

## Authentification du système sur LDAP

Les configurations que nous allons effectuer sur notre contrôleur de domaine auront un gros impact sur le serveur même. Le tout consiste à ce que votre serveur Linux puisse s'authentifier sur le service LDAP.

C'est ici que nous allons démêler un peu l'authentification des différents intervenants sur le domaine.

- Contrôleurs de domaine Linux;
- Clients Linux;
- Client Windows;
- Serveurs membres Linux;
- Serveurs membres Windows;
- Services sous un serveur Linux.

### Authentification avec PAM

Le module d'authentification PAM (*Pluggable Authentication Module*) permet l'intégration de plusieurs types de technologie d'authentification (Unix, LDAP, etc.) pour les différents services, tel *login*, *passwd*, *rlogin*, *su*, *ssh*, *ftp*, etc. ce sans aucun changement dans les services.

Pour notre part, nous allons utiliser le module *pam\_ldap* créé par PADL Software qui va permettre l'authentification des utilisateurs et groupes sur le service LDAP. Les fichiers de configuration de PAM se retrouvent dans le répertoire */etc/pam.d*. Nous parlons des fichiers de configuration PAM, car chacun des services utilisant PAM a son propre fichier de configuration.

Point à remarquer, sous Gentoo tous les services utilisant PAM comme mécanisme d'authentification inclus le fichier de configuration *system-auth* dans le leur. Cette inclusion va nous simplifier la vie, car nous auront seulement ce fichier à modifier.

Il vous faudra aussi prendre en considération, que tous les fichiers de configuration des services utilisant PAM vont désormais supporter LDAP, ce qui n'est pas toujours une bonne chose. A vous de déterminer si vous incluez toujours le fichier *system-auth*.

**NOTE:** Si vous désirez de plus ample informations supplémentaires sur le module *pam\_ldap*, visitez le site de PADL au [http://www.padl.com/OSS/pam\\_ldap.html](http://www.padl.com/OSS/pam_ldap.html).

#### NOTES







Windows veut accéder aux fichiers, le système NSS va vérifier si l'utilisateur demandeur existe, de quels groupes il fait parti et est-ce qu'il a les droits suffisants.

Pour connaître l'utilisateur et savoir de quels groupes il fait parti, le mécanisme NSS regarde dans son fichier `/etc/nsswitch.conf`.

Ce dernier indique que le service LDAP est une référence qui contient les informations des utilisateurs et des groupes. NSS fait alors la demande à l'aide de la librairie `nss_ldap.so` qui communique avec le côté serveur du contrôleur de domaine.

La recherche se fait alors dans l'annuaire LDAP qui renvoie ses informations au mécanisme NSS qui autorise ou non l'accès au répertoire ou au fichier.

### Synthèse avec PAM/NSS

Si nous avons des **clients Linux** qui s'authentifieraient sur notre contrôleur de domaine, cette relation serait quasi identique que celle du contrôleur de domaine. Le *côté client* se situerait sur le poste Linux, alors que le *côté serveur* serait situé sur notre contrôleur de domaine.

Il en serait de même pour les **serveurs autonomes Linux**.

Par contre si nous avons des **clients Windows** qui s'authentifieraient sur notre contrôleur de domaine Linux, cette relation serait différente. Le mécanisme d'authentification du poste Windows se connecterait sur `stunnel` qui communiquerait avec le service Samba. Le service Samba communiquerait alors avec l'annuaire LDAP. Le côté client PAM et NSS est alors inutilisé.

Il en serait de même pour les **serveurs autonomes Windows**.

Donc en résumé, avec cette configuration:

Les contrôleurs de domaine Linux utilisent les mécanismes PAM/NSS qui se connectent au service LDAP situé sur leur propre système.

Les postes Linux utilisent les mécanismes PAM/NSS qui se connectent au service LDAP situé sur le contrôleur de domaine.

NOTES



Les postes Windows et les serveurs autonomes Windows utilisent leur propre mécanisme qui se connecte au service Samba de notre contrôleur de domaine. Samba se branche alors à l'annuaire LDAP pour trouver ses informations d'authentification.

Les serveurs autonomes Linux, tant qu'à eux, utilisent les mécanismes PAM/NSS qui se connectent au service LDAP situé sur le contrôleur de domaine.

## NOTES



## Installation de pam\_ldap et de nss\_ldap

### Intégration de pam\_ldap

Pour faire l'installation de la librairie *pam\_ldap*, saisissez la commande:

```
USE="ssl" emerge pam_ldap
```

Une fois l'installation terminée, vérifier que la librairie est correctement installé.

```
equery uses pam_ldap
```

Faites ensuite la modification du fichier *system-auth* situé dans le répertoire */etc/pam.d*. Puis ajouter ou modifier les lignes en gras dans votre fichier.

```
vim /etc/pam.d/system-auth
```

```

#%PAM-1.0
auth      required      pam_env.so
auth      sufficient    pam_unix.so try_first_pass likeauth nullok
auth      sufficient    pam_ldap.so use_first_pass
auth      required      pam_deny.so

account   required      pam_unix.so
account   sufficient    pam_ldap.so

password  required      pam_cracklib.so difok=2 minlen=8 dcredit=2 ocredit=2
retry=3
password  sufficient    pam_unix.so try_first_pass use_authok nullok
sha512 shadow
password  sufficient    pam_ldap.so use_authok
password  required      pam_deny.so

session   required      pam_limits.so
session   required      pam_env.so
session   required      pam_unix.so
session   optional     pam_ldap.so
session   optional     pam_permit.so

```

L'ordre des entrées dans les fichiers de configuration de PAM est extrêmement important. Aussi, assurez-vous que la syntaxe est impeccable. Si cette syntaxe est incorrecte, votre système ne fonctionnera plus correctement et vous serez dans l'incapacité de vous authentifier sur votre ordinateur.

Bon prévoyons le pire. Si vous êtes dans cette situation, il suffit simplement de redémarrer sur votre InstallCD, de remonter la partition root et de modifier le fichier désiré (blanc de mémoire? revoyez le module 2 - Installation de Gentoo).

### Intégration de nss\_ldap

Pour faire l'installation de la librairie nss\_ldap, saisissez la commande:

```
emerge nss_ldap
```

Encore une fois, vérifiez que la librairie est correctement installée. Prenez le temps de le faire pour chacune des installations, cela peut vous faire sauver du temps en cas d'erreur.

```
equery uses nss_ldap
```

Faites ensuite la modification du fichier *nsswitch.conf* situé dans le répertoire */etc*. Puis ajuster votre fichier pour qu'il ressemble à ceci.

```
vim /etc/nsswitch.conf
```

```
#passwd:    compat
#shadow:    compat
#group:     compat

passwd:    files ldap
shadow:    files ldap
group:     files ldap

# passwd:   db files nis
# shadow:   db files nis
# group:    db files nis

hosts:     files dns wins
networks:   files dns

services:   db files
protocols:  db files
```

## NOTES



