Sensitive data

Alice AINSA

Access to sensitive data

Access to sensitive date

We want OpenObs users to be able to request access to the exact location of sensitive data within a specific geographical and taxonomic scope.

User not connected

- All basic features
- Reporting an observation to change its validity level
- Create an account & log in

User connected Role User

- Requests for viewing sensitive data
- Requests for validation of reports + viewing sensitive data

Rights to access sensitive data

- View precise location within accepted perimeters (geographical & taxonomic scope)

Rights to validation (within the accepted perimeters)

- View sensitive data
- View reports
- Modify validity level

User connected Role Admin

- Manages user rights request (Administration tab)

Steps needed

For sensitive data visualisation :

- Connection module with differents roles
- Request form for access to sensitive data within a specific scope
- Secure the access root to sensitive data (ensure that only authorized users can access precise locations within the defined scope)
- Add new fields to the database (related to unblurred location)
- Visualize sensitive data

Connection

Connection module

Connection using ala-security-project : https://github.com/AtlasOfLivingAustralia/ala-security-project
& ala-auth : https://github.com/AtlasOfLivingAustralia/ala-security-project/tree/develop/ala-auth

We use INPN CAS, already used by the INPN website
Different Roles are defined (Admin, User, Validator)

This integration is essential to ensure that only authorized persons can access to the request form

In practice, easy to implement : only configuration needs to be set
Map the fields with the names on our CAS (in French)
→ ALA expects attributes in English, and the CAS returns them in French
Find the correct file to modify the configuration :
→ openobs-hub : application.groovy & application.yml
→ install-docker : biocache-hub-config.properties

Connection

OpenobsAuthService.groovy

```
    UserDetails userDetails() {
        return userApiService.findById(getUserId())
//        new UserDetails(
//                id: Long.valueOf(authService.getUserId()),
//                userId: authService.getUserId(),
//                userName: authService.getUserName()?.toLowerCase(),
//                email: authService.getEmail()?.toLowerCase(),
//                firstName: authService.getFirstName() ?: "",
//                lastName: authService.getLastName() ?: "",
//                locked: false,
//                activated: true,
//                roles: authService.getUserRoles()
//            )
    }
```

Fields names


```
"login" : "soudin",
"cryptedPassword" : "5e5cc2a5717d827a2ceb6129348c37fd96964384",
"lastname" : "Oudin",
"firstname" : "Simon",
"civility" : "Mme",
"address" : null,
"email" : "simon.oudin@mnhn.fr",
"pseudo" : null,
"phone" : null,
"fax" : null,
"comment" : null,
"regionId" : null,
"organization" : {
  "id" : null,
  "name" : "Pastrèsnet"
},
```

Connection

openobs-install-docker : biocache-hub-config.properties

config/biocache-hub-config.properties

```
@@ -187,10 +187,26 @@ odataws.organizations.public.param=openObsContributor=true
187 187 logger.baseUrl=$SERVER_URL/logger-service/service
188 188
189 189 # CAS Config
190     - security.cas.bypass=true
191     - disableCAS=true
192     - webservice.jwt=false
193     - security.cas.service=$SERVER_URL/openobs-hub
    190 + #security.cas.bypass=true
    191 + #webservice.jwt=false
    192 + #security.cas.service=$SERVER_URL/openobs-hub
    193 +
    194 + disableCAS=false
    195 +
    196 + ## Openobs specific
    197 + security.cas.appServerName = $SERVER_URL
    198 + security.cas.casServerName=$CAS_URL
    199 + security.cas.casServerUrlPrefix=$CAS_URL/auth
    200 + security.cas.loginUrl=$CAS_URL/auth/login
    201 + security.cas.logoutUrl=$CAS_URL/auth/logout
    202 + auth.admin_role = "INPN_USER"
    203 +
    204 + ## Ala specific
    205 + security.cas.roleAttribute=authority
    206 + security.cas.ignoreCase=true
    207 + security.cas.authCookieName=ALA-Auth
    208 + security.cas.uriFilterPattern=/admin.*,/alaAdmin.*,/download.*
    209 + security.cas.uriExclusionFilterPattern=/occurrences/shapeUpload,/img.*,/css.*,/js.*,.*json,/help/.*
```

openobs-hub

grails-app/conf/application.groovy

```
@@ -56,16 +56,7 @@ headerAndFooter.baseURL= "http://localhost"
56 56  *  NOTE: Some of these will be ignored if default_config exists
57 57 \**********************************************************************/
58 58 grails.serverURL = 'https://10.0.57.28/ala-hub'
59     - serverName = 'https://10.0.57.28/ala-hub'
60     - security.cas.appServerName = "https://10.0.57.28/ala-hub"
61     - security.cas.service = "https://10.0.57.28/ala-hub"
62     - security.cas.casServerName = 'http://test-cas-patrinat.mnhn.fr/'
63     - security.cas.loginUrl = 'http://test-cas-patrinat.mnhn.fr/auth/login'
64     - security.cas.logoutUrl = 'http://test-cas-patrinat.mnhn.fr/auth/logout'
65     - security.cas.casServerUrlPrefix = 'http://test-cas-patrinat.mnhn.fr/auth/'
66     - security.cas.bypass = false // set to true for non-ALA deployment
67     - auth.admin_role = "ROLE_ADMIN"
68     -
    59 + ignoreCookie= 'true'
69 60 useDownloadPlugin=true
70 61 allowDownload=false
```

grails-app/conf/application.yml

```
@@ -104,13 +104,3 @@ headerAndFooter:
104 104 server:
105 105     servlet:
106 106         contextPath: '/openobs-hub'
107     -
108     - security:
109     -     cas:
110     -         enabled: false # default is true, undefined behaviour if this omitted
111     -     oidc:
112     -         enabled: true # default is false
113     -         discoveryUri: 'https://auth-test.ala.org.au/cas/oidc/.well-known'
114     -         clientId: 'change me'
115     -         secret: 'change me'
116     -         scope: 'openid profile email ala roles'
    107 \ No newline at end of file
```

Request form

Request form for access to sensitive data within a specific scope

Addition on our side on openobs-hub with GORM grails.
Online documentation : https://gorm.grails.org/latest/hibernate/manual/index.html to create a specific database with the differents requests

We had to modify 2 configurations files in 2 different project ...

config/biocache-hub-config.properties +10 −0 Viewed

```
@@ -170,6 +170,16 @@ downloads.staticDownloadsUrl=
# Other settings
################################################################################

# Hibernate settings
hibernate.dialect=org.hibernate.dialect.PostgreSQLDialect
#hibernate.hbm2ddl.auto=create-drop
hibernate.hbm2ddl.auto=update

# GORM settings
grails.gorm.default.constraints=nullable:false
grails.gorm.autowire=true
grails.gorm.events=true

# OpenObs API REST URL
openobs.rest.baseUrl=http://restapi:8080/api
```

grails-app/conf/application.yml

```
@@ -116,4 +116,37 @@ security:
        discoveryUri: 'https://auth-test.ala.org.au/cas/oidc/.well-known'
        clientId: 'change me'
        secret: 'change me'
-       scope: 'openid profile email ala roles'
\ No newline at end of file
+       scope: 'openid profile email ala roles'
+
+---
+
+hibernate:
+    cache:
+        queries: false
+        use_second_level_cache: false
+        use_query_cache: false
+
+dataSource:
+    pooled: true
+    jmxExport: true
+    driverClassName: org.postgresql.Driver
+    dialect: org.hibernate.dialect.PostgreSQLDialect
+    username: validation
+    password: validation
+
+
+environments:
+    development:
+        dataSource:
+            dbCreate: update
+            url: jdbc:postgresql://bddopenobs:5432/validation
+    test:
+        dataSource:
+            dbCreate: update
+            url: jdbc:postgresql://bddopenobs:5432/validation
+    production:
+        dataSource:
+#           dbCreate: create-drop
+            dbCreate: update
+            url: jdbc:postgresql://bddopenobs:5432/validation
+
```

Request form

Bienvenue
Alice AINSA

Mon compte

Accéder à vos infos
Déconnexion
Voir mes demandes
Demander des droits
Gérer les droits

Cadre de la demande / du projet *

- ☐ Etude naturaliste
- ☐ Etude d'impact
- ☐ Recherche scientifique (thèse, etc...)
- ☐ Publication (atlas, présentation, etc)
- ☐ Programme dans le cadre d'un appui à la décision publique
- ☐ Programme conventionné avec PatriNat
- ☐ Echange entre plateformes du SINP
- ☐ Autre

'otre demande s'inscrit dans le cadre d'un projet, précisez :

Nom du projet *

Périmètre géographique *

Périmètre taxonomique *

Description du projet *

Informations générales sur la demande

Emprise géographique *

- ○ Ensemble de la France métropolitaine et des territoires d'outre-mer (continental et marin)
- ○ Choisir le zonage

Emprise taxonomique *

- ○ Groupes grand public
- ○ Autre groupe

Précision sur la demande *

☐ J'accepte les conditions d'utilisation des données *

☐ Je m'engage à partager les nouvelles données générées au cours de mon projet et à accepter leur partage et leur diffusion dans le cadre du Système d'information de l'inventaire du patrimoine naturel *

soumettre effacer

Secure access roots

Secure the access roots to sensitive data

Try with ALA using oicd and jwt

Servers

http://openobs.test.mnhn.fr/biocache-service - Generated server url

Available authorizations ×

JWT (http, Bearer)

Value:

Authorize Close

Authorize

Download Services for downloading occurrences and specimen data

- GET /occurrences/offline/download Asynchronous occurrence download
- POST /occurrences/offline/download Asynchronous occurrence download
- GET /occurrences/facets/download Downloads the complete list of values in the supplied facet

sensitive-controller

- GET /sensitive/secured
- GET /sensitive/public

Secure access roots

Only configuration modification to add oicd and jwt
Using Keycloack to generate token (jwt)

```
{
  "sub": "1234567890",
  "name": "Alice",
  "iat": 1516239022,
  "geom": "France",
  "taxa": "Mammals"
}
```

Secure with params geom & taxa ?

```
  security:
    oauth2:
      resourceserver:
        jwt:
          issuer-uri: http://localhost:7080/realms/Openobs  # URL du fournisseur OIDC
          jwk-set-uri: http://localhost:7080/realms/Openobs/protocol/openid-connect/certs  # URL du JWKSet
pac4j:
  oidc:
    client-id: openobs_biocacheservice_client
    client-secret: 'WOc11umJVRDeEJrpK6fL6IjbsLm2WzuN'
    discovery-uri: http://localhost:7080/realms/Openobs/.well-known/openid-configuration
    jwk-set-uri: http://localhost:7080/realms/Openobs/protocol/openid-connect/certs
security:
  oidc:
    enabled: true
    ala-userid-claim: sub
    scope: "openid profile email roles taxo geom"
    custom-params: "taxo: poissons"

  jwt:
    enabled: true
    clientId: 'openobs_biocacheservice_client'
    secret: 'WOc11umJVRDeEJrpK6fL6IjbsLm2WzuN'
    discoveryUri: 'http://localhost:7080/realms/Openobs/.well-known/openid-configuration'
```

Secure access roots

Other possibility with spring security by creating a new filter : JwtAuthenticationFilter.java
→ Create a JWTpersonalized

src/main/java/au/org/ala/biocache/config/SecurityConfig.java +2 −1 View file @ 09616f93

```
1   1   package au.org.ala.biocache.config;
2   2
    3 + import au.org.ala.ws.JwtAuthenticationFilter;
3   4   import au.org.ala.ws.security.AlaWebServiceAuthFilter;
4   5
5   6   import org.pac4j.core.config.Config;
... ... @@ -28,8 +29,8 @@ public class SecurityConfig extends WebSecurityConfigurerAdapter {
28  29      @Override
29  30      protected void configure(HttpSecurity http) throws Exception {
30  31
    32 +         http.addFilterBefore(new JwtAuthenticationFilter(), BasicAuthenticationFilter.class);
31  33
32      -         http.addFilterBefore(alaWebServiceAuthFilter, BasicAuthenticationFilter.class);
33  34          http.authorizeRequests()
34  35                  .antMatchers(
35  36                          "/",
... ...
```

New fields

Add new fields to the database (related to unblurred location)

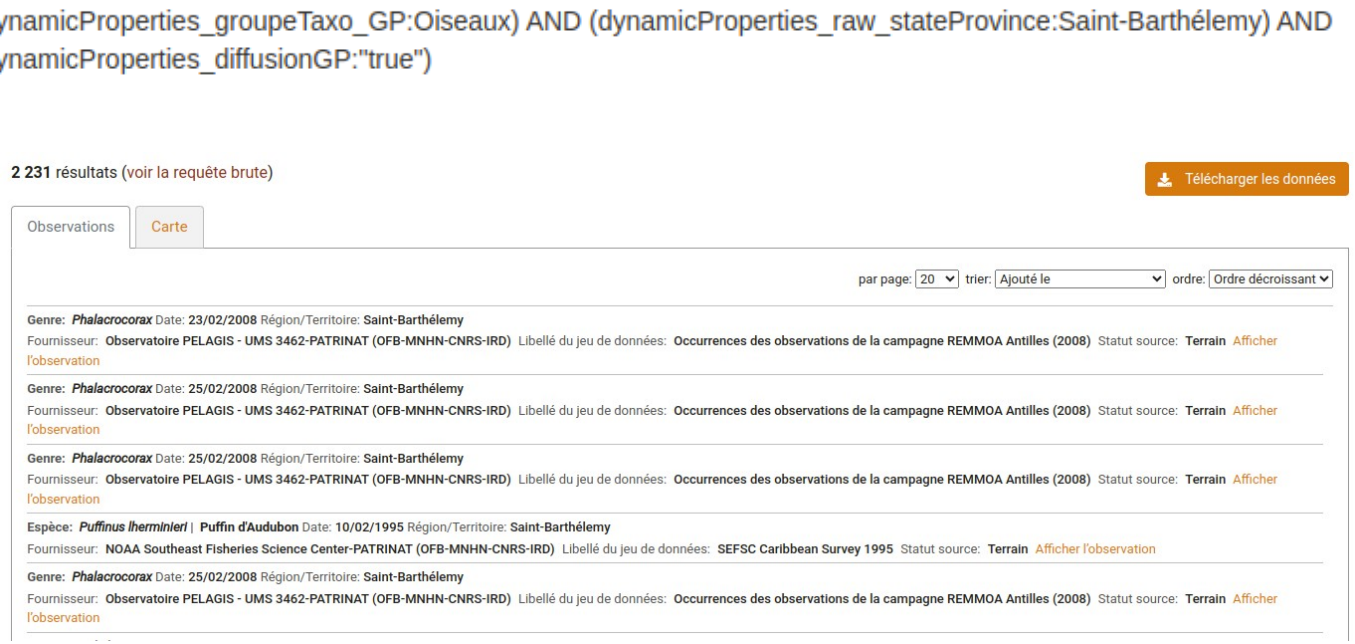
New fields for each sensitive data with location precision (minimumElevationInMeters**C**, maximumElevationInMeters**C**, minimumDepthInMeters**C**, maximumDepthInMetersC, decimalLatitudeC, decimalLongitudeC, coordinateUncertaintyInMetersC, natureObjetGeoC, geodeticDatumC, dataGeneralizationsC, localityC, municipalityC, municipalityCodeC, municipalityResearchC, epciC, epciCodeC,countyC, countyCodeC, stateProvinceC, stateProvinceCodeC, maille10CodeC, footprintWKTC)

→ same names ending with C

Research

Result of the research

Once the request for access to sensitive data has been approved for a specific geographical and taxonomic scope, the idea is that the search results will filter the data accordingly, displaying the values of the new database fields, such as municipalityC instead of municipality, both on the map and on the detail pages.



Issues

- Lack of documentation on ALA
- Many repositories on GitHub, making it difficult to navigate
- Example for the connection: very simple (only config files to modify), but it's hard to identify which files and in which module, and some customisation with the fields names

Thank you for your attention