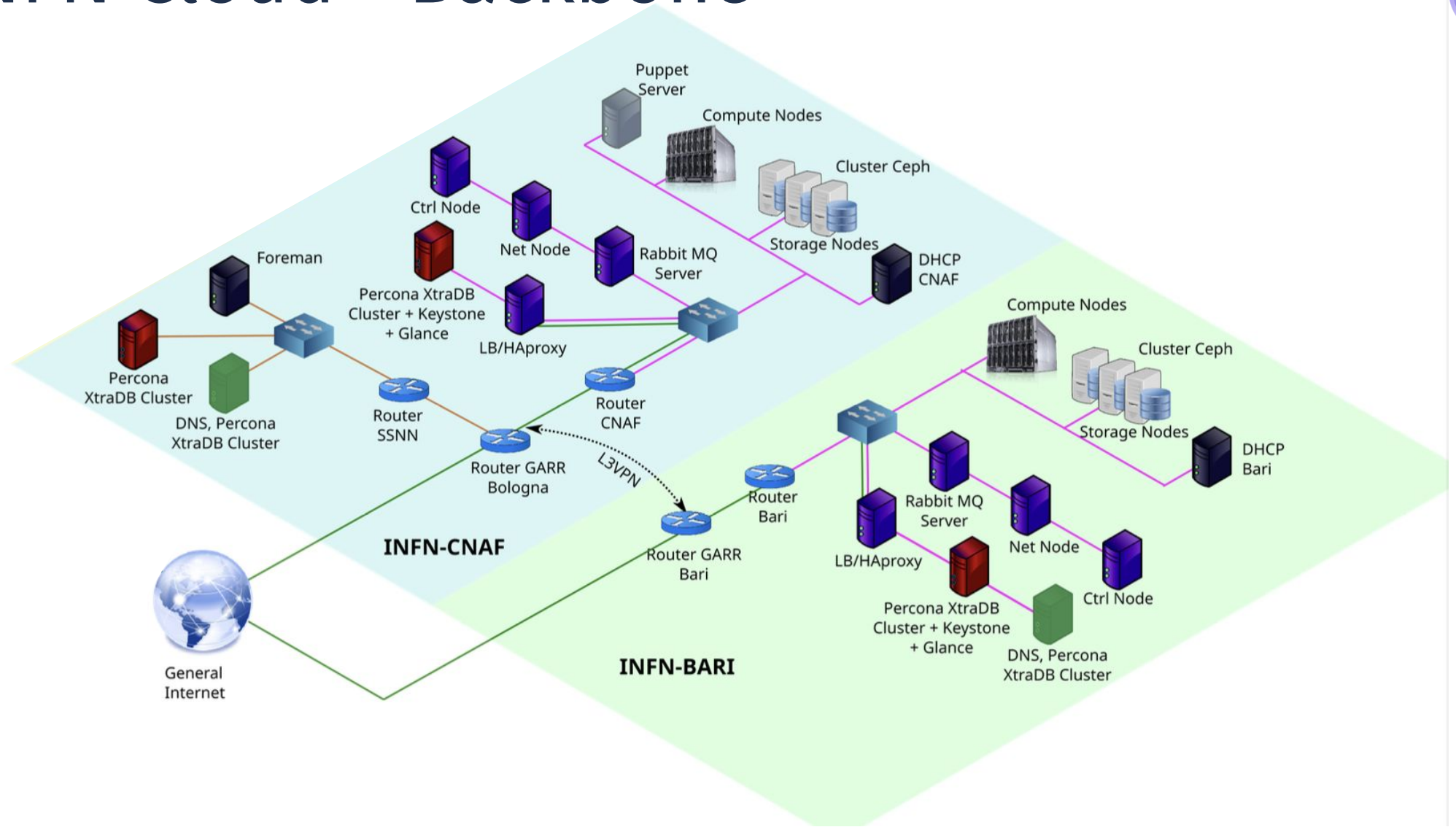
INFN Cloud - Backbone

- Core per INFN Cloud
- Infrastruttura distribuita su 2 sedi INFN, dette regioni
  - Bari e CNAF + VM sui SSNN per cluster che necessitano del quorum
  - Infrastruttura di rete basata su L3VPN del GARR per rendere «vicini» i due siti
- Basata su software open source OpenStack di tipo IaaS
  - Immagini
  - Self-service network
  - VM
  - Volumi (HDD, SSD)
- Base per PaaS e SaaS

Federazione / Ruolo del backbone

- **Il “backbone di INFN Cloud”**, una cloud OpenStack distribuita su due data center, **è l’infrastruttura dedicata ad ospitare i servizi centrali di INFN Cloud**, **le attività di R&D, i testbed, le risorse dedicate alla formazione**.
- Per quel che riguarda lo storage ad oggetti S3, **il backbone ospita i bucket personali degli utenti** che servono da backend anche per il backup dei servizi istanziati dagli utenti stessi e per la gestione del software
- L’infrastruttura del backbone è pensata per replicare i **servizi** ed i dati sui suoi due data center in modo da renderli **resilienti a criticità gravi**, anche al down di un data center
- In una fase iniziale, con poche risorse aggiuntive, sul backbone venivano ospitati anche molti servizi degli utenti, oggi questa funzione è demandata principalmente alle cloud federate anche a causa di un problema di performance del block storage, problema che è in via di risoluzione

INFN Cloud - Backbone



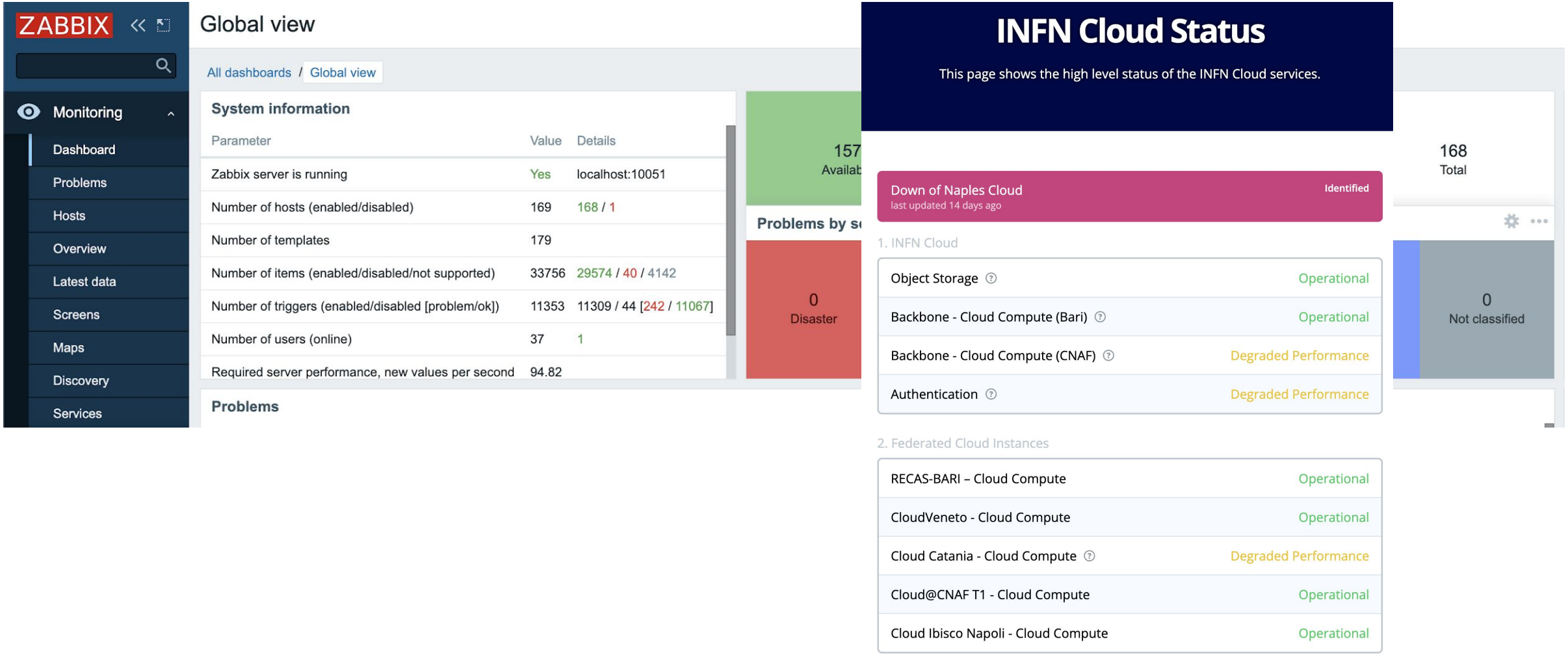
INFN Cloud - Provisioning

- Tutti i servizi «core» di IaaS, PaaS e SaaS sono installati, configurati, gestiti e monitorati tramite tool automatici
  - HW: Foreman e Puppet
  - Servizi IaaS: Foreman e Puppet
  - Servizi PaaS: Puppet e Ansible
  - Servizi SaaS: Puppet e Ansible
- Riproducibilità delle installazioni
- Monitoraggio e autocorrezione delle configurazioni delle installazioni
- Ripristino in tempi brevi in caso di fallimenti

INFN Cloud - Monitoring

- Tutto monitorato tramite Zabbix, view generale dello stato di tutta l'infrastruttura
  - Probe sviluppati internamente
  - Invia allarmi in caso di fallimento a WP1
  - View per utenti su https://status.cloud.infn.it
- Stato dell'infrastruttura Backbone e delle Cloud federate sono monitorate tramite Rally
  - Controlla le funzionalità di Openstack
    - Crea VM, creo volume, collego volume a VM, associo FIP, …
  - Invia allarmi al sito che non passa il test riportando il problema

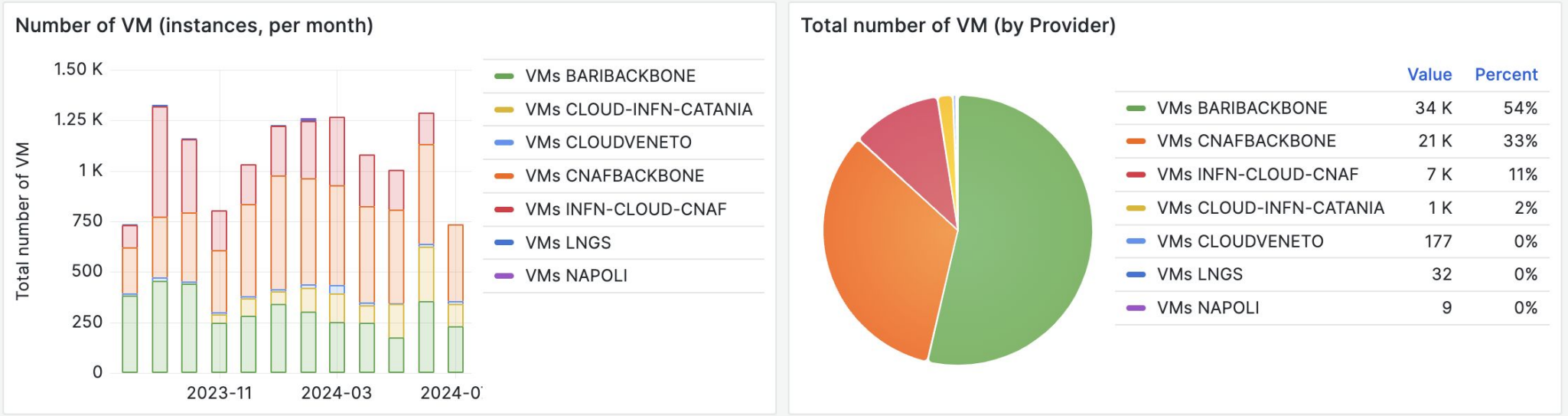
INFN Cloud - Monitoring

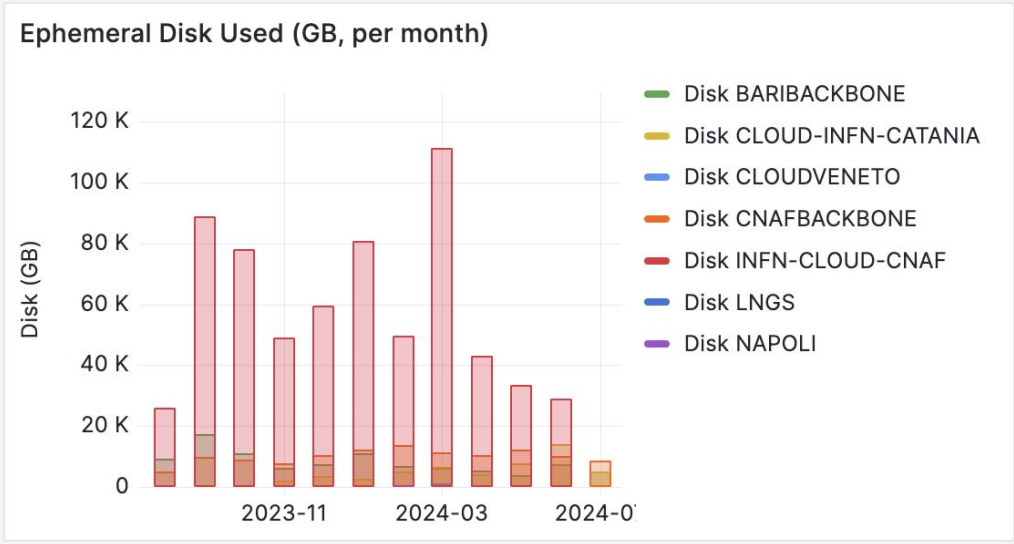


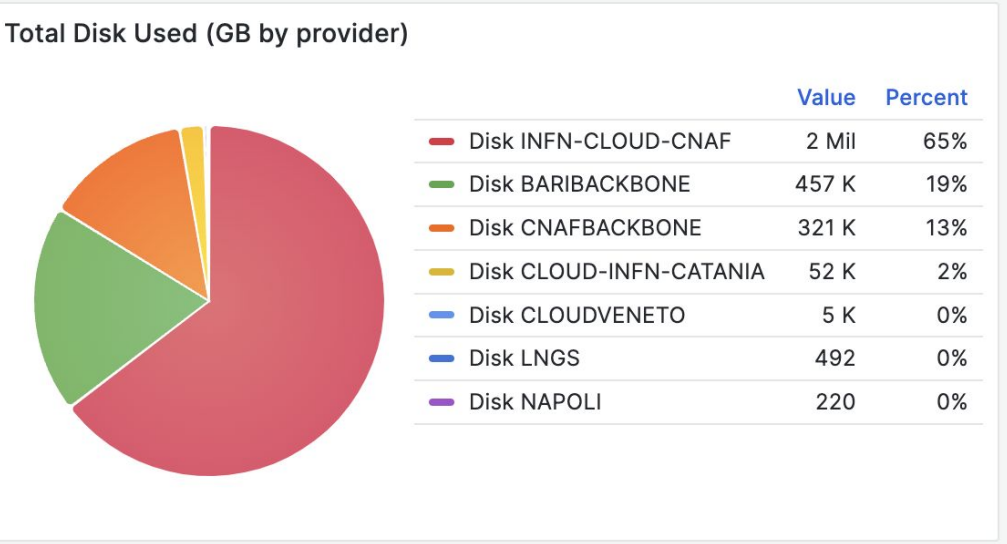
INFN Cloud - Accounting

- Raccolta centralizzata dei record sull'utilizzo delle risorse
  - Aggregati per mese in base:
    - Gruppo/esperimento
    - Utente
    - Sito
- Visualizzazione tramite Grafana
  https://accounting.cloud.infn.it:3000
- Indispensabile per capite lo stato di utilizzo delle risorse e per referaggio dei pledge per gli anni successivi

INFN Cloud - Accounting







Federazione siti cloud

- I siti INFN mettono a disposizione risorse:
  - Proprie
  - Pledged
  - Progetto (ICSC, Terabit)
- Le risorse sono disponibili tramite diversi protocolli:
  - Cloud (OpenStack, K8S, S3)
  - Grid (HTCondor-CE, Webdav, Tape REST-API)
- Le risorse vengono orchestrate dalla PaaS INFN (INDIGO- DataCLoud Orchestrator)
  - Punto di accesso unico per gli utenti
  - INFN alloca le risorse Pledge e di Progetto nei vari siti
  - La PaaS schedula le infrastrutture richieste dagli esperimenti dove quest'ultimi hanno i Pledge assegnati in maniera del tutto trasparente

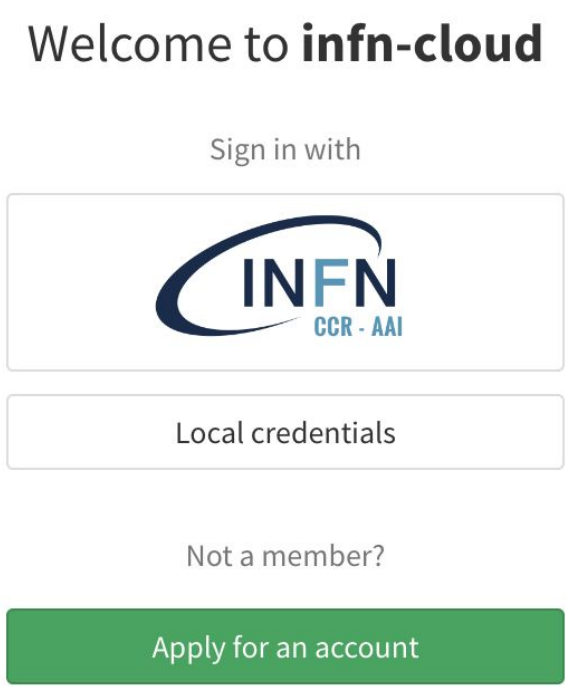
Federazione siti cloud

- Siti federati Cloud
  - Cloud@CNAF, RECAS-Bari, CloudVeneto, INFN-Catania, IBISCO-Napoli
  - Principalmente risorse Openstack (1400 VM, 4000 CPU, 16TB RAM, 380TB disco)
  - In corso federazione con tutti i T2 INFN, anche con soluzioni diverse come K8s
- Siti federati GRID
  - INFN-T1, INFN-Bari, INFN-Padova, INFN-Napoli,....
  - Principalmente federazione di Storage disco e tape
- Risorse EPIC, certificate ISO 27001, 27017 e 27018
  - EPIC Cloud (CNAF), RECAS-Bari, INFN-Catania
  - In fase di sviluppo

Servizi

- I servizi «core» sono basati sulle risorse backbone
  - Tutti i servizi che servono alla federazione
    - IAM, PaaS
  - Tutti i servizi SaaS
- Sfruttano la natura distribuita del backbone per alta affidabilità dei vari servizi

Servizi - IAM

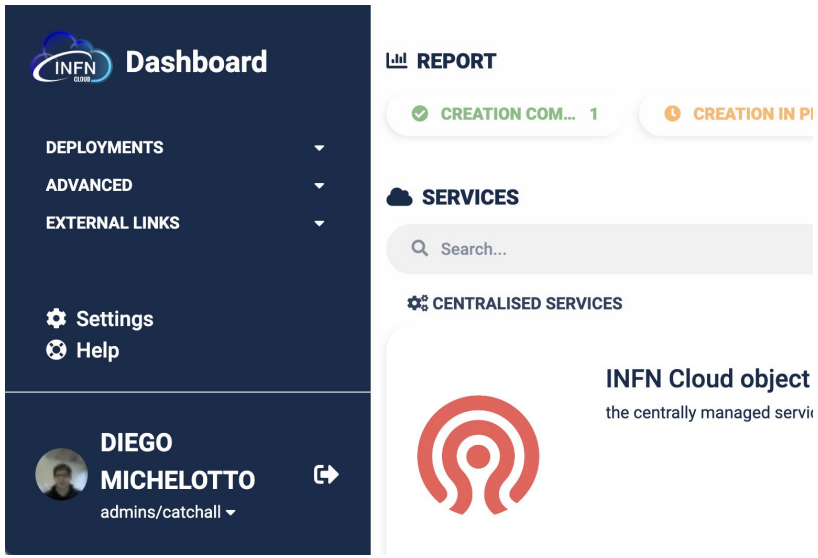


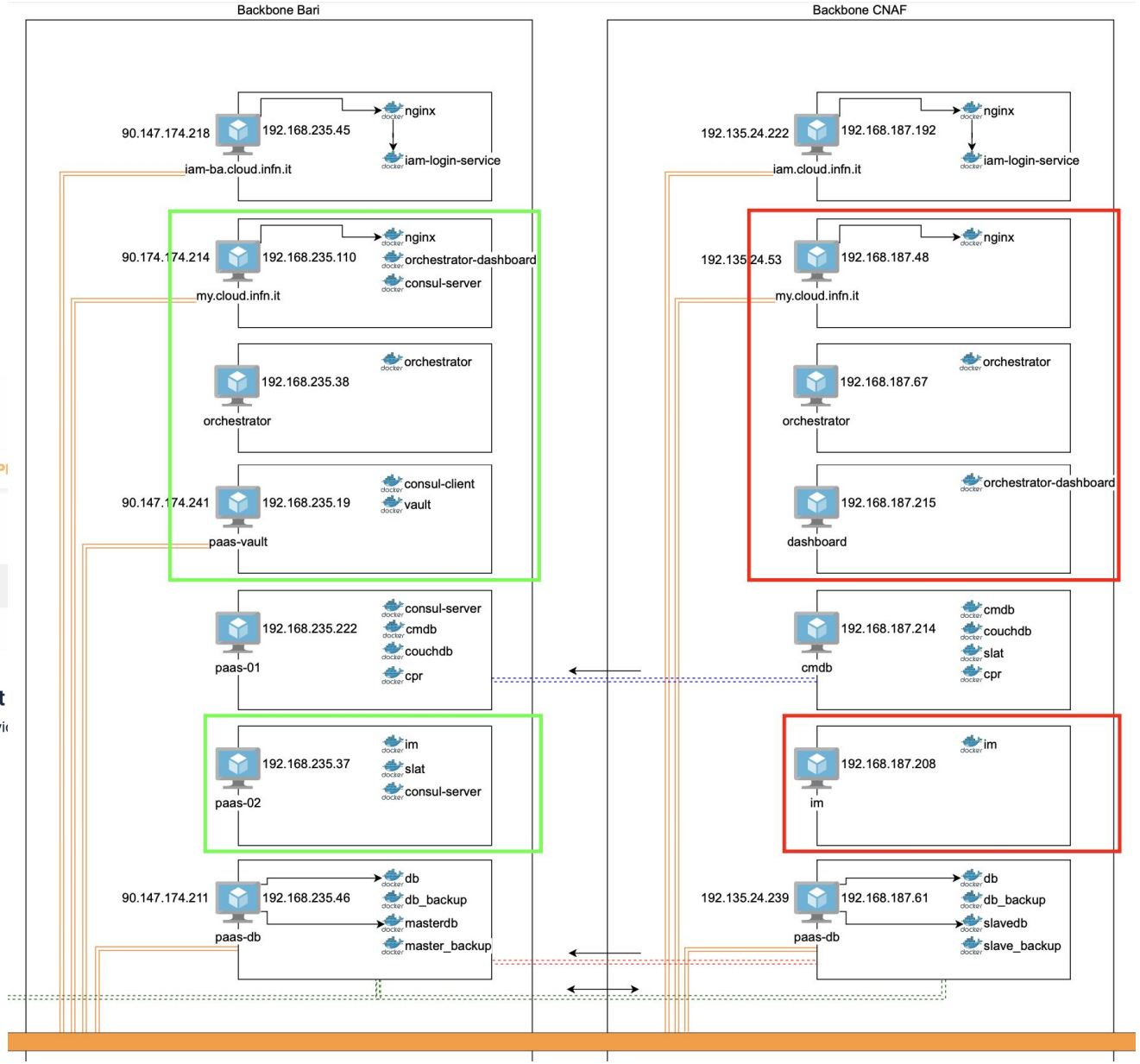
- Servizio di autenticazione per tutta INFN Cloud
  - https://iam.cloud.infn.it
  - https://iam-icsc.cloud.infn.it
- 2 istanze di cui 1 attiva sui IaaS backbone
  - 1 istanza per regione
- Failover tramite DNS
- Uso di database multi master Percona

Servizi - PaaS

- Composta da diversi servizi tra cui PaaS Dashboard (https://my.cloud.infn.it, https://icsc.cloud.infn.it) e orchestratore
- Tutti i servizi sono replicati su entrambi le regioni del backbone
- 1 sola PaaS attiva, failover tramite DNS
- Uso di diverse metodologie di replica dei database
  - Percona multi master
  - Mysql active/standby
  - CouchDB replication

Servizi - PaaS





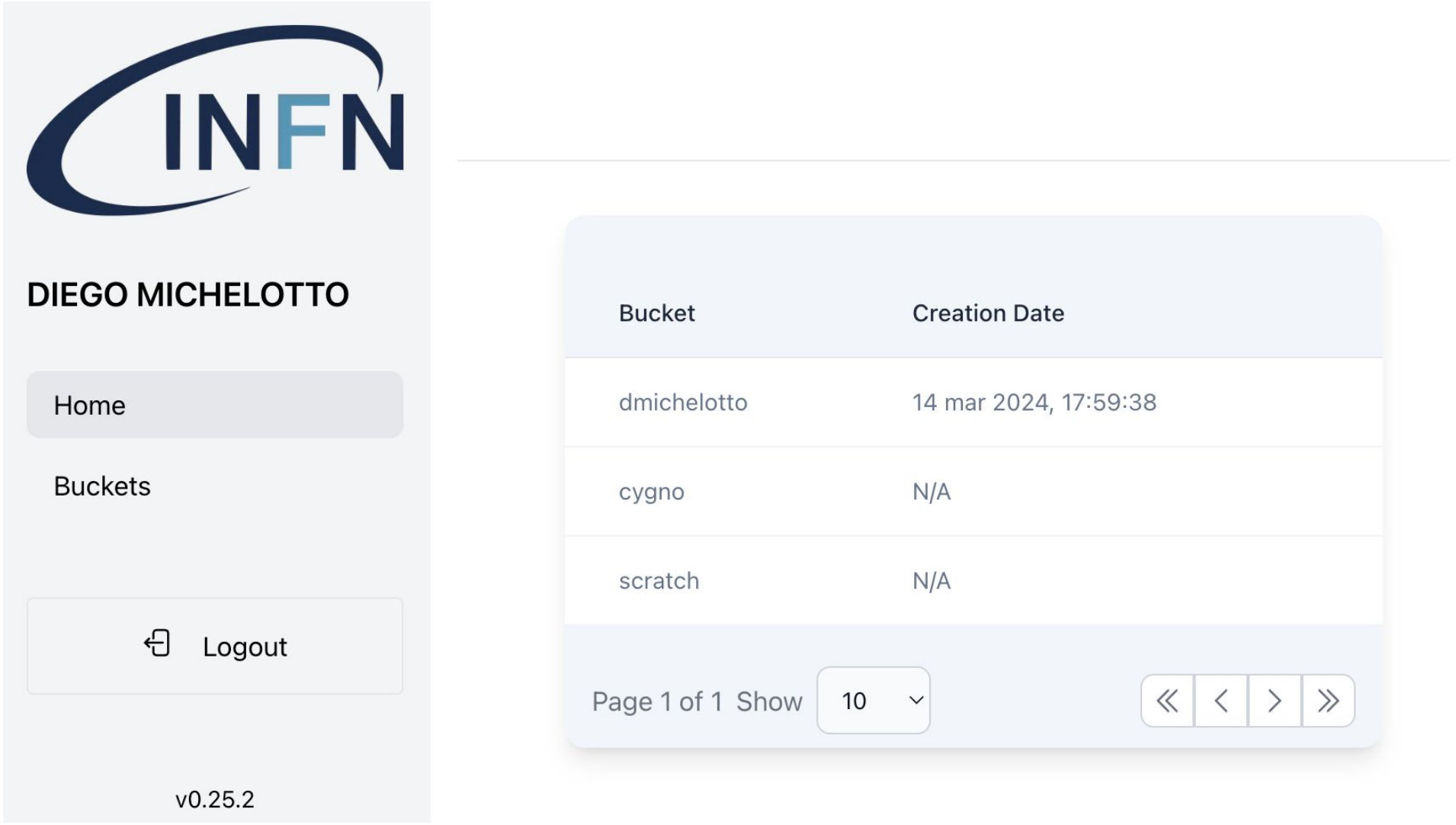
Servizi – FTS + Rucio

- FTS
  - 2 istanze attive contemporaneamente sulle 2 regioni del backbone
  - Load balancing via DNS
  - Uso di postgres su una regione con una replica sull'altra regione
    - Elezione automatica del nodo principale tramite repmgr
- RUCIO
  - In fase di deployment per l'istanza catch-all
  - 2 istanze, una per regione
  - In fase di studio per il deployment dei RUCIO di esperimento
  - Tutti i deployment di RUCIO utilizzeranno l'istanza FTS di INFN Cloud

Servizi – S3

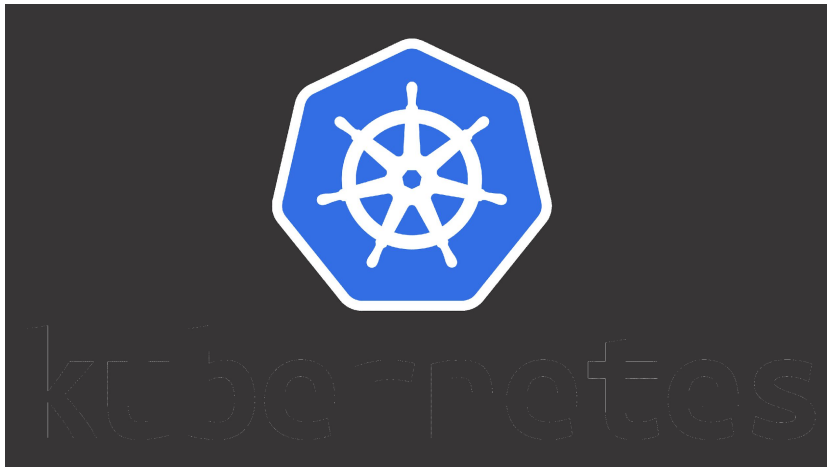
- Basato su Ceph RGW
  - Configurazione multisito, tutti i dati sono replicati su entrambi i siti del backbone in maniera automatica
  - 1 sito active, l'altro stand-by
  - Failover tramite DNS e Ceph
- Web UI per accesso ai bucket https://s3webui.cloud.infn.it
  - 2 istanze, una per sito, entrambe attive
- Usato per:
  - Bucket personali
  - Backup servizi (infrastrutturali, personali)
  - Backend per servizi (Container registry, Notebook as a Service, ecc.)
  - Sync&Share

Servizi – S3


INFN
DIEGO MICHELOTTO
Home
Buckets
Logout
v0.25.2
Bucket
Creation Date
dmichelotto
14 mar 2024, 17:59:38
cygno
N/A
scratch
N/A
Page 1 of 1 Show
10

Servizi - NaaS

- 2 cluster K8s, uno per ogni regione
- Utente tramite la PaaS richiede l'esecuzione di un Jupyter Notebook che lo istanzia su uno dei due cluster
- Vedi prossime presentazioni



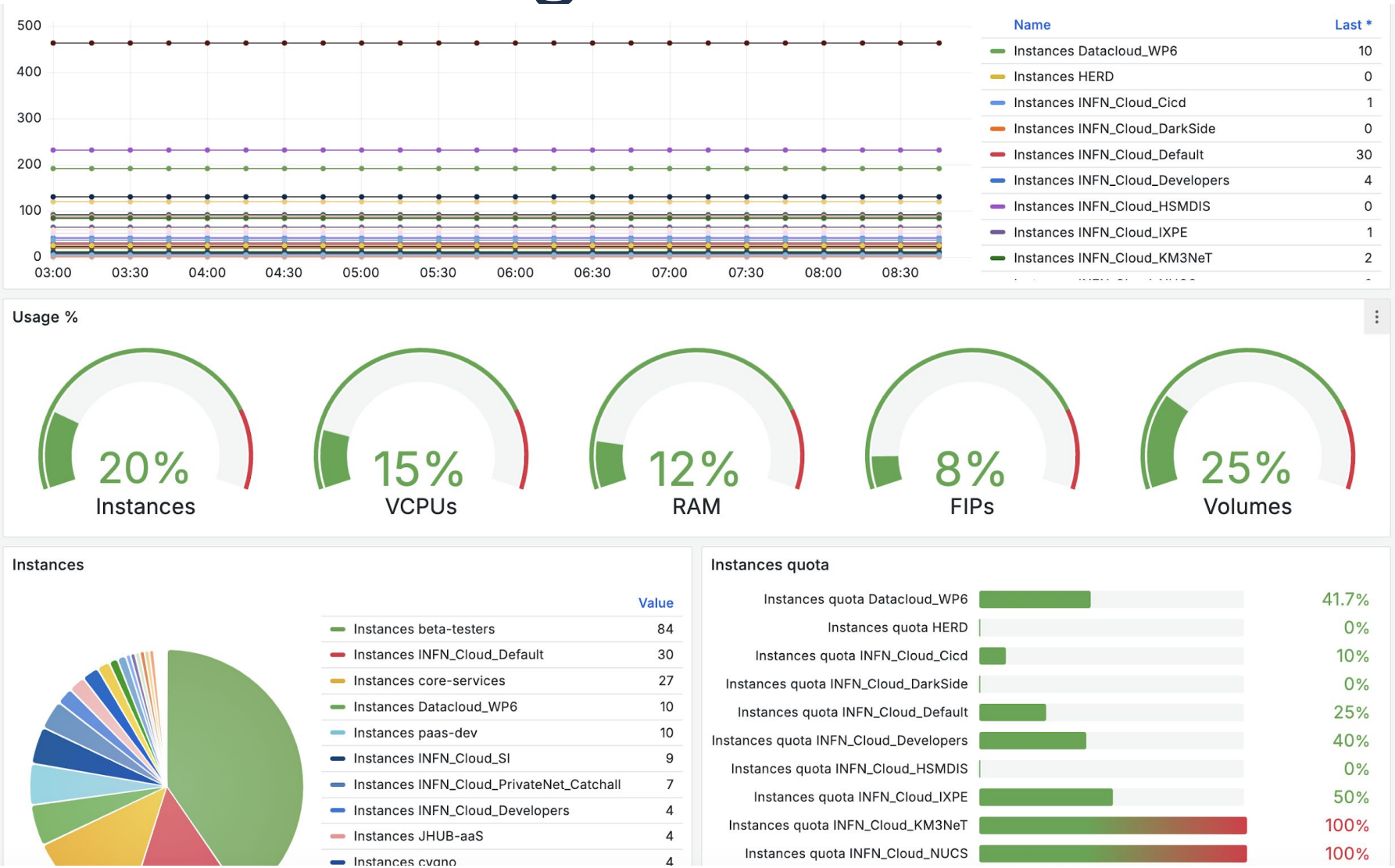
Servizi – Container Registry

- Servizio basato su Harbor
- 2 istanze, una per ogni regione del backbone
- 1 istanza attiva
- Failover tramite DNS
- Usano S3 come backend, le stesse immagini sono disponibili su entrambe le istanze, inoltre i dati sono replicati su entrambi i siti

Servizi - Monitoring

- Istanza di Grafana che presenta le informazioni sull'utilizzo delle risorse dei vari gruppi/esperimenti
- Su richiesta si possono richiedere dashboard particolari
- Backend mysql con backup su S3

Servizi - Monitoring



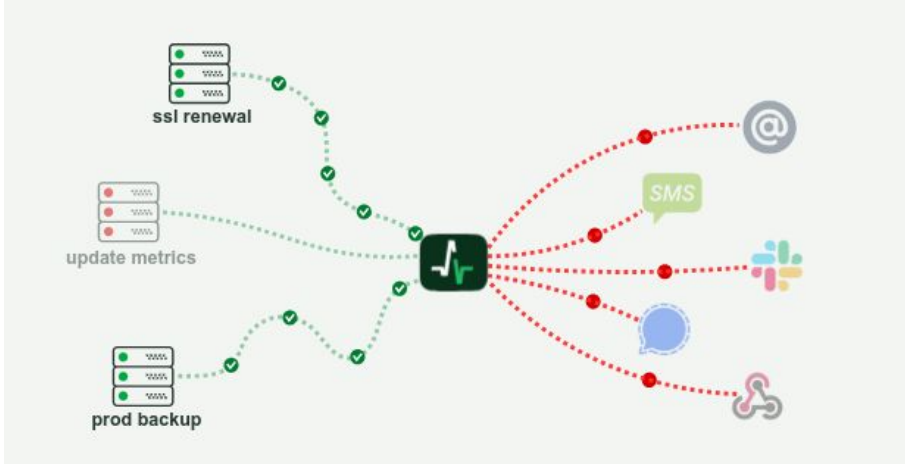
Servizi - DNS

- Wildcard DNS basato su xip.io, in fase di transizione di verso nip.io
- Si base su power dns con backend database percona multi master, distribuito sui due siti
- Tutte le macchine posso essere indirizzate come <NOME ARBITRARIO>.<IP>.myip.cloud.infn.it
- Possibile richiedere un dominio dedicato per gruppo/esperimento
- I deployment della PaaS sono indirizzati tramite questo DNS

nip.io

Servizi - Healthchecks

- Applicazione di monitoring basata su sul software di healthchecks.io
- Disponibile su https://healthchecks.cloud.infn.it
- Creazione di alert in modalità self service
- Propedeutico all'uso degli strumenti che verranno offerti per il backup, in fase di documentazione e test



Conclusioni

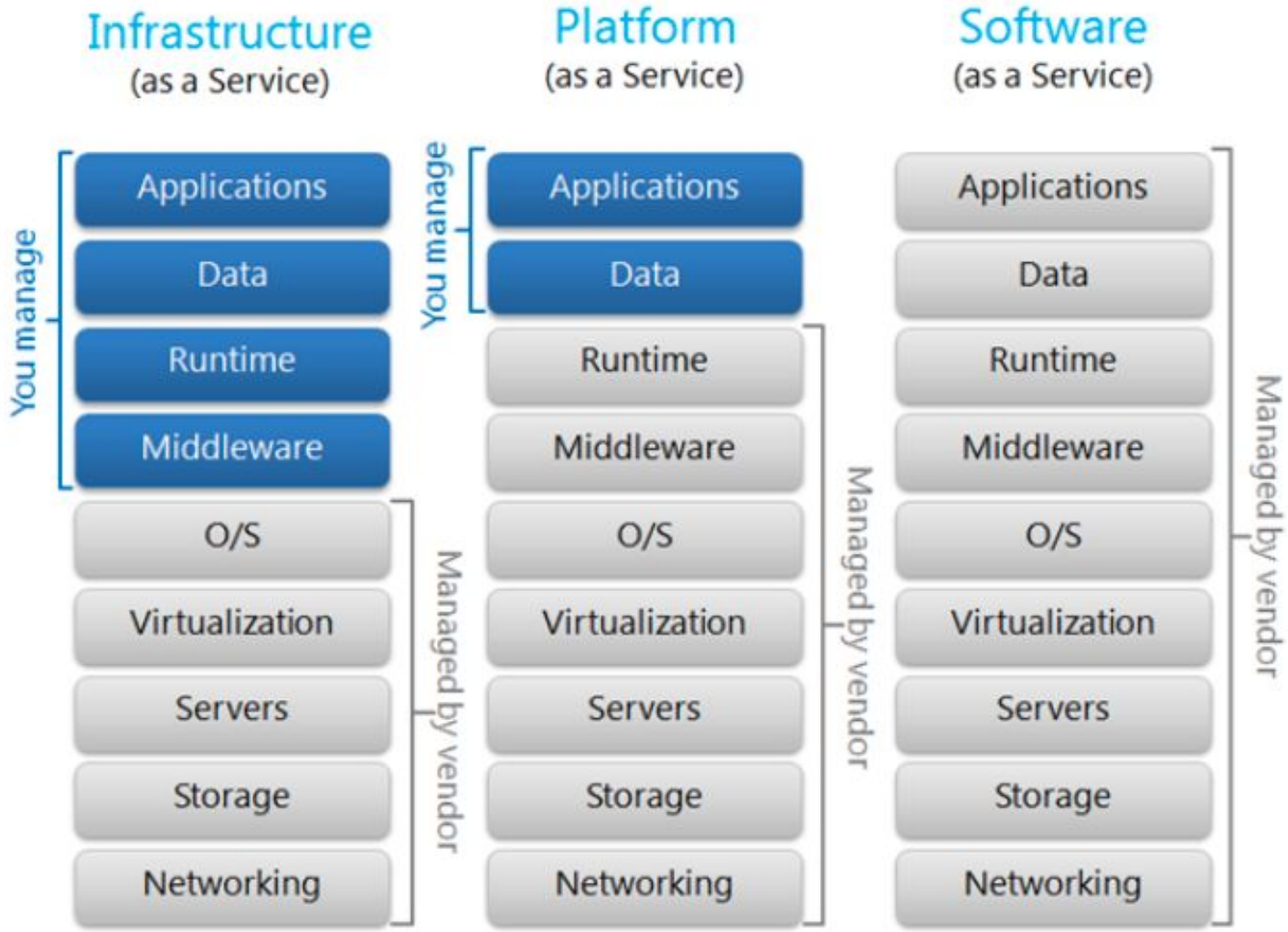
- Molti servizi a tutti i livelli, IaaS, PaaS e SaaS
- Attenzione sull’alta disponibilità dei servizi
- Presto in arrivo altri servizi, ora in fase prototipale
  - Backup as a Service
  - CVMFS as a Service

Backup slides

Cloud computing

- La definizione del NIST (Nastional Institute of Standards and Technology): Fornitura di tecnologia di informazionee comunicazione (ICT) come servizio
- Si può differenziare in base:
  - al livello di gestione demandata all'utente IaaS, PaaS e SaaS
  - alla tipologia di deployment Public, Hybrid, Private o Cummunity
  - Al tipo di isolamento delle risorse Dedicated o Multi-tenant

Cloud computing IaaS, PaaS, SaaS



Cloud computing IaaS, PaaS, **SaaS**

- Cloud application services or “Software as a Service” (SaaS) are probably the most popular form of cloud computing and are easy to use. SaaS uses the Web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients’ side. Most SaaS applications can be run directly from a Web browser, without any downloads or installations required. SaaS eliminates the need to install and run applications on individual computers. With SaaS, it’s easy for enterprises to streamline their maintenance and support, because everything can be managed by vendors: applications, runtime, data, middleware, O/S, virtualization, servers, storage, and networking. Gmail is one famous example of an SaaS mail provider.

Cloud computing IaaS, **PaaS**, SaaS

- The most complex of the three, cloud platform services or “Platform as a Service” (PaaS) deliver computational resources through a platform. What developers gain with PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective, eliminating the need to buy the underlying layers of hardware and software. One comparison between SaaS vs. PaaS has to do with what aspects must be managed by users, rather than providers: With PaaS, vendors still manage runtime, middleware, O/S, virtualization, servers, storage, and networking, but users manage applications and data.
- PaaS provides the computing infrastructure, the hardware, and the platforms that areinstalled on top of the hardware. Similar to the way that you might create macros in Excel, PaaS allows you to create applications using software components that are controlled by a third-party vendor. PaaS is highly scalable , and users don’t have to worry about platform upgrades or having their site go down during maintenance. Users who benefit most from PaaS include companies who want to increase the effectiveness and interactivity of a large staff. For the needs of larger companies and independent software vendors, Apprenda is one provider of a private PaaS for .Net business-application development and deployment.

Cloud computing **IaaS**, PaaS, SaaS

- Cloud infrastructure services, known as “Infrastructure as a Service” (IaaS), deliver computer infrastructure (such as a platform virtualization environment), storage, and networking. Instead of having to purchase software, servers, or network equipment, users can buy these as a fully outsourced service that is usually billed according to the amount of resources consumed. Basically, in exchange for a rental fee, a third party allows you to install a virtual server on their IT infrastructure. Compared to SaaS and PaaS, IaaS users are responsible for managing more: applications, data, runtime, middleware, and O/S. Vendors still manage virtualization, servers, hard drives, storage, and networking. What users gain with IaaS is infrastructure on top of which they can install any required platforms. Users are responsible for updating these if new versions are released.

Cloud computing Private, Hyprib, Public, Community

- Public cloud (off-site and remote) describes cloud computing where resources are dynamically provisioned on an on-demand, self- service basis over the Internet, via web applications/web services, open API, from a third-party provider who bills on a utility computing basis.
- A private cloud environment is often the first step for a corporation prior to adopting a public cloud initiative. Corporations have discovered the benefits of consolidating shared services on virtualized hardware deployed from a primary datacenter to serve local and remote users.
- A hybrid cloud environment consists of some portion of computing resources on-site (on premise) and off-site (public cloud). By integrating public cloud services, users can leverage cloud solutions for specific functions that are too costly to maintain on-premise such as virtual server disaster recovery, backups and test/development environments.
- A community cloud is formed when several organizations with similar requirements share common infrastructure. Costs are spread over fewer users than a public cloud but more than a single tenant.

Cloud computing Dedicated, Multi-tenant

- I modelli di isolamento nel Cloud (spesso ignorati) sono importanti e si dividono in:
  - Infrastrutture dedicate
  - Infrastrutture “multi-tenant” (con diversi [tipi di] clienti)
- Il tipo di isolamento è importante per molti aspetti, come:
  - Segmentazione delle risorse
  - Protezione dei dati
  - Sicurezza delle applicazioni
  - Auditing
  - Disaster recovery