

Activitat UD6

IMPORTANT! Realitza les següents activitats en la màquina virtual LINUX:

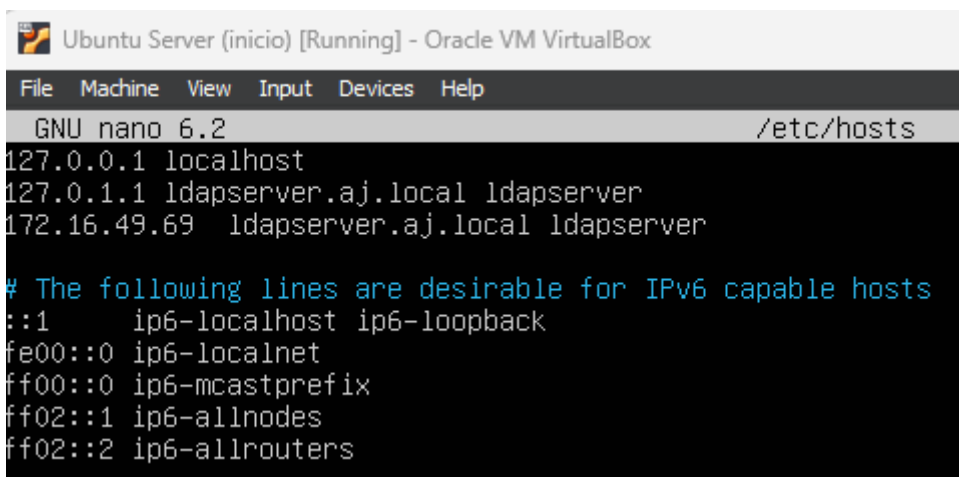
Activitat 1. Anem a crear i instal·lar en un servidor OpenLDAP, per dur a terme una gestió senzilla dels usuaris i els grups d'LDAP (protocolo ligero de acceso directo).

Tant el servidor com el client han d'estar dins el mateix rang de xarxa.

Configuració del servidor LDAP

1.- Modificam l'arxiu hosts.

- `sudo nano /etc/hosts`
 - Agregam davall de les altres direccions, la IP del nostre servidor:
 - *Exemple:* 192.168.10.100 prova.local



```
Ubuntu Server (inicio) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 ldapserver.aj.local ldapserver
172.16.49.69 ldapserver.aj.local ldapserver

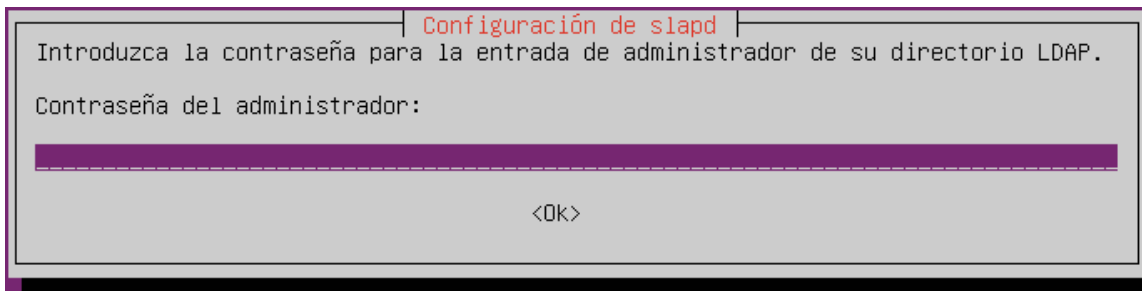
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

2.- Instal·lem el del servidor OpenLDAP slapd i el paquet ldap-utils, paquets que conté les utilitats d'administració d'LDAP:

- “`sudo apt-get install slapd`”
- “`sudo apt-get install ldap-utils`”
- Contrasenya administrador de la màquina.

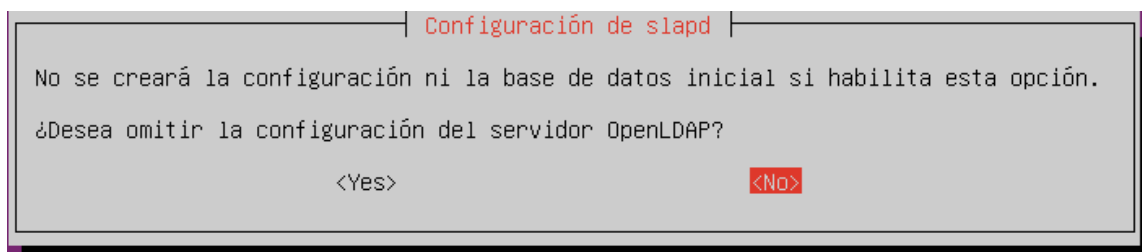
```
Ubuntu Server (inicio) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aj@aj:~$ sudo apt-get install slapd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
```

```
aj@aj:~$ sudo apt-get install ldap-utils -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
```

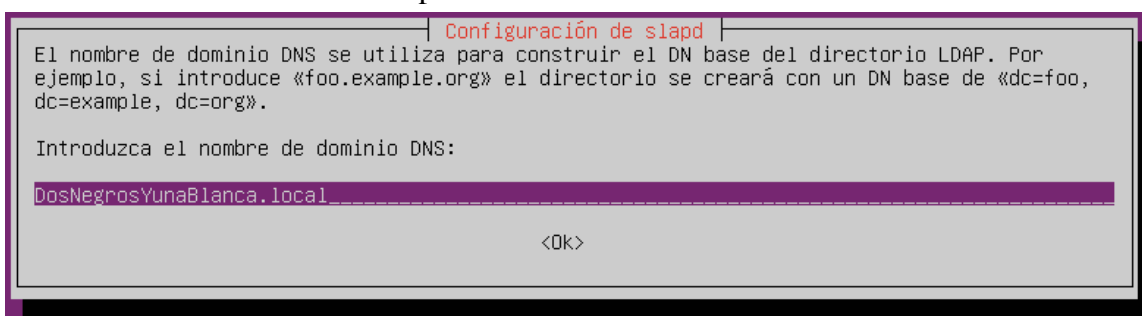


3.- Executem el següent comamndament: “sudo dpkg-reconfigure slapd”.

- Seleccionem “NO”



- Escrivim nom del domini “prova.local”



- Organització “prova”

Configuración de slapd

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

DosNegrosYunaBlanca

<OK>

- Password (APUTA'L!!!!) ç

Configuración de slapd

Introduzca de nuevo la misma contraseña de administrador para su directorio LDAP para verificar que la introdujo correctamente.

Confirme la contraseña:

<OK>

- Password (APUTA'L!!!!)
- Seleccionem "YES"
- Seleccionem "YES"

Configuración de slapd

Existen ficheros en «/var/lib/ldap» que probablemente interrumpen el proceso de configuración. Si activa esta opción, se moverán los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.

¿Desea mover la base de datos antigua?

☒ <Yes> ☐ <No>

4.- Modifiquem l'arxiu "base.ldif", aquest arxiu contendrà l'estructura del active directory.

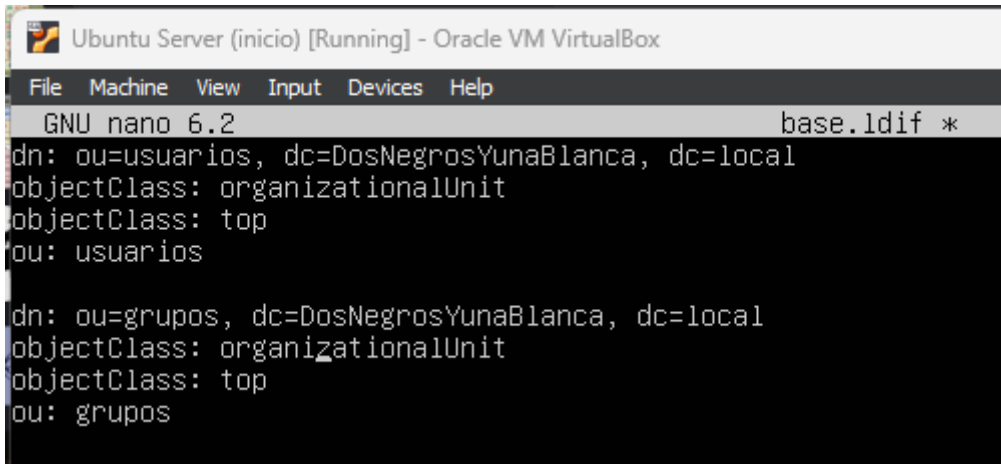
- Sudo nano base.ldif

```
dn: ou=usuarios, dc=prova, dc=local
objectClass: organizationalUnit
objectClass: top
ou: usuarios
```

```
dn: ou=grupos, dc=prova, dc=local
objectClass: organizationalUnit
```

objectClass: top

ou: grupos



```
Ubuntu Server (inicio) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 6.2 base.ldif *
dn: ou=usuarios, dc=DosNegrosYunaBlanca, dc=local
objectClass: organizationalUnit
objectClass: top
ou: usuarios

dn: ou=grupos, dc=DosNegrosYunaBlanca, dc=local
objectClass: organizationalUnit
objectClass: top
ou: grupos
```

- dn: ou=usuarios, dc=prova, dc=local: Defineix el Distinguished Name (DN) de la primera entrada com una unitat organitzativa anomenada "usuarios" dins del domini "prova.local".
- objectClass: organizationalUnit: Indica que l'entrada es de tipus "organizationalUnit", lo que significa que es una unitat organitzativa en el directori.
- objectClass: top: Especifica que aquesta entrada es de tipus "top", que es la classe superior en la jerarquia de classes de LDAP.
- ou: usuarios: Defineix l'atribut "ou" amb el valor "usuarios", que es el nom de la unidad organitzativa.
- dn: ou=grupos, dc=prova, dc=local: crea una unitat organitzativa anomenada "grupos" en el mateix domini.
- objectClass: organizationalUnit: Indica que l'entrada es de tipus "organizationalUnit".
- objectClass: top: Especifica que aquesta entrada es de tipus "top".
- ou: grupos: Defineix l'atributo "ou" amb el valor "grups", que és el nom de la segona unitat organitzativa.

Cream dues unitats organitzatives.

- Una vegada guardat aquest fitxer, l'hem d'executar:

- Sudo ldapadd -x -D cn=admin,dc=prova,dc=local -W -f base.ldif

```
aj@aj:~$ sudo ldapadd -x -D cn=admin,dc=DosNegrosYunaBlanca,dc=local -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios, dc=DosNegrosYunaBlanca, dc=local"
adding new entry "ou=grupos, dc=DosNegrosYunaBlanca, dc=local"
```

5.- Modifiquem l'arxiu "content.ldif", aquest arxiu contendrà informació sobre els objectes que formaran part del active directory.

- Sudo nano content.ldif

```
dn: cn=alumnes, ou=grupos, dc=prova, dc=local
objectClass: posixGroup
cn: alumnes
gidNumber: 10000
memberUid: alumnes
```

```
dn: uid=joan,ou=usuarios,dc=prova,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: joan
sn: asix
userPassword: 12345
loginShell: /bin/bash
uidNumber: 2002
gidNumber: 10000
homeDirectory: /home/joan
```

```
Ubuntu Server (inicio) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 6.2 content.ldif *
dn: cn=alumnes, ou=grupos, dc=DosNegrosYunaBlanca, dc=local
   objectClass: posixGroup
   cn: alumnes
   gidNumber: 10000
   memberUid: alumnes

dn: Uid=Austin, ou=usuarios, dc=DosNegrosYunaBlanca, dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Austin
sn: asix
userPassword: santi
loginShell: /bin/bash
uidNumber: 2002
gidNumber: 10000
homeDirectory: /home/Austin_
```

- dn: cn=alumnes, ou=grupos, dc=prova, dc=local:
 - dn (Distinguished Name) especifica l'ubicació única d'aquesta entrada en l'arbre de directori LDAP.
 - En aquest cas, l'entrada es troba en la unitat organitzativa (ou) "grupos" dins del domini "prova.local", i el seu nom comú (cn) es "alumnes".
- objectClass: posixGroup:
 - objectClass especifica la classe de l'objecte. En aquest cas, es un grup POSIX (posixGroup), que és una classe estàndard en LDAP utilitzada per a representar grups d'usuaris amb atributs compatibles amb POSIX.
- cn: alumnes:
 - cn (Common Name) especifica el nom comú del grup, que en aquest cas és "alumnes".
- gidNumber: 10000:
 - gidNumber especifica el nombre d'identificació del grup (GID). Cada grup POSIX ha de tenir un nombre GID únic. En aquest cas,

el GID és 10000.

- memberUid: alumnes:
 - memberUid especifica els noms dels usuaris (UID) dels membres que pertanyin a aquest grup. En aquest cas, el grup "alumnes" té un membre amb el nom d'usuari "alumnes".

En resum, aquest codi està creant una entrada de grup en un directori LDAP amb classe posixGroup. Aquest grup s'anomena "alumnes" i té un GID de 10000, a més té un membre amb el nom d'usuari "alumnes". Aquest tipus de representació es comu en entorns que segueixen l'estàndard de POSIX per a la gestió d'usuaris i grups.

- dn: uid=joan,ou=usuarios,dc=prova,dc=local:
 - dn (Distinguished Name) especifica l'ubicació única d'aquesta entrada l'arbre de directori LDAP.
 - L'entrada se troba a en la unitat organitzativa (ou) "usuarios" dins del domini "prova.local". El nom d'usuari (uid) es "joan".
- objectClass: inetOrgPerson:
 - objectClass especifica la classe de l'objecte. En aquest cas, és inetOrgPerson, que és una classe estàndard en LDAP utilitzada per a representar informació sobre persones en una organització.
- objectClass: posixAccount:
 - posixAccount és una altre classe que proporciona atributs relacionats amb comptes POSIX. Això inclou atributs com uidNumber, gidNumber, homeDirectory, i loginShell, que son comuns en entorns basats en Unix.
- objectClass: shadowAccount:
 - shadowAccount és una classe adicional que s'utilitza per a representar informació de compta de sombra en sistemes basats en Unix. La compta de sombra emmagatzema informació com la data d'expiració de la contrasenya i altres polítiques de seguretat relacionades.

- cn: joan:
 - cn (Common Name) especifica el nom comú de l'usuari, que en aquest cas és "joan".
- sn: asix:
 - sn (Surname) especifica el llinatge de l'usuari, que en aquest cas es "asix".
- userPassword: 12345:
 - userPassword emmagatzema la contrasenya de l'usuari. En aquest cas, la contrasenya és "12345".
- loginShell: /bin/bash:
 - loginShell especifica la shell d'inici de sessió de l'usuari. En aquest cas, és "/bin/bash".
- uidNumber: 2002:
 - uidNumber especifica el nombre de identificació d'usuari (UID) de l'usuari. En aquest cas, és 2002.
- gidNumber: 10000:
 - gidNumber especifica el nombre d'identificació de grup (GID) de l'usuari. En aquest cas, és 10000.
- homeDirectory: /home/joan:
 - homeDirectory especifica el directori d'inici de l'usuario. En aquest cas, és "/home/joan".

En resumen, aquest codi està creant una entrada d'usuari en un directori LDAP amb varies classes, incloent inetOrgPerson, posixAccount, i shadowAccount. Proporciona informació detallada sobre l'usuari, como el seu nom, llinatge, contrasenya informació de compte POSIX y compte de ombra en sistemes basats en Unix.

- Una vegada guardat aquest fitxer, l'hem d'executar:
 - Sudo ldapadd -x -D cn=admin,dc=prova,dc=local -W -f content.ldif

```
aj@aj:~$ sudo ldapadd -x -D cn=admin,dc=DosNegrosYunaBlanca,dc=local -W -f content.ldif
Enter LDAP Password:
adding new entry "cn=alumnos, ou=grupos, dc=DosNegrosYunaBlanca, dc=local"
adding new entry "Uid=Austin,ou=usuarios,dc=DosNegrosYunaBlanca,dc=local"
```


Configuració del Client

1.- Instal·lem els paquets de ldap.

- Sudo apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db nscd

ldap-utils

```
bj@aj-VirtualBox:~$ sudo apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db nscd ldap-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libde265-0 libflashrom1 libftdi1-2 libheif1 liblvm13 libmng2 libmypaint-1.5-1 libmypaint-common
```

○ ldap://192.168.0.102 (IP servidor)

Configuring ldap-auth-config

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://hostname or IP[:port]/. ldaps:// or ldapi:// can also be used. The port number is optional. Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldap://192.168.2.101

<Ok>

○ dc=prova,dc=local

Configuring ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=DosNegrosYUnaBlanca,dc=local

<Ok>

○ Version 3 ldap

Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldaps. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3

2

<Ok>

○ YES

Configuring ldap-auth-config

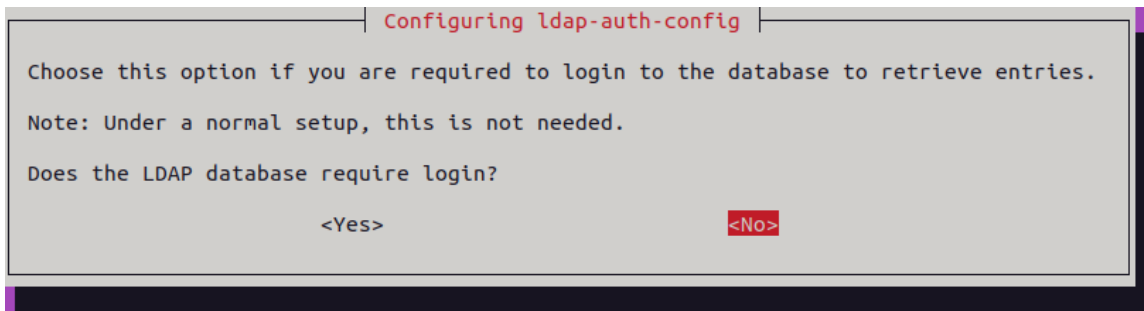
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords. The password will be stored in a separate file which will be made readable to root only. If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

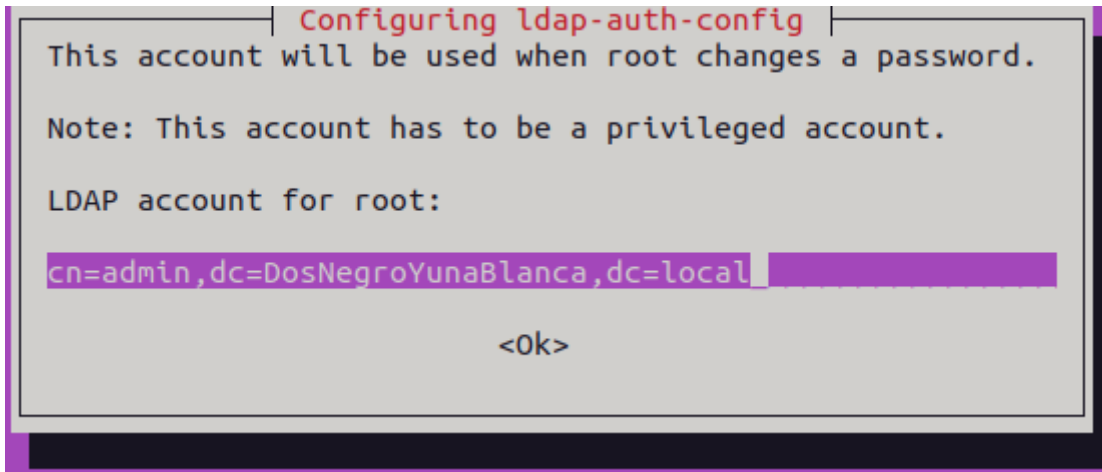
<Yes>

<No>

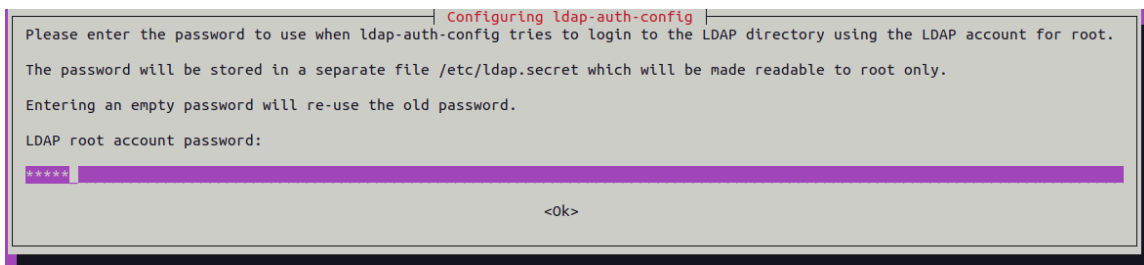
○ NO consultas de login



- cn=admin,dc=prova,dc=local

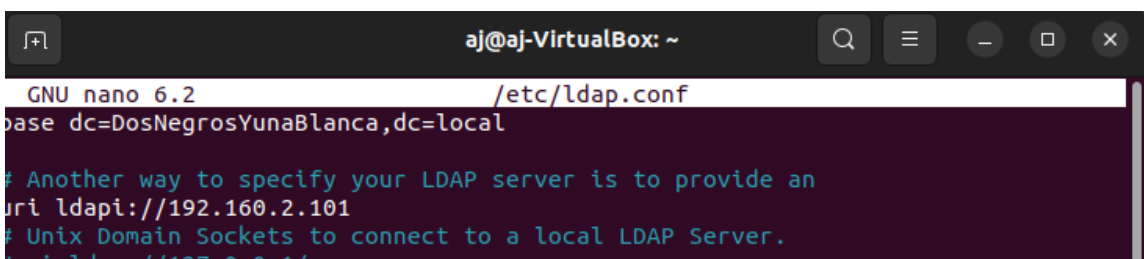


- Password



2.- A partir d'aquí hem de modificar tres fitxers:

- Primer fitxer: /etc/ldap.conf
 - Revisar línia: Uri ldap://192.168.0.102



- Ceram línia: #bind_policy hard

- La substituïm per: bind_policy soft

```
# immediately.  
bind_policy soft
```

- Ceram línia: pam_password md5

- La substituïm per: pam_password crypt

```
# necessary. This is the default.  
pam_password crypt  
  
# Hash password locally; required for Un  
# Windows LDAP servers, and works with t
```

- Segon fitxer: /etc/ldap/ldap.conf

- Localitzem el següent bloc d'informació:

```
#BASE dc=example,dc=com
```

```
#URI ldap://ldap.example.com ldap://ldap-master.example
```

```
#SIZELIMIT 12
```

```
#TIMELIMIT 15
```

```
#DEREF never
```

- Ho deixem d'aquesta manera:

```
BASE dc=prova,dc=local
```

```
URI ldap://ldap.prova.local
```

```
SIZELIMIT 0
```

```
TIMELIMIT 15
```

```
DEREF never
```

```

GNU nano 6.2 /etc/ldap/ldap.conf *
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE    dc=DosNegrosYunaBlanca,dc=local
#URI      ldap://ldap.DosNegrosYunaBlanca.local

SIZELIMIT    0
TIMELIMIT    15
DEREF        never

# TLS certificates (needed for GnuTLS)
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt

```

- Tercer fitxer: /etc/nsswitch.conf

- Localitzem el següent bloc d'informació:

Passwd: files systemd

Group: files systemd

Shadow: files

Gshadow: files

Hosts: files mdns4_minimal [NOTFOUND=return] dns

Networks: files

Protocols: db files

Services: db files

Ethers: db files

Rpc: db files

Netgroup nis

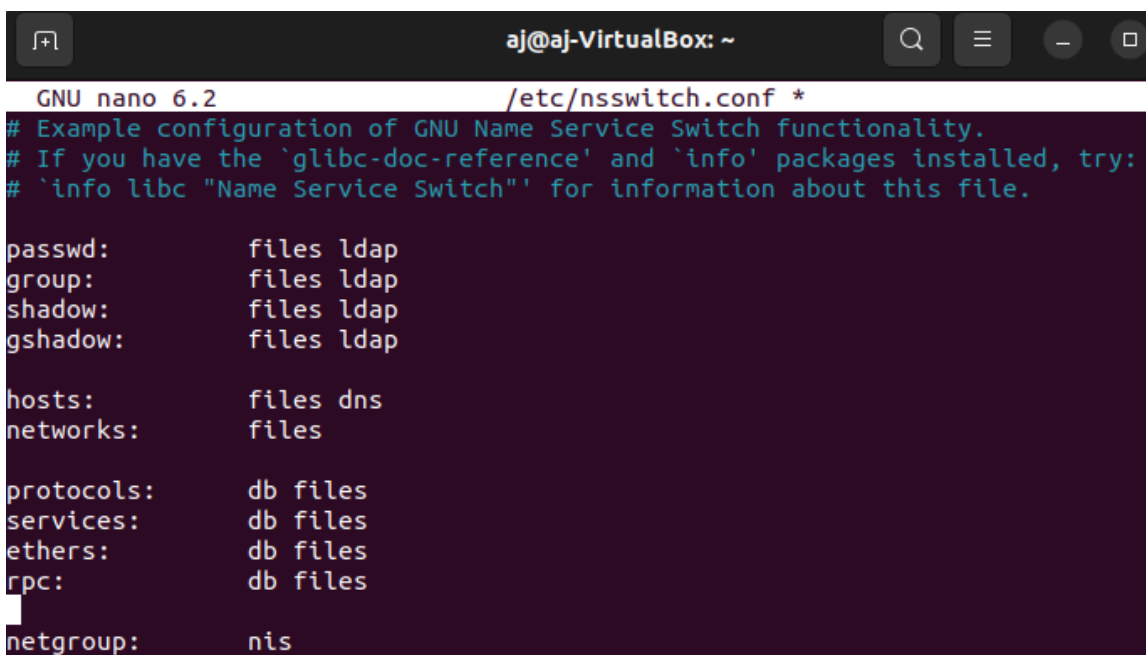
- Ho deixem d'aquesta manera:

Passwd: files ldap

Group: files ldap
Shadow: files ldap
Gshadow: files ldap

Hosts: files dns
Networks: files
Protocols: db files
Services: db files
Ethers: db files
Rpc: db files

Netgroup: nis



```
GNU nano 6.2 /etc/nsswitch.conf *
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

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

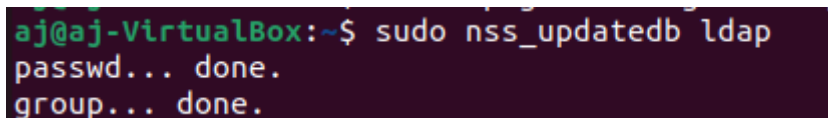
hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

3.- Llancem la següent ordre, per tal de carregar tota la base de dades del servidor LDAP dins del client.

- Sudo nss_updatedb ldap



```
aj@aj-VirtualBox:~$ sudo nss_updatedb ldap
passwd... done.
group... done.
```

4.- Llançem la següent ordre:

- getent passwd
 - Han d'aparèixer els usuaris creats dins del servidor LDAP.

```
Austin:x:2002:10000:Austin:/home/Austin:/bin/bash
aj@aj-VirtualBox:~$
```

5.- Actualitzem la base de dades:

- Sudo pam-auth-update

```
Austin:x:2002:10000:Austin:/home/Austin:/bin/bash
aj@aj-VirtualBox:~$ sudo pam-auth-update
```

6.- Editem dos fitxers:

- Primer fitxer: Sudo nano /etc/pam.d/common-session
 - Perquè al usuari quan inici sessió se li crei la carpeta personal.
- Agreguem a la primera línia:
 - session required pam_mkhomedir.so skel=/etc/skel/ umask=0022

```
aj@aj-VirtualBox: ~
GNU nano 6.2 /etc/pam.d/common-session *
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
#
```

- Segon fitxer: sudo nano /etc/pam.d/common-password
 - Cerquem la següent línia:
 - Password [success=1 user_unknown=ignore default=die] pam_ldap.so
(ha de quedar així, eliminem la part del darrera)

```
aj@aj-VirtualBox: ~
GNU nano 6.2 /etc/pam.d/common-password *
#for compatibility . The "obscure" option replaces the old
#'OBSCURE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password requisite pam_pwquality.so retry=3
password [success=3 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt
password sufficient pam_sss.so use_authtok
password [success=1 user_unknown=ignore default=die] pam_ldap.so
```