INFN CCR
Istituto Nazionale di Fisica Nucleare
Commissione Calcolo e Reti

INFN CNAF
Istituto Nazionale di Fisica Nucleare
Centro Nazionale per la Ricerca e lo Sviluppo nelle Tecnologie Informatiche e Telematiche

IAM as a Service on INFN Cloud

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

Federica Fanzago (federica.fanzago@pd.infn.it)

Federico Fornari (federico.fornari@cnaf.infn.it)

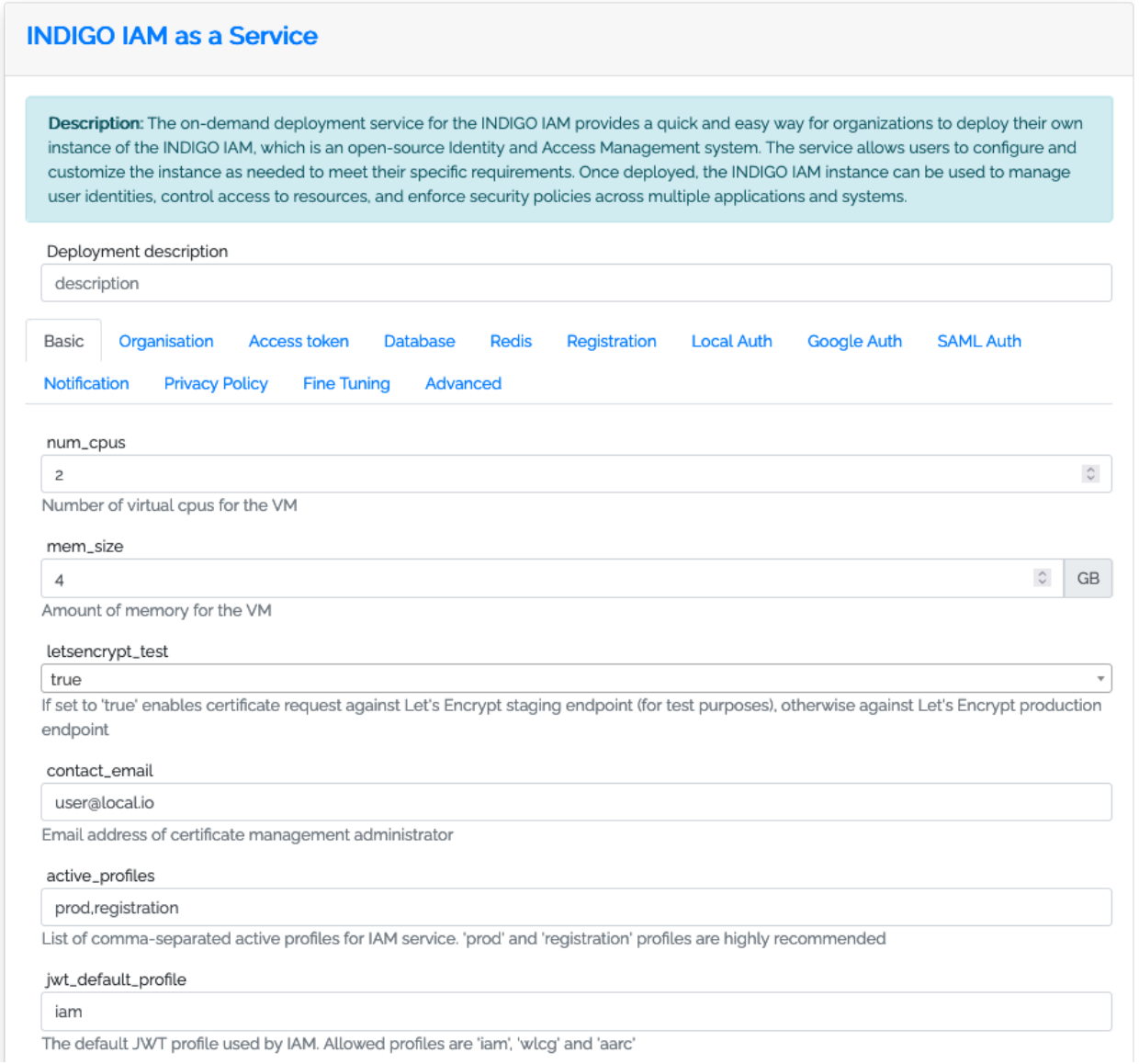
Introduction

- Why Indigo IAM as a Service on INFN Cloud?

- Because:
  - Many scientific collaborations and projects (including WLCG) leverage Indigo IAM as a powerful tool for Authentication and Authorization management
  - The most straightforward way to provide INFN researchers with Indigo IAM would be adding a related INFN Cloud service to the present Portfolio
- Why to provide it as a Cloud Service?
  - To facilitate the automatic instantiation of the service on a single VM, providing essential configuration parameters for the initialization

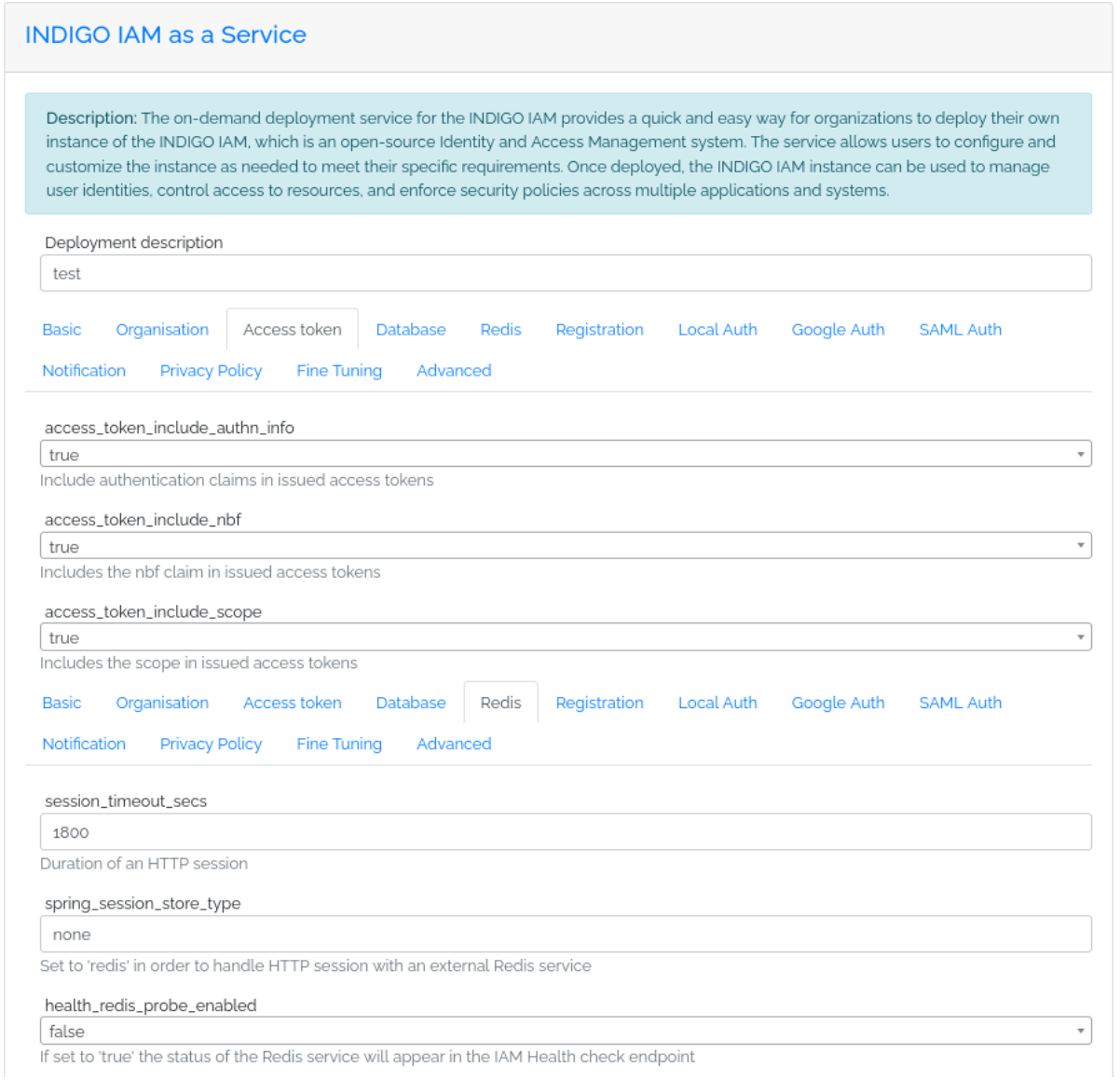
Basic Parameters

- **VM size**: memory, CPUs (default values are a good starting point)
- **letsencrypt_test**: default true to use Let's Encrypt test certificates
- **contact_email**: reference person's address for certificate renewal
- **active_profiles**: Spring profiles for IAM allowing user registration and password reset; optionally add *oidc* or *saml* for authentication with external providers
- **jwt_default_profile**: by default *iam*, used to configure the claims contained in the token; can also be *wlcg* or *aarc*



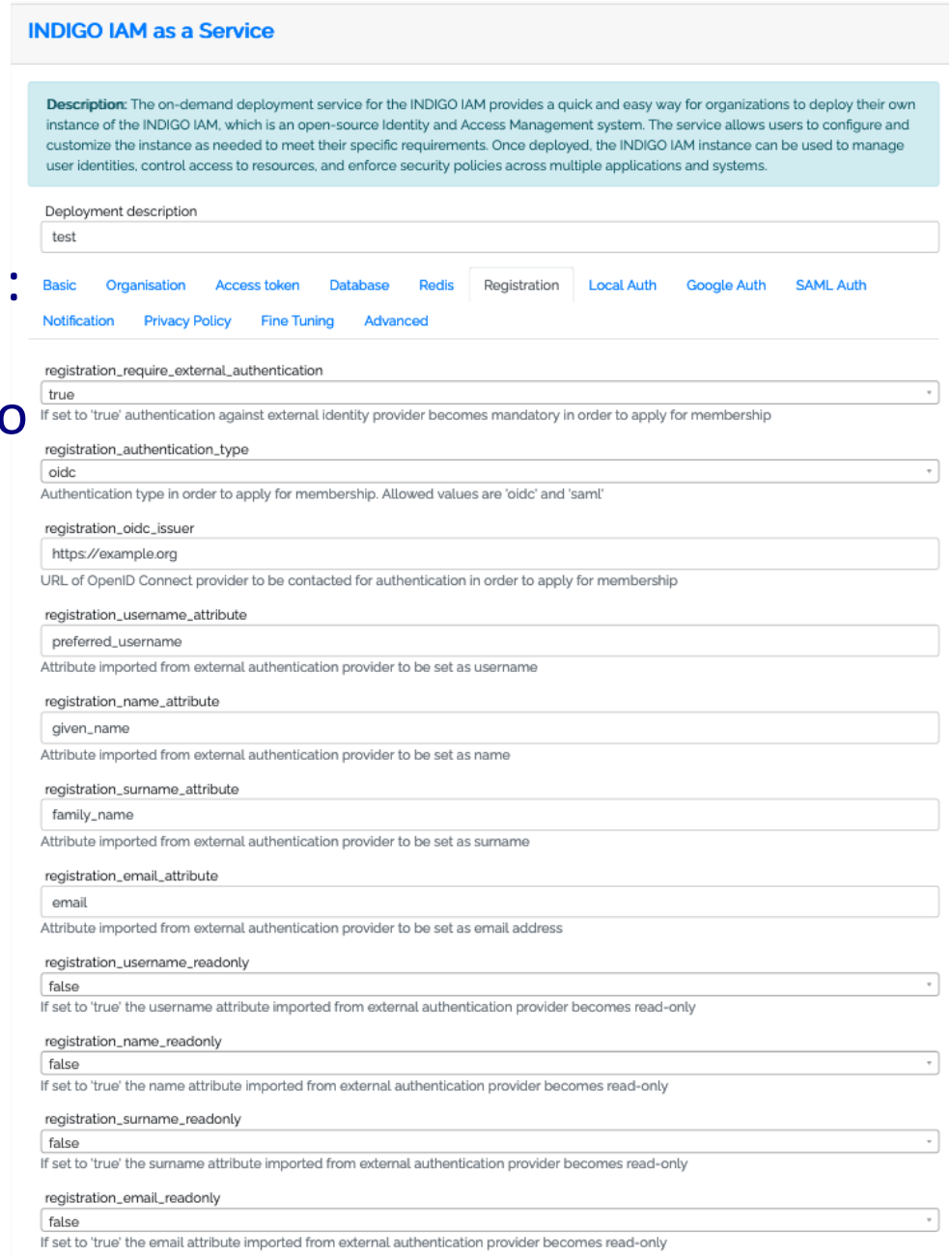
Token Profile and Redis

- **access_token_include_authn_info**: include user information in the token (username, groups, etc.)
- **access_token_include_nbf**: add an *nbf* claim to the token (*nbf* means *not before*, i.e. token validity starting point)
- **access_token_include_scope**: add the *scope* claim to the token
- To manage multiple backends it may be useful to configure **redis** to keep data consistent for a given user session



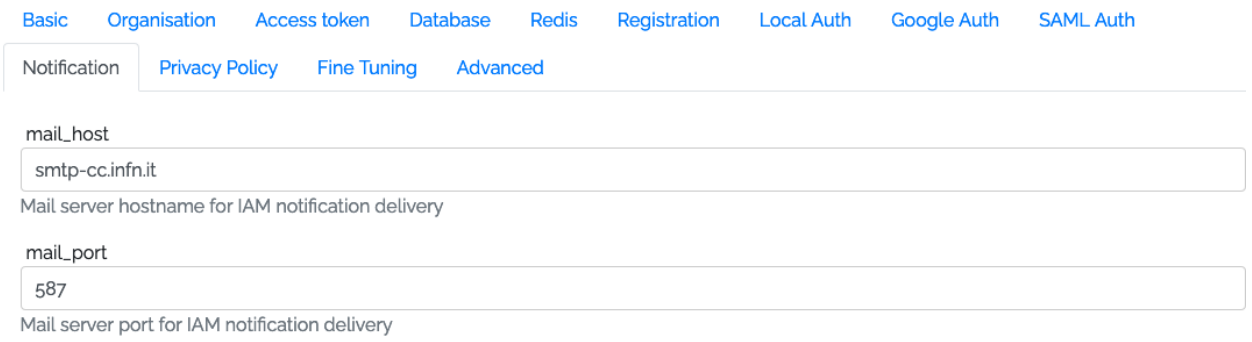
Registration Parameters

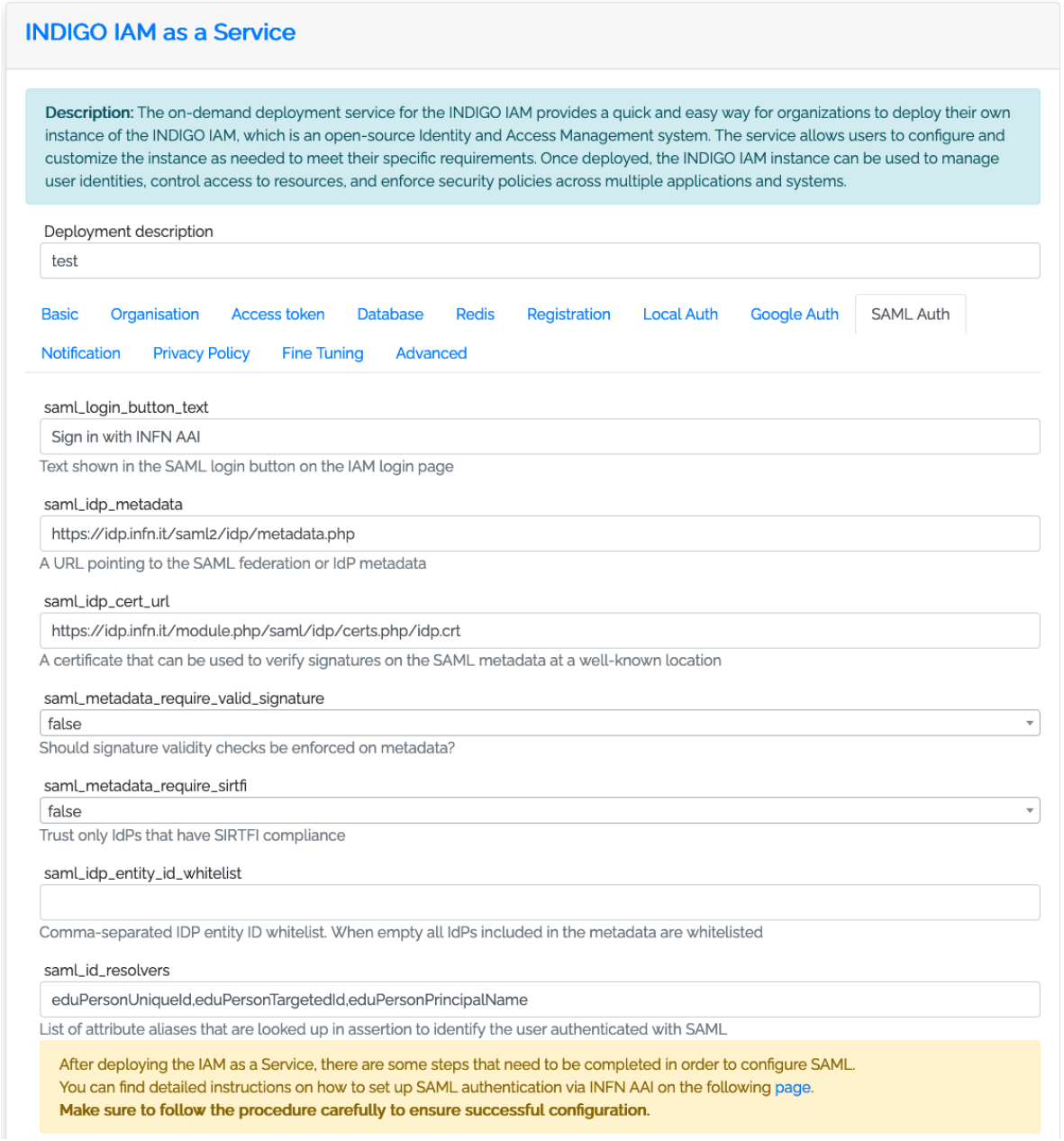
- **registration_require_external_authentication**: enable authentication for registration via external providers; by default it is false, if set to true you can choose between *oidc* and *saml*; besides, you need to add profile *oidc* or *saml* to **active_profiles** (see *Basic* parameters)
- **registration_[...]_attribute**: used to indicate which attributes provided by the external provider are taken as registration parameter values
- **registration_[...]_readonly**: if set to true prevents the user from changing the registration parameter imported from the external provider



SAML and Notifications

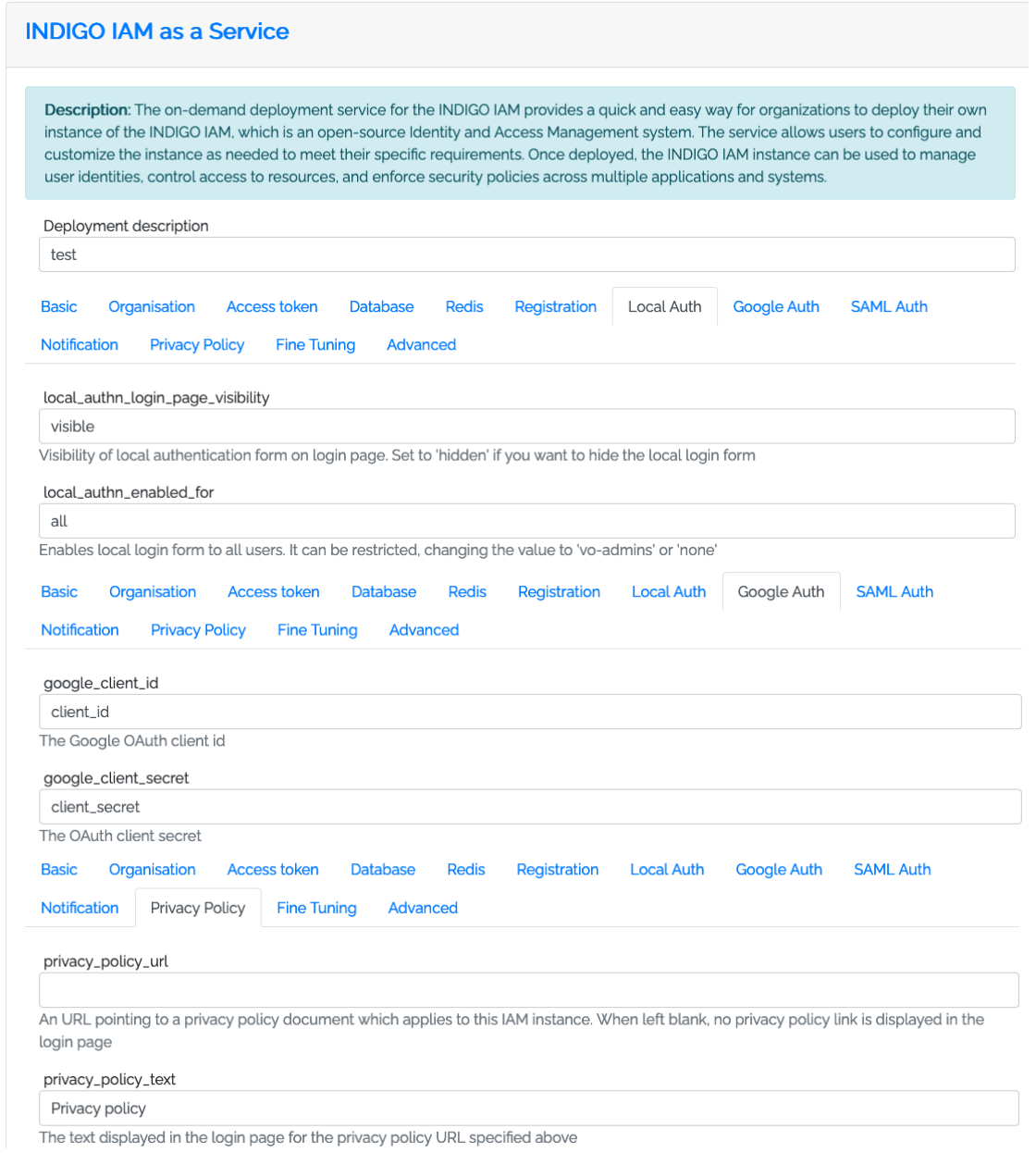
- **SAML Authentication** is by default configured to use the INFN AAI provider; some required actions before and after deployment are specified in a disclaimer
- **mail_host**: by default is set to the INFN mail server, which requires having an enabled account; otherwise you can use another suitably configured mail server





AuthN and Privacy Policy

- **local_authn_login_page_visibility**: allows the user to provide local username and password fields on the IAM login page
- **google_client_id** and **google_client_secret**: parameters of the Google OAuth client for authentication through Google as identity provider
- **privacy_policy_url**: parameter for policy acceptance by the user; the policy document must be provided via a URL
- For *Fine Tuning*, the most important parameter is **IAM version** (1.8.0 by default)



Conclusions and future plans

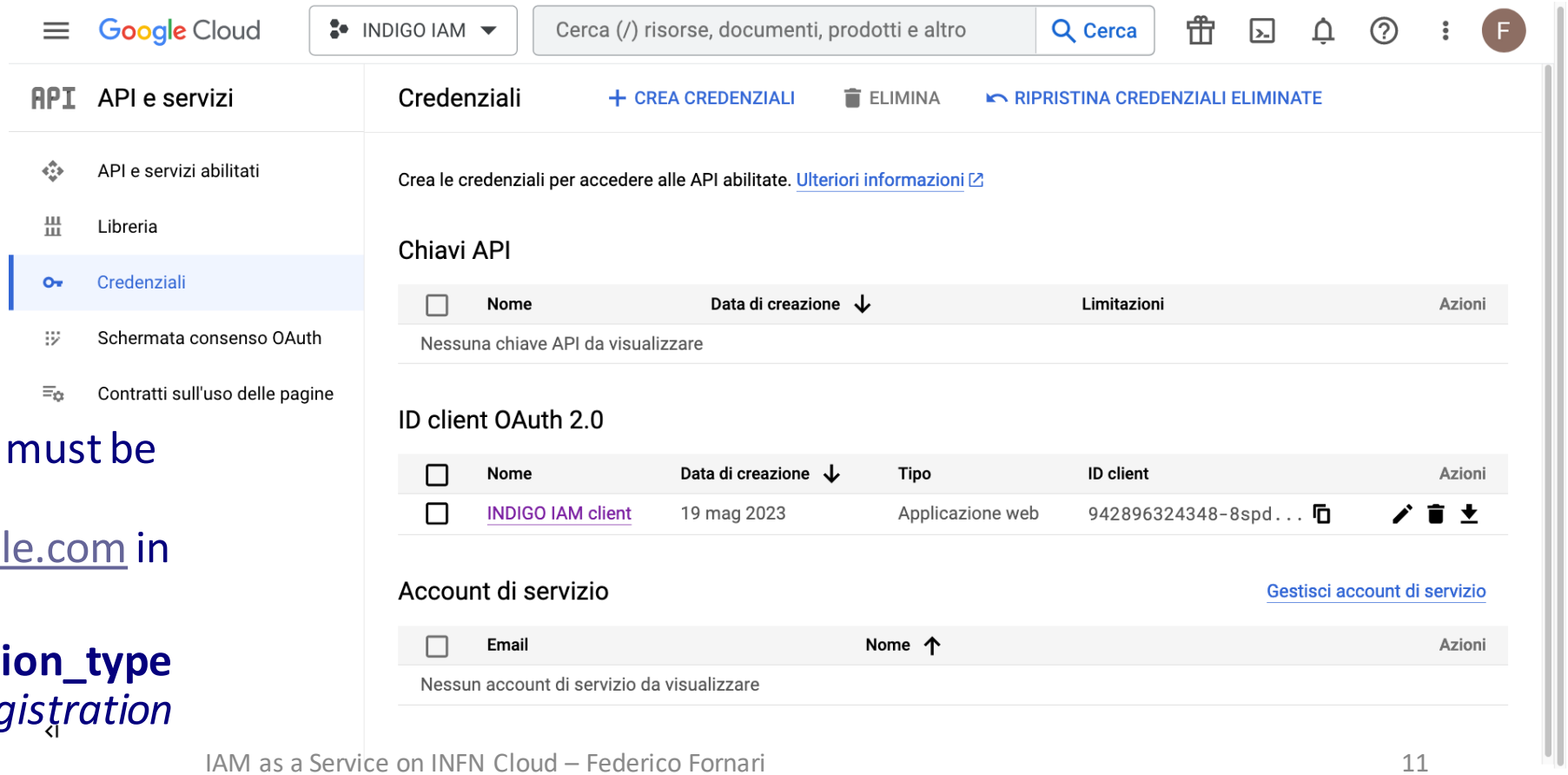
- Indigo IAM is a powerful tool to implement AuthN/AuthZ for the usage of computing and storage resources
- INFN Cloud users may efficiently configure, install and manage IAM instances through Indigo IAM as a Service
- The possibility to automatically add a DNS entry for a newly created IAM instance would let INFN Cloud users setup a more easily addressable service (DNS as a Service: WIP)
- The development of an automatic system for IGTF certificates request would be the key feature to integrate VOMS AA in IAM as a Service

THANK YOU VERY MUCH!

BACKUP SLIDES

Google OIDC Configuration for INDIGO IAM

- **google_client_id** and **google_client_secret** OAuth credentials can be generated after creating a Google Cloud Project, following the instructions available at https://developers.google.com/identity/openid-connect/openid-connect
- When setting up Google OpenID Connect Authentication, always remember that:
  - *oidc* must be added to **active_profiles** in *Basic* Parameters tab
  - **registration_oidc_issuer** must be set to https://accounts.google.com in *Registration* tab
  - **registration_authentication_type** must be set to *oidc* in *Registration* tab



Google OIDC Configuration for INDIGO IAM

- **After** IAM deployment, you must go back to your Google Cloud Project and update the *Redirect URI* for INDIGO IAM with a URL including the FQDN assigned to your instance