Gestion d'identités PSL – Installation LDAP

Entr'ouvert SCOP – http ://www.entrouvert.com

Table des matières

1 Installation du système de base

La procédure décrite dans cette documentation doit être effectuée après l'installation du système de base décrite dans la documentation « *Gestion d'identités PSL – Installation de base* ».

1.1 Rappel sur la la synchronisation des horloges

Il est très important de faire en sorte que toutes les machines de la solution soient à l'heure. C'est par exemple obligatoire pour tout ce qui concerne les synchronisation LDAP.

Pour cela, vous pouvez installer le paquet `ntp` :

```
# apt-get install ntp
```

Éventuellement, si vous disposez d'un serveur NTP local, vous pouvez l'indiquer dans le fichier `/etc/ntp.conf`. Par défaut, `ntp` utilise les serveurs du projet Debian (`*.debian.pool.ntp.org`).

Note : le paquet `ntp` n'est pas installé par défaut car certains systèmes de virtualisation peuvent proposer une horloge système déjà synchronisée par la machine hôte.

2 Installation du composant LDAP

Installer le paquet `slapd-supann` :

```
# apt-get install slapd-supann
```

Cette installation va déclencher l'installation de tous les composants logiciels (paquets) nécessaires à la mise en place d'un serveur OpenLDAP `slapd` conforme à la norme SUPANN 2009.

Après la première installation, il faut procéder à la mise à zéro des données et de la configuration de `slapd`.

3 Commande slapd-supann

Le pilotage bas niveau du système s'effectue en grande partie via une commande spécifique développée dans le cadre de ce projet : `slapd-supann`

```
# slapd-supann help
syntaxe : slapd-supann commande ...

commandes disponibles :
help        cette aide
import      import d'un ou plusieurs fichiers LDIF
metasync    synchronise un annuaire distant dans le méta-annuaire local
newdb       création d'une nouvelle base, avec un nouveau suffixe
reset       mise à zéro complète
restore     restauration des données depuis un répertoire
save        sauvegarde de la configuration et des données
```

4 Mise à zéro (*reset*)

La commande de mise à zéro doit être lancée après l'installation. Elle met à zéro la configuration du LDAP (conformance norme SUPANN 2009) ainsi que toute les données :

```
# slapd-supann reset
```

Note : au début de cette opération de mise à zéro le système va demander une confirmation, car **toutes les données LDAP vont être effacées**, y compris les configurations.

Exemple d'exécution :

```
# slapd-supann reset

  *************
  *           *   La configuration et toutes les données
  * ATTENTION *   de l'annuaire LDAP vont être définitivement
  *           *   effacées. Avez-vous fait un backup ?
  *************

Confirmez la MISE A ZÉRO COMPLÈTE de l'annuaire LDAP.

Tapez oui en toutes lettres : oui
[ ok ] Stopping OpenLDAP : slapd.
Effacement de la configuration et des données ..ok
Installation de la nouvelle configuration ..
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
ok
Installation des schémas ..
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
_#################### 100.00% eta   none elapsed            none fast !
Closing DB...
ok
Pose de certificats SSL par défaut (invalides)
«  /usr/share/slapd-supann/ssl.pem  » -> «  /etc/ldap/ssl/slapd.pem  »
«  /usr/share/slapd-supann/ssl.key  » -> «  /etc/ldap/ssl/slapd.key  »
ok
[ ok ] Starting OpenLDAP : slapd.
Installation de la racine du méta-annuaire (o=meta) ..
(add) olcDatabase={2}mdb,cn=config
(add) o=meta
```

```
ok
root@ldap1-psl :~#
```

5 Ajout d'une base (*newdb*)

La commande `newdb` permet d'ajouter une base dans le LDAP, typiquement avec le suffixe de l'établissement `dc=quelquechose,dc=fr`.

La commande est interactive, elle pose quelques questions puis créé une nouvelle base dans l'annuaire, avec un administrateur dédié dont il faudra saisir le mot de passe. Exemple de réponses aux questions :

```
# slapd-supann newdb
Suffixe de la base à créer (exemple : dc=dauphine,dc=fr) :
-> dc=quelquechose,dc=fr

Choisir un mot de passe administrateur (uid=admin,ou=people,dc=quelquechose,dc=fr) :
->
Une nouvelle fois :
->

Nom de l'organisation (o=...) :
uniquement des majuscules, sans accent
Exemple : ENS
-> QUELQUECHOSE

Code de l'établissement, préfixé par son origine (supannEtablissement={ORIG}CODE)
Exemples :
 {UAI}0350936C          Université de Rennes 1
 {SIRET}18004312700067  AMUE
 {CNRS}MOY1400          Délégation régionale de Toulouse du CNRS
-> {UAI}0610000X

Récapitulatif :
Suffixe : dc=quelquechose,dc=fr
Nom : QUELQUECHOSE
Code UAI : {UAI}0610000X
DN entité établissement : supannCodeEntite=QUELQUECHOSE,ou=structures,dc=quelquechose,

Créer cette base ? (taper oui)
-> oui
```

```
Chargement de la définition de la nouvelle base annuaire (/tmp/newdbsUdiiW.ldif) :
(add) olcDatabase={1}mdb,cn=config
(add) olcDatabase={1}mdb,cn=config
(add) olcOverlay={0}syncprov,olcDatabase={1}mdb,cn=config
(add) olcOverlay={1}accesslog,olcDatabase={2}mdb,cn=config
(add) olcOverlay={2}refint,olcDatabase={2}mdb,cn=config
(add) olcOverlay={3}constraint,olcDatabase={2}mdb,cn=config
(add) olcOverlay={4}unique,olcDatabase={2}mdb,cn=config
(add) dc=quelquechose,dc=fr
(add) ou=people,dc=quelquechose,dc=fr
(add) uid=admin,ou=people,dc=quelquechose,dc=fr
(add) ou=structures,dc=quelquechose,dc=fr
(add) supannCodeEntite=QUELQUECHOSE,ou=structures,dc=quelquechose,dc=fr
(add) ou=groups,dc=quelquechose,dc=fr
(add) cn=admin,ou=groups,dc=quelquechose,dc=fr
OK
#
```

Résultat :

- une base `dc=quelquechose,dc=fr` est ajoutée dans l'annuaire
- l'administrateur attribué à cette base est `uid=admin,ou=people,dc=quelquechose,dc=fr` avec le mot de passe choisi lors de la commande `newdb`.
- les logs des requêtes sur cette base sont dans `cn=accesslog,dc=quelquechose,dc=fr`

6 Installation d'un certificat SSL valide

Note : cette procédure peut être effectuée plus tard, lorsqu'un certificat valide sera nécessaire à la connexion au LDAP. Ce n'est pas nécessaire pour la liaison avec les composants LdapSaisie et IdP de la solution PSL.

Le serveur `slapd` utilise par défaut des certificats SSL « tests » qui ne seront pas valides en production.

Il faut obtenir un certificat valable auprès de son fournisseur habituel :

- signé par une autorité reconnue ;
- dont le nom corresponde au nom de la machine ;
- avec de bonnes dates de validité.

Ensuite, copier les clés obtenues sur ces emplacements :

- `/etc/ldap/ssl/slapd.pem` : certificat (clé publique signée par l'AC)
- `/etc/ldap/ssl/slapd.key` : clé privée

Au niveau des droits :

- `/etc/ldap/ssl/slapd.pem` doit être lisible par tout utilisateur
- `/etc/ldap/ssl/slapd.key` ne doit être lisible que par `slapd`

Pour cela, utiliser les commandes suivantes :

```
# chown -R root :openldap /etc/ldap/ssl
# chmod 0755 /etc/ldap/ssl
# chmod 0644 /etc/ldap/ssl/slapd.pem
# chmod 0640 /etc/ldap/ssl/slapd.key
```

Une fois le certificat et la clé privée installés, il faut **relancer le service `slapd`** avec la commande `service slapd restart`

```
# service slapd restart
[ ok ] Stopping OpenLDAP : slapd.
[ ok ] Starting OpenLDAP : slapd.
#
```

---

7 Historique du document

20150217 tnoel – première version

20150227 tnoel – ajout section newdb