



Istituto Nazionale di Fisica Nucleare
Commissione Calcolo e Reti



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@cnafe.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?



INDIGO IAM as a Service



- 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*

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
description

Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth
Notification Privacy Policy Fine Tuning Advanced

num_cpus
2
Number of virtual cpus for the VM

mem_size
4 GB
Amount of memory for the VM

letsencrypt_test
true
If set to 'true' enables certificate request against Let's Encrypt staging endpoint (for test purposes), otherwise against Let's Encrypt production endpoint

contact_email
user@local.io
Email address of certificate management administrator

active_profiles
prod,registration
List of comma-separated active profiles for IAM service. 'prod' and 'registration' profiles are highly recommended

jwt_default_profile
iam
The default JWT profile used by IAM. Allowed profiles are 'iam', 'wlcg' and '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

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

Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth

Notification Privacy Policy Fine Tuning Advanced

access_token_include_authn_info

true

Include authentication claims in issued access tokens

access_token_include_nbf

true

Includes the nbf claim in issued access tokens

access_token_include_scope

true

Includes the scope in issued access tokens

Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth

Notification Privacy Policy Fine Tuning Advanced

session_timeout_secs

1800

Duration of an HTTP session

spring_session_store_type

none

Set to 'redis' in order to handle HTTP session with an external Redis service

health_redis_probe_enabled

false

If set to 'true' the status of the Redis service will appear in the IAM Health check endpoint

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

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

Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth

Notification Privacy Policy Fine Tuning Advanced

registration_require_external_authentication

true

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

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 surname

registration_email_attribute

email

Attribute imported from external authentication provider to be set as email address

registration_username_readonly

false

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

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

Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth

Notification Privacy Policy Fine Tuning Advanced

mail_host
smtp-cc.infn.it
Mail server hostname for IAM notification delivery

mail_port
587
Mail server port for IAM notification delivery

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

Basic Organisation Access token Database Redis Registration Local Auth Google Auth SAML Auth

Notification Privacy Policy Fine Tuning Advanced

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
false
Should signature validity checks be enforced on metadata?

saml_metadata_require_sirtfi
false
Trust only IdPs that have SIRTFI compliance

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

saml_id_resolvers
eduPersonUniqueid,eduPersonTargetedId,eduPersonPrincipalName
List of attribute aliases that are looked up in assertion to identify the user authenticated with SAML

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.

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)

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

[Basic](#) [Organisation](#) [Access token](#) [Database](#) [Redis](#) [Registration](#) [Local Auth](#) [Google Auth](#) [SAML Auth](#)

[Notification](#) [Privacy Policy](#) [Fine Tuning](#) [Advanced](#)

local_authn_login_page_visibility

visible

Visibility of local authentication form on login page. Set to 'hidden' if you want to hide the local login form

local_authn_enabled_for

all

Enables local login form to all users. It can be restricted, changing the value to 'vo-admins' or 'none'

[Basic](#) [Organisation](#) [Access token](#) [Database](#) [Redis](#) [Registration](#) [Local Auth](#) [Google Auth](#) [SAML Auth](#)

[Notification](#) [Privacy Policy](#) [Fine Tuning](#) [Advanced](#)

google_client_id

client_id

The Google OAuth client id

google_client_secret

client_secret

The OAuth client secret

[Basic](#) [Organisation](#) [Access token](#) [Database](#) [Redis](#) [Registration](#) [Local Auth](#) [Google Auth](#) [SAML Auth](#)

[Notification](#) [Privacy Policy](#) [Fine Tuning](#) [Advanced](#)

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 login page

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_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

The screenshot shows the Google Cloud IAM console interface. The top navigation bar includes the Google Cloud logo, the project name 'INDIGO IAM', and a search bar. The left sidebar contains a menu with 'API e servizi' selected, and sub-items: 'API e servizi abilitati', 'Libreria', 'Credenziali' (highlighted), 'Schermata consenso OAuth', and 'Contratti sull'uso delle pagine'. The main content area is titled 'Credenziali' and includes buttons for '+ CREA CREDENZIALI', 'ELIMINA', and 'RIPRISTINA CREDENZIALI ELIMINATE'. Below this, there are three sections:

- Chiavi API**: A table with columns 'Nome', 'Data di creazione', 'Limitazioni', and 'Azioni'. It shows 'Nessuna chiave API da visualizzare'.
- ID client OAuth 2.0**: A table with columns 'Nome', 'Data di creazione', 'Tipo', 'ID client', and 'Azioni'. It contains one entry: 'INDIGO IAM client' created on '19 mag 2023', of type 'Applicazione web', with ID '942896324348-8spd...'. Action icons for edit, delete, and download are visible.
- Account di servizio**: A table with columns 'Email' and 'Nome'. It shows 'Nessun account di servizio da visualizzare'.

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**

The screenshot shows the Google Cloud IAM console interface. At the top, there is a navigation bar with the Google Cloud logo, a dropdown menu for 'INDIGO IAM', and several utility icons (search, gift, code, bell, help, and a profile icon 'F'). Below the navigation bar, a sidebar on the left lists various API and service options: 'API e servizi', 'API e servizi abilitati', 'Libreria', 'Credenziali' (highlighted in blue), 'Schermata consenso OAuth', and 'Contratti sull'uso delle pagine'. The main content area is titled 'ID client per Applicazione web' and includes an 'ELIMINA' button. The text below the title reads 'Per l'uso con richieste provenienti da un server web'. A text input field labeled 'URI 1 *' contains the URL 'https://90.147.174.40.myip.cloud.infn.it/openid_connect_login'. Below the input field is a '+ AGGIUNGI URI' button. At the bottom of the main area, there is a note: 'Nota: l'applicazione delle impostazioni potrebbe richiedere da cinque minuti a qualche ora'. At the very bottom, there are two buttons: 'SALVA' and 'ANNULLA'.