

OpenLDAP Centralisation authentication Linux

Identification : Fournit une/des informations qui identifie une personne, etc (ex : un nom)

Authentification : L'authentification vérifie/prouve les informations fournies dans l'identification

Supprimer la base de données BDB de openldap :

```
rm * /var/lib/ldap/
```

Créer deux comptes systèmes etu3 et etu4 :

```
useradd -d /home/etu3 -m -s /bin/bash etu3
passwd etu3
useradd -d /home/etu4 -m -s /bin/bash etu4
passwd etu4
```

Installer l'outil de migration :

```
apt install migrationtools
export PERLLIB=/usr/share/migrationtools
```

Modifier le fichier /usr/share/migrationtools/migrate_coomon.ph :

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "stsio.lan"
# Default base
$DEFAULT_BASE = "dc=stsio,dc=lan";
```

Migration :

```
./migrate_base.pl > ./init_base_migration.ldif
./migrate_passwd.pl /etc/passwd >> ./init_base_migration.ldif
./migrate_group.pl /etc/group >> ./init_base_migration.ldif
```

Créer l'annuaire :

```
systemctl stop slapd.service
slapadd -l /usr/share/migrationtools/init_base_migration.ldif
slapcat
slaptest
chown -R openldap:openldap /var/lib/ldap/
slapindex
systemctl start slapd.service
```

Supprimer etu3 et etu4 en local :

```
userdel etu3
userdel etu4
```

Installer libnss :

```
apt install libnss-ldap
```

Modifier le fichier /etc/nsswitch.conf :

```
passwd:    files systemd ldap
group:     files systemd ldap
shadow:    files ldap
```

Modifier le fichier /etc/libnss-ldap.conf :

```
host 127.0.0.1
base dc=stsio,dc=lan
ldap_version 3
rootbinddn cn=admin,dc=stsio,dc=lan
scope sub
pam_filter objectclass=posixaccount
pam_login_attribute uid
pam_member_attribute gid
pam_password crypt
```

Redémarrer le service nscd :

```
systemctl restart nscd.service
```

Test :

```
getent passwd
getent group
getent shadow
```

etu3 et etu4 doivent apparaitre

Permettre l'authentification sur le client depuis les comptes de l'annuaire :
modifier le fichier /etc/pam_ldap.conf :

```
#IP de l'annuaire LDAP
host 127.0.0.1
base dc=stsio,dc=lan
ldap_version 3
rootbinddn cn=admin,dc=stsio,dc=lan
scope sub
pam_filter objectclass=posixaccount
pam_login_attribute uid
pam_member_attribute gid
pam_password crypt
```

On peut maintenant se connecter depuis un compte de l'annuaire.