**Gestion de la sécurité sous georchestra**

2014-10-22 16:25 GMT+02:00 Julien Sabatier <sab...@gmail.com>:

 -  ADMINISTRATOR = admin geoserver

 -  SV\_ADMIN = admin geonetwork

 - MOD\_LDAPADMIN = admin des utilisateurs et groupes

 - MOD\_ANALYTICS = accès aux stats de la plateforme

 - MOD\_EXTRACTORAPP = accès à l'extracteur

 - SV\_EDITOR = editeur de fiches de MD

 - SV\_REVIEWER = relecteur de fiches de MD

 - SV\_USER = utilisateur simple de georchestra

 - PENDING\_USERS = utilisateur ayant demandé un compte, non encore validé

**1. La documentation d'installation précise certains mécanismes coté annuaire ldap**

<https://github.com/georchestra/georchestra/blob/master/doc/setup/openldap.md>

L’annuaire doit également respecter certaines règles pour le nommage des groupes/rôles.

* Les groupes/rôles préfixés par EL\_ seront appliqués aux groupes Geonetwork
* Les groupes/rôles préfixés SV\_ sont des rôles communs à tous les modules (dans Geonetork, les rôles SV\_ correspondent aux profils, dans d’autres applications ils ont une signification différente : laquelle en dehors de édition sous mapfishapp??)
* SV\_ADMIN donne des permissions administrateur dans toutes les applications (hors geoserver )
* SV\_EDITOR donne des droits en écriture dans une application si cette notion a un sens (actuellement, cela concerne seulement Geonetwork et Mapfishapp)
* SV\_REVIEWER donne des droits de relecteur validateur (actuellement, cela concerne seulement Geonetwork)
* SV\_USER donne seulement des droits en lecture seule dans toutes les applications mais, l’utilisateur étant authentifié, il peut bénéficier d’autres permissions (dépendantes de l’application)

**2. Utilisation des gorupes ldap :**

|  |
| --- |
| **Groupes prédéfinis georchestra dans l'annuaire ldap et usage au sein des applications****(**<https://github.com/georchestra/LDAP/blob/master/georchestra.ldif>**)** |
| **Ldap** | **Geonetwork**  | **Geoserver** | **MapfishApp** | **Extractor** | **Autres** |
| ADMINISTRATOR | ---- | Statut Administrateur | ---- | Spécial pour compte d'extraction | ---- |
| SV\_ADMIN | Profil Administrator | ---- | ---- | ---- | ---- |
| MOD\_LDAPADMIN | ---- | ---- | ---- | ---- | Accès appli ldapadmin |
| MOD\_ANALYTICS | ---- | ---- | ---- | ---- | Accès appli Analytics |
| MOD\_EXTRACTORAPP |  |  |  | Accès extractor |  |
| SV\_EDITOR | Profil Editor | ---- | Rôle d'éditeur | ---- | ---- |
| SV\_REVIEWER | Profil Reviewer | ---- | ---- | ---- | ---- |
| SV\_USER | Chaque compte doit être memebre de ce groupe à minima pour accéder aux applications en mode connecté |
| PENDING\_USERS | Utilisateur dont la création du compte est en cours de validation. Les membres de ce groupe ne peuvent pas se connecter. |

|  |
| --- |
| **Autres groupes dans l'annuaire ldap (*création par les administrateurs de l'IDS*) et usage au sein des applications** |
| **Ldap** | **Geonetwork** | **Geoserver** | **Autres** |
| EL\_MonGroupe | Synchronisation avec MonGroupe (création automatique au besoin) et application du profil selon l'appartenance aux groupes SV\_ (voir groupes prédéfinis Georchestra plus haut) | ---- | ---- |
| GroupeLibre | ---- | Application des droits accordés au rôle geoserver nommé ROLE\_ GroupeLibre s'il existe (pas de création automatique) | ---- |

Sécuriser geonetwork sous georchestra:

* Principes de fonctionnement :
	+ Il est inutile de créer des comptes ou groupes par l'interface d'administration de geonetwork.
	+ Lors de la connexion d'un utilisateur l'application geonetwork récupère les informations ldap (*compte et groupes d'appartenance*) et synchronise avec le contenu de ses tables (création / synchronisation d'utilisateurs, de groupes, d'appartenance à des groupes).
	+ Les groupes ldap prédéfinis SV\_\* servent à définir le profil de l'utilisateur (*un seul profil actif pour l'ensemble des groupes auxquels appartient l'utilisateur - Georchestra en version 13.09 ne supporte pas encore la notion de profil spécifique à un groupe comme par exemple 'être éditeur du groupe1 et relecteur du groupe2'*)
	+ Les groupes ldap EL\_\* servent à définir les groupes geonetwork auxquels l'utilisateur appartient.
	+ Les éditeurs ou administrateurs accordent des 'privilèges ou droits' à des groupes geonetwork (*pas de droits nominatifs aux utilisateurs*) sur chaque fiche de métadonnées.
	+ Geonetwork fournit de la documentation sur l'utilisation des profils et des privilèges : <http://geonetwork-opensource.org/manuals/trunk/fra/users/editor/metadata_ownership/index.html>
	+ Chaque fiche de métadonnées est associée à un propriétaire et un groupe propriétaire qui ont des droits spécifiques (*droits par défaut à la création d'une fiche : le créateur peut tout faire et le groupe peut voir la fiche*).



* 2 cas d'usage courant de sécurisation :
	+ **1 administrateur geonetwork** pouvant **tout faire** et notamment donner des **privilèges aux groupe 'Tous'** , 'Invité' ou 'Intranet'. Le compte a seulement besoin d'être créé sous ldap et membre du groupe prédéfini ldap SV\_ADMIN qui lui fournit le profil 'Administrator' sous geonetwork.
	+ **1 éditeur de fiche métadonnées**. Le compte est à créer sous ldap et membre du groupe prédéfini SV\_EDITOR. Cela ne suffit toutefois pas; le compte doit aussi être membre d'au moins un groupe EL\_\* (à créer sous ldap si nécessaire) ce qui lui permettra alors de créer des fiches associées à ce(s) groupe(s) et également d'éditer les fiches pour lesquelles le privilège 'Editer' est accordé à ce(s) groupe(s).

Sécuriser geoserver sous georchestra (sans geofence):

* Principes de fonctionnement :
	+ Il est inutile de créer des comptes ou groupes par l'interface d'administration de geoserver.
	+ Lors de la connexion d'un utilisateur l'application geoserver récupère les informations ldap (*compte et groupes d'appartenance*) mais ne synchronise rien avec sa gestion de compte / groupe qui est alors inutilisée. Une simple **correspondance entre les groupes ldap et les rôles** (**pas les groupes**) geoserver est établie en faisant correspondre un groupe ldap 'NomLibre' à un évenuel rôle geoserver nommé 'ROLE\_NomLibre'. L'utilisateur connecté appartenant au groupe ldap 'NomLibre' aura accès aux ressources que le rôle geoserver 'ROLE\_NomLibre' peut accéder.
	+ Le groupe ldap 'ADMINISTRATOR' permet d'avoir un accès administrateur à geoserver.
	+ Les administrateurs geoserver accordent des droits à des rôles geoserver sur des ressources (couches uniques, ensemble de couches, ...).
	+ Une couche pour laquelle aucune règle n'est définie est accessible en lecture pour tous.
	+ Geoserver fournit de la documentation sur la sécurité : <http://docs.geoserver.org/2.3.2/user/security/index.html>
* 2 cas d'usage courant de sécurisation :
	+ **1 administrateur geoserver** pouvant **tout faire** et notamment donner des **droits aux rôles**. Le compte a seulement besoin d'être créé sous ldap et membre du groupe prédéfini ldap ADMINISTRATOR qui lui fournit le profil 'Administrator' sous geoserver.
	+ **Sécuriser un ensemble de couches** (accès en lecture seule par exemple) :
		- Sous statut administrateur geoserver créer un rôle nommé par exemple ROLE\_SecuLecture et définir une règle (Sécurité des données) autorisant ce rôle à accéder en lecture à l'ensemble de couches désiré.
		- Sous ldap créer un groupe nommé SecuLecture et inscrire comme membres les comptes ldap devant bénéficier de l'accès séurisé.

Avec l’utilisation de Geofence pour la sécurité des couches il n’y a plus la notion de ROLE geoserver et on utilise l’application geofence pour accorder des droits aux groupes ldap sur les objets geoserver (serveur, service OGC, requête OGC, workspace et layer).