The INFN-Cloud PaaS Dashboard

Marica Antonacci
marica.antonacci@ba.infn.it
on behalf of the INFN Cloud Project

EGI Conference 2020
2-5 November 2020 - Online
Outline

- INFN Cloud Overview
- PaaS Orchestration & TOSCA
- The INFN Cloud Web Dashboard
  - The service catalogue
  - Main dashboard functionalities
- Conclusions
The INFN Cloud

• INFN Cloud aims to offer a full set of high-level cloud services to INFN user communities
  • the service catalogue is not static: new applications are included through a defined “on-boarding” process for new use-cases

• Architecturally INFN Cloud is a federation of existing infrastructures
  • the **INFN Cloud backbone**: it consists of two tightly coupled federated sites (BARI and CNAF)
  • a scalable set of satellite sites, geographically distributed across Italy, and loosely coupled.

• Key enabling factors for the federation
  • leverage the same authentication/authorization layer based on **INDIGO-IAM**;
  • agree on a consistent set of policies and participation rules (user management, SLA, security, etc.);
  • transparent and dynamic orchestration of the resources across all the federated infrastructures through the **INDIGO PaaS Orchestrator**
PaaS TOSCA(*) Orchestration

(*) Topology and Orchestration Specification for Cloud Applications

Ref: TOSCA Simple Profile in YAML Version 1.1
PaaS Interfaces: the user perspective

- PaaS REST APIs
- Orchestrator CLI
- Orchestrator bindings (go, python)

Requirements:
- TOSCA knowledge (at least basic)
- installation/configuration of CLI tools
- authentication token management

Pros:
- No TOSCA knowledge is needed
- accessible via web
- automatic token management after user login
- easy to use and intuitive

Orchestrator Dashboard (development started during the DEEP-HybridDatacloud Project)
INDIGO IAM manages the authentication/authorization through the whole stack (from PaaS to IaaS)

Users are organized in different IAM groups.

Each group can access a specific set of services from the dashboard (personalized view) and is mapped onto a dedicated tenant on the federated clouds.
The service catalogue

The catalogue is a graphical representation of the TOSCA templates repository that we have been developing extending the INDIGO-DC custom types

- Each card in the catalogue is associated to one or more templates;
- We are following a lego-like approach, building on top of reusable components and exploiting the TOSCA service composition pattern.

Main objectives:

#1 - build added value services on top of IaaS and PaaS infrastructures
#2 - lower the entry barrier for non-skilled scientists
Service request customization

The configuration form allows the user to specify requirements for the deployment in a straightforward way:

- checking the mandatory fields
- hiding the complexity of TOSCA
  - related fields are collapsed into a single input (e.g. num_cpu & mem_size into flavor)
  - complex TOSCA types are managed with dedicated Javascript functions (e.g. the ports specification)
Advanced configurations

The dashboard allows also to bypass the automatic scheduling implemented by the Orchestrator: the user can choose a specific provider to send his/her deployment request to.

Under the hood:

the drop-down menu is automatically created by the Dashboard interacting the SLA Manager Service to get the list of providers for the user; before submitting the request to the Orchestrator, the Dashboard completes the TOSCA template including the proper SLA placement policy:

```
policies:
  - deploy_on_specific_site:
      type: tosca.policies.indigo.SlaPlacement
      properties:
        sla_id: 5e1daa90d000a819fe11ca56
```
Deployment outputs and notifications

A notification system is implemented in the Dashboard: the user receives an automatic email as soon as the deployment is ready.

Then, the details about the deployed service can be accessed through the Dashboard.
Secrets management

The Dashboard is integrated with Hashicorp Vault (Secrets Manager) to support some functionalities, e.g.

- ssh key pair management
- service credentials store (e.g. AWS)

The Vault has been integrated with INFN Cloud IAM (jwt auth) and proper policies grant read and/or write permissions to specific Vault paths depending on the user claims.
Conclusions

• The INFN Cloud PaaS Dashboard makes it easy to discover, select, configure and request the deployment of services that fit the needs and requirements of the INFN research communities.
• New applications and services are continuously included in the catalogue and the Dashboard is enriched with new functionalities to support them.
• Both the addition of a new service in the marketplace and the federation of a new resource provider are quite simple processes, thanks to the flexibility and extensibility of the PaaS architecture and implementation.
Thank you for your attention!