AUTENTICAZIONE

Installazione LDAP

Se non è configurato un server DNS è meglio aggiungere IP ed FQDN corrispondente nel file `/etc/hosts`:

```
192.168.100.xx      hpxx.<vostrogruppo>.localdomain
```

- Installiamo il server ldap:

```
# sudo apt install slapd ldap-utils
```

  - Inseriamo due volte la password di amministratore (ad esempio "`laslaslas`")

- Configuriamo il server ldap:

```
# sudo dpkg-reconfigure slapd
```

  - Chiede se lasciare vuota la configurazione… scegliete NO.
  - ***Scegliamo il nome del nostro dominio ldap (ad esempio <vostrogruppo>`.localdomain`)***
  - Scegliamo il nome dell'organizzazione (ad esempio `las`)
  - impostiamo la password dell' amministratore della struttura LDAP appena creata(ad esempio "laslaslas") e impostiamo il formato di memorizzazione, in particolare per il backend scegliamo come consigliato MDB
  - selezioniamo no alla rimozione del database nel caso di disinstallazione di slapd (per eventuali nuove installazioni, partendo da un certo database)
  - ed infine spostiamo se esiste il vecchio database.

Lightweight Directory Access Protocol – LDAP - DIT

- Modifichiamo il file di configurazione principale `ldap.conf` aggiungendo il dominio di esempio impostato in precedenza:

```
# sudo nano /etc/ldap/ldap.conf
```

  - Inseriamo le righe:

```
BASE dc=<vostrogruppo>,dc=localdomain
uri ldap://127.0.0.1 ldap://192.168.100.xx
ldap://hpxx.<vosrtrogruppo>.localdomain
```

- Riavviamo il demone slapd e abilitiamolo ad avviarsi all'avvio:

```
# sudo systemctl restart slapd
# sudo systemctl enable slapd
```

- Per verificare il corretto funzionamento della connessione LDAP eseguire il seguente comando

```
# sudo ldapwhoami -H ldap:// -x # dovreste ottenere anonymous
# sudo ldapsearch -x
```

LDAP – Creazione gruppi

- In ldap, per creare gruppi e utenti è necessario creare un file che definisce l'oggetto da creare come schema ldap. Creiamo il file `group.ldif` per il gruppo `studlas` con il seguente contenuto:

```
# cat group.ldif
dn: cn=studlas,dc=<vostrogruppo>,dc=localdomain
objectClass: top
objectClass: posixGroup
gidNumber: 3000
# sudo ldapadd -x -W -D
"cn=admin,dc=<vostrogruppo>,dc=localdomain" -f group.ldif
```

LDAP – Creazione utenti

- Stessa cosa anche per l'utente da creare:

```
# cat user.ldif
dn: uid=<nomeutente>,cn=studlas,dc=<vostrogruppo>,dc=localdomain
   objectClass: top
   objectClass: account
   objectClass: posixAccount
   objectClass: shadowAccount
   cn: <nomeutente>
   uid: <nomeutente>
   uidNumber: 16859
   gidNumber: 3000
   homeDirectory: /home/<nomeutente>
   loginShell: /bin/bash
   gecos: <Nome> <Cognome>
   userPassword: {crypt}x
   shadowLastChange: 0
   shadowMax: 0
   shadowWarning: 0
```

- `# sudo ldapadd -x -W -D "cn=admin,dc=<vostrogruppo>,dc=localdomain" -f user.ldif`

LDAP – verifica

- Per testare la configurazione controllate con `ldapsearch`:

```
# ldapsearch -x


. . . . . .
dn: cn=studlas,dc=<vostrogruppo>,dc=localdomain
objectClass: top
objectClass: posixGroup
gidNumber: 3000
cn: studlas

# <vostroutente>, studlas, <vostrogruppo>.localdomain
dn: uid=fromano,cn=studlas,dc=<vostrogruppo>,dc=localdomain
objectClass: top
. . . . .
```

LDAP – nss e pam

- Installiamo le estensioni ldap per nsswitch e pam:

```
# sudo apt install libnss-ldap libpam-ldap
```

- Attenzione: potrebbe esserei\ richiesto di inserire dei parametri:

  `URI ldap` mettete:

  `ldapi://127.0.0.1 ldap://192.168.100.xx`
  `ldap://hpxx.dc=<vostrogruppo>,dc=localdomain`

  `Domain ldap` mettete:

  `dc=<vostrogruppo>,dc=localdomain`

  `Admin ldap` mettete:

  `cn=admin,dc=<vostrogruppo>,dc=localdomain`

LDAP – nss e pam

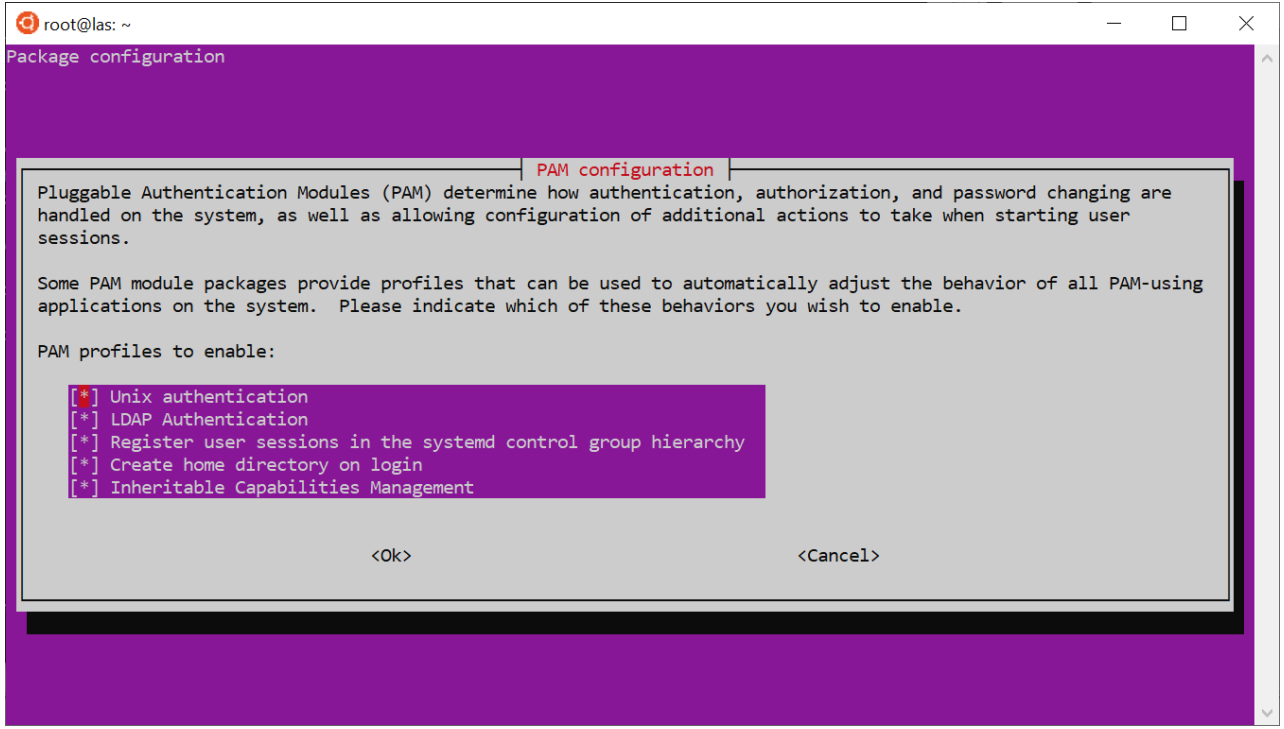
- Modifichiamo il file `/etc/nsswitch.conf` *in questo modo*

```
passwd: files systemd ldap
group: files systemd ldap
shadow: files systemd ldap
gshadow:        files
hosts:          files dns
networks:       files
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
netgroup: nis
```

LDAP – nss e pam

- Utilizziamo pam-auth-update per sistemare la configurazione di pam:

```
# pam-auth-update
```



LDAP – nss e pam

- Editate il file `/etc/pam.d/common-password` in modo che la riga 26 risulti così:

```
password [success=1 user_unknown=ignore default=die]
pam_ldap.so try_first_pass
```

- Cambiare la password all'utente:
- `# sudo ldappasswd -x -D "cn=admin,dc=<vostrogruppo>,dc=localdomain" -W -S \ "uid=fromano,cn=studlas,dc=<vostrogruppo>,dc=localdomain"`
- Testiamo se tutto funziona:

```
# getent passwd <nomeutente>

# getent group studlas

# su – <nomeutente>

# ssh <nomeutente>@localhost

# ssh <nomeutente>@192.168.100.xx
```

Provate anche con l' ip di un altro gruppo.

LDAP

- Come faccio ad utilizzare il server ldap appena configurato per gestire altri client?