AGGIORNAMENTO DI UN SERVER LDAP PER CONTROLLO DEGLI ACCESSI CENTRALIZZATO

Autore: Alessandro Tacchini, INAF OAS - Bologna

INDICE

1. Introduzione

Il controllo centralizzato degli accessi, la cosiddetta AAA (Authentication Authorization Accounting), è ormai diventata una caratteristica imprescindibile per la gestione di sistemi che si rivolgono a gruppi di utenti sia molto grandi che relativamente piccoli.
Il vantaggio di avere un unico soggetto deputato a gestire e distribuire ad un gruppo di macchine fisiche, o virtuali o ancora strumenti che richiedono un accesso, alcune informazioni di sistema, tipo username e password, è noto sin dai tempi di NIS (Network Information Service) della SUN Microsystems.
Al giorno d'oggi vi sono due sistemi alternativi tra cui scegliere questo tipo di funzionalità: LDAP[1] (Lightweight Directory Access Protocol) e ACTIVE DIRECTORY[2].
Anche se i due sistemi non sono totalmente incompatibili, in INAF - OAS (Osservatorio di Astrofisica e Scienza dello Spazio) si utilizza OpenLDAP[3] perchè è Open source, ha un buon supporto da parte della comunità informatica ed è nativo dell'ambiente UNIX/LINUX (la quasi totalità dei server che vengono utilizzati è Linux).
ACTIVE DIRECTORY è una soluzione proprietaria di Microsoft ed è complicato utilizzarla per sistemi Linux.

---

[1] https://ldap.com/
[2] https://learn.microsoft.com/it-it/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
[3] https://www.openldap.org/

La versione di OpenLDAP presente fino al 2021 era talmente datata[4] da essere un pericolo per la sicurezza informatica.
Lo scopo di questo documento è descrivere le operazioni necessarie al passaggio all'ultima versione che non è direttamente compatibile con quella vecchia.
Non si tratta di un caso banale, che richiederebbe solamente di installare un nuovo webmin ed importare direttamente i dati, ma di qualcosa di peculiare che ha richiesto un lavoro impegnativo.

2. Recupero dati dal server originale

Il server originale consiste di una macchina virtuale con 2 GB di RAM ed una CPU con 2 core, uno spazio storage di 8 GB.
Il sistema operativo è un Linux CentOS 5.11.
Considerando che il supporto di sicurezza per quella versione di CentOS è terminato nel 2017 risulta evidente la necessità di effettuare un aggiornamento ad un sistema più moderno.
La versione di Openldap utilizzata al momento della migrazione è la 2.3.43 e l'interfaccia di gestione è Webmin 1.75.

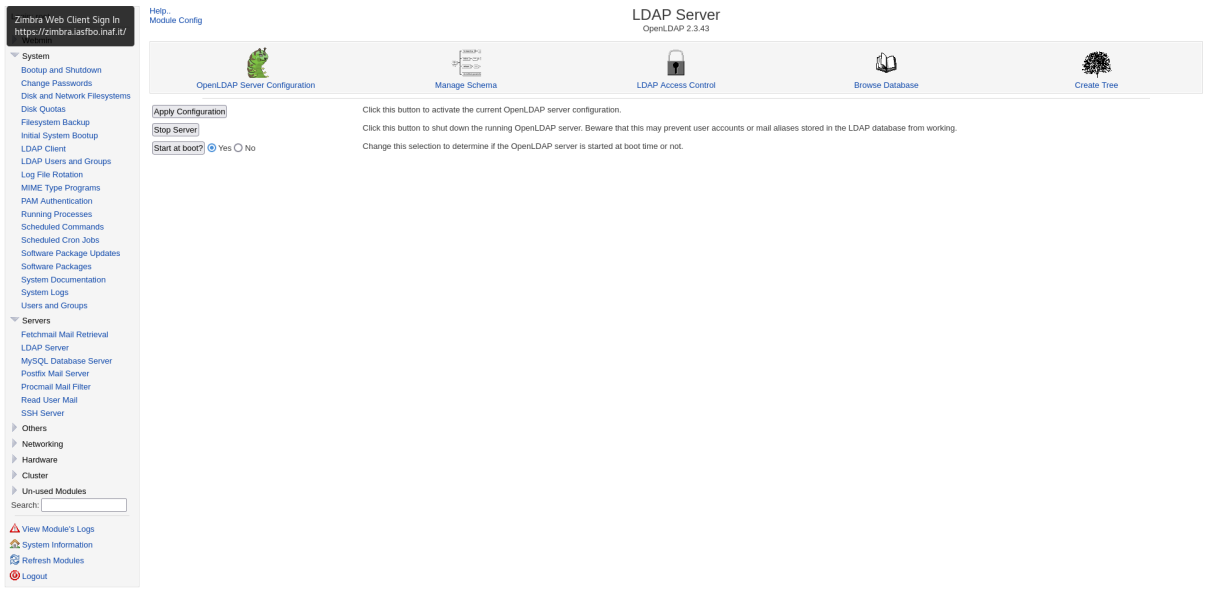

Fig.1 Interfaccia dell'LDAP server su Webmin

[4] Openldap 2.3.3

Gli schema utilizzati sono abbastanza comuni, a parte “eduperson”, ma non tutti verranno mantenuti.
Per semplicità si è deciso di concentrarsi sulle informazioni veramente importanti, “common name” “uid” e “password”.

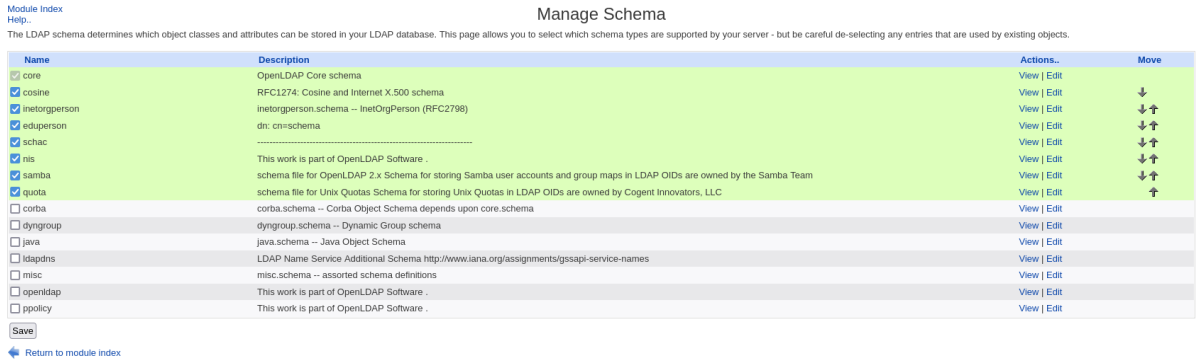

Fig.2 schema utilizzati

Invece di copiare il file /etc/openldap/slapd.conf e da quello poi creare la configurazione sul nuovo server (che utilizza un altro approccio basato su database contenuti in directory) si è scelto un altro approccio.
L’unica operazione è stata quella di effettuare il dump dell’intero database ldap col comando:

```
slapcat -l iasf2021.ldif
```

Il file iasf2021.ldif contiene l’intero albero LDAP a partire dalla radice, da questo file si ricaveranno le parti che saranno importate sul nuovo server.
Durante le operazioni di migrazione, dump del vecchio LDAP – trasferimento file – preparazione del nuovo LDAP – importazione dati, è importante che non vengano fatte modifiche al database per mantenere coerenza e non perdere dati.

Purtroppo questo non è avvenuto e si sono dovuti aggiungere al database alcuni nuovi utenti.
Per ovviare al problema è stato effettuato un nuovo dump del database poco prima di terminare la migrazione al nuovo

```
slapcat -l newoas.ldif
```

e facendo la differenza tra i due dump si sono ottenuti i record dei nuovi utenti da inserire nel nuovo server.

3. Nuovo server LDAP

La scelta di procedere in modo manuale e di non utilizzare una delle soluzioni integrate tipo Webmin o Freeipa[5] è stata dettata dalle condizioni al contorno. In particolare la necessità di non usare per nulla ticket Kerberos[6] ed il tempo limitato per mettere in produzione il nuovo server.
La nuova macchina si chiama oasldap ed è costituita da una macchina virtuale con le seguenti caratteristiche: 2 GB di RAM, un processore con 2 core ed uno storage da 80 GB.
Il sistema operativo è un Linux CentOS 7.9 e la versione di Openldap installata è la 2.4.44.
In questa versione non è più raccomandabile intervenire direttamente sui file di configurazione ed i file stessi sono organizzati in modo diverso dalla vecchia versione.
Se si deve intervenire è opportuno usare comandi come ldapadd o ldapmodify, o anche ldapdelete.
Dopo aver effettuato un'installazione di base di CentoOS ed un aggiornamento si è installato Openldap con il comando:

```
yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel
```

poi si è aggiornato il firewall per permettere il servizio:

[5] https://www.freeipa.org/page/Main_Page
[6] Requisito avanzato dal responsabile del Cluster di Calcolo OAS

```
firewall-cmd --add-service=ldap --permanent
firewall-cmd reload
firewall-cmd --reload
```

e si è avviato il servizio

```
systemctl start slapd
systemctl enable slapd
```

Il comando slappasswd consente di creare un hash per la password di root di LDAP

```
slappasswd
```

Si è copiato ed incollato l'hash così ottenuto nel file ldaprootpasswd.ldif il cui contenuto è

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}3nm5EeVoWJipKUCxxxxxxxxxxxxxxxxxxxx
```

col comando

```
ldapadd -Y EXTERNAL -H ldapi:/// -f ldaprootpasswd.ldif
```

si è impostata la password per Openldap.
Successivamente si è creato un nuovo database partendo da un file di esempio e si sono aggiunti gli schema di cui c'è necessità

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap:ldap /var/lib/ldap/*
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

A questo punto si è effettuata una operazione importante, la creazione della struttura dell'albero del nuovo LDAP simile a quella del vecchio.
Per fare questo si sono creati 3 file: db.ldif, monitor.ldif, base.ldif.

db.ldif

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=xxxx,dc=xxx,dc=it

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=xxxx,dc=xxx,dc=it

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}3nm5EeVoWJipKxxxxxxxxxxxxxxxxxxxxxxxx
```

monitor.ldif

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth"
read by dn.base="cn=admin,dc=xxxx,dc=xxx,dc=it" read by * none
```

base.ldif

```
dn: dc=xxxx,dc=xxx,dc=it
dc: xxxx
objectClass: top
objectClass: domain

dn: cn=admin,dc=xxxx,dc=xxx,dc=it
```

```
objectClass: organizationalRole
cn: admin
description: LDAP Manager

dn: ou=People,dc=xxxx,dc=xxx,dc=it
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=xxxx,dc=xxx,dc=it
objectClass: organizationalUnit
ou: Group
```

Questi file sono stati aggiunti ad LDAP

```
ldapmodify -Y EXTERNAL  -H ldapi:/// -f db.ldif
ldapmodify -Y EXTERNAL  -H ldapi:/// -f monitor.ldif
ldapadd -x -W -D "cn=admin,dc=xxxx,dc=xxx,dc=it" -f base.ldif
```

Una volta creata la struttura dell'albero si è potuto importare i dati partendo dai file iasf2021.ldif e newoas.ldif.
La struttura di questi file è del tipo:

```
dn: uid=john,ou=People,dc=example,dc=com
uid: john
givenName: John
sn::
cn::
loginShell: /bin/false
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/john
shadowMin: -1
shadowMax: 999999
shadowWarning: 7
shadowInactive: -1
shadowExpire: -1
shadowFlag: 0
```

```
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
structuralObjectClass: inetOrgPerson
entryUUID:
creatorsName: cn=Manager,dc=example,dc=com
createTimestamp:
userPassword::
entryCSN:
modifiersName: cn=Manager,dc=example,dc=com
modifyTimestamp:
```

Il problema è che alcuni dei campi sono stati generati nuovamente alla creazione del nuovo ldap per cui è stato necessario eliminare tutti quelli che hanno generato errore.
Per esempio:

```
cat iasf2021.ldif | grep -v "entryCSN\|entryUUID\|structuralObjectClass\|creatorsName\|createTimestamp\|modifiersName\|modifyTimestamp" > people_updated.ldif
```

Altri campi eliminati sono stati: eduPerson, samba, schac, quota, schacUserEntitlements, objectClass: systemQuotas, schacUserStatus:.

Partendo dai due file iniziali ed operando delle correzioni successive si è giunti ad avere due file: people_updated9.ldif per gli utenti, gropus2.ldif per i gruppi.
A questo punto sono stati inseriti in LDAP coi comandi:

```
ldapadd -x -W -D "cn=admin,dc=xxxx,dc=xxx,dc=it" -f people_updated9.ldif
ldapadd -x -W -D "cn=admin,dc=xxxx,dc=xxx,dc=it" -f gropus2.ldif
```

A questo punto si ha un server LDAP perfettamente funzionante, tuttavia per interagire con esso servono comandi del tipo ldapadd o ldapdelete, oppure ldappasswd per modificare la password di un utente.
È molto più comodo usare un'interfaccia grafica.

4. Ldap Account Manager

Ldap Account Manager (LAM) è un frontend grafico di semplice utilizzo.
Per installarlo ci sono alcuni requisiti, specialmente su php.
Sono stati utilizzati i comandi:

```
yum install httpd httpd-tools php php-fpm php-mysqlnd php-opcache php-gd php-xml php-mbstring php-json php-gmp php-zip php-ldap

systemctl enable --now php-fpm

wget https://github.com/LDAPAccountManager/lam/releases/download/lam_7_7/ldap-account-manager-7.7-0.fedora.1.noarch.rpm

rpm -i ldap-account-manager-7.7-0.fedora.1.noarch.rpm

yum install mod_ssl openssl

systemctl start httpd
systemctl enable httpd
```

Dopodichè si configura tutto via web browser collegandosi alla pagina
https://xxxxxxx.xxx.it/lam

In alto a destra c’è il pulsante per la configurazione

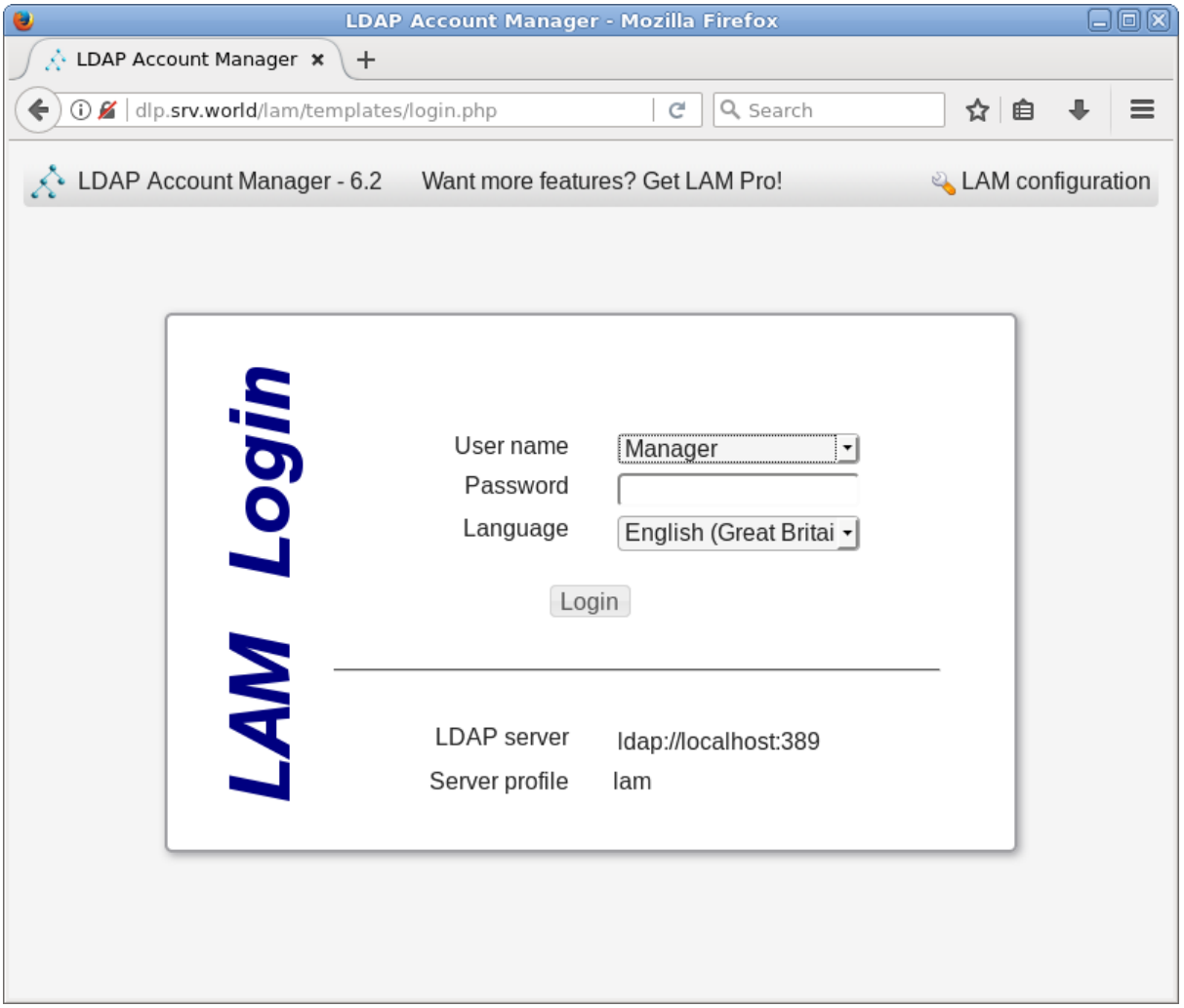

Fig.3 pagina di login di Ldap Account Manager

Poi si seleziona Edit server profile

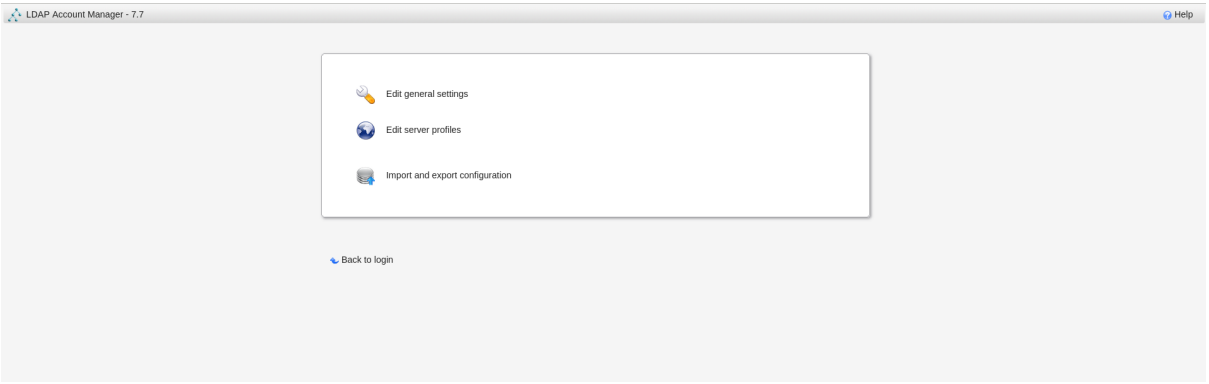

Fig.4 Configurazione di LAM

Si compilano i campi in modo da riferirsi al server LDAP già installato

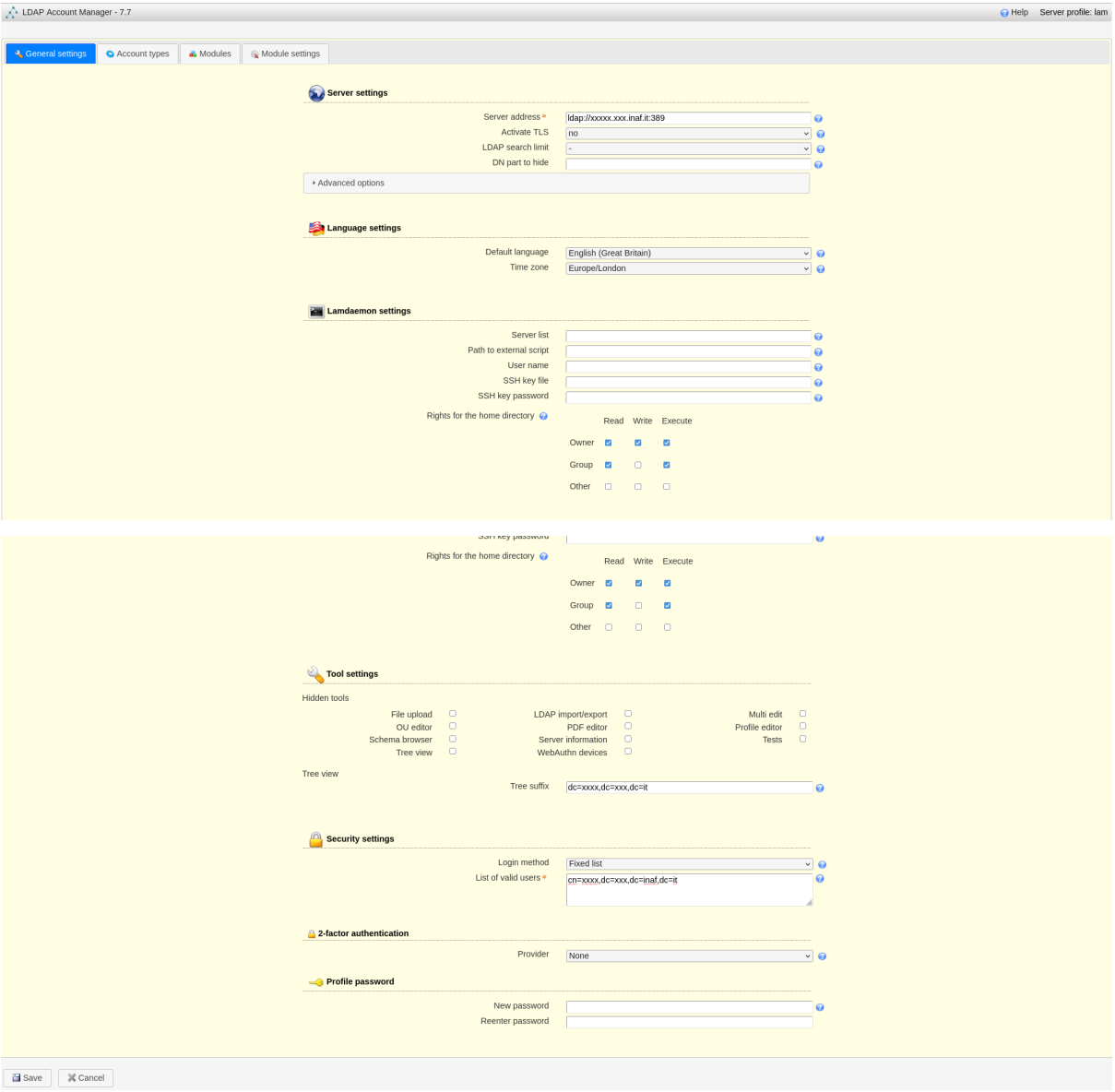

Fig.5 inserimento riferimenti server LDAP

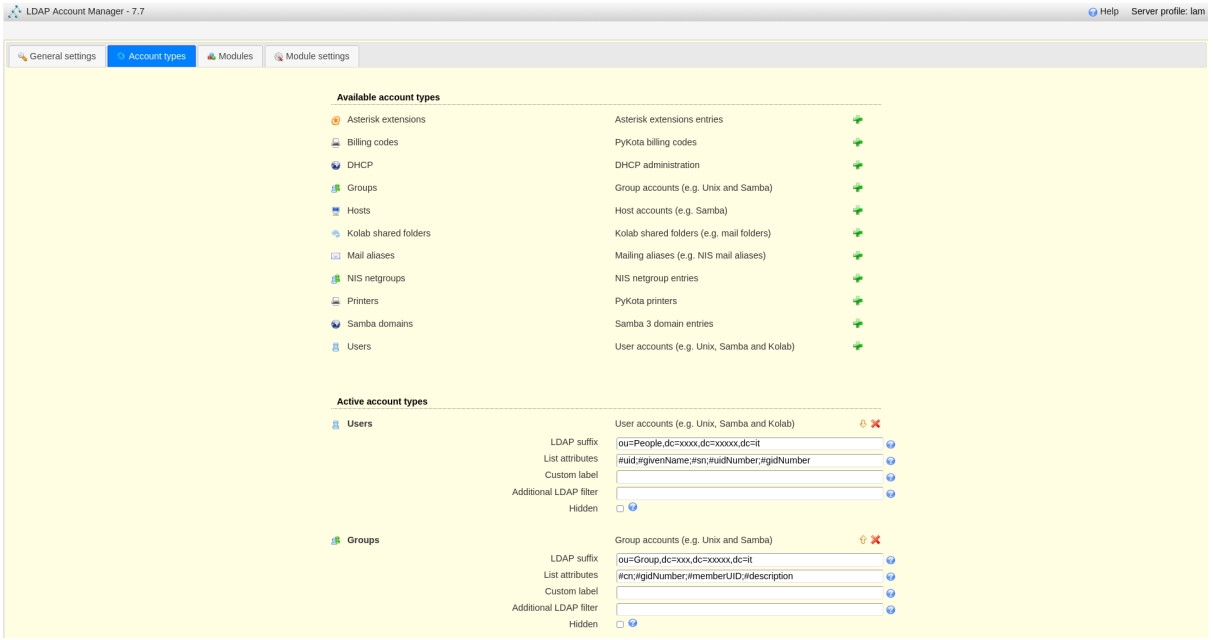

Fig.6 inserimenti riferimenti al server LDAP per i gruppi e gli utenti

Si possono selezionare i moduli che risultano più utili

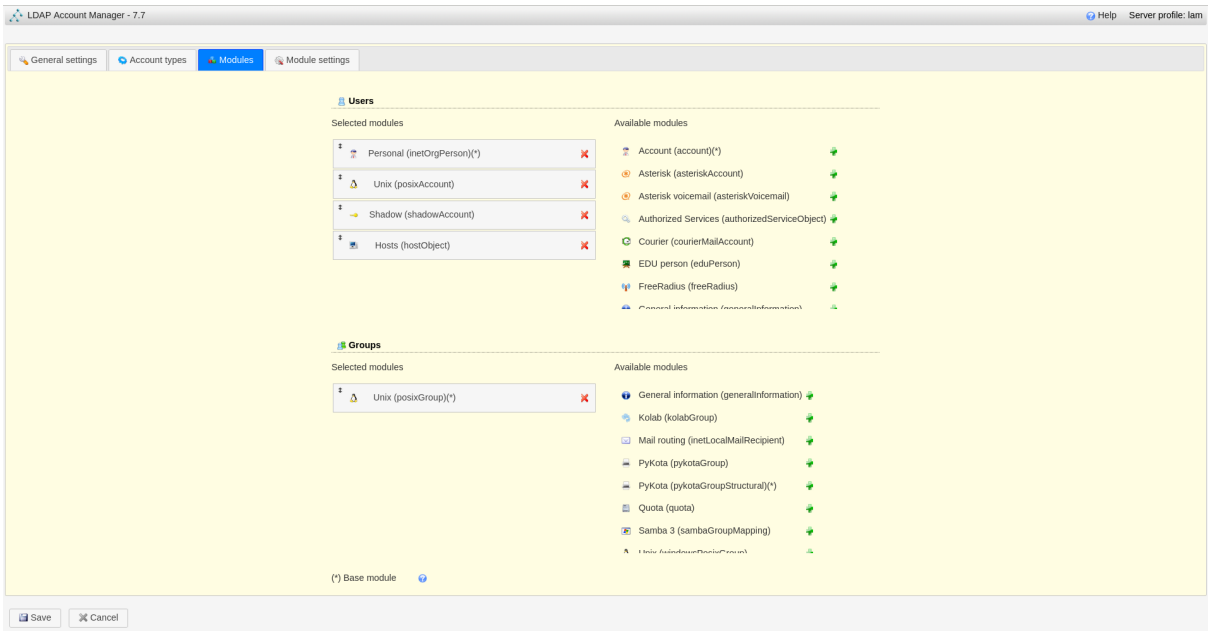

Fig.7 moduli per campi opzionali in LAM

L’interfaccia principale di gestione degli utenti

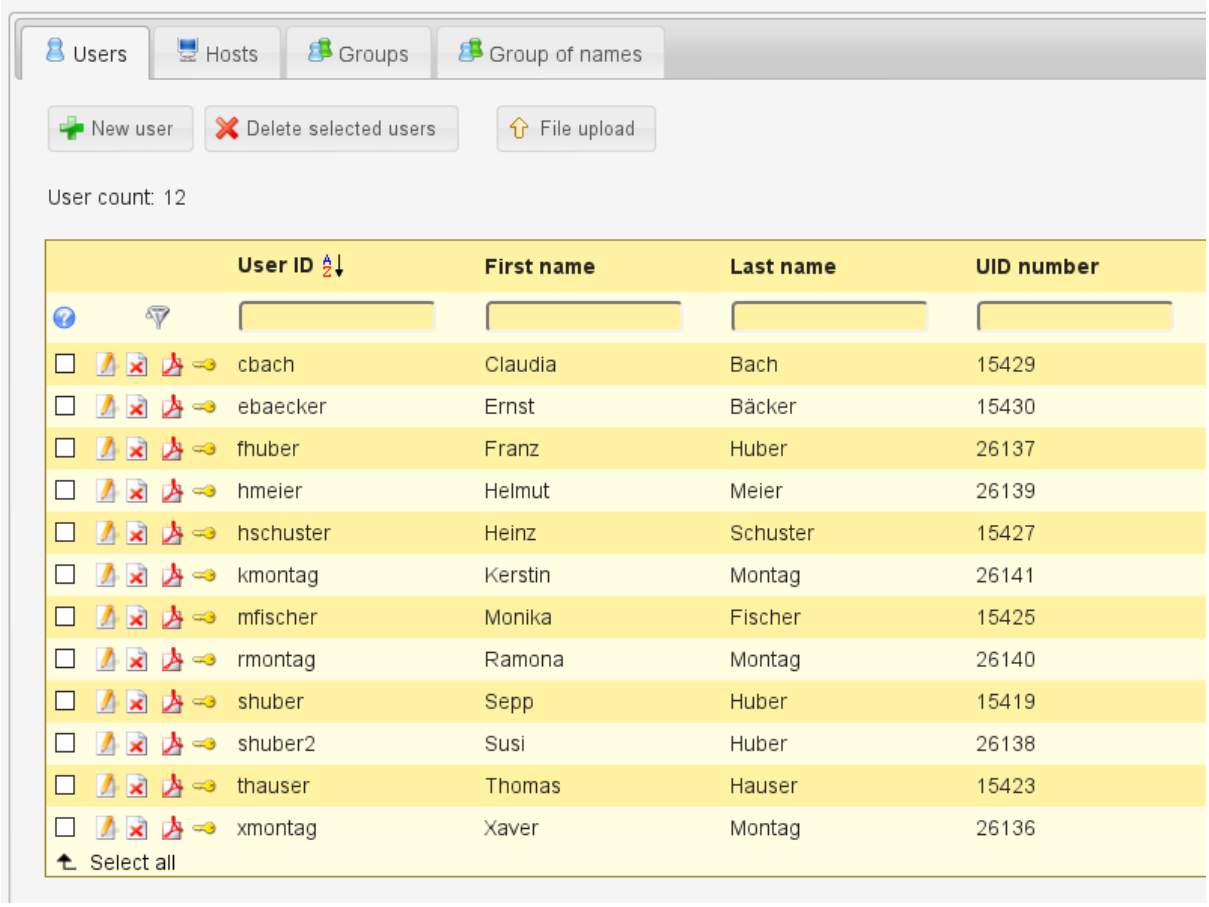

Fig.8 Interfaccia principale di gestione

Un aspetto negativo di Ldap Account manager in versione free è la mancanza di un meccanismo che permetta agli utenti di gestire la propria password in autonomia.