

Securité des données GeoServer vs GeoFence

F. Van Der Biest – F. Gravin

camptocamp[®]

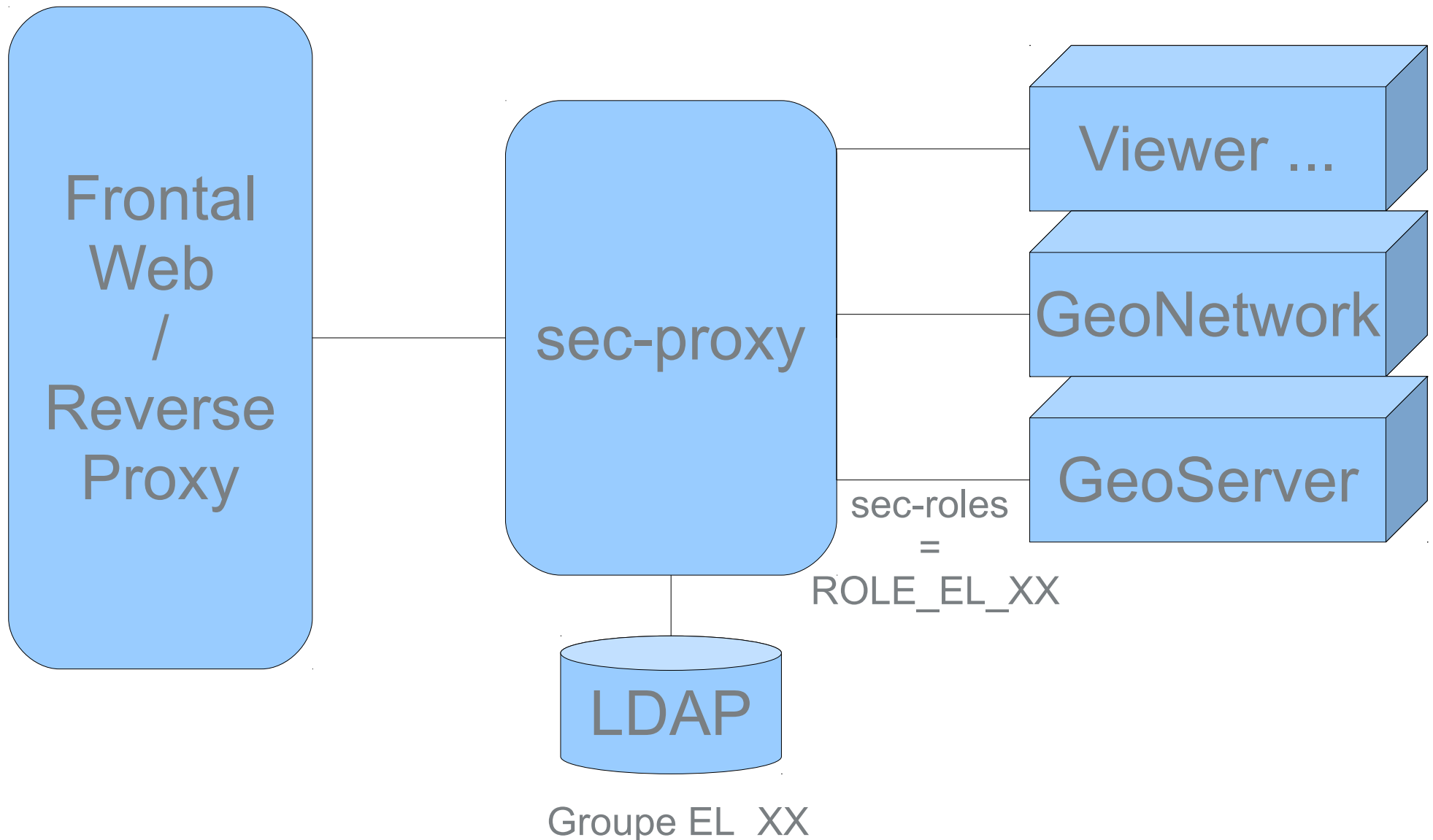
INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS

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

<input type="checkbox"/> Role	Parent	Parameters
<input type="checkbox"/> ROLE_AP_ARS		
<input type="checkbox"/> ROLE_AP_CADASTRE_MAJIC		
<input type="checkbox"/> ROLE_AP_DEMO_COMMENTAIRE		
<input type="checkbox"/> ROLE_AP_GT_ENSEIGNEMENT		
<input type="checkbox"/> ROLE_AP_GT_LITTORAL		
<input type="checkbox"/> ROLE_AP_SRCE_ELABORATION		
<input type="checkbox"/> ROLE_SP_AUTRE		
<input type="checkbox"/> ROLE_SP_COLLECTIVITE_TERRITORIALE		
<input type="checkbox"/> ROLE_SP_ETABLISSEMENT_PUBLIC		
<input type="checkbox"/> ROLE_SP_GCIS		
<input type="checkbox"/> ROLE_SP_MEMBRE_GIP		
<input type="checkbox"/> ROLE_SP_ORGANISME_RELAIS		
<input type="checkbox"/> ROLE_SP_SECTEUR_ASSOCIATIF		
<input type="checkbox"/> ROLE_SP_SERVICE_ETAT		
<input type="checkbox"/> ROLE_SV_EDITOR		
<input type="checkbox"/> ROLE_SV_USER		

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

The screenshot displays the GeoFence GUI interface. At the top, there is a map of France with a blue outline indicating a geofence area. Below the map is a scale bar showing 100 km and 50 mi. A coordinate pair is visible in the bottom right of the map area: **-1.0088523046875 44.2547198828**.

Below the map is a navigation bar with tabs for **User Management**, **Groups**, **Instances**, and **Rules**. The **User Management** tab is active, showing a table of users.

User Name	Date Creation	Enabled	Admin	E-mail	Password		
dollivier		<input checked="" type="checkbox"/>	<input type="checkbox"/>	dollivier@pigma.org		
fpagezy		<input checked="" type="checkbox"/>	<input type="checkbox"/>	f.imagine@wanadoo.fr		
spailaugue		<input checked="" type="checkbox"/>	<input type="checkbox"/>	stephane.paillaugue@ora		
jpalamo		<input checked="" type="checkbox"/>	<input type="checkbox"/>	pignada@gmail.com	Groups	Remove
fparizeau		<input checked="" type="checkbox"/>	<input type="checkbox"/>	fparizeau@cc-val-de-garo	Groups	Remove
rbpastol		<input checked="" type="checkbox"/>	<input type="checkbox"/>	rbpastol@pigma.org	Groups	Remove
ppastuszka		<input checked="" type="checkbox"/>	<input type="checkbox"/>	pastuszka@pierroton.inra	Groups	Remove
vpaulien		<input checked="" type="checkbox"/>	<input type="checkbox"/>	vpaulien@pigma.org	Groups	Remove
fpaupe		<input checked="" type="checkbox"/>	<input type="checkbox"/>	fabrice.paupe@agriculture	Groups	Remove
mpellegris		<input checked="" type="checkbox"/>	<input type="checkbox"/>	sig@adacl40.org	Groups	Remove

At the bottom of the table, there is a pagination bar showing **Page 1 of 27** and a status bar indicating **Displaying 1 - 25 of 670** with an **Add User** button.

A **User Service** popup is visible on the right side of the table, displaying **Found 669 Records**.



GeoFence GUI

The screenshot displays the GeoFence GUI interface. At the top, a map is visible. Below it is the 'Edit rule' form, which contains a table for defining rule parameters. The form includes a 'SUBMIT' button and a 'CANCEL' button.

	User	Group	Instance	Service	Request	Workspace	Layer	Grant
0	fpaupe	*	default-gs	WMS	GetMap	test	pigma_departem	DENY

Below the form is a map with a scale bar (50 mi) and a coordinate display: 1.0785500390625 42.881428867188.

The bottom section of the GUI shows a navigation menu with 'User Management', 'Groups', 'Instances', and 'Rules'. The 'Rules' tab is active, displaying a table of existing rules.

	User	Group	Instance	Service	Request	Workspace	Layer	Grant				
0	fpaupe	*	default-gs	WMS	*	test	pigma_departem	DENY	Edit rule	Details	Remove	+
1	dollivier	*	default-gs	WFS	GETFEATURE	test	pigma_departem	DENY	Edit rule	Details	Remove	+
3	*	*	default-gs	*	*	test	pigma_departem	ALLOW	Edit rule	Details	Remove	+



GeoFence GUI

Editing Details for Rule #3

Layer Details Layer Attributes

Layer Details

Default Style: Select a Style

CQL Read:

CQL Write:

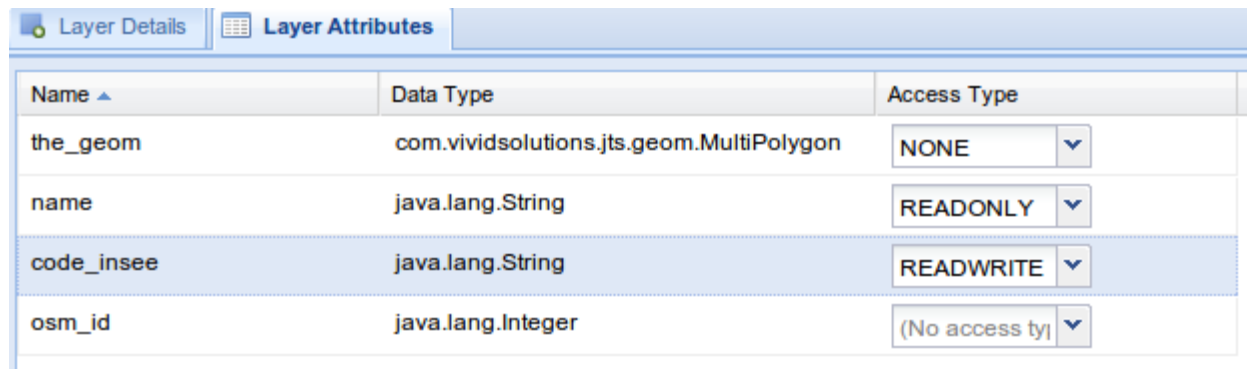
Allowed Area: SRID=4326;POLYGON((-0.673769
296875
43.903157382813,0.08428734375
44.858967929688,1.68829125

Allowed Area
MetaData Field: geometry

Draw Area Save Cancel



GeoFence GUI



The screenshot shows the 'Layer Attributes' panel in a software interface. It contains a table with four columns: 'Name', 'Data Type', and 'Access Type'. The 'code_insee' row is highlighted in blue. The 'Access Type' column contains dropdown menus with various options.

Name ▲	Data Type	Access Type
the_geom	com.vividsolutions.jts.geom.MultiPolygon	NONE ▼
name	java.lang.String	READONLY ▼
code_insee	java.lang.String	READWRITE ▼
osm_id	java.lang.Integer	(No access ty) ▼



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



to camp 

camp **to** camp

INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS