

# Unification des mots de passe Linux et Windows

Institut de Physique Nucléaire  
Orsay

# Unification des mots de passe

## Linux et Windows

### **Avant 2006 :**

- Sous Unix, Linux : base de données NIS
- Sous windows : Active Directory

### **Conséquences :**

- 2 comptes différents
- 2 mots de passe à gérer pour l'utilisateur

# Unification des mots de passe Linux et Windows

**En 2006 :**

Comme NIS n'évoluait plus et n'incluait pas de cryptage, la migration vers LDAP s'imposait.

Le package Fedora openldap-servers fourni des scripts de migration des bases NIS en bases LDAP.

# Unification des mots de passe

## Linux et Windows

### Le principe de l'unification :

- Créer 2 bases des comptes sous LDAP et Active Directory. Les identifiants (login) des utilisateurs doivent être identiques.
- Utiliser la base LDAP pour les informations liées au compte (UID, GUID, home, shell ...)
- Utiliser la base Active Directory pour l'authentification en mode kerberos

# Unification des mots de passe

## Linux et Windows

**Sur le client Linux** on fait appel à un serveur kerberos et à un serveur LDAP.

Les packages openldap et nss\_ldap (utilisation dans PAM) créent 2 fichiers : /etc/openldap/ldap.conf et /etc/ldap.conf

Il faut y définir le nom du serveur et le nom de la base utilisée.

PAM permet de définir comment on fait les authentications.

# Unification des mots de passe

## Linux et Windows

**/etc/ldap.conf**

# The distinguished name of the search base.

base dc=ipnorsay,dc=fr

uri ldap://ipnldap/ ldap://ipnldap2/

ssl no

tls\_cacertdir /etc/openldap/cacerts

pam\_password md5

# Unification des mots de passe

## Linux et Windows

**`/etc/openldap/ldap.conf`**

URI ldap://ipnldap/ ldap://ipnldap2/

BASE dc=ipnorsay,dc=fr

# /etc/krb5.conf

[libdefaults]

default\_realm = IPNO.IN2P3.FR

[realms]

IPNO.IN2P3.FR = {

kdc = ipnodc3.in2p3.fr

kdc = ipnodc2.in2p3.fr

kdc = ipnodc1.in2p3.fr

admin\_server = ipnodc3.in2p3.fr

admin\_server = ipnodc2.in2p3.fr

admin\_server = ipnodc1.in2p3.fr

}

[domain\_realm]

ipno.in2p3.fr = IPNO.IN2P3.FR

.ipno.in2p3.fr = IPNO.IN2P3.FR



# /etc/pam.d/system-auth

```
auth    required    pam_env.so
auth    sufficient   pam_unix.so nullok try_first_pass
auth    requisite    pam_succeed_if.so uid >= 100 quiet
auth    sufficient   pam_krb5.so use_first_pass
auth    required     pam_deny.so
```

```
account required    pam_unix.so broken_shadow
account sufficient   pam_succeed_if.so uid < 100 quiet
account [default=bad success=ok user_unknown=ignore] pam_krb5.so
account required     pam_permit.so
```

```
password requisite    pam_cracklib.so try_first_pass retry=3
password sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password sufficient    pam_krb5.so use_authtok
password required      pam_deny.so
```

```
session optional     pam_keyinit.so revoke
session required      pam_limits.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required      pam_unix.so
session optional      pam_krb5.so
```

# Unification des mots de passe

## Linux et Windows

**/etc/nsswitch.conf**

passwd: files ldap

shadow: files ldap

group: files ldap

hosts: files dns

netgroup: files ldap

automount: files ldap

# Unification des mots de passe Linux et Windows

Sous Fedora et sur le client Linux, la commande **system-config-authentication** permet de modifier une partie des fichiers ci-dessus.

Au niveau du **serveur Linux**, il faut modifier le fichier `/etc/openldap/slapd.conf`

# /etc/openldap/slapd.conf

```
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/redhat/autofs.schema
include      /etc/openldap/schema/nis.schema
```

```
# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2
```

```
pidfile      /var/run/slapd.pid
argsfile     /var/run/slapd.args
database     bdb
suffix "dc=ipnorsay,dc=fr"
rootdn "cn=manager,dc=ipnorsay,dc=fr"
```

```
#defaultaccess read
sizelimit 3000
```

```
# augmenter le cachesize par défaut pour corriger le bug suivant :
# bdb(dc=ipnorsay,dc=fr): Unable to allocate memory for transaction detail
cachesize 5000
```

## **/etc/openldap/slapd.conf (suite)**

```
rootpw {SSHA}WNGbLfycRB/fLOJO6piJE+3YSMvmPKwn
```

```
# Augmenter la taille du pool de threads
```

```
threads      32
```

```
# Indices to maintain for this database
```

```
index objectclass eq
```

```
index uid eq,pres
```

```
index uidNumber eq
```

```
index gidNumber eq
```

```
index memberUid eq,pres
```

```
index cn,sn pres,eq,sub
```

```
index nisMapName eq,pres
```

## /etc/openldap/slapd.conf (fin)

#index

userPassword,shadowLastChange,shadowMax,shadowMin,shadowWarning,shadowInactive,shadowExpire,  
shadowFlag

eq,pres

# Replicas of this database

replogfile /var/lib/ldap/replog

replica host=ipnli15:389

bindmethod=simple

binddn="cn=replicator,dc=ipnorsay,dc=fr"

credentials=motdepasse

access to attr=userPassword

by self write

by anonymous auth

by dn.base="cn=manager,dc=ipnorsay,dc=fr" write

by \* none

access to \*

by self write

by dn.base="cn=manager,dc=ipnorsay,dc=fr" write

by \* read

# Unification des mots de passe

## Linux et Windows

### Les problèmes rencontrés :

Pour une base de 800 comptes avec 100 postes linux un nombre très important de requêtes et des logs a posé de gros problèmes de performance (lenteur, occupation du disque)

### Les solutions :

- Au niveau du client, garder les informations qui ont été recherchées dans la base des comptes en activant le cache **nscd** pour diminuer les requêtes.
- Au niveau du serveur, réserver une place pour la base dans la mémoire RAM.

# Unification des mots de passe

## Linux et Windows

Le type de la base est bdb.

Dans `/var/lib/ldap/DB_CONFIG` :

- Mettre `set-tx-max` à 100 pour augmenter le nombre de transactions simultanées.
- Augmenter la taille du cache :

```
set-cachesize 0 52478800
```



# Unification des mots de passe

## Linux et Windows

Pour les fichiers log :

- création d'un lien de `/var/log/ldap.log` vers `/vol0/log/ldap/ldap.log` afin de les placer sur une partition importante en taille et différente de la racine.
- Faire une rotation journalière des fichiers `ldap.conf` en modifiant `/etc/logrotate.conf`. Ceci afin que la taille des fichiers reste raisonnable

# Unification des mots de passe Linux et Windows

Pour tous renseignements, contacter  
Benjamin Préciado : [preciado@ipno.in2p3.fr](mailto:preciado@ipno.in2p3.fr)