SEAMLESS ACCESS TO FEDERATED RESOURCES FOR MULTI-DISCIPLINARY SCIENTIFIC RESEARCH THROUGH THE NATIONAL INFN CLOUD INFRASTRUCTURE: AN OVERVIEW OF THE ARCHITECTURE, SERVICES, AND FUTURE DEVELOPMENT

Marica Antonacci (INFN)
marica.antonacci@ba.infn.it

EGI Conference 2023

Cloud computing

A game-changer in scientific research

Opportunities

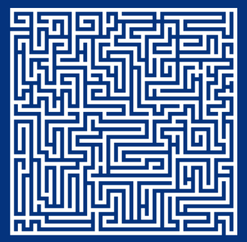
Collaboration

Accessibility

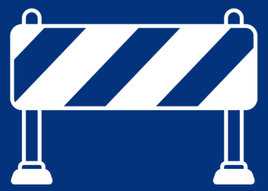
Speed

Obstacles

Integration challenge



Technical complexity



Cultural barriers

INFN CLOUD

https://www.cloud.infn.it

- In **production** since March 2021
- Based on **scalable** and **production grade** solutions
- A **customisable portfolio of services** accessible through various interfaces (web, terminal, API)

Architectural foundations

No vendor lock-in

Open-source, vendor-neutral architecture

Federation

of existing Cloud infrastructures for both compute and data

Dynamic Orchestration

of resources via the INDIGO PaaS Orchestrator

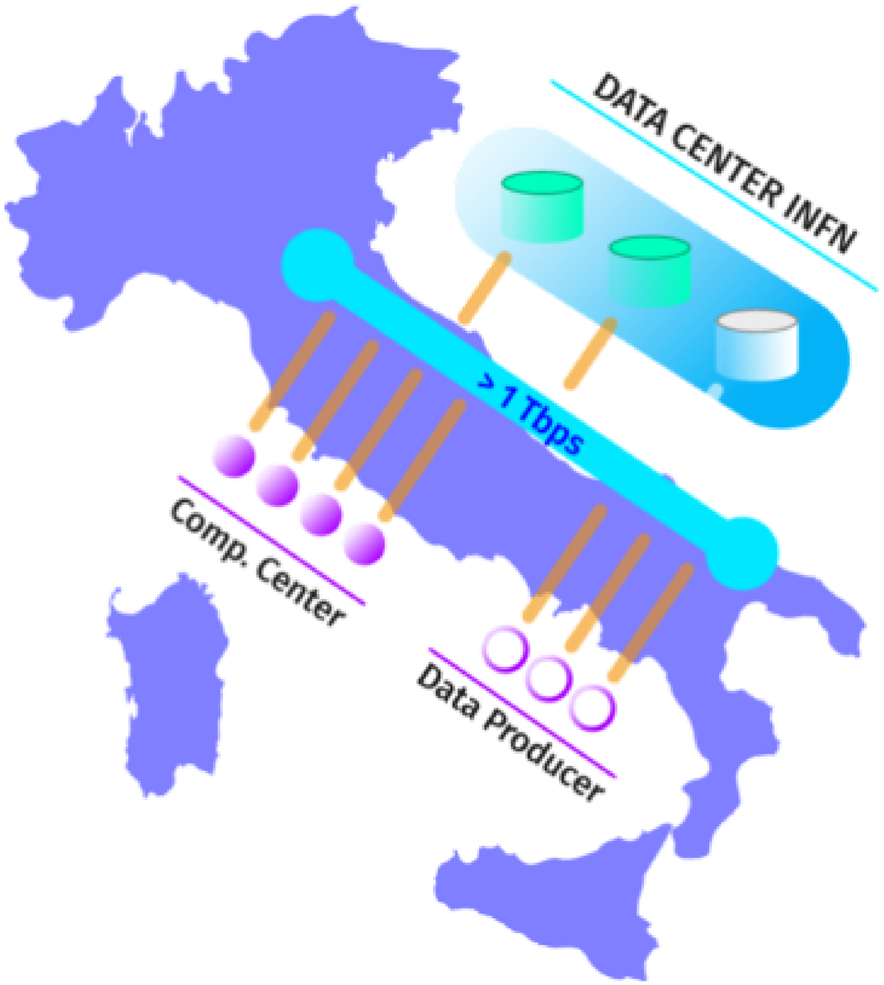
Consistent AuthN/AuthZ

at all cloud levels via OpenID-Connect/OAuth2

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.

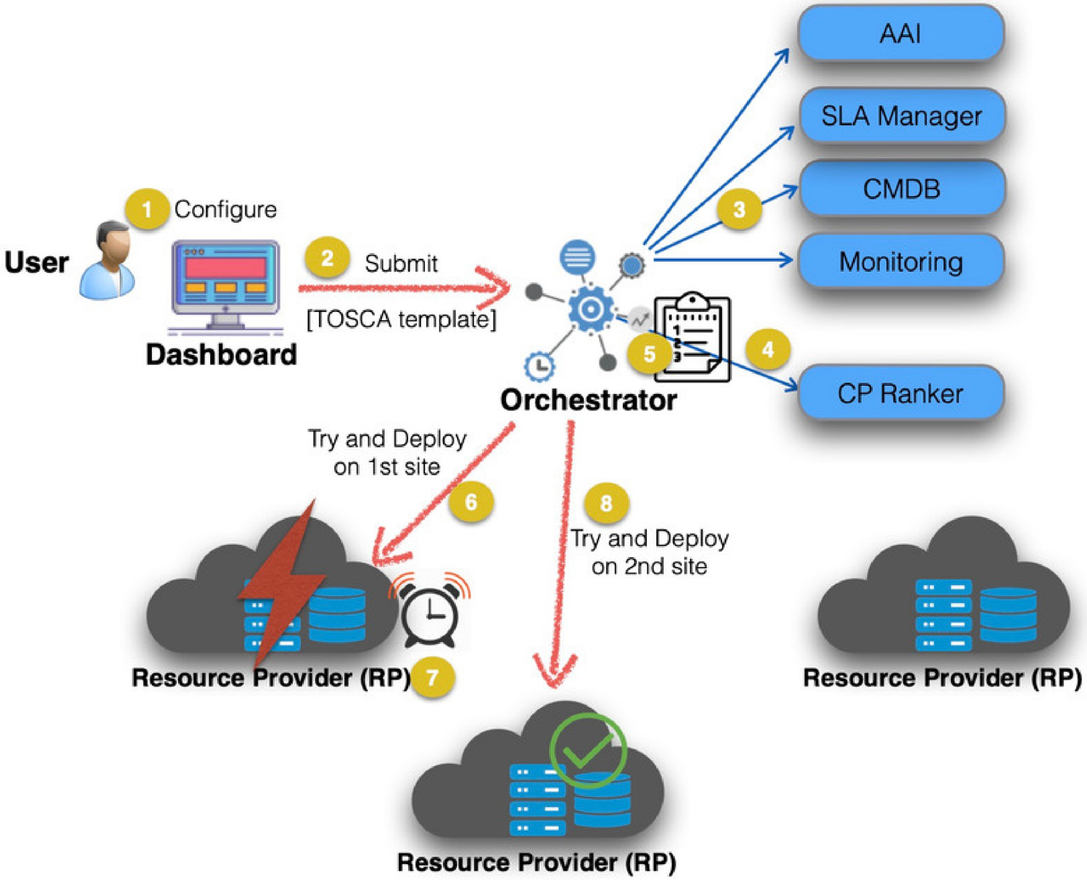
INFN Cloud core services and some centralised, fully managed, high-level services are hosted on the Backbone. This allows us to leverage **high-availability** and **disaster recovery** capabilities to ensure that these critical services are always available and operating at peak efficiency.



The federation middleware

The INDIGO PaaS Orchestrator enables the federation of distributed and heterogeneous compute environments: clouds, docker orchestration platforms, HPC systems.

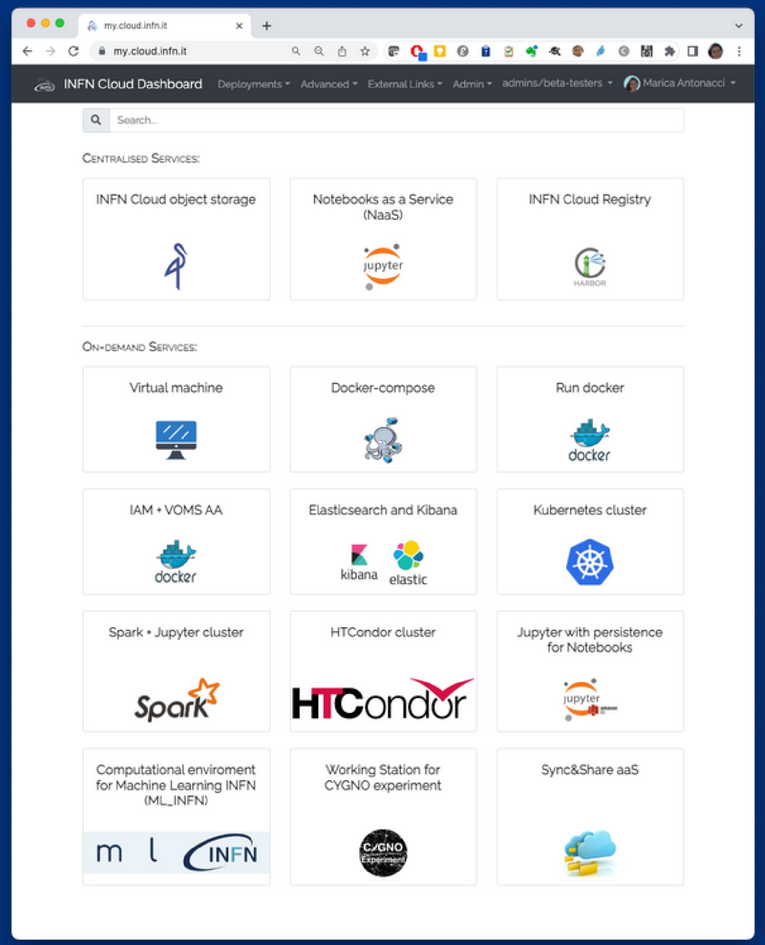
- **Smart scheduling** → Automatic selection of the best provider
  - based on compute/storage requirements vs provider capabilities including the following criteria:
    - Resource quotas (SLA)
    - Monitoring data
    - Support for specialized hardware (GPU, Infiniband)
    - Data location
- Support for **hybrid deployments** and network orchestration
- **Client interfaces** for advanced users (REST APIs, CLI, python bindings) and end-users (web dashboard - no skills required)



The PaaS Dashboard

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
- Dynamic view of service catalog (depending on the user group membership)
- Secrets management (via Vault integration)



The service implementation strategy

The employed strategy is based on the **Infrastructure as Code paradigm**.
Users describe "What" is needed rather than "**How**" a specific service or functionality should be implemented.
The adopted technologies enable a Lego-like approach: **services can be composed and modules reused** to create the desired infrastructure.

TOSCA is used to model the topology of the whole application stack

Ansible is used to automate the configuration of the virtual environments

Docker is used to encapsulate the high-level application software and runtime

General purpose services

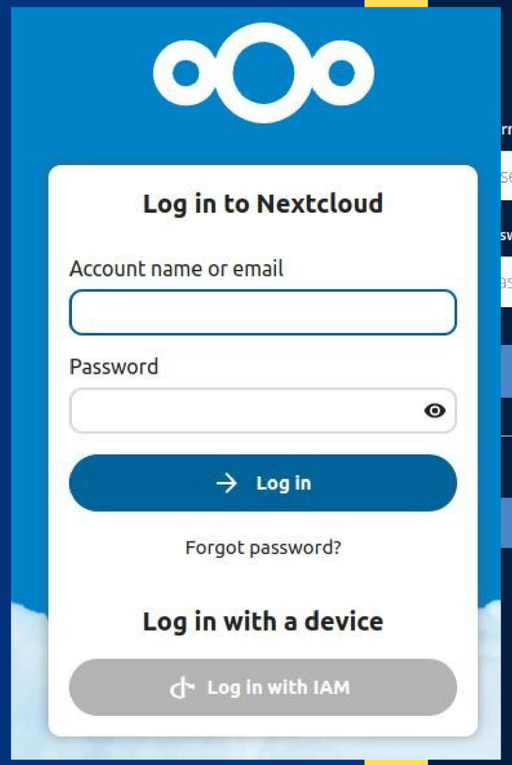
Virtual Machine with or without external block storage

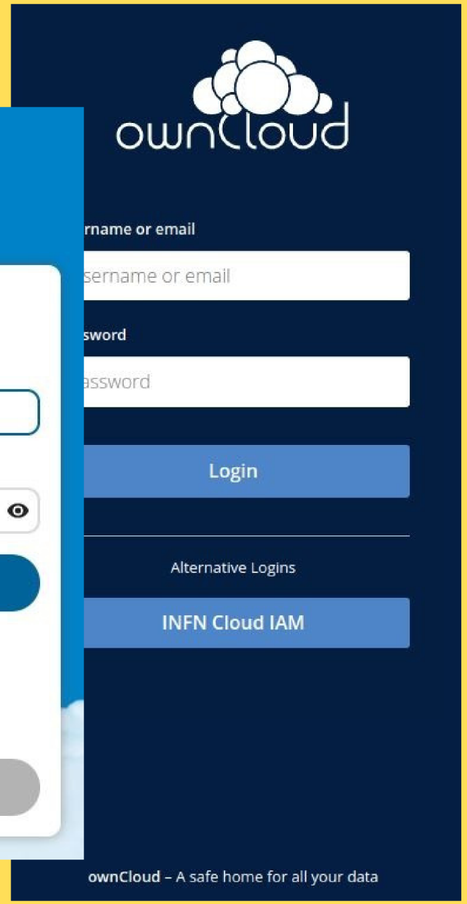
eventually equipped with docker engine and docker-compose, on top of which dockerized services can be automatically started

File Sync&Share

based on OwnCloud/NextCloud with

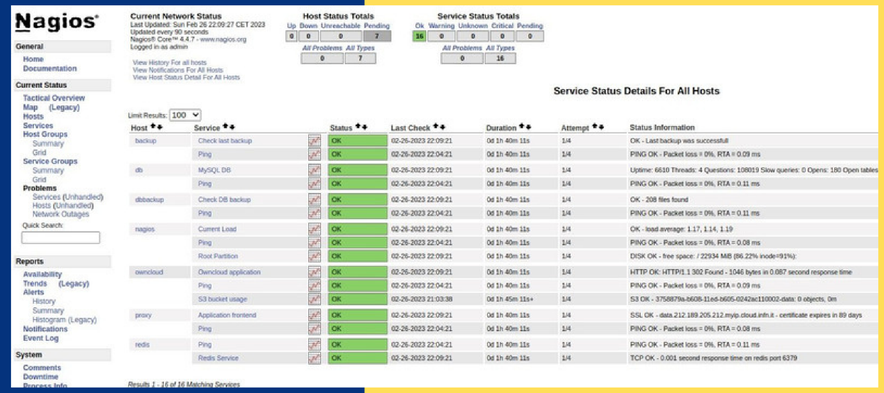
- replicated backend storage on the S3-compliant Object Storage provided by the INFN Cloud infrastructure;
- automatic configuration for enabling INDIGO IAM OpenID Connect authentication;
- pre-installed and configured backup cron jobs for safely storing configuration and data on the Object Storage for future restore in case of disaster;
- integrated application and backup monitoring based on Nagios





Data Analytics

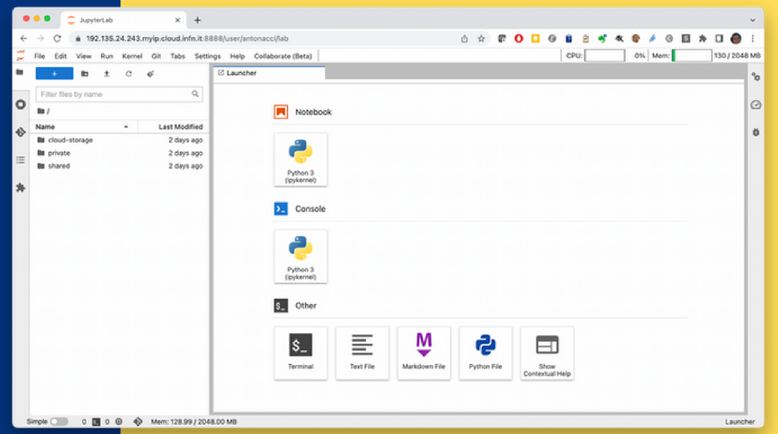
based on Elasticsearch, a powerful search and indexing engine, and Kibana for data visualization and exploration.

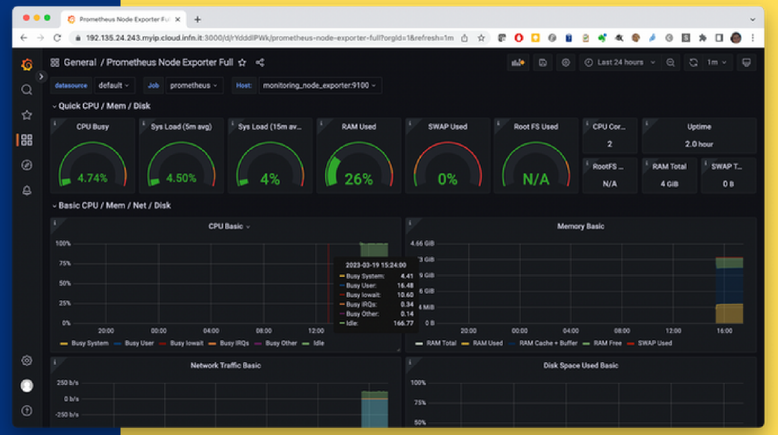


On-demand interactive data analysis environments

Web-based multi-user interactive development environment for notebooks, code and data built on **JupyterLab** and enahnced with:

- **persistent storage areas** for storing results and notebooks for future re-use;
- a **monitoring** system based on Prometheus and Grafana for collecting relevant metrics;
- **experiment-specific customizations** (pre-installed libraries, drivers, configurations, etc.)



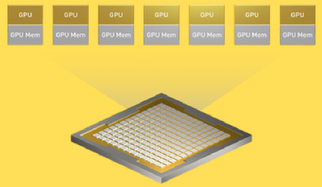


Working Station for CYGNO experiment

Cygno experiment for Dark Matter direct detection: Python/ROOT kernels, pre-installed libraries for event reconstruction, data analysis and simulation (based on GEANT4 and Garfield++ software), CVMFS mounts

ML-INFN Project, an INFN-funded project aiming at lowering the potential barriers for accessing specialized hardware for the exploitation of Machine Learning techniques: in this case the JupyterLab instances are able to access one or more GPUs as the needed drivers and configurations are automatically managed. Moreover, **GPU partitioning** (based on the nvidia MIG feature) is also supported for optimal utilization.

Computational enviroment for Machine Learning INFN (ML_INFN)



Kubernetes-based advanced services

- On-demand deployment of complete Kubernetes clusters with a monitoring system based on Prometheus and Grafana
  - supporting the deployment of mixed nodes (CPU + GPU).

- Automated deployment of applications on top of Kubernetes, such as HTCondor and Spark clusters integrated with Jupyter.
  - the automation is achieved by leveraging the two templating languages, TOSCA and Helm

HTCondor

jupyter

APACHE Spark

kubernetes

OASIS TOSCA

+

HELM

Centralised fully managed services

Object Storage

INFN Cloud object storage

Notebook as a Service

Notebooks as a Service (NaaS)

jupyter

Registry (Harbor)

INFN Cloud Registry

Users access these services through the SaaS (Software-as-a-Service) model.

Users are responsible for administering **on-demand services**, including updates and daily operations.

However, in the case of **centrally managed services**, the INFN Cloud team is in charge of maintenance and day-to-day operations.

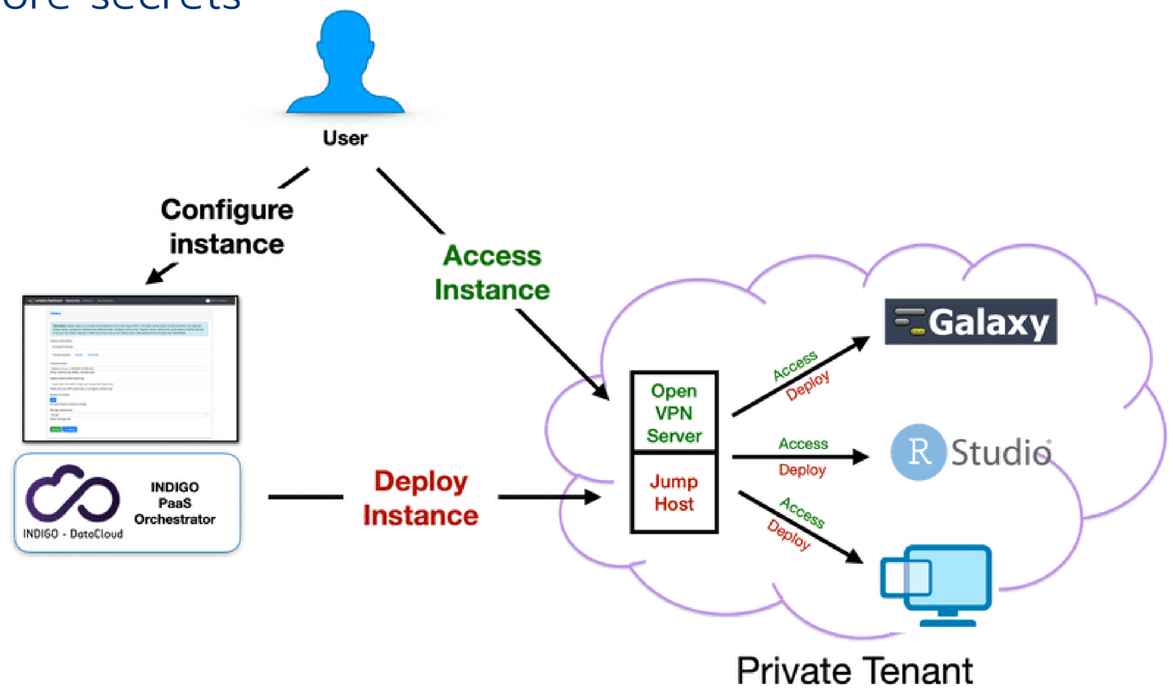
Secure environments

Data security, legal, and ethical requirements for genetic and medical data are becoming increasingly stringent. Therefore we have been working to implement the necessary measures to improve the security of the deployed services.

- The PaaS Orchestration system has been extended to allow for the deployment of VMs on private networks (the contextualization is done via a "**jump host**")
- Moreover, a **Vault** instance is made available to store secrets

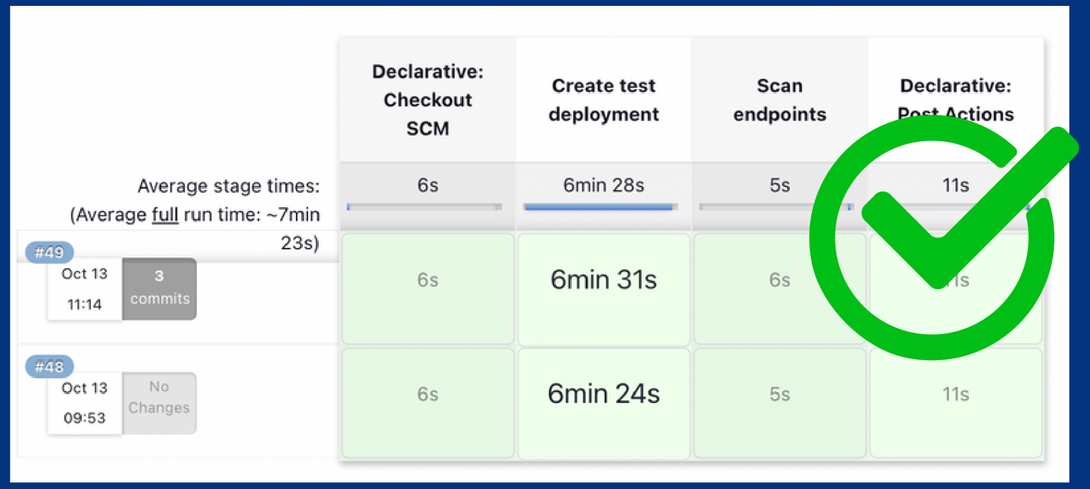
The deployment can be accessed by the user through **VPN**.

- To authenticate users, a PAM module has been developed that uses IAM by taking advantage of the device code authorization flow. The implementation is based on OpenVPN.



Continous testing & improvement

It is critical to provide service templates that are often updated and incorporate security patches.
We built an automated testing system using Jenkins that allows us to test the TOSCA templates with pre-defined, fully automated job pipelines.
These pipelines run automated tests on each of the services in the catalogue, including scans for security vulnerabilities.



	Declarative: Checkout SCM	Create test deployment	Scan endpoints	Declarative: Post Actions
Average stage times: (Average full run time: ~7min 23s)	6s	6min 28s	5s	11s
#49 Oct 13 11:14 3 commits	6s	6min 31s	6s	11s
#48 Oct 13 09:53 No Changes	6s	6min 24s	5s	11s

Conclusions

- INFN Cloud aims to address the new challenges of computing for scientific research.
- It provides researchers with easy access to distributed resources in a transparent way, allowing them to perform complex analyses without requiring specialized IT knowledge.
- Additionally, the platform enables the deployment of complex services with just a few clicks, streamlining the research process and enabling researchers to focus on their work.
- Future work will focus on improving the scheduling algorithm to enhance the platform's performance.
- Integrated solutions for data management across distributed sites will be provided (based for example on Rucio + FTS)

Thank you

www.cloud.infn.it