Securité des données
GeoServer vs GeoFence

F. Van Der Biest – F. Gravin

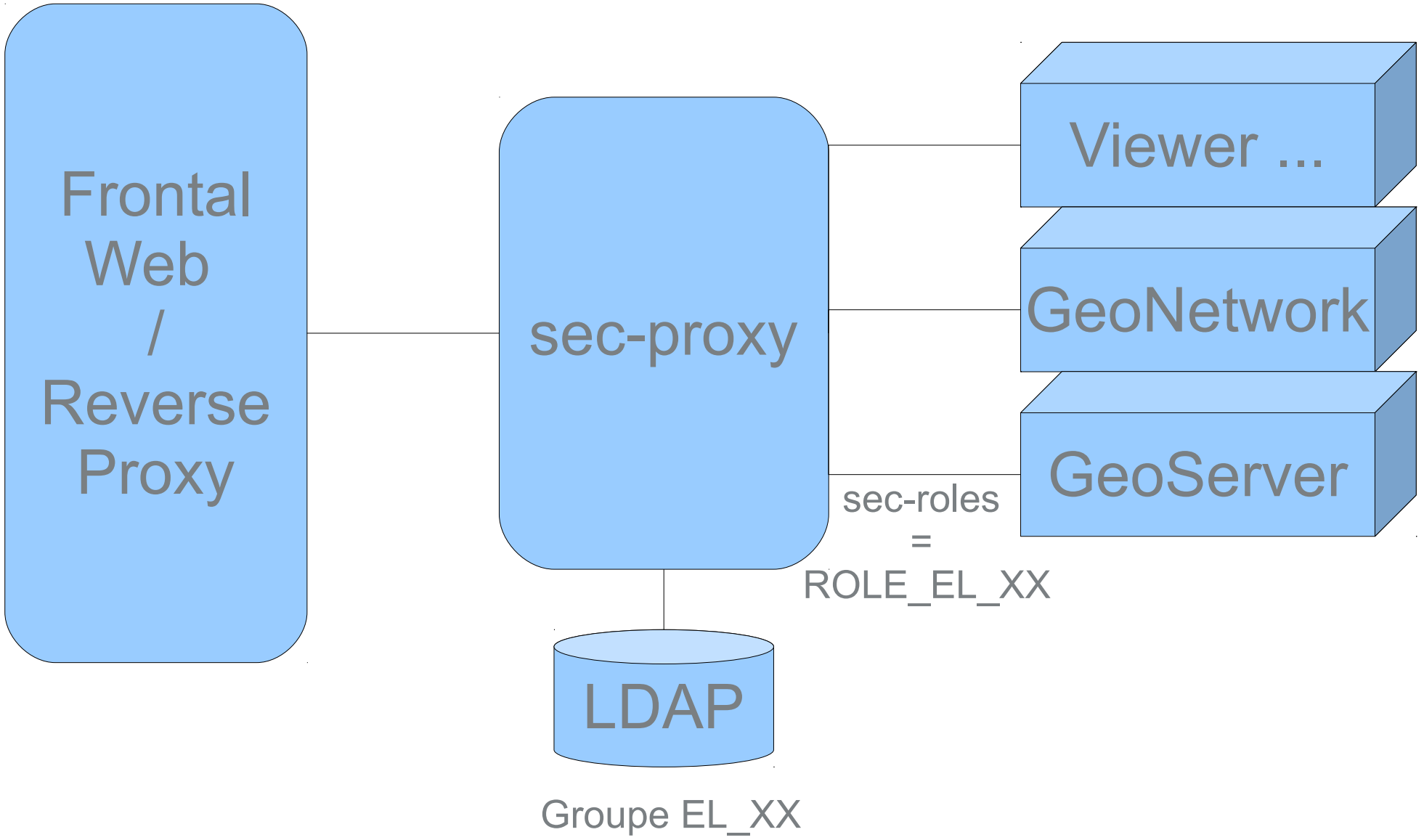
camptocamp

INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS

Plan

- Rappels sur le fonctionnement du sec-proxy
- Sécurité des données native avec GeoServer
- Sécurité des données avec GeoFence
- Avantages / Inconvénients

Rappels architecture applicative geOrchestra



GeoServer Sécurité

- Utilisateurs et groupes GeoServer non utilisés
- Rôles mappés sur le contenu des headers sec-roles

Role	Parent	Parameters
ROLE_AP_ARS		
ROLE_AP_CADASTRE_MAJIC		
ROLE_AP_DEMO_COMMENTAIRE		
ROLE_AP_GT_ENSEIGNEMENT		
ROLE_AP_GT_LITTORAL		
ROLE_AP_SRCE_ELABORATION		
ROLE_SP_AUTRE		
ROLE_SP_COLLECTIVITE_TERRITORIALE		
ROLE_SP_ETABLISSEMENT_PUBLIC		
ROLE_SP_GCIS		
ROLE_SP_MEMBRE_GIP		
ROLE_SP_ORGANISME_RELAIS		
ROLE_SP_SECTEUR_ASSOCIATIF		
ROLE_SP_SERVICE_ETAT		
ROLE_SV_EDITOR		
ROLE_SV_USER		

<< < 1 > >> Results 1 to 16 (out of 16 items)

GeoServer – règles

- Motif d'une règle :
  - workspace.layer.permission=role[,role2,...]
- Permissions :
  - r — Accès en lecture
  - w — Accès en écriture
  - a — Droits d’administration
- Notes :
  - a implique r + w
  - w et r sont indépendants
  - unicité des triplets workspace.layer.permission

Règles de priorisation des règles;-)

- Les règles sont évaluées en commençant par les plus précises :
  - celle concernant la couche demandée ou, si inexistante :
  - celle concernant le namespace demandé ou, si inexistante :
  - celle de l'espace global

- Pour une requête OGC donnée (qui correspond à une permission r ou w), la première règle trouvée est sélectionnée à l'exception de toute autre

Autre formulation

- si une règle n’est pas spécifiée explicitement pour une couche, les permissions sont héritées de son espace de nommage.
- si une règle n’est pas spécifiée explicitement pour un espace de nommage, les permissions globales sont héritées.

Exemple de configuration

- *.*.r = ROLE_TRUSTED
  - Accès restreint en lecture aux membres de ROLE_TRUSTED
- *.*.w = ROLE_NO_ONE
  - WFS-T interdit
- poi.*.r = *
  - Accès en lecture autorisé à tout le monde dans espace de travail « poi », sauf ...
- poi.military_bases.r = ROLE_MILITARY
- poi.military_bases.w = ROLE_MILITARY
  - ... pour la couche military_bases accessible aux militaires

GeoServer – sécurité des services

- Motif des règles :
  - <service>.<operation|*>=<role>[,<role2>,...]
- Avec :
  - **service** vaut wms ou wfs ou wcs
  - **operation** vaut getMap ou getFeature ou ...
  - **role** est la liste des rôles, séparés par des virgules
- Exemple :
  - wfs.* = ROLE_WFS
  - wfs.Transaction = ROLE_WFS_WRITE

Paramétrage du mode « catalogue »

- Définit les modalités d'accès :
  - aux données (couches)
  - aux métadonnées des couches :
    - dans le document capabilities des services
    - via des requêtes spécifiques (WFS DescribeFeatureType & WCS DescribeCoverage)

Mode “Hide / Caché”

- Il s’agit du mode par défaut : sécurité maximale.
  - Les métadonnées des couches sécurisées sont cachées,
  - Les données des couches sécurisées sont inaccessibles.

Mode “Challenge”

- Les métadonnées sont librement accessibles pour toutes les couches :
  - document “capabilities” complet,
  - requêtes DescribeFeatureType & DescribeCoverage toujours fonctionnelles.
- L’accès aux couches sécurisées déclenche une demande d’authentification par mot de passe (HTTP 401)
- Pour résumer : **l’information sur toutes les couches est publique, mais l’accès aux données est restreint**.

Mode “Mixed / Mélangé”

- Les métadonnées sont filtrées et protégées :
  - document “capabilities” filtré en fonction des droits de l’utilisateur courant,
  - les requêtes DescribeFeatureType & DescribeCoverage déclenchent une demande d’authentification par mot de passe (HTTP 401) pour les couches sécurisées.
- L’accès aux couches sécurisées déclenche une demande d’authentification par mot de passe (HTTP 401)
- Pour résumer : **l’accès aux métadonnées et aux données est restreint**. C’est le mode recommandé.

GeoFence

Solution Open Source qui surcharge les mécanismes d'Authentification et d'Autorisation de Geoserver

- Licence GPL
- Sources : https://github.com/geosolutions-it/geofence

GeoFence A&A

- Authentification
  - Intégrée dans l'architecture de GeoServer
  - Intégrée dans l'architecture de geOrchestra
- Autorisation
  - Autorisation sur les données
  - Autorisation sur les services

GeoFence Autorisation

- Surcharge la gestion des autorisations de GeoServer
- Fournit un système de règles externes
- Traite les requêtes à la volée.
- Les contrôles d'accès sont basés sur :
  - Les utilisateurs
  - Les groupes
  - Les rôles (geOrchestra)

GeoFence Autorisation

- Contrôle affiné
  - Services
  - Opérations
  - Espaces de travail
  - Couches
  - Attributs
- Application Web spécifique
  - REST API
  - GUI
- Scalable
  - 1 GeoFence peut contrôler N instances de GeoServer

GeoFence architecture

- GUI
  - Core : GUI logic, implémentée avec GWT
  - Webapp : l'interface produisant le .war final
- GeoServer (GeoFence probe)
  - Security
    - surcharge le module security de GeoServer.
    - Implémente le ResourceAccessManager qui transfère les requêtes à une instance distante de GeoFence
  - Webapp

GeoFence architecture

- GeoFence Probe est déployé dans chaque GeoServer
- GeoFence se base sur le nom d'instance des GeoServer pour sélectionner les règles.
- GeoFence probe interroge GeoFence pour chaque requête et lui fournit :
  - Son nom d'instance
  - L'utilisateur en cours
  - Les détails de la requête
- GeoFence fournit des règles d'accès pour que la probe traite à la volée la requête

GeoFence architecture

- Le ResourceAccessManager de GeoFence utilise un système de cache
- Le cache peut être configuré
  - Nombre d'entrées
  - Temps d'expiration
- Le cache fournit une API REST
  - Supprimer le cache
  - Statistiques

GeoFence - Système de règles

- Authorisations basées sur la priorité des règles
  - Type de règle : **ALLOW** / **DENY** / **LIMIT**
  - La première règle qui correspond est celle prise en compte
- Les filtres peuvent être appliqués sur les champs
  - Roles
  - Instance GeoServer
  - Services OGC (e.g WMS)
  - Opérations liées aux services OGC (e.g GetCapabilities)
  - Espaces de travail
  - Nom des couches

GeoFence Système de règles

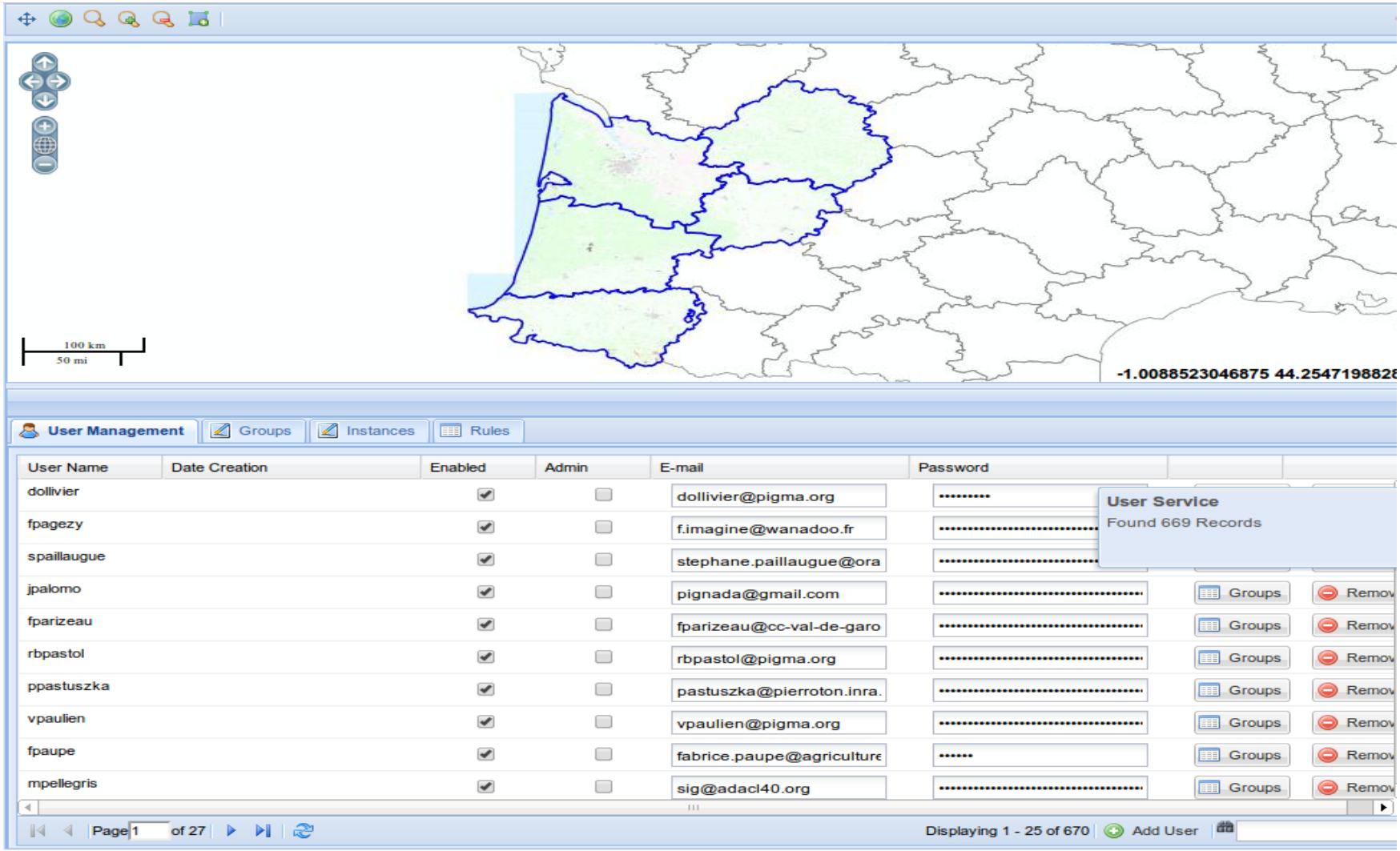
- Règles affinées pour les couches
  - Restriction géographique
  - Restriction sur les attributs
  - Restriction sur les styles disponibles
  - Restriction basées sur des filtres CQL

GeoFence Interface REST

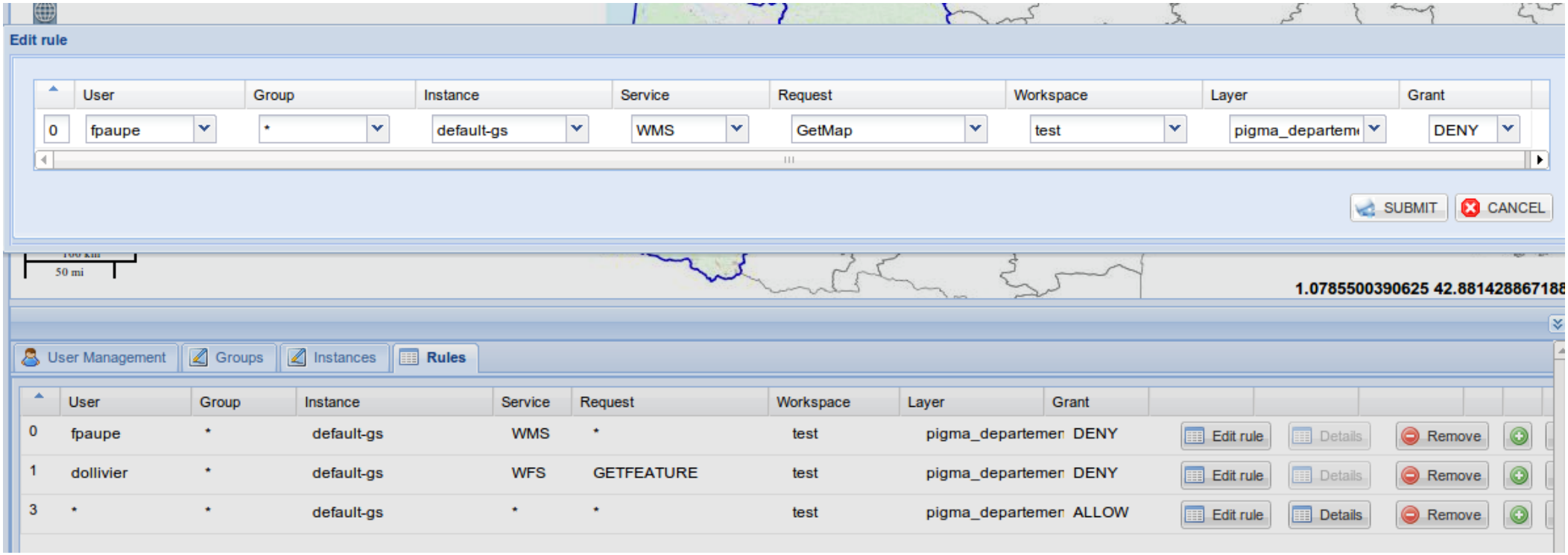
- Gestion des éléments
  - Utilisateurs et groupes
  - Instances GeoServer
  - Règles

https://github.com/geosolutions-it/geofence/wiki/REST-API

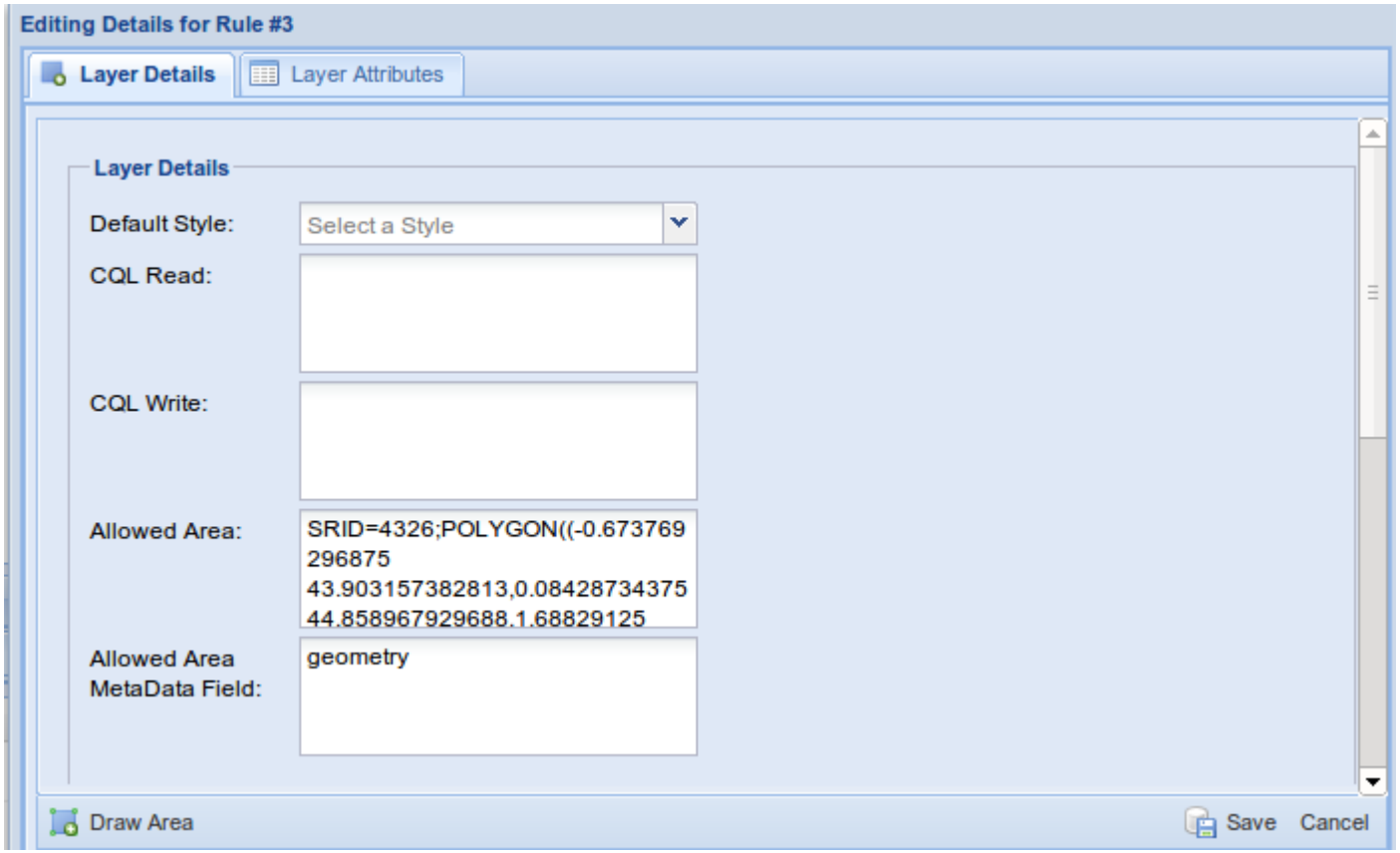
GeoFence GUI



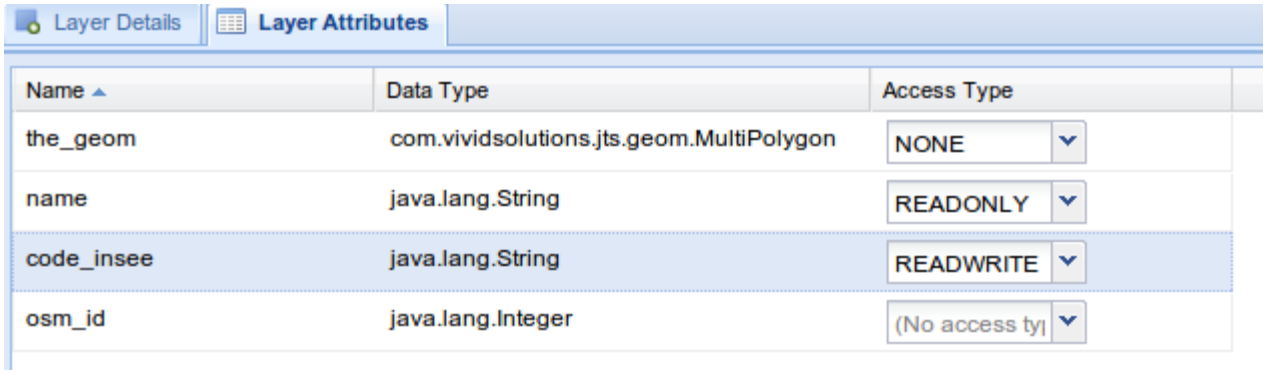
GeoFence GUI



GeoFence GUI



GeoFence GUI



Import depuis geOrchestra

- Java application georchestra2geofence
  - https://github.com/georchestra/geofence/tree/georchestra/src/sample

- Import des groupes
  - A partir d'export LDIF
    - "cn=EL_GROUP1,ou=groups,dc=georchestra,dc=org,133"
  - Nécessaire pour importer les règles
  - Doit importer un external id à partir du champ 'ou'

Import depuis geOrchestra

- A partir d'un fichier de règles GeoServer
  - workspace1.layer1.r=GROUP1,GROUP2
- Intègre les règles via l'API REST
- Gère la transposition GeoServer -> GeoFence
  - P1 – ALLOW GROUP1 pour workspace1.layer1
  - P1 – ALLOW GROUP2 pour workspace1.layer1
  - P1000 – DENY ALL pour workspace1.layer1
  - P2000 – ALLOW ALL sur ALL

Avantages / Inconvénients GeoServer

- Relativement simple
- Bonne intégration
- Documentation ++
- Grosse communauté

- Impossible de désactiver WFS ou WCS pour une couche ou un espace de travail

Avantages / Inconvénients GeoFence

- Granularité forte des règles
- Possibilité de restreindre sur un périmètre :
  - Statique (spécifique à la règle)
  - Dynamique (spécifique à l'utilisateur connecté)

- Lourdeur des règles
- UI peu conviviale
- Intégration moyenne
- Documentation
- Petite communauté
- Contraintes LDAP


tocamp
camptocamp
INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS