

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

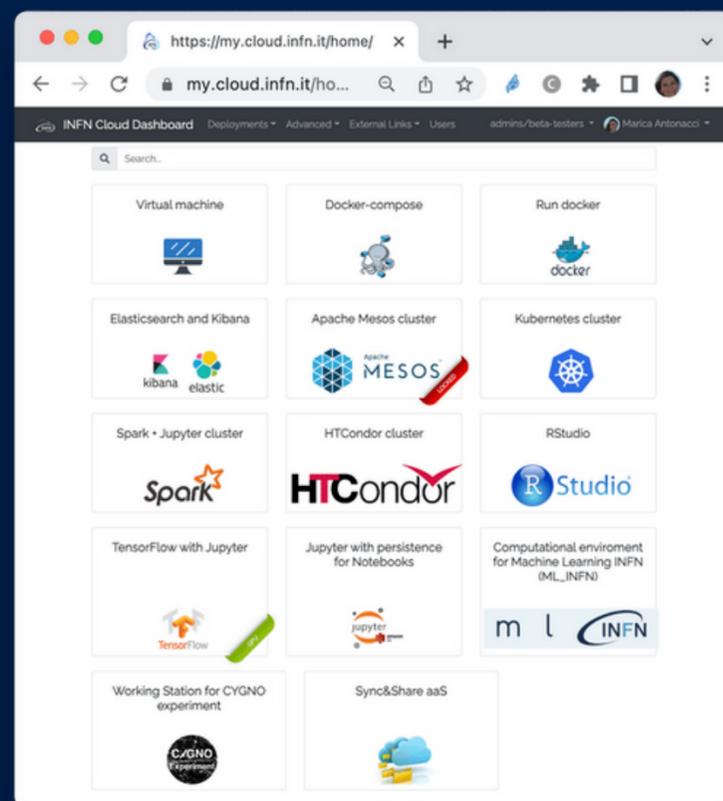
# FEDERAZIONE DINAMICA DI RISORSE

## attraverso l'ORCHESTRATORE PaaS

che implementa funzionalità di federazione di infrastrutture cloud distribuite e di scheduling.

La federazione INFN Cloud oggi include:

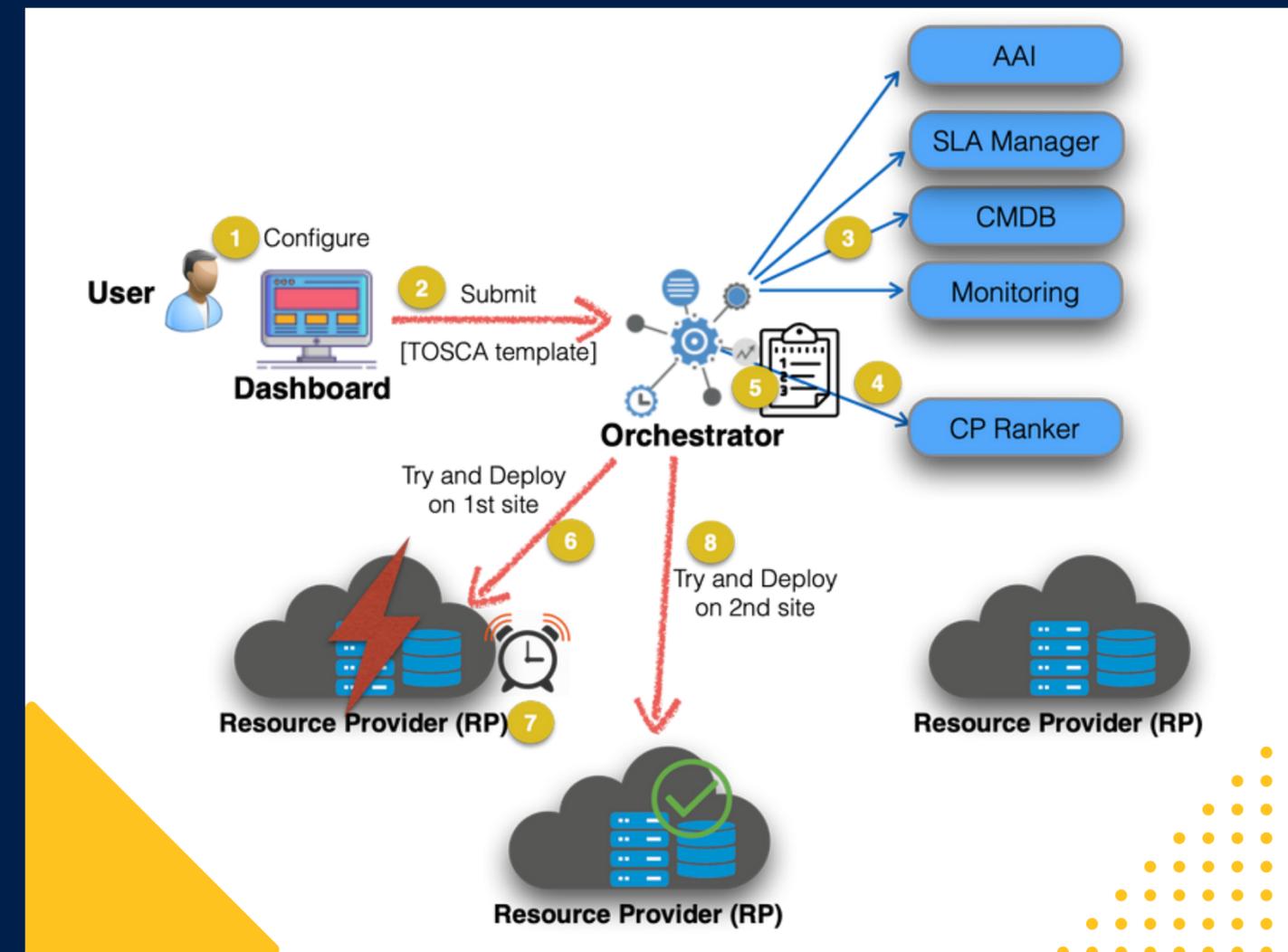
- Backbone sulle sedi di CNAF e Bari
  - Cloud federate: ReCaS-BARI, Cloud@CNAF, CloudVeneto.
- In corso la federazione di Cloud CT.



# 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 sfruttata 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

# 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

### Kubernetes cluster

Description: Deploy a single master Kubernetes 1.23.8 cluster

Deployment description

Configuration **Advanced**

admin\_token  
.....

Password token for accessing K8s dashboard

number\_of\_nodes  
3

Number of K8s node VMs

ports

Ports to open on the K8s master VM

master\_flavor  
--Select--

Number of vCPUs and memory size of the K8s master VM

node\_flavor  
--Select--

Number of vCPUs and Memory Size of each K8s node VM

## Scegli la strategia di scheduling

- automatico
- manuale

### Kubernetes cluster

Description: Deploy a single master Kubernetes 1.23.8 cluster

Deployment description

Configuration **Advanced**

Configure scheduling:  
 Auto  Manual

Select a provider:  
RECAS-BARI: org.openstack.nova

Set deployment creation timeout (minutes) 720

Do not delete the deployment in case of failure

Send a confirmation email when complete



# Gestisci i tuoi deployment

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

The screenshot shows the 'My deployments' page in the INFN Cloud Dashboard. It features a table with columns for Description, Deployment Identifier, Status, Creation time, Deployed at, and Actions. Two deployments are listed: 'jupyter' and 'neo4j', both with a 'CREATE\_COMPLETE' status. A context menu is open over the 'jupyter' deployment, listing actions such as Edit, Show template, Log, Request Ports, Manage VMs, Lock, and Delete.

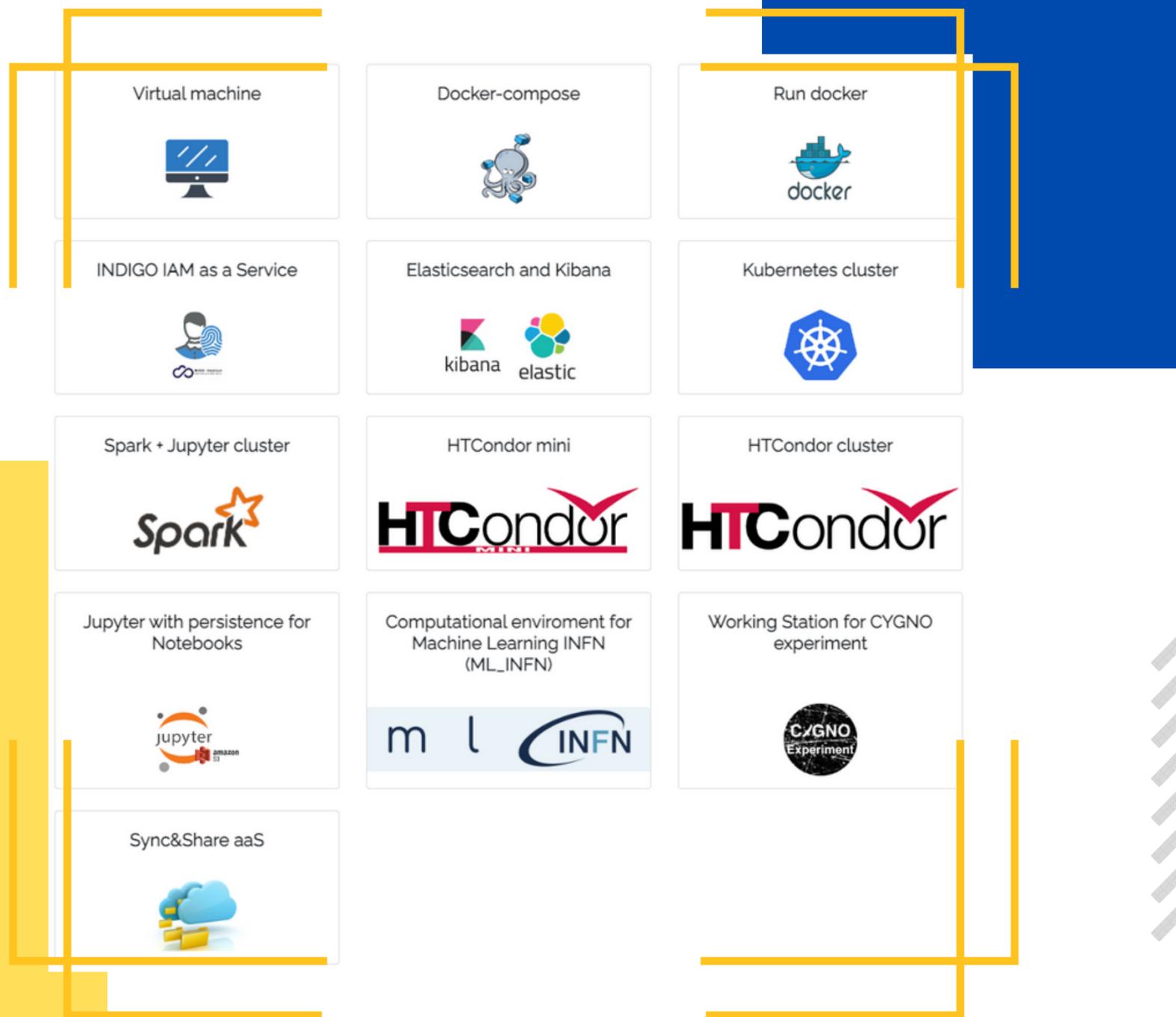
Description	Deployment Identifier	Status	Creation time	Deployed at	Actions
jupyter	11edeb78-ea15-7178-9cc9-0242a79ac9f5	CREATE_COMPLETE	2023-05-05 19:13:00	CLOUD-CNAF	Details
neo4j	11eddd55-bb5d-357a-9cc9-0242a79ac9f5	CREATE_COMPLETE	2023-04-17 19:26:00	BACKBONE-BARI	Details

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

The screenshot shows the 'Virtual Machines' page for a specific deployment. It displays a table with columns for Name, Hardware configuration, Network interfaces, Status, and Actions. One VM is listed: 'vm-server-783cd774-eb79-11ed-bc56-fa163e45010f'. The hardware configuration includes 2 cores, 4096.0 MB of RAM, and a 20.0 GB disk. The network interfaces are 'net\_interface\_0\_ip: 10.10.0.225' and 'net\_interface\_1\_ip: 131.154.96.229'. The VM status is 'STARTED', and there are buttons for 'Stop VM' and 'Start VM'.

Name	Hardware configuration	Network interfaces	Status	Actions
vm-server-783cd774-eb79-11ed-bc56-fa163e45010f	cores: 2 ram: 4096.0 MB disk: 20.0 GB Operating System: ubuntu 20.04	net_interface_0_ip: 10.10.0.225 net_interface_1_ip: 131.154.96.229	STARTED	Stop VM Start VM





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



# 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.



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



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.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
backup	Check last backup	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	OK - Last backup was successful
db	MySQL DB	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	Uptime: 6610 Threads: 4 Questions: 108019 Slow queries: 0 Opens: 180 Open tables:
dbbackup	Check DB backup	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.11 ms
dbbackup	Ping	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	OK - 208 files found
nagios	Current Load	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.11 ms
nagios	Ping	OK	02-26-2023 22:04:21	0d 1h 40m 11s	1/4	OK - load average: 1.17, 1.14, 1.19
nagios	Root Partition	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.08 ms
owncloud	Owncloud application	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	DISK OK - free space: / 22934 MB (86.22% inode+91%)
owncloud	Ping	OK	02-26-2023 22:04:21	0d 1h 40m 11s	1/4	HTTP OK: HTTP/1.1 302 Found - 1046 bytes in 0.087 second response time
owncloud	S3 bucket usage	OK	02-26-2023 21:03:38	0d 1h 45m 11s+	1/4	PING OK - Packet loss = 0%, RTA = 0.09 ms
proxy	Application frontend	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	S3 OK - 3758879a-b608-11e4-b605-0242ac110002-data: 0 objects, 0m
redis	Ping	OK	02-26-2023 22:04:21	0d 1h 40m 11s	1/4	SSL OK - data.212.189.205.212.mypcloud.inf.it - certificate expires in 89 days
redis	Redis Service	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.08 ms
redis	Redis Service	OK	02-26-2023 22:04:21	0d 1h 40m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.11 ms
redis	Redis Service	OK	02-26-2023 22:09:21	0d 1h 40m 11s	1/4	TCP OK - 0.001 second response time on redis port 6379

# 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:

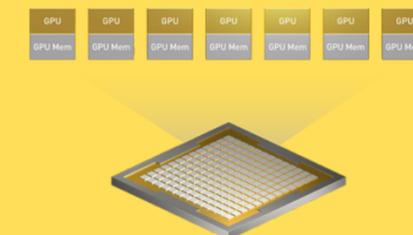
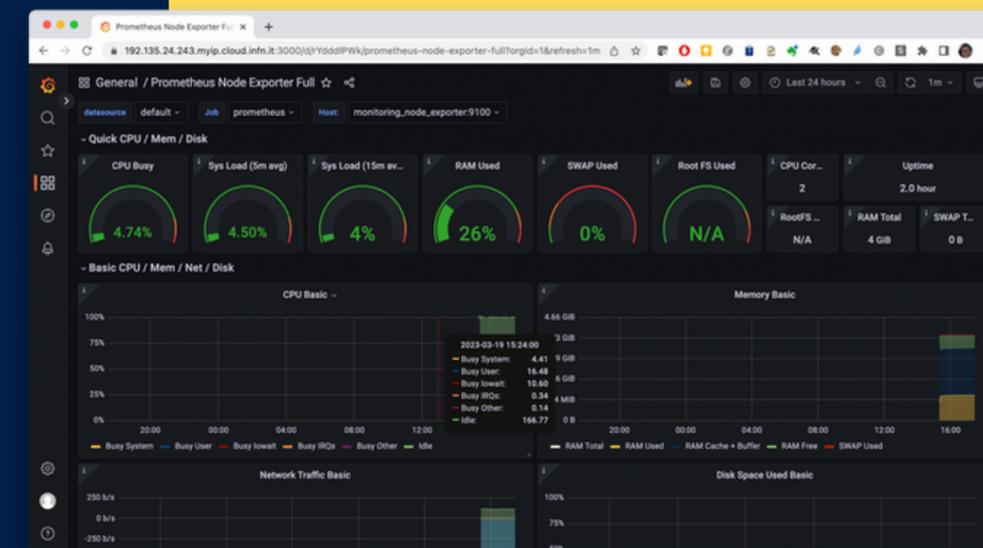
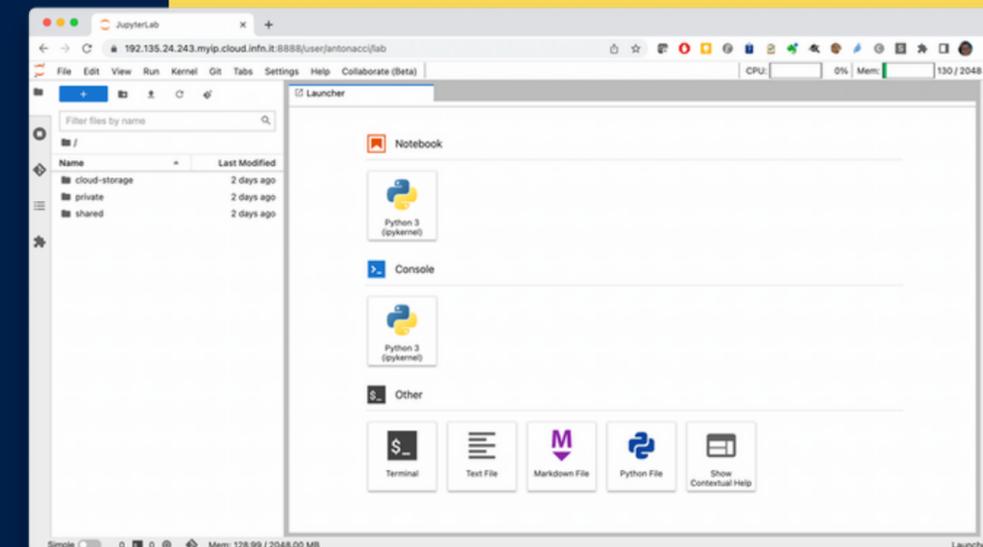
- Aree di storage persistenti per salvare i risultati e i notebook per utilizzi futuri.
- Un sistema di monitoraggio basato su Prometheus e Grafana per raccogliere metriche rilevanti.
- Personalizzazioni specifiche per gli esperimenti, come librerie pre-installate, driver, configurazioni, ecc.



Le personalizzazioni per **Cygn**o 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.



# SERVIZI AVANZATI BASATI SU KUBERNETES

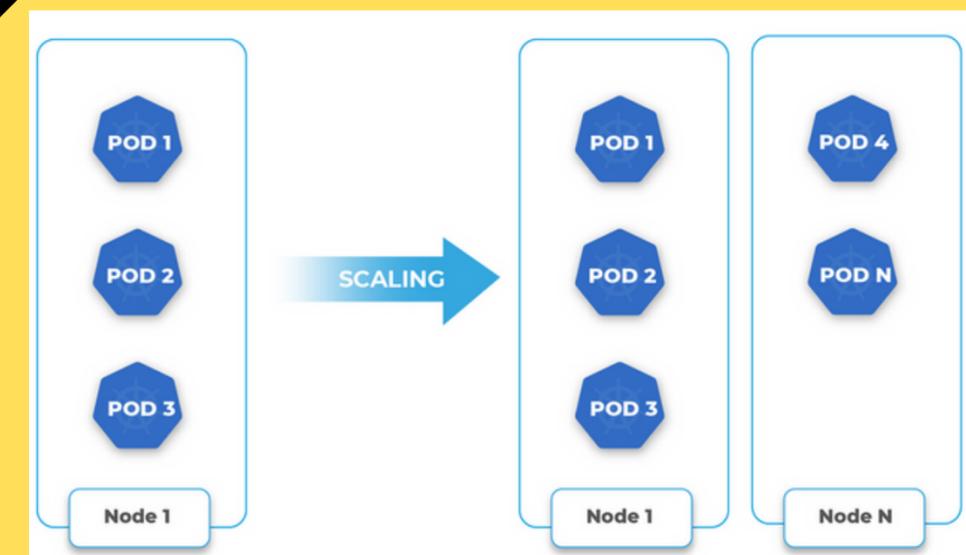
- Creazione on-demand di cluster k8s completi di sistema di monitoring basato su Prometheus e Grafana
  - con supporto al deployment di cluster con nodi misti, CPU + GPU
- Deployment automatico di applicazioni e cluster su k8s come HTCondor e cluster Spark integrato con Jupyter.
  - l'automazione è stata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

OASIS  TOSCA



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



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)



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

INFN Cloud object storage



## Notebook as a Service

Notebooks as a Service  
(NaaS)



## Registry (Harbor)

INFN Cloud Registry



**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.





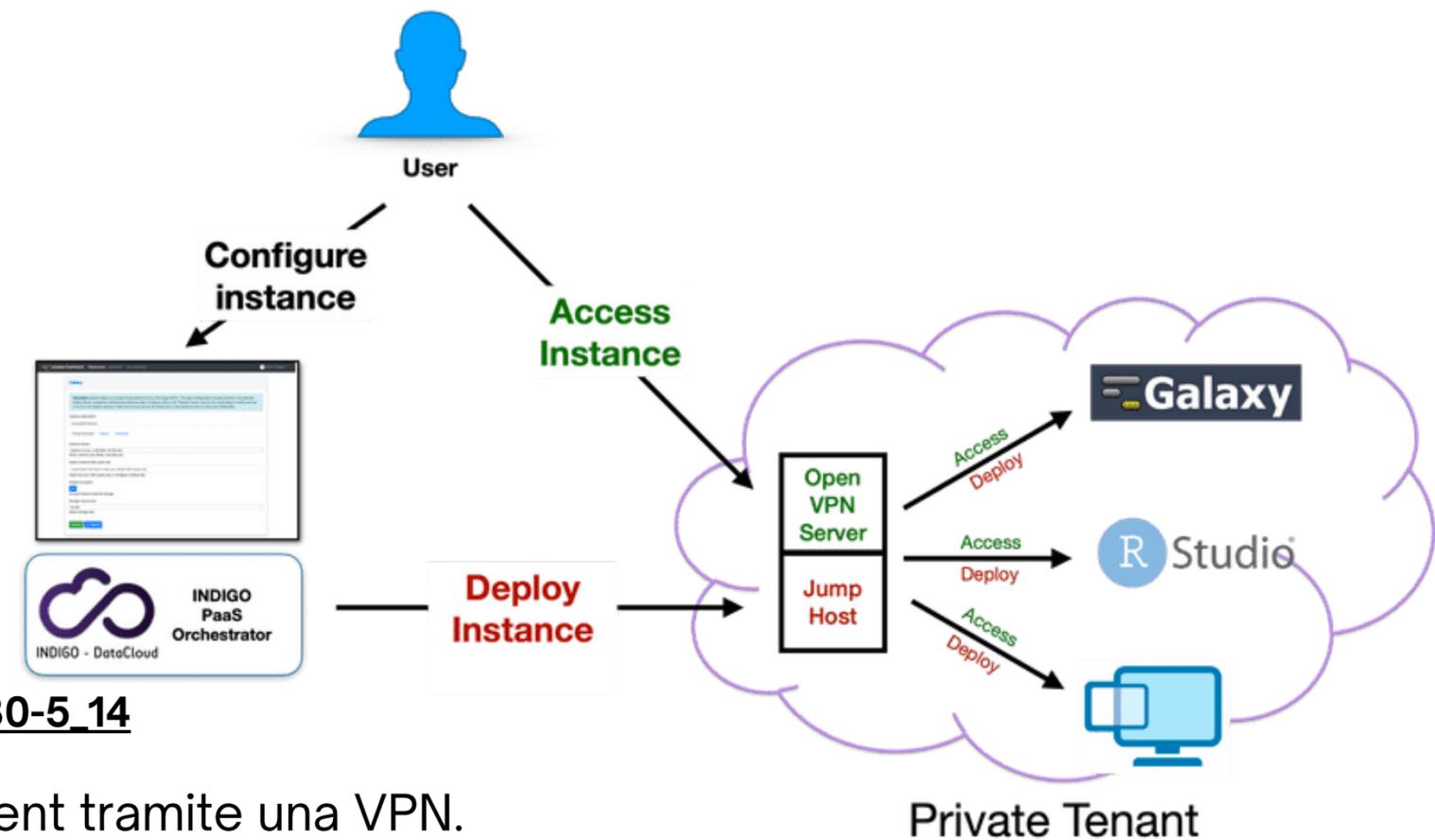
# DEPLOYMENT SU RETE PRIVATA

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



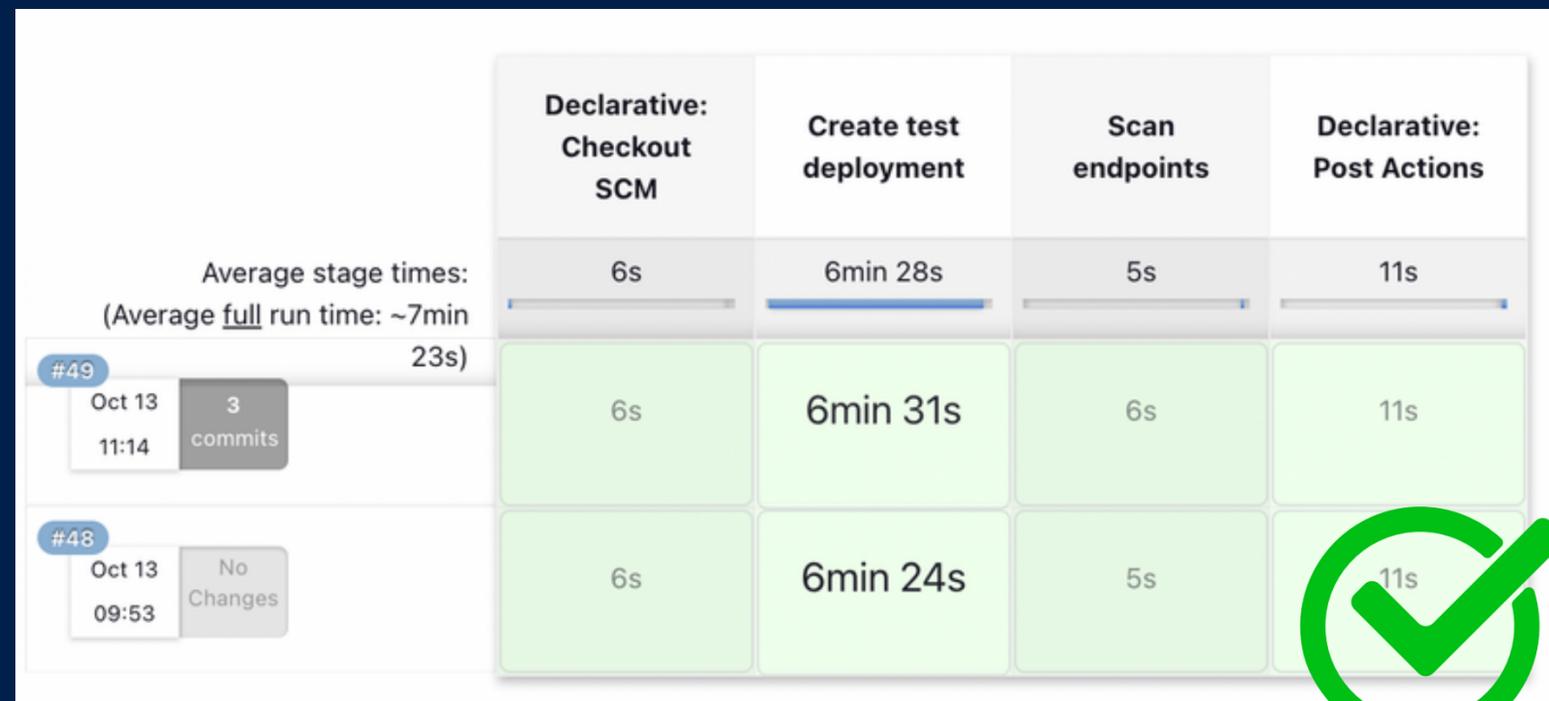
Gli utenti possono accedere ai deployment tramite una VPN. Per autenticarli è stato sviluppato un **modulo PAM** che utilizza IAM e il device code flow. L'implementazione di riferimento è basata su OpenVPN.



# CONTINUOUS TESTING & IMPROVEMENT

Abbiamo implementato un sistema di test automatico basato su **Jenkins** che consente di testare i template TOSCA con pipeline predefinite completamente automatizzate.

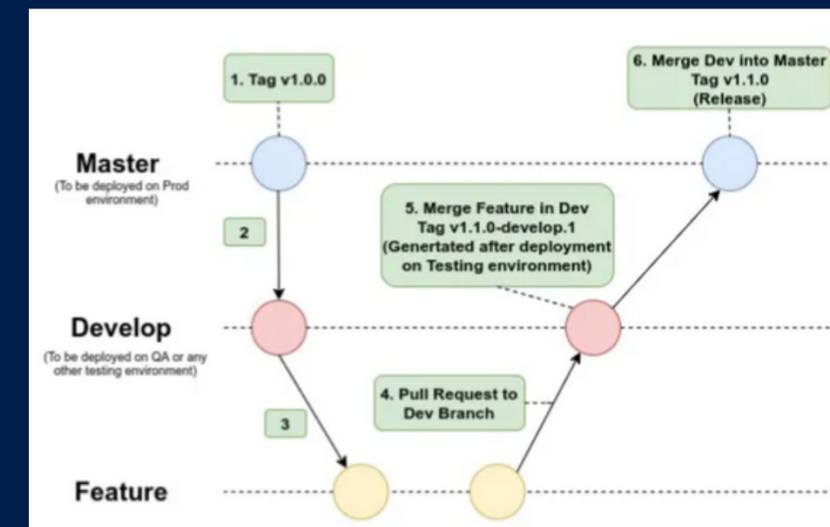
Queste pipeline eseguono controlli automatici per ciascuno dei servizi disponibili nel catalogo, incluse scansioni relative a vulnerabilità di sicurezza.



## 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



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



EUROPEAN OPEN  
SCIENCE CLOUD





# DATA CLOUD WP5 TEAM

WP Leaders: Antonacci M., Vianello E.

24 iscritti alla mailing list [datacloud-software@lists.infn.it](mailto: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](http://WWW.CLOUD.INFN.IT)