**Création des comptes utilisateurs dans georchestra**

Table des matières

[Traitement d’une demande utilisateur 2](#_Toc22200589)

[Utilisateur sans login ldap INRA 2](#_Toc22200590)

[Utilisateur avec login ldap INRA 2](#_Toc22200591)

[Nouveautés 2019 : 5](#_Toc22200592)

**Pour mémoire** (voir aussi [https://appgeodb.nancy.inra.fr/donnees/documentations/ids/principes/Gestion%20S%c3%a9curit%c3%a9%20sous%20georchestra.docx](https://appgeodb.nancy.inra.fr/donnees/documentations/ids/principes/Gestion%20S%C3%A9curit%C3%A9%20sous%20georchestra.docx) )

 -  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

La création automatique via le lien de demande de création de compte (*sur l’écran de connexion tel que ci-dessous*) est remplacée par l’accés à une page expliquant comment effectuer la demande.



(Cette surcharge implique une modification du fichier casLoginView.jsp de l’application CAS à l’emplacement tomcat6/webapps/cas/WEB-INF/view/jsp/default/ui)

# Traitement d’une demande utilisateur

## Utilisateur sans login ldap INRA

L’application ldapadmin peut être utilisée (accessible depuis l’écran d’administration) sans oublier d’inscrire le compte à minima dans le groupe SV\_USER.

* Se connecter à l’IDS avec un compte habilité puis accéder à ldapadmin
* Cliquer sur le bouton ‘New User’
* Après avoir renseigné les informations obligatoires (nom, prénom, mail) et facultatives (organisation) et validé cliquer sur le bouton ‘Save’
* Sélectionner le compte qui vient d’être créé et inscrivez-le à minima dans le groupe SV\_USER (utilisez la commande Apply changes).



* Sélectionner le compte qui vient d’être créé et cliquer sur le bouton ‘Reset password’ ce qui donnera accès à une interface chargée de prévenir le nouvel utilisateur en lui adressant un lien de modification de mot de passe. Sans cette étape l’utilisateur n’est pas informé et personne ne connaît le mot de passe associé.

A noter que l’on n’a pas le choix du login ni du mot de passe. Si cela pose problème il faudra utiliser la même procédure que pour un utilisateur disposant d’un login ldap INRA (voir ci-après) en tapant NON dans la colonne ldap.

## Utilisateur avec login ldap INRA

Comme nous devons maîtriser le login, mais aussi le password (de la forme {SASL}monlogin@inra.fr ) nous ne pouvons actuellement utiliser ldapadmin et devons nous appuyer sur un job talend téléchargeable ici : <https://appgeodb.nancy.inra.fr/donnees/documentations/ids/modes_operatoires/gestion_comptes/genere_compte.zip>

L’installation et la configuration de ce job sont décrites en **Annexe**.

* Créer un fichier ldap.csv contenant les renseignements nécessaires sous cette forme :

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Operation | Nom | Prenom | login | mail | ldap | geonet\_admin | geonet\_editor | geoserver\_admin | app\_ldapadmin | app\_extractor | app\_analytics | autres\_groupes |
| A | Dupont | Pierre | pdupont | Pierre.dupont@paris.inra.fr | OUI | NON | NON | NON | NON | NON | NON |  |

* Placer ce fichier à l’emplacement configuré pour le job.
* Lancer le script de démarrage du job :

|  |  |  |
| --- | --- | --- |
| OS | IDS | Script |
| LINUX | Bac à sable | \genere\_compte\genere\_compte\_run\_bas\_ncy.sh |
| LINUX | Production | \genere\_compte\genere\_compte\_run\_agroenvgeo.sh |
| WINDOWS | Bac à sable | \genere\_compte\genere\_compte\_run\_bas\_ncy.bat |
| WINDOWS | Production | \genere\_compte\genere\_compte\_run\_agroenvgeo.bat |

En fin de traitement le job liste les comptes, celui venant d’être créé apparaît normalement en fin de listing. Si des erreurs surviennent un fichier .err sera produit pour vous aider à comprendre et résoudre le problème.

* Vous pouvez ensuite utiliser ldapadmin pour vérifier les informations et compléter si besoin.
* Adresser un mail pour informer l’utilisateur de la création de son compte en lui précisant qu’il utilise les informations ldap INRA pour se connecter à l’IDS

Le job genere\_compte doit être exécuté par une personne habilitée à créer des comptes dans l’annuaire ldap (voir [https://appgeodb.nancy.inra.fr/donnees/documentations/ids/principes/Gestion%20de%20plusieurs%20racines%20ldap%20&%20d%c3%a9l%c3%a9gation%20de%20droits.docx](https://appgeodb.nancy.inra.fr/donnees/documentations/ids/principes/Gestion%20de%20plusieurs%20racines%20ldap%20%26%20d%C3%A9l%C3%A9gation%20de%20droits.docx) ). Il permet la création d’un compte (ou plusieurs) à partir d’un fichier d’entrée contenant les informations utiles. Il crée le ou les compte(s) et s’occupe de l’inscription au sein de certains groupes prédéfinis.

**Installation du JOB Talend** (nécessite une JVM en état de marche sur le poste qui l’exécute)

Télécharger le job :

<https://appgeodb.nancy.inra.fr/donnees/documentations/ids/modes_operatoires/gestion_comptes/genere_compte.zip>

Décompresser l’archive pour obtenir une arborescence telle que ci-après :



Le dossier genere\_compte contient les scripts de lancement du job. La différence entre la création d’un compte sur le bac à sable et la création d’un compte en production est minime, les 2 scripts étant identiques à l’exception près d’un contexte d’exécution différent. Le contexte agroenvgeo représente la configuration pour la production tandis que le contexte bas\_ncy représente la configuration pour le bac à sable.

**Configurations du JOB Talend**

Le dossier contexts sous recupere\_idmax\_0\_1 contient 2 fichiers éditables :

* Agroenvgeo.properties
* Bas\_ncy.properties
* Ces 2 fichiers ont la même forme



* **Ils doivent être personnalisés** avec notamment les informations de connexion à l’annuaire ldap :
	+ Mdp : doit contenir le mot de passe de l’opérateur qui exécute le job (compte IDS)
	+ Utilisateur : contient les informations identifiant le compte qui exécute le job (remplacer loginldap par votre login)
	+ Mdp\_default : mot de passe qui sera généré pour les comptes non ldap INRA si le job est utilisé pour cet usage.
	+ Dossier\_donnees : indique le chemin ou le fichier contenant la liste des comptes à créer sera déposé.
	+ Fic\_source : si vous choisissez de ne pas nommer votre fichier contenant la liste des comptes à créer ldap.csv alors il vous faut indiquer son nom dans cette variable.

# Nouveautés 2019 :

En attendant la migration vers une version 19.04 il a été décidé de mettre à niveau le job Talend tout en le réduisant au strict nécessaire, à savoir la création du compte dans l’arborescence ldap, l’appartenance à des groupes pouvant se faire via ldapadmin de l’IDS.

La perspective serait d’utiliser le mode natif de l’IDS et de n’utiliser un outil tiers (talend ou autre) que pour modifier le mot de passe d’un utilisateur qui dispose déjà d’un compte ldap INRA (INRAE), ce mot de passe devant respecter une convention particulière dans ce cas précis; le système natif imposant le login il y aurait probablement nécessité de renseigner l’information pour un éventuel renommage.

Le principe au 17/10/2019 est donc simple :

* Récupération du job Talend mis à disposition : <https://appgeodb.nancy.inra.fr/donnees/documentations/ids/modes_operatoires/gestion_comptes/genere_compte.zip>
* Décompresser l’archive.
* Personnaliser le ou les fichiers de contexte du job principal genere\_compte



* Les fichiers de contexte sont déjà préparés pour adresser les versions bac à sable (bas) ou production (agroenvgeo) en version 16.12 (actuelle) ou 19.04 (à venir). La modification de ces fichiers peut concerner (*en vert : très certainement à personnaliser – en rose/bleu : à ne pas personnaliser ici si le job n’est pas dans un dossier type home c à d inaccessible à d’autres utilisateurs*)
* **Dossier\_donnees :** dossier où le fichier contenant les informations de compte à créer sera disponible.
* **Fic\_source :** nom du fichier au format csv qui contiendra les informations de compte à créer.
* **Mdp\_default :** mot de passe affecté à un nouveau compte si celui-ci n’est pas connu du ldap INRA.
* **Mdp et utilisateur :** mot de passe et login de l‘utilisateur qui lance le traitement et doit bénéficier du privilège de création de compte ldap (membre d’un groupe spécial non visible depuis l’IDS).
* Préparer le lancement du job en personnalisant les scripts (.bat pour windows, .sh pour linux)



* Chaque script lance l’exécution du job avec une syntaxe telle que

java …. **ids.genere\_compte\_0\_1.genere\_compte** --context=nomcontexte %\*

* Il est possible de dupliquer ces scripts pour répondre au besoin d’exécuter le job sur différents environnements (contexte).
* Il est possible aussi de surcharger tout ou partie des variables de contexte en appelant le script avec des paramètres (grâce à ‘%\*’ qui se trouve en fin de ligne). Par exemple vous pourriez utiliser la syntaxe (sur une seule ligne) :

Genere\_compte\_run.bat

--context\_param mdp="monmotdepasse"

 –context\_param utilisateur="uid=albenard,ou=users,dc=idsbas1612,dc=inra,dc=fr"

\* Les caractères \ ne doivent pas être utilisés pour le paramètre utilisateur contrairement au contenu des fichiers de contexte.

Toutes les opérations ci-dessus ne sont à effectuer qu’une seule fois (en quelque sorte l’installation du nécessaire)

* Renseigner le fichier contenant les informations de compte à créer (en conformité avec les variables de contexte). Le format de ce fichier, encodé en utf8 avec un spéarateur ‘;’est le suivant :

nom;prenom;login;mail;ldap\_inra

Dupont;Georges;gdupont;georges.dupont@inra.fr;OUI

Durand;René;rdurand;rene.durand@partenaire.com;NON

De manière plus lisible :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| nom | prenom | login | mail | ldap\_inra |
| Dupont | Georges | gdupont | georges.dupont@inra.fr | OUI |
| Durand | René | rdurand | rene.durand@partenaire.com | NON |

* Utiliser votre script pour exécuter le traitement.
* Utiliser ldapadmin pour inscrire le nouveau compte dans les groupes (à minima user). Il faut être membre du role mod\_ldapadmin pour accéder à cette possibilité.

Conseil :

L’ajout d’une commande ‘pause’ dans le script permet de sortir moins violemment et de voir les indications d’erreur le cas échéant.

Un raccourci sur votre bureau (accessible uniquement à vous) peut permettre un lancement facile du script en passant les paramètre sensibles (mot de passe …) dans la ligne de commande. Ce raccourci doit démarrer dans le même dossier que le script qu’il exécute afin de conserver l’accès aux librairies java avec un chemin relatif.