Gestion d'identités PSL – Installation LdapSaisie

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* ».

2 Installation du composant LdapSaisie

Installer le paquet `ldapsaisie-supann` :

```
# apt-get install ldapsaisie-supann
```

Cette installation va déclencher l'installation de tous les composants logiciels (paquets) nécessaires à la mise en place de l'interface LdapSaisie connectable avec un annuaire SUPANN 2009.

La configuration se fait en deux étapes

- configuration du logiciel LdapSaisie proprement dit
- connexion du logiciel avec le serveur web Apache

3 Configuration de LdapSaisie

Modifier le fichier `/etc/ldapsaisie/local/conf/config.local.inc.php` pour faire correspondre les valeurs avec celles de la base créée dans l'annuaire LDAP (commande `slapd-supann newdb`).

Note : les éditeurs vi ou nano sont disponibles pour cela. Si vous êtes débutant sous Linux, préférez l'éditeur nano, plus accessible. Vous pouvez aussi installer d'autres éditeurs (`apt-get install vim` ou `apt-get instal emacs`)

```
# nano /etc/ldapsaisie/local/conf/config.local.inc.php
```

Le fichier est en PHP, attention à la syntaxe, ne retirez pas de virgule ou de paranthèse, etc.

Exemple d'un fichier renseigné :

```
<?php
/*******************************************************************************
 * Copyright (C) 2014 Easter-eggs
 * http ://ldapsaisie.labs.libre-entreprise.org
 *
 * Author : See AUTHORS file in top-level directory.
 *
 * This program is free software ; you can redistribute it and/or
 * modify it under the terms of the GNU General Public License version 2
 * as published by the Free Software Foundation.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY ; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program ; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, USA.

*******************************************************************************/

$debug = false ;

$supann_configs = array(
```

```
  array(
    'ldap_config' => array(
      /* adresse IP ou nom DNS du serveur LDAP */
      'host'     => '192.168.1.2',
      /* port d'écoute (devrait toujours être 389) */
      'port'     => 389,
      /* LDAPv3, ne pas changer */
      'version'  => 3,
      /* activation d'une connexion chiffrée TLS. Si true, il faut s'assurer
       * d'avoir un certificat valide sur le serveur LDAP, sinon ajouter cette
       * ligne à la fin de /etc/ldap/ldap.conf :
       *     TLS_REQCERT allow
      */
      'starttls' => false,

       /* nom de la base créée avec "newdb" */
      'basedn'   => 'dc=quelquechose,dc=fr',
      /* DN de l'administrateur, il faut juste modifier le suffixe dc=...  qui
       * doit être égal à la valeur du basedn précédent */
      'binddn'   => 'uid=admin,ou=people,dc=quelquechose,dc=fr',
      /* mot de passe de l'administrateur choisi lors du "newdb" */
      'bindpw'   => 'as;KUAq*6123',

      /* ne pas toucher si vous ne savez pas ce que vous faîtes ...*/
      'options'  => array(),
      'filter'   => '(objectClass=*)',
      'scope'    => 'sub'
    ),
    'globals' => array(
      /* indiquer ici le DN de l'entité parente de l'établissement,
       * par exemple
       *    supannCodeEntite=QUELQUECHOSE,ou=structures,dc=quelquechose,dc=fr
       * où QUELQUECHOSE est le code choisi lors du "newdb"
       */
      'LS_SUPANN_ETABLISSEMENT_DN' => 'supannCodeEntite=QUELQUECHOSE,ou=structures,dc=
      /* code UAI indiqué lors du newdb */
      'LS_SUPANN_ETABLISSEMENT_UAI' => '{UAI}0610000X',
      /* nom de domaine pour construire les eduPersonPrincipalName,
       * qui seront au format login@modifiez-moi.fr */
      'LS_SUPANN_EPPN_DOMAIN' => 'quelquechose.fr',
    ),
  ),
);
```

La configuration de LdapSaisie, automatiquement modifiée par le paquet `ldapsaisie-supann`, est déjà conforme à SUPANN 2009.

4 Configuration d'Apache pour exposer LdapSaisie

Le serveur HTTP Apache est déjà installé par `ldapsaisie-supann`. Il reste à le configurer. Une configuration par défaut est fournie qu'il suffit d'activer, voici la procédure pour cela.

Activer le module SSL d'Apache :

```
# a2enmod ssl
```

Puis activer la configuration par défaut du site qui exposer LdapSaisie :

```
# a2ensite ldapsaisie.conf
```

Il faut ensuite indiquer le *ServerName* au niveau de la configuration du site, dans le début du fichier `/etc/apache2/sites-enabled/ldapsaisie.conf` :

```
# nano /etc/apache2/sites-enabled/ldapsaisie.conf
```

Par exemple :

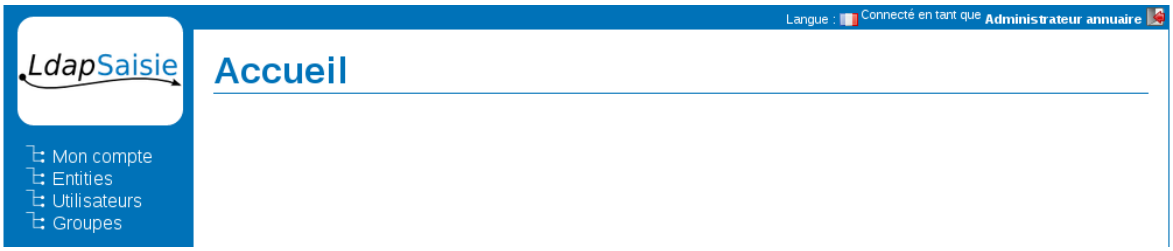
```
# extrait de /etc/apache2/sites-enabled/ldapsaisie.conf
    # où il faut modifier le ServerName
<VirtualHost * :443>
  ServerName ldapsaisie.quelquechose.fr   # <-- indiquer ici le nom DNS de la machine
  ...
```

Enfin, relancer le service `apache2` pour prendre en compte ces modifications de sa configuration :

```
# service apache2 restart
```

L'interface est alors accessible sur `https ://ldapsaisie.quelquechose.fr`

Pour se connecter, utiliser l'identifiant `admin` et le mot de passe choisi lors de la création de la base sur le serveur LDAP (`newdb`).



4.1 Installation d'un certificat pour HTTPS

Le certificat installé par défaut pour Apache est bien entendu invalide.

Pour installer un certificat valide (correspondant au nom du serveur et signé par une autorité reconnu) il faut en copier les clés un répertoire, par exemple `/etc/apache2/ssl` qui peut être créé pour l'occasion, puis indiquer l'emplacement des clés dans la configuration `/etc/apache2/sites-enabled/ldapsaisie.conf` :

```
# extrait de /etc/apache2/sites-enabled/ldapsaisie.conf
(...)
SSLCertificateFile    /etc/apache2/ssl/certificate.pem
SSLCertificateKeyFile /etc/apache2/ssl/private-key.key
```

Ensuite relancer le service pour prendre en compte la modification

```
# service apache2 restart
```

4.2 Adaptations de la configuration Apache

Le fichier `ldapsaisie.conf` fourni par la solution pour configurer Apache est un modèle, un exemple. Si vous connaissez bien la configuration Apache pour exposer un service PHP, et/ou si vous avez des besoins spécifiques de configuration, vous pouvez tout à fait créer votre propre configuration Apache. Vous pouvez même utiliser un autre serveur HTTP.

Cependant, la solution n'est supportée que pour Apache et pour un fichier de configuration qui ne soit pas trop distant du modèle `ldapsaisie.conf`.

5 Connexion au serveur LDAP en SSL/TLS

Il est préférable que LdapSaisie se connecte au serveur LDAP en TLS. Pour cela, modifier la valeur starttls dans la configuration de LdapSaisie, c'est-à-dire la ligne :

```
'starttls' => false,
```

dans le fichier `/etc/ldapsaisie/local/conf/config.local.inc.php`.

Attention, le certificat du serveur LDAP doit être valide. Si ce n'est pas le cas (par exemple lors de tests) vous devez modifier la configuration du client LDAP du système et lui dire de toujours accepter les certificat. Pour ce faire, ajouter la ligne suivante dans `/etc/ldap/ldap.conf` :

```
TLS_REQCERT allow
```

Au final, le fichier `/etc/ldap/ldap.conf` doit ressembler à cela :

```
# cat /etc/ldap/ldap.conf

# Exemple d'un fichier /etc/ldap/ldap.conf·qui accepte
# n'importe quel certificat serveur

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
TLS_REQCERT allow
```

---

6 Historique du document

20150217 tnoel – première version