MARICA ANTONACCI (INFN BARI)
PER IL TEAM DI INFN CLOUD

EVOLUZIONE E UTILIZZO DELLA PAAS NELL'INFRASTRUTTURA DISTRIBUITA INFN CLOUD

FOCUS SUI NUOVI SVILUPPI E SERVIZI PER GLI UTENTI

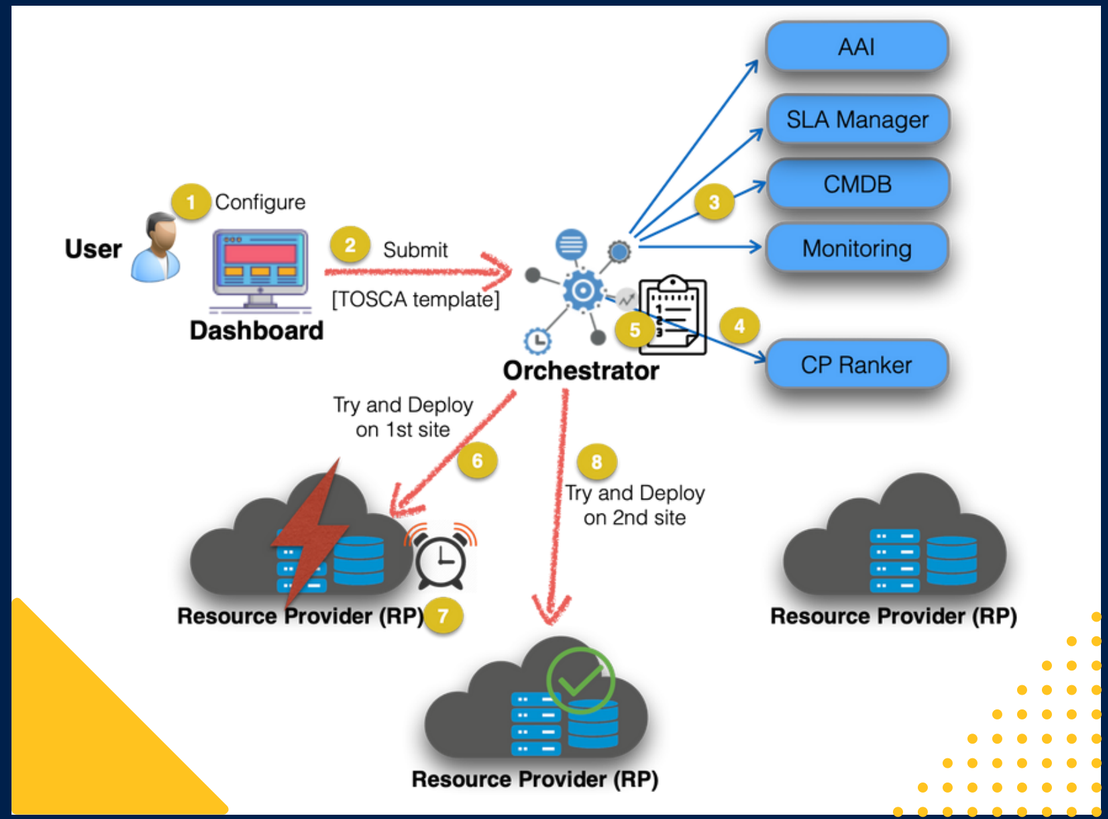
WORKSHOP SUL CALCOLO NELL'INFN - LOANO, 22-26 MAGGIO 2023

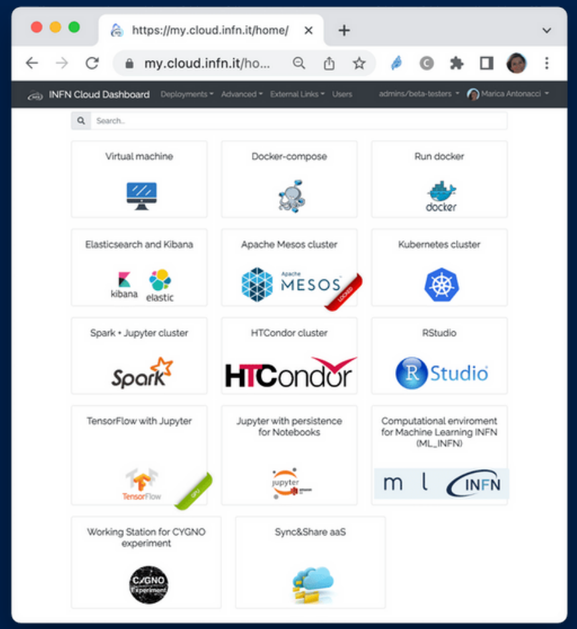
FEDERAZIONE DINAMICA DI RISORSE

attraverso l'ORCHESTRATORE PaaS

che implementa funzionalità di federazione di infrastrutture cloud distribuite e di scheduling.
La federazione INFN Cloud oggi include:

- Backbone sulle sedi di CNAF e Bari
- Cloud federate: ReCaS-BARI, Cloud@CNAF, CloudVeneto. In corso la federazione di Cloud CT.



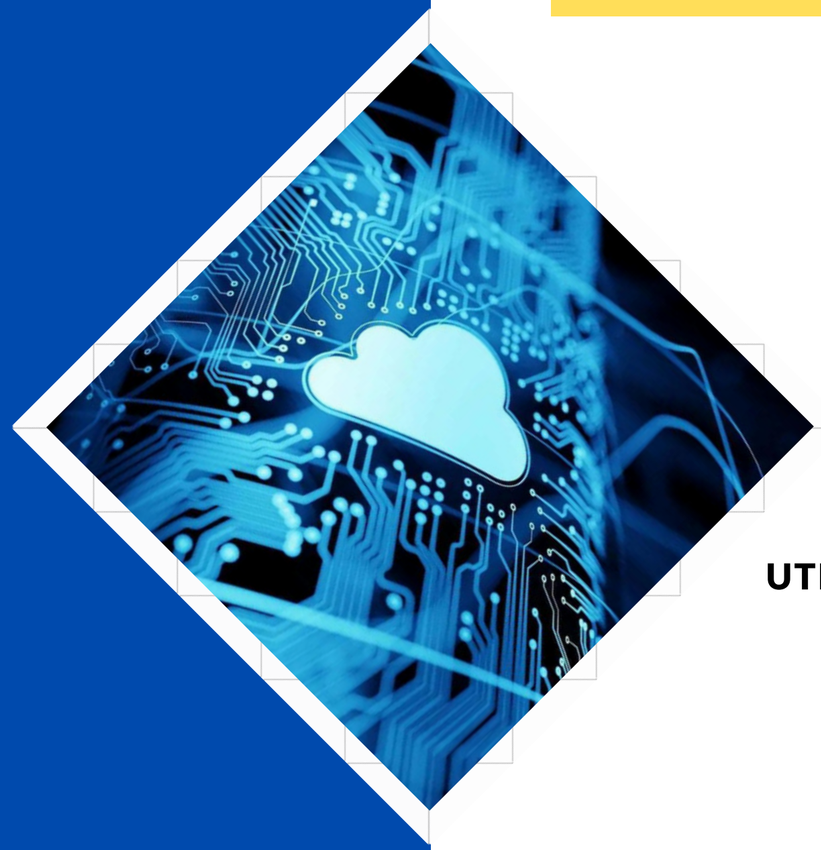


ACCESSO DIRETTO AL PORTFOLIO DEI SERVIZI

attraverso la dashboard di INFN Cloud

Il portale web rappresenta il punto di accesso ai servizi del portfolio di INFN Cloud ed offre un'interfaccia intuitiva e user-friendly

IN DUE ANNI DI PRODUZIONE



2580

RICHIESTE DI DEPLOYMENT

135

UTENTI HANNO CREATO ALMENO UN DEPLOYMENT

14

PROGETTI

+ TRAINING

USATO PER CORSI DI FORMAZ.

+ BETA-TESTERS

USATO PER SVILUPPO E TEST

232

DEPLOYMENT ATTIVI

69% CATCHALL

9% ML-INFN

5% CYGNO

3% HERD

LA DASHBOARD

l'interfaccia web che trasforma la gestione dei deployment in un'esperienza fluida e senza sforzo

Autenticazione basata su OpenID-Connect

La dashboard implementa il supporto per provider di tipo OpenID-Connect, in particolare INDIGO IAM

Multi-tenancy

Gli utenti sono organizzati in gruppi. L'appartenenza a uno o più gruppi è propagata da IAM attraverso il token e sfrutatta per l'autorizzazione in tutto lo stack

Gestione dei secrets

La dashboard è integrata con Hashicorp Vault per la gestione dei secrets dei deployment (p.e. chiavi ssh, encryption keys, etc.)

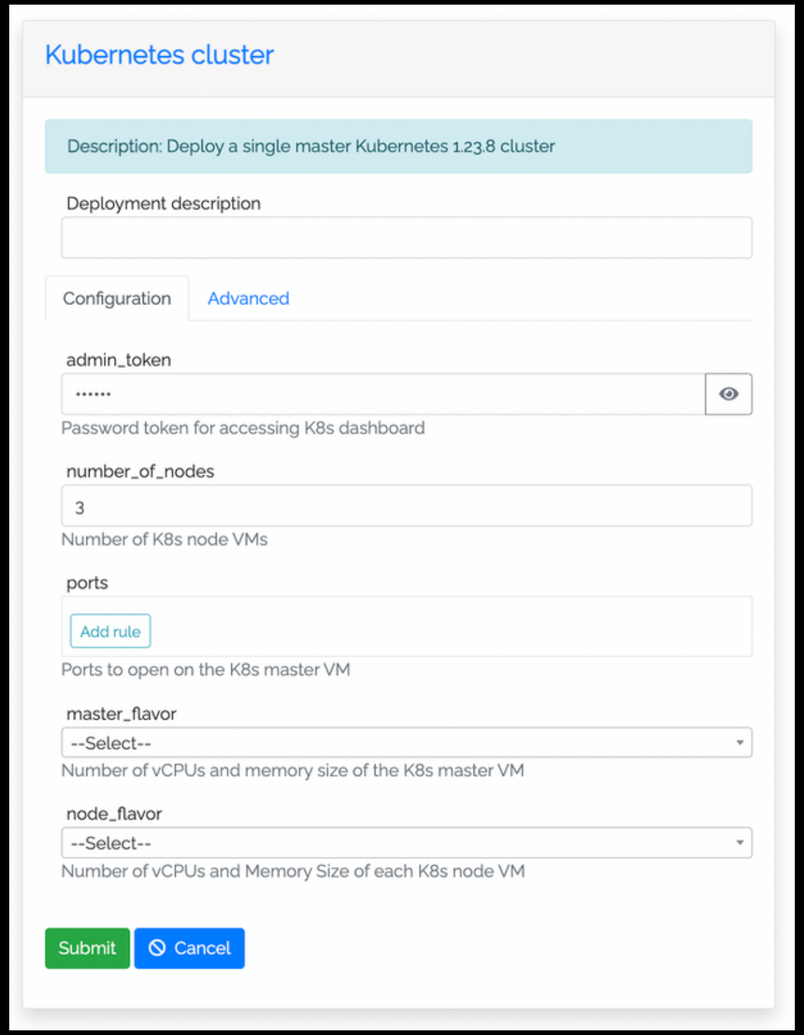
Catalogo dinamico dei servizi

Nuovi servizi possono essere aggiunti facilmente nella dashboard, semplicemente caricando nuovi template nel repository configurato

Paper IWSG2022: https://doi.org/10.5281/zenodo.7883082

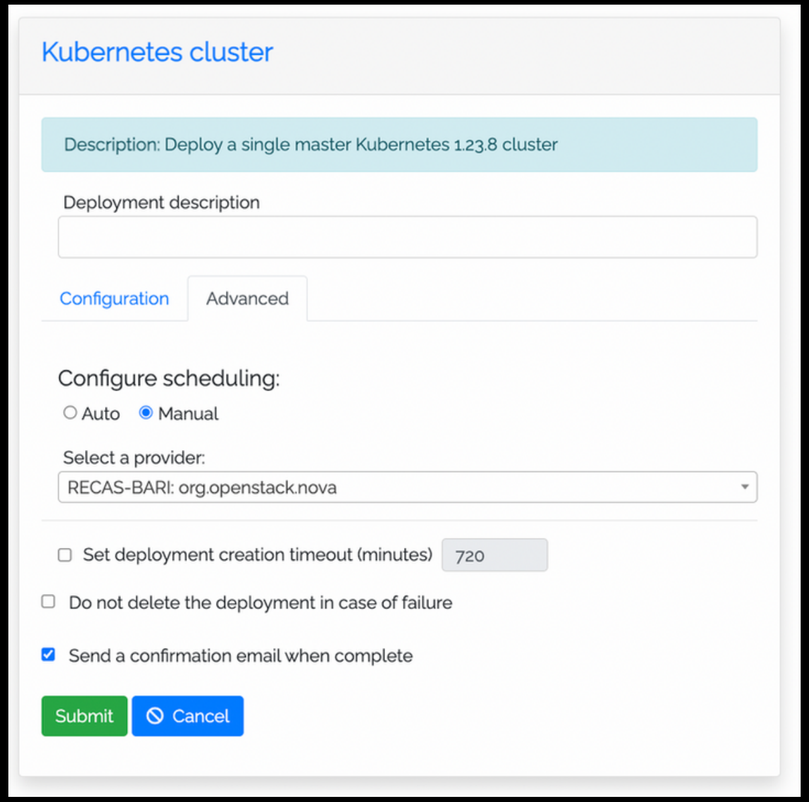
Richiedi un servizio *(anche complesso come un cluster k8s)* in pochi click

Personalizza il tuo deployment
tramite i parametri di input nel form di configurazione



Scegli la strategia di scheduling

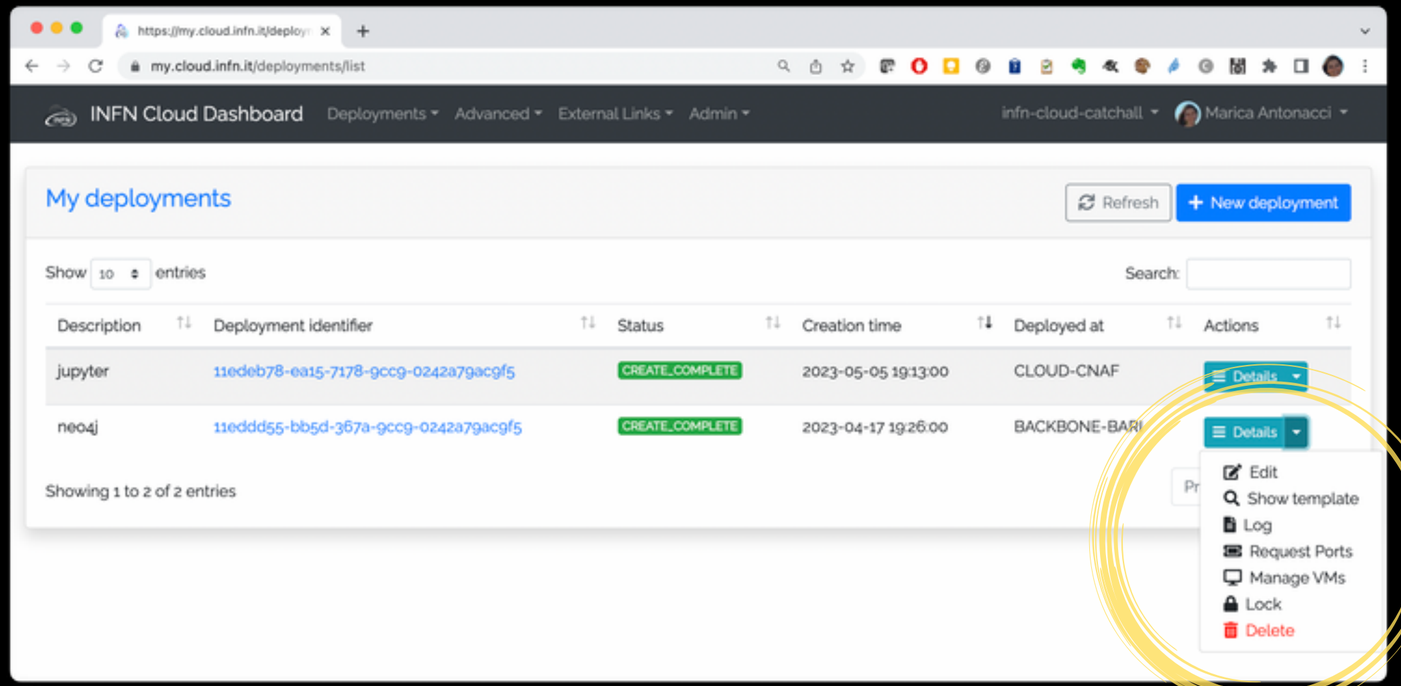
- **automatico**
- **manuale**

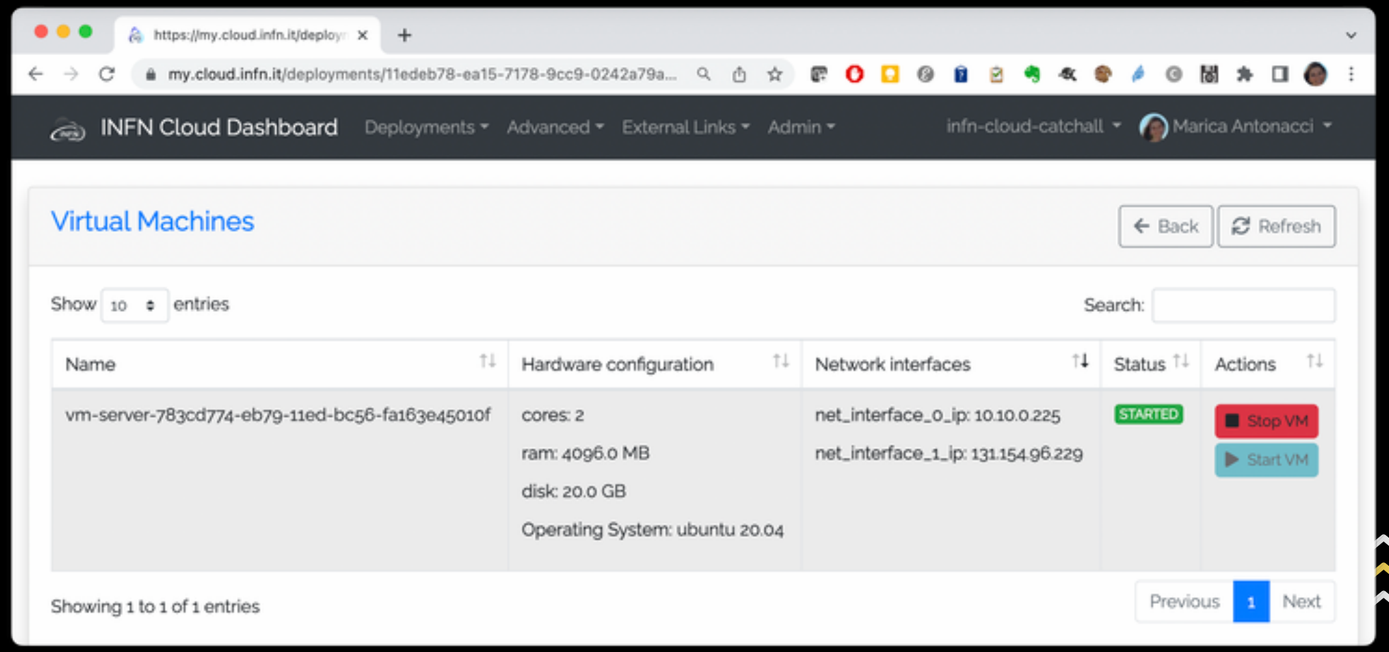


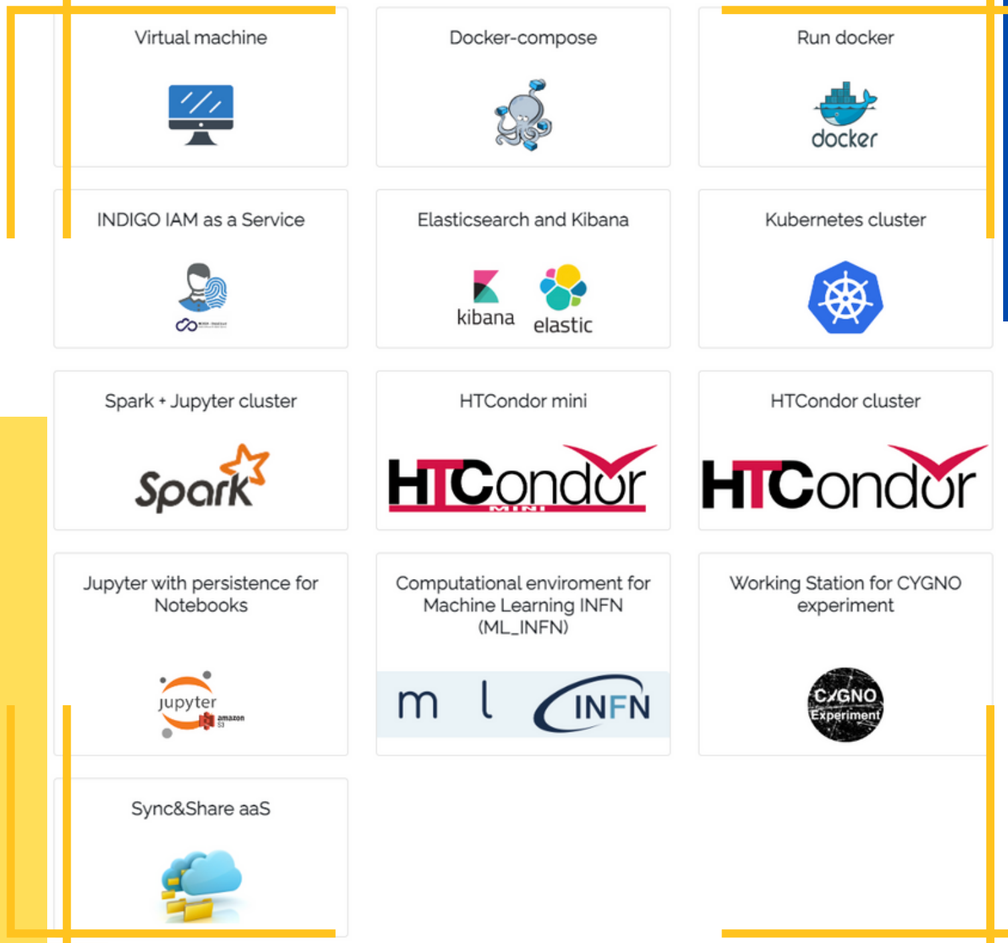
Gestisci i tuoi deployment

Accedi alle informazioni dei deployment (output, log, template, etc.).

Opera in autonomia sulle VM del deployment. (Presto sarà possibile anche gestire le porte).







La strategia utilizzata si fonda sul paradigma "**Infrastructure as Code**".
Gli utenti descrivono "cosa" è necessario anziché "come" implementare un servizio.
Le tecnologie adottate consentono un approccio simile a quello dei mattoncini Lego: i servizi possono essere combinati e i moduli possono essere riutilizzati per creare l'infrastruttura desiderata.

L'IMPLEMENTAZIONE DEI SERVIZI

OASIS TOSCA

ANSIBLE

docker

SERVIZI "GENERAL PURPOSE"

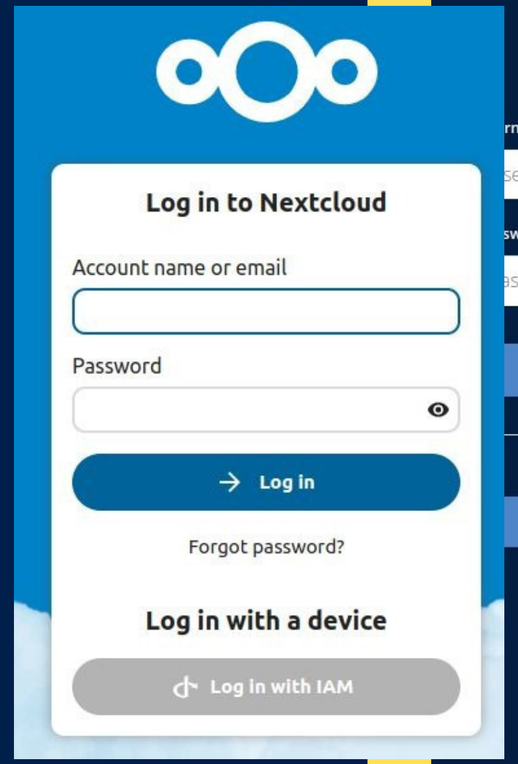
Macchina virtuale con o senza volume aggiuntivo

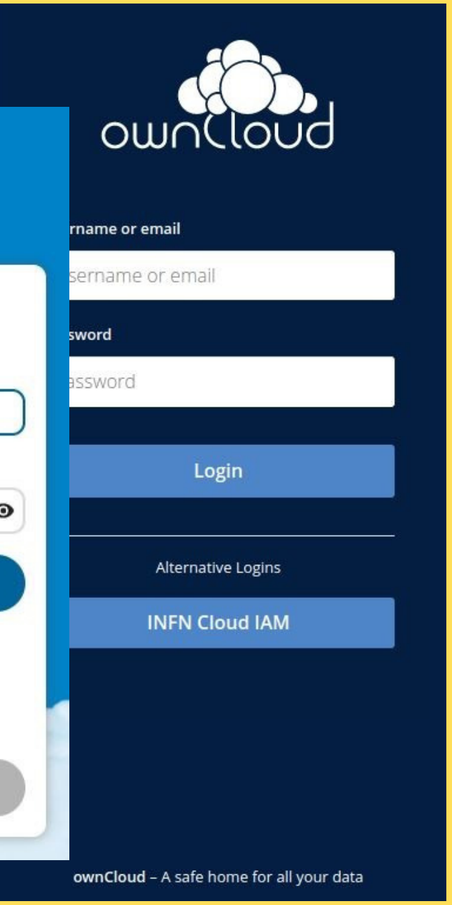
E' possibile richiedere anche l'installazione e configurazione di docker o docker-compose e la possibilità di far partire automaticamente servizi utente tramite un docker compose file.

File Sync&Share

Soluzione basata su OwnCloud o NextCloud che include le seguenti funzionalità:

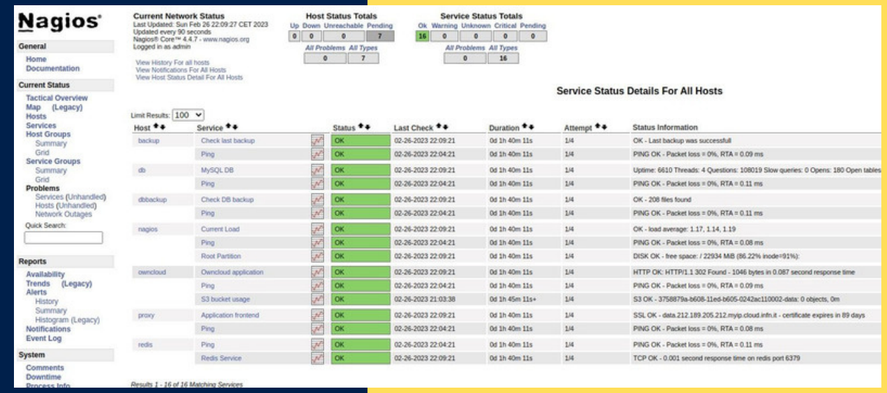
1. backend replicato sull'Object Storage S3 fornito dal Backbone.
2. Configurazione automatica per autenticazione via INDIGO IAM.
3. Cron job pre-installati e configurati per eseguire il backup sicuro delle configurazioni e dei dati sull'Object Storage
4. Monitoraggio integrato delle applicazioni e dei backup basato su Nagios.



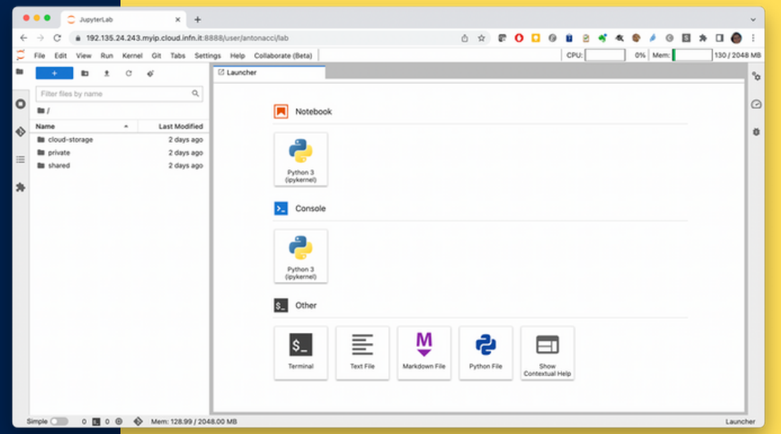


Gestione e analisi dati

Il servizio istanzia un'infrastruttura basata su Elasticsearch, un potente motore di ricerca e indicizzazione, e Kibana per la visualizzazione e l'esplorazione dei dati

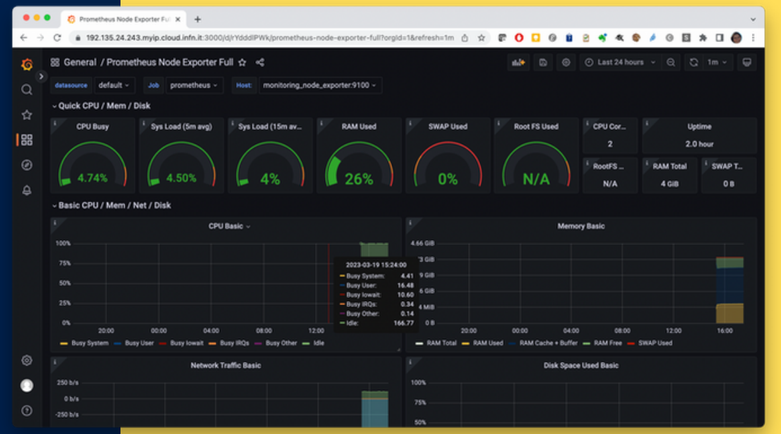


AMBIENTI INTERATTIVI PER L'ANALISI DATI



Creazione on-demand di ambienti di sviluppo interattivo basato su **JupyterLab** per notebook, codice e dati, accessibile tramite web e supportato da diverse funzionalità aggiuntive:

- Aree di storage persistenti per salvare i risultati e i notebook per utilizzi futuri.
- Un sistema di monitoraggio basato su Prometheus e Grafana per raccogliere metriche rilevanti.
- Personalizzazioni specifiche per gli esperimenti, come librerie pre-installate, driver, configurazioni, ecc.

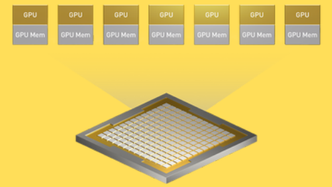


Working Station for CYGNO experiment

Le personalizzazioni per **Cygno** includono:
kernel Python/ROOT, librerie pre-installate per la ricostruzione degli eventi, l'analisi dei dati e la simulazione (basate sui software GEANT4 e Garfield++), mount CVMFS.

Per il progetto **ML-INFN** le istanze di JupyterLab sono in grado di accedere a una o più GPU: i driver e le configurazioni necessarie vengono gestiti automaticamente.
Inoltre, è supportato anche il **partizionamento delle GPU** (basata sulla funzionalità nvidia MIG) per un utilizzo ottimale.

Computational enviroment for Machine Learning INFN (ML_INFN)



SERVIZI AVANZATI BASATI SU KUBERNETES

- Creazione on-demand di cluster k8s completi di sistema di monitoring basato su Prometheus e Grafana
  - con supporto al deployment di cluster con nodi misti, CPU + GPU
- Deployment automatico di applicazioni e cluster su k8s come HTCondor e cluster Spark integrato con Jupyter.
  - l'automazione è stata realizzata integrando due templating language, TOSCA ed Helm

OASIS TOSCA

HELM

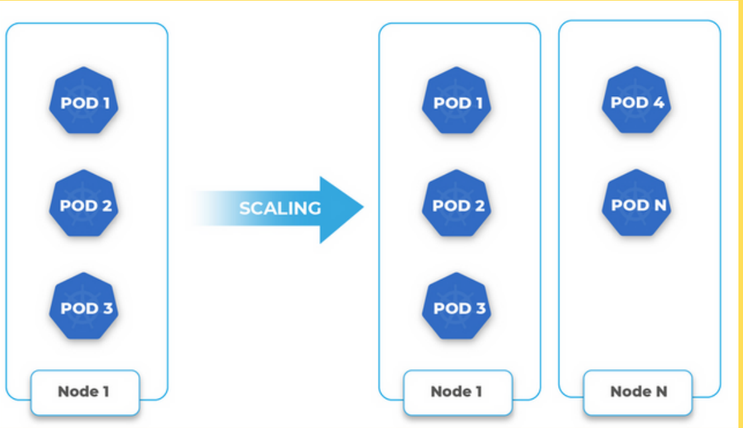
HTCondor

jupyter

APACHE Spark™

kubernetes

WORK IN PROGRESS



NEW!

INDIGO IAM as a Service

Questo servizio consente alle comunità di creare e configurare la propria istanza di **INDIGO IAM** secondo le proprie esigenze specifiche.

HTCondor mini

HTCondor MINI

Consente di istanziare un cluster HTCondor in configurazione all-in-one, utile per scopi di test e sperimentazione.

VEDI DEMO "IAM AS A SERVICE SU INFN CLOUD" (FORNARI F., FANZAGO F.)

Jupyter + Matlab (with persistence for Notebooks)

jupyter

MATLAB

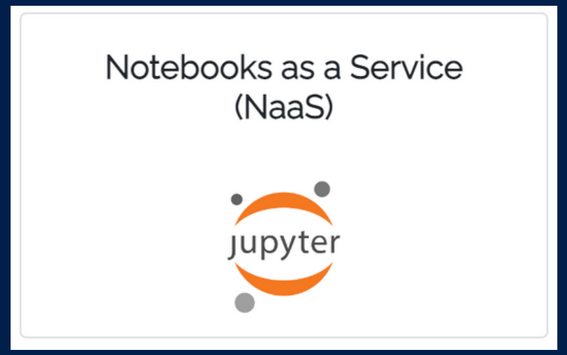
Consente di istanziare un ambiente Jupyter in cui è integrato MATLAB.

VEDI DEMO "MATLAB AS A SERVICE SU INFN CLOUD" (FORNARI F.)

SERVIZI CENTRALIZZATI

Object Storage

Notebook as a Service



Registry (Harbor)

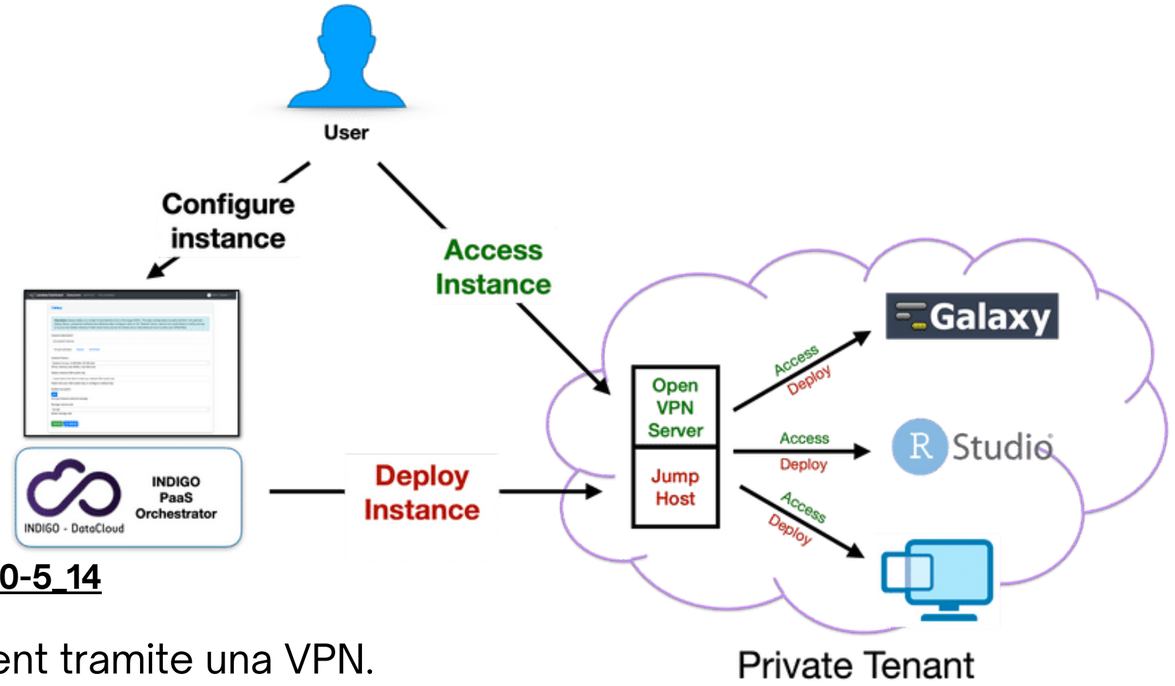
Gli utenti accedono a questi servizi tramite la modalità SaaS

Per i **servizi on-demand** gli utenti sono responsabili dell'amministrazione del servizio, inclusi gli aggiornamenti e l'operatività quotidiana.
Invece nel caso dei **servizi gestiti centralmente**, è il team di INFN Cloud che si occupa della manutenzione e delle operazioni quotidiane.

DEPLOYMENT SU RETE PRIVATA

Il sistema di orchestrazione PaaS è stato esteso per consentire il deployment di macchine virtuali su reti private (isolate dall'esterno).
Questo workflow prevede che la contestualizzazione avvenga tramite un "jump host".

Use-case: gestione di dati genetici e medici



https://doi.org/10.1007/978-3-031-25380-5_14

Gli utenti possono accedere ai deployment tramite una VPN.
Per autenticarli è stato sviluppato un **modulo PAM** che utilizza IAM e il device code flow. L'implementazione di riferimento è basata su OpenVPN.

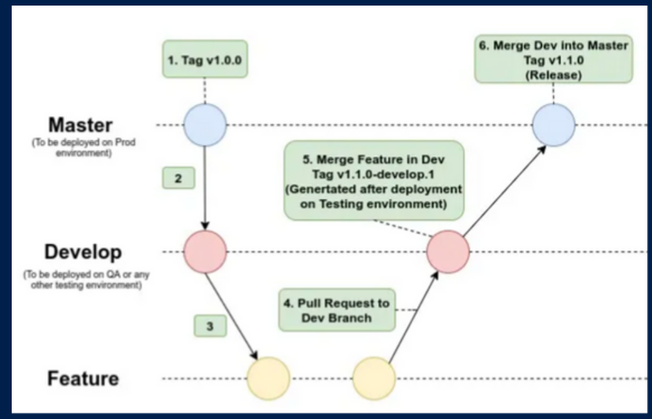
CONTINOUS TESTING & IMPROVEMENT

Abbiamo implementato un sistema di test automatico basato su **Jenkins** che consente di testare i template TOSCA con pipeline predefinite completamente automatizzate.
Queste pipeline eseguono controlli automatici per ciascuno dei servizi disponibili nel catalogo, incluse scansioni relative a vulnerabilità di sicurezza.

TOSCA types Release Management

basato sul tool **semantic-release** in combinazione con la CI di baltig

Ci consente di ricostruire come è stato fatto un deployment (quali versioni di TOSCA type, ansible roles, etc.)



LE SFIDE ATTUALI E FUTURE

- Il sistema di orchestrazione PaaS sarà fondamentale per la federazione e orchestrazione delle risorse nel contesto dei progetti **PNRR**.
- Attualmente lo sviluppo (sinergico) viene portato avanti non solo in DataCloud ma anche in numerosi progetti europei

C-SCALE

interTwin

AI4 | eosc

EGI-ACE

- Al momento, oltre all'installazione di INFN Cloud, gestiamo l'operatività di altre istanze di PaaS per servizi di produzione:

Laniakea

deep Hybrid DataCloud training facility

EUROPEAN OPEN SCIENCE CLOUD

DATACLOUD WP5 TEAM

WP Leaders: Antonacci M., Vianello E.

24 iscritti alla mailing list datacloud-software@lists.infn.it

Sviluppo di servizi basati su TOSCA/ansible

Antonacci M., Ciangottini D., Fornari F., Gattari M., Sinisi F., Spiga D., Stalio S., Vino G.

Sviluppo Middleware PaaS + dashboard

Antonacci M.

Sviluppo IAM

Agostini F., Miccoli R., Vianello E.

Supporto al test dei servizi

Fanzago F., Sgaravatto M., Verlato M., Pellegrino C.

Altri iscritti

Michelotto D., Fattibene, Peco, Savarese, Andronico, Costantini, Giommi, Dal Pra, Donvito, Cesini

GRAZIE PER L'ATTENZIONE

WWW.CLOUD.INFN.IT