Introduction

• Fernando Aguilar
  • IFCA (CSIC-UC), Computing resources
  • Service development
  • LifeWatch ERIC PPP, EGI-LifeWatch Competence Centre

• LifeWatch-ERIC
  • RI for Biodiversity and Ecosystem research in Europe
  • LifeWatch-ERIC seeks to understand the complex interactions between species and the environment, taking advantage of High-Performance, Grid and Big Data computing systems, and the development of advanced modelling tools to implement management measures aimed at preserving life on Earth.

• How?
  • Offering new opportunities for large-scale scientific development
  • Enabling accelerated data capture with innovative new technologies
  • Supporting knowledge-based decision-making for biodiversity and ecosystem management
  • Providing training, dissemination and awareness programmes.
The problem

Current Status
- Different Roles
- Different institutions
- Different Services
- Different AAI
Roles/Users

Who/Where are your users typically?
• LifeWatch ICT sites administrators
• LifeWatch Developers (Solvers)
• LifeWatch Researchers
• Citizen Scientists

What kinds of resources do they need to access?
• Infrastructures (IaaS): Site administrators
• PaaS: Solvers
• Applications (SaaS): Solvers Researchers, Citizen Scientists

Where are the resources hosted?
• ICT Core (Distributed). Links to EGI.
General Information for the Solution

• The central system will run at the LW ICT Core in Spain

• It will provide authentication and authorization services for all LW central and distributed systems, as well as other interested e-infrastructures like EMBRC, DiSSCO.

• It will allow cross-authentication with other identity providers like eduGain, EGI, etc.

• Selected solution must be deployed in the LifeWatch ICT Core.

• The IDP will be used:

  • to give access to restricted LW services. The services may be restricted because of processing power or storage demands.
    • to protect user data and scripts that are stored on the infrastructure (unix home folders, etc)
    • to give access to data not yet in the public domain. (data in databases, project moratorium period)
    • to distinguish between users uploading data to the system (RvLab, eLab, data explorer)
    • to give access to Openstack configuration interface and computing resources at infrastructure layer.
    • To manage roles/groups and authorize them to access specific services.

• Currently, the different user apps manage their own users. The institutional credentials could be federated in the Identity Provider.

• Two components suggested by AARC: Identity Provider, Token Translator System.
INDIGO IAM – First Choice

• Compatible: OIDC (priority), SAML (interesting, eduGain).
• Federation of 1-N Institutions. Citizen Scientists (Social IDs).
• Roles Management. Role mapping (e.g. Google users to Citizen Scientist).
• Identity linking (optional).
• Group Management. Some groups are allowed to do...
• Distributed, clustered. High availability. Via Database.

• Deployed, but problems with federating N IdPs.
Solution (Keycloak)

- Compatible: OIDC (priority), SAML (interesting, eduGain).
- Federation of 1-N Institutions. Citizen Scientists (Social IDs).
- Roles Management. Role mapping (e.g. Google users to Citizen Scientist).
- Identity linking (optional).
- Group Management. Some groups are allowed to do...
- Distributed, clustered. High availability. NATIVE
LifeWatch Pilot – AARC BPA
Keycloak – User Roles, Groups

Users coming from Google IdP are mapped to Citizen group.

Users are manually added Admin group
Configure userinfo

Client Templates > template_test > Mappers > test_role

- Protocol: openid-connect
- ID: db48c16b-014b-4adc-b399-21eb3bf3add9
- Name: test_role
- Consent Required: OFF
- Mapper Type: User Realm Role
- Realm Role Prefix: role_
- Multivalued: OFF
- Token Claim Name: role
- Claim JSON Type: String
- Add to ID token: OFF
- Add to access token: OFF
- Add to userinfo: ON

Save | Cancel
More Role mapping

Add Identity Provider Mapper

Name: CSIC_users
Mapper Type: SAML Attribute to Role
Attribute Name: urn:mace:terena.org:shac1:attribute-def:scac.personalUniqueID
Friendly Name:
Attribute Value: CSIC.es
Role: Developer

EduGain_users

ID: 3d462ae6-54a3-4879-863f-54994f7094c
Name: eduGain_users
Mapper Type: Hardcoded Role
Role: CitizenScientists

636176@csic.es

Role Mappings

Realm Roles
Available Roles:
admin
create-realm

Assigned Roles:
CitizenScientists
Developer
offline_access
uma_authorization

Effective Roles:
CitizenScientists
Developer
offline_access
uma_authorization

Client Roles
Select client to view roles for client

Save Cancel
Simple Python OIDC script to test

{"family_name": 'Aguilar', 'email': 'aguilarf@unican.es', 'sub': 'c6d064d1-b016-49b1-8bde-3ceb12d22abd', 'given_name': 'Fernando0', 'role': '[role_offline_access, role_admin, role_create-realm, role_uma_authorization]', 'preferred_username': 'admin', 'name': 'Fernando0 Aguilar'}

{"family_name": 'Aguilar', 'email': 'fernandoaguilar87@gmail.com', 'sub': 'a05bf658-2b1f-4725-8a06-50edae99d88f', 'given_name': 'Fernando Aguilar', 'role': '[role_offline_access, role_CitizenScientists, role_uma_authorization]', 'preferred_username': 'fernandoaguilar87@gmail.com', 'name': 'Fernando Aguilar'}
Keycloak – App Configuration

• Web based applications:
  • Rshiny (OIDC under Apache), Rstudio (Native plugin in pro version)
  • Data Portals: GBIF, Digital Knowledge Preservation Framework (EOSChub), Automatic Image Analysis (OIDC under Apache), etc.
  • Citizen Science apps: Natusfera, PAIRQURS (with EUDAT services).
  • Geoserver (OIDC plugin), GIS-based services.

• Applications with bridges to HPC.
  • RvLab (Internal User DB) – TTS needed
  • TRUFA (slurm batch system) – Internal User DB - TTS needed

• Mobile Apps
  • Natusfera App
  • Plant classification

• Cloud Computing resources.
  • OpenStack (OIDC compatible. Tested with IFCA SSO)
• Keycloak deployed in test environment.
• IdP Federation: IFCA SSO, Google, Github, internal users.
• Test with WikiToLearn solution for federation eduGAIN.
• REDIRIS support to federate eduGAIN.
• Configuration analysis.
• Role mapping.
• Role in userinfo for OIDC.
• Plugin developments: TRUFA, OpenStack keystone (supported by EGI).
• Planning deployment in production: High Availability, distributed.
Lessons learned

• Proposed solutions (EGI check-in, B2ACCESS, INDIGO IAM). All of them OK.
• Keycloak selected due to specific characteristics, “easy” to deploy/maintain, flexible, different operational modes...
• Very customized config
• Recommendations:
  • Analyze your services, users.
  • Try to be open: your needs could change.
  • Standard technologies
  • I recommend Keycloak as solution
• Future plan
  • Deploy on production: Critical service = High Availability
  • Be integrated in LifeWatch portal. Official IdP
  • Integrated in LFW services
Thank you
Any Questions?

fernando.aguilar@lifewatch.eu