





# 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)

The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this license or copyright law is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this license.







### Introduction

Why Indigo IAM as a Service on INFN Cloud?





#### Because:

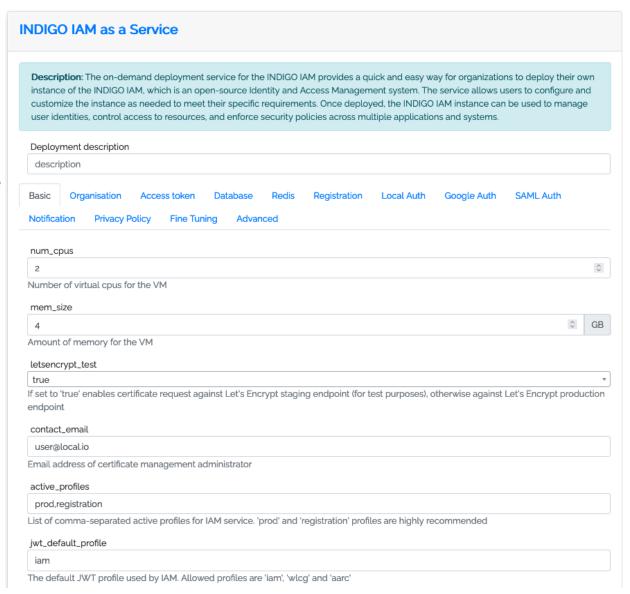
- Many scientific collaborations and projects (including WLCG) leverage Indigo IAM as a powerful tool for Authentication and Authorization management
- The most straightforward way to provide INFN researchers with Indigo IAM would be adding a related INFN Cloud service to the present Portfolio
- Why to provide it as a Cloud Service?
  - To facilitate the automatic instantiation of the service on a <u>single</u> 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

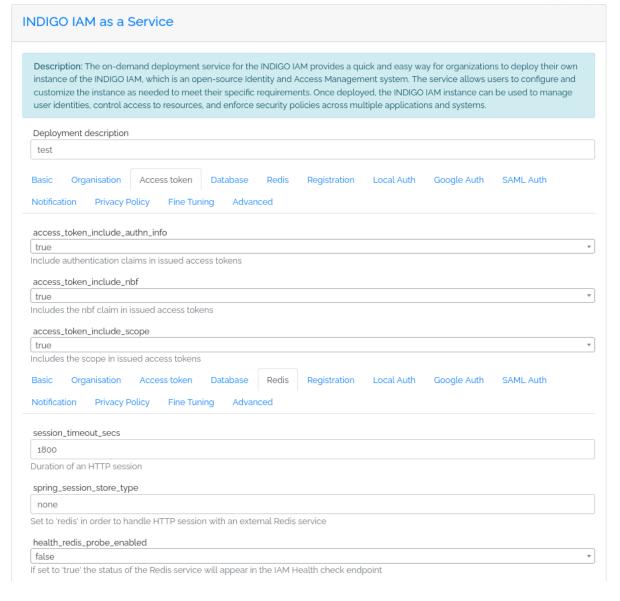






### **Token Profile and Redis**

- 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







#### INDIGO IAM as a Service

### **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

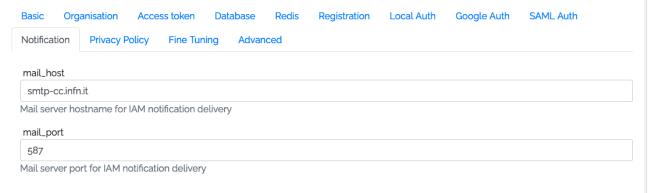
<b>Description</b> : The on-demand deployment service for the INDIGO IAM provides a quick and easy way for organizations to deploy their own instance of the INDIGO IAM, which is an open-source Identity and Access Management system. The service allows users to configure and customize the instance as needed to meet their specific requirements. Once deployed, the INDIGO IAM instance can be used to manage user identities, control access to resources, and enforce security policies across multiple applications and systems.	
Deployment description	
test	
Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth Notification Privacy Policy Fine Tuning Advanced	
registration_require_external_authentication	
true	٧
If set to 'true' authentication against external identity provider becomes mandatory in order to apply for membership	
registration_authentication_type	
oidc	*
Authentication type in order to apply for membership. Allowed values are 'oidc' and 'saml'	
registration_oidc_issuer	
https://example.org	
URL of OpenID Connect provider to be contacted for authentication in order to apply for membership	
registration username attribute	
registration_username_attribute	
preferred_username Attribute imported from external authentication provider to be set as username	
registration_name_attribute	
given_name	
Attribute imported from external authentication provider to be set as name	
registration_surname_attribute	
family_name	
Attribute imported from external authentication provider to be set as sumame	
registration amail attribute	
registration_email_attribute email	
Attribute imported from external authentication provider to be set as email address	
Autibute imported from external additional provider to be set as email address	
registration_username_readonly	
false	v
If set to 'true' the username attribute imported from external authentication provider becomes read-only	
registration_name_readonly	
false	*
If set to 'true' the name attribute imported from external authentication provider becomes read-only	
registration_surname_readonly	
false	*
If set to 'true' the surname attribute imported from external authentication provider becomes read-only	
registration_email_readonly	
false	v
If set to 'true' the email attribute imported from external authentication provider becomes read-only	





### **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



#### INDIGO IAM as a Service Description: The on-demand deployment service for the INDIGO IAM provides a quick and easy way for organizations to deploy their own instance of the INDIGO IAM, which is an open-source Identity and Access Management system. The service allows users to configure and customize the instance as needed to meet their specific requirements. Once deployed, the INDIGO IAM instance can be used to manage user identities, control access to resources, and enforce security policies across multiple applications and systems. Deployment description test SAML Auth saml\_login\_button\_text Sign in with INFN AAI Text shown in the SAML login button on the IAM login page saml\_idp\_metadata https://idp.infn.it/saml2/idp/metadata.php A URL pointing to the SAML federation or IdP metadata saml\_idp\_cert\_url https://idp.infn.it/module.php/saml/idp/certs.php/idp.crt A certificate that can be used to verify signatures on the SAML metadata at a well-known location saml\_metadata\_require\_valid\_signature Should signature validity checks be enforced on metadata? saml\_metadata\_require\_sirtfi Trust only IdPs that have SIRTFI compliance

After deploying the IAM as a Service, there are some steps that need to be completed in order to configure SAML. You can find detailed instructions on how to set up SAML authentication via INFN AAI on the following page.

Make sure to follow the procedure carefully to ensure successful configuration.

Comma-separated IDP entity ID whitelist. When empty all IdPs included in the metadata are whitelisted

List of attribute aliases that are looked up in assertion to identify the user authenticated with SAML

edu Person Unique Id, edu Person Targeted Id, edu Person Principal Name

saml\_idp\_entity\_id\_whitelist

saml\_id\_resolvers





## **AuthNand 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)

#### INDIGO IAM as a Service

Description: The on-demand deployment service for the INDIGO IAM provides a quick and easy way for organizations to deploy their own instance of the INDIGO IAM, which is an open-source Identity and Access Management system. The service allows users to configure and customize the instance as needed to meet their specific requirements. Once deployed, the INDIGO IAM instance can be used to manage user identities, control access to resources, and enforce security policies across multiple applications and systems. Deployment description local\_authn\_login\_page\_visibility Visibility of local authentication form on login page. Set to 'hidden' if you want to hide the local login form local authn enabled for Enables local login form to all users. It can be restricted, changing the value to 'vo-admins' or 'none Google Auth google\_client\_id client\_id The Google OAuth client id google\_client\_secret client\_secret The OAuth client secret privacy\_policy\_url An URL pointing to a privacy policy document which applies to this IAM instance. When left blank, no privacy policy link is displayed in the privacy\_policy\_text Privacy policy The text displayed in the login page for the privacy policy URL specified above





## 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 Cloud

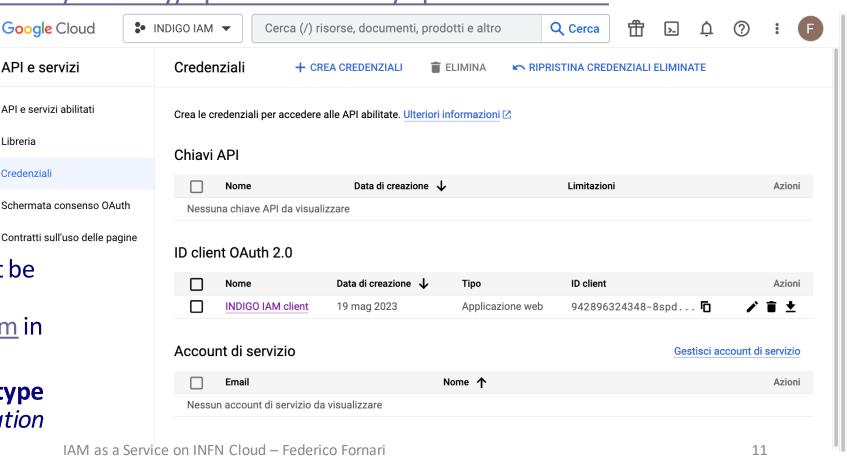
API e servizi abilitati

API e servizi

Libreria

Credenziali

- **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

