Gestion de plusieurs racines au sein d'un même ldap

# Installation du service avec une seule base

Le script d'installation ldap et le nécessaire : <https://svngeodb.nancy.inra.fr/svn/scripts/trunk/serveurs%20virtuels/installations/slapd/>

Les informations concernant la personnalisation de la base au sein de ce script pourrait être revisitées pour respecter la documentation georchestra (moyennant quelques précisions) : <https://github.com/georchestra/LDAP/blob/master/README.md.>

# Principes de création d'une base ldap

* Le dossier hébergeant la base (1 dossier par base) doit être accessible en écriture par l'utilisateur qui lance le processus slapd : *chown ldap:ldap /data/ldap*
* Il convient de préparer un fichier contenant les informations relatives à la nouvelle base comme le fichier georchestra-bootstrap.ldif accessible sur le github georchestra (<https://github.com/georchestra/LDAP/blob/master/georchestra-bootstrap.ldif>). Personnaliser selon le besoin.
* La commande de création de la base s'exécute avec cn=config qui nécessite au préalable d'enregistrer le mot de passe de configuration ldap (<http://idmoim.blogspot.fr/2014/05/ldapadd-insufficient-access-50-openldap.html>):
  + dans le fichier /etc/openldap/slapd.d/cn=config/olcDatabase={0}config.ldif ajouter ou modifier si nécessaire l'entrée *olcRootPW*: ...
  + redémarrer le service si modification (*service slapd restart*)
  + *ldapadd -W -D "cn=config" -f mabase-bootstrap.ldif* où le fichier mabase-bootstrap.ldif représente le fichier préparé précédemment.
  + Ce procédé est préféré à la syntaxe de la documentation georchestra *(sudo ldapadd -Y EXTERNAL -H ldapi:/// -f georchestra-bootstrap.ldif)* qui ne fonctionne pas nativement
* Un nouveau fichier éditable est alors présent dans le dossier /etc/openldap/slapd.d/cn=config/. Il contient les informations de configuration de la nouvelle base. Le dossier hébergeant cette base est alors alimenté. Il est généralement nécessaire de l'éditer pour configurer le mot de passe (entrée olcRootPW:: IXJhY2luMzsg dans laquelle le second caractère ':' est à supprimer et le mot de passe à modifier). Un redémarrage du service est une fois encore nécessaire.

A noter que la création de la base ne créé pas la racine mais seulement un conteneur qui sera utilisé pour les requêtes concernant certains espaces de nommage (olcSuffix) et accessible selon les droits définis dans le fichier de configuration.

# Principes de création d'une racine ldap

Une racine ldap correspond ici à un domaine ou espace de nommage tel que monids.mondomaine.fr. Une racine contient une arborescence d'objets tels des conteneurs, des groupes, des utilisateurs, le tout étant enregistré dans une base. Nous ne nous intéressons ici qu'à la création du conteneur de niveau supérieur, le reste relevant de l'alimentation de la base / racine traité au chapitre suivant.

* Il convient de préparer un fichier contenant les informations relatives à la nouvelle racine comme le fichier georchestra-root.ldif accessible sur le github georchestra (<https://github.com/georchestra/LDAP/blob/master/georchestra-root.ldif>). Les informations doivent être cohérentes avec celle concernant la base conteneur.
* La commande de création de la racine se fait avec l'autorité déclarée pour la base (voir entrée olcRootDN dans le fichier de configuration de la base)
  + *ldapadd -D"cn=admin,dc=monids,dc=mondomaine,dc=fr" -W -f maracine-root.ldif* où le fichier maracine-root.ldif représente le fichier préparé précédemment.

# Alimentation d'une branche (racine) de l'annuaire

L'alimentation de l'annuaire pour une conformité georchestra nécessite de créer certains groupes d'utilisateurs et d'y affecter les utilisateurs, eux aussi à créer précédemment. Ces opérations peuvent être faites à l'aide d'outils de gestion d'annuaires ldap (phpldapadmin, Apache Directopry Studio) ou bien par import de fichiers notamment au format ldif. Nus décrivons ci-après ce dernier mode.

* Il convient de préparer un fichier contenant les informations relatives à notre organisation comme le fichier georchestra.ldif accessible sur le github georchestra (<https://github.com/georchestra/LDAP/blob/master/georchestra.ldif>). Il convient de personnaliser ce fichier en remplaçant notamment ' dc=georchestra,dc=org' par ce qui correspond à notre organisation / racine.
* La commande d'intégration des informations se fait avec l'autorité déclarée pour la racine / base
  + *ldapadd -D"cn=admin, dc=monids,dc=mondomaine,dc=fr " -W -f organisation.ldif* où le fichier organisation.ldif représente le fichier préparé précédemment.

# Fonctionnnalié membre de

Une extension disponible sur le github de georchestra permet d'obtenir la fonctionnalité d'appartenance à des groupes pour un utilisateur donné.

# Délégation de droits sur une branche de l’annuaire ldap :

Dans le cas de plusieurs racines ldap il convient d’identifier le fichier de configuration de la racine pour laquelle on souhaite déléguer ; au 17 juin 2015 nous avons la configuration suivante :

|  |  |
| --- | --- |
| **Nom racine** | **Fichier de configuration** |
| dc=idsbas,dc=inra,dc=fr | /etc/openldap/slapd.d/cn=config/olcDatabase={3}hdb.ldif |
| dc=sioea,dc=inra,dc=fr | /etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif |

Dans le fichier de configuration identifier les directives olcAccess (s’il y en a) qui sont ordonnées et définissent les droits applicables sur les objets de l’annuaire (sauf pour CN=admin qui dispose du droit d’écriture pour tous les objets). La documentation complète de cette directive est accessible à l’url : <http://linux.die.net/man/5/slapd.access>

Le système analyse les règles dans l’ordre et s’arrête lorsqu’il a trouvé une règle qui correspond à l’utilisateur connecté. Il faut donc placer les règles générales après les règles particulières.

Par exemple

Compléter

olcAccess: {3}to \* by dn="cn=admin,dc=idsbas,dc=inra,dc=fr" write by \* read

par

olcAccess: {4}to \* by group="cn=MOD\_LDAPADMIN,ou=groups,dc=idsbas,dc=inra,dc=fr" write

Ne donnera pas le droit d’écriture au group LDAPADMIN car le système détecte le droit read pour \* dès la règle N° 3.

Il faut alors tout regrouper en une seule règle avec la gestion des droits du groupe MOD\_LDAPADMIN définie avant le droit read pour tous

Par exemple :

**olcAccess: {3}to \*** by dn="cn=admin,dc=idsbas,dc=inra,dc=fr" write by group="cn=MOD\_LDAPADMIN,ou=groups,dc=idsbas,dc=inra,dc=fr" write by \* read